Algebraic Combinatorics

An International Conference in Honor of Eiichi Bannai's 60th Birthday

Sendai International Center
June 26–30, 2006

Algebraic Combinatorics

An International Conference in Honor of Eiichi Bannai's 60th Birthday

ORGANIZING COMMITTEE

Akihiro Munemasa, local organizer (Tohoku, Japan)
Mitsugu Hirasaka (Pusan, Korea)
Tatsuro Ito (Kanazawa, Japan)
Masanobu Kaneko (Fukuoka, Japan)
Izumi Miyamoto (Yamanashi, Japan)
Sung Yell Song (Ames, USA)

SPONSORS

Kyushu University COE Program

Graduate School of Information Sciences, Tohoku University

Preface

The conference "Algebraic Combinatorics" is an annual conference dedicated to topics in algebraic combinatorics, including association schemes, codes, designs, finite geometry, graphs, and groups. The conference in the year 2006, which was the 23rd of the series, was dedicated to the work of Eiichi Bannai in celebration of his 60th birthday.

Algebraic Combinatorics has seen a remarkable growth since the 1984 publication of Bannai and Ito's book, "Algebraic Combinatorics I: Association Schemes." Research development on this subject proceeded at an extraordinary pace in various directions in the last two decades. The main goal of the conference was to disseminate some of the recent developments on the subject to the mathematical community. The conference also had the objective to bring together Bannai's associates and other mathematicians, with strong personal and professional ties with him, to celebrate his career in tribute to his 60th birthday, and to discuss various emerging mathematical topics for which algebraic and combinatorial techniques are needed.

This volume consists of 37 papers presented at the conference. The topics of the volume reflect the wide range of areas to which Eiichi Bannai has made substantial contributions during his exemplary career.

We are very grateful for the generous financial support of Kyushu University COE program "Development of Dynamic Mathematics with High Functionality," Graduate School of Information Sciences of Tohoku University, and JSPS Grants-in-Aid for Scientific Research No.16340010 (Eiichi Bannai), No.18340022 (Tatsuro Ito) and No.17340020 (Akihiro Munemasa). Without their financial support, a conference of this magnitude would not have been possible.

The Organizers
January, 2007

Contents

Jack Koolen, On a conjecture of Bannai and Ito 13
Andries Brouwer, Connectivity of distance-regular graphs 17
William J. Martin, Some new constructions of imprimitive cometric association schemes 19
Diana Cerzo, Non-existence of imprimitive Q-polynomial schemes of exceptional type with $d = 4$ 32
Chih-wen Weng, Triangle-free distance-regular graphs 37
Akira Hiraki, A characterization of the odd graphs and the doubled odd graphs with a few of their intersection numbers 47
Alexandre A. Makhnev, On distance-regular graphs and their automorphisms 53
Jon-Lark Kim, Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles 57
Michael Giudici, Transitive decompositions of graphs 67
Sergei Evdokimov, Normal cyclotomic schemes over a finite commutative ring 72
Paul Terwilliger, The q-tetrahedron algebra 76
Ayumu Hoshino, Polyhedral realizations of crystal bases for quantum algebras 92
Kenichiro Tanabe, The fixed point subalgebra of the vertex operator algebra associated to the Leech lattice by an automorphism of order three 98
Tayuan Huang, A class of error-correcting pooling designs on complexes 107
Nachimuthu Manickam, A survey of results on distribution invariants of association schemes 113
Christine Bachoc, Upper bounds for the kissing number from semidefinite programming 119
Jiro Sekiguchi, An analogy between a real field and finite prime fields on six-line arrangement on a projective plane 136
Hao Shen, Embeddings of resolvable group divisible designs with block size 3 141
Chihiro Suetake, A contraction of divisible designs 146
Neil J. A. Sloane, Gleason's theorem on self-dual codes and its generalizations 151
Maria Carmen V. Amarra, $(1 - u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$ 170
Attila Sali, Codes that attain minimum distance in all possible directions 174
Romar B. dela Cruz, Hilbert series and free distance bounds for quaternary convolutional codes 185
Mikhail Klin, A family of Higmanian association schemes on 40 points: A computer algebra approach 190
Sung Y. Song, Group-case commutative association schemes and their character tables 204
Kanat Abdukhalikov, Association schemes related to universally optimal configurations 214
Koichiro Harada, Rediscovered theorems 218
Eiichi Bannai, On the zeros of Hecke type Faber polynomials 224
Patrick Solé, Double circulant codes from two class association schemes 262
Keisuke Shiromoto, Designs from subcode supports of linear codes 275

Hajime Tanaka, A new proof of the Assmus–Mattson theorem based on the Terwilliger algebra 284
Etsuko Bannai, New examples of Euclidean tight 4-designs 292
Masashi Shinohara, On three-distance sets in the three-dimensional Euclidean space . 301
Tatsuya Fujisaki, Trees and spanning trees on m-uniform hypergraphs 306
Fumihito Oda, A center of the Grothendieck ring Green functor 314
Brian Curtin, Isomorphisms and homomorphisms of graphs 321
Takuya Ikuta, An infinite class of non-symmetric spin models, potts models, and Hadamard matrices 326

List of Participants

Abdukhalikov, Kanat (Kyushu University, Japan)
Akiyama, Kenji (Fukuoka University, Japan)
Amarra, Maria Carmen V. (University of the Philippines, Philippines)
Ando, Kiyoshi (The University of Electro-Communications, Japan)
Araya, Makoto (Shizuoka University, Japan)
Asai, Tsunenobu (Kinki University, Japan)
Bachoc, Christine (Université Bordeaux, France)
Balmaceda, Jose Maria (University of the Philippines, Philippines)
Bannai, Eiichi (Kyushu University, Japan)
Bannai, Etsuko (Kyushu University, Japan)
Betsumiya, Koichi (Jobu University, Japan)
Betty, Rowena Alma (University of the Philippines, Philippines)
Brouwer, Andries (Eindhoven University of Technology, The Netherlands)
Cerzo, Diana (International Christian University, Japan)
Cheng, Shun-Jen (National Taiwan University, Taiwan)
Choi, Sul-young (Le Moyne College, USA)
Curtin, Brian (University of South Florida, USA)
van Dam, Edwin (Tilburg University, The Netherlands)
de Guzman, Eric (Yamagata University, Japan)
dela Cruz, Romar (University of the Philippines, Philippines)
Deza, Michel-Marie (CNRS, France)
Egawa, Yoshimi (Tokyo University of Science, Japan)
Endo, Yoshinori (Fukushima University, Japan)
Enomoto, Hikoe (Keio University, Japan)
Evdokimov, Sergei (Petersburg Department of Steklov Institute of Mathematics, Russia)
Feng, Rongquan (Peking University, China)
Fuji-Hara, Ryoh (University of Tsukuba, Japan)
Fujisaki, Tatsuya (Kyushu University, Japan)
Fujiwara, Yuichiro (Nagoya University, Japan)
Fukushima, Hiroshi (Gunma University, Japan)
Giudici, Michael (The University of Western Australia, Australia)
Hanaki, Akihide (Shinshu University, Japan)
Harada, Koichiro (The Ohio State University, USA)
Harada, Masaaki (Yamagata University, Japan)
Hasegawa, Koji (Tohoku University, Japan)
Hiraki, Akira (Osaka Kyoiku University, Japan)
Hiramine, Yutaka (Kumamoto University, Japan)
Hirasaka, Mitsugu (Pusan National University, Korea)
Hoshino, Ayumu (Sophia University, Japan)
Hosoya, Rie (International Christian University, Japan)
Huang, Tayuan (National Chiao-Tung University, Taiwan)
Ibukiyama, Tomoyoshi (Osaka University, Japan)
Ikuta, Takuya (Kobe Gakuin University, Japan)
Ishikawa, Masao (Tottori University, Japan)
Ito, Tatsuro (Kanazawa University, Japan)
Ivanov, Alexander A. (Imperial College, UK)

Imai, Hideo (Tohoku University, Japan)
Iwasaki, Shiro (Hitotsubashi University, Japan)
Jimbo, Masakazu (Nagoya University, Japan)
Jurišić, Aleksandar (IMFM, Slovenia)
Kamijo, Akira (Hokkaido University, Japan)
Kaneko, Masanobu (Kyushu University, Japan)
Ke, Wen-Fong (National Cheng Kung University, Taiwan)
Kido, Hiroaki (Kyushu University, Japan)
Kim, Jon-Lark (University of Louisville, USA)
Kitazume, Masaaki (Chiba University, Japan)
Kiyota, Masao (Tokyo Medical and Dental University, Japan)
Klin, Mikhail (Ben-Gurion University of the Negev, Israel)
Koolen, Jack (POSTECH, Korea)
Koshitani, Shigeo (Chiba University, Japan)
Lang, Michael (Bradley University, USA)
Makhnev, Alexander (The Ural Branch of the Russian Academy of Sciences, Russia)
Maki, Norimichi (Mizuho IR, Japan)
Manickam, Nachimuthu (DePauw University, USA)
Marrero, Osvaldo (Villanova University, USA)
Martin, William J. (Worcester Polytechnic Institute, USA)
Matsui, Hiroaki (Tohoku University, Japan)
Miao, Ying (University of Tsukuba, Japan)
Miezaki, Tsuyoshi (Kyushu University, Japan)
Miyabayashi, Hiroki (Yamagata University, Japan)
Miyamoto, Izumi (University of Yamanashi, Japan)
Miyamoto, Masahiko (University of Tsukuba, Japan)
Mizukawa, Hiroshi (National Defense Academy in Japan, Japan)
Munemasa, Akihiro (Tohoku University, Japan)
Nakagawa, Nobuo (Kinki University, Japan)
Nakamura, Kirio (Kobe University, Japan)
Nakashima, Yasuhiro (Tohoku University, Japan)
Niwasaki, Takashi (Ehime University, Japan)
Nomura, Kazumasa (Tokyo Medical and Dental University, Japan)
Nozaki, Hiroshi (Kyushu University, Japan)
Nozawa, Sohei (Chiba University, Japan)
Oda, Fumihito (Toyama National College of Technology, Japan)
Okada, Soichi (Nagoya University, Japan)
Onaga, Yoshishige (Hokkaido University, Japan)
Oura, Manabu (Kochi University, Japan)
Ozeki, Michio (Yamagata University, Japan)
Saito, Akira (Nihon University, Japan)
Sakurai, Katsuyoshi (Yamagata University, Japan)
Sali, Attila (Alfréd Rényi Institute of Mathematics, Hungary)
Sasaki, Hiroki (Shinshu University, Japan)
Sawa, Masanori (Nagoya University, Japan)
Sawabe, Masato (Chiba University, Japan)
Sekiguchi, Jiro (Tokyo University of Agriculture and Technology, Japan)
Shen, Hao (Shanghai Jiao Tong University, China)
Shigezumi, Junichi (Kyushu University, Japan)

Shimabukuro, Osamu (Fukushima National College of Technology, Japan)
Shimakura, Hiroki (Hokkaido University, Japan)
Shinoda, Kenichi (Sophia University, Japan)
Shinohara, Masashi (Kyushu University, Japan)
Shiromoto, Keisuke (Aichi Prefectural University, Japan)
Sloane, Neil J. A. (AT&T, USA)
Solé, Patrick (CNRS, France)
Song, Sung Yell (Iowa State University, USA)
Suetake, Chihiro (Oita University, Japan)
Sumi, Toshio (Kyushu University, Japan)
Suprijanto, Djoko (Kyushu University, Japan)
Suzuki, Hiroshi (International Christian University, Japan)
Tagami, Makoto (Kanazawa University, Japan)
Tagami, Yuki (Tohoku University, Japan)
Takegahara, Yugen (Muroran Institute of Technology, Japan)
Tamura, Hiroki (Tohoku University, Japan)
Tanabe, Kenichiro (Hokkaido University, Japan)
Tanaka, Hajime (Tohoku University, Japan)
Tanaka, Yasuhiko (Oita University, Japan)
Taniguchi, Tetsuji (Kyushu University, Japan)
Taya, Hisao (Tohoku University, Japan)
Terada, Junya (Shinshu University, Japan)
Terwilliger, Paul (University of Wisconsin, Madison, USA)
Tokushige, Norihide (Ryukyu University, Japan)
Tomiyama, Masato (Ishikawa National College of Technology, Japan)
Uno, Katsuhiro (Osaka Kyoiku University, Japan)
Wada, Tomoyuki (Tokyo University of Agriculture and Technology, Japan)
Waki, Katsushi (Yamagata University, Japan)
Watanabe, Toshihiro (Gifu University, Japan)
Weng, Chih-wen (National Chiao-Tung University, Taiwan)
Yamada, Hiromichi (Hitotsubashi University, Japan)
Yamaki, Hiroyoshi (Tsukuba, Japan)
Yamauchi, Hiroshi (The University of Tokyo, Japan)
Yokoyama, Kazuhiro (Rikkyo University, Japan)
Yoshiara, Satoshi (Tokyo Woman's Christian University, Japan)
Yoshida, Hitomi (Hokkaido University, Japan)
Yoshida, Tomoyuki (Hokkaido University, Japan)

Monday, June 26, 2006

Time	Speaker	Lecture Title
09:30 - 09:50		*Registration*
09:50 - 10:00		*Opening*
10:00 - 10:50	**Jack Koolen**	On a Conjecture of Bannai and Ito
10:50 - 11:10		*Break*
11:10 - 12:00	**Andries Brouwer**	Connectivity of Distance-Regular Graphs
12:00 - 14:00		*Lunch Break*
14:00 - 14:20	**William J. Martin**	Imprimitive Cometric Association Schemes
14:20 - 14:40	**Diana Cerzo**	On Imprimitive Q-Polynomial Schemes of Exceptional Type
14:40 - 15:00	**Chih-wen Weng**	Triangle-Free Distance-Regular Graphs
15:00 - 15:20		*Break*
15:20 - 15:40	**Akira Hiraki**	A Characterization of the Odd Graphs and the Doubled Odd Graphs With a Few of Their Intersection Numbers
15:40 - 16:00	**Alexandre A. Makhnev**	On Distance-Regular Graphs and Their Automorphisms
16:00 - 16:20	**Jon-Lark Kim**	Small Weight Codewords in LDPC Codes Defined by (Dual) Classical Generalized Quadrangles
16:20 - 16:40		*Break*
16:40 - 17:00	**Michael Giudici**	Transitive Decompositions of Graphs
17:00 - 17:20	**Sergei Evdokimov**	Normal Cyclotomic Schemes Over a Finite Commutative Ring

Tuesday, June 27, 2006

Time	Speaker	Lecture Title
09:10 - 10:00	**Paul Terwilliger**	The q-Tetrahedron Algebra
10:00 - 10:20		*Break*
10:20 - 10:40	**Ayumu Hoshino**	Polyhedral Realizations of Crystal Bases for Quantum Algebras
10:40 - 11:00	**Kenichiro Tanabe**	The Fixed Point Subalgebra of the Vertex Operator Algebra Associated to the Leech Lattice by an Automorphism of Order Three
11:00 - 11:20		*Break*
11:20 - 11:40	**Edwin van Dam**	Equidistant Latin Hypercube Designs
11:40 - 12:00	**Tayuan Huang**	Error-Correcting Pooling Designs Associated With Finite Geometries and Association Schemes
12:00 - 12:20	**N. Manickam**	Distribution Invariants of Association Schemes
12:20 - 14:10		*Lunch Break*
14:10 - 15:00	**Christine Bachoc**	Upper Bounds for the Kissing Number From Semi-Definite Programming
15:00 - 15:20		*Break*
15:20 - 15:40	**Rongquan Feng**	On the Ranks of Bent Functions
15:40 - 16:00	**Jiro Sekiguchi**	An Analogy Between a Real Field and Finite Prime Fields on Six-Line Arrangements on a Projective Plane
16:00 - 16:20	**Hao Shen**	Embeddings of Resolvable Group Divisible Designs
16:20 - 16:40		*Break*
16:40 - 17:00	**Chihiro Suetake**	A Contraction of Divisible Designs
17:00 - 17:20	**Hiroki Tamura**	Some Constructions of Almost D-Optimal Designs

Wednesday, June 28, 2006

Time	Speaker	Lecture Title
09:10 - 10:00	**Neil J. A. Sloane**	Gleason's Theorem on Self-Dual Codes and Its Generalizations
10:00 - 10:20		*Break*
10:20 - 10:40	**Maria Carmen V. Amarra**	$(1-u)$-Cyclic Codes Over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$
10:40 - 11:00	**Michio Ozeki**	Complete Coset Weight Enumeration of a Dual Pair in Binary Codes
11:00 - 11:20		*Break*
11:20 - 11:40	**Attila Sali**	Codes That Achieve Minimum Distance in All Directions
11:40 - 12:00	**Romar B. dela Cruz**	Hilbert Series and Free Distance Bounds for Quaternary Convolutional Codes
		Excursion After Lunch

Thursday, June 29, 2006

Time	Speaker	Lecture Title
09:10 - 10:00	**A.A. Ivanov**	Amalgams: A Machinery of the Modern Theory of Finite Groups
10:00 - 10:20		*Break*
10:20 - 11:10	**Mikhail Klin**	Computer Algebra Experimentation With Coherent Configurations and Association Schemes
11:10 - 11:30		*Break*
11:30 - 11:50	**Sung Y. Song**	Group-Case Primitive Commutative Association Schemes and Their Character Tables
11:50 - 12:10	**Kanat Abdukhalikov**	Association Schemes Related to Universally Optimal Configurations
12:10 - 14:00		**Group Photo**/*Lunch Break*
14:00 - 14:50	**Koichiro Harada**	Rediscovered Theorems
14:50 - 15:10		*Break*
15:10 - 16:00	**Michel Deza**	Elementary Elliptic (R, q)-Polycycles
16:00 - 16:20		*Break*
16:20 - 17:10	**Eiichi Bannai**	Title to be announced
18:00 -		*Conference Dinner*

Friday, June 30, 2006

Time	Speaker	Lecture Title
09:10 - 10:00	**Patrick Solé**	Double Circulant Codes From Two Class Association Schemes
10:00 - 10:20		*Break*
10:20 - 10:40	**Keisuke Shiromoto**	Designs From Subcode Supports of Linear Codes
10:40 - 11:00	**Hajime Tanaka**	A New Proof of the Assmus-Mattson Theorem Based on the Terwilliger Algebra
11:00 - 11:20		*Break*
11:20 - 11:40	**Etsuko Bannai**	New Examples of Euclidean Tight 4-Designs
11:40 - 12:00	**Masashi Shinohara**	On Three-Distance Sets in the Three-Dimensional Euclidean Space
12:00 - 14:00		*Lunch Break*
14:00 - 14:20	**Tatsuya Fujisaki**	Trees and Spanning Trees in m-Uniform Hypergraphs
14:20 - 14:40	**Sul-young Choi**	Antimiddles of Trees
14:40 - 15:00		*Break*
15:00 - 15:20	**Fumihito Oda**	A Center of the Grothendieck Ring Green Functor
15:20 - 15:40	**Brian Curtin**	Isomorphisms and Homomorphisms of Graphs
15:40 - 16:00	**Takuya Ikuta**	Some Spin Models of Index 4 and Potts Models

On a conjecture of Bannai and Ito

J. H. Koolen
Department of Mathematics, POSTECH
Hyoja-dong, Namgu, Pohang 790-784 Korea
e-mail: koolen@postech.ac.kr

September 10, 2006

1 Introduction

In their 1984 book Bannai and Ito conjectured that there are finitely many distance-regular graphs with fixed valency $k \geq 3$ [3, p.237].

The first result towards this conjecture is the Feit-Higman Theorem [10] which states that the girth of a generalized polygon is bounded by 12, unless the valency equals 2 in which case you obtain the ordinary polygons. Ito [11] classified the bipartite cubic distance-regular graphs. Using this result of Ito, Biggs et al. [8] were able to classify the cubic distance-regular graphs.

Bannai and Ito continued to work on this conjecture and in the series of papers [4], [5], [6] and [7], they showed that their conjecture holds for $k = 3, 4$, and also for the class of bipartite distance-regular graphs.

Also the result of Feit-Higman has been extended. For example Bannai and Ito, and, independently, Damerell showed that a Moore graph with valency $k \geq 3$ has diameter at most 2. Later this was extended to disatnce-regular graphs with diameter $D \geq 2$ and $(c_{D-1}, a_{D-1}, b_{D-1}) = (1, a_1, b_1)$. For those distance-regular graphs, it was shown by Banna-Ito, Damerell, Fuglister, Roos-Van Zanten and others that the diameter is bounded by 13.

In more recent years, Moulton and myself [13, 14], have shown that the Bannai-Ito conjecture is true for valency 10 and less, under the condition that there are no triangles in the graph.

Last year, Bang, Moulton and myself were able to remove the assumption triangle-free, see [1] . In [2] we showed that the Bannai-Ito conjecture holds

for the class of regular near polygons, and also for the class of geodetic distance-regular graphs (A graph is called *geodetic* if any two vertices are joined by a unique shortest path.). This extends the result of Bannai-Ito for the class of bipartite distance-regular graphs. The generalized polygons are a special case of regular near polygons, so it also extends the Feit-Higman Theorem.

2 Methods

Let Γ be a distance-regular graph with diameter D at least 2 and valency k. Let
$\mathtt{h} := \#\{i \mid (c_i, a_i, b_i) = (1, a_1, b_1)\}$,
and
$\mathtt{t} := \#\{i \mid (c_i, a_i, b_i) = (b_1, a_1, 1)\}$.
Then it is easy to see that if $\mathtt{t} \neq 0$, then $\{i \mid (c_i, a_i, b_i) = (b_1, a_1, 1)\} = \{D - \mathtt{t}, D - \mathtt{t} + 1, \ldots, D - 1\}$. The Bannai-Ito conjecture is equivalent to show that the diameter is bounded by a function of 2, and this is not possible if $k = 2$, as there are infinitely many polygons.
A.A. Ivanov [12] showed that $D \leq 4^{k}\mathtt{h}$. This implies that one only needs to show that $\mathtt{h}$ is bounded by k.
To show that $\mathtt{h}$ is bounded by a function in k, one of the tools one uses is that two algebraic conjugated eigenvalues must have the same multiplicity.

The idea of Bannai-Ito behind the proof that their conjecture holds for bipartite distance-regular graphs is as follows:
First they show the existence of an eigenvalue θ very close to $2\sqrt{k-1}$. Then they show that the multiplicity of θ is of the order $v/\mathtt{h}^3$, where v is the number of vertices of Γ. If $\mathtt{h}$ is large then θ has to have an algebraic conjugate η. Then either $|\eta| < 2\sqrt{k-1}$ or $|\eta| > 2\sqrt{k-1}$. In the first case they showed that the multiplicity of η is of order at least $v/\mathtt{h}$ and in the second case of order at most $va^{-\mathtt{h}}$, where $a > 1$ does not depend on η. So this shows that $\mathtt{h}$ can not too big.
For the general case it seems to hard to approximate the multiplicities of eigenvalues precise enough. Only if you assume that the intersection arrays behave well, then one can approximate the multiplicities well enough. This is the case for regular near polygons and geodetic distance-regular graphs. It would be interesting to show that for given C and $k \geq 3$ there are finitely

many distance-regular graphs with $\#\{i \mid c_i b_i \neq 1\} \leq C$.

References

[1] S. Bang, J. H. Koolen and V. Moulton, Two theorems concerning the Bannai-Ito conjecture, submitted.

[2] S. Bang, J. H. Koolen and V. Moulton, For fixed valency, there are finitely many regular near polygons and geodetic distance-regular graphs, submitted.

[3] E. Bannai and T. Ito, Algebraic combinatorics I: Association schemes, *Benjamin/Cummings, Menlo Park, CA*, 1984

[4] E. Bannai and T. Ito, On distance-regular graphs with fixed valency, *Graphs and Combinatorics* **3** 95–109, 1987

[5] E. Bannai and T. Ito, On distance-regular graphs with fixed valency III, *Journal of Algebra* **107** 43–52, 1987

[6] E. Bannai and T. Ito, On distance-regular graphs with fixed valency II, *Graphs and Combinatorics* **4** 219–228, 1988

[7] E. Bannai and T. Ito, On distance-regular graphs with fixed valency IV, *European Journal of Combinatorics* **10** 137–148, 1989

[8] N.L. Biggs, A.G. Boshier, J. Shawe-Taylor, Cubic distance-regular graphs, *J. London Math. Soc.* **33** 385–394, 1986.

[9] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, *Springer-Verlag, Berlin,* 1989

[10] W. Feit and G. Higman, The non-existence of certain generalized polygons, *Journal of Algebra* **1** 114–131, 1964

[11] T.Ito Bipartite distance-regular graphs of valency three, *Linear Algebra Appl.* **46** 195–213, 1982

[12] A. A. Ivanov, Bounding the diameter of a distance-regular graph, *Soviet Mathematics Doklady* **28** 149–152, 1983

[13] J. H. Koolen and V. Moulton, On a conjecture of Bannai and Ito: There are finitely many distance-regular graphs with degree 5,6 or 7, *European Journal of Combinatorics* **23** 987–1006, 2002

[14] J. H. Koolen and V. Moulton, There are finitely many triangle-free distance-regular graphs with degree 8,9 or 10, *Journal of Algebraic Combinatorics* **19** 205–217, 2004.

On the connectivity of distance-regular graphs

Andries E. Brouwer
Department of Mathematics, Techn. University Eindhoven,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands

July 2006

Executive summary

The vertex connectivity of a non-complete distance-regular graph of valency $k > 2$ equals k.

Discussion

A distance-regular graph of valency $k > 2$ is very connected. Problems to consider include:

(i) Expansion: If removing a set S of vertices disconnects the graph, and A is the vertex set of the smallest of the resulting components, can one give a lower bound for $|S|/|A|$ independent of the graph, but maybe only dependent on the diameter? Examples: removing 17 edges from the Biggs-Smith graph cuts it into two halves of size 51; removing the middle level (of size about $2^{2n}/\sqrt{\pi n}$) from the Hamming $2n$-cube cuts it into two halves.

(ii) Vertex connectivity: Show for a separating set of vertices S that $|S| \geq k$ with equality iff S is the set of neighbours of a vertex.

(iii) Connectedness of large subgraphs: Give sufficient conditions for $\Gamma_{\geq e}(\alpha)$ (the subgraph on the vertices at distance at least e to some vertex α) to be connected.

Partial answers:

(i) It is well-known that a graph is a good expander when its second largest eigenvalue θ is much smaller than the largest eigenvalue k. For distance-regular graphs of diameter 3 one has $\theta < \frac{1}{2}\sqrt{3}k$.

(ii) This was shown for diameter 2 by Brouwer & Mesner (1985). At the Sendai conference in honour of Eiichi Bannai's 60th birthday (2006) I announced this for diameter 3. In Brouwer & Haemers (2005) the edge-connectivity was determined: one has to remove at least k edges to disconnect, and if removal of precisely k edges disconnects the graph, then they are the edges incident with a single vertex. During the Sendai conference, Jack Koolen remarked that the techniques of that paper, together with those used for $d = 3$, probably suffice for the general case, and that turns out to be the case. A joint paper is in preparation.

(iii) In [1] it is shown that generalized polygons are connected far away from a vertex or flag, with the exception of a few small cases. This is important in the theory of buildings.

References

[1] A. E. Brouwer, *The complement of a geometric hyperplane in a generalized polygon is usually connected*, pp. 53–57 in: Finite geometry and combinatorics - Proc. Deinze 1992, F. De Clerck et al. (eds.), London Math. Soc. Lect. Note Ser. 191, Cambridge Univ. Press, 1993.

[2] A. E. Brouwer & W. H. Haemers, *Eigenvalues and perfect matchings*, Linear Alg. Appl. **395** (2005) 155–162.

[3] A. E. Brouwer & J. H. Koolen, *The vertex-connectivity of a distance-regular graph*, preprint.

[4] A. E. Brouwer & D. M. Mesner, *The connectivity of strongly regular graphs*, Europ. J. Combin. **6** (1985) 215-216.

Some new constructions of imprimitive cometric association schemes

William J. Martin
Department of Mathematical Sciences
and
Department of Computer Science
Worcester Polytechnic Institute
Worcester, Massachusetts
martin@wpi.edu

Mikhail Muzychuk
Department of Computer Science and Mathematics
Netanya Academic College
Netanya 42365 Israel
muzy@netanya.ac.il

Jason Williford
Department of Mathematical Sciences
Worcester Polytechnic Institute
Worcester, Massachusetts
jsw@wpi.edu

August 30, 2006

Dedicated to Professor Eiichi Bannai on the occasion of his 60$^{\text{th}}$ birthday.

Abstract

In a recent paper [9], the authors introduced the extended Q-bipartite double of an almost dual bipartite cometric association scheme. Since the association schemes arising from linked systems of symmetric designs are almost dual bipartite, this gives rise to a new infinite family of 4-class cometric schemes which are both Q-bipartite and Q-antipodal. These schemes, the schemes arising from linked systems, and all Q-polynomial bipartite distance-regular graphs enjoy a curious property: the relations restricted to any subcollection of the Q-antipodal classes is again a cometric association

scheme. We proved in [9] that this always holds for Q-antipodal schemes; we call such schemes "dismantlable". In this note, we explore a few examples of this phenomenon in more detail.

0.1 Outline of the paper

This paper has three meager goals. Mainly, we give an overview of the paper [9] by the same authors on which the talk in Sendai was based. In the process of doing this, we give a brief but self-contained account of linked systems of symmetric designs and a new family of 4-class Q-polynomial schemes based on them. Another goal is to discuss some specific examples of association schemes related to the results of [9].

1 Background material

Let $(X, \mathbf{A})$ be a symmetric d-class association scheme [1, 2] on v vertices with Schur idempotents $\mathbf{A} = \{A_0, \ldots, A_d\}$, primitive (ordinary) idempotents $E_0, \ldots, E_d$, eigenmatrices P and $Q = vP^{-1}$, valencies k_i and multiplicities m_j. When we say $(X, \mathbf{A})$ is *cometric* (or *Q-polynomial*), we imply that the ordering $E_0, E_1, \ldots, E_d$ is a Q-polynomial ordering. That is, the *Krein parameters* q_{ij}^k given by

$$E_i \circ E_j = \frac{1}{v} \sum_{k=0}^{d} q_{ij}^k E_k$$

(where $\circ$ denotes Schur — or entrywise — multiplication) satisfy

- $q_{ij}^k = 0$ whenever $k < |i - j|$ or $k > i + j$, and
- $q_{ij}^{i+j} > 0$ whenever $i + j \leq d$.

The parameters of a cometric scheme $(X, \mathbf{A})$ are entirely determined by its *Krein array*

$$\iota^*(X, \mathbf{A}) = \{b_0^*, b_1^*, \ldots, b_{d-1}^*; c_1^*, c_2^*, \ldots, c_d^*\}$$

where $b_j^* = q_{1,j+1}^j$, $c_j^* = q_{1,j-1}^j$ and we also define $a_j^* = q_{1j}^j = m_1 - b_j^* - c_j^*$.

A cometric scheme is *Q-bipartite* if all $a_j^* = 0$. This is equivalent to the condition that $q_{ij}^k = 0$ whenever $i + j + k$ is odd. A cometric scheme is *Q-antipodal* if $b_j^* = c_{d-j}^*$ for all j except possibly $j = \lfloor \frac{d}{2} \rfloor$.

An association scheme is *imprimitive* if some graph in the scheme is disconnected. As is well-known, it follows in this case that some union of relations is a non-trivial equivalence relation on X. In the next theorem and henceforth, we will let I_w (or simply I) denote the $w \times w$ identity matrix and J_r (or J) will denote the all ones matrix of order $r \times r$.

Theorem 1.1 (see [1, 2]). *The following are equivalent:*

(i) $(X, \mathbf{A})$ *is imprimitive;*

(ii) *for some $j > 0$, E_j has repeated columns;*

(iii) *for some subset $\mathcal{I} = \{i_0 = 0, i_1, \ldots, i_s\}$ of $\{0, 1, \ldots, d\}$ and some ordering of the vertices $\sum_{h=0}^{s} A_{i_h} = I_w \otimes J_r$ for some integers w and r with $v = wr$, $1 < w, r < v$;*

(iv) *for some subset $\mathcal{J} = \{j_0 = 0, j_1, \ldots, j_s\}$ of $\{0, 1, \ldots, d\}$ and some ordering of the vertices $\sum_{h=0}^{s} E_{j_h}$ has form $\frac{1}{r}(I_w \otimes J_r)$ for some integers w and r with $v = wr$, $1 < w, r < v$.*

(v) *The Bose-Mesner algebra $\mathcal{A}$ of the scheme contains a proper Schur-closed subalgebra of dimension at least two not containing I.*

The same scheme may have several such imprimitivity systems and our language must distinguish them; for example, the vertex set of a scheme which is Q-antipodal admits a partition into "Q-antipodal classes" and a scheme which is Q-bipartite has a "Q-bipartite imprimitivity system" which partitions the vertices into "dual bipartite classes". (If we are to further develop a theory of cometric schemes which are not distance-regular graphs, there is probably a need for more appropriate terminology.) In each case, we will use r for the size of a class and $w = v/r$ for the number of such classes in this partition. As above, the set $\mathcal{I}$ contains all indices $0 \leq i \leq d$ for which A_i has all zeros on blocks indexed by distinct classes and the set $\mathcal{J}$ contains all indices $0 \leq j \leq d$ for which E_j has all columns indexed by any class identical.

Theorem 1.2 (Suzuki [12]). *Suppose (X,A) is an imprimitive cometric association scheme. Then one of the following holds:*

- *$(X, \mathbf{A})$ is Q-bipartite and $\mathcal{J} = \{0, 2, 4, \ldots\}$;*
- *$(X, \mathbf{A})$ is Q-antipodal and $\mathcal{J} = \{0, d\}$;*
- *$d = 4$, $\iota^*(X, \mathbf{A}) = \{m, m-1, 1, b_3^*; 1, c_2^*, m - b_3^*, 1\}$ and $\mathcal{J} = \{0, 3\}$;*
- *$d = 6$, $\iota^*(X, \mathbf{A}) = \{m, m-1, 1, b_3^*, b_4^*, 1; 1, c_2^*, m - b_3^*, 1, c_5^*, m\}$ (where $a_2^* = a_4^* + a_5^*$) and $\mathcal{J} = \{0, 3, 6\}$.* □

At this Sendai conference, Cerzo and Suzuki [6] showed that there are no association schemes of the third type in the list. No examples are known of the last type, either.

If $(X, \mathbf{A})$ is cometric with Q-polynomial ordering $0, 1, \ldots, d$, then the entries in column 1 of the matrix Q are all distinct and we may define a *natural ordering* on the relations by the requirement that $Q_{01} > Q_{11} > \cdots > Q_{d1}$. We will use this throughout the paper.

2 Overview of results

In this section, we give the results of [9] without proofs.

2.1 The extended Q-bipartite double

Our first result is a construction dual to the "extended bipartite double" construction of [2, Sec. 1.11].

We begin with the bipartite double. If we take any scheme with associate matrices A_i and primitive idempotents E_j $(0 \le i, j \le d)$, then the bipartite double has associate matrices

$$A_i^+ = \begin{bmatrix} A_i & 0 \\ 0 & A_i \end{bmatrix} \qquad \text{and} \qquad A_i^- = \begin{bmatrix} 0 & A_i \\ A_i & 0 \end{bmatrix}$$

and primitive idempotents

$$E_j^+ = \frac{1}{2}\begin{bmatrix} E_j & E_j \\ E_j & E_j \end{bmatrix} \qquad \text{and} \qquad E_j^- = \frac{1}{2}\begin{bmatrix} E_j & -E_j \\ -E_j & E_j \end{bmatrix}.$$

A cometric scheme $(X, \mathbf{A})$ is *almost dual bipartite* if $a_j^* = 0$ for $j < d$ but $a_d^* \neq 0$. Bannai and Ito [1, p315] proved that the bipartite double of an almost dual bipartite cometric scheme is cometric as well, with Q-polynomial ordering $E_0^+, E_1^-, E_2^+, E_3^-, \ldots, E_0^-$. The Hermitian forms dual polar space graphs $[{}^2A_{2d-1}(r)]$ give an infinite family of examples, with arbitrarily large diameter, where this bipartite double is cometric but not metric. The scheme we now describe in Theorem 2.1(i) is called the *extended Q-bipartite double*.

Theorem 2.1. *Let $(X, \mathbf{A})$ be a d-class cometric association scheme on v vertices with primitive idempotents E_j and Krein parameters a_j^*, b_j^*, c_j^* satisfying $b_j^* + c_{j+1}^* = m_1 + 1$ for $0 \le j < d$. Then*

(i) *there exists an association scheme $(\hat{X}, \hat{\mathbf{A}})$ on $2v$ vertices where $\hat{X} = X \times \{0, 1\}$ and*

$$\hat{\mathbf{A}} = \left\{ A_0^+,\ A_1^+ + A_d^-,\ A_2^+ + A_{d-1}^-,\ \ldots,\ A_0^- \right\}$$

where $A_0, A_1, A_2, \ldots$ is the natural ordering of Schur idempotents in the original scheme. Moreover, this is a Q-bipartite cometric scheme with Q-polynomial ordering

$$E_0^+,\ E_0^- + E_1^-,\ E_1^+ + E_2^+,\ E_2^- + E_3^-,\ \ldots,\ E_d^{\pm}$$

where the last matrix is E_d^+ if d is odd and E_d^- if d is even;

(ii) *the idempotent $E_1 + E_2$ generates a cometric fusion scheme $(X, \bar{\mathbf{A}})$ of the original scheme $(X, \mathbf{A})$; this is the Q-bipartite quotient of the scheme $(\hat{X}, \hat{\mathbf{A}})$.*

The Krein array for the fusion scheme in part (ii) is

$$\iota^*(X, \hat{\mathbf{A}}) = \left\{ m_1 + m_2, \frac{b_1^* b_2^*}{c_2^*}, \frac{b_3^* b_4^*}{c_2^*}, \ldots, \frac{b_{d-2}^* b_{d-1}^*}{c_2^*};\ 1, \frac{c_3^* c_4^*}{c_2^*}, \frac{c_5^* c_6^*}{c_2^*}, \ldots, \frac{c_d^*(m_1+1)}{c_2^*} \right\}$$

when d is odd and

$$\iota^*(X, \hat{\mathbf{A}}) = \left\{ m_1 + m_2, \frac{b_1^* b_2^*}{c_2^*}, \frac{b_3^* b_4^*}{c_2^*}, \ldots, \frac{b_{d-3}^* b_{d-2}^*}{c_2^*};\ 1, \frac{c_3^* c_4^*}{c_2^*}, \frac{c_5^* c_6^*}{c_2^*}, \ldots, \frac{c_{d-1}^* c_d^*}{c_2^*} \right\}$$

when d is even.

Example 2.2 (A. Munemasa, personal communication). *The Soicher graph Σ for $M_{22}:2$ is a distance-regular graph of diameter three having intersection array $\iota(\Sigma) = \{110, 81, 12; 1, 18, 90\}$. The underlying association scheme (X, A) is cometric with Krein array $\iota^*(X, \mathrm{A}) = \{55, 49, 21; 1, 7, 35\}$ so Theorem 2.1(i) applies. We then obtain a 4-class scheme which is both metric and cometric. This distance-regular graph was discovered by Meixner and has intersection array $\{176, 135, 24, 1; 1, 24, 135, 176\}$. If A_0, A_1, A_2, A_3 are the distance matrices of the Soicher graph, then Munemasa observed that the adjacency matrix of the Meixner graph can be expressed as*

$$A_1^+ + A_3^- = \begin{bmatrix} A_1 & A_3 \\ A_3 & A_1 \end{bmatrix}$$

as in part **(i)** *of the theorem.* □

Several open parameter sets for diameter three cometric distance-regular graphs also satisfy the conditions of Theorem 2.1. These include

$$\begin{array}{rr} v = 322 & \{60, 45, 8;\ 1, 12, 50\} \\ v = 392 & \{69, 56, 10;\ 1, 14, 60\} \\ v = 378 & \{78, 50, 9;\ 1, 15, 60\} \\ v = 800 & \{119, 100, 15;\ 1, 20, 105\} \\ v = 900 & \{174, 110, 18;\ 1, 30, 132\}. \end{array}$$

Example 2.3. *The block scheme of the 4-$(11, 5, 1)$ Witt design is a cometric scheme with Krein array $\iota^*(X, \mathrm{A}) = \{10, \frac{242}{27}, \frac{11}{5};\ 1, \frac{55}{27}, \frac{44}{5}\}$. Clearly the conditions of Theorem 2.1(i) are met. But the extended Q-bipartite double of this scheme is already well-known: it is the block scheme of the 5-$(12, 6, 1)$ Witt design with Krein array $\iota^*(X, \mathrm{A}) = \{11, 10, \frac{242}{27}, \frac{11}{5}; 1, \frac{55}{27}, \frac{44}{5}, 11\}$. By the same token, the induced association scheme on the even subcode of the perfect binary Golay code (i.e., the dual scheme of the coset graph of the perfect code), with Krein array $\iota^*(X, \mathrm{A}) = \{23, 22, 21;\ 1, 2, 3\}$, has as its extended Q-bipartite double the induced scheme on the extended binary Golay code with Krein array $\iota^*(X, \mathrm{A}) = \{24, 23, 22, 21;\ 1, 2, 3, 24\}$.*

2.2 Linked systems of symmetric designs

A *symmetric* (v, k, λ) *design* [8] is an incidence structure based on two disjoint sets $\mathcal{P}_1$ and $\mathcal{P}_2$ of v objects each, called *points* and *blocks*, respectively, such that

- each block is incident with k points;
- any two distinct blocks are incident with λ common points;
- each point is incident with k blocks;
- any two distinct points are incident with λ common blocks;
- the design is non-degenerate: $0 < \lambda < k < v$.

Clearly the definition is symmetric in the role of points and blocks. The incidence graph G of such a design is a bipartite distance-regular graph of diameter three with intersection array $\iota(G) = \{k, k-1, k-\lambda; 1, \lambda, k\}$. Such an incidence graph is always cometric and every bipartite distance-regular graph with diameter three arises in this way. If we order the eigenvalues of G in decreasing order,

$$k > \sqrt{n} > -\sqrt{n} > -k$$

where $n = k - \lambda$ is the *order* of the design, this yields a Q-polynomial ordering E_0, E_1, E_2, E_3 of the primitive idempotents for the Bose-Mesner algebra $\mathcal{A}$ of the scheme. (Note that E_0, E_2, E_1, E_3 is a second Q-polynomial ordering.) The rank of E_1 is $m_1 = v - 1$. This is a Q-antipodal 3-class scheme with Q-antipodal imprimitivity system $\{\mathcal{P}_1, \mathcal{P}_2\}$. For more information on symmetric designs, the reader is referred to Lander's monograph [8].

We now summarize some material from [4] and [10]. A *linked system of ℓ symmetric (v, k, λ) designs* is a graph G defined on a vertex set

$$X = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \cdots \cup \mathcal{P}_{\ell+1}$$

where $\pi = \{\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{\ell+1}\}$ is a partition of X into $\ell + 1$ sets of size v each, enjoying the following properties:

1. partition π is a proper coloring of G: no edge of G has both ends in the same class $\mathcal{P}_i$;
2. for any $i \neq j$, the subgraph of G induced on $\mathcal{P}_i \cup \mathcal{P}_j$ is the incidence graph of a symmetric (v, k, λ) design;
3. for any three distinct classes $\mathcal{P}_i, \mathcal{P}_j, \mathcal{P}_k$, the number of common neighbors of a vertex x in $\mathcal{P}_i$ and a vertex y in $\mathcal{P}_j$ which lie in $\mathcal{P}_k$ depends only on whether x and y are adjacent in G or not; it does not depend on the choice of x and y nor on the choice of i, j and k.

Let σ denote the number of common neighbors in $\mathcal{P}_k$ of x in $\mathcal{P}_i$ and y, adjacent to x, in $\mathcal{P}_j$ $(i \neq j \neq k \neq i)$. Let τ denote the same parameter for x and y non-adjacent in G. Then we have, by double-counting

$$\{(x, y, z) |\ x \sim z \sim y,\ y \in \mathcal{P}_j,\ z \in \mathcal{P}_k\}$$

for fixed $x \in \mathcal{P}_i$,

$$k\sigma + (v - k)\tau = k^2. \tag{2.1}$$

In determining σ and τ, Cameron [4] next considers the blocks M_{ij} of the adjacency matrix of G:

$$A_1 = \begin{bmatrix} 0 & M_{12} & M_{13} & \cdots \\ M_{21} & 0 & M_{23} & \cdots \\ M_{31} & M_{32} & 0 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

where $M_{ji} = M_{ij}^T$ is the submatrix recording adjacencies in G from vertices in $\mathcal{P}_j$ to vertices in $\mathcal{P}_i$. Noting that

$$\det(M_{ij}) = \det(M_{ij}^T) = kn^{\frac{v-1}{2}}$$

for all $i \neq j$, he takes determinants of both sides of the equation

$$M_{ik}M_{jk}^T = (\sigma - \tau)M_{ij} + \tau J$$

to obtain

$$k^2 n^{v-1} = kn^{\frac{v-1}{2}}(\sigma - \tau)^{v-1}\frac{1}{k}(k\sigma + (v-k)\tau).$$

Using Equation (2.1) and simplifying, we find

$$(\tau - \sigma)^2 = n,$$

yielding

$$\sigma = \frac{1}{v}\left(k^2 \pm \sqrt{n}(v-k)\right), \qquad \tau = \frac{k}{v}\left(k \mp \sqrt{n}\right)$$

where signs are chosen appropriately to make σ and τ integers. It follows from $k^2 \equiv n \bmod v$ and $v > 2n$ that at most one choice of signs gives us integer values for σ and τ. Replacing the designs by their complements yields a complementary system of linked $(v, v-k, v-2k+\lambda)$-designs. Note that the complementary system has the same order n, but the signs in the corresponding formulae for its σ and τ are opposite to the ones of the original system. Thus we can always assume that

$$\sigma = \frac{1}{v}(k^2 - \sqrt{n}(v-k)), \ \tau = \frac{k}{v}(k + \sqrt{n}).$$

Note that this fixes $\tau - \sigma$ to be $\sqrt{n}$, and we can no longer assume $2k < v$ as is customary in design theory.

Assume now that G is a linked system of ℓ symmetric (v, k, λ) designs. Since σ is an integer, $\ell > 1$ implies that the order $n = k - \lambda$ is a perfect square. We then obtain a 3-class association scheme $(X, \mathbf{B})$ with associate matrices

$$B_0 = I, \quad B_1 = A(\tilde{G}), \quad B_2 = A(G_2), \quad B_3 = A(G)$$

where G_2 is the union of the $\ell + 1$ complete graphs on the Q-antipodal classes $\mathcal{P}_i$ and $\tilde{G}$ is the multipartite complement of G; this is a linked system of ℓ symmetric $(v, v-k, v-2k+\lambda)$ designs. These matrices satisfy

$$B_i B_j = \sum_{h=0}^{3} p_{ij}^h B_h$$

where the intersection numbers p_{ij}^h, first given by Mathon [10], are recorded in the matrices $L_i = [p_{ij}^h]_{h,j}$ below:

$$L_1 = \begin{bmatrix} 0 & \ell(v-k) & 0 & 0 \\ 1 & \frac{\ell-1}{v}\left[(v-k)^2 + k\sqrt{n}\right] & v-k-1 & (\ell-1)\frac{k}{v}\left[v-k-\sqrt{n}\right] \\ 0 & \ell(v-2k+\lambda) & 0 & \ell(k-\lambda) \\ 0 & (\ell-1)\frac{v-k}{v}\left[v-k-\sqrt{n}\right] & v-k & (\ell-1)\frac{v-k}{v}\left[k+\sqrt{n}\right] \end{bmatrix},$$

$$L_2 = \begin{bmatrix} 0 & 0 & v-1 & 0 \\ 0 & v-k-1 & 0 & k \\ 1 & 0 & v-2 & 0 \\ 0 & v-k & 0 & k-1 \end{bmatrix},$$

$$L_3 = \begin{bmatrix} 0 & 0 & 0 & \ell k \\ 0 & (\ell-1)\frac{k}{v}[v-k-\sqrt{n}] & k & (\ell-1)\frac{k}{v}[k+\sqrt{n}] \\ 0 & \ell(k-\lambda) & 0 & \ell\lambda \\ 1 & (\ell-1)\frac{v-k}{v}[k+\sqrt{n}] & k-1 & \frac{\ell-1}{v}[k^2-(v-k)\sqrt{n}] \end{bmatrix}.$$

(Trivially, $L_0 = I$.) The eigenmatrices for this scheme are then

$$P = \begin{bmatrix} 1 & \ell(v-k) & v-1 & \ell k \\ 1 & \ell\sqrt{n} & -1 & -\ell\sqrt{n} \\ 1 & -\sqrt{n} & -1 & \sqrt{n} \\ 1 & k-v & v-1 & -k \end{bmatrix}, \qquad Q = \begin{bmatrix} 1 & v-1 & \ell(v-1) & \ell \\ 1 & \frac{k}{\sqrt{n}} & -\frac{k}{\sqrt{n}} & -1 \\ 1 & -1 & -\ell & \ell \\ 1 & \frac{k-v}{\sqrt{n}} & \frac{v-k}{\sqrt{n}} & -1 \end{bmatrix}$$

and the Krein array is $\iota^*(X, \mathbf{B}) = \{b_0^*, b_1^*, b_2^*; c_1^*, c_2^*, c_3^*\}$ where

$$b_0^* = c_3^* = m = v-1, \qquad b_1^* = \ell c_2^* = \frac{\ell}{\ell+1}\left(v-2+\frac{1}{\sqrt{n}}(v-2k)\right), \qquad b_2^* = c_1^* = 1.$$

For $\ell > 1$, the scheme is no longer metric and there is only one Q-polynomial ordering of the primitive idempotents. In the matrices above, we have used the natural ordering of relations, ensuring $Q_{01} > Q_{11} > Q_{21} > Q_{31}$.

2.3 New family of 4-class Q-antipodal Q-bipartite schemes

Let $\mathbf{B} = \{B_0, B_1, B_2, B_3\}$ be the associate matrices of the association scheme arising from a linked system of symmetric designs on vertex set X with parameters

$$v = 16s^2, \qquad n = 4s^2, \qquad k = 2s(4s-1), \qquad \lambda = 2s(2s-1)$$

where s is a positive integer. (From above, for $\ell > 1$, we need the order n to be a square. We will need $v = 2k + 2\sqrt{n}$ in order to ensure $b_1^* + c_2^* = m_1 + 1$. So our design must satisfy $v = 4n$ and n must be even for p_{11}^1 to be integral when ℓ is even.) Now applying Theorem 2.1, we obtain the following:

Theorem 2.4. *Let $(X, \mathbf{B})$ be a linked system of symmetric designs with parameters $v = 16s^2$, $k = 2s(4s-1)$ and $\lambda = 2s(2s-1)$ and let $Y = X \times \{0,1\}$. Consider $\mathbf{A} = \{A_0 = I, A_1, A_2, A_3, A_4\}$ given by*

$$A_1 = \begin{bmatrix} B_3 & B_1 \\ B_1 & B_3 \end{bmatrix}, \quad A_2 = \begin{bmatrix} B_2 & B_2 \\ B_2 & B_2 \end{bmatrix}, \quad A_3 = \begin{bmatrix} B_1 & B_3 \\ B_3 & B_1 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 0 & I \\ I & 0 \end{bmatrix}.$$

Then $(Y, \mathbf{A})$ is a 4-class Q-antipodal Q-bipartite cometric association scheme.

The Krein array for this scheme is $\iota^*(Y, \mathbf{A}) = \{v, v-1, \ell\frac{v}{\ell+1}, 1;\ 1, \frac{v}{\ell+1}, v-1, v\}$ which shows that any such scheme is both Q-bipartite and Q-antipodal.

Now we demonstrate that there are linked systems of designs known which satisfy the conditions of the above theorem.

In fact, only one infinite family of linked systems of symmetric designs is known [4]. A description of these linked systems based on the Kerdock codes is cited in [4] as private communication from J. M. Goethals. The first published description is based on the "Cameron-Seidel scheme" [5].

The Cameron-Seidel scheme corresponds to a system of $\ell = 2^{2t+1} - 1$ linked symmetric $(2^{2t+2}, 2^{2t+1} - 2^t, 2^{2t} - 2^t)$ designs, where t can be any positive integer. So, by deleting Q-antipodal classes, we obtain a system of ℓ such linked designs for any $\ell < 2^{2t+1}$. Each of these systems has order $n = k - \lambda = 2^{2t}$ an even square and $v = 4n$. So the construction given in Theorem 2.4 applies and we have an infinite family of 4-class Q-antipodal Q-bipartite cometric association schemes with $s = 2^{t-1}$ in the language above.

We note that the Krein parameters are easily computed from the second eigenmatrix Q:

$$Q = \begin{bmatrix} 1 & v & (\ell+1)(v-1) & \ell v & \ell \\ 1 & 2^{t+1} & 0 & -2^{t+1} & -1 \\ 1 & 0 & -\ell-1 & 0 & \ell \\ 1 & -2^{t+1} & 0 & 2^{t+1} & -1 \\ 1 & -v & (\ell+1)(v-1) & -\ell v & \ell \end{bmatrix}.$$

The Krein array is given above. An important feature to note is that, unless $\ell + 1$ divides v, the Krein parameter $c_2^* = q_{11}^2$ is non-integral. So these schemes cannot be duals of metric schemes in general. Moreover, for $\ell > 1$, the schemes cannot be metric since they are Q-antipodal with more than two Q-antipodal classes.

2.4 Structure of Q-bipartite schemes

A bipartite distance-regular graph obviously has $w = 2$ bipartite halves; the next theorem is dual to this.

Theorem 2.5 ([3]). *If $(X, \mathbf{A})$ is Q-bipartite with w dual bipartite classes of size r each, then $r = 2$.*

A special case of this result has been known for some time: a Q-polynomial antipodal distance-regular graph must be a double cover of its folded graph [2, Theorem 8.2.4].

Still assuming the natural ordering on relations, in the Q-bipartite case with vertices ordered so that dual bipartite pairs appear consecutively, this gives $A_0 + A_d = I_{v/2} \otimes J_2$. Moreover, the dual bipartite classes are mapped via $u_1 : v \mapsto E_1 v$ to opposing points on lines through the origin in V_1 (or in $\mathbb{R}^m$). This observation gives us the following two corollaries.

Corollary 2.6 ([9]). *Let $(X, \mathbf{A})$ be a Q-bipartite cometric association scheme with the natural ordering on relations. Then, for the first eigenspace, the sequence $m_1 = Q_{01} > Q_{11} > \cdots > Q_{d1}$ is symmetric about the origin. In particular, $Q_{\frac{d}{2},1} = 0$ whenever d is even.*

Corollary 2.7 ([9]). *Let $(X, \mathbf{A})$ be a Q-bipartite cometric association scheme with natural ordering on relations. Then the intersection numbers satisfy*

$$p_{ij}^k = p_{i,d-j}^{d-k}$$

for all $0 \leq i, j, k \leq d$.

2.5 Structure of Q-antipodal schemes

Gardiner proved (cf. [2, Prop. 4.2.2]): for any antipodal distance-regular graph of valency k, the index r of the cover is bounded above by k. Therefore, we expect the number, w, of Q-antipodal classes to be bounded above by the first multiplicity, m_1. The following result is a bit weaker.

Theorem 2.8 ([9]). *Let $(X, \mathbf{A})$ be a d-class Q-antipodal association scheme with w Q-antipodal classes of size r each. If d is odd, then $w \leq m_1$. If d is even, then $w \leq m_2$.*

Considering sign change patterns in columns of the matrix Q, we use some results on Sturm sequences to obtain the following:

Corollary 2.9 ([9]). *In any d-class Q-antipodal scheme, $\lfloor \frac{d}{2} \rfloor$ non-trivial relations occur between vertices in the same Q-antipodal class and $\lceil \frac{d}{2} \rceil$ relations occur between classes. Namely, for i odd, the partition into Q-antipodal classes is a proper vertex coloring of graph G_i and for i even, each component of G_i lies entirely within some Q-antipodal class.*

The intersection numbers of Q-antipodal schemes behave in a manner similar to those of bipartite graphs.

Corollary 2.10 ([9]). *Let $(X, \mathbf{A})$ be a Q-antipodal cometric association scheme with relations ordered naturally. Then the intersection numbers satisfy*

$$p_{ij}^k = 0$$

unless either $i + j + k$ is even or ijk is odd.

A Q-antipodal cometric association scheme with Q-antipodal classes $X_1, \ldots, X_w$ is *dismantlable* if, for any proper subset $\{X_{i_1}, \ldots, X_{i_{w'}}\}$ of its Q-antipodal classes the set of induced graphs $(G_i)_{Y \times Y}$ where $0 \leq i \leq d$ and $Y = X_{i_1} \cup \cdots \cup X_{i_{w'}}$ is again an association scheme. For $w' = 1$, it is a standard result (originally due to Rao, Ray-Chaudhuri and Singhi - see [2, Section 2.4]) that we find a subscheme on each X_i and these all have the same parameters. (Here, we call this the *local scheme*.)

Theorem 2.11. *Every Q-antipodal scheme is dismantlable. The subscheme induced on any non-trivial collection of w' Q-antipodal classes is cometric for $w' \geq 1$ and Q-antipodal with d classes for $w' > 1$.*

Example 2.12. *The first example in the family constructed in Theorem 2.4 has 96 vertices. Here, we study a smaller example, which is somewhat degenerate. We begin with a 3-class scheme on 12 vertices which comes from the symmetric $(4,3,2)$ design (3-cube). (While, under an appropriate ordering of idempotents, $k > i + j$ implies $q_{ij}^k = 0$, this scheme is not cometric). Our 4-class scheme has twenty-four vertices and $m_1 = 4$.*

While the positioning of one bipartite half of the vertices of a regular 3-cube in $\mathbb{R}^3$ uniquely determines the location of the remaining four vertices, for the 4-cube in $\mathbb{R}^4$, there are two solutions for the placement of the "black vertices" given feasible coordinates for all the white vertices. What is more, these two sets of 8 black vertices themselves form a regular Euclidean 4-cube. What we have just described is the geometry of the first eigenspace of our association scheme. The twenty-four points so described in $\mathbb{R}^4$ are the vertices of the well-known 24-cell. Since the polytope is antipodal, the association scheme is also Q-bipartite.

The Q-antipodal classes for this scheme are the three 8-sets described above, each of which has a 16-cell (or hyperoctahedron) as its convex hull. The Q-antipodal property is reflected in the relative positioning of these three 8-vertex polyhedra. Between any two Q-antipodal classes, the induced subgraph of the graph corresponding to the matrix A_1 in our scheme is the graph of the 4-cube $H(4,2)$. It is easy to check that there is no way to pack a fourth 16-cell into this configuration and retain the pairwise relationships we have described. We believe that this Euclidean packing problem is at the heart of the study of Q-antipodal cometric schemes. □

Example 2.13. *The coset graph of the shortened ternary Golay code, labeled (A17) in [2, p365] has intersection array $\{20, 18, 4, 1; 1, 2, 18, 20\}$; this is an antipodal distance-regular graph belonging to a translation scheme. The dual association scheme is Q-antipodal on $v = 243$ vertices with $w = 3$ Q-antipodal classes. Removing one of these, we obtain a Q-antipodal scheme on 162 vertices having $w = 2$ Q-antipodal classes which is not metric. Note that this scheme has parameters*

$$d = 4,\ v = 162,\ \iota^*(X, \mathbf{A}) = \{20, 18, 3, 1; 1, 3, 18, 20\}$$

formally dual to those of an unknown diameter four bipartite distance-regular graph, but it is not realizable as a translation scheme.

Example 2.14. *The same idea applied to graphs labeled (A16) and (A18) on page 365 of [2] yield new Q-antipodal schemes with parameters*

$$d = 5,\ v = 486,\ \iota^*(X, \mathbf{A}) = \{22, 20, \frac{27}{2}, 2, 1;\ 1, 2, \frac{27}{2}, 20, 22\},\ w = 2$$

$$d = 6,\ v = 1536,\ \iota^*(X, \mathbf{A}) = \{21, 20, 16, 8, 2, 1;\ 1, 2, 4, 16, 20, 21\},\ w = 3.$$

On the same page of [2], the dual of this last scheme is ruled out by counting hexagons.

We briefly mention some more special cases of Theorem 2.11. A Q-polynomial distance-regular graph is Q-antipodal if and only if it is bipartite. The Q-antipodal classes are

precisely the $w = 2$ bipartite color classes. The induced configuration on either one of these classes has long been known to be a cometric association scheme (see [2, Prop. 4.2.2] and preceding discussion). So the theorem is trivial in the metric case. It clearly also holds (by definition) for any linked system of symmetric designs and therefore also for the new family of 4-class schemes introduced in Section 2.2.

The octahedron is a Q-antipodal scheme with $r = 2$ and $w = 3$. In this case, $m_1 = 3$ while $m_1 = 2$ for any induced subscheme on $w' = 2$ Q-antipodal classes. In spite of this, for Q-antipodal schemes with three or more classes, these two multiplicities coincide.

Theorem 2.15 ([9]). *For a Q-antipodal d-class association scheme with $d \geq 3$ and w Q-antipodal classes of size r, the first multiplicity m_1 does not depend on w but only on the parameters of the local scheme.*

Indeed, bounds much better than that given in Theorem 2.8 are known in the case of linked systems of symmetric designs (i.e., $d = 3$). For example, we have the trivial bound $w \leq 2$ when n is not a square. Moreover, since $m_2 = (w-1)m_1$ in this case, we obtain

$$1 + m_2 = 1 + (w-1)m_1 \leq \operatorname{rank}(E_1 \circ E_1) \leq \frac{1}{2}m_1(m_1+1)$$

giving $w \leq \frac{m_1+2}{2}$. Mathon [10] and Noda [11] give stronger bounds for the number of linked symmetric (v, k, λ) designs, but only in the case when the quantity $(\sigma - \tau)(v - 2k)$ is positive. For example, we note that their bounds do not apply to the case $v = 36$, $n = 9$.

In the paper [9], we give a list of all cometric association schemes known to us which are not metric. Another version of this list is maintained on the web at `http://users.wpi.edu/~martin/RESEARCH/QPOL/`.

References

[1] E. Bannai and T. Ito. Algebraic Combinatorics I: Association Schemes. Benjamin-Cummings, Menlo Park (1984).

[2] A. E. Brouwer, A. M. Cohen and A. Neumaier. Distance-Regular Graphs. Springer-Verlag, Berlin (1989).

[3] A. E. Brouwer, C. D. Godsil, J. H. Koolen and W. J. Martin. Width and dual width of subsets in metric and cometric association schemes. *J. Combin. Th. Ser. A* **102** (2003), 255-271.

[4] P. J. Cameron. On groups with several doubly-transitive permutation representations. *Math. Z.* **128** (1972), 1-14.

[5] P. J. Cameron and J. J. Seidel. Quadratic forms over GF(2). *Proc. Koninkl. Nederl. Akademie van Wetenschappen, Series A*, Vol. 76 *Indag. Math.*, **35** (1973), 1-8.

[6] D. Cerzo and H. Suzuki. On imprimitive Q-polynomial schemes of exceptional type. Preprint, 2006.

[7] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Repts. Suppl.* **10** (1973).

[8] E. S. Lander. Symmetric Designs: An Algebraic Approach. London Math. Soc. Lecture Note Series, no. 74, Cambridge Univ. Press, Cambridge (1983).

[9] W. J. Martin, M. Muzychuk and J. S. Williford. Imprimitive cometric association schemes: constructions and analysis. *To appear, J. Alg. Combin.*, 2006 preprint.

[10] R. Mathon. The systems of linked 2-(16,6,2) designs. *Ars Comb.* **11** (1981), 131–148.

[11] R. Noda R. On homogeneous system of linked symmetric designs. *Math. Z.* **138** (1974), 15-20.

[12] H. Suzuki. Imprimitive Q-polynomial association schemes. *J. Alg. Combin.* **7** (1998), no. 2, 165–180.

Non-existence of Imprimitive Q-polynomial Schemes of Exceptional Type with $d = 4$

DIANA CERZO* and HIROSHI SUZUKI†
Department of Mathematics, International Christian University
Mitaka, Tokyo 181-8585, Japan

June 24, 2006

Abstract

In [3], it was shown that an imprimitive Q-polynomial scheme $\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$ is either dual bipartite, dual antipodal or of class 4 or 6. In this paper, it will be shown that the scheme of class 4 does not occur using the integrality conditions of the entries of the first eigenmatrix of $\mathcal{X}$. These integrality conditions arise from the fact that $\mathcal{X}$ has exactly one Q-polynomial ordering [4].

1 Introduction

It was shown that an imprimitive P-polynomial scheme is either antipodal or bipartite. (See for example [1, 2]). A similar classification for Q-polynomial schemes was obtained by the second author in [3]. He showed that they are either dual antipodal or dual bipartite or of class $d = 4$ or $d = 6$ with dual intersection arrays, given respectively by

$$\iota^*(\mathcal{X}) = \begin{Bmatrix} * & 1 & c_2^* & m - b_3^* & 1 \\ 0 & 0 & a_2^* & 0 & m-1 \\ m & m-1 & 1 & b_3^* & * \end{Bmatrix}$$

where $a_2^* \neq 0$, and

$$\iota^*(\mathcal{X}) = \begin{Bmatrix} * & 1 & c_2^* & c_3^* & 1 & c_5^* & m \\ 0 & 0 & a_4^* + a_5^* & 0 & a_4^* & a_5^* & 0 \\ m & m-1 & 1 & b_3^* & b_4^* & 1 & * \end{Bmatrix}$$

where $a_2^* = a_4^* + a_5^* \neq 0$.

In this paper, we will eliminate the case $d = 4$ using the integrality conditions of the entries of the first eigenmatrix of $\mathcal{X}$. These integrality conditions arise from the fact that $\mathcal{X}$ has exactly one Q-polynomial ordering [4].

*Email: g066722yamata.icu.ac.jp, dianne_cerzoyahoo.com
†Electronic mail: hsuzuki@icu.ac.jp

2 Non-existence of the scheme with $d = 4$

Throughout the rest of this paper, we suppose that $\mathcal{Y} = (Y, \{R_i\}_{0 \le i \le d})$ is the association scheme of class 4, $m > 2$, with dual intersection array

$$\iota^*(\mathcal{X}) = \begin{Bmatrix} * & 1 & c & m-b & 1 \\ 0 & 0 & m-c-1 & 0 & m-1 \\ m & m-1 & 1 & b & * \end{Bmatrix}$$

where $m - c - 1 \neq 0$.

Lemma 1 *Let $\mathcal{X}$ be a Q-polynomial scheme with Q-idempotent E_1, $K = \boldsymbol{Q}(\{p_i(j) \mid 0 \le i, j \le d\})$. Then the following holds:*

(i) *$K/\boldsymbol{Q}$ is a Galois extension;*

(ii) *for any Galois automorphism σ of $K/\boldsymbol{Q}$*

$$E_1^\sigma = \frac{1}{|X|} \sum_{i=0}^{d} q_1(i)^\sigma A_i$$

generates $\mathcal{M}$ under Hadamard multiplication;

(iii) *If $\mathcal{X}$ has exactly one Q-polynomial ordering, then $[K : \boldsymbol{Q}] = 1$ and all the entries of the first eigenmatrix are integers;*

(iv) *If $\mathcal{X}$ has another Q-polynomial ordering, then $[K : \boldsymbol{Q}] = 2$;*

Proof.

(i) Since a Galois extension is a normal extension of characteristic 0, we only show that K is a normal extension of $\mathbf{Q}$. Let $\sigma : K \longrightarrow \overline{\mathbf{Q}}$ be an injective homomorphism, where $\overline{\mathbf{Q}}$ denotes the algebraic closure of $\boldsymbol{Q}$. Let σ act on E_i entry-wise. Clearly $(E_i \circ E_j)^\sigma = E_i^\sigma \circ E_j^\sigma$. It is easy to verify that $(E_i E_j)^\sigma = E_i^\sigma E_j^\sigma$. Thus, for all $0 \le i, j \le d$,

$$\begin{aligned} (E_i E_j)^\sigma &= \delta_{ij} E_j^\sigma, \\ {E_0}^\sigma + E_1^\sigma + \cdots + E_d^\sigma &= I, \\ E_i^\sigma &= \frac{1}{|X|} \sum_{i=0}^{d} q_i(j)^\sigma A_j. \end{aligned} \tag{1}$$

Hence, $\{E_0^\sigma, E_1^\sigma, \ldots, E_d^\sigma\} = \{E_0, E_1, \ldots, E_d\}$, i.e. σ permutes $E_0, E_1, \ldots, E_d$. Let $E_i^\sigma = E_{i^\sigma}$. Since $(A_i E_j)^\sigma = (p_i(j) E_j)^\sigma$, then $A_i E_{j^\sigma} = p_i(j)^\sigma E_{j^\sigma}$. This implies that $p_i(j)^\sigma = p_i(j^\sigma)$. Therefore, $K^\sigma = K$ and $K/\boldsymbol{Q}$ is a Galois extension.

(ii) Let σ be in $\mathrm{Gal}(K/\boldsymbol{Q})$. Clearly $E_i^\sigma = v_i^{*\sigma}(E_1^\sigma)$ where $v_i^{*\sigma}(x)$ denotes the polynomial obtained by applying σ to the coefficients of $v_i^*(x)$. Thus, E_1^σ generates the Bose-Mesner algebra $\mathcal{M}$.

(iii) & (iv) Suppose that $\sigma \in \mathrm{Gal}(K/Q)$ and $E_1^\sigma = E_1$. Note that

$$\mathrm{Span}\{E_0, E_1, E_1 \circ E_1\} = \mathrm{Span}\{E_0, E_1, E_2\} \tag{2}$$

and this subspace of $\mathcal{M}$ is closed under ordinary multiplication. Since $(E_1 \circ E_1)^\sigma = E_1 \circ E_1$, $E_0^\sigma = E_0$, and $E_1^\sigma = E_1$, applying σ to both sides of (2), we have

$$\langle E_0, E_1, (E_1 \circ E_1)\rangle = \langle E_0, E_1, {E_2}^\sigma\rangle.$$

Hence ${E_2}^\sigma = E_2$ as E_2 is an idempotent. Doing this inductively for the rest of the E_i's, we have $E_i^\sigma = E_i$ for all $0 \le i \le d$. Thus, $q_i(j)^\sigma = q_i(j)$ for all i, j which implies that $p_j(i)^\sigma = p_j(i)$, i.e. σ fixes K. Hence $\sigma = \mathrm{id}$.

Suppose that $\mathcal{X}$ has exactly one Q-polynomial ordering. Then, from (ii), for any $\sigma \in \mathrm{Gal}(K/Q)$, $E_1^\sigma = E_1$. Thus, from the above paragraph, $\mathrm{Gal}(K/Q) = [K : Q] = 1$. Note that since all entries of the P-matrix are algebraic integers, these must be integers.

Suppose that $\mathcal{X}$ is Q-polynomial with respect to E_j, where $j \neq 1$. Let $\sigma \neq \mathrm{id}$. Since E_1^σ generates $\mathcal{M}$, $E_1^\sigma = E_j$. Let $\tau \in \mathrm{Gal}(K/Q)$. By (ii), either $E_1^\tau = E_1$ or $E_1^\tau = E_j$. If $E_1^\tau = E_1$, $\tau = \mathrm{id}$. Suppose that $E_1^\tau = E_j$. Then ${E_1}^{\tau\sigma^{-1}} = E_1$ which implies that $\tau\sigma^{-1} = \mathrm{id}$. Therefore $\tau = \sigma$. Thus, $\mathrm{Gal}(K/Q) = 2$ and $[K : Q] = 2$. ∎

Lemma 2 *The scheme $\mathcal{Y}$ has eigenmatrices given by the following:*

$$P = \begin{bmatrix} 1 & r_1 n & r_2 n & r_3 n & m \\ 1 & \alpha_1 & \alpha_2 & \alpha_3 & -1 \\ 1 & \frac{\alpha_1^3 m^2 - m(r_1 n)^2 \alpha_1}{(nr_1)^3(m-1)} & \frac{\alpha_2^3 m^2 - m(r_2 n)^2 \alpha_2}{(nr_2)^3(m-1)} & \frac{\alpha_3^3 m^2 - m(r_3 n)^2 \alpha_3}{(nr_3)^3(m-1)} & -1 \\ 1 & -r_1 & -r_2 & -r_3 & m \\ 1 & \frac{r_1^2 n}{r_1 n(m-1) - \alpha_1 m} & \frac{r_2^2 n}{r_2 n(m-1) - \alpha_2 m} & \frac{r_3^2 n}{r_3 n(m-1) - \alpha_3 m} & -1 \end{bmatrix}$$

$$Q = \begin{bmatrix} 1 & m & \frac{m(m-1)}{c} & n & bn \\ 1 & \frac{\alpha_1 m}{r_1 n} & \frac{(\alpha_1 m)^2 - m(r_1 n)^2}{c(r_1 n)^2} & -1 & \frac{br_1 n}{r_1 n(m-1) - \alpha_1 m} \\ 1 & \frac{\alpha_2 m}{r_2 n} & \frac{(\alpha_2 m)^2 - m(r_2 n)^2}{c(r_2 n)^2} & -1 & \frac{br_2 n}{r_2 n(m-1) - \alpha_2 m} \\ 1 & \frac{\alpha_1 m}{r_3 n} & \frac{(\alpha_3 m)^2 - m(r_3 n)^2}{c(r_3 n)^2} & -1 & \frac{br_3 n}{r_3 n(m-1) - \alpha_3 m} \\ 1 & -1 & -\frac{mr_2 n}{c} & n & bn \end{bmatrix},$$

where $m = \mathrm{rank}\, E_1$, $n = m_3$, and

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \tag{3}$$

$$r_1 + r_2 + r_3 = m + 1. \tag{4}$$

Proof. Note that

$$B_0^* + B_3^* = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & \frac{m-1}{c} & \frac{m-1}{c} & 0 & \frac{m-1}{c} \\ \frac{m(m-1)}{(m-b)c} & 0 & 0 & \frac{m(m-1)}{(m-b)c} & 0 \\ 0 & \frac{m-1}{(m-b)c} & \frac{m-1}{(m-b)c} & 0 & \frac{m-1}{(m-b)c} \end{bmatrix}$$

has rank 2. Thus, by the isomorphism $\gamma : \mathcal{M} \to \mathcal{M}'$, $E_0 + E_3$ is also of rank 2. Since $E_0 + E_3 = \sum_{i \in \mathcal{I}} A_i$, $|\mathcal{I}| = 2$ and we may assume that $\mathcal{I} = \{0, 4\}$.

Therefor we have

$$r(E_0 + E_3) = (A_0 + A_4), \tag{5}$$

where $r = 1 + k_4$. Therefore we have

$$\begin{aligned} p_0(i) + p_4(i) &= 0 \qquad (i = 1, 2, 4), \\ p_0(3) + p_4(3) &= r. \end{aligned}$$

Hence, $p_4(i) = -1$ $(i = 1, 2, 4)$ and $p_4(0) = k_4 = p_4(3)$. Since

$$A_4 = \sum_{i=0}^{d} p_4(i) E_i = k_4 E_0 - E_1 - E_2 + k_4 E_3 - E_4, \tag{6}$$

$$\begin{aligned} E_1 \circ A_4 &= E_1 \circ (k_4 E_0 - E_1 - E_2 + k_4 E_3 - E_4) \\ &= \frac{1}{|X|} \left[-m E_0 + (r - m) E_1 + (r - m) E_2 - m E_3 + (r - 1) E_4 \right]. \end{aligned} \tag{7}$$

Also,

$$E_1 \circ A_4 = \frac{q_1(4)}{|X|} A_4 = \frac{q_1(4)}{|X|} (k_4 E_0 - E_1 - E_2 + k_4 E_3 - E_4). \tag{8}$$

Equating the coefficients of E_0 and E_1 in (7) and (7), we obtain

$$q_1(4) = -\frac{m}{r - 1} \text{ and } -q_1(4) = r - m$$

which implies that $r = 1 + m$ and $k_4 = m$.

By orthogonality and (5),

$$\begin{aligned} q_0(i) + q_3(i) &= 0 \qquad (i = 1, 2, 3) \\ q_0(0) + q_3(0) &= q_0(4) + q_3(4) = \frac{|X|}{1 + m} = 1 + n, \end{aligned}$$

where $n = m_3$. Hence $q_3(i) = -1$ $(i = 1, 2, 3)$ and $q_3(4) = n$.

Let $p_i(1) = \alpha_i$ and $p_i(3) = -r_i$ for $i = 1, 2, 3$. Then we have

$$k_i = r_i n, \quad q_1(i) = \frac{\alpha_i m}{r_i n} \tag{9}$$

for $i = 1, 2, 3$ and $q_1(4) = -1$. Note that $r_i > 0$ as $k_i = r_i n$ $(i = 1, 2, 3)$.

Since $PQ = |X| I$, the sum of the entries in the ith row $(i \neq 1)$ must be zero. Hence

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \tag{10}$$

$$r_1 + r_2 + r_3 = m + 1. \tag{11}$$

Since $q_1(i)^2 = m - c q_2(i)$,

$$q_2(i) = v_2^*(q_1(i)) = \frac{q_1(i)^2 - m}{c} = \frac{(\alpha_i m)^2 - m(r_i n)^2}{c(r_i n)^2}.$$

Since

$$E_1 \circ E_4 = \frac{1}{|X|}(bE_3 + (m-1)E_4),$$

we have for $1 \leq i \leq 4$,

$$\begin{aligned} q_1(i)q_4(i) &= bq_3(i) + (m-1)q_4(i) \\ q_4(i) &= \frac{-bq_3(i)}{m-1-q_1(i)}. \end{aligned}$$

In particular,

$$m_4 = q_4(0) = \frac{-bn}{m-1-m} = bn.$$

Hence for $1 \leq i \leq 4$,

$$\begin{aligned} p_i(4) &= \frac{-bq_3(i)k_i}{(m-1-q_1(i))m_4} = \frac{-q_3(i)k_i}{n(m-1-q_1(i))} = \frac{r_i n}{n(m-1-\frac{\alpha_i m}{r_i n})} \\ &= \frac{r_i^2 n}{r_i n(m-1)-\alpha_i m}. \end{aligned}$$

The rest of the entries of the eigenmatrices can be solved easily. ∎

Theorem 3 *The scheme with $d = 4$ does not occur.*

Proof. By inspection of B_i^* $(2 \leq i \leq 4)$, or by using [4, Theorem 2], it is easy to see that $\mathcal{Y}$ has exactly one Q-polynomial ordering. By Lemma 1, all entries of the first eigenmatrix P are integers. In particular, $\alpha_1, \alpha_2, \alpha_3$ are integers and r_1, r_2, r_3 are positive integers.

Since $\mathcal{Y}$ is Q-polynomial, $q_1(1)$, $q_1(2)$, $q_1(3)$ are distinct. Thus, some of the α_i's are nonzero. Hence by (3), at least one of them is negative. Set $\alpha = \alpha_i < 0$ and $r' = r_i$. Then

$$1 \leq \frac{r'^2 n}{(m-1)rn - \alpha m} < \frac{r'^2 n}{(m-1)rn} = \frac{r'}{m-1}.$$

Thus, $r' > m-1$. Since r' and m are integers, $r' \geq m$. However, since $r_i \geq 1$ $(0 \leq i \leq 3)$, by (4), $r' < m$. Therefore the scheme with $d = 4$ does not occur. ∎

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I.* Benjamin-Cummings, California, 1984.

[2] A. E. Brouwer, A. M. Cohen, and A. Neumaier, *Distance-Regular Graphs.* Spring Verlag, Berlin, 1989.

[3] H. Suzuki, Imprimitive Q-polynomial association Schemes, J. Alg. Combin. 7 (1998), no. 2, 165–180.

[4] H. Suzuki, Association Schemes with multiple Q-polynomial structures, J. Alg. Combin. 7 (1998), no. 2, 181–196.

Triangle-free Distance-regular Graphs *

Yeh-jong Pan † Min-hsin Lu ‡ Chih-wen Weng ‡

September 5, 2006

1 Introduction

We will prove the following two theorems.

Theorem 1.1. *Let Γ denote a distance-regular graph with diameter $d \geq 3$ and intersection numbers $a_1 = 0$, $a_2 \neq 0$. Then the following (i)-(iii) are equivalent.*

(i) Γ is Q-polynomial and Γ contains no parallelograms of length 3.

(ii) Γ is Q-polynomial and Γ contains no parallelograms of any length i for $3 \leq i \leq d$.

(iii) Γ has classical parameters (d, b, α, β) with $b < -1$.

Theorem 1.2. *With the notation and assumptions of Theorem 1.1, suppose (i)-(iii) hold. Then each of*

$$\frac{b(b+1)^2(b+2)}{c_2}, \quad \frac{(b-2)(b-1)b(b+1)}{2+2b-c_2} \tag{1.1}$$

is an integer. Moreover

$$c_2 \leq b(b+1). \tag{1.2}$$

*Work partially supported by the National Science Council of Taiwan, R.O.C.

†Department of Applied Mathematics National Chiao Tung University 1001 Ta Hsueh Road Hsinchu, Taiwan 30010, R.O.C. Email: yjpan@mail.tajen.edu.tw Fax: +886-3-5724679

‡Department of Applied Mathematics, National Chiao Tung University, Taiwan R.O.C.

2 Preliminaries

The following two theorems about distance-regular graphs with the Q-polynomial property and with classical parameters will be used in this paper.

Theorem 2.1. *[6, Theorem 3.3] Assume Γ is Q-polynomial with respect to a primitive idempotent E, and let $\theta_0^*, \ldots, \theta_d^*$ denote the corresponding dual eigenvalues. Then the following (i), (ii) hold.*

(i) For all integers $1 \leq h \leq d$, $0 \leq i, j \leq d$ and for all $x, y \in X$ such that $\partial(x, y) = h$,

$$\sum_{\substack{z \in X \\ \partial(x,z)=i \\ \partial(y,z)=j}} E\hat{z} - \sum_{\substack{z \in X \\ \partial(x,z)=j \\ \partial(y,z)=i}} E\hat{z} = p_{ij}^h \frac{\theta_i^* - \theta_j^*}{\theta_0^* - \theta_h^*}(E\hat{x} - E\hat{y}). \tag{2.1}$$

(ii) For an integer $3 \leq i \leq d$,

$$\theta_{i-2}^* - \theta_{i-1}^* = \sigma(\theta_{i-3}^* - \theta_i^*) \tag{2.2}$$

for appropriate $\sigma \in \mathbb{R} \setminus \{0\}$.

Theorem 2.2. *[6, Theorem 4.2] Let Γ denote a distance-regular graph with diameter $d \geq 3$. Choose $b \in \mathbb{R} \setminus \{0, -1\}$. Then the following (i), (ii) are equivalent.*

(i) Γ is Q-polynomial with associated dual eigenvalues $\theta_0^*, \theta_1^*, \ldots, \theta_d^*$ satisfying

$$\theta_i^* - \theta_0^* = (\theta_1^* - \theta_0^*) \begin{bmatrix} i \\ 1 \end{bmatrix} b^{1-i} \quad \text{for} \quad 1 \leq i \leq d.$$

(ii) Γ has classical parameters (d, b, α, β) for some real constants α, β.

Pick an integer $2 \leq i \leq d$. By a *parallelogram* of length i in Γ, we mean a 4-tuple $xyzw$ of vertices of X such that

$$\partial(x, y) = \partial(z, w) = 1, \quad \partial(x, z) = i,$$
$$\partial(x, w) = \partial(y, w) = \partial(y, z) = i - 1.$$

See Figure 1.

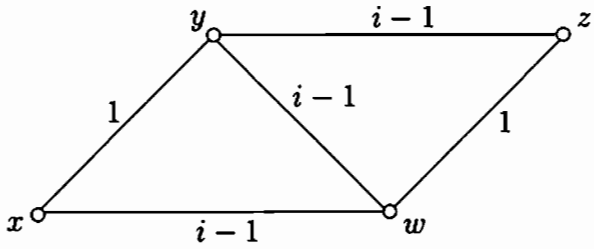


Figure 1: A parallelogram of length i.

3 Proof of Theorem 1.1

In this section we prove our first main theorem. We start with a lemma.

Lemma 3.1. *Let Γ denote a Q-polynomial distance-regular graph with diameter $d \geq 3$ and intersection number $a_1 = 0$. Fix an integer i for $2 \leq i \leq d$ and three vertices x, y, z such that*

$$\partial(x,y) = 1, \quad \partial(y,z) = i-1, \quad \partial(x,z) = i.$$

Then the quantity

$$s_i(x,y,z) := |\Gamma_{i-1}(x) \cap \Gamma_{i-1}(y) \cap \Gamma_1(z)| \tag{3.1}$$

is equal to

$$a_{i-1}\frac{(\theta_0^* - \theta_{i-1}^*)(\theta_2^* - \theta_i^*) - (\theta_1^* - \theta_{i-1}^*)(\theta_1^* - \theta_i^*)}{(\theta_0^* - \theta_{i-1}^*)(\theta_{i-1}^* - \theta_i^*)}. \tag{3.2}$$

In particular (3.1) is independent of the choice of the vertices x, y, z.

Proof. Let $s_i(x,y,z)$ denote the expression in (3.1) and set

$$\ell_i(x,y,z) = |\Gamma_i(x) \cap \Gamma_{i-1}(y) \cap \Gamma_1(z)|.$$

Observe

$$s_i(x,y,z) + \ell_i(x,y,z) = a_{i-1}. \tag{3.3}$$

By (2.1) we have

$$\sum_{\substack{w \in X \\ \partial(y,w)=i-1 \\ \partial(z,w)=1}} E\hat{w} - \sum_{\substack{w \in X \\ \partial(y,w)=1 \\ \partial(z,w)=i-1}} E\hat{w} = a_{i-1}\frac{\theta_{i-1}^* - \theta_1^*}{\theta_0^* - \theta_{i-1}^*}(E\hat{y} - E\hat{z}). \tag{3.4}$$

Taking the inner product of (3.4) with $\hat{x}$ using the assumption $a_1 = 0$, we obtain

$$s_i(x,y,z)\theta^*_{i-1} + \ell_i(x,y,z)\theta^*_i - a_{i-1}\theta^*_2 = a_{i-1}\frac{\theta^*_{i-1} - \theta^*_1}{\theta^*_0 - \theta^*_{i-1}}(\theta^*_1 - \theta^*_i). \tag{3.5}$$

Solving $s_i(x,y,z)$ by using (3.3) and (3.5), we get (3.2). □

From Lemma 3.1, $s_i(x,y,z)$ is a constant for any vertices x, y, z with $\partial(x,y) = 1$, $\partial(y,z) = i-1$, $\partial(x,z) = i$.

Definition 3.2. We let s_i denote the expression in (3.1). Note that $s_i = 0$ if and only if Γ contains no parallelograms of length i.

The proof of the following lemma is essentially in [7].

Lemma 3.3. *Let Γ denote a distance-regular graph with classical parameters (d, b, α, β). Suppose intersection numbers $a_1 = 0$ and $a_2 \neq 0$. Then $\alpha < 0$ and $b < -1$.*

Proof of Theorem 1.1:

(ii)⇒(i) This is clear.

(iii)⇒(ii) Suppose Γ has classical parameters. Then Γ is Q-polynomial with associated dual eigenvalues $\theta^*_0, \theta^*_1, \ldots, \theta^*_d$ satisfying

$$\theta^*_i - \theta^*_0 = (\theta^*_1 - \theta^*_0)\begin{bmatrix} i \\ 1 \end{bmatrix} b^{1-i} \quad \text{for } 1 \le i \le d. \tag{3.6}$$

We need to prove $s_i = 0$ for $3 \le i \le d$. To compute s_i in (3.2), observe from (3.6) that

$$\theta^*_{i-1} - \theta^*_i = (\theta^*_0 - \theta^*_1)b^{1-i} \quad \text{for } 1 \le i \le d. \tag{3.7}$$

Summing (3.7) for consecutive i, we find

$$(\theta^*_1 - \theta^*_i) = (\theta^*_0 - \theta^*_1)(b^{-1} + b^{-2} + \cdots + b^{1-i}), \tag{3.8}$$

$$(\theta^*_1 - \theta^*_{i-1}) = (\theta^*_0 - \theta^*_1)(b^{-1} + b^{-2} + \cdots + b^{2-i}), \tag{3.9}$$

$$(\theta^*_2 - \theta^*_i) = (\theta^*_0 - \theta^*_1)(b^{-2} + b^{-3} + \cdots + b^{1-i}), \tag{3.10}$$

$$(\theta^*_0 - \theta^*_{i-1}) = (\theta^*_0 - \theta^*_1)(b^{0} + b^{-1} + \cdots + b^{2-i}) \tag{3.11}$$

for $3 \leq i \leq d$. Evaluating (3.2) by using (3.7)-(3.11), we find $s_i = 0$ for $3 \leq i \leq d$.

(i)⇒(iii) Observe $s_3 = 0$. Then by setting $i = 3$ in (3.2) and using the assumption $a_2 \neq 0$, we find

$$(\theta_0^* - \theta_2^*)(\theta_2^* - \theta_3^*) - (\theta_1^* - \theta_2^*)(\theta_1^* - \theta_3^*) = 0. \tag{3.12}$$

Set

$$b := \frac{\theta_1^* - \theta_0^*}{\theta_2^* - \theta_1^*}. \tag{3.13}$$

Then

$$\theta_2^* = \theta_0^* + \frac{(\theta_1^* - \theta_0^*)(b+1)}{b}. \tag{3.14}$$

Eliminating θ_2^*, θ_3^* in (3.12) using (3.14) and (2.2), we have

$$\frac{-(\theta_1^* - \theta_0^*)^2(\sigma b^2 + \sigma b + \sigma - b)}{\sigma b^2} = 0. \tag{3.15}$$

for appropriate $\sigma \in \mathbb{R} \setminus \{0\}$. Since $\theta_1^* \neq \theta_0^*$,

$$\sigma b^2 + \sigma b + \sigma - b = 0,$$

and hence

$$\sigma^{-1} = \frac{b^2 + b + 1}{b}. \tag{3.16}$$

From Theorem 2.2, to prove that Γ has classical parameter, it suffices to prove that

$$\theta_i^* - \theta_0^* = (\theta_1^* - \theta_0^*)\begin{bmatrix} i \\ 1 \end{bmatrix} b^{1-i} \quad \text{for} \quad 1 \leq i \leq d. \tag{3.17}$$

We prove (3.17) by induction on i. The case $i = 1$ are trivial and case $i = 2$ is from (3.14). Now suppose $i \geq 3$. Then (2.2) implies

$$\theta_i^* = \sigma^{-1}(\theta_{i-1}^* - \theta_{i-2}^*) + \theta_{i-3}^* \tag{3.18}$$

Evaluate (3.18) using (3.16) and the induction hypothesis, we find $\theta_i^* - \theta_0^*$ is as in (3.17). Therefore, Γ has classical parameters (d, b, α, β) for some scalars α, β. Note that $b < -1$ from Lemma 3.3. □

4 Proof of Theorem 1.2

Recall that a sequence x, y, z of vertices of Γ are *geodetic* whenever

$$\partial(x,y) + \partial(y,z) \;=\; \partial(x,z).$$

Recall that a sequence x, y, z of vertices of Γ are *weak-geodetic* whenever

$$\partial(x,y) + \partial(y,z) \leq \partial(x,z) + 1.$$

Definition 4.1. A subset $\Omega \subseteq X$ is *weak-geodetically closed* if for any weak-geodetic sequence x, y, z of Γ,

$$x,\ z \in \Omega \Longrightarrow y \in \Omega.$$

Theorem 4.2. *[9, Proposition 6.7, Theorem 4.6] Let $\Gamma = (X, R)$ denote a distance-regular graph with diameter $d \geq 3$. Assume that the intersection numbers $a_1 = 0$ and $a_2 \neq 0$. Suppose that Γ contains no parallelograms of length 3. Then for each pair of vertices $v, w \in X$ at distance $\partial(v,w) = 2$, there exists a weak-geodetically closed subgraph Ω of diameter 2 in Γ containing v, w. Furthermore Ω is strongly regular with intersection numbers*

$$a_i(\Omega) \;=\; a_i(\Gamma), \tag{4.1}$$

$$c_i(\Omega) \;=\; c_i(\Gamma), \tag{4.2}$$

$$b_i(\Omega) \;=\; a_2(\Gamma) + c_2(\Gamma) - a_i(\Omega) - c_i(\Omega) \tag{4.3}$$

for $0 \leq i \leq 2$.

Applying Theorem 4.2 to the case of classical parameters with some computations, we find

Corollary 4.3. *Let Γ denote a distance-regular graph with classical parameters (d, b, α, β), where $d \geq 3$. Assume Γ has intersection numbers $a_1 = 0$ and $a_2 \neq 0$. Then there exists a weak-geodetically closed subgraph Ω of diameter 2. Furthermore the intersection numbers of Ω satisfy*

$$b_0(\Omega) \;=\; (1+b)(1-\alpha b), \tag{4.4}$$

$$b_1(\Omega) \;=\; b(1-\alpha-\alpha b), \tag{4.5}$$

$$c_2(\Omega) \;=\; (1+b)(1+\alpha), \tag{4.6}$$

$$a_2(\Omega) \;=\; -(1+b)^2\alpha, \tag{4.7}$$

$$|\Omega| \;=\; \frac{(1+b)(b\alpha-2)(b\alpha-1-\alpha)}{(1+\alpha)}. \tag{4.8}$$

Proposition 4.4. *[9, Proposition 3.2] Let Γ denote a distance-regular graph with diameter $d \geq 3$. Suppose there exists a weak-geodetically closed subgraph Ω of Γ with diameter 2. Then the intersection numbers of Γ satisfy the following inequality*

$$a_3 \geq a_2(c_2 - 1) + a_1. \tag{4.9}$$

Applying the above Proposition to the case of classical parameters, we find

Corollary 4.5. *Let Γ denote a distance-regular graph with classical parameters (d, b, α, β), where $d \geq 3$. Suppose the intersection numbers $a_1 = 0$ and $a_2 \neq 0$. Then*

$$c_2 \leq b^2 + b + 2. \tag{4.10}$$

We will decrease the upper bound of c_2 in (4.10). We need the following lemma.

Lemma 4.6. *Let Γ denote a distance-regular graph with classical parameters (d, b, α, β), where $d \geq 3$. Assume the intersection numbers $a_1 = 0$ and $a_2 \neq 0$. Let Ω be a weak-geodetically closed subgraph of diameter 2 in Γ. Let $r > s$ denote the nontrivial eigenvalues of the strongly regular graph Ω. Then the following (i), (ii) hold:*

(i) The multiplicity of r is

$$f = \frac{(b\alpha - 1)(b\alpha - 1 - \alpha)(b\alpha - 1 + \alpha)}{(\alpha - 1)(\alpha + 1)}. \tag{4.11}$$

(ii) The multiplicity of s is

$$g = \frac{-b(b\alpha - 1)(b\alpha - 2)}{(\alpha - 1)(\alpha + 1)}. \tag{4.12}$$

Proof. From [3, Theorem 21.1], we have

$$f = \frac{1}{2}\{v - 1 + \frac{(v-1)(c_2 - a_1) - 2k}{\sqrt{(c_2 - a_1)^2 + 4(k - c_2)}}\}, \tag{4.13}$$

$$g = \frac{1}{2}\{v - 1 - \frac{(v-1)(c_2 - a_1) - 2k}{\sqrt{(c_2 - a_1)^2 + 4(k - c_2)}}\}, \tag{4.14}$$

where $v = |\Omega|$ and k is the valency of Ω. (4.11), (4.12) are (4.13), (4.14) in the case of classical parameters. □

Corollary 4.7. *Let Γ denote a distance-regular graph with classical parameters (d, b, α, β), where $d \geq 3$. Assume Γ has intersection numbers $a_1 = 0$ and $a_2 \neq 0$. Then*

$$\frac{b(b+1)^2(b+2)}{c_2}, \tag{4.15}$$

$$\frac{(b-2)(b-1)b(b+1)}{2+2b-c_2} \tag{4.16}$$

are both integers.

Proof. Let f and g be as (4.11), (4.12). Set $\rho{=}\alpha(1+b)$. Note ρ is an integer, since $\rho = c_2 - 1 - b$. Then both

$$f + g - (1 - 3b^2 - b\rho + b^2\rho - b^3) = \frac{2b + 5b^2 + 4b^3 + b^4}{1 + b + \rho} = \frac{b(b+1)^2(b+2)}{c_2}$$

and

$$f - g - (1 - 3b^2 - b\rho + b^2\rho + b^3) = \frac{2b - b^2 - 2b^3 + b^4}{-1 - b + \rho} = \frac{(b-2)(b-1)b(b+1)}{2 + 2b - c_2}$$

are integers since f, g, b and ρ are integers. □

Proposition 4.8. *Let Γ denote a distance-regular graph with classical parameters (d, b, α, β), where $d \geq 3$. Assume Γ has intersection numbers $a_1 = 0$ and $a_2 \neq 0$. Then $c_2 \leq b(b+1)$.*

Proof. Recall $c_2 \leq b^2 + b + 2$ by (4.10). First, suppose

$$c_2 = b^2 + b + 2. \tag{4.17}$$

Then the integral condition (4.15) becomes

$$b^2 + 3b + \frac{-4b}{b^2 + b + 2}. \tag{4.18}$$

Since $0 < -4b < b^2 + b + 2$ for $b \leq -5$, we have $-4 \leq b \leq -2$. For $b = -4$ or -3, expression (4.18) is not an integer. The remaining case $b{=}{-2}$ implies $\alpha = -5$ by (4.6), $v = 28$ by (4.8) and $g = 6$ by (4.12). It contradicts to $v \leq \frac{1}{2}g(g+3)$ [3, Theorem 21.4]. Hence $c_2 \neq b^2 + b + 2$. Next suppose $c_2 = b^2 + b + 1$. Then (4.16) becomes

$$-b^2 + b + 1 + \frac{1}{b^2 - b - 1}. \tag{4.19}$$

It fails to be an integer since $b < -1$. □

Proof of Theorem 1.2:

The results come from Corollary 4.7 and Proposition 4.8. □

Example 4.9. [4] Hermitian forms graph $Her_2(d)$ is a distance-regular graph with classical parameters (d, b, α, β) with $b = -2$, $\alpha = -3$ and $\beta = -((-2)^d + 1)$, which satisfies $a_1 = 0$, $a_2 \neq 0$ and $c_2 = b(b+1)$.

Example 4.10. [3, p. 237] Gerwitz graph is a distance-regular graph with diameter 2 and intersection numbers $a_1 = 0$, $c_2 = 2$, $k = 10$, which can be written as classical parameters (d, b, α, β) with $d = 2$, $b = -3$, $\alpha = -2$, $\beta = -5$, so we have $c_2 = \dfrac{(b+1)^2}{2}$.

Conjecture 4.11. *(Gerwitz graph does not grow.) There is no distance-regular graph with classical parameters* $(d, -3, -2, -\dfrac{1+(-3)^d}{2})$, *where* $d \geq 3$.

There is a similar conjecture of Conjecture 4.11 for the complement part in $a_1 \neq 0$. See [10, Theorem 10.3] for details.

References

[1] E. Bannai and T. Ito. *Algebraic Combinatorics I: Association Schemes.* Benjamin/Cummings, London, 1984.

[2] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs.* Springer-Verlag, Berlin, 1989.

[3] J. H. van Lint, and R. M. Wilson. *A Course in Combinatorics.* Cambridge University Press, 1992.

[4] Ivanov, A.A., Shpectorov, S.V.. Characterization of the association schemes of Hermitian forms over $GF(2^2)$. *Geom. Dedicata*, 30:23–33, 1989.

[5] P. Terwilliger. The subconstituent algebra of an association scheme I. *J. Alg. Combin.*, 1:363–388, 1992.

[6] P. Terwilliger. A new inequality for distance-regulargraphs. *Discrete Math.*, 137:319–332, 1995.

[7] C. Weng. Kite-Free P- and Q-Polynomial Schemes *Graphs and Combinatorics*, 11:201-207, 1995.

[8] C. Weng. Parallelogram-Free Distance-Regular Graphs. *J. Combin. Theory Ser. B*, 71(2):231–243, 1997.

[9] C. Weng. Weak-Geodetically Closed Subgraphs in Distance-Regular Graphs. *Graphs and Combinatorics*, 14:275–304, 1998.

[10] C. Weng. Classical distance-regular graphs of negative type. *J. Combin. Theory Ser. B*, 76:93–116, 1999.

[11] $\check{S}$. Miklavič. Q-polynomial distance-regular graphs $a_1 = 0$. *European J. Combin.*, 25(7):911–920, 2004.

[12] J. H. Koolen and V. Moulton. There are finitely many triangle-free distance-regular graphs with degree 8, 9 or 10. *J. Algebraic Combin.*, 19(2):205–217, 2004.

[13] A. Jurišić, J. Koolen and $\check{S}$. Miklavič. On triangle-free distance-regular graphs with an eigenvalue multiplicity equal to the valency. *Preprint.*

Yeh-jong Pan
Department of Applied Mathematics
National Chiao Tung University
1001 Ta Hsueh Road
Hsinchu, Taiwan 30010, R.O.C.
Email: `yjpan@mail.tajen.edu.tw`
Fax: +886-3-5724679

Chih-wen Weng
Department of Applied Mathematics
National Chiao Tung University
1001 Ta Hsueh Road
Hsinchu, Taiwan 30010, R.O.C.
Email: `weng@math.nctu.edu.tw`
Fax: +886-3-5724679

A Characterization of the Odd graphs and the doubled Odd graphs with a few of their intersection numbers

Akira Hiraki, Osaka Kyoiku University

1. Definitions

$\Gamma = (V\Gamma, E\Gamma)$: a connected graph of diameter d.

$$\Gamma_j(x) = \{ y \in V\Gamma \mid \partial_\Gamma(x,y) = j \}.$$

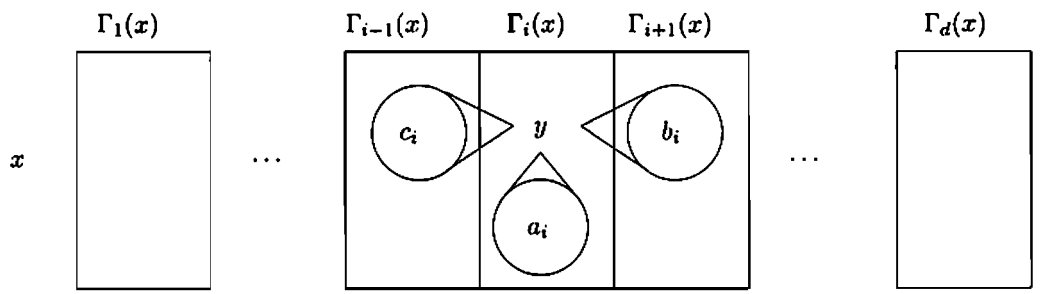
For $x, y \in V\Gamma$ with $\partial_\Gamma(x,y) = i$, let

$$\begin{aligned} C_i(x,y) &= \Gamma_{i-1}(x) \cap \Gamma_1(y), \\ A_i(x,y) &= \Gamma_i(x) \cap \Gamma_1(y), \\ B_i(x,y) &= \Gamma_{i+1}(x) \cap \Gamma_1(y), \end{aligned}$$

A connected graph Γ is said to be **distance-regular** if

$$c_i = |C_i(x,y)|, \quad a_i = |A_i(x,y)|, \quad b_i = |B_i(x,y)|$$

depend only on $i = \partial_\Gamma(x,y)$ rather than the choice of x, y.



Then c_i, a_i, b_i are called **the intersection numbers of** Γ.

In particular, $k = b_0$ is called **the valency of** Γ. The array

$$\iota(\Gamma) = \begin{Bmatrix} * & c_1 & \cdots & c_i & \cdots & c_{d-1} & c_d \\ a_0 & a_1 & \cdots & a_i & \cdots & a_{d-1} & a_d \\ b_0 & b_1 & \cdots & b_i & \cdots & b_{d-1} & * \end{Bmatrix}.$$

is called **the intersection array of** Γ.

Let X be a set of $2m+1$ elements, and set

$$X_m = \{ P \subseteq X : |P| = m \}, \quad X_{m+1} = \{ Q \subseteq X : |Q| = m+1 \}.$$

Odd graph O_{m+1} is a graph with

$$V\Gamma = X_m, \quad E\Gamma = \{ (P, P') : P \cap P' = \emptyset \}$$

Doubled Odd graph $2O_{m+1}$ is a bipartite graph with

$$V\Gamma = X_m \cup X_{m+1}, \quad E\Gamma = \{ (P, Q) : P \subset Q \}$$

Then O_{m+1} and $2O_{m+1}$ are distance-regular graphs with

$O_{2t+1} : d = 2t$

$$\left\{ \begin{array}{ccccccccc} * & 1 & 1 & 2 & 2 & \cdots & t & t \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t+1 \\ 2t+1 & 2t & 2t & 2t-1 & 2t-1 & \cdots & t+1 & * \end{array} \right\},$$

$O_{2t} : d = 2t-1$

$$\left\{ \begin{array}{ccccccccc} * & 1 & 1 & 2 & 2 & \cdots & t-1 & t \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t \\ 2t & 2t-1 & 2t-1 & 2t-2 & 2t-2 & \cdots & t+1 & * \end{array} \right\},$$

$2O_{m+1} : d = 2m+1$

$$\left\{ \begin{array}{ccccccccc} * & 1 & 1 & 2 & 2 & \cdots & m & m & m+1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ m+1 & m & m & m-1 & m-1 & \cdots & 1 & 1 & * \end{array} \right\}.$$

Theorem 1. ([1, Cypers] and [5, Koolen] : cf [6, Ray-Chaudri & Sprager].)

Let Γ be a DRG with

$$\left\{ \begin{array}{cccccc} * & 1 & 1 & 2 & 2 & \cdots \\ 0 & 0 & 0 & 0 & 0 & \cdots \\ m+1 & m & m & m-1 & m-1 & \cdots \end{array} \right.$$

Then $\Gamma \simeq O_{m+1}$ or $2O_{m+1}$.

Theorem 2. ([3, Hiraki].)

Let Γ be a DRG with

$$\left\{ \begin{array}{ccccccccc} * & 1 & \cdots & 1 & 2 & \cdots & 2 & & \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & \\ k & k-1 & \cdots & k-1 & k-2 & \cdots & k-2 & & \end{array} \right\}.$$

$$\underbrace{\qquad}_{r} \qquad \underbrace{\qquad}_{s}$$

Then

$$s \leq \frac{r+4}{3}.$$

Corllary 3. Let Γ be a DRG as in Theorem 2.

If $s = r \geq 2$, then $r = 2$ and $\Gamma \simeq O_k$ or $2O_k$.

2. The diameter bound for bipartite DRGs

Let Γ be a DRG of diameter d and $a_1 = \cdots = a_{d-1} = 0$.

$$r = r(\Gamma) := \max\{\, i \mid (c_i, a_i, b_i) = (c_1, a_1, b_1) \,\}.$$

$$\left\{ \begin{array}{ccccccccc} * & 1 & \cdots & 1 & & c & c' & & \\ 0 & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & \\ k & k-1 & \cdots & k-1 & & b & b' & & \end{array} \right\}.$$

$$\underbrace{\qquad}_{r} \qquad\qquad \underbrace{\qquad}_{m} \qquad \underbrace{\qquad}_{m+r}$$

Theorem 4. ([7, 8, Terwilliger])

$$c_{m+r} \geq c_m + 1 \quad \text{for all} \quad 1 \leq m \leq d - r.$$

In particular,

$$d \leq (k-1)r + 1$$

Remark. This bound is tight. (Hypercubes $H(d, 2)$, Doubled Odd graph $2O_d$)

Theorem 5. ([4, Koolen])

$$d = (k-1)r + 1 \quad \Leftrightarrow \quad \Gamma \simeq H(d, 2) \text{ or } 2O_d$$

Moreover, if $r \geq 2$ and $\Gamma \not\simeq 2O_d$ then

$$d \leq (k-1)r + 1 - \left[\frac{k-3}{2}\right],$$

3. Some inequalities for DRGs

Lemma 6. Γ : DRG of diameter d. Suppose $c_q < c_{q+1}$, $a_q = 0$ and $m+q \leq d$. Then

$$c_m \leq c_{m+q} - c_q. \quad \text{and} \quad b_{m+q} \leq b_m - c_q.$$

Remarks. The equalities in Lemma 6 are always hold for $H(d,2)$, O_k and $2O_k$. Put $q = r$ in the first inequality we have Terwillger's inequality $c_m \leq c_{m+r} - 1$

Sketch of proof of Lemma 6. (See [2] for more detail.)

Let $u, v, w \in V\Gamma$ with $\partial_\Gamma(u,v) = m$, $\partial_\Gamma(v,w) = q$, $\partial_\Gamma(u,w) = m+q$.

$$Y := C_m(u,v), \quad Z := C_{m+q}(u,w) \setminus C_q(v,w)$$

Count

$$\{ (y,z) \mid y \in Y,\ z \in Z,\ \partial_\Gamma(y,z) = q \}$$

in two ways. Then

$$|Y|(c_{q+1} - c_q) \quad = \quad \# \quad \leq \quad |Z|(c_{q+1} - c_q)$$

and

$$c_m \quad = \quad |Y| \quad \leq \quad |Z| \quad = \quad (c_{m+q} - c_q)$$

as $c_q < c_{q+1}$. The first inequality is proved.

Let $u, v, w \in V\Gamma$ with $\partial_\Gamma(u,v) = m$, $\partial_\Gamma(v,w) = q$, $\partial_\Gamma(u,w) = m+q$.

$$Y' := B_{m+q}(u,w), \quad Z' := B_m(u,v) \setminus C_q(w,v)$$

Count

$$\{ (y,z) \mid y \in Y',\ z \in Z',\ \partial_\Gamma(y,z) = q \}$$

in two ways. Then

$$|Y'|(c_{q+1} - c_q) \quad = \quad \# \quad \leq \quad |Z'|(c_{q+1} - c_q)$$

and

$$b_{m+q} \quad = \quad |Y'| \quad \leq \quad |Z'| \quad = \quad b_m - c_q$$

■

4. A characterization of O_k and $2O_k$

Theorem 7. Γ : DRG of diameter d and $2 \leq r \leq m \leq d-r-1$,

Suppose $a_m = a_{m+r} = 0$ and $1 = c_{m+r} - c_m$. Then $\Gamma \simeq O_k$ or $2O_k$.

An application of this theorem we have the following diameter bound for bipartite DRGs.

Theorem 8. Γ : bipartite DRG of diameter d, and valency $k \geq 4$.

$$r = r(\Gamma) := \max\{\, i \mid (c_i, a_i, b_i) = (c_1, a_1, b_1) \,\}.$$

Suppose $\Gamma \not\simeq 2O_k$. Then

$$d \leq \left[\frac{k+2}{2}\right] r + 1.$$

■

The reader is referred to [2] for proof of the results.

References

[1] H. Cuypers, The dual Pasch's axiom, *Europ. J. Combin.* **13** (1992), 15-31.

[2] A. Hiraki, A Characterization of the Odd graphs and the doubled Odd graphs with a few of their intersection numbers, to appear in *Europ. J. Combin.*

[3] A. Hiraki, Applications of the retracing method for distance-regular graphs, *Europ. J. Combin.* **26** (2005), 717–727.

[4] J. H. Koolen, On subgraphs in distance-regular graphs, *J. Alg. Combin.* **1** (1992), 353-362.

[5] J. H. Koolen, On Uniformly geodetic graphs, *Graphs and Combin.* **9** (1993), 325-333.

[6] D. K. Ray-Chaudhuri and A. P. Sprague. Characterization of projective incidence structures, *Geom. Dedicata.* **5** (1976), 361–376.

[7] P. Terwilliger, The diameter of bipartite distance-regular graph, *J. of Combin. Theory* Ser. B **32** (1982), 182–188.

[8] P. Terwilliger, Distance-regular graph and (s, c, a, k)-graphs, *J. of Combin. Theory* Ser. B **34** (1983), 151–164.

ON DISTANCE-REGULAR GRAPH AND THEIR AUTOMORPHISMS

Makhnev Alexandre A.

Let Γ be a distance-regular graph of diameter d with v vertices. Then for basic matrices $A_0, ..., A_d$ and for matrices $E_0, ..., E_d$ of the orthogonal projections onto the eigenspaces $W_0, W_1, ..., W_d$ ($W_0 = \langle \mathbf{1} \rangle$) from $\mathbf{C}^v$ we have

$$A_i = \sum_{j=0}^{d} P_{ij} E_j \text{ and } E_i = v^{-1} \sum_{j=0}^{d} Q_{ij} A_j,$$

where P and Q are first and second eigenmatrices of an association scheme corresponding Γ.

The image of E_i is the ith eigenspace W_i, and so E_i affords the character χ_i of the automorphism group G of Γ. For $g \in G$ we have

$$\chi_i(g) = v^{-1} \sum_{j=0}^{d} Q_{ij} \alpha_j(g),$$

where $\alpha_j(g)$ is the numbers of vertices x of Γ such that $d(x, x^g) = j$.

Let Γ be a distance-regular graph with intersection array $\{60, 45, 8; 1, 12, 50\}$ and $g \in \mathrm{Aut}(\Gamma)$. Then $v = 1 + 60 + 225 + 36 = 322$, Γ_2 is strongly regular graph and

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 45 & 21/2 & -1 & -25/2 \\ 207 & 0 & -23/5 & 23 \\ 69 & -23/2 & 23/5 & -23/2 \end{pmatrix}.$$

So $\chi_2(g) = (45\alpha_0(g) - \alpha_2(g) + 5\alpha_3(g)/70$, $\chi_3(g) = (5\alpha_0(g) + \alpha_2(g))/20 - 23/2$.

Theorm 1 (Gavrilyuk A.L., Makhnev A.A.). *Let* Γ *be a distance-regular graph with intersection array* $\{60, 45, 8; 1, 12, 50\}$, g *be an element of prime order* $p \geq 5$ *of* $\mathrm{Aut}(\Gamma)$ *and* $\Omega = \mathrm{Fix}(g)$. *Then one of the following holds.*

(1) Ω *is empty graph and* $p = 7$ *or* 23.

(2) $p = 5$ *and either* $\Omega = \{a, b\}$ *and* $d(a, b) = 3$, *or* $|\Omega| = 7$ *and* $\Gamma_3(a) \cap \Omega$ *is* 6*-clique for some vertex* $a \in \Omega$.

Corollary 1. *Let* Γ *be a distance-regular graph with intersection array* $\{60, 45, 8; 1, 12, 50\}$. *Then* Γ *is not distance-transitive.*

Suppose that a group $G = \mathrm{Aut}(\Gamma)$ acts distance-transitive on Γ. Let a be a vertex of Γ. Then $H = G_a$ acts transitive on $\Gamma_i(a)$ for $i \in \{1, 2, 3\}$. So for $b_i \in \Gamma_i(a)$ and for $F_i = H_{b_i}$ we obtain equalities $|H : F_1| = 60$, $|H : F_2| = 225$ and $|H : F_3| = 36$. Hence F_3 contains Sylow 5-subgroup P of H and $|P|$ is devided by 25. Further $[a] \cap \Gamma_3(b_3)$ contains two P-orbits of order 5 and by theorem $[a] \cap \Gamma_3(b_3)$ is a union of two isolated 5-cliques. So $\Gamma_3(x)$ is 6×6-grid for any vertex x of Γ. But Gavrilyuk proved that it is impossible.

Let Γ be a distance-regular graph with intersection array $\{8, 7, 5; 1, 1, 4\}$ and $g \in \mathrm{Aut}(\Gamma)$. Then

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 54 & 81/4 & 27/28 & -27/7 \\ 50 & -25/4 & -25/4 & 5 \\ 30 & -15 & 30/7 & -15/7 \end{pmatrix}.$$

So $\chi_2(g) = (5\alpha_0(g) + \alpha_3(g))/12 - 25/4$, $\chi_3(g) = (7\alpha_0(g) + 3\alpha_2(g) + 2\alpha_3(g))/21 - 15$.

Theorm 2 (Belousov I.N., Makhnev A.A.). *Let Γ be a distance-regular graph with intersection array $\{8,7,5;1,1,4\}$, g be an element of prime order of $\mathrm{Aut}(\Gamma)$ and $\Omega = \mathrm{Fix}(g)$. Then one of the following holds.*

(1) *Ω is empty graph and $p = 3$ or 5.*

(2) *$\Omega = \{a, b\}$ is 2-clique and $p = 7$.*

(3) *$p = 2$ and*

(i) $d(a, b) = 3$ for any two vertices $a, b \in \Omega$ and $|\Omega| = 3, 5, 7, 9, 11, 13$, or

(ii) Ω contains two vertices of valency 4, eight vertices of valency 2 and one or three vertices of valency 0, or

(iii) Ω contains gexagon and one isolated vertex.

Corollary 2. *Let Γ be a distance-regular graph with intersection array $\{8,7,5;1,1,4\}$. Then Γ is not vertex-transitive.*

Let Γ be a distance-regular graph with intersection array $\{8,7,5;1,1,4\}$, $G = \mathrm{Aut}(\Gamma)$. Then $v = 1+8+56+70 = 135$ and $\pi(G) \subseteq \{2,3,5,7\}$. Let a be a vertex of Γ, $H = G_a$. Then $\pi(H) \subset \{2,7\}$ and $|G : H|$ devides $3^3 \cdot 5$. So H acts intransitive on $\Gamma_3(a)$, and Γ is not distance-transitive.

If G contains an element f of order pr, where p, r is distinct prime, $p < r$, then $p = 2$ and $r = 3$.

Lemma. *The following are true.*

(1) *G contains no regular subgroups.*

(2) *If* $b_i \in \Gamma_i(a)$, $F_i = H_{b_i}$, *then* $|F_1|$ *devides* 7, $|F_2| = 1$ *and* $|F_3|$ *devides* 4.

(3) *If* S *be a Sylow* 2*-subgroup of* H, *then* $|S|$ *devides* 8.

Let G acts vertex-transitive on Γ. As 135 is not a prime power, then the socle G_0 of the group G is simple nonabelian group and G_0 acts vertex-transitive on Γ. Set $H_0 = G_0 \cap H$. Then $|G_0 : H_0| = 3^3 \cdot 5$ and $|G|$ devides $2^3 3^3 5 \cdot 7$.

If Sylow 2-subgroup S_0 of G_0 is abelian, then by [1,2] $G_0 \simeq L_2(8)$, $L_2(q)$, $q \equiv 3, 5 \ (mod\, 8)$, ${}^2G_2(3^{2n-1})$ or J_1. In contrary case S_0 is dihedral group of order 8 and by [3] $G_0 \simeq L_2(q)$, $q \equiv 7, 9 \ (mod\ 16)$ or A_7. As $|G_0|$ devides $2^3 3^3 5 \cdot 7$, then $G_0 \simeq L_2(q)$ or A_7. But $|G_0|$ is devides by $3^3 5$, so $G_0 \simeq L_2(3^3)$, a contradiction with 13 is not devides $|G|$.

References

[1] J. Walter, "The characterization of finite groups with abelian Sylow 2-subgroups", Ann. Math. 1969, v. 89, 405–514.

[2] E. Bombieri, "Thompson's problem ($\sigma^2 = 3$)", Invent. Math. 1980, v. 58, 77–100.

[3] D. Gorenstein, J. Walter, "The characterization of finite groups with dihedral Sylow 2-subgroups", I-IV // Ill. J. Math. 1962, v. 6, 553-593; J. Algebra 1965, v. 2, 85–151; 218–270; 354–393.

Small weight codewords in LDPC codes defined by (dual) classical generalized quadrangles

Jon-Lark Kim*, Keith E. Mellinger† and Leo Storme‡

Abstract

We find lower bounds on the minimum distance and characterize codewords of small weight in low-density parity check codes defined by (dual) classical generalized quadrangles. We analyze the geometry of the non-singular parabolic quadric in $PG(4,q)$ to find information about the low-density parity check codes defined by $Q(4,q)$, $\mathcal{W}(q)$ and $\mathcal{H}(3,q^2)$. For $\mathcal{W}(q)$ and $\mathcal{H}(3,q^2)$, we are able to describe small weight codewords geometrically. For $Q(4,q)$, q odd, and for $\mathcal{H}(4,q^2)^D$, we improve the best known lower bounds on the minimum distance, again only using geometric arguments.

Keywords: LDPC code, generalized quadrangle, minimum distance
Classification: 51E12, 94B05

1 Introduction

The concept of low-density parity check (LDPC) codes was introduced by Gallager [4], and it was shown in [15] that these codes perform well under iterative probabilistic decoding. A binary *LDPC code* C, in its broader sense, is a linear block code defined by a sparse parity check matrix H, i.e., H has much fewer 1s than 0s. When the columns of H have a constant weight ρ and the rows of H also have a constant weight γ, we call C an (ρ, γ)-*regular LDPC code*. When LDPC codes are decoded using Gallager's decoding method, their empirical performance is known to be excellent [15], [13].

Early known LDPC codes have been constructed randomly [4], [15]. There are several types of explicit constructions of LDPC codes. One is based on permutation matrices [3], [22]. Another one is based on Ramanujan graphs [16], [18], expander graphs [19], and q-regular bipartite graphs [10].

In 2001, Kou et al. [11] examined classes of LDPC codes defined by incidence structures in finite geometries. Since then, other LDPC codes have been produced based on various incidence

*The first author acknowledges support by a Research Initiation Grant from University of Louisville
†The second author acknowledges support by a Faculty Development Grant from the University of Mary Washington
‡The third author thanks the Fund for Scientific Research Flanders-Belgium for a research grant

structures in discrete mathematics and finite geometry (for example, [7], [8], [9], [14], [23], [24]). In particular, Vontobel and Tanner [23] considered the LDPC codes generated by generalized polygons, focusing on generalized quadrangles. They demonstrated that some generalized quadrangle LDPC codes perform well under the sum product algorithm [15]. Later, Liu and Pados [12] showed that all LDPC codes derived from finite classical generalized quadrangles are quasi-cyclic, and they gave the explicit size of the circulant blocks in the parity check matrix. Their simulation results show that several generalized polygon LDPC codes have powerful bit-error-rate performance when decoding is carried out via low-complexity variants of belief propagation [12].

In [6], the problem of determining the minimum distance of LDPC codes was addressed. We contribute in this article to the problem of finding the minimum distance of LDPC codes defined by the incidence structure of (dual) classical finite generalized quadrangles. We find improved lower bounds on these minimum distances of these codes and characterize their low weight codewords using geometric techniques.

This paper consists of five sections. Section 2 gives an introduction to generalized quadrangles and LDPC codes defined by them. Section 3 classifies geometrically the small weight codewords in the LDPC code defined by $\mathcal{W}(q)$. In Sections 4 and 5, we improve the lower bounds on the minimum weight of codewords in $\mathcal{Q}(4,q)$, q odd, and $\mathcal{H}(4,q^2)^D$, respectively. Similar results can also be obtained for the LDPC codes $\mathrm{LU}(3,q)$ given in [10] but are omitted due to a limited space.

2 Generalized quadrangles

We provide a brief overview of generalized quadrangles and refer the reader to [5] or [17] for more details.

A *generalized quadrangle* Γ, also denoted by GQ, is defined axiomatically as a set of points and lines such that:

(a) any two distinct points are on at most one common line,

(b) all lines are incident with the same number of points, and all points are incident with the same number of lines, and,

(c) if the point P of Γ is not incident with the line ℓ of Γ, then there is precisely one line through P intersecting ℓ.

Note that the last axiom forces the non-existence of triangles in generalized quadrangles. The common number of points on a line is denoted by $s+1$, and the common number of lines through a point is denoted by $t+1$. The pair (s,t) is called the *parameters* of the generalized quadrangle Γ, and Γ is also denoted by $\mathrm{GQ}(s,t)$. Interchanging the roles of points and lines in a generalized quadrangle Γ of order (s,t) gives the *dual* generalized quadrangle $\Gamma^D = \overline{\Gamma}$ of order (t,s). Counting techniques show that the number of points in a $\mathrm{GQ}(s,t)$ is $(s+1)(st+1)$ and the number of lines is $(t+1)(st+1)$.

All of the generalized quadrangles that we will discuss in this article arise, up to duality, naturally in a finite projective space $PG(n,q)$. The first family of generalized quadrangles is denoted by $\mathcal{Q}(n,q)$. Consider a non-singular quadric $\mathcal{Q}$ of projective index 1 in the projective space $PG(n,q)$,

$n = 3, 4$, or 5. The points of $\mathcal{Q}$ together with the lines of $\mathcal{Q}$, which are the subspaces of maximal dimension contained in $\mathcal{Q}$, form the generalized quadrangle $\mathcal{Q}(n, q)$. We concentrate on the cases $n = 4, 5$. The GQ $\mathcal{Q}(4, q)$ is formed by a non-singular parabolic quadric of $PG(4, q)$. Without loss of generality, we can define this quadric by the quadratic form $X_0^2 + X_1X_2 + X_3X_4 = 0$, and in this case $s = t = q$. When $n = 5$, the GQ $\mathcal{Q}^-(5, q)$ is formed by the non-singular elliptic quadric in $PG(5, q)$. Without loss of generality, this quadric can be defined by a quadratic equation $f(X_0, X_1) + X_2X_3 + X_4X_5 = 0$, where $f(X_0, X_1)$ is an irreducible homogeneous quadratic form over $GF(q)$. In this case, $s = q$ and $t = q^2$.

Now let $\mathcal{U}$ be a non-singular Hermitian variety in $PG(n, q^2)$, $n = 3$ or 4. Without loss of generality, we can use the equation $X_0^{q+1} + X_1^{q+1} + \cdots + X_n^{q+1} = 0$ to define $\mathcal{U}$. The points of $\mathcal{U}$, together with the lines of $\mathcal{U}$, define a generalized quadrangle, denoted by $\mathcal{H}(n, q^2)$. In this case, $s = q^2$ and $t = q$ when $n = 3$; and $s = q^2$ and $t = q^3$ when $n = 4$.

Finally, the points of $PG(3, q)$, together with the self-polar lines of a symplectic polarity η, form a generalized quadrangle $\mathcal{W}(q)$ with $s = t = q$. The geometry is quite interesting in this case. We obtain a set of $q^3 + q^2 + q + 1$ lines of $PG(3, q)$ with the property that through every point P of $PG(3, q)$, there are exactly $q + 1$ coplanar lines of $\mathcal{W}(q)$ lying in the plane P^η, and in every plane Π, there are exactly $q + 1$ concurrent lines of $\mathcal{W}(q)$ passing through the point Π^η.

The above described generalized quadrangles are called the *classical* generalized quadrangles, and their duals are called the *dual classical* generalized quadrangles.

In a generalized quadrangle, we denote the set of points collinear with a point P by $P^\perp$, and the set of lines intersecting a given line ℓ by $\ell^\perp$. For $\mathcal{W}(q)$, $P^\perp = P^\eta$.

The following relations between these (dual) classical generalized quadrangles are known [17].

Theorem 2.1. (1) *The generalized quadrangle $\mathcal{Q}(4, q)$ is isomorphic to the dual of $\mathcal{W}(q)$.*

(2) *The generalized quadrangles $\mathcal{W}(q)$ and $\mathcal{Q}(4, q)$ are self-dual if and only if q is even.*

(3) *The generalized quadrangle $\mathcal{Q}^-(5, q)$ is isomorphic to the dual of $\mathcal{H}(3, q^2)$.*

For many applications, we are interested in the *binary* linear code with this incidence matrix H as parity check matrix. Nevertheless, we can also address the codes defined by H over the finite field $GF(q)$ in the cases $\mathcal{Q}(n, q)$ and $\mathcal{W}(q)$, and over the finite field $GF(q^2)$ in the case $\mathcal{H}(n, q^2)$, or over the prime field $GF(p)$ of $GF(q = p^h)$ or $GF(q^2 = p^{2h})$. We will address the problem of finding the minimum distance of LDPC codes and of characterizing small weight codewords in LDPC codes. The methods applied here are valid both for binary LDPC codes, LDPC codes over $GF(q)$ or $GF(q^2)$, and for LDPC codes over $GF(p)$ [2].

Let $\mathcal{C}$ be a binary linear code defined by the parity check matrix H. For every binary LDPC code, there is an associated bipartite graph, called the "Tanner graph", which represents the code. In this setting, the Tanner graph is simply the bipartite incidence graph of the corresponding geometry. It is well regarded in the theory of low-density parity check codes that high girth in this graph increases the efficiency of the decoding. In general, girth 4 is considered to be poor. Note that using generalized quadrangles, or some subset thereof, implies a girth of at least 8 in the Tanner graph. This is one motivation for studying LDPC codes arising from generalized quadrangles, or from a subset of a generalized quadrangle.

LDPC code	Order (s,t)	d
$\mathcal{W}(q)$, $q=2^e$	(q,q)	$2(q+1)$
$\mathcal{W}(q)$, q odd	(q,q)	$2(q+1)$
$\mathcal{Q}(4,q)$, q odd	(q,q)	$\gtrapprox \frac{(q+1)\sqrt{q}}{2}$
$\mathcal{Q}^-(5,q)$	(q,q^2)	$\geq (q+1)(q^2-q+2)$
$\mathcal{H}(3,q^2)$	(q^2,q)	$2(q+1)$
$\mathcal{H}(4,q^2)$	(q^2,q^3)	$\geq (q^2+1)(q^3-q^2+2)$
$\mathcal{H}(4,q^2)^D$	(q^3,q^2)	$\geq \mathbf{q\sqrt{(q^2+1)(q-1)}+q^2+2}$

Table 1: New minimum distances of GQ LDPC codes

Let $\mathcal{C}$ be an LDPC code defined by a generalized quadrangle Γ, or by a subset Γ of a generalized quadrangle. A codeword $\mathbf{c}=(c_1,c_2,\ldots,c_n)$ in $\mathcal{C}$ satisfies $\mathbf{c}H^T=\bar{0}$. Hence, the codeword $\mathbf{c}$ defines through its non-zero positions which correspond to points of Γ,

(*) a set S of points of Γ such that every line of Γ contains 0 or at least 2 of the points of S.

Alternatively, we can work in the dual generalized quadrangle Γ^D. Here, this codeword $\mathbf{c}$ defines

(**) a set S of lines of Γ^D such that every point of Γ^D lies on 0 or on at least 2 of the lines of S.

We will refer to these as Property (*) and (**). These properties (*) and (**) can be used for binary LDPC codes, and for LDPC codes over $GF(q)$, $GF(q^2)$, or over $GF(p)$, p prime. We note that (*) and (**) are necessary conditions that codewords must satisfy. More precisely, we use for instance (**) to get information on which lines belong to such a set S. Then we look for the coordinates in $\mathbf{c}$ corresponding to these lines of S.

Table 1 summarizes the new bounds on the minimum distances of LDPC codes defined by the (dual) classical generalized quadrangles. The new lower bounds on the minimum distance d for the LDPC codes arising from $\mathcal{Q}(4,q)$, q odd, and $\mathcal{H}(4,q^2)^D$ are written in boldface. In these two cases, we have improved greatly the bounds given in [12], [20, 21, 23].

These lower bounds are in accordance with the results of Bagchi and Sastry [1] who showed that the minimum distance is at least $2(t+1)$, with equality if and only if the generalized quadrangle $\Gamma=\mathrm{GQ}(s,t)$ contains subquadrangles of order $(1,t)$.

In the case $\mathcal{W}(q)$, we characterize small weight codewords in the corresponding LDPC codes, using geometric arguments. In the case $\mathcal{Q}(4,q)$, q odd, and $\mathcal{H}(4,q^2)^D$, we improve the lower bound on d greatly by using geometric arguments.

3 Small weight codewords in $\mathcal{W}(q)$

The goal in this section is to classify geometrically the small weight codewords in the LDPC code $\mathcal{C}$ defined by $\mathcal{W}(q)$. We remind the reader that, by Property (*), a codeword corresponds to a

set S of points of $\mathcal{W}(q)$ with the property that every line of $\mathcal{W}(q)$ meets S in 0 or in at least 2 points. As $\mathcal{Q}(4,q)$ is isomorphic to the dual of $\mathcal{W}(q)$, we work in $PG(4,q)$ and look at sets of lines lying in a parabolic quadric of $PG(4,q)$ such that every point lies on 0 or on at least 2 of these lines (Property (**)). Since we are working in $\mathcal{W}(q)^D$, the columns of H correspond to the lines of $\mathcal{W}(q)^D = \mathcal{Q}(4,q)$ and the rows of H correspond to the points of $\mathcal{W}(q)^D = \mathcal{Q}(4,q)$. We will therefore describe the coordinate positions in a codeword by their corresponding lines in $\mathcal{Q}(4,q)$.

It is known that the minimum distance, and hence minimum weight, of the LDPC code defined by $\mathcal{W}(q)$ is $2(q+1)$ [1]. We have already mentioned that codewords of weight $2(q+1)$ are relatively easy to generate when we describe them on the dual generalized quadrangle $\mathcal{Q}(4,q)$.

Let $\mathcal{R} = \{\ell_1, \ldots, \ell_{q+1}\}$ and $\mathcal{R}^{opp} = \{m_1, \ldots, m_{q+1}\}$ be a regulus and its opposite regulus. The vector with 1 in the coordinates representing the lines in $\mathcal{R}$ and -1 in the coordinates representing the lines in $\mathcal{R}^{opp}$ is clearly a codeword of the LDPC code arising from $\mathcal{Q}(4,q)^D = \mathcal{W}(q)$.

Now consider two hyperbolic quadrics lying in $\mathcal{Q}(4,q)$ that intersect in a planar conic C. Let $\mathcal{R}_1, \mathcal{R}_1^{opp}, \mathcal{R}_2$, and $\mathcal{R}_2^{opp}$ be the reguli in these two quadrics. Moreover, let

$$\mathcal{R}_1 = \{\ell_1^{(1)}, \ldots, \ell_{q+1}^{(1)}\}, \ \mathcal{R}_1^{opp} = \{m_1^{(1)}, \ldots, m_{q+1}^{(1)}\},$$

$$\mathcal{R}_2 = \{\ell_1^{(2)}, \ldots, \ell_{q+1}^{(2)}\}, \ \mathcal{R}_2^{opp} = \{m_1^{(2)}, \ldots, m_{q+1}^{(2)}\}.$$

Then, the vector $\mathbf{v}$ with a 1 in the coordinates corresponding to the lines $\ell_i^{(1)}$ and $\ell_i^{(2)}$, and a -1 in the coordinates corresponding to the lines $m_j^{(1)}$ and $m_j^{(2)}$, forms a codeword of weight $4q+4$ of the LDPC code arising from $\mathcal{Q}(4,q)^D = \mathcal{W}(q)$.

In a similar fashion, consider two hyperbolic quadrics $\mathcal{H}_1$ and $\mathcal{H}_2$ of $\mathcal{Q}(4,q)$ intersecting in a pair of intersecting lines. Let $\mathbf{v}_1$ be the vector corresponding to $\mathcal{H}_1$. So, $\mathbf{v}_1$ has 1 in the coordinates corresponding to the lines of one of the reguli ruling $\mathcal{H}_1$, -1 in the coordinates corresponding to the lines of the opposite regulus ruling $\mathcal{H}_1$, and zero elsewhere. Define $\mathbf{v}_2$ similarly for $\mathcal{H}_2$, where the two common lines of $\mathcal{H}_1$ and $\mathcal{H}_2$ have the same symbol in $\mathbf{v}_1$ and $\mathbf{v}_2$. Now, the difference $\mathbf{v}_1 - \mathbf{v}_2$ is a codeword of weight $4q$ of the LDPC code $\mathcal{C}$ arising from $\mathcal{Q}(4,q)^D = \mathcal{W}(q)$. The sum $\mathbf{v}_1 + \mathbf{v}_2$ gives a codeword of weight $4q$ if $\mathcal{C}$ is a binary code, and a codeword of weight $4q+2$ if $\mathcal{C}$ is not a binary code.

We prove that the above described codewords are the smallest weight codewords of $\mathcal{C}$, different from those of minimal weight. Essentially, they can be described as being linear combinations of codewords of minimum weight $2(q+1)$.

For even larger weights, this will be true. We will characterize codewords in the LDPC code arising from $\mathcal{W}(q)$, up to weight $\sqrt{q}(q+1)$, as linear combinations of codewords of minimum weight $2(q+1)$. For weights larger than $4q+4$, we will not describe all the different weights of these linear combinations explicitly, since this becomes too tedious to describe.

So, from this point on, let $\mathbf{c}$ be a codeword of $\mathcal{C}$ of weight at most $2\delta(q+1) \leq \sqrt{q}(q+1)$. Such a codeword is easily obtained by, for instance, taking the lines of δ reguli and opposite reguli

of hyperbolic quadrics $\mathcal{Q}^+(3,q)$ inside $\mathcal{Q}(4,q)$, or equivalently, by taking linear combinations of δ codewords of minimum weight in the LDPC code arising from $\mathcal{W}(q)$.

We use property (**) and identify the codeword $\mathbf{c}$ with the set B of lines of $\mathcal{Q}(4,q)$ corresponding to the non-zero positions in the codeword $\mathbf{c}$, and characterize B by using the property that every point of $\mathcal{Q}(4,q)$ lies on 0 or on at least two lines of B. We omit the proof of the following.

Proposition 3.1. *For $q > 9$, if the line ℓ_1 is in B, then there is a hyperbolic quadric $\mathcal{Q} \cong \mathcal{Q}^+(3,q)$ of $\mathcal{Q}(4,q)$ containing ℓ_1 and such that each regulus of $\mathcal{Q}$ contains at least $q - 2\delta + 1$ lines of B.*

Remark 3.2. Following the results of Bagchi and Sastry [1] which characterize the codewords of smallest weight $2(q+1)$ as being a regulus and its opposite regulus, we wish to characterize the codewords of weight in between $2q+3$ and $2\delta(q+1)$. So no single hyperbolic quadric $\mathcal{Q}$ can contain all the lines of B.

We also assume by induction on the weights of the codewords of $\mathcal{C}$ that all codewords of $\mathcal{C}$ of weight smaller than the weight of $\mathbf{c}$ have been characterized as being linear combinations of codewords of minimal weight $2(q+1)$.

We have shown the following results whose proofs are omitted.

Proposition 3.3. *Let B be any set of at most $2\delta(q+1) \leq \sqrt{q}(q+1)$ lines of $\mathcal{Q}(4,q)$, $q \geq 11$, such that every point of $\mathcal{Q}(4,q)$ lies on either 0 or on at least 2 lines of B. Then all the lines of B lie in at most $\delta + 1$ distinct hyperbolic quadrics of $\mathcal{Q}(4,q)$ having in every regulus at least $q - 2\delta + 1$ lines of B.*

Proposition 3.4. *In the LDPC code defined by $\mathcal{W}(q)$, $q \geq 11$, every codeword of weight at most $\sqrt{q}(q+1)$ is a linear combination of codewords of minimal weight $2(q+1)$.*

Proposition 3.5. *In the LDPC code defined by $\mathcal{H}(3,q^2)$, $q \geq 11$, every codeword of weight at most $\sqrt{q}(q+1)$ is a linear combination of codewords of minimal weight $2(q+1)$.*

4 Minimum weight of the LDPC code of $\mathcal{Q}(4,q)$, q odd

For q even, $\mathcal{W}(q)$ is self-dual (Theorem 2.1 (2)), so the preceding results also give characterization results on the small weight codewords of the LDPC code defined by $\mathcal{W}(q)^D = \mathcal{Q}(4,q)$.

For q odd, $\mathcal{W}(q)$ is not self-dual. This can also be seen by the fact that the results for the LDPC code defined by $\mathcal{W}(q)^D = \mathcal{Q}(4,q)$ are different from those for the LDPC code defined by $\mathcal{W}(q)$.

We now improve greatly the lower bound $d \geq 2(q+2)$ on the minimum distance of the LDPC code arising from $\mathcal{Q}(4,q)$, q odd.

From Property (*), codewords in the LDPC code arising from $\mathcal{Q}(4,q)$ define sets of points in the parabolic quadric $\mathcal{Q}(4,q)$ with the property that every line of $\mathcal{Q}(4,q)$ meets this point set in 0 or in at least 2 points. Let S be a set of points with this property.

Lemma 4.1. *Let x be the maximal size of intersection of S with a conic C of $\mathcal{Q}(4,q)$. Then $|S| \geq x(q+1)/2$.*

Proof. Let C be a conic of $\mathcal{Q}(4,q)$ containing x points of S. As no two lines of $\mathcal{Q}$ are coplanar, the points of $S \cap C$ lie on $x(q+1)$ lines of $\mathcal{Q}(4,q)$. Using properties of the parabolic quadric $\mathcal{Q}(4,q)$, q odd, there are at most 2 points collinear with all points of C [17]. We subtract $2x$ to not consider the incidences of these points with the lines of $\mathcal{Q}(4,q)$ through the points of $S \cap C$. So, there are at least $x(q-1)$ other lines of $\mathcal{Q}(4,q)$ through the points of $S \cap C$. They all contain at least one point of S not in C.

A point of $\mathcal{Q}(4,q)$, not collinear with all points of C, is collinear with at most two points of $S \cap C$. So, there are at least $x(q-1)/2$ other points in S. Adding the x points of $S \cap C$, $|S| \geq x(q-1)/2 + x = x(q+1)/2$. □

Lemma 4.2. *Let x be the maximal size of intersection of S with a conic of $\mathcal{Q}(4,q)$, q odd. Then,*

$$|S| \geq \frac{q^2}{2x} + 3\frac{q}{2} + \frac{x}{8} + 2.$$

Proof. Select a point P of S and consider the $q+1$ lines of $\mathcal{Q}(4,q)$ through P. They all contain at least one other point P_i, $i = 0, \ldots, q$, of S. The points $P_0, \ldots, P_q$ are pairwise non-collinear.

Each point P_i, $i = 0, \ldots, q$, is collinear with at least $q+1$ other points of S; P included.

For $P_i \neq P_j$, $P_i^\perp \cap P_j^\perp$ is a conic of $\mathcal{Q}(4,q)$, containing at most x points of S. Then

$$|S| \geq |\cup_{j=0}^{i} (P_j^\perp \cap S) \setminus \{P, P_j\}| \geq \sum_{j=0}^{i} (q - jx) = q(i+1) - \frac{xi(i+1)}{2} = f(i).$$

The maximum for $f(i)$ is obtained for $i = (2q-x)/(2x)$. Plugging this value into f gives $f\left(\frac{2q-x}{2x}\right) = \frac{q^2}{2x} + \frac{q}{2} + \frac{x}{8}$. Adding the points $P, P_0, \ldots, P_q$ gives

$$|S| \geq \frac{q^2}{2x} + 3\frac{q}{2} + \frac{x}{8} + 2.$$

□

Set

$$\frac{x(q+1)}{2} = \frac{q^2}{2x} + \frac{3q}{2} + \frac{x}{8} + 2.$$

This is valid for

$$x = \frac{8 + 6q + 4\sqrt{(q+1)^3 + 3q + 3}}{3 + 4q}.$$

So

$$|S| \geq \frac{(q+1)x}{2} = \frac{(q+1)(4 + 3q + 2\sqrt{(q+1)^3 + 3q + 3})}{3 + 4q}.$$

Theorem 4.3. *The LDPC code arising from $\mathcal{Q}(4,q)$, q odd, has minimum distance at least*

$$\frac{(q+1)(4 + 3q + 2\sqrt{(q+1)^3 + 3q + 3})}{3 + 4q} \approx \frac{(q+1)\sqrt{q}}{2}.$$

Computer searches gave the following exact values for the minimum distance of binary LDPC codes arising from $\mathcal{Q}(4,q)$, q odd, q small.

Theorem 4.4. *The minimum distances of the binary LDPC codes arising from $\mathcal{Q}(4,3)$ and $\mathcal{Q}(4,5)$ are 10 and 20, respectively.*

5 Minimum weight of codewords in $\mathcal{H}(4,q^2)^D$

We now consider the Hermitian variety $\mathcal{U}$ in $PG(4,q^2)$ defining the GQ $\mathcal{H}(4,q^2)$. In this setting, we will make use of the isomorphism between $\mathcal{H}(3,q^2)^D$ and $\mathcal{Q}^-(5,q)$ (Theorem 2.1 (3)).

Lemma 5.1. ([17]) *For three pairwise skew lines ℓ_1,ℓ_2 and ℓ_3 of $\mathcal{H}(3,q^2)$, $|\{\ell_1,\ell_2,\ell_3\}^\perp| = q+1$.*

Lemma 5.2. *Every non-zero codeword of the LDPC code defined by $\mathcal{H}(4,q^2)^D$ has weight at least $q\sqrt{(q^2+1)(q-1)}+q^2+2$.*

References

[1] B. Bagchi and N.S. Narasimha Sastry, Codes associated with generalized polygons, Geom. Dedicata, Vol. 27 (1988) pp. 1-8.

[2] M.C. Davey and D.J.C. MacKay, Low density parity check codes over $GF(q)$, IEEE Communications Letters, Vol. 2, No. 6 (1998) pp. 165-167.

[3] M.P.C. Fossorier, Quasicyclic low-density parity-check codes from circulant permutation matrices, IEEE Trans. Inform. Theory, Vol. 50 (2004) pp. 1788-1793.

[4] R.G. Gallager, Low density parity check codes, IRE Trans. Inform. Theory, Vol. 8 (1962) pp. 21-28.

[5] J.W.P. Hirschfeld and J.A. Thas, *General Galois Geometries.* Oxford University Press (1991).

[6] X.Y. Hu, M.P.C. Fossorier and E. Eleftheriou, On the computation of the minimum distance of low-density parity-check codes, 2004 IEEE International Conference on Communications, Vol. 2 (2004) pp. 767-771.

[7] S.J. Johnson and S.R. Weller, Construction of low-density parity-check codes from Kirkman triple systems, In Proc. IEEE Globecom Conf., San Antonio, TX, Nov. 2001, available at http://www.ee.newcastle.edu.au/users/staff/steve/

[8] S.J. Johnson and S.R. Weller, Regular low-density parity-check codes from combinatorial designs, In Proc. IEEE Inform. Theory Workshop, Cairns, Australia, Sep. 2001, pp. 90-92.

[9] S.J. Johnson and S.R. Weller, Codes for iterative decoding from partial geometries, Proc. IEEE Int. Sym. Inform. Theory, Switzerland, June 30 - July 5, (2002), 6 page, extended abstract, available at http://murray.newcastle.edu.au/users/staff/steve/

[10] J.-L. Kim, U. Peled, I. Perepelitsa, V. Pless and S. Friedland, Explicit construction of families of LDPC codes with no 4-cycles, IEEE Trans. Inform. Theory, Vol. 50 (2004) pp. 2378–2388.

[11] Y. Kou, S. Lin and M.P.C. Fossorier, Low-density parity-check codes based on finite geometries: a rediscovery and new results, IEEE Trans. Inform. Theory, Vol. 47, No. 7 (2001) pp. 2711–2736.

[12] Z. Liu and D.A. Pados, LDPC codes from generalized polygons, IEEE Trans. Inform. Theory, Vol. 51, No. 11 (2005) pp. 3890–3898.

[13] D.J.C. MacKay, Good error correcting codes based on very sparse matrices, IEEE Trans. Inform. Theory, Vol. 45 (1999) pp. 399-431.

[14] D.J.C. MacKay and M.C. Davey, Evaluation of Gallager codes for short block length and high rate applications, Codes, Systems and Graphical Models, B. Marcus and J. Rosenthal, editors, Vol. 123, IMA in Math. and its Appl., Springer-Verlag, New York, (2000) pp. 113–130.

[15] D.J.C. MacKay and R.M. Neal, Near Shannon limit performance of low density parity check codes, Electron. Lett., Vol. 32, No. 18 (1996) pp. 1645–1646.

[16] G.A. Margulis, Explicit constructions of graphs without short cycles and low density codes, Combinatorica, Vol. 2 (1982) pp. 71–78.

[17] S.E. Payne and J.A. Thas, *Finite Generalized Quadrangles*, Pitman Advanced Publishing Program, (1984).

[18] J. Rosenthal and P.O. Vontobel, Construction of LDPC codes using Ramanujan graphs and ideas from Margulis. Proc. 38th Allerton Conf. on Communications, Control, and Computing, P.G Voulgaris and R. Srikant, Eds., Oct. 4-6, (2000) pp. 248–257.

[19] M. Sipser and D.A. Spielman, Expander codes, IEEE Trans. Inform. Theory, Vol. 42 (1996) pp. 1710–1722.

[20] R.M. Tanner, A recursive approach to low-complexity codes, IEEE Trans. Inform. Theory, Vol. 27 (1981) pp. 533–547.

[21] R.M. Tanner, Minimum-distance bounds by graph analysis, IEEE Trans. Inform. Theory, Vol. 47 (2001) pp. 808–821.

[22] R.M. Tanner, D. Sridhara, A. Sridharan, T.E. Fuja and D.J. Costello, Jr., LDPC block and convolutional codes based on circulant matrices, IEEE Trans. Inform. Theory, Vol. 50 (2004) pp. 2966–2984.

[23] P. O. Vontobel and R M. Tanner, Construction of codes based on finite generalized quadrangles for iterative decoding, Proceedings of 2001 IEEE Intern. Symp. Inform. Theory, (2001) p. 223.

[24] S.R. Weller and S.J. Johnson, Regular low-density parity-check codes from oval designs, European Transactions on Telecommunications Vol. 14, No. 5 (2003) pp. 399-409.

Addresses of the authors:

Jon-Lark Kim
University of Louisville
Department of Mathematics
328 Natural Sciences Building
Louisville, KY 40292, USA
(jl.kim@louisville.edu, http://www.math.louisville.edu/~jlkim)

Keith E. Mellinger
Department of Mathematics
University of Mary Washington
1301 College Avenue, Trinkle Hall
Fredericksburg, VA 22401
(kmelling@umw.edu, http://people.umw.edu/ ~kmelling)

Leo Storme
Ghent University
Department of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22
9000 Ghent, Belgium
(ls@cage.ugent.be, http://cage.ugent.be/~ls)

Transitive decompositions of graphs

Michael Giudici
School of Mathematics and Statistics
The University of Western Australia
35 Stirling Highway
Crawley WA 6009 Australia
email: giudici@maths.uwa.edu.au

A *decomposition* of a graph is a partition of the edge set. One can also look at partitions of the arc set but in this talk we restrict our attention to edges. If each part of the decomposition is a spanning subgraph then we call the decomposition a *factorisation* and the parts are called *factors*. Decompositions are especially interesting when the subgraphs induced by each part are pairwise isomorphic. Such decompositions are known as *isomorphic decompositions*. Decompositions of graphs have been widely studied and much attention has been paid to determining when a given graph can be decomposed into copies of a certain subgraph, for example, cycles or 1-factors. See for example [2, 8, 9, 10, 16].

A special class of decompositions is transitive decompositions. A *G-transitive decomposition* of a graph Γ is a decomposition which is invariant under some group G of automorphisms of Γ such that G acts transitively on the set of parts of the decomposition. This class of decompositions has been widely studied in many different guises. A *partial linear space* is a set of points and a set of subsets of the point set called *lines*, such that each pair of points is contained in at most one line. Given a decomposition of a graph into complete subgraphs, we can form a partial linear space with point set the set of vertices and line set the set of parts of the decomposition. Since each edge lies in only one part, every pair of points lies in at most one line, and so we indeed have a partial linear space. If the decomposition is G-transitive, then the partial linear space is G-line-transitive, and if G is also transitive on the set of arcs of the graph then the partial line space is G-flag-transitive. Conversely, given a G-line-transitive partial linear space we can construct a G-transitive decomposition of the collinearity graph of the partial linear space, that is, of the graph with vertices the set of points such that two points are adjacent if they lie on the same line. In the special case where the original graph is a complete graph then we have a linear space, that is, every two points lie on a unique line. Flag-transitive linear spaces were classified in [3].

If G is an arc-transitive group of automorphisms of the complete graph K_n then G acts 2-transitively on a set of size n. Cameron and Korchmáros [4] have determined all factorisations of complete graphs into 1-factors with a 2-transitive automorphism group, while Sibley [15] has extended this to a classification of all G-transitive decompositions of complete graphs such that G is 2-transitive. Sibley calls such decompositions *2-transitive edge-coloured graphs*. Recently all G-transitive decompositions of graphs with G rank 3 of product action [1] have been characterised.

A special class of transitive decompositions are *homogeneous factorisations*. These are G-transitive decompositions such that the kernel of the action of G on the partition is vertex-transitive. This forces all parts of the decomposition to be spanning subgraphs and so we do indeed have a factorisation. Homogeneous factorisations of complete graphs were first introduced in [13] as a generalisation of vertex-transitive self-complementary graphs. The concept was extended to arbitrary graphs in [11].

The **Johnson graph** $J(n,k)$ is the graph with vertex set the set of k-subsets of an n-set such that two vertices are adjacent if they intersect in a $(k-1)$-set. Since $J(n,k) \cong J(n,n-k)$ we always assume that $2k \leq n$. If $2k < n$ then $\mathrm{Aut}(J(n,k)) = S_n$ while when $n = 2k$ we have $\mathrm{Aut}(J(n,k)) = S_n \times S_2$.

Cuaresma studied homogeneous factorisations of Johnson graphs in her PhD thesis [5]. In particular, she proved that there are no homogeneous factorisations of $J(n,k)$ for $k \geq 4$ and showed that homogeneous factorisations of $J(n,3)$ exist if and only if $n = 8$ or $n = 2^l + 1$ for l a power of an odd prime. Moreover, all such homogeneous factorisations were determined. The homogeneous factorisations of $J(n,2)$ were also completely determined, except for a couple of unresolved cases where G is an affine group. When G is not affine, the only homogeneous factorisations of $J(n,2)$ have index two and occur for $n-1 = q \equiv 1 \pmod 4$ and G a 3-transitive subgroup of $\mathrm{P\Gamma L}(2,q)$.

Despite the scarcity of homogeneous factorisations of Johnson graphs there are three infinite families of transitive decompositions of $J(n,k)$.

Construction 1. *Let X be an n-set. For each $(k-1)$-subset Y of X, let P_Y be the complete subgraph of $J(n,k)$ of size $n-k+1$ induced on the set of k-subsets containing Y. Since the symmetric group S_n acts transitively on the set of all $(k-1)$-subsets of X, it follows that*

$$\mathcal{P}_\cap = \{P_Y \mid Y \text{ a } (k-1)\text{-subset of } X\}$$

is an S_n-transitive decomposition of $J(n,k)$.

Construction 2. *Let X be an n-set. For each $(k+1)$-subset W of X, let Q_W be the complete subgraph of $J(n,k)$ of size $k+1$ induced on the set of k-subsets contained in W. Then*

$$\mathcal{P}_\cup = \{Q_W \mid W \text{ a } (k+1)\text{-subset of } X\}$$

is an S_n-transitive decomposition of $J(n,k)$.

Construction 3. *Let X be an n-set and $\{a,b\} \subseteq X$. Then*

$$M_{\{a,b\}} = \{\{\{a\} \cup Y, \{b\} \cup Y\}\} \mid Y \text{ a } (k-1)\text{-subset of } X \backslash \{a,b\}\}$$

is a matching with $\binom{n-2}{k-1}$ edges. Since S_n acts 2-transitively on X it follows that

$$\mathcal{P}_\ominus = \{M_{\{a,b\}} \mid \{a,b\} \subseteq X\}$$

is an S_n-transitive decomposition.

Constructions 1 and 2 were first pointed out to us by Michael Orrison and Construction 1 is used in [14] for the analysis of unranked data. After my talk at the conference, Misha Klin brought to my attention that Constructions 1 and 2 were used in [12] to aid in determining maximal subgroups of the symmetric groups.

Recently Devillers, Praeger, Li and the speaker have been involved in a project to determine all G-transitive decompositions of the Johnson graphs $J(n,k)$ with G arc-transitive [6]. We will now outline some of the results in the case where $G \leqslant S_n$. The case where $n = 2k$ and $G \not\leqslant S_n$ is dealt with in [6]. We first need the possibilities for G. Given a subset A of a set X, we use $\overline{A}$ to denote the complement of A in X.

Proposition 4. *[5, Proposition 3.2] Let $\Gamma = J(n,k)$ and $G \leqslant S_n$. The graph Γ is G-arc transitive if and only if G is k-homogeneous and, for A any k-subset, G_A is transitive on $A \times \overline{A}$.*

Corollary 5. *If $G \leqslant S_n$ is $(k+1)$-transitive, then Γ is G-arc transitive. If Γ is G-arc transitive, then $G \leqslant S_n$ is $k-$ and $(k+1)$-homogeneous.*

Suppose that $\mathcal{P}$ is a G-transitive decomposition of Γ such that $G^{\mathcal{P}}$ is imprimitive. Then there is a partition $\mathcal{P}'$ of the edge-set of Γ refined by $\mathcal{P}$ and preserved by G such that $G^{\mathcal{P}'}$ is primitive. Thus we may restrict our attention to studying only those G-transitive decompositions for which G acts primitively on the edge-partition. We call such decompositions *G-primitive decompositions.*

The first group to look at is $G = S_n$. We have the following classification.

Theorem 6. *[6] The S_n-primitive decompositions of $J(n,k)$ are:*

- *$\mathcal{P}_\cap$,*
- *$\mathcal{P}_\cup$ for $n \neq 2k+2$,*
- *$\mathcal{P}_\ominus$ for $(n,k) \neq (4,2)$,*
- *a partition with parts isomorphic to $2K_{k+1}$ for $n = 2k+2$,*
- *a partition with parts isomorphic to $6K_2$ for $(n,k) = (6,3)$, and*
- *a partition with parts isomorphic to C_4 for $(n,k) = (4,2)$.*

We note that the partition with parts isomorphic to $2K_{k+1}$ arises since for $n = 2k+2$, the stabiliser of a $(k+1)$-subset is not maximal in S_n and so $\mathcal{P}_\cup$ is not an S_n-primitive decomposition in this case. Similarly, the partition with parts isomorphic to C_4 arises as the stabiliser of a 2-set is not maximal in S_4.

If $G = A_n$ then we find two further primitive decompositions.

Theorem 7. *[6] The A_n-primitive decomposition of $J(n,k)$ which are not preserved by S_n are:*

- *a partition with parts isomorphic to C_5 for $(n,k) = (5,2)$, and*
- *a partition with Petersen graphs as parts for $(n,k) = (6,3)$.*

By Corollary 5, the only subgroups of S_n which are arc-transitive on $J(n,k)$ for $k \geq 5$ are A_n and S_n. For $k = 4$ there are two additional arc-transitive groups: M_{24} when $n = 24$ and M_{12} when $n = 12$.

Theorem 8. *[6] The M_{24}-primitive decompositions of $J(24,4)$ are:*

- *$\mathcal{P}_\cap$, with parts K_{21},*

- $\mathcal{P}_\ominus$, *with parts* $\binom{22}{3}K_2$,
- *a partition with parts* $21K_5$,
- *a partition with parts* $J(8,4)$.

The third partition occurs as the stabiliser of a 5-subset is not maximal in M_{24} and so $\mathcal{P}_\cup$ is not an M_{24}-primitive decomposition. Moreover, in the case of the fourth partition, we get one part for each octad of the Witt design $S(5,8,24)$.

Theorem 9. *[6] The M_{12}-primitive decompositions of $J(12,4)$ are:*

- $\mathcal{P}_\cap$, *with parts* K_9,
- $\mathcal{P}_\ominus$, *with parts* $\binom{10}{3}K_2$,
- *a partition with parts* $66K_5$,
- *a partition with parts* $16K_2$,
- *a partition with parts* $36K_2$,
- *two partitions with parts* $12K_3$,
- *a partition with parts* $2J(6,4)$,
- *a partition with parts isomorphic to a graph on 165 vertices with valency 8 and automorphism group* M_{11}.

The third partition occurs as the stabiliser of a 5-subset is not maximal in M_{12} and so $\mathcal{P}_\cup$ is not an M_{12}-primitive decomposition. In the seventh case, we get one part for each pair of complementary hexads in the Witt design $S(5,6,12)$. The graph in the last decomposition is very intriguing and is studied further in [7].

The G-primitive decompositions of $J(n,2)$ and $J(n,3)$ with G arc-transitive are determined in [6]. Some of the interesting ones include:

- $(n,k) = (23,3)$, $G = M_{23}$ and parts $J(7,3)$.
- $(n,k) = (11,3)$, $G = M_{11}$ and parts $J(5,2)$.
- $(n,k) = (11,3)$, $G = M_{11}$ and parts a graph on 55 vertices, valency 6 and automorphism group PSL(2, 11).
- $(n,k) = (22,2)$, $G = M_{22}$ and parts $J(6,2)$.
- $(n,k) = (2^d,2)$, $G = \mathrm{AGL}(d,2)$ and parts $2^{d-2}K_{2,2,2}$.
- $(n,k) = (q+1,2)$, $G = \mathrm{PGL}(2,q)$ and parts $J(q_0,2)$ where $q = q_0^r$.

References

[1] J. Bamberg, G. Pearce and C. E. Praeger, Transitive decompositions of graph products: rank 3 product action type, submitted.

[2] J. Bosák, Decompositions of Graphs, Kluwer Academic Publishers, Dordrecht, The Netherlands, 1990.

[3] F. Buekenhout, A. Delandtsheer, J. Doyen, P. B. Kleidman, M. W. Liebeck, and J. Saxl, Linear spaces with flag-transitive automorphism groups. Geom. Dedicata 36 (1990), 89–94.

[4] P. J. Cameron and G. Korchmáros, One-factorizations of complete graphs with a doubly transitive automorphism group. Bull. London Math. Soc. 25 (1993), 1–6.

[5] M. C. Cuaresma, Homogeneous Factorisations of Johnson Graphs, PhD, University of Philippines, 2004.

[6] A. Devillers, M. Giudici, C. H. Li and C. E. Praeger, Primitive decompositions of Johnson graphs, in preparation.

[7] A. Devillers, M. Giudici, C. H. Li and C. E. Praeger, A remarkable Mathieu graph tower, in preparation.

[8] F. Harary, R. W. Robinson and N. C. Wormald, Isomorphic factorisations. I. Complete graphs, Trans. Amer. Math. Soc. 242 (1978), pp. 243-260.

[9] F. Harary and R. W. Robinson, Isomorphic factorisations X: unsolved problems, J. Graph Theory 9 (1985), pp. 67-86.

[10] K. Heinrich, Graph decompositions and designs, in: The CRC Handbook of Combinatorial Designs, Charles J. Colbourn and Jeffrey H. Dinitz, (Editors), CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1996, pp. 361-366.

[11] M. Giudici, C.H. Li, P. Potočnik and C. E. Praeger, Homogeneous factorisations of graphs and digraphs. European J. Combin. 27 (2006), 11–37.

[12] L. A. Kalužnin and M. H. Klin, On some maximal subgroups of symmetric and alternating groups, Mat. Sbornik 87 (1972) 91–121 (in Russian).

[13] C. H. Li and C. E. Praeger, On partitioning the orbitals of a transitive permutation group, Trans. Amer. Math. Soc. 355 (2003), 637–653.

[14] D. K. Maslen, M. E. Orrison and D. N. Rockmore, Computing isotypic projections with the Lanczos iteration, SIAM J. Matrix Anal. Appl. 25 (2003), 784–803.

[15] T. Sibley, On classifying finite edge colored graphs with two transitive automorphism groups. J. Combin. Theory Ser. B 90 (2004), no. 1, 121–138.

[16] R. M. Wilson, Decompositions of complete graphs into subgraphs isomorphic to a given graph, in: Proceedings of the Fifth British Combinatorial Conference (Univ. Aberdeen, Aberdeen, 1975), pp. 647–659. Congressus Numerantium, No. XV, Utilitas Math., Winnipeg, Man., 1976.

Normal cyclotomic schemes over a finite commutative ring

Sergei Evdokimov
Steklov Institute of Mathematics
at St. Petersburg
evdokim@pdmi.ras.ru

Ilia Ponomarenko
Steklov Institute of Mathematics
at St. Petersburg
inp@pdmi.ras.ru

Extended abstract

Let R be a finite commutative ring[1] and K a subgroup of its multiplicative group $R^\times$. Denote by $\mathrm{Rel}(K,R)$ the set of all binary relations on R of the form $\{(x,y)\in R\times R : y-x\in rK\}$, $r\in R$. Then the pair

$$\mathrm{Cyc}(K,R)=(R,\mathrm{Rel}(K,R))$$

is an association scheme on R. We call it a *cyclotomic scheme over* R corresponding to the group K. Clearly, it is the scheme of 2-orbits of the group $\Gamma(K,R)=\{\gamma_{a,b} : a\in K, b\in R\}$ where $\gamma_{a,b}$ is the permutation of the set R taking x to $ax+b$. In particular, it is a Cayley scheme over the additive group R^+ of R or a translation scheme in the sense of [1]. Moreover, the multiplications by elements of $R^\times$ are Cayley isomorphisms of this scheme.

Cyclotomic schemes over a field were introduced by P. Delsarte (1973) in connection with coding theory. In [5] it was proved that any such scheme is uniquely determined up to isomorphism by its 3-dimensional intersection numbers. Cyclotomic schemes over rings were introduced and studied in [2] within the framework of the duality theory for association schemes. We also mention paper [4] where cyclotomic schemes over Galois rings were used to construct amorphous association schemes. Here we are interested in the automorphism groups of cyclotomic schemes.

Probably, as the first result on the automorphism groups of cyclotomic schemes one should consider the well-known Burnside theorem on permutation groups of prime degree. In fact, this theorem completely determine the former groups for a prime field. In the case of an arbitrary finite field we have the following result which is the interpretation of an old number-theoretical result from [3] (see also [1, p.389]).

Theorem 1 *If C is a cyclotomic scheme over a finite field $\mathbb{F}$, then* $\mathrm{Aut}(C)\le \mathrm{A\Gamma L}_1(\mathbb{F})$ *whenever* $\mathrm{rk}(C)>2$.

For the cyclotomic schemes over the ring $\mathbb{Z}_n$ of integers modulo a positive integer n the analog of Theorem 1 is not true. Indeed, any such scheme being a Cayley scheme over a cyclic group $\mathbb{Z}_n^+$ can be treated up to language as an S-ring over the same group. In accordance with [6, 5] any such S-ring can be constructed from normal S-rings and

[1]Throughout the paper all rings are supposed to have identity.

S-rings of rank 2 by means of tensor products and generalized wreath products (or wedge products in terms of [6]). Here normal S-rings are exactly those coming from cyclotomic schemes $\mathcal{C}$ such that $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(\mathbb{Z}_n) = \mathrm{AGL}_1(\mathbb{Z}_n)$. However, even among the S-rings corresponding to cyclotomic schemes there exist non-normal ones.

The above discussion leads to the following definition.

Definition 1 *A cyclotomic scheme $\mathcal{C}$ over a finite commutative ring R is called normal if* $\mathrm{Aut}(\mathcal{C}) \le \mathrm{A\Gamma L}_1(R)$.

Our goal is to identify the normal cyclotomic schemes.[2] Since any finite commutative ring is the direct product of local rings, the following theorem reduces the general case to the local one (and, moreover, gives some product formula for two-points stabilizers of the automorphism group). Below for $R = \prod_i R_i$ we use the following notation. For a cyclotomic scheme $\mathcal{C} = \mathrm{Cyc}(K, R)$ set $\mathcal{C}_i = \mathrm{Cyc}(K_i, R_i)$ where K_i is defined from the equality $\varphi_i(K_i) = K \cap \varphi_i(R_i^\times)$ with φ_i being the monomorphism of $R_i^\times$ to $R^\times$ such that the jth component of $\varphi_i(x)$ equals x for $j = i$, and equals 1_{R_j} for $j \ne i$.

Theorem 2 *Let $R = \prod_i R_i$ be a finite commutative ring and $\mathcal{C}$ a cyclotomic scheme over R. Then*

$$\mathrm{Aut}(\mathcal{C})_{u,v} = \prod_i \mathrm{Aut}(\mathcal{C}_i)_{u_i,v_i}$$

where $u = 0_R$, $v = 1_R$ and $u_i = 0_{R_i}$, $v_i = 1_{R_i}$ for all i. In particular, the scheme $\mathcal{C}$ is normal iff the scheme $\mathcal{C}_i$ is normal for all i.

The following theorem gives a necessary condition for a cyclotomic scheme over a local ring to be normal. We do not know any example when this condition is not sufficient. Below we set $I_0 = \{x \in \mathrm{rad}(R) : x\,\mathrm{rad}(R) = \{0\}\}$.

Theorem 3 *Let a cyclotomic scheme $\mathrm{Cyc}(K, R)$ over a finite local commutative ring R be normal. Suppose that $K = K + I$ for some ideal I of R. Then $I = \{0\}$ unless $q = 2$ where q is the order of the residue field of R. Moreover, if $q = 2$, then $I \subset I_0$.*

The proofs of Theorems 2 and 3 are based on the ideas of [5].

Let R be a local commutative ring. Given a group $K \le R^\times$ denote by $\mathcal{I}_K$ the set of all ideals I of R such that $K + I = K$ or, equivalently, $1 + I \subset K$. It is convenient for us to formulate the following definition.

Definition 2 *A group $K \le R^\times$ is called pure if the condition $I \in \mathcal{I}_K$ implies that $I = \{0\}$.*

If R is a field, then obviously any subgroup of $R^\times$ is pure. Besides, Theorem 3 implies that for $q > 2$ the group K is pure whenever the scheme $\mathrm{Cyc}(K, R)$ is normal. It turns out that for the Galois rings of odd characteristic other than fields this necessary condition of normality is also sufficient. (The case of even characteristic is more complicated and will be treated in a subsequent paper.)

Theorem 4 *Let R be a Galois ring of odd characteristic other than a field. Then the scheme $\mathrm{Cyc}(K, R)$ is normal iff the group K is pure.*

[2] The case $R = \mathbb{Z}_n$ was treated in [5].

Let $R = \mathrm{GR}(p^d, r)$ be a Galois ring of characteristic p^d with the residue field of cardinality $q = p^r$ where p is a prime. If $d > 1$ and $p > 2$ (the case of Theorem 4), then it is easy to see that a group $K \leq R^\times$ is pure iff it does not contain the group $1 + p^{d-1}R$. On the other hand, if $d = 1$, i.e. $R = \mathbb{F}$ is a field of cardinality q, then the equality $\mathrm{rk}(\mathcal{C}) = 2$ implies that $\mathrm{Aut}(\mathcal{C}) = \mathrm{Sym}(\mathbb{F})$. Besides, $\mathrm{Sym}(\mathbb{F}) \leq \mathrm{A\Gamma L}_1(\mathbb{F})$ iff $q \leq 4$. Thus after combining Theorems 4 and 1 we come to the following statement.

Theorem 5 *Let $R = \mathrm{GR}(p^d, r)$ with $p > 2$. Then a cyclotomic scheme $\mathrm{Cyc}(K, R)$ is normal exactly in one of the following cases:*

(1) *$d = 1$ and either $(p, r) = (3, 1)$ or $K \neq R^\times$,*

(2) *$d > 1$ and $K \not\geq 1 + p^{d-1}R$.*

One of the ideas to prove the sufficiency in Theorem 4 is to develop a reduction technique for cyclotomic schemes over an arbitrary local ring R. We note that for an ideal I of R the scheme $\mathrm{Cyc}(\pi_I(K), R/I)$ where $\pi_I : R \to R/I$ is the natural epimorphism, can be treated as a factor-scheme of the scheme $\mathrm{Cyc}(K, R)$. This simple observation is used in the proof of the following reduction statement. Below we set $\pi_0 = \pi_{I_0}$.

Theorem 6 *Let R be a finite local commutative ring, $\mathcal{C} = \mathrm{Cyc}(K, R)$ where $K \leq R^\times$ is a pure group, and $\mathcal{C}' = \mathrm{Cyc}(K', R')$ where $K' = \pi_0(K)$ and $R' = R/I_0$. Then the scheme $\mathcal{C}$ is normal whenever so is the scheme $\mathcal{C}'$.*

Unfortunately, in the general case the group K' is not pure (even if R is a Galois ring of even characteristic). So Theorem 6 cannot be used for a direct inductive proof of the normality of the scheme $\mathcal{C}$. However, if R is a Galois ring of odd characteristic, then this is true and Theorem 4 is reduced to the case $\mathrm{rad}(R)^2 = \{0\}$. Thus, due to Theorem 1 it suffices to prove the following statement.

Theorem 7 *Let R be a finite local commutative ring other than a field for which $\mathrm{rad}(R)^2 = \{0\}$. Then the scheme $\mathrm{Cyc}(K, R)$ is normal whenever the group K is pure.*

Theorems 6 and 7 are proved by using the S-ring technique. Namely, for a cyclotomic scheme $\mathcal{C}$ over R together with the ordinary (addition) S-ring over R^+ corresponding to $\mathcal{C}$ we consider its *multiplication* S-ring $\mathcal{A}$ over $R^\times$ (when R is a field this S-ring was introduced and studied in [5]; in the general case the definition is similar). Everything is reduced to the case of a pure group $K \leq \mathcal{T}\mathcal{U}_0$ where $\mathcal{T}$ is the Teichmüller subgroup of $R^\times$ and $\mathcal{U}_0 = 1 + I_0$. Then the group $\mathrm{Aut}(\mathcal{C})_{u,v}$ acts faithfully on $R^\times$ and the image of this action equals $\mathrm{Aut}(\mathcal{A})$. Moreover, in this case the S-ring $\mathcal{A}$ contains the groups $\mathcal{T}$ and $\mathcal{U} = 1 + \mathrm{rad}(R)$, and becomes trivial after adding to it the cosets by any of these groups. This enables us to prove that the group $\mathrm{Aut}(\mathcal{C})$ normalizes the group $\mathrm{AGL}_1(R)$. The latter means that $\mathrm{Aut}(\mathcal{C}) \leq \mathrm{A\Gamma L}_1(R)$, i.e. the scheme $\mathcal{C}$ is normal.

In fact, the developed technique permits us to obtain the following sufficient condition of normality for an arbitrary finite local commutative ring R: the scheme $\mathrm{Cyc}(K, R)$ is normal whenever the group K is strongly pure. (Here we call a group $K \leq R^\times$ *strongly pure* if it is pure and the group $\pi_0(K)$ is strongly pure unless R is a field.) It should be noted that this condition is not necessary.

In some cases one can say a little bit more on the automorphism group of a normal cyclotomic scheme $\mathcal{C} = \mathrm{Cyc}(K, R)$ where R is a finite local commutative ring. For instance, if $K \leq \mathcal{T}$ and R is not a field, then

$$\mathrm{Aut}(\mathcal{C}) \leq \mathrm{AGL}_1(R).$$

This inclusion remains true also in some other cases. In particular, this is so if the group K is strongly pure, and either $K \leq \mathcal{U}$ or the residue filed $\mathbb{F}$ of R is prime. The reason of this is that in both cases the natural mapping

$$\mathrm{Aut}_{\mathcal{C}}(R) \to \mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$$

is a monomorphism and the group $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$ is trivial where by definition $\mathrm{Aut}_{\mathcal{C}}(R)$ (resp. $\mathrm{Aut}_{\mathcal{C}}(\mathbb{F})$) consists of all automorphisms of R (resp. $\mathbb{F}$) that are automorphisms of $\mathcal{C}$ (resp. the factor-scheme of $\mathcal{C}$ on $\mathbb{F}$). It should be noted that generally the kernel of the quotient homomorphism $\mathrm{Aut}(R) \to \mathrm{Aut}(\mathbb{F})$ is not trivial. For instance, for $R = \mathbb{F}[X]/(X^2)$ the group $\mathrm{Aut}(R)$ is isomorphic to the semidirect product of $R^\times$ by $\mathrm{Aut}(\mathbb{F})$ (indeed, the mapping $a + b\pi \mapsto a^\sigma + b^\sigma \alpha \pi$ where $a, b \in \mathbb{F}$ and $\pi = X \mod X^2$, is an automorphism of R for any $\sigma \in \mathrm{Aut}(\mathbb{F})$ and $\alpha \in R^\times$).

It should be noted that the developed technique permits us to give a new proof of Theorem 1 that is completely based on the theory of S-rings over a finite cyclic group (see [5, 6]). In fact, from the results of this theory it follows that the multiplication S-ring corresponding to the cyclotomic scheme $\mathcal{C}$ satisfying the hypothesis of the theorem, is normal. This implies that the group $\mathrm{Aut}(\mathcal{C})$ normalizes the group $\mathrm{AGL}_1(\mathbb{F})$ and consequently the scheme $\mathcal{C}$ is normal.

References

[1] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance-regular graphs*, Springer, Berlin, 1989.

[2] R. W. Goldbach, H. L. Claasen, *Cyclotomic schemes over finite rings*, Indag. Math. (N.S.), **3** (1992), 301–312.

[3] R. McConnel, *Pseudo-ordered polynomials over a finite field*, Acta Arith., **8** (1963), 127–151.

[4] T. Ito, A. Munemasa, M. Yamada, *Amorphous association schemes over the Galois rings of characteristic* 4, European J. Combin., **12** (1991), 513–526.

[5] S. Evdokimov, I. Ponomarenko, *Characterization of cyclotomic schemes and normal Schur rings over a cyclic group*, Algebra and Analysis, **14** (2002), 2, 11–55. (English translation in St. Petersburg Math. J., **14** (2003), no. 2, 189–221.)

[6] K. H. Leung, S. H. Man, *On Schur Rings over Cyclic Groups, II*, J. Algebra, **183** (1996), 273–285.

The q-tetrahedron algebra

Tatsuro Ito
Kanazawa University

Paul Terwilliger
University of Wisconsin

Contents

- The tetrahedron algebra $\boxtimes$
- The q-tetrahedron algebra $\boxtimes_q$
- An action of $\boxtimes_q$ on certain distance-regular graphs

Warmup: The Lie algebra $\mathfrak{sl}_2$

Throughout, $\mathbb{K}$ will denote an algebraically closed field with characteristic 0.

Recall that $\mathfrak{sl}_2$ is the Lie algebra over $\mathbb{K}$ with a basis e, f, h and Lie bracket

$$[h,e] = 2e, \qquad [h,f] = -2f,$$
$$[e,f] = h.$$

The equitable basis for $\mathfrak{sl}_2$

Define

$$x = h, \qquad y = 2e - h, \qquad z = -2f - h.$$

Then x, y, z is a basis for $\mathfrak{sl}_2$ and

$$[x,y] \;=\; 2x + 2y,$$

$$\begin{aligned} [y,z] &= 2y+2z, \\ [z,x] &= 2z+2x. \end{aligned}$$

We call x, y, z the **equitable basis** for $\mathfrak{sl}_2$.

Warmup: The $\mathfrak{sl}_2$ loop algebra

Definition Let $L(\mathfrak{sl}_2)$ denote the Lie algebra over $\mathbb{K}$ consisting of the $\mathbb{K}$-vector space $\mathfrak{sl}_2 \otimes \mathbb{K}[T, T^{-1}]$ with T indetermate, and Lie bracket

$$[u \otimes a, v \otimes b] = [u, v] \otimes ab$$

for $u, v \in \mathfrak{sl}_2$ and $a, b \in \mathbb{K}[T, T^{-1}]$.

We call $L(\mathfrak{sl}_2)$ the $\mathfrak{sl}_2$ **loop algebra**.

The $\mathfrak{sl}_2$ loop algebra

The $\mathfrak{sl}_2$ loop algebra is related to the Kac-Moody algebra associated with the Cartan matrix

$$A := \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}.$$

This is explained in the next lemma.

The $\mathfrak{sl}_2$ loop algebra

Lemma The algebra $L(\mathfrak{sl}_2)$ is isomorphic to the Lie algebra over $\mathbb{K}$ that has generators e_i, f_i, h_i, $i = 0, 1$ and the following relations:

$$\begin{aligned} h_0 + h_1 &= 0, \\ [h_i, e_j] &= A_{ij} e_j, \\ [h_i, f_j] &= -A_{ij} f_j, \\ [e_i, f_j] &= \delta_{ij} h_i, \\ [e_i, [e_i, [e_i, e_j]]] &= 0, \qquad i \neq j, \\ [f_i, [f_i, [f_i, f_j]]] &= 0, \qquad i \neq j. \end{aligned}$$

An isomorphism is given by

$$\begin{aligned} e_0 &\to f \otimes T, & e_1 &\to e \otimes 1, \\ f_0 &\to e \otimes T^{-1}, & f_1 &\to f \otimes 1, \\ h_0 &\to -h \otimes 1, & h_1 &\to h \otimes 1. \end{aligned}$$

The equitable presentation for

the $\mathfrak{sl}_2$ loop algebra

The following presentation of $L(\mathfrak{sl}_2)$ will be useful.

Lemma [Hartwig+T] $L(\mathfrak{sl}_2)$ is isomorphic to the Lie algebra over $\mathbb{K}$ that has generators x_i, y_i, z_i, $i = 0, 1$ and the following relations:

$$\begin{aligned}
x_0 + x_1 &= 0, \\
[x_i, y_i] &= 2x_i + 2y_i, \\
[y_i, z_i] &= 2y_i + 2z_i, \\
[z_i, x_i] &= 2z_i + 2x_i, \\
[z_i, y_j] &= 2z_i + 2y_j, && i \neq j, \\
[y_i, [y_i, [y_i, y_j]]] &= 4[y_i, y_j], && i \neq j, \\
[z_i, [z_i, [z_i, z_j]]] &= 4[z_i, z_j], && i \neq j.
\end{aligned}$$

The tetrahedron algebra

Definition [Hartwig+T] The tetrahedron algebra $\boxtimes$ is the Lie algebra over $\mathbb{K}$ that has generators

$$\{x_{ij} \mid i, j \in \mathbb{I}, i \neq j\} \qquad \mathbb{I} = \{0, 1, 2, 3\}$$

and the following relations:

(i) For distinct $i, j \in \mathbb{I}$,

$$x_{ij} + x_{ji} = 0.$$

(ii) For mutually distinct $h, i, j \in \mathbb{I}$,

$$[x_{hi}, x_{ij}] = 2x_{hi} + 2x_{ij}.$$

(iii) For mutually distinct $h, i, j, k \in \mathbb{I}$,

$$[x_{hi}, [x_{hi}, [x_{hi}, x_{jk}]]] = 4[x_{hi}, x_{jk}].$$

The algebra $\boxtimes$

Comments on $\boxtimes$

The algebra $\boxtimes$ has essentially six generators, and it is natural to identify these with the six edges of a tetrahedron.

For each face of the tetrahedron the three surrounding edges form a basis for a subalgebra of $\boxtimes$ that is isomorphic to $\mathfrak{sl}_2$.

Any five of the six edges of the tetrahedron generate a subalgebra of $\boxtimes$ that is isomorphic to the $\mathfrak{sl}_2$ loop algebra.

It turns out that each pair of opposite edges generate a subalgebra of $\boxtimes$ that is isomorphic to the Onsager algebra (See physics literature)

View of $\boxtimes$, cont.

Let us call these Onsager subalgebras. Then $\boxtimes$ is the direct sum of its three Onsager subalgebras.

$\boxtimes$ itself is isomorphic to the **three-point loop algebra**

$$\mathfrak{sl}_2 \otimes \mathbb{K}[T, T^{-1}, (T-1)^{-1}].$$

The $\boxtimes$-modules

For his Ph.D. thesis, recently Hartwig classified the finite dimensional irreducible $\boxtimes$-modules.

It turns out that these modules are in bijection with a linear algebraic object called a **tridiagonal pair of Krawtchouk type**.

We now review this bijection.

Tridiagonal pairs

In what follows V will denote a vector space over $\mathbb{K}$ with finite positive dimension.

We consider a pair of linear transformations $A : V \to V$ and $A^* : V \to V$.

Definition of a Tridiagonal pair

We say the pair A, A^* is a **Tridiagonal pair** on V whenever (1)–(4) hold below.

1. Each of A, A^* is diagonalizable on V.
2. There exists an ordering $V_0, V_1, \ldots, V_d$ of the eigenspaces of A such that

$$A^* V_i \subseteq V_{i-1} + V_i + V_{i+1} \qquad (0 \leq i \leq d),$$

where $V_{-1} = 0$, $V_{d+1} = 0$.

3. There exists an ordering $V_0^*, V_1^*, \ldots, V_\delta^*$ of the eigenspaces of A^* such that

$$AV_i^* \subseteq V_{i-1}^* + V_i^* + V_{i+1}^* \qquad (0 \leq i \leq \delta),$$

where $V_{-1}^* = 0$, $V_{\delta+1}^* = 0$.

4. There is no subspace $W \subseteq V$ such that $AW \subseteq W$ and $A^*W \subseteq W$, other than $W = 0$ and $W = V$.

Tridiagonal pairs of Krawtchouk type

Referring to our definition of a tridiagonal pair,
it turns out $d = \delta$; we call this common value the **diameter** of the pair.
The pair has **Krawtchouk type** whenever

- The eigenvalue of A for the eigenspace V_i is $d - 2i$ $(0 \leq i \leq d)$;
- The eigenvalue of A^* for the eigenspace V_i^* is $d - 2i$ $(0 \leq i \leq d)$.

The f.d. irreducible $\boxtimes$-modules

Hartwig's results concerning tridiagonal pairs and $\boxtimes$-modules are contained in the following two theorems and subsequent remark.

Theorem [Hartwig] Let V denote a finite dimensional irreducible $\boxtimes$-module. Then the generators x_{01}, x_{23} act on V as a tridiagonal pair of Krawtchouk type.

Theorem [Hartwig] Let V denote a vector space over $\mathbb{K}$ with finite positive dimension and let A, A^* denote a tridiagonal pair on V of Krawtchouk type. Then there exists a unique $\boxtimes$-module structure on V such that the generators x_{01}, x_{23} act as A, A^* respectively. This $\boxtimes$-module structure is irreducible.

The f.d. irreducible $\boxtimes$-modules

Remark [Hartwig] Combining the above two theorems we obtain a bijection between the following two sets:

(i) the isomorphism classes of finite dimensional irreducible $\boxtimes$-modules.

(ii) the isomorphism classes of tridiagonal pairs of Krawtchouk type.

The algebra $\boxtimes_q$

We are now ready to define the q-tetrahedron algebra $\boxtimes_q$. As we will see,

- $\boxtimes_q$ is related to the quantum group $U_q(\mathfrak{sl}_2)$ in roughly the same way that $\boxtimes$ is related to $\mathfrak{sl}_2$.
- $\boxtimes_q$ is related to the $U_q(\mathfrak{sl}_2)$ loop algebra in roughly the same way that $\boxtimes$ is related to the $\mathfrak{sl}_2$ loop algebra.

• The finite dimensional irreducible $\boxtimes_q$-modules are in bijection with a kind of tridiagonal pair said to have q-Krawtchouk type.

The q-tetrahedron algebra

From now on we fix a nonzero scalar $q \in \mathbb{K}$ that is not a root of 1.
We define

$$[n]_q = \frac{q^n - q^{-n}}{q - q^{-1}} \qquad n = 0, 1, 2, \ldots$$

We let $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$ denote the cyclic group of order 4.

The q-tetrahedron algebra

Definition Let $\boxtimes_q$ denote the unital associative $\mathbb{K}$-algebra that has generators

$$\{x_{ij} \mid i, j \in \mathbb{Z}_4,\ j - i = 1 \text{ or } j - i = 2\}$$

and the following relations:

(i) For $i, j \in \mathbb{Z}_4$ such that $j - i = 2$,

$$x_{ij}x_{ji} = 1.$$

(ii) For $h, i, j \in \mathbb{Z}_4$ such that the pair $(i - h, j - i)$ is one of $(1,1), (1,2), (2,1)$,

$$\frac{qx_{hi}x_{ij} - q^{-1}x_{ij}x_{hi}}{q - q^{-1}} = 1.$$

(iii) For $h, i, j, k \in \mathbb{Z}_4$ such that $i - h = j - i = k - j = 1$,

$$x_{hi}^3 x_{jk} - [3]_q x_{hi}^2 x_{jk} x_{hi} + [3]_q x_{hi} x_{jk} x_{hi}^2 - x_{jk} x_{hi}^3 = 0.$$

The algebra $U_q(\mathfrak{sl}_2)$

We now discuss how $\boxtimes_q$ is related to the quantum algebra $U_q(\mathfrak{sl}_2)$.

Definition Let $U_q(\mathfrak{sl}_2)$ denote the unital associative $\mathbb{K}$-algebra with generators $K^{\pm 1}$, $e^{\pm}$ and the following relations:

$$\begin{aligned} KK^{-1} &= K^{-1}K = 1, \\ Ke^{\pm}K^{-1} &= q^{\pm 2}e^{\pm}, \\ [e^+, e^-] &= \frac{K - K^{-1}}{q - q^{-1}}. \end{aligned}$$

The equitable presentation of $U_q(\mathfrak{sl}_2)$

The following presentation of $U_q(\mathfrak{sl}_2)$ will be useful.

Lemma [Ito-T-Weng] The algebra $U_q(\mathfrak{sl}_2)$ is isomorphic to the unital associative $\mathbb{K}$-algebra with generators $x^{\pm 1}$, y, z and the following relations:

$$\begin{aligned} xx^{-1} = x^{-1}x &= 1, \\ \frac{qxy - q^{-1}yx}{q - q^{-1}} &= 1, \\ \frac{qyz - q^{-1}zy}{q - q^{-1}} &= 1, \\ \frac{qzx - q^{-1}xz}{q - q^{-1}} &= 1. \end{aligned}$$

We call $x^{\pm 1}, y, z$ the **equitable generators** for $U_q(\mathfrak{sl}_2)$.

$\boxtimes_q$ and $U_q(\mathfrak{sl}_2)$

The algebra $\boxtimes_q$ is related to $U_q(\mathfrak{sl}_2)$ as follows.

Proposition [Ito-T] For $i \in \mathbb{Z}_4$ there exists a $\mathbb{K}$-algebra homomorphism from $U_q(\mathfrak{sl}_2)$ to $\boxtimes_q$ that sends

$$\begin{aligned} x &\to x_{i,i+2}, \quad x^{-1} \to x_{i+2,i}, \\ y &\to x_{i+2,i+3}, \quad z \to x_{i+3,i}. \end{aligned}$$

The $U_q(\mathfrak{sl}_2)$ loop algebra

We now consider how $\boxtimes_q$ is related to the $U_q(\mathfrak{sl}_2)$ loop algebra.

Definition Let $U_q(L(\mathfrak{sl}_2))$ denote the unital associative $\mathbb{K}$-algebra with generators K_i, $e_i^{\pm}$, $i = 0, 1$ and the following relations:

$$\begin{aligned} K_0K_1 &= K_1K_0 = 1, \\ K_i e_i^{\pm} K_i^{-1} &= q^{\pm 2} e_i^{\pm}, \\ K_i e_j^{\pm} K_i^{-1} &= q^{\mp 2} e_j^{\pm}, \qquad i \neq j, \\ [e_i^+, e_i^-] &= \frac{K_i - K_i^{-1}}{q - q^{-1}}, \\ [e_0^{\pm}, e_1^{\mp}] &= 0, \end{aligned}$$

$$(e_i^{\pm})^3 e_j^{\pm} - [3]_q (e_i^{\pm})^2 e_j^{\pm} e_i^{\pm} + [3]_q e_i^{\pm} e_j^{\pm} (e_i^{\pm})^2 - e_j^{\pm} (e_i^{\pm})^3 = 0, \qquad i \neq j.$$

We call $U_q(L(\mathfrak{sl}_2))$ the $U_q(\mathfrak{sl}_2)$ **loop algebra**.

The eq. presentation for $U_q(L(\mathfrak{sl}_2))$

The following presentation of $U_q(L(\mathfrak{sl}_2))$ will be useful.

Theorem [Ito-T] The loop algebra $U_q(L(\mathfrak{sl}_2))$ is isomorphic to the unital associative $\mathbb{K}$-algebra with generators x_i, y_i, z_i, $i = 0, 1$ and the following relations:

$$\begin{aligned}
x_0x_1 = x_1x_0 &= 1, \\
\frac{qx_iy_i - q^{-1}y_ix_i}{q - q^{-1}} &= 1, \\
\frac{qy_iz_i - q^{-1}z_iy_i}{q - q^{-1}} &= 1, \\
\frac{qz_ix_i - q^{-1}x_iz_i}{q - q^{-1}} &= 1, \\
\frac{qz_iy_j - q^{-1}y_jz_i}{q - q^{-1}} &= 1, \qquad i \neq j,
\end{aligned}$$

$$\begin{aligned}
y_i^3y_j - [3]_q y_i^2y_jy_i + [3]_q y_iy_jy_i^2 - y_jy_i^3 = 0, \qquad i \neq j, \\
z_i^3z_j - [3]_q z_i^2z_jz_i + [3]_q z_iz_jz_i^2 - z_jz_i^3 = 0, \qquad i \neq j.
\end{aligned}$$

$\boxtimes_q$ and $U_q(L(\mathfrak{sl}_2))$

$\boxtimes_q$ is related to $U_q(L(\mathfrak{sl}_2))$ as follows.

Proposition [Ito-T] For $i \in \mathbb{Z}_4$ there exists a $\mathbb{K}$-algebra homomorphism from $U_q(L(\mathfrak{sl}_2))$ to $\boxtimes_q$ that sends

$$\begin{aligned}
x_0 &\to x_{i+2,i}, \quad x_1 \to x_{i,i+2}, \\
y_0 &\to x_{i,i+1}, \quad y_1 \to x_{i+2,i+3}, \\
z_0 &\to x_{i+1,i+2}, \quad z_1 \to x_{i+3,i}.
\end{aligned}$$

The type of a $\boxtimes_q$-module

We now turn our attention to the finite dimensional irreducible $\boxtimes_q$-modules.

For such a module V there exist an integer $d \geq 0$ and a scalar $\varepsilon \in \{1, -1\}$ such that for each generator x_{ij} the action on V is semisimple with eigenvalues $\{\varepsilon q^{d-2n} \mid 0 \leq n \leq d\}$.

We call ε the **type** of V.

Replacing each generator x_{ij} by εx_{ij} the type becomes 1.

The f.d. irreducible $\boxtimes_q$-modules

We now discuss how the finite dimensional irreducible $\boxtimes_q$-modules are related to tridiagonal pairs.

Definition A tridiagonal pair A, A^* is said to have **q-Krawtchouk type** whenever

- The eigenvalue of A for the eigenspace V_i is q^{d-2i} for $(0 \leq i \leq d)$;
- The eigenvalue of A^* for the eigenspace V_i^* is q^{d-2i} for $(0 \leq i \leq d)$.

The f.d. irreducible $\boxtimes_q$-modules

Our results concerning tridiagonal pairs and $\boxtimes_q$-modules are contained in the following two theorems and subsequent remark.

Theorem [Ito+T] Let V denote a finite dimensional irreducible $\boxtimes_q$-module of type 1. Then the generators x_{01}, x_{23} act on V as a tridiagonal pair of q-Krawtchouk type.

Theorem [Ito+T] Let V denote a vector space over $\mathbb{K}$ with finite positive dimension and let A, A^* denote a t.d. pair on V of q-Krawtchouk type. Then there exists a unique $\boxtimes_q$-module structure on V such that the generators x_{01}, x_{23} act as A, A^* respectively. This $\boxtimes_q$-module structure is irreducible and type 1.

The f.d. irreducible $\boxtimes_q$-modules

Remark [Ito+T] Combining the above two theorems we obtain a bijection between the following two sets:

(i) the isomorphism classes of finite dimensional irreducible $\boxtimes_q$-modules of type 1.

(ii) the isomorphism classes of tridiagonal pairs of q-Krawtchouk type.

$\boxtimes_q$ and distance-regular graphs

Our next goal is to display an action of $\boxtimes_q$ on certain distance-regular graphs.

For the rest of the talk we let $\mathbb{K} = \mathbb{C}$.

We let $\Gamma = (X, R)$ denote a distance-regular graph with vertex set X, edge set R, and diameter $D \geq 3$.

Let $V = \mathbb{C}X$ denote the standard module of Γ.

The Bose-Mesner algebra

Recall the **Bose-Mesner algebra** M of Γ has a basis of **distance-matrices** $A_0, \ldots, A_D$ and a basis of **primitive idempotents** $E_0, \ldots, E_D$.

Recall that V has a decomposition

$$V = \sum_{i=0}^{D} E_i V \qquad \text{(orthog. dir. sum)},$$

where the orthogonality is with respect to the dot product

$$\langle u, v \rangle = u^t \overline{v} \qquad (u, v \in V).$$

For $0 \leq i \leq D$ the space $E_i V$ is a **common eigenspace** for M.
Moreover E_i acts on V as the **projection** onto this eigenspace.

The Dual Bose-Mesner algebra

From now on fix a vertex $x \in X$. Recall the corresponding **dual Bose-Mesner algebra** M^* has a basis of **dual distance-matrices** $A_0^*, \ldots, A_D^*$ and a basis of **dual primitive idempotents** $E_0^*, \ldots, E_D^*$.

Recall that V has a decomposition

$$V = \sum_{i=0}^{D} E_i^* V \qquad \text{(orthog. dir. sum)},$$

and that

$$E_i^* V = \mathrm{Span}\{y \mid y \in X,\ \partial(x, y) = i\}.$$

We call $E_i^* V$ the i**th subconstituent** of Γ with respect to x.
Note that E_i^* acts on V as the projection onto $E_i^* V$.

The subconstituent algebra

We let T denote the subalgebra of $\mathrm{Mat}_X(\mathbb{C})$ generated by the Bose-Mesner algebra M and the dual Bose-Mesner algebra M^*.

We call T the **subconstituent algebra** of Γ with respect to x.

We note that:

- T is noncommutative in general.
- T is semi-simple since it is closed under the conjugate-transpose map.

An assumption

From now on we make an assumption about Γ.

We fix integers q, ε with $q \neq 1$, $q \neq -1$.

We assume the intersection numbers of Γ have the form

$$c_i = q^{2i-2} \frac{q^{2i} - 1}{q^2 - 1},$$

$$b_i = (\varepsilon + 1 - q^{2i}) \frac{q^{2D} - q^{2i}}{q^2 - 1}$$

for $0 \leq i \leq D$.

The significance of the assumption

The above assumption means that

- Γ has classical parameters;
- Γ is formally self dual.

The significance of the assumption

The assumption implies:

The eigenvalue of A_1 (resp. A_1^*) associated with the eigenspace E_iV (resp. E_i^*V) is of the form

$$C_1 + C_2 q^{D-2i}$$

for $0 \leq i \leq D$, for some scalars C_1, C_2.

Remark There are several known infinite families of distance-regular graphs that satisfy the assumption. For instance the "bilinear forms" graphs, the "alternating forms" graphs, the "Hermitean forms"graphs, and the "quadratic forms" graphs.

For their definitions see the book **Distance-regular graphs** by Brouwer, Cohen and Neumaier.

The assumption and $\boxtimes_q$

For Γ satisfying the above assumption we will display an action of $\boxtimes_q$ on the standard module V.

This action will induce a homomorphism from $\boxtimes_q$ onto T.

The $\boxtimes_q$-action on V

We now construct our $\boxtimes_q$-action on V.

To do this, we define some matrices in $\mathrm{Mat}_X(\mathbb{C})$:

$$A, \quad A^*,$$
$$B, \quad B^*,$$
$$K, \quad K^*,$$
$$\Phi, \quad \Psi.$$

The matrix A

Recall that for $0 \leq i \leq D$ the eigenvalue of the matrix A_1 associated with E_iV is

$$C_1 + C_2 q^{D-2i}.$$

We define $A \in \mathrm{Mat}_X(\mathbb{C})$ so that

$$A_1 = C_1 I + C_2 A.$$

Thus for $0 \leq i \leq D$ the eigenvalue of A associated with the eigenspace $E_i V$ is

$$q^{D-2i}.$$

The matrix A^*

Recall that for $0 \leq i \leq D$ the eigenvalue of the matrix A_1^* associated with $E_i^* V$ is

$$C_1 + C_2 q^{D-2i}.$$

We define $A^* \in \mathrm{Mat}_X(\mathbb{C})$ so that

$$A_1^* = C_1 I + C_2 A^*.$$

Thus for $0 \leq i \leq D$ the eigenvalue of A^* associated with the eigenspace $E_i^* V$ is

$$q^{D-2i}.$$

The matrices K, Φ

For $-1 \leq i, j \leq D$ we define

$$V_{ij} = (E_0^* V + \cdots + E_i^* V) \cap (E_0 V + \cdots + E_j V).$$

For $0 \leq i, j \leq D$ we have

$$\begin{aligned} V_{i,j-1} &\subseteq V_{ij}, \\ V_{i-1,j} &\subseteq V_{ij}, \end{aligned}$$

so that

$$V_{i,j-1} + V_{i-1,j} \subseteq V_{ij}.$$

The matrices K, Φ, cont.

For $0 \leq i, j \leq D$ we define

$$\tilde{V}_{ij} = V_{ij} \cap (V_{i,j-1} + V_{i-1,j})^{\perp}.$$

It turns out that

$$V = \sum_{i=0}^{D} \sum_{j=0}^{D} \tilde{V}_{ij} \qquad \text{(direct sum)}.$$

The matrices K, Φ, cont.

We define $K \in \mathrm{Mat}_X(\mathbb{C})$ so that

$$K - q^{i-j} I \quad \text{vanishes on} \quad \tilde{V}_{ij}$$

for $0 \leq i, j \leq D$.

We define $\Phi \in \mathrm{Mat}_X(\mathbb{C})$ so that

$$\Phi - q^{i+j-D} I \quad \text{vanishes on} \quad \tilde{V}_{ij}$$

for $0 \leq i, j \leq D$.

The matrices B, B^*, K^*, Ψ

We just defined the matrices K, Φ.

Using the same procedure with the sequence $E_0, \ldots, E_D$ replaced by $E_D, \ldots, E_0$ we get B, Ψ.

Using the original procedure with $E_0^*, \ldots, E_D^*$ replaced by $E_D^*, \ldots, E_0^*$ we get B^*, Ψ^{-1}.

Using the original procedure with $E_0, \ldots, E_D$ replaced by $E_D, \ldots, E_0$ and $E_0^*, \ldots, E_D^*$ replaced by $E_D^*, \ldots, E_0^*$ we get K^*, Φ^{-1}.

A comment

It turns out that each of

$$A, \quad A^*,$$
$$B, \quad B^*,$$
$$K, \quad K^*,$$
$$\Phi, \quad \Psi$$

is contained in T. Moreover Φ, Ψ are central in T.

In addition...

Some relations

We have

$$\begin{aligned}
\frac{qAB - q^{-1}BA}{q - q^{-1}} &= \Psi, \\
\frac{qBA^* - q^{-1}A^*B}{q - q^{-1}} &= \Psi^{-1}, \\
\frac{qA^*B^* - q^{-1}B^*A^*}{q - q^{-1}} &= \Psi^{-1}, \\
\frac{qB^*A - q^{-1}AB^*}{q - q^{-1}} &= \Psi.
\end{aligned}$$

More relations

We have

$$\begin{aligned}
\frac{qK^{-1}A - q^{-1}AK^{-1}}{q - q^{-1}} &= \Phi^{-1}, \\
\frac{qBK^{-1} - q^{-1}K^{-1}B}{q - q^{-1}} &= \Phi\Psi^{-1}, \\
\frac{qKA^* - q^{-1}A^*K}{q - q^{-1}} &= \Phi^{-1}, \\
\frac{qB^*K - q^{-1}KB^*}{q - q^{-1}} &= \Phi\Psi.
\end{aligned}$$

Yet more relations

We have

$$\begin{aligned}
\frac{qA^*K^{*-1} - q^{-1}K^{*-1}A^*}{q - q^{-1}} &= \Phi^{-1}, \\
\frac{qK^*B^* - q^{-1}B^*K^*}{q - q^{-1}} &= \Psi^{-1}\Phi, \\
\frac{qAK^* - q^{-1}K^*A}{q - q^{-1}} &= \Phi^{-1},
\end{aligned}$$

$$\frac{qK^{*-1}B - q^{-1}BK^{*-1}}{q - q^{-1}} = \Psi\Phi.$$

The q-Serre relations

We have

$$A^3A^* - [3]_qA^2A^*A + [3]_qAA^*A^2 - A^*A^3 = 0,$$

$$A^{*3}A - [3]_qA^{*2}AA^* + [3]_qA^*AA^{*2} - AA^{*3} = 0,$$

$$B^3B^* - [3]_qB^2B^*B + [3]_qBB^*B^2 - B^*B^3 = 0,$$

$$B^{*3}B - [3]_qB^{*2}BB^* + [3]_qB^*BB^{*2} - BB^{*3} = 0.$$

The $\boxtimes_q$-action on V

Comparing the above relations with the defining relations for $\boxtimes_q$ we routinely obtain the following

Theorem There exists a $\boxtimes_q$-module structure on V such that the generators x_{ij} act as follows:

generator	action on V
x_{01}	$A\Phi\Psi^{-1}$
x_{12}	$B\Phi^{-1}$
x_{23}	$A^*\Phi\Psi$
x_{30}	$B^*\Phi^{-1}$
x_{02}	$K\Psi^{-1}$
x_{13}	$K^*\Psi$

In conclusion

We first recalled the tetrahedron algebra $\boxtimes$ and showed that its finite dimensional irreducible modules are in bijection with the tridiagonal pairs of Krawtchouk type.

We then defined the q-tetrahedron algebra $\boxtimes_q$ and showed that its finite

dimensional irreducible modules are in bijection with the tridiagonal pairs of q-Krawtchouk type.

Finally we displayed an action of $\boxtimes_q$ on the standard module of a distance-regular graph that is formally self-dual with classical parameters.

Thank you for your attention!

THE END

Polyhedral Realization of Crystal Bases for Quantum Algebras

Ayumu HOSHINO, Sophia University

e-mail: ayumu-h@mm.sophia.ac.jp

Algebraic Combinatorics:
An International Conference in Honor of
Eiichi Bannai's 60th birthday
(Sendai International center, June.27.2006)

The author is supported by Grant-in-Aid for JSPS Fellows.

0. Introduction

- $c_{\lambda\nu}^{\mu}$ (L-R number): multiplicity of $V(\lambda) \otimes V(\nu)$
  (*i.e.* $V(\lambda) \otimes V(\nu) \cong \bigoplus_{\mu} V(\mu)^{\oplus c_{\lambda\nu}^{\mu}}$).

Describe the $c_{\lambda\nu}^{\mu}$ using the "crystal base" theory.

- "Crystal base" is a basis at "$q \to 0$" of the quantum algebra, which is a q-analogue of (Kac-Moody) Lie algebra.
- Polyhedral realization of crystal base is one method for explicitly describing the crystal base, which is introduced by Nakashima and Zelevinsky [NZ]. We can describe a vector of crystal bases as a lattice point of certain convex polyhedron in an $\mathbb{Z}$-lattice.
- L-R number $c_{\lambda\nu}^{\mu}$ is expressed by the number of points satisfying some conditions in some polyhedron.

1. Definition of the quantum algebra $U_q(\mathfrak{g})$

Notations:

- $\mathfrak{g}$: (symmetrizable Kac-Moody) Lie algebra
  (I : finite index set, P : weight lattice),
- $A = (a_{ij})_{i,j \in I}$: (generalized) Cartan matrix,
- $(\mathfrak{t}, \{\alpha_i\}_{i \in I}, \{h_i\}_{i \in I})$: Cartan data,
- $P^* \ni \{h_i\}_{i \in I}$: dual lattice,
- P_+ : set of dominant integral weights.

Definition 1. *The quantum algebra $U_q(\mathfrak{g}) := \langle e_i, f_i, q^h \rangle_{i \in I, h \in P^*}$ is an associative algebra with 1 over $\mathbb{Q}(q)$ defined by following relations:*

$$
\begin{aligned}
& q^0 = 1, \ q^h q^{h'} = q^{h+h'} && (h, h' \in P^*), \\
& q^h e_i q^{-h} = q^{\langle h, \alpha_i \rangle} e_i && (i \in I, h \in P^*), \\
& q^h f_i q^{-h} = q^{-\langle h, \alpha_i \rangle} f_i && (i \in I, h \in P^*), \\
& [e_i, f_j] = \delta_{i,j} \frac{t_i - t_i^{-1}}{q_i - q_i^{-1}} && (i, j \in I),
\end{aligned}
$$

where $q_i = q^{(\alpha_i, \alpha_i)/2}$, $t_i = q^{(\alpha_i, \alpha_i) h_i / 2}$. And

$$
\sum_{k=0}^{1-a_{ij}} (-1)^k e_i^{(k)} e_j e_i^{(1-a_{ij}-k)} = \sum_{k=0}^{1-a_{ij}} (-1)^k f_i^{(k)} f_j f_i^{(1-a_{ij}-k)} = 0 \quad (i, j \in I, i \neq j),
$$

where $e_i^{(n)} = e_i^n / [n]_i!$, $f_i^{(n)} = f_i^n / [n]_i!$ ($[n]_i = \frac{q_i^n - q_i^{-n}}{q_i - q_i^{-1}}$, $[n]_i! = \prod_{k=1}^{n} [k]_i$ $(n \in \mathbb{Z}_{\geq 0})$).

Remark 2. *$U_q(\mathfrak{g})$ is a q-analogue of the universal enveloping algebra $U(\mathfrak{g})$ of (Kac-Moody) Lie algebra $\mathfrak{g}$ ($\mathfrak{g} \hookrightarrow U(\mathfrak{g}) \rightsquigarrow U_q(\mathfrak{g})$).*

$$
q \to 1 \implies U_q(\mathfrak{g}) \to U(\mathfrak{g}).
$$

Remark 3. *The integrable highest weight representations of $U_q(\mathfrak{g})$ is the same as the ones of (Kac-Moody) Lie algebras in the case of q: generic.*

Remark 4. *When $q \to 0$, subalgebra $U_q^-(\mathfrak{g}) := \langle f_i \rangle_{i \in I}$ and integrable highest weight module $V(\lambda)$ have spacial bases called crystal base, which is constructed by Kashiwara [K1]. We can construct the bases of $V(\lambda)$ by the crystal bases, which is called "global bases"[K2].*

2. Definition of the crystal base

Let M be an integrable highest weight module of $U_q(\mathfrak{g})$. Any $u \in M_\lambda$ ($\lambda \in P$) are expressed by

$$u = \sum_{n \geq 0} f_i^{(n)} u_n$$

$$\left(f_i^{(n)} := \frac{f_i^n}{[n]_i!}, \quad [n]_i := \frac{q_i^n - q_i^{-n}}{q_i - q_i^{-1}}, \quad q_i := q^{(\alpha_i, \alpha_i)/2} \right)$$

for $u_n \in \ker e_i \cap M_{\lambda + n\alpha_i}$. Here we define the "Kashiwara operator" $\tilde{e}_i, \tilde{f}_i \in \mathrm{End}(M)$ ($i \in I$) as follows:

$$\tilde{e}_i u := \sum_{n \geq 1} f_i^{(n-1)} u_n, \quad \tilde{f}_i u := \sum_{n \geq 0} f_i^{(n+1)} u_n.$$

We define

$$A := \{ f(q) \in \mathbb{Q}(q) : f(q) \text{ is regular at } q = 0 \}.$$

Definition 5 (Crystal base).
A pair (L, B) is the crystal base of M if:
(i) L is free sub-A-module of M such that $M \cong \mathbb{Q}(q) \otimes_A L$.
(ii) B is a base of the $\mathbb{Q}$-vector space L/qL.
(iii) $L = \oplus_{\lambda \in P} L_\lambda$, $B = \sqcup_{\lambda \in P} B_\lambda$, where $L_\lambda := L \cap M_\lambda$, $B_\lambda := B \cap L_\lambda / qL$.
(iv) $\tilde{e}_i L \subset L$ and $\tilde{f}_i L \subset L$.
(v) $\tilde{e}_i B \subset B \sqcup \{0\}$ and $\tilde{f}_i B \subset B \sqcup \{0\}$.
(vi) For $u, v \in B$, $\tilde{f}_i u = v \iff \tilde{e}_i v = u$.

Now, let u_λ be the highest weight vector of $V(\lambda)$. We set

$$\begin{aligned} L(\lambda) &:= \sum_{i_j \in I, l \geq 0} A \tilde{f}_{i_l} \cdots \tilde{f}_{i_1} u_\lambda, \\ B(\lambda) &:= \{ \tilde{f}_{i_l} \cdots \tilde{f}_{i_1} u_\lambda \bmod qL(\lambda) : i_j \in I, l \geq 0 \}. \end{aligned}$$

Theorem 6 (Kashiwara [K1]).
A pair $(L(\lambda), B(\lambda))$ is the crystal base of $V(\lambda)$.

Similarly, we can define $\tilde{e}_i$, $\tilde{f}_i \in \mathrm{End}(U_q^-(\mathfrak{g}))$. We set

$$\begin{aligned} L(\infty) &:= \sum_{i_j \in I, l \geq 0} A \tilde{f}_{i_l} \cdots \tilde{f}_{i_1} u_\infty \quad (u_\infty : \text{unit}), \\ B(\infty) &:= \{ \tilde{f}_{i_l} \cdots \tilde{f}_{i_1} u_\infty \bmod qL(\infty) : i_j \in I, l \geq 0 \}. \end{aligned}$$

Then a pair $(L(\infty), B(\infty))$ is the crystal base of $U_q^-(\mathfrak{g})$ ([K1]).

Theorem 7 (Kashiwara [K2]). *For an integrable highest weight module $V(\lambda)$ there is a isomorphism G such that*

$$\{G(b) : b \in B(\lambda)\}$$

is a base of $V(\lambda)$. We call $G(b)$ the "global base".

Theorem 8 (tensor pruduct).
For $U_q(\mathfrak{g})$-modules V_1 and V_2 we set (L_1, B_1), (L_2, B_2) are their crystal bases respectively. And we set

$$\begin{aligned} L &:= L_1 \otimes_A L_2, \\ B &:= B_1 \otimes B_2 := \{b_1 \otimes b_2 : b_i \in B_i\}. \end{aligned}$$

(i) (L, B) is the crystal base of $V_1 \otimes_{\mathbb{Q}(q)} V_2$.
(ii) For $u \in B_1, v \in B_2$, we define

$$\begin{aligned} \varepsilon_i(v) &:= max \{n \geq 0 : \tilde{e}_i^n v \neq 0\}, \\ \varphi_i(u) &:= max \{n \geq 0 : \tilde{f}_i^n u \neq 0\}. \end{aligned}$$

Then

$$\tilde{e}_i(u \otimes v) = \begin{cases} \tilde{e}_i u \otimes v & \text{if } \varphi_i(u) \geq \varepsilon_i(v), \\ u \otimes \tilde{e}_i v & \text{if } \varphi_i(u) < \varepsilon_i(v), \end{cases}$$

$$\tilde{f}_i(u \otimes v) = \begin{cases} \tilde{f}_i u \otimes v & \text{if } \varphi_i(u) > \varepsilon_i(v), \\ u \otimes \tilde{f}_i v & \text{if } \varphi_i(u) \leq \varepsilon_i(v). \end{cases}$$

3. Polyhedral realization of $B(\infty)$ and $B(\lambda)$

Kashiwara embedding

For a crystal $B_i := \{ (x)_i \mid x \in \mathbb{Z} \} \cong \mathbb{Z}$ $(i \in I)$ we obtain the following embedding ([K3]):

$$\begin{aligned} \Psi_i : B(\infty) &\hookrightarrow B(\infty) \otimes B_i \\ u_\infty &\mapsto u_\infty \otimes (0)_i . \end{aligned}$$

Here, we fix an infinite sequence of indices $\iota = (\cdots, i_2, i_1)$ $(i_k \in I)$ satisfying certain conditions. We can get the following embedding associated with ι (Kashiwara embedding ([K3])):

$$\begin{aligned} \Psi_\iota : B(\infty) &\hookrightarrow B(\infty) \otimes B_{i_1} \\ &\hookrightarrow B(\infty) \otimes B_{i_2} \otimes B_{i_1} \\ &\cdots \\ &\hookrightarrow B(\infty) \otimes B_{i_l} \otimes \cdots \otimes B_{i_2} \otimes B_{i_1} \\ &\cong \mathbb{Z}^\infty \\ &\quad (u_\infty \mapsto u_\infty \otimes (\cdots, 0, 0)) \end{aligned}$$

$$(\mathbb{Z}^\infty = \{ (\cdots, x_2, x_1) \mid x_j \in \mathbb{Z},\ x_k = 0 \ (k \gg 0) \}).$$

- Polyhedral realization of $B(\infty)$ is one method of explicitly describing the Im Ψ_ι.
- We can also construct the polyhedral realization of $B(\lambda)$.

Known results

- $B(\infty)$: A_n, $A^{(1)}_{n-1}$, arbitrary rank 2 ([NZ] 1997)
- $B(\lambda)$: A_n, $A^{(1)}_{n-1}$, arbitrary rank 2 ([N1] 1999)
- $B(\infty)$, $B(\lambda)$: B_n, C_n, D_n, E_6, E_7, E_8, F_4 ([H1] 2005)

New results

- $B(\infty)$: $B^{(1)}_n$, $C^{(1)}_n$, $D^{(1)}_n$, $A^{(2)}_{2n}$, $A^{(2)}_{2n-1}$, $D^{(2)}_{n+1}$ (H. preprint)

Here, we present the polyhedral realizations for B_5 and G_2.

• B_5 case:

We set

$$\iota := (\cdots, 5, \cdots, 2, 1, 5, \cdots, 2, 1). \tag{1}$$

For $\vec{x} := (x_{25}, \cdots, x_2, x_1) \in \mathbb{Z}^{\oplus 25}$, the polyhedral realization of $B(\infty)$ for B_5 is described as following convex cone:

Example 9 ($B(\infty)$ B_5**-case).**

$$x_1 \geq 0$$

$$x_2 \geq x_6 \geq 0$$

$$x_3 \geq x_7 \geq x_{11} \geq 0$$

$$x_4 \geq x_8 \geq x_{12} \geq x_{16} \geq 0$$

$$x_5 \geq x_9 \geq x_{13} \geq x_{17} \geq x_{21}$$

$$x_{10} \geq x_{14} \geq x_{18} \geq x_{22}$$

$$x_{15} \geq x_{19} \geq x_{23}$$

$$x_{20} \geq x_{24}$$

$$x_{25} \geq 0$$

(the other $x_j \equiv 0$*).*

Let λ be $\lambda = \sum_{i=1}^{5} \lambda_i \Lambda_i$ (Λ_i : fundamental weight). We fix ι as (1).

Example 10 ($B(\lambda)$ B_5**-case).** *The polyhedral realization of* $B(\lambda)$ *for* B_5 *is described by adding the following inequalities to the one of* $B(\infty)$*:*

$$\begin{aligned}
\lambda_1 &\geq x_1, \\
\lambda_2 &\geq x_2 - x_1,\ x_6, \\
\lambda_3 &\geq x_3 - x_2,\ x_7 - x_6,\ x_{11}, \\
\lambda_4 &\geq x_4 - x_3, \cdots, \\
\lambda_5 &\geq x_5 - x_4,\ -x_5 - x_8 + x_9, \cdots .
\end{aligned}$$

• G_2 case.
Let λ be $\lambda = \lambda_1 \Lambda_1 + \lambda_2 \Lambda_2$.

Example 11. *We set* $\iota := (\cdots, 2, 1, 2, 1)$. *The polyhedral realization of* $B(\lambda)$ *for* G_2 *is described by* Σ *as below:*

$$\Sigma \ := \ \{\vec{x} = (x_6, \cdots, x_2, x_1) \in \mathbb{Z}^{\oplus 6} : \varphi(\vec{x}) \geq 0\},$$

where φ *is an element of*

$$\left\{ \begin{array}{llll} x_1, & x_2 - x_3, & 2x_3 - x_4, & x_4 - 2x_5, \\ & x_5 - x_6, & & \\ \lambda_1 - x_1, & \lambda_2 + x_1 - x_2, & \lambda_2 + 2x_4 - 3x_3, & \\ \lambda_2 + 3x_3 - 2x_4, & \lambda_2 + x_4 - 3x_5, & \lambda_2 - x_6 & \end{array} \right\}.$$

5. Description of the $c_{\lambda\nu}^{\mu}$
We set

$$\lambda := \sum_{i=1}^{k} l_i \Lambda_i, \quad \mu := \sum_{i=1}^{k} m_i \Lambda_i, \quad \nu := \sum_{i=1}^{k} n_i \Lambda_i,$$

where Λ_i : fundamental weight, $i \in I$, $l_i, m_i, n_i \in \mathbb{Z}_{\geq 0}$ and k: rank of $U_q(\mathfrak{g})$. We define
- $V(\lambda)_\beta$: weight space of $V(\lambda)$ with the weight β,
- $V(\lambda)_{\beta,\nu} := \{v \in V(\lambda)_\beta : e_i^{n_i+1} v = 0$ for any $i \in I\}$.

Fact 12. $c_{\lambda\,\nu}^{\mu} = \dim V(\lambda)_{\mu-\nu,\nu}$.

Proposition 13 (Kashiwara [K2]). *For any $i \in I$ and $n \in \mathbb{Z}_{\geq 0}$,*

$$\{v \in V(\lambda) : e_i^{n+1} v = 0\} = \mathbb{Q}(q) \otimes G(\{b \in B(\lambda) : \tilde{e}_i^{n+1} b = 0\}).$$

Combining these facts, we can describe $c_{\lambda\,\nu}^{\mu}$ as the number of $b \in B(\lambda)$ satisfying the following conditions:

(C1). weight of b is $\mu - \nu$,

(C2). $\varepsilon_i(b) \leq n_i$ for any $i \in I$.

• Description of the $c_{\lambda\,\nu}^{\mu}$ for G_2

We set $\lambda := l_1\Lambda_1 + l_2\Lambda_2$, $\mu := m_1\Lambda_1 + m_2\Lambda_2$, $\nu := n_1\Lambda_1 + n_2\Lambda_2$ $(l_i, m_i, n_i \in \mathbb{Z}_{\geq 0},\ i = 1, 2)$.
For $\vec{x} \in \Sigma$, we can describe the conditions (C1) and (C2) as follows:

(C1) $wt(\vec{x}) = \mu - \nu \Longleftrightarrow$

$$l_1 + n_1 - m_1 = x_1 - x_2 + x_3 - x_4 + x_5 - x_6,$$
$$l_2 + n_2 - m_2 = -3x_1 + 2x_2 - 3x_3 + 2x_4 - 3x_5 + 2x_6.$$

(C2) $\varepsilon_i(\vec{x}) \leq n_i \Longleftrightarrow$

$$n_i \geq \max(X_{1;i}, X_{2;i}, X_{3;i}, X_i) \quad \text{for } i = 1, 2,$$

where $X_{j;i}$ and X_i are defined by :

$$X_{1;1} := x_1 - x_2 + 2x_3 - x_4 + 2x_5 - x_6,$$
$$X_{2;1} := x_3 - x_4 + 2x_5 - x_6,$$
$$X_{3;1} := x_5 - x_6,$$
$$X_1 := -l_1 + 2x_1 - x_2 + 2x_3 - x_4 + 2x_5 - x_6,$$
$$X_{1;2} := x_2 - 3x_3 + 2x_4 - 3x_5 + 2x_6,$$
$$X_{2;2} := x_4 - 3x_5 + 2x_6,$$
$$X_{3;2} := x_6,$$
$$X_2 := -l_2 - 3x_1 - 2x_2 - 3x_3 - 2x_4 - 3x_5 - 2x_6.$$

Then we have

Theorem 14 (G_2 case).

$$c_{\lambda,\nu}^{\mu} = \sharp\{\vec{x} \in \Sigma : \vec{x} \textit{ satisfies } \textbf{(C1)} \textit{ and } \textbf{(C2)}\}.$$

Reference

[BZ] A. Berenstein, A. Zelevinsky, Tensor product multiplicities, canonical bases and totally positive varieties, Invent. Math., **143** (2001), 77–128.

[GZ] I. M. Gelfand and A. Zelevinsky, Multiplicities and regular bases for gl_n, Group Theoretical Methods in Physics, vol. II, Science Press, Utrecht, 1986, 147–159.

[H1] A. Hoshino, Polyhedral Realizations of Crystal Bases for Quantum Algebras of Finite Types, J. Math. Phys., **46** (2005), no. 11, 113514, 31 pp.

[H2] A. Hoshino, Affine crystal bases and polyhedral realizations, preprint.

[K1] M. Kashiwara, On crystal bases of the q-analogue of universal enveloping algebras, Duke Math. J.,**63** (1991),465–516.

[K2] M. Kashiwara, Global crystal bases of quantum groups, Duke Math. J., **69** (1993), 455–485.

[K3] M. Kashiwara, Crystal base and Littelmann's refined Demazure character formula, Duke Math. J., **63** (1993), 839–858.

[N1] T. Nakashima, Crystal bases and a generalization of the Littlewood-Richardson rule for the classical Lie algebras, Comm. Math. Phys., **154** (1993), 215–243.

[N2] T. Nakashima, Polyhedral Realizations of Crystal Bases for Integrable Highest Weight Modules, J.Algebra **219**, (1999),571–597.

[NZ] T. Nakashima, A. Zelevinsky, Polyhedral Realizations of Crystal Bases for Quantized Kac-Moody Algebras, Advances in Mathematics **131**, No.1,(1997),253–278.

THE FIXED POINT SUBALGEBRA OF THE VERTEX OPERATOR ALGEBRA ASSOCIATED TO THE LEECH LATTICE BY AN AUTOMORPHISM OF ORDER THREE

KENICHIRO TANABE AND HIROMICHI YAMADA

1. INTRODUCTION

Let V be a vertex operator algebra. For an automorphism g of V of finite order, the space $V^g = \{v \in V \mid gv = v\}$ of fixed points is a subalgebra of V called an orbifold of the vertex operator algebra V. In the case where V is the lattice vertex operator algebra V_L associated to a positive definite even lattice L and the automorphism g is a canonical lift $\hat{\theta}$ of the -1 isometry $\theta : \alpha \mapsto -\alpha$ of the lattice L, the orbifold $V_L^{\hat{\theta}} = V_L^+$ has been studied extensively. In fact, the representation theory of V_L^+, that is, the classification of simple modules and the determination of fusion rules, together with the rationality of V_L^+ are established. However, it is difficult to investigate an orbifold in general, even if the original vertex operator algebra V is well understood.

For a V-module (M, Y_M), one can define a new V-module $(M \circ g, Y_{M \circ g})$ by $M = M \circ g$ as a vector space and $Y_{M \circ g}(v, z) = Y_M(gv, z)$, $v \in V$. Then $M \mapsto M \circ g$ induces a permutation on a complete set $\mathcal{M}$ of representatives of equivalence classes of simple V-modules. If $M \cong M \circ g$, M is said to be g-stable.

Now, assume that g is of prime order and V is rational, C_2-cofinite, and of CFT-type. There are known examples of simple V^g-modules.

(1) If $M \in \mathcal{M}$ is g-stable, then $M(\varepsilon) = \{u \in M \mid gu = \xi^\varepsilon u\}$, $0 \le \varepsilon \le |g| - 1$, are simple V^g-modules, where $\xi = \exp(2\pi\sqrt{-1}/|g|)$.

(2) If $\{M^0, M^1, \ldots, M^{|g|-1}\}$ is a g-orbit in $\mathcal{M}$, then M^i, $0 \le i \le |g| - 1$, are equivalent simple V^g-modules.

(3) If $V^T(g^i)$ is a simple g^i-twisted V-module, then $V^T(g^i)(\varepsilon) = \{u \in V^T(g^i) \mid g^i u = \xi^\varepsilon u\}$, $0 \le \varepsilon \le |g| - 1$, $1 \le i \le |g| - 1$ are simple V^g-modules.

These simple V^g-modules are inequivalent each other (cf. [6, 12]). It is conjectured that any simple V^g-module is one of these simple modules.

In this note we shall study an orbifold of the Leech lattice vertex operator algebra by an automorphism of order 3. Actually, we discuss orbifold of a wider class of lattice vertex operator algebras by an automorphism of order 3. We start with a lattice $L \cong \sqrt{2}$ (A_2-lattice) and an isometry τ of L of order 3. Using a τ-invariant self-orthogonal $\mathbb{Z}_2 \times \mathbb{Z}_2$-code C of length ℓ and a self-orthogonal $\mathbb{Z}_3$-code D of the same length, we build a positive definite even lattice $L_{C \times D}$ of rank 2ℓ. The isometry τ can be extended to a fixed-point-free isometry of $L_{C \times D}$. We want to classify the simple modules for the orbifold $V_{L_{C \times D}}^{\hat{\tau}}$ of the lattice vertex operator algebra $V_{L_{C \times D}}$ by an automorphism $\hat{\tau}$ of order 3 which is a lift of the isometry τ of $L_{C \times D}$.

2000 *Mathematics Subject Classification.* 17B69.

Key words and phrases. vertex operator algebra, orbifold, Leech lattice, Monster simple group.

In our argument we deal with not only simple current extensions but also certain nonsimple current extensions. There is a nice theory for simple current extensions (cf. [16]), whereas nonsimple current extensions are complicated and difficult to study. In order to avoid the difficulty, we only consider the special case where D is a self-dual code and C is a τ-invariant self-dual code with the minimum weight at least 4. In this case the lattice $L_{C\times D}$ is unimodular and there is a unique simple $V_{L_{C\times D}}$-module, namely, $V_{L_{C\times D}}$ itself. Likewise, there is a unique simple $\hat{\tau}^i$-twisted $V_{L_{C\times D}}$-module $V^T_{L_{C\times D}}(\hat{\tau}^i)$, $i = 1, 2$. Under this hypothesis we have the following theorem.

Theorem. Suppose D is a self-dual code and C is a τ-invariant self-dual code with the minimum weight at least 4. Then the vertex operator algebra $V^{\hat{\tau}}_{L_{C\times D}}$ is rational and C_2-cofinite. Moreover, every simple $V^{\hat{\tau}}_{L_{C\times D}}$-module is isomorphic to one of $V_{L_{C\times D}}(\varepsilon)$, $V^T_{L_{C\times D}}(\hat{\tau}^i)(\varepsilon)$, $\varepsilon = 0, 1, 2$, $i = 1, 2$.

We remark that the Leech lattice Λ can be expressed as $L_{C\times D}$ for some C and D which satisfy the hypothesis of the theorem (cf. Example 2.5 below).

The details of this work will appear elsewhere ([15]).

2. Lattice $L_{C\times D}$

Let α_1, α_2 be simple roots of type A_2 and set $\alpha_0 = -\alpha_1 - \alpha_2$. Thus $\langle \alpha_i, \alpha_i\rangle = 2$ and $\langle \alpha_i, \alpha_j\rangle = -1$ for $i \neq j$. Set $\beta_i = \sqrt{2}\alpha_i$, $i = 0, 1, 2$. Let $L = \mathbb{Z}\beta_1 + \mathbb{Z}\beta_2 \cong \sqrt{2}\,(A_2$-lattice). Let τ be the isometry of L induced by the permutation $\alpha_1 \mapsto \alpha_2 \mapsto \alpha_0 \mapsto \alpha_1$. Then τ is fixed-point-three and of order 3.

A $\mathbb{Z}_2 \times \mathbb{Z}_2$-code of length ℓ means an additive subgroup of $\mathcal{K}^\ell$, where $\mathcal{K} = \{0, a, b, c\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ is Klein's four-group. We call it a $\mathcal{K}$-code also. For $x, y \in \mathcal{K}$, define

$$x \circ y = \begin{cases} 1 & \text{if } x = y \neq 0, \\ -\frac{1}{2} & \text{if } x \neq y, x \neq 0, y \neq 0, \\ 0 & \text{if } x = 0 \text{ or } y = 0, \end{cases}$$

$$x \cdot y = \begin{cases} 1 & \text{if } x \neq y, x \neq 0, y \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Note that $2(x \circ y) \equiv x \cdot y \pmod{2\mathbb{Z}}$. For $\lambda = (\lambda_1, \ldots, \lambda_\ell)$, $\mu = (\mu_1, \ldots, \mu_\ell) \in \mathcal{K}^\ell$, let $\lambda \cdot \mu = \sum_{i=1}^{\ell} \lambda_i \cdot \mu_i \in \mathbb{Z}_2$. The orthogonal form $(\lambda, \mu) \mapsto \lambda \cdot \mu$ on $\mathcal{K}^\ell$ was used in [8, 10]. For a $\mathcal{K}$-code C of length ℓ, we define its dual code by

$$C^\perp = \{\lambda \in \mathcal{K}^\ell \mid \lambda \cdot \mu = 0 \text{ for all } \mu \in C\}.$$

A $\mathcal{K}$-code C is said to be self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$. For $\lambda = (\lambda_1, \ldots, \lambda_\ell) \in \mathcal{K}^\ell$, its support is defined to be $\mathrm{supp}(\lambda) = \{i \mid \lambda_i \neq 0\}$. The cardinality of $\mathrm{supp}(\lambda)$ is called the weight of λ. We denote the weight of λ by $\mathrm{wt}(\lambda)$. A $\mathcal{K}$-code C is said to be even if $\mathrm{wt}(\lambda)$ is even for every $\lambda \in C$.

We define an action of τ on $\mathcal{K}$ by $\tau(0) = 0$, $\tau(a) = b$, $\tau(b) = c$, and $\tau(c) = a$. Then τ also acts on $\mathcal{K}^\ell$ by $\tau(\lambda) = (\tau(\lambda_1), \ldots, \tau(\lambda_\ell))$.

Lemma 2.1. ([10, Lemma 2.8]) *Let C be a $\mathcal{K}$-code of length ℓ.*

(1) *If C is even, then C is self-orthogonal.*

(2) *If C is τ-invariant, then C is even if and only if C is self-orthogonal.*

Remark 2.2. *A self-orthogonal $\mathcal{K}$-code is not necessarily even. For instance, the $\mathcal{K}$-code $C = \{(0,0,\dots,0),(a,0,\dots,0)\}$ is self-orthogonal but it is not even.*

A ternary code or a $\mathbb{Z}_3$-code of length ℓ is a subspace of the vector space $\mathbb{Z}_3^\ell$. For $\gamma = (\gamma_1,\dots,\gamma_\ell)$, $\delta = (\delta_1,\dots,\delta_\ell) \in \mathbb{Z}_3^\ell$, we consider the ordinary inner product $\gamma \cdot \delta = \sum_{i=1}^{\ell} \gamma_i\delta_i \in \mathbb{Z}_3$. The dual code $D^\perp$ of a $\mathbb{Z}_3$-code D is defined to be

$$D^\perp = \{\gamma \in \mathbb{Z}_3^\ell \mid \gamma \cdot \delta = 0 \text{ for all } \delta \in D\}.$$

Then D is said to be self-orthogonal if $D \subseteq D^\perp$ and self-dual if $D = D^\perp$. We define the support and the weight of $\gamma = (\gamma_1,\dots,\gamma_\ell) \in \mathbb{Z}_3^\ell$ in the same way as before, that is, $\mathrm{supp}(\gamma) = \{i \mid \gamma_i \neq 0\}$ and $\mathrm{wt}(\gamma)$ is the cardinality of $\mathrm{supp}(\gamma)$.

We use the same notation as in [3, 8, 9, 14] to denote the 12 cosets $L^{(x,i)}$, $x \in \mathcal{K}$, $i \in \mathbb{Z}_3$ of $L \cong \sqrt{2}$ (A_2-lattice) in its dual lattice $L^\perp$. Thus

$$\begin{aligned} L^{(x,i)} &= \beta(x) + i(-\beta_1 + \beta_2)/3 + L \\ &= \{\beta(x) + (-i/3 + m_1)\beta_1 + (i/3 + m_2)\beta_2 \mid m_1, m_2 \in \mathbb{Z}\}. \end{aligned}$$

Here $\beta(x) \in L^\perp$ is defined by $\beta(0) = 0$, $\beta(a) = \beta_2/2$, $\beta(b) = \beta_0/2$, and $\beta(c) = \beta_1/2$. We have $\tau(L^{(x,i)}) = L^{(\tau(x),i)}$.

For $\lambda = (\lambda_1,\dots,\lambda_\ell) \in \mathcal{K}^\ell$ and $\gamma = (\gamma_1,\dots,\gamma_\ell) \in \mathbb{Z}_3^\ell$, let

$$L_{(\lambda,\gamma)} = L^{(\lambda_1,\gamma_1)} \oplus \cdots \oplus L^{(\lambda_\ell,\gamma_\ell)} \subseteq (L^\perp)^{\oplus\ell}, \tag{2.1}$$

where $(L^\perp)^{\oplus\ell}$ is an orthogonal sum of ℓ copies of $L^\perp$. Moreover, for a $\mathcal{K}$-code C of length ℓ and a $\mathbb{Z}_3$-code D of the same length, set

$$L_{C\times D} = \bigcup_{\lambda\in C,\gamma\in D} L_{(\lambda,\gamma)}, \tag{2.2}$$

which is an additive subgroup of $(L^\perp)^{\oplus\ell}$. However, $L_{C\times D}$ is not an integral lattice in general. In the case where $C = \mathcal{K}^\ell$ and $D = \mathbb{Z}_3^\ell$, $L_{C\times D}$ coincides with $(L^\perp)^{\oplus\ell}$. If $C = \{0\}$ and $D = \{0\}$ are the zero code, then $L_{\{0\}\times\{0\}} = L^{\oplus\ell}$. We extend τ to an isometry of $(L^\perp)^{\oplus\ell}$ componentwise.

Denote by $\beta_i^{(s)}$ the element $\beta_i \in L$ in the s-th entry of $(L^\perp)^{\oplus\ell}$. Similarly, we denote $\beta(x) \in L^\perp$ in the s-th entry by $\beta(x)^{(s)}$. Then any element $\alpha \in L_{(\lambda,\gamma)}$ with $\lambda = (\lambda_1,\dots,\lambda_\ell) \in \mathcal{K}^\ell$ and $\gamma = (\gamma_1,\dots,\gamma_\ell) \in \mathbb{Z}_3^\ell$ can be written in the form

$$\alpha = \sum_{s=1}^{\ell} \left(\beta(\lambda_s)^{(s)} + (-\gamma_s/3 + m_1^{(s)})\beta_1^{(s)} + (\gamma_s/3 + m_2^{(s)})\beta_2^{(s)}\right) \tag{2.3}$$

for some $m_1^{(s)}, m_2^{(s)} \in \mathbb{Z}$.

Let $\beta \in L_{(\mu,\delta)}$ with $\mu = (\mu_1,\dots,\mu_\ell) \in \mathcal{K}^\ell$ and $\delta = (\delta_1,\dots,\delta_\ell) \in \mathbb{Z}_3^\ell$ be

$$\beta = \sum_{s=1}^{\ell} \left(\beta(\mu_s)^{(s)} + (-\delta_s/3 + n_1^{(s)})\beta_1^{(s)} + (\delta_s/3 + n_2^{(s)})\beta_2^{(s)}\right) \tag{2.4}$$

for $n_1^{(s)}, n_2^{(s)} \in \mathbb{Z}$. In order to describe the inner product $\langle\alpha,\beta\rangle$ modulo $2\mathbb{Z}$ in $(L^\perp)^{\oplus\ell}$, we denote the elements of $\mathcal{K} = \{0,a,b,c\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$0 \leftrightarrow (0,0), \quad a \leftrightarrow (0,1), \quad b \leftrightarrow (1,1), \quad c \leftrightarrow (1,0) \tag{2.5}$$

and let $\lambda_s = (\lambda_{s,1}, \lambda_{s,2}), \mu_s = (\mu_{s,1}, \mu_{s,2}) \in \mathcal{K}$ in this notation. Thus $\lambda_{s,i}, \mu_{s,i} \in \{0, 1\}$. We have

$$\langle \alpha, \beta \rangle \equiv \sum_{s=1}^{\ell} \Big(\lambda_s \circ \mu_s + \frac{4}{3}\gamma_s\delta_s + \lambda_{s,1}(\delta_s + n_2^{(s)}) + \lambda_{s,2}(\delta_s + n_1^{(s)}) + \mu_{s,1}(\gamma_s + m_2^{(s)}) + \mu_{s,2}(\gamma_s + m_1^{(s)}) \Big) \pmod{2\mathbb{Z}}. \tag{2.6}$$

The inner product modulo $\mathbb{Z}$ reduces to (cf. the proof of [8, Theorem 5.7])

$$\langle \alpha, \beta \rangle \equiv \sum_{s=1}^{\ell} \Big(\frac{1}{2}\lambda_s \cdot \mu_s + \frac{1}{3}\gamma_s\delta_s \Big) \pmod{\mathbb{Z}}. \tag{2.7}$$

Let $(L_{C\times D})^{\perp} = \{\alpha \in (\mathbb{Q} \otimes_{\mathbb{Z}} L)^{\oplus \ell} \mid \langle \alpha, L_{C\times D} \rangle \subseteq \mathbb{Z}\}$. Then the following lemma holds.

Lemma 2.3. $(L_{C\times D})^{\perp} = L_{C^{\perp}\times D^{\perp}}$.

By the above lemma, we see that $L_{C\times D}$ is an integral lattice if and only if both of C and D are self-orthogonal. The first assertion of the next lemma follows from (2.6). The second assertion is a special case of the above lemma (cf. [8, Theorems 5.6, 5.7]).

Lemma 2.4. (1) *If C is even and D is self-orthogonal, then $L_{C\times D}$ is an even lattice.*
(2) *If C and D are self-dual, then $L_{C\times D}$ is a unimodular lattice.*

Example 2.5. *For $\ell = 4$, let C and D be a $\mathcal{K}$-code and a $\mathbb{Z}_3$-code with generating matrices*

$$\begin{pmatrix} a & a & 0 & 0 \\ b & b & 0 & 0 \\ 0 & 0 & a & a \\ 0 & 0 & b & b \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 \end{pmatrix},$$

respectively. Then the lattice $L_{\{0\}\times D}$ is a $\sqrt{2}\,(E_8$-lattice) and $L_{C\times D}$ is an E_8-lattice. Note that D is the $[4, 2, 3]$ ternary tetra code.

For $\ell = 12$, let D be an orthogonal sum of three copies of the $[4, 2, 3]$ ternary tetra code and C be a $\mathcal{K}$-code with generating matrix

$$\begin{pmatrix} a & a & 0 & 0 & a & a & 0 & 0 & 0 & 0 & 0 & 0 \\ c & c & 0 & 0 & c & c & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a & a & 0 & 0 & a & a & 0 & 0 \\ 0 & 0 & 0 & 0 & c & c & 0 & 0 & c & c & 0 & 0 \\ 0 & 0 & a & a & 0 & 0 & a & a & 0 & 0 & 0 & 0 \\ 0 & 0 & c & c & 0 & 0 & c & c & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & a & a & 0 & 0 & a & a \\ 0 & 0 & 0 & 0 & 0 & 0 & c & c & 0 & 0 & c & c \\ 0 & 0 & a & 0 & 0 & 0 & 0 & a & 0 & 0 & c & b \\ 0 & 0 & b & 0 & 0 & 0 & 0 & b & 0 & 0 & a & c \\ a & b & 0 & 0 & 0 & c & 0 & 0 & 0 & c & 0 & 0 \\ b & c & 0 & 0 & 0 & a & 0 & 0 & 0 & a & 0 & 0 \end{pmatrix}$$

Then $L_{C\times D}$ is the Leech lattice Λ (cf. [8]). In both cases C is τ-invariant and self-dual and D is self-dual.

3. Vertex operator algebra $V_{L_{C\times D}}^{\hat{\tau}}$

Suppose C is a τ-invariant self-orthogonal $\mathcal{K}$-code of length ℓ and D is a self-orthogonal $\mathbb{Z}_3$-code of the same length. Then $L_{C\times D}$ is a positive definite even lattice by Lemmas 2.1 and 2.4. The isometry τ permutes the cosets $L^{(x,i)}$, $x \in \mathcal{K}$, $i \in \mathbb{Z}_3$ of L in $L^\perp$ by $\tau(L^{(x,i)}) = L^{(\tau(x),i)}$. Thus τ induces an isometry of $L_{C\times D}$, for we are assuming that C is τ-invariant. Note that τ is fixed-point-free on $L_{C\times D}$.

Following [7], we consider a central extension

$$1 \to \langle \kappa_2 \rangle \to \hat{L}_{C\times D} \xrightarrow{-} L_{C\times D} \to 1 \tag{3.1}$$

of the free abelian group $L_{C\times D}$ by an order 2 group $\langle \kappa_2 \rangle$ with associated commutator map $c_0(\alpha,\beta) = \langle \alpha,\beta\rangle + 2\mathbb{Z}$. Thus $aba^{-1}b^{-1} = \kappa_2^{\langle \bar{a},\bar{b}\rangle}$ for $a, b \in \hat{L}_{C\times D}$. Such a central extension is unique up to equivalence. Let $\hat{\theta} \in \operatorname{Aut} \hat{L}_{C\times D}$ be the distinguished lift of the isometry $\theta : \alpha \mapsto -\alpha$ of $L_{C\times D}$ defined by (cf. [7, (10.3.12)])

$$\hat{\theta} : \hat{L}_{C\times D} \to \hat{L}_{C\times D}; \quad a \mapsto a^{-1}\kappa_2^{\langle \bar{a},\bar{a}\rangle/2}. \tag{3.2}$$

Then $\hat{\theta}^2 = 1$, $\overline{\hat{\theta}(a)} = -\bar{a}$ for $a \in \hat{L}_{C\times D}$, and $\hat{\theta}(\kappa_2) = \kappa_2$.

There is a lift $\hat{\tau} \in \operatorname{Aut} \hat{L}_{C\times D}$ of τ such that $\hat{\tau}^3 = 1$, $\overline{\hat{\tau}(a)} = \tau(\bar{a})$ for $a \in \hat{L}_{C\times D}$, and $\hat{\tau}(\kappa_2) = \kappa_2$. Moreover, $\hat{\theta}\hat{\tau} = \hat{\tau}\hat{\theta}$ by (3.2) since $\langle \cdot, \cdot \rangle$ is τ-invariant.

We fix a section $L_{C\times D} \to \hat{L}_{C\times D}; \alpha \mapsto e^\alpha$ for later use. Consider the sublattice $L_{\{0\}\times D}$ of $L_{C\times D}$. By (2.6), $\langle \alpha,\beta\rangle \in 2\mathbb{Z}$ for any $\alpha,\beta \in L_{\{0\}\times D}$. Thus the inverse image $\hat{L}_{\{0\}\times D}$ of $L_{\{0\}\times D}$ under the homomorphism $\hat{L}_{C\times D} \xrightarrow{-} L_{C\times D}$ splits, that is, $\hat{L}_{\{0\}\times D} \cong L_{\{0\}\times D} \times \langle \kappa_2 \rangle$. Hence we can choose $e^\alpha \in \hat{L}_{\{0\}\times D}$ for $\alpha \in L_{\{0\}\times D}$ so that $e^0 = 1$ is the identity of the group, $e^\alpha e^\beta = e^{\alpha+\beta}$, $\hat{\theta}(e^\alpha) = e^{-\alpha}$, and $\hat{\tau}(e^\alpha) = e^{\tau(\alpha)}$. For $\alpha \notin L_{\{0\}\times D}$, we take $e^\alpha \in \hat{L}_{C\times D}$ to be an arbitrary $a \in \hat{L}_{C\times D}$ such that $\bar{a} = \alpha$.

Let $\mathbb{C}\{L_{C\times D}\} = \mathbb{C}[\hat{L}_{C\times D}]/(\kappa_2+1)\mathbb{C}[\hat{L}_{C\times D}]$ be the twisted group algebra of $L_{C\times D}$. By abuse of notation we write the same symbol e^α to denote the image of $e^\alpha \in \hat{L}_{C\times D}$ in $\mathbb{C}\{L_{C\times D}\}$. Then $e^\alpha e^\beta = (-1)^{\langle \alpha,\beta\rangle} e^\beta e^\alpha$ in $\mathbb{C}\{L_{C\times D}\}$. The automorphisms $\hat{\theta}$ and $\hat{\tau}$ naturally induce automorphisms of $\mathbb{C}\{L_{C\times D}\}$, also. The vertex operator algebra $V_{L_{C\times D}}$ associated to the lattice $L_{C\times D}$ is defined to be $V_{L_{C\times D}} = S(\hat{\mathfrak{h}}^-) \otimes \mathbb{C}\{L_{C\times D}\}$, where $S(\hat{\mathfrak{h}}^-)$ is a highest weight module for a Heisenberg algebra. As a vector space $S(\hat{\mathfrak{h}}^-)$ is isomorphic to a polynomial algebra with variables $\alpha_1^{(s)}(-n)$, $\alpha_2^{(s)}(-n)$, $n \in \mathbb{Z}_{>0}$, $1 \le s \le \ell$. Now $\hat{\theta}$ and $\hat{\tau}$ act on $S(\hat{\mathfrak{h}}^-)$ by $\hat{\theta}(\alpha_j^{(s)}(-n)) = -\alpha_j^{(s)}(-n)$ and $\hat{\tau}(\alpha_j^{(s)}(-n)) = \tau(\alpha_j^{(s)})(-n)$. Accordingly, $\hat{\theta}$ and $\hat{\tau}$ act on $V_{L_{C\times D}}$ by $\hat{\theta}(u \otimes a) = \hat{\theta}(u) \otimes \hat{\theta}(a)$ and $\hat{\tau}(u \otimes a) = \hat{\tau}(u) \otimes \hat{\tau}(a)$ for $u \in S(\hat{\mathfrak{h}}^-)$ and $a \in \mathbb{C}\{L_{C\times D}\}$. In fact, $\hat{\theta}$ and $\hat{\tau}$ are automorphisms of the vertex operator algebra $V_{L_{C\times D}}$ of order 2 and 3, respectively.

We consider the fixed point subalgebra $V_{L_{C\times D}}^{\hat{\tau}} = \{v \in V_{L_{C\times D}} \mid \hat{\tau}v = v\}$ of $V_{L_{C\times D}}$ by $\hat{\tau}$ as a module for $(V_L^{\hat{\tau}})^{\otimes \ell}$. We shall use the same notation as in [14] for simple $V_L^{\hat{\tau}}$-modules $V_{L^{(0,i)}}(\varepsilon)$, $V_{L^{(c,i)}}$, $V_L^{T_{\chi_i}}(\hat{\tau})(\varepsilon)$, and $V_L^{T_{\chi_i'}}(\hat{\tau}^2)(\varepsilon)$, $i,\varepsilon = 0,1,2$. For simplicity of notation, we also denote $V_L^{T_{\chi_i}}(\hat{\tau})(\varepsilon)$ and $V_L^{T_{\chi_i'}}(\hat{\tau})(\varepsilon)$ by $V_L^{T,i}(\hat{\tau})(\varepsilon)$ and $V_L^{T,i}(\hat{\tau}^2)(\varepsilon)$, respectively.

Let $C/\sim_\tau$ be the set of τ-orbits in C. Since τ is fixed-point-free on C, the nonzero codewords of C are divided into a union of τ-orbits of length 3. We write $\lambda \sim_\tau \mu$ if

λ and μ belong to a τ-orbit in C. Likewise, $\mathcal{K}^\ell/\sim_\tau$ denotes the set of τ-orbits in $\mathcal{K}^\ell$.

By (2.2) and (2.1), we have

$$\begin{aligned} V_{L_{C\times D}} &= \bigoplus_{\lambda\in C,\gamma\in D} V_{L_{(\lambda,\gamma)}} \\ &= \bigoplus_{\lambda\in C,\gamma\in D} V_{L^{(\lambda_1,\gamma_1)}}\otimes\cdots\otimes V_{L^{(\lambda_\ell,\gamma_\ell)}}. \end{aligned}$$

Note that $V_{L_{(\lambda,\gamma)}} = V_{L^{(\lambda_1,\gamma_1)}}\otimes\cdots\otimes V_{L^{(\lambda_\ell,\gamma_\ell)}}$ is a simple $(V_L)^{\otimes\ell}$-module.

The automorphism $\hat\tau$ of $V_{L_{C\times D}}$ transforms $V_{L_{(\lambda,\gamma)}}$ into $V_{L_{(\tau(\lambda),\gamma)}}$, since $\tau(L_{(\lambda,\gamma)}) = L_{(\tau(\lambda),\gamma)}$. If $\lambda = 0$ is the zero codeword of C, then $V_{L_{(0,\gamma)}} = V_{L^{(0,\gamma_1)}}\otimes\cdots\otimes V_{L^{(0,\gamma_\ell)}}$ is $\hat\tau$-invariant. For $\lambda\neq 0$, we have

$$\begin{aligned} &\{v\in V_{L_{(\lambda,\gamma)}}\oplus V_{L_{(\tau(\lambda),\gamma)}}\oplus V_{L_{(\tau^2(\lambda),\gamma)}} \mid \hat\tau v = v\} \\ &\quad = \{v+\hat\tau v+\hat\tau^2 v \mid v\in V_{L_{(\lambda,\gamma)}}\} \\ &\quad \cong V_{L_{(\lambda,\gamma)}}. \end{aligned}$$

Hence

$$V^{\hat\tau}_{L_{C\times D}} \cong \Big(\bigoplus_{\gamma\in D} V^{\hat\tau}_{L_{(0,\gamma)}}\Big)\oplus\Big(\bigoplus_{\substack{0\neq\lambda\in C/\sim_\tau\\ \gamma\in D}} V_{L_{(\lambda,\gamma)}}\Big).$$

Moreover,

$$\begin{aligned} V^{\hat\tau}_{L_{(0,\gamma)}} &= \{v\in V_{L_{(0,\gamma)}} \mid \hat\tau v = v\} \\ &= \bigoplus_{\varepsilon_1+\cdots+\varepsilon_\ell\equiv 0 \pmod 3} V_{L^{(0,\gamma_1)}}(\varepsilon_1)\otimes\cdots\otimes V_{L^{(0,\gamma_\ell)}}(\varepsilon_\ell) \end{aligned}$$

is a direct sum of simple $(V^{\hat\tau}_L)^{\otimes\ell}$-modules. In the case where $\lambda\neq 0$, we recall that

$$\begin{aligned} V_{L^{(0,i)}} &= V_{L^{(0,i)}}(0)\oplus V_{L^{(0,i)}}(1)\oplus V_{L^{(0,i)}}(2), \\ V_{L^{(a,i)}} &\cong V_{L^{(b,i)}} \cong V_{L^{(c,i)}} \end{aligned}$$

as $V^{\hat\tau}_L$-modules and consequently we know how $V_{L_{(\lambda,\gamma)}} = V_{L^{(\lambda_1,\gamma_1)}}\otimes\cdots\otimes V_{L^{(\lambda_\ell,\gamma_\ell)}}$ decomposes into a direct sum of simple $(V^{\hat\tau}_L)^{\otimes\ell}$-modules.

4. Simple $V^{\hat\tau}_{L_{C\times D}}$-modules

We keep the notation in the preceding section. Thus C is a τ-invariant self-orthogonal $\mathcal{K}$-code of length ℓ and D is a self-orthogonal $\mathbb{Z}_3$-code of the same length. First of all we discuss simple $V^{\hat\tau}_{L_{C\times D}}$-modules which appear in the simple $V_{L_{C\times D}}$-modules and in the simple $\hat\tau$- or $\hat\tau^2$-twisted $V_{L_{C\times D}}$-modules.

(1) Simple $V^{\hat\tau}_{L_{C\times D}}$-modules in simple $V_{L_{C\times D}}$-modules

The cosets of $L_{C\times D}$ in its dual lattice $(L_{C\times D})^\perp = L_{C^\perp\times D^\perp}$ are $L_{(\mu+C)\times(\delta+D)} = L_{(\mu,\delta)} + L_{C\times D}$, $\mu\in C^\perp/C$, $\delta\in D^\perp/D$. Thus every simple $V_{L_{C\times D}}$-module is isomorphic to one of $V_{L_{(\mu+C)\times(\delta+D)}}$, $\mu\in C^\perp/C$, $\delta\in D^\perp/D$ by [2]. We have $V_{L_{(\mu+C)\times(\delta+D)}}\circ\hat\tau = V_{L_{(\tau^{-1}(\mu)+C)\times(\delta+D)}}$. In particular, $V_{L_{(\mu+C)\times(\delta+D)}}$ is $\hat\tau$-stable if and only if $\mu = 0$. Then $V_{L_{C\times(\delta+D)}}(\varepsilon) = \{v\in V_{L_{C\times(\delta+D)}} \mid \hat\tau v = \xi^\varepsilon v\}$, $\varepsilon = 0,1,2$, and $V_{L_{(\mu+C)\times(\delta+D)}}$, $0\neq\mu\in C/\sim_\tau$ are inequivalent simple $V^{\hat\tau}_{L_{C\times D}}$-modules.

(2) Simple $V^{\hat\tau}_{L_{C\times D}}$-modules in simple $\hat\tau$-twisted $V_{L_{C\times D}}$-modules

Following a general method of [4] and [11], we can construct a family of simple $\hat{\tau}$-twisted $V_{L_{C\times D}}$-modules $V_{L_{C\times D}}^{T,\eta}(\hat{\tau}) = S[\tau]\otimes T_{\psi_\eta}$ parametrized by $\eta = (\eta_1, \dots, \eta_\ell) \in D^\perp/D$. Any simple $\hat{\tau}$-twisted $V_{L_{C\times D}}$-module is isomorphic to one of these by [5, Theorem 10.2.]. Let $V_{L_{C\times D}}^{T,\eta}(\hat{\tau})(r) = \{v \in V_{L_{C\times D}}^{T,\eta}(\hat{\tau}) \mid \hat{\tau}v = \xi^r v\}$, $r = 0, 1, 2$, which are simple $V_{L_{C\times D}}^{\hat{\tau}}$-modules. They decompose into a direct sum of simple $(V_L^{\hat{\tau}})^{\otimes\ell}$-modules as follows.

$$V_{L_{C\times D}}^{T,\eta}(\hat{\tau})(r) \cong \bigoplus_{\substack{(\gamma_1,\dots,\gamma_\ell)\in D \\ \varepsilon_1+\cdots+\varepsilon_\ell\equiv r \pmod 3}} V_L^{T,\eta_1-\gamma_1}(\hat{\tau})(\varepsilon_1)\otimes\cdots\otimes V_L^{T,\eta_\ell-\gamma_\ell}(\hat{\tau})(\varepsilon_\ell).$$

Each direct summand is a tensor product of simple $V_L^{\hat{\tau}}$-modules which appear in simple $\hat{\tau}$-twisted V_L-modules. The minimum weight of $V_{L_{C\times D}}^{T,\eta}(\hat{\tau})(r)$ is $\ell/9$, $2/3+\ell/9$, or $1/3+\ell/9$ according as $r = 0$, 1, or 2.

(3) Simple $V_{L_{C\times D}}^{\hat{\tau}}$-modules in simple $\hat{\tau}^2$-twisted $V_{L_{C\times D}}$-modules

As in the $\hat{\tau}$-twisted case, we can construct a family of simple $\hat{\tau}^2$-twisted $V_{L_{C\times D}}$-modules $V_{L_{C\times D}}^{T,\eta}(\hat{\tau}^2) = S[\tau^2]\otimes T_{\psi_\eta}$, $\eta \in D^\perp/D$. Let $V_{L_{C\times D}}^{T,\eta}(\hat{\tau}^2)(r)$ be the eigenspace for $\hat{\tau}^2$ in $V_{L_{C\times D}}^{T,\eta}(\hat{\tau}^2)$ with eigenvalue ξ^r. It is a simple $V_{L_{C\times D}}^{\hat{\tau}}$-module. We have

$$V_{L_{C\times D}}^{T,\eta}(\hat{\tau}^2)(r) \cong \bigoplus_{\substack{(\gamma_1,\dots,\gamma_\ell)\in D \\ \varepsilon_1+\cdots+\varepsilon_\ell\equiv r \pmod 3}} V_L^{T,\eta_1-\gamma_1}(\hat{\tau}^2)(\varepsilon_1)\otimes\cdots\otimes V_L^{T,\eta_\ell-\gamma_\ell}(\hat{\tau}^2)(\varepsilon_\ell).$$

as $(V_L^{\hat{\tau}})^{\otimes\ell}$-modules. The minimum weight of $V_{L_{C\times D}}^{T,\eta}(\hat{\tau}^2)(r)$ is $\ell/9$, $2/3+\ell/9$, or $1/3+\ell/9$ according as $r = 0$, 1, or 2.

We remark that $V_{L_{C\times D}}^{T,\eta}(\hat{\tau}^i)$, $i = 1, 2$ does not depend on the $\mathcal{K}$-code C.

Our purpose is to classify all simple $V_{L_{C\times D}}^{\hat{\tau}}$-modules. We begin with the case where both of C and D are the zero code. In this case the classification of simple $V_{L_{\{0\}\times\{0\}}}^{\hat{\tau}}$-modules is obtained by [6, Theorem 6.14] and fusion rules of simple $V_L^{\hat{\tau}}$-modules (cf. [13]). In fact, we have the following theorem.

Theorem 4.1. *The vertex operator algebra $V_{L_{\{0\}\times\{0\}}}^{\hat{\tau}}$ is rational and C_2-cofinite. The following is a complete set of representatives of equivalence classes of simple $V_{L_{\{0\}\times\{0\}}}^{\hat{\tau}}$-modules.*

(1) $V_{L_{(0,\gamma)}}(r)$, $\gamma \in \mathbb{Z}_3^\ell$, $r = 0, 1, 2$.

(2) $V_{L_{(\lambda,\gamma)}}$, $0 \neq \lambda \in \mathcal{K}^\ell/\sim_\tau$, $\gamma \in \mathbb{Z}_3^\ell$.

(3) $V_{L_{\{0\}\times\{0\}}}^{T,\eta}(\hat{\tau}^i)(r)$, $i = 1, 2$, $\eta \in \mathbb{Z}_3^\ell$, $r = 0, 1, 2$.

Our next step is the classification of simple modules for $V_{L_{\{0\}\times D}}^{\hat{\tau}}$, that is, the case where C is the zero code. We note that $V_{L_{\{0\}\times D}}^{\hat{\tau}} = \bigoplus_{\gamma\in D} V_{L_{(0,\gamma)}}^{\hat{\tau}}$ is a simple current extension of $V_{L_{\{0\}\times\{0\}}}^{\hat{\tau}}$ and so it is not difficult to study (cf. [16]). The following theorem holds.

Theorem 4.2. *The vertex operator algebra $V_{L_{\{0\}\times D}}^{\hat{\tau}}$ is rational and C_2-cofinite. The following is a complete set of representatives of equivalence classes of simple $V_{L_{\{0\}\times D}}^{\hat{\tau}}$-modules.*

(1) $V_{L_{\{0\}\times(\delta+D)}}(r)$, $\delta \in D^\perp/D$, $r = 0, 1, 2$.

(2) $V_{L_{\{\lambda\}\times(\delta+D)}}$, $0 \neq \lambda \in K^{\ell}/\sim_{\tau}$, $\delta \in D^{\perp}/D$.
(3) $V^{T,\eta}_{L_{\{0\}\times D}}(\hat{\tau}^i)(r)$, $i = 1,2$, $\eta \in D^{\perp}/D$, $r = 0,1,2$.

Finally, we consider the simple $V^{\hat{\tau}}_{L_{C\times D}}$-modules. If $C \neq \{0\}$, then $V^{\hat{\tau}}_{L_{C\times D}}$ contains some nonsimple current $V^{\hat{\tau}}_{L_{\{0\}\times D}}$-modules and certain technical difficulties occur. Because of this reason, we restrict ourselves to the case where D is a self-dual code and C is a τ-invariant self-dual code with the minimum weight at least 4. In this case there is only one simple $\hat{\tau}^i$-twisted $V_{L_{C\times D}}$-module, for $D^{\perp}/D$ is trivial. We denote the unique simple $\hat{\tau}^i$-twisted $V_{L_{C\times D}}$-module by $V^T_{L_{C\times D}}(\hat{\tau}^i)$, $i = 1,2$. Our main result is as follows.

Theorem 4.3. *Assume that D is a self-dual code and C is a τ-invariant self-dual code with the minimum weight at least 4. Then the vertex operator algebra $V^{\hat{\tau}}_{L_{C\times D}}$ is rational and C_2-cofinite. There are exactly nine equivalence classes of simple modules which are represented by the following ones.*

(1) $V_{L_{C\times D}}(r)$, $r = 0,1,2$.
(2) $V^T_{L_{C\times D}}(\hat{\tau}^i)(r)$, $i = 1,2$, $r = 0,1,2$.

We note that the codes C and D for the expression of the Leech lattice Λ as $L_{C\times D}$ in Example 2.5 satisfy the hypothesis of the theorem.

5. Further discussions

One of the most remarkable examples of orbifold is the fixed points subalgebra $V^{\hat{\theta}}_{\Lambda}$ of the Leech lattice vertex operator algebra V_{Λ} by the distinguished lift $\hat{\theta}$ of the -1 isometry θ of Λ ([7]). In fact, $V^{\hat{\theta}}_{\Lambda}$ has four equivalence classes of simple modules represented by $V^{+}_{\Lambda} = V^{\hat{\theta}}_{\Lambda}$, V^{-}_{Λ}, $V^{T,+}_{\Lambda}$, and $V^{T,-}_{\Lambda}$, where V^{T}_{Λ} is a unique simple $\hat{\theta}$-twisted V_{Λ}-module. Frenkel, Lepowsky and Meurman [7] constructed the moonshine vertex operator algebra $V^{\natural}$ as a direct sum $V^{+}_{\Lambda} \oplus V^{T,+}_{\Lambda}$ of the orbifold V^{+}_{Λ} and its simple module $V^{T,+}_{\Lambda}$. They also proved that the automorphism group $\mathrm{Aut}\, V^{\natural}$ is isomorphic to the monster simple group $\mathbb{M}$. The involution $\hat{\theta}$ corresponds to a $2B$ element of $\mathbb{M}$.

Now, choose C and D so that $L_{C\times D} = \Lambda$ (cf. Example 2.5). Recall that $\ell = 12$ in this case. Among the three simple $V^{\hat{\tau}}_{\Lambda}$-modules which appear in a unique simple $\hat{\tau}$-twisted V_{Λ}-module $V^{T}_{\Lambda}(\hat{\tau})$, namely, $V^{T}_{\Lambda}(\hat{\tau})(r)$, $r = 0,1,2$, only $V^{T}_{\Lambda}(\hat{\tau})(1)$ has integral weights. Similarly, among the simple $V^{\hat{\tau}}_{\Lambda}$-modules which appear in a unique simple $\hat{\tau}^2$-twisted V_{Λ}-module $V^{T}_{\Lambda}(\hat{\tau}^2)$, only $V^{T}_{\Lambda}(\hat{\tau}^2)(1)$ has integral weights. It is quite natural to expect that $V^{\hat{\tau}}_{\Lambda} \oplus V^{T}_{\Lambda}(\hat{\tau})(1) \oplus V^{T}_{\Lambda}(\hat{\tau}^2)(1)$ possesses a vertex operator algebra structure and it is isomorphic to $V^{\natural}$. The weight 2 space of $V^{\hat{\tau}}_{\Lambda}$, $V^{T}_{\Lambda}(\hat{\tau})(1)$, and $V^{T}_{\Lambda}(\hat{\tau}^2)(1)$ are of dimension 65664, 65610, and 65610, respectively. Since $\hat{\tau}$ acts on $V^{\hat{\tau}}_{\Lambda}$, $V^{T}_{\Lambda}(\hat{\tau})(1)$, and $V^{T}_{\Lambda}(\hat{\tau}^2)(1)$ as 1, ξ, and ξ^2, respectively, the trace of the action of $\hat{\tau}$ on the weight 2 space is 54. This agrees with the value of the character $\chi_1 + \chi_2$ at $3B$ elements, where χ_1 and χ_2 are the principal character and the irreducible character of $\mathbb{M}$ of degree 196883 (cf. [1]). Thus $\hat{\tau}$ should correspond to a $3B$ element of $\mathbb{M}$.

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *ATLAS of Finite Groups*, Oxford Univ. Press, 1985.

[2] C. Dong, Vertex algebras associated with even lattices, *J. Algebra* **161** (1993), 245–265.
[3] C. Dong, C.H. Lam, K. Tanabe, H. Yamada and K. Yokoyama, $\mathbb{Z}_3$ symmetry and W_3 algebra in lattice vertex operator algebras, *Pacific J. Math.* **215** (2004), 245–296.
[4] C. Dong and J. Lepowsky, The algebraic structure of relative twisted vertex operators, *J. Pure Appl. Algebra* **110**(1996), 259–295.
[5] C. Dong, H.S. Li and G. Mason, Modular-invariance of trace functions in orbifold theory and generalized moonshine, *Comm. Math. Phys.* **214** (2000), 1–56.
[6] C. Dong and G. Yamskulna, Vertex operator algebras, generalized doubles and dual pairs, *Math. Z.* **241** (2002), 397–423.
[7] I. B. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Pure and Applied Math., Vol. **134**, Academic Press, 1988.
[8] K. Kitazume, C.H. Lam and H. Yamada, Decomposition of the moonshine vertex operator algebra as Virasoro modules, *J. Algebra*, **226** (2000), 893–919.
[9] K. Kitazume, C.H. Lam and H. Yamada, 3-state Potts model, moonshine vertex operator algebra and $3A$ elements of the monster group, *IMRS*, No. **23** (2003), 1269–1303.
[10] C.H. Lam and H. Yamada, $\mathbb{Z}_2 \times \mathbb{Z}_2$ codes and vertex operator algebras, *J. Algebra* **224** (2000), 268–291.
[11] J. Lepowsky, Calculus of twisted vertex operators, *Proc. Natl. Acad. Sci. USA* **82** (1985), 8295–8299.
[12] M. Miyamoto and K. Tanabe, Uniform product of $A_{g,n}(V)$ for an orbifold model V and G-twisted Zhu algebra, *J. Algebra* **274** (2004), 80–96.
[13] K. Tanabe, On intertwining operators and finite automorphism groups of vertex operator algebras, *J. Algebra* **287** (2005), 174–198.
[14] K. Tanabe and H. Yamada, The fixed point subalgebra of a lattice vertex operator algebra by an automorphism of order three, to appear in *Pacific J. Math.*
[15] K. Tanabe and H. Yamada, in preparation.
[16] H. Yamauchi, Module categories of simple current extensions of vertex operator algebras, *J. Pure Appl. Algebra* **189** (2004), 315–328.

(K. Tanabe) DEPARTMENT OF MATHEMATICS, HOKKAIDO UNIVERSITY, SAPPORO 060-0810, JAPAN
E-mail address: ktanabe@math.sci.hokudai.ac.jp

(H. Yamada) DEPARTMENT OF MATHEMATICS, HITOTSUBASHI UNIVERSITY, KUNITACHI, TOKYO 186-8601, JAPAN
E-mail address: yamada@math.hit-u.ac.jp

A Class of Error-Correcting Pooling Designs on Complexes

Tayuan Huang [*1], Kaishun Wang [2] and Chih-wen Weng [3]

Abstract: As a generalization of d^e-disjunct matrices and *(w,r;d)-cover- free-families*, the notion of $(s,l)^e$ - *setwise disjunct* matrices is introduced for error-correcting *pooling designs* on complexes (or called *set pooling designs*). A decoding algorithm for pooling designs based on $(s,l)^e$ - *setwise disjunct* matrices is considered. We also show that *(w,r;d)-cover- free- families* under some numerical constraints form a class of $(s,l)^e$ - *setwise disjunct* matrices.

Key words: disjunct matrices, generalized cover free families, pooling designs on complexes.

Dedicated to Professor Eiichi Bannai on the occasion of his 60th birthday

1 Introduction

The notion of *superimposed codes* or d-disjunct matrices was first introduced in 1964 by Kautz and Singleton [7] in the context of superimposed binary codes, it has been generalized to d^e-disjunct matrices in 1989 by D'yachkov et. al. [2] and in 1997 by Macula [8], to superimposed (s,l)-codes, superimposed (s,l)-designs in 2002 by D'yachkov, Vilenkin, Macula, and Torney [1], and finally to $(w,r;d)$- cover free families recently in 2004 by Stinson and Wei [9].

In the context of $(s,l;e)$-*cover- free- families*, d-disjunct matrices with $(s,l;e) = (1,d;1)$ have been generalized to d^e- disjunct matrices with $(s,l;e) = (1,d;e+1)$ for error-correcting purpose [2, 8]; on the other hand, it has also been generalized to (s,l)-superimposed designs [1] with $(s,l;e) = (s,l;1)$ for the purpose of group testing on complexes. All these structures have found their applications in the designs of combinatorial group testing algorithms applicable to DNA library screening, and they are therefore also called *pooling designs* with various additional properties; see [3, 4] for more details.

In this paper, as a generalization of d^e-disjunct matrices and $(s,l;e)$-*cover- free-families*, the notion of $(s,l)^e$ - *setwise disjunct* matrices is introduced for error - correcting *pooling designs on complexes*. We show that $(s,l;e)$-*cover- free- families* indeed form a class of $(s,l)^e$ - *setwise disjunct* matrices in Section 3; followed by a decoding algorithm for error-correcting pooling designs based on $(s,l)^e$ - *setwise disjunct* matrices given in Section 4.

[1,3] Department of Applied Mathematics, National Chiao-Tung University, Hsinchu Taiwan, {thuang, weng}@math.nctu.edu.tw

[2] Department of Mathematics, Beijing Normal University, Beijing 10230 China, wangks@bnu.cdu.cn

2 Preliminary

The notion of pooling designs on complexes can be traced back to Torney [10] in 1999, and was called *sets pooling designs*. Consider the use of set systems for non-adaptive set pooling designs for positive family $\{P_1,...,P_j\} \subseteq \binom{[t]}{i}$ and M be the incidence matrix of the set system of order $N \times t$. The following two models were introduced by Torney in [10]; the second model might fit better in practice because it satisfies more stringent requirements:

1. unions of j of the intersection of i distinct d's must be distinct whenever the j of i-subsets are distinct; i.e., $\bigcup_{i\in I}(\bigcap_{a\in P_i} C_a) \neq \bigcup_{j\in I'}(\bigcap_{b\in P_j} C_b)$ whenever $I \neq I'$
2. consider j+1 distinct i-subsets of $[t]$, form the corresponding i-intersection of the respective d's; no union of j of these i-intersections should include the remaining i-intersection, i.e., $\bigcap_{a\in P_i} C_a \not\subset \bigcup_{i\in I}(\bigcap_{a\in P_i} C_a)$.

See [10] for more details.

The second model mentioned above has been carried out by D'yachkov, Vilenkin, Macula, and Torney [1] as follows: for positive integers s, l and t such that $s+l \leq t$, let $\wp(s,l,t)$ be the family of all antichains $\wp = \{P_1, P_2,..., P_k\}$ with $P_i \subseteq [t]$ and $|P_i| \leq l$ for each $i \leq k \leq s$.

Definition [1, p. 197] A binary matrix M of order $N \times t$ is called

1. a *superimposed* (s,l)*-code* if, for any two disjoint subsets S, L of $[t]$ with $|S| = s$ and $|L| = l$, there exists a row with entry 1 over L and 0 over S.
2. a *superimposed* (s,l) - *design* if $\bigcup_{P_i\in\wp}\left(\bigcap_{j\in P_i} C_j\right) \neq \bigcup_{P_i'\in\wp'}\left(\bigcap_{j\in P_i'} C_j\right)$ for distinct $\wp = \{P_1, P_2,..., P_k\}$, $\wp' = \{P_1', P_2', ..., P_h'\} \in \wp(s,l,t)$.

They showed that each (s,l)-superimposed code is an (s,l)-superimposed design, and each (s,l)-superimposed design is an $(s-1,l)$-superimposed code and an $(s,l-1)$-superimposed code as well.

On the other hand, the following notion of *(w,r;d)-cover-free-family* was introduced by Stinson and Wei.

Definition [9] Let w, r and d be positive integers, a set system $(X, \Im)$ is called a *(w,r;d)-cover-free-family* (or *(w,r;d)-CFF*) provided that for any blocks $B_1,..., B_w \in \Im$ and any other r blocks $A_1,..., A_r \in \Im$, we have that

$$\left|\bigcap_{1\leq i\leq w} B_i - \bigcup_{1\leq j\leq r} A_j\right| \geq d.$$

Less formally, the intersection of any w blocks contains at least d elements not in the union of r other blocks.

Note that the point-block incidence matrix of a $(l,s;1)$-*cover-free-family* is indeed a superimposed (s,l)-code. Motivated by the second model considered by Torney [10], amd as a common generalization of d^e -disjunct matrices and $(w,r;d)$-*cover-free-families*, the notion of $(s,l)^e$ - *setwise disjunct* matrices is introduced for pooling designs on complexes.

Definition: For positive integers s,l with $s+l \le t$, a binary matrix M of order $N \times t$ is called an $(s,l)^e$ - *setwise disjunct* matrix if

$$\left| \bigcap_{i \in A} C_i - \bigcup_{P_i \in \wp} \left(\bigcap_{j \in P_i} C_j \right) \right| \ge e$$

for any antichain $\wp = \{P_1, P_2, ..., P_k\} \in \wp(s,l,t)$, and for any $A \subseteq [t]$ with $|A| \le l$ and $A \notin \wp$.

An $(s,l)^e$- *setwise disjunct* matrices M can be used for a pooling design on complexes in the following way.

Let the columns of M be identified with the set of samples and its rows are identified with pools for testing such that $M(i,j) = 1$ if the j-th sample is included in the i-th pool. Suppose the set $[t] = \{1, 2, ..., t\}$ represent the set of samples with a (unknown and to be identified) positive family $\wp = \{P_1, P_2, ..., P_k\}$ of the power set $\wp([t])$ of $[t]$, each test checks whether a pool contains at least one positive set $P_i \in \wp$ completely. After the testing, the outcome vector

$$o(\wp) = o(\wp, M) = \text{the characteristic vector of the set } \bigcup_{P_i \in \wp} \left(\bigcap_{j \in P_i} C_j \right)$$

is reported for $\wp = \{P_1, P_2, ..., P_k\} \in \wp(s,l,t)$ if there is no error occurred during the processes. *i.e.*, a test is reported *positive* only if it contains a certain positive subset P_i. Suppose instead that the report $o(\wp) + \varepsilon$ with an error vector ε is received, Theorem 4 shows that the error occurring during the testing processing can be detected whenever the weight of ε is at most e, or even the errors can be corrected whenever the weight of ε is no larger than $\left\lfloor \frac{e-1}{2} \right\rfloor$. In case $l = 1$, then each $P_i \in \wp$ is reduced to a singleton, and it then reduces to d^e - disjunct matrices whenever $k = d$.

3. A class of $(s,l)^e$ - setwise disjunct matrices

Some good explicit constructions of generalized cover-free families, as well as non-constructive existence result using the probabilistic method including the Lovasz Local Lemma can be found in [9], some bounds (i.e., necessary conditions) for generalized cover-free families were obtained through two different approaches.

Theorem 2 The point-block incidence matrix M of an $(l,s;e)$ - cover free family $\{C_1, C_2, ..., C_t\}$ is an $(s,l)^e$ - setwise disjunct matrix of order $N \times t$.

Proof: For any antichain $\wp = \{P_1, P_2, ..., P_k\} \in \wp(s,l,t)$, and for any $A \subseteq [t]$ with $|A| \le l$ and $A \notin \wp$, let $a_i \in P_i$ for $i \le k \le s$ and let $S \subseteq [t]$ be an s-subset containing $\{a_1, ..., a_k\}$.

Then $\bigcup_{P_i \in \wp} \left(\bigcap_{j \in P_i} C_j \right) \subseteq \bigcup_{1 \le i \le k} C_{a_i} \subseteq \bigcup_{j \in S} C_j$, and hence

$$\left| \bigcap_{i \in A} C_i - \bigcup_{P_i \in \wp} \left(\bigcap_{j \in P_i} C_j \right) \right| \ge \left| \bigcap_{i \in A} C_i - \bigcup_{j \in S} C_j \right| \ge \left| \bigcap_{i \in A'} C_i - \bigcup_{j \in S} C_j \right| \ge e$$

where $A \subseteq A' \subseteq [t]$ with $|A'| = l$ because $\{C_1, C_2, ..., C_t\}$ is an $(l, s; e)$ - generalized cover free family. **Q.E.D.**

Lemma 3 Let M be an $(s,l)^e$ - setwise disjunct matrix, then the Hamming distance $d_H(o(\wp), o(\wp'))$ between $o(\wp)$ and $o(\wp')$ is at least e whenever $\wp, \wp' \in \wp(s,l,t)$ are distinct.

Proof: Without loss of generality, we may assume that $\wp' - \wp$ is non-empty and $A \in \wp' - \wp$, we have

$$\left| \bigcap_{i \in A} C_i - \bigcup_{B \in \wp} \left(\bigcap_{j \in B} C_j \right) \right| \ge e$$

by definition, and therefore $d_H(o(\wp), o(\wp')) \ge e$. **Q.E.D.**

For an $(s,l)^e$ - setwise disjunct matrix M, we are interested to know the minimum distance, i.e., the minimum of the set $\{ d_H(o(\wp), o(\wp')) \mid \wp, \wp' \in \wp(s,l,t) \}$.

Theorem 4 An $(s,l)^e$ - setwise disjunct matrix is a superimposed (s,l)-design with the minimum distance at least $2e$.

Proof: Let $\wp = \{P_1, P_2, ..., P_k\}$, $\wp' = \{P_1', P_2', ..., P_k'\} \in \wp(s,l,t)$ not comparable, then

$$\begin{aligned} & d_H(o(\wp), o(\wp')) \\ &= \left| \bigcup_{P_i \in \wp} \left(\bigcap_{j \in P_i} C_j \right) - \bigcup_{P_i' \in \wp'} \left(\bigcap_{j \in A_i} C_j \right) \right| + \left| \bigcup_{P_i' \in \wp'} \left(\bigcap_{j \in P_i'} C_j \right) - \bigcup_{P_i \in \wp} \left(\bigcap_{j \in P_i} C_j \right) \right| \\ &\ge \left| \bigcap_{j \in P_i} C_j - \bigcup_{P_i' \in \wp'} \left(\bigcap_{j \in P_i'} C_j \right) \right| + \left| \left(\bigcap_{j \in P_i'} C_j \right) - \bigcup_{P_i \in \wp} \left(\bigcap_{j \in P_i} C_j \right) \right| \\ &\ge 2e. \text{ Q.E.D.} \end{aligned}$$

4. A decoding algorithm for pooling designs based on $(s,\ell)^e$ - setwise disjunct matrices

The methodology used by Kautz-Singleton [7] has been generalized to a decoding method for polling designs based on d^e - disjunct matrices [5]. In this section, we shall show that similar argument works well also for a decoding algorithm of polling designs based on $(s,\ell)^e$ - setwise disjunct matrices.

Let χ_A with $A \subseteq [N]$ be the output vector for the group testing over the (to be identified) positive family $\wp = \{P_1, ..., P_k\}$, the following theorem provides an decoding algorithm over the $(s, \ell)^e$ - setwise disjunct matrix M.

Theorem 5 Let $A \subseteq [N]$, and let

$$\wp_A = \left\{ Z \,\middle|\, |Z| \le l, \text{and} \left| \bigcap_{j \in Z} C_j - \chi_A \right| \le \left\lfloor \frac{e-1}{2} \right\rfloor \right\}.$$

Then the following hold:

1. If $d_H(o(\wp), \chi_A) \le \left\lfloor \frac{e-1}{2} \right\rfloor$, then $\wp = \wp_A$.
2. Suppose $d_H(o(\wp), \chi_A) \le e-1$ and $\left| \bigcup_{B \in \wp_A} B \right| \le s$, then $o(\wp) = \chi_A$ if and only if $o(\wp_A) = \chi_A$.

Proof: To prove 1, let $Z \in \wp$, then $\bigcap_{i \in Z} C_i \subseteq o(\wp)$, and hence

$$\left| \bigcap_{j \in Z} C_j - \chi_A \right| \le d_H(o(\wp), \chi_A) \le \left\lfloor \frac{e-1}{2} \right\rfloor,$$

it follows that $Z \in \wp_A$. On the other hand, if $Z \in \wp_A$ but $Z \notin \wp$, then $\left| \bigcap_{j \in Z} C_j - o(\wp) \right| \ge e$ by definition. Since $d_H(o(\wp), \chi_A) \le \left\lfloor \frac{e-1}{2} \right\rfloor$, we then have $\left| \bigcap_{j \in Z} C_j - \chi_A \right| \ge \left\lfloor \frac{e-1}{2} \right\rfloor + 1$, a contradiction.

To prove 2, it is clear if $\wp = \wp_A$. Now suppose that $\wp \ne \wp_A$ then

$$d_H(o(\wp), \chi_A) > \left\lfloor \frac{e-1}{2} \right\rfloor$$

as just shown; in particular, $o(\wp) \ne \chi_A$. Hence,

$$d_H(o(\wp), \chi_A) \ge d_H(o(\wp), o(\wp_A)) - d_H(o(\wp_A), \chi_A) \ge e - (e-1) = 1,$$

and $o(\wp) \ne \chi_A$ as required. **Q.E.D**

References:

1. A. D'yachkov and P. Vilenkin, A. Macula, and D. Torney, Families of finite sets in which no intersection of ℓ sets is covered by the union of s others, Journal of Combinatorial Theory, Series A 99, 195-218 (2002).
2. A.G. D'yachkov, V.V. Rykov and A. M. Rashad, Superimposed distance codes, Problems of Control and Information Theory, Vol. 18(4), pp. 237-250, 1989.
3. D.-Z. Du and H.Q. Ngo, A survey on combinatorial group testing algorithms with applications to DNA library screening, DIMACS Series in Discrete Mathematics and Theoretical Computer Science Vol. 55, pp 171-182, 2000.

4. D.-Z. Du and F. K. Hwang, Pooling Designs and Nonadaptive Group Testing, World Scientific 2006.
5. T. Huang and C. Weng, A note on decoding of superimposed codes, Journal of Combinatorial Optimization 7 (2003) 383-384.
6. T. Huang and C. Weng, Pooling spaces and non-adaptive pooling designs, Discrete Mathematics 282 (2004) 163-169.
7. W. Kautz and R. Singleton, Nonrandom binary superimposed codes, IEEE Trans. Inf. Theory, 10, (1964) 363-377.
8. A.J. Macula, Error-correcting nonadaptive group testing with d^e-disjunct matrices, Discrete Appl. Math. 80 (2-3) (1997) 217-222.
9. D. R. Stinson and R. Wei, Generalized cover-free families, Discrete Mathematics 279 (2004) 463-477.
10. D. C. Torney, Set Pooling Designs, Annals of Combinatorics 3(1999) 95-101.

A Survey of Results on Distribution Invariants of Association Schemes

Nachimuthu Manickam
Department of Mathematics
DePauw University
Greencastle, Indiana 46135
USA

Introduction

Let $\chi = \left(X, \{R_i\}_{i=0}^{d}\right)$ be a symmetric association scheme and $\mathfrak{R}^X = V_0 \perp V_1 \perp \ldots \perp V_d$ be the orthogonal decomposition of $\mathfrak{R}^X$, the vector space generated by the elements of X over the field of real numbers $\mathfrak{R}$, with each V_i being the maximal common eigenspace of the adjacency matrices of χ. A vector $\omega \in \mathfrak{R}^X$ is said to be a general vector if and only if $\langle \omega, x \rangle \neq 0$ for all x in X. For i, $1 \leq i \leq d$, we define the i-th distribution invariant $Vt_i(\chi)$ as $Vt_i(\chi) = \min_{\omega} \left| \{ x \varepsilon X | \omega \varepsilon V_i, \langle \omega, x \rangle > 0 \text{ and } \omega \text{ general} \} \right|$. Let ω be a general vector for which $\left| \{ x \varepsilon X | \langle \omega, x \rangle > 0 \} \right| = Vt_i(\chi)$. Then the set $\{ x \varepsilon X | \langle \omega, x \rangle > 0 \}$ is called the ith distributed set. Several papers have appeared on distribution invariants since it was introduced in [3].

Calculating the first distribution invariant is itself a hard problem. When we talk about first distribution invariants, we usually order the maximal common eigenspaces $V_1, V_2, \cdots, V_d$ according to the increasing order of the eigenvalues of the adjacency matrix A_1.

The following theorem, due to Bier and Delsarte, gives certain bounds on the distribution invariants, but they are not of much use in practical calculations. First a definition:

Definition: Let $\sum = \left(X, \{R_i\}\right)$ $o \leq i \leq d$ be a distance regular graph of diameter d and let T be a subset of $\{1, 2, \ldots, d\}$. Then a subset of $Y \subseteq X$ is said to be a T-design if its characteristic vector $\Phi(Y)$ is orthogononal to the space V_T. $V_T = \perp_{i \in T} V_i$

Theorem 1.1 (Bier & Delsarte): If Y_I and Y_J represent I and J designs, where $I \subseteq \{1,2,\ldots,d\}$ and $J = \{1,2,\ldots,d\} \setminus I$ then

(i.) $Vt_J \leq |Y_I|$ and

(ii.) If $\sum$ admits a transitive automorphism group, then $\frac{|X|}{|Y_I|} \leq Vt_I$.

First Distribution Invariant of Johnson Scheme $J(n,d)$

From the structure of the first eigenspace V_1 of the Johnson scheme $J(n,d)$, it can be shown that calculating the first distribution invariant of $J(n,d)$ is equivalent to answering the following question

Question: Let n,d be positive integers such that $2d \le n$. Let $a_1,\ldots,a_n$ be real numbers satisfying $a_1 + a_2 + \ldots + a_n \ge 0$. Then how many d-subsets of the set $\{a_1,\ldots,a_n\}$ will give a non-negative partial sum? [4](Strictly speaking, we should call these multisets as some of the a_i may be repeated).

Denote by $A(a_1,a_2,\ldots,a_n,d)$ the number of d-subsets of the set $\{a_1,\ldots,a_n\}$ which give a non-negative partial sum. Then it can be shown that the first distribution invariant of $J(n,d)$, $Vt_1(J(n,d)) = \min_{a_1,a_2,\ldots a_n \in R}\{A(a_1,\ldots,a_n;d)\}$.

Remark: If we take $\{a_1,a_2,\ldots,a_n\} = \{n-1,-1,-1,\ldots,-1\}$ then $A(a_1,a_2,\ldots,a_n,d) = \binom{n-1}{d-1}$ Hence $Vt_1(J(n,d)) \le \binom{n-1}{d-1}$

Theorem 1: If d divides n, then $Vt_1(J(n,d)) = \binom{n-1}{d-1}$ for all $n \ge 2d$.

Lemma 1: If $Vt_1(J(n,d)) = \binom{n-1}{d-1}$ holds for some $n > d > 0$, then $Vt_1(J(n+d,d)) = \binom{n+d-1}{d-1}$ also holds [9]

Proof: It is enough to prove that for any sequence of $n+d$ numbers $a_1,\ldots,a_{n+d}$ such that $\sum_{i=1}^{n+d} a_i \ge 0$, there are at least $\binom{n+d-1}{d-1}$ d-subsets of these numbers with non-negative sums. For the given sequence of a_i's, we will count the number of pairs (A,B) in two different ways, where A and B are disjoint d-subsets of the set $S = \{a_1,\ldots,a_{n+d}\}$ and the sum of the numbers in B is negative. Let X denote the number of d-subsets of S with negative sums. Then the number of the above pairs is, on one hand, $X \cdot \binom{n}{d}$. On the other hand, if we pick A arbitrarily, then two things may happen. Either the sum of the numbers in A is negative (this may happen in X ways) or the sum of the numbers is A is non-negative (this happens in $\binom{n+d}{d} - X$ ways). In the first case, the sum of the remaining numbers is positive, so by our assumption that $A(n,d) = \binom{n-1}{d-1}$ there should be at most $\binom{n-1}{d}$ possibilities to pick up a set B from them, giving a negative sum.

Clearly we have at most $\binom{n}{d}$ choices to pick up B in the second case. Thus, this counting gives us that the number of the pairs is at most $X\cdot\binom{n-1}{d}+\left[\binom{n+d}{d}-X\right]\cdot\binom{n}{d}$, resulting in the inequality $X\cdot\binom{n}{d}\le X\binom{n-1}{d}+\left[\binom{n+d}{d}-X\right]\cdot\binom{n}{d}$. Rearranging the inequality we get $X\le\binom{n+d-1}{d}$, which is clearly equivalent to the result stated in the lemma.

Lemma 2: If $Vt_1(J(n,d))=\binom{n-1}{d-1}$ holds for some $n>d>0$, then for every integer $k>0$, $Vt_1(J(kn,d))=\binom{kn-1}{d-1}$ also holds [9].

Proof: Proof of this lemma is similar to the one given above. Now count the pairs (P,A) in two different ways where P is a partition of $S=\{a_1,\ldots,a_{kn}\}$ into k-subsets of Size n and A is a d-subset of any class of P such that sum of the numbers in A is negative.

These two lemmas really constitute induction steps for possible proofs that $Vt_1(J(n,d))=\binom{n-1}{d-1}$ for some pairs (n,d) One case where both of them are useful, independent of each other, is when $d|n$. $Vt_1(J(d,d))=1=\binom{d-1}{d-1}$ obviously holds, and thus, with the help of any of the above lemmas, $Vt_1(J(n,d))=\binom{n-1}{d-1}$ holds if $d|n$.

Theorem 2: $Vt_1(J(n,d))=\binom{n-1}{d-1}$ whenever $n\ge d^{2d+1}$.

Proof: Note that, if we can prove that for d and m positive integers $Vt_1(J(md+1,d))$ holds, then by lemma 2 $Vt_1(J(2md+2,d))$, ..., $Vt_1(J((d-1)md+d-1,d))$ and by theorem 2 2 $Vt_1(J((d-1)md+d,d))$ also hold. Next, using lemma 1, we get that $Vt_1(J(n,d))$ holds if $n\ge(d-1)md+d$, since in this case there will be an element i of the set $\{md+1,2md+2,\ldots,(d-1)md+d-1,(d-1)md+d\}$ such that n-i is non-negative and $d|(n-i)$. So, if m is big enough to satisfy $\binom{m+1}{d}\ge\binom{md}{d-1}$ then $Vt_1(J(m+1,d))=\binom{md}{d-1}$ holds. This is satisfied if $m>d^{2d}+d^2$, so by previous remarks $Vt_1(J(n,d))=\binom{n-1}{d-1}$ holds if $n>(d-1)(d^{2d}+d^2)+d$ or roughly $n>d^{2d+1}$. We think that the above bound is very far from the truth. In fact, we can give examples of pairs (n,d) where $Vt_1(J(n,d))<\binom{n-1}{d-1}$ only if n is very small compared to d, that is $n<4d$. The question of determining $A(n,d)$ is meaningless if $d<n$. If

d<n<2d, consider n in the form n=d+r. The n-tuple {1, 1, ..., 1, 1-2-d} will give $\binom{d+r-1}{d}$ d-subsets of non-negative sum which is always less than $\binom{d+r-1}{d-1}$ If 2d < n < 3d, n + 2d+r, consider the n-tuple {2, 2, ..., 2, 2-2d-r, 2-2d-r}. This has $\binom{2d+r-2}{d}$ d-subsets of non-negative sum which is less than $\binom{2d+r-1}{d-1}$ if, for example, $r < \frac{d}{2}$ This means that $Vt_1(J(5,2))$, $Vt_1(J(7,3))$, $Vt_1(J(8,3))$, $Vt_1(J(9,4))$, and $Vt_1(J(10,4))$ or in general $Vt_1(J(2d+1,d))$ are all less than the corresponding value of $\binom{n-1}{d-1}$. Finally, if 3d<n<4d and n is in the form n=3d+r, then take the n-tuple {3, 3, ..., 3, 3-r-3d, 3-r-3d, 3-r-3d} This gives $\binom{3d+r-3}{d}$ d-subsets of non-negative sums which is less than $\binom{3d+r-1}{d-1}$ if r is small compared with d, in particular if $d \geq 3$ and $r = 0(d)$ or $r = 1$ So $Vt_1(J(3d+1,d)) < \binom{3d}{d-1}$ if $d \geq 3$.

In all of the above examples, the number of the d-subsets giving negative sums were equal to $\binom{n-\left[\frac{n}{d}\right]}{d}$ for the given pair of n and d if d is not a divisor of n and n<4d. The same pattern of example could be continued for n>4d, but in those cases the number of d-subsets with a negative sum, this is $\binom{n-\left[\frac{n}{d}\right]}{d}$ is never less than $\binom{n-1}{d-1}$

The results given above and some other aspects of the problem encourage us to state the following conjecture [9].

Conjecture 1: For n>d>0, if d is not a divisor of n, then $Vt_1(J(n,d))$ is the minimum of $\binom{n-1}{d-1}$ and $\binom{n-\left[\frac{n}{d}\right]}{d}$ and $Vt_1(J(n,d)) = \binom{n-1}{d-1}$ if $d|n$. In particular, $Vt_1(J(n,d)) = \binom{n-1}{d-1}$ if $n \geq 4d$.

Srinivasan has pointed out an important application of this conjecture in [11]; he has shown that the validity of this conjecture settles some special cases of a number-theoretic conjecture by Alladi, Erdös, and Vaaler on multiplicative functions [1]. In [3], Bhatttacharya showed that the conjecture is true whenever $n \geq d^{\ell d+1} e^d d^{d+1}$ which is a slight improvement over the bound $n \geq d^{\ell d+1}$ given in [9]. For $d = 3$, it was shown in [5] that whenever $n \geq 11$, $Vt_1(J(n,3)) = \binom{n-1}{2}$. The rest of the cases n=8 and 10 (n=9 is automatically true by Theorem 1) were settled in [10]. Also a simple proof for the validity of the conjecture for d=3 is furnished in [10]

In the case of the q-analogue Johnson scheme $Jq(n,d)$, it is shown in [9] that $Vt_1\left(J_q(n,d)\right) = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q$ whenever d divides n, where $\begin{bmatrix} n \\ m \end{bmatrix}_q$ stands for the Gauessian integer $\begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)..(q^n-q^{m-1})}{(q^m-1)\ (q^m-q^{m-1})}$.

When d does not divide n, it is still an open problem

For the Hamming Scheme $H(n, q)$, it is shown in [5] that $Vt_1\left(H(n,q)\right) = q^{n-1}$ for all n and q. For the q-analogue Hamming Scheme, $Hq(n, d)$ (also called the association scheme of bilinear forms), $Vt_1\left(Hq(n,d)\right) = q^{n(d-1)}$ for all n, d, and q. This fact was proven in [7] using W-complement d-spreads introduced in [6].

I would like to point out here that no work has been done on higher order distribution invariants.

References

1. K. Alladi, P. Erdös, and J.D. Vaaler. Muptiplicative functions and Small Divisors. Theory and Diophantine Problems (Progr. Math)), 70 :1-14, 1987

2. E. Bannai and T. Ito, Algebraic Combinatorics I, Association Schemes, Benjamin/Cummings Lecture mote series in Math. 1984

3. A. Bhattachaya On a Conjecture of Manickam and Singhi Discrete Mathematics, 272: 259-261, 2003.

4. T. Bier and N. Manickam. The First Distribution in Variant of the Johnson Scheme SEAMS Bull. Math, 11(1) 61-68, 1987.

5. N. Manickam, Ph.D. thesis, The Ohio State University, 1986.

6. N. Manickam, W-Complement of Spreads, Singleton Systems, European Journal of Combinatorics. Vol 8 (4), 1987.

7. N. Manickam, First Distributed Sets in the Association Scheme of Bilinear Forms, Colloquia Mathematica Societatis Jangs Bolyai 60. Sets, Graphs, and Numbers. Budapest (Hungary), 1991.

8. N. Manickam and M. Miklös, On the Number of Non-Negative Partial Sums of a Non-Negative Sum, Colloquia Mathematica Societatis Jano Bolyai 52. Combinatorics, Eger (Hungary), 1987

9. N. Manickam and N.M. Singhi First Distribution Invariants and E-K-R Theorems Journal of Combinatorial Theory, Series A, 40(1): 91-103, 1988.

10. G. Marino and G. Shiaselotti, A Method to Count the Positive 3-Subsets in a Set of Real Numbers with Nonnegative sums European Journal of Combinatorics, 23(5)

Upper bounds for the Kissing Number from Semidefinite Programming

Christine Bachoc (in collaboration with Frank Vallentin)

Laboratoire A2X
Université Bordeaux 1

Algebraic Combinatorics
In honor of Eiichi Bannai's 60th birthday
June 26 - June 30, 2006

INTRODUCTION

- The linear programming method, originally due to Philippe Delsarte, is usually the best method to obtain upper bounds for sphere packing problems.
- We introduce a semidefinite programming method on the unit sphere of the Euclidian space.
- It contains the old LP method so in principle obtains better bounds, in particular on kissing numbers. However the numerical computations have not been completed yet so I will not claim any improvements of previous bounds.

  Wait and see !
- Our work is inspired by A. Schrijver recent work on binary codes (IEEE Tran. IT 2005).

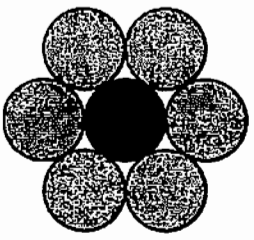
CONTENT OF THE TALK

- Review on the kissing number
- Review on the LP method
- Our SDP method

THE KISSING NUMBER τ_n

Definition. *τ_n is the maximal number of spheres of radius 1 that can touch a given sphere of the same radius 1 in $\mathbb{R}^n$.*

- Example: $n = 2$, $\tau_2 = 6$



- Known values of τ_n: $n = 1, 2, 3, 4, 8, 24$.

KNOWN VALUES OF τ_n

n	τ_n	construction	author
1	2	$\{-1, 1\}$	
2	6	A_2	
3	12	A_3, reg. icos.	Schütte-V. d. Waerden, 1954
		∞otly many	
4	24	D_4	Oleg Musin, 2003
		unique ?	
8	240	E_8	Odlyzko-Sloane, Levenshtein, 1979
		unique	Bannai-Sloane, 1981
24	196560	$S(\Lambda_{24})$	Odlyzko-Sloane, Levenshtein, 1979
		unique	Bannai-Sloane, 1981

KNOWN BOUNDS FOR τ_n

- Oleg Musin (2003) uses a variation on the LP method to obtain $\tau_4 = 24$ and reprove $\tau_3 = 12$, and Florian Pfender generalizes it and slightly strengthens some bounds ($n = 9, 10, 16, 17, \ldots$ (2005)).
- For other values of n, the current upper bounds are all obtained with Delsarte LP method.
- Spherical codes with given minimal angular distance:
  The determination of τ_n is a special case of the determination of the maximal number $A(n, \theta)$ of points of the unit sphere S^{n-1} with minimal angular distance θ since

$$\tau_n = A(n, \pi/3).$$

MAIN INGREDIENTS

- The LP method steps on polynomials $P_k^n(t)$ associated to S^{n-1} satisfying the following positivity property:

$$\text{for all finite } C \subset S^{n-1}, \sum_{(c,c') \in C^2} P_k^n((c,c')) \geq 0.$$

- Our SDP method steps on matrices $S_k^n(u,v,t)$ with polynomial coefficients satisfying the following positivity property:

$$\text{for all finite } C \subset S^{n-1}, \sum_{(c,c',c'') \in C^3} S_k^n((c,c'),(c,c''),(c',c'')) \succeq 0$$

REVIEW OF THE LP METHOD

- The unit sphere $S^{n-1} := \{x \in \mathbb{R}^n \mid (x,x) = 1\}$ is (2-point) homogeneous under the action of the group $\mathrm{O}(\mathbb{R}^n)$.
- $\mathrm{Pol}_d(S^{n-1})$: the space of real polynomial functions of degree at most d on S^{n-1}
  - induced action of $\mathrm{O}(\mathbb{R}^n)$.
  - $\mathrm{O}(\mathbb{R}^n)$-invariant scalar product:

$$< f, g >= \frac{1}{\omega_n} \int_{S^{n-1}} f(x) g(x) d\omega_n(x)$$

- Under the action of $\mathrm{O}(\mathbb{R}^n)$,

$$\mathrm{Pol}_d(S^{n-1}) = H_0^n \perp H_1^n \perp \cdots \perp H_d^n$$

where $H_k^n \simeq \mathrm{Harm}_k^n$ (homogeneous and harmonic polynomials of degree k in n variables). Let $h_k^n := \dim(\mathrm{Harm}_k^n)$.

REVIEW OF THE LP METHOD

- $P_k^n(t)$: the Gegenbauer polynomials with parameter $n/2-1$ (up to mult. cste)
  - $\deg(P_k^n) = k$
  - $P_k^n(1) = 1$
  - $k \neq l$, $\int_{-1}^{1} P_k(t)P_l(t)(1-t^2)^{(n-3)/2}dt = 0$
- These polynomials are related to the irreducible spaces H_k^n:

$$\left(x \to P_k^n((x,y))\right) \in H_k^n,$$

- Addition formula: for all $(e_1, e_2, \ldots, e_{h_k^n})$ orthonormal basis of H_k^n,

$$P_k^n((x,y)) = \frac{1}{h_k^n} \sum_{i=1}^{h_k^n} e_i(x)e_i(y).$$

REVIEW OF THE LP METHOD

- Proof of the positivity property:

$$\sum_{(c,c')\in C^2} P_k^n((c,c')) = \sum_{(c,c')\in C^2} \Big(\frac{1}{h_k^n} \sum_{i=1}^{h_k^n} e_i(c)e_i(c')\Big)$$

$$= \frac{1}{h_k^n} \sum_{i=1}^{h_k^n} \Big(\sum_{c,c'\in C} e_i(c)e_i(c')\Big) = \frac{1}{h_k^n} \sum_{i=1}^{h_k^n} \Big(\sum_{c\in C} e_i(c)\Big)^2 \geq 0.$$

- A rewritting of the positivity property: let

$$x(u) := \frac{1}{|C|}|\{(c,c') \in C^2 \mid (c,c') = u\}| \quad -1 \leq u \leq 1$$

then

$$\sum_u x(u)P_k^n(u) \geq 0.$$

REVIEW OF THE LP METHOD

- Properties of $x(u) := \frac{1}{|C|}|\{(c,c') \in C^2 \mid (c,c') = u\}|$:
  - $x(1) = 1$
  - $x(u) \geq 0$
  - If the minimal angular distance of C is θ, $x(u) = 0$ if $u \in]\cos\theta, 1[$.
  - $|C| = \sum_{u \in [-1,1]} x(u)$
  - $\sum_u x(u) P_k^n(u) \geq 0$ for all $1 \leq k \leq d$
- These conditions are all linear inequalities in the $x(u)$. They lead to a linear program whose solution gives an upper bound of $A(n,\theta) - 1$:

REVIEW OF THE LP METHOD

$$\max\{ \sum_{u \in [-1,\cos\theta]} x(u) :$$
$$x(u) = 0 \text{ for almost all } u \in [-1,\cos\theta]$$
$$x(u) \geq 0 \text{ for all } u \in [-1,\cos\theta]$$
$$1 + \sum_{u \in [-1,\cos\theta]} x(u) P_k^n(u) \geq 0 \text{ for all } 1 \leq k \leq d\}$$

The dual program is:

$$\min\{ \sum_{k=1}^{d} f_k :$$
$$f_k \geq 0,$$
$$\sum_{k=1}^{d} f_k P_k^n(u) \leq -1 \text{ for all } u \in [-1,\cos\theta]\}$$

REVIEW OF THE LP METHOD

Theorem. *Let $F(t) = \sum_{k=0}^{d} f_k P_k^n(t)$ be a polynomial of degree at most d in $\mathbb{R}[t]$. If the following two conditions are fullfiled:*

1. *$f_k \geq 0$ for all $k \geq 1$ and $f_0 > 0$*
2. *$F(u) \leq 0$ for all $u \in [-1, \cos\theta]$*

then,

$$A(n, \theta) \leq \frac{F(1)}{f_0}.$$

Famous example: $n = 8$, $\cos\theta = 1/2$,

$$F(t) = (t+1)(t+1/2)^2 t^2 (t-1/2)$$

leads to

$$\tau_8 \leq 240.$$

WHAT ARE LP AND SDP ?

A linear program, primal problem:

$$\begin{aligned} \min\{ \quad & b_1 x_1 + \cdots + b_m x_m : \\ & a_{10} + a_{11} x_1 + \cdots + a_{1m} x_m \geq 0 \\ & \cdots \\ & a_{r0} + a_{r1} x_1 + \cdots + a_{rm} x_m \geq 0 \} \end{aligned}$$

dual problem:

$$\begin{aligned} \max\{ \quad & -(a_{10} y_1 + \cdots + a_{r0} y_r) : \\ & y_j \geq 0 \\ & a_{11} y_1 + \cdots + a_{r1} y_r = b_1 \\ & \cdots \\ & a_{1m} y_1 + \cdots + a_{rm} y_r = b_m \} \end{aligned}$$

$$p^* = d^*$$

WHAT ARE LP AND SDP ?

A semidefinite program, primal problem:

$$\begin{aligned} \min\{ \quad & b_1 x_1 + \cdots + b_m x_m : \\ & A_0 + x_1 A_1 + \cdots + x_m A_m \succeq 0\} \end{aligned}$$

where A_i are $r \times r$ symmetric matrices.

Rq: The convex domain $A_0 + x_1 A_1 + \cdots + x_m A_m \succeq 0$ is not polyhedral like for LP (but piecewise defined by algebraic inequalities).

Dual problem:

$$\begin{aligned} \max\{ \quad & -\mathrm{Trace}(A_0 Z) : \\ & Z \succeq 0 \\ & \mathrm{Trace}(A_i Z) = b_i\} \end{aligned}$$

WHAT ARE LP AND SDP ?

- Covers LP with

$$A_i = \begin{pmatrix} a_{1i} & & \\ & \ddots & \\ & & a_{ri} \end{pmatrix}$$

- Often, the matrices A_i have a common diagonal block structure.
- $p^* = d^*$ under mild conditions
- Algorithms are essentially as efficient on SDP as on LP. We use CSDP 5.0 a package developped by Brian Borcherds.
- Roughly speaking: interior point methods construct successive pairs of feasible solutions of Primal and Dual, which objective function values converge to the optimal value and affords guaranteed lower and upper bounds for this optimal value.

AN SDP PROVIDING AN UPPER BOUND FOR $A(n,\theta)$

The general strategy:

- Find symmetric matrices S_k^n s.t.

$$\text{for all finite } C \subset S^{n-1},\ \sum_{(c,c',c'')\in C^3} S_k^n((c,c'),(c,c''),(c',c'')) \succeq 0$$

- Define $x(u,v,t) := \frac{1}{|C|}|\{(c,c',c'') \in C^3 \mid (c,c') = u, (c,c'') = v, (c',c'') = t\}|$. Then, $x(u,u,1) = x(u)$ and

$$\begin{cases} \sum_u x(u,u,1)P_k^n(u) \geq 0 \text{ for all } k \geq 1 \\ \sum_{u,v,t} x(u,v,t)S_k^n(u,v,t) \succeq 0 \text{ for all } k \geq 0. \end{cases}$$

- Together with other conditions, these properties lead to an SDP that contains the initial Delsarte LP.

ACTION OF $\mathrm{O}(\mathbb{R}^{n-1})$

- We fix $e \in S^{n-1}$, and let $H := \mathrm{Stab}(\mathrm{O}(\mathbb{R}^n), e) \simeq \mathrm{O}(\mathbb{R}^{n-1})$.
- Decomposition of Harm_k^n under the action of H:

$$\mathrm{Harm}_k^n \simeq \oplus_{i=0}^k \mathrm{Harm}_i^{n-1}.$$

- Decomposition of $\mathrm{Pol}_d(S^{n-1})$, with $H_{i,k}^{n-1} \simeq \mathrm{Harm}_i^{n-1}$:

$(\mathrm{O}(\mathbb{R}^n))$	$\mathrm{Pol}_d(S^{n-1})$	H_0^n	H_1^n	$\dots$	H_d^n
(H)	$\mathrm{Pol}_d(S^{n-1})$	$H_{0,0}^{n-1}$	$H_{0,1}^{n-1}$	$\dots$	$H_{0,d}^{n-1}$
			$H_{1,1}^{n-1}$	$\dots$	$H_{1,d}^{n-1}$
				$\ddots$	$\vdots$
					$H_{d,d}^{n-1}$

- The isotypic components of the H-decomposition of $\mathrm{Pol}_d(S^{n-1})$ are:

$$\mathcal{I}_k := H_{k,k}^{n-1} \perp \cdots \perp H_{k,d}^{n-1} \simeq (d-k+1)\,\mathrm{Harm}_k^{n-1}\,.$$

- To each $\mathcal{I}_k$ is associated an essentially unique 'zonal matrix' of size $(d-k+1)$, satisfying a 'positivity property', in the following way:

ZONAL MATRICES

Theorem. *Let $\mathcal{I} = R_0 \perp R_1 \perp \cdots \perp R_m \simeq (m+1)R$ be an isotypic component of $\mathrm{Pol}_d(S^{n-1})$ under the action of H, with R an H-irreducible space of dimension h. Let $(e_{0,1}, \ldots, e_{0,h})$ be an orthonormal basis of R_0 and let $\phi_i : R_0 \to R_i$ be H-isomorphisms preserving $<,>$. Let $e_{i,j} = \phi_i(e_{0,j})$, so that $(e_{i,1}, \ldots, e_{i,h})$ is an orthonormal basis of R_i. Let*

$$E(x) := \frac{1}{\sqrt{h}} \begin{pmatrix} e_{0,1}(x) & \cdots & e_{0,h}(x) \\ \vdots & & \vdots \\ e_{m,1}(x) & \cdots & e_{m,h}(x) \end{pmatrix}$$

$$\textit{and} \quad Z(x,y) := E(x)E(y)^t.$$

Then the following properties hold for the $(m+1) \times (m+1)$ matrix Z:

1. *For all $g \in H$, $Z(g(x), g(y)) = Z(x,y)$.*
2. *For all finite set $C \subset S^{n-1}$, $\sum_{(c,c') \in C^2} Z(c,c') \succeq 0$.*

- Proof of 2.: if $E(C) := \sum_{c \in C} E(c)$, then

$$\sum_{(c,c') \in C^2} Z(c,c') = (E_C)(E_C)^t \succeq 0.$$

- This theorem associates to each $\mathcal{I}_k$ a matrix denoted Z_k^n.
- The orbits of H acting on pairs $(x,y) \in S^{n-1}$ are determined by $((e,x),(e,y),(x,y))$.
- Therefore, because of 1., there exists matrices $Y_k^n(u,v,t)$ such that

$$Z_k^n(x,y) = Y_k^n((e,x),(e,y),(x,y)).$$

Next step is the computation of Y_k^n.

Theorem. *For all* $0 \le i,j \le d-k$,

$$\left(Y_k^n\right)_{i,j}(u,v,t) = \lambda_{i,j} P_i^{n+2k}(u) P_j^{n+2k}(v) Q_k^{n-1}(u,v,t)$$

where

$$Q_k^{n-1}(u,v,t) := \left((1-u^2)(1-v^2)\right)^{k/2} P_k^{n-1}\left(\frac{t-uv}{\sqrt{(1-u^2)(1-v^2)}}\right)$$

$$\text{and} \quad \lambda_{i,j} = \frac{\omega_n}{\omega_{n-1}} \frac{\omega_{n+2k-1}}{\omega_{n+2k}} (h_i^{n+2k} h_j^{n+2k})^{1/2}$$

If $\quad P_k(t) = a_k t^k + a_{k-2} t^{k-2} + a_{k-4} t^{t-4} + \dots$

then $\quad Q_k(u,v,t) = a_k (t-uv)^k$

$$+ a_{k-2}(t-uv)^{k-2}(1-u^2)(1-v^2)$$

$$+ a_{k-4}(t-uv)^{k-4}\left((1-u^2)(1-v^2)\right)^2 + \dots$$

Sketch of proof: We need explicit orthonormal basis of the spaces $H_{k,k+i}$. We use the following construction: for all $x \in S^{n-1}$, let

$$x = ue + \sqrt{1-u^2}\zeta$$

where $u = (x, e)$ and $\zeta \in S^{n-1} \cap (\mathbb{R}e)^{\perp} = S^{n-2}$.

$$f \in H_k^{n-1} \subset \mathrm{Pol}_k(S^{n-2}) \longmapsto \varphi(f) \in \mathrm{Pol}_k(S^{n-1})$$

defined by:

$$\varphi(f)(x) = (1-u^2)^{k/2} f(\zeta).$$

We have:

- φ commutes with the action of H
- $\varphi(H_k^{n-1}) = H_{k,k}^{n-1}$
- $H_{k,k+i}^{n-1} = \varphi(H_k^{n-1}) P_i(u)$ for some polynomial P_i of degree i.
- $i < j$, $H_{k,k+i}^{n-1} \perp H_{k,k+j}^{n-1} \Longrightarrow P_i \perp P_j$.

SYMMETRIZATION

Corollary. *Let S_k^n be defined by:*

$$S_k^n = \frac{1}{6} \sum_{\sigma} \sigma Y_k^n$$

where σ runs over the group (denoted S_3) of permutations of $\{u, v, t\}$. Then the matrices S_k^n are symmetric and have symmetric coefficients, and we have:

$$\textit{For all finite } C \subset S^{n-1}, \sum_{(c,c') \in C^2} Y_k^n((e,c),(e,c'),(c,c')) \succeq 0$$

and

$$\textit{For all finite } C \subset S^{n-1}, \sum_{(c,c',c'') \in C^3} S_k^n((c,c'),(c,c''),(c',c'')) \succeq 0.$$

THE SDP

$$x(u,v,t) := \frac{1}{|C|}|\{(c,c',c'') \in C^3 \mid (c,c') = u, (c,c'') = v, (c',c'') = t\}|.$$

- $u, v, t \in [-1, 1]$
- The matrix
$$\begin{pmatrix} 1 & u & v \\ u & 1 & t \\ v & t & 1 \end{pmatrix},$$
is positive semidefinite. This is equivalent to
$$1 + 2uvt - u^2 - v^2 - t^2 \geq 0.$$

- $x(u,u,1) = x(u)$.

- The $x(u,v,t)$ satisfy the following obvious properties:
$$\begin{cases} x(u,v,t) \geq 0 \\ x(1,1.1) = 1 \\ x(\sigma(u),\sigma(v),\sigma(t)) = x(u,v,t) \text{ for all } \sigma \in S_3 \\ \sum_{u,v,t} x(u,v,t) = |C|^2 \text{ and } \sum_{u} x(u,u,1) = |C| \end{cases}$$

- Moreover,
$$\begin{cases} \sum_{u} x(u,u,1) P_k^n(u) \geq 0 \text{ for all } k \geq 1 \\ \sum_{u,v,t} x(u,v,t) S_k^n(u,v,t) \succeq 0 \text{ for all } k \geq 0. \end{cases}$$

Let

$$D = \{(u,v,t) \mid -1 \le u \le v \le t \le \cos\theta \text{ and } 1 + 2uvt - u^2 - v^2 - t^2 \ge 0\}$$

$$D_0 = \{(u,u,1) \mid -1 \le u \le \cos\theta\} \qquad I = [-1, \cos\theta]$$

If the minimal angular distance of C is θ, we have moreover

$$x(u,v,t) = 0 \text{ if } (u,v,t) \notin D \cup D_0 \cup \{(1,1,1)\}$$

(up to permutation).

From the above discussion, an optimal solution to the following semidefinite program in the variables $x'(u,v,t) = m(u,v,t)x(u,v,t)$, where $m(u,v,t) = [\mathrm{S}_3 : \mathrm{Stab}(\mathrm{S}_3, (u,v,t))]$, is an upper bound for $A(n,\theta) - 1$:

$$\begin{aligned}
\max\{ \quad & \frac{1}{3}\sum_{u \in I} x'(u,u,1) : \\
& x'(u,v,t) = 0 \quad \text{for almost all } (u,v,t) \in D \cup D_0 \\
& x'(u,v,t) \ge 0 \quad \text{for all } (u,v,t) \in D \cup D_0 \\
& \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \sum_{u \in I} x'(u,u,1)\frac{1}{3}\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + \sum_{(u,v,t) \in D} x'(u,v,t)\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \succeq 0 \\
& 3 + \sum_{u \in I} x'(u,u,1)P_k^n(u) \ge 0 \quad \text{for all } 1 \le k \le d \\
& S_k^n(1,1,1) + \sum_{(u,v,t) \in D \cup D_0} x'(u,v,t)S_k^n(u,v,t) \succeq 0 \quad \text{for all } 0 \le k \le d\}
\end{aligned}$$

Third constraint: we have

$$|C|^2 = 1 + \sum_{(u,v,t)\in D\cup D_0} x'(u,v,t) = \Big(1 + \sum_{u\in I} x(u,u,1)\Big)^2,$$

which implies that

$$\sum_{(u,v,t)\in D} x'(u,v,t) + \frac{1}{3}\sum_{u\in I} x'(u,u,1) - \frac{1}{9}\Big(\sum_{u\in I} x'(u,u,1)\Big)^2 \geq 0.$$

The last condition is equivalent to: $\begin{pmatrix} 1 & B \\ B & C \end{pmatrix} \succeq 0$ with

$$\begin{cases} B = \dfrac{1}{3}\displaystyle\sum_{u\in I} x'(u,u,1) \\ C = \displaystyle\sum_{(u,v,t)\in D} x'(u,v,t) + \dfrac{1}{3}\sum_{u\in I} x'(u,u,1) \end{cases}$$

THE DUAL SDP

With $\langle A, B\rangle = \mathrm{Trace}(AB)$ and $S_k^n(1,1,1) = 0$ for $k \geq 1$, the dual SDP expression is:

Theorem. *The following semidefinite optimization problem gives an upper bound on* $A(n,\theta) - 1$*:*

$$\begin{aligned} \min\{ \quad & \sum_{k=1}^{d} a_k + b_{11} + \langle F_0, S_0^n(1,1,1)\rangle : \\ & a_k \geq 0, \quad \begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix} \succeq 0, \quad F_k \succeq 0, \\ & (i) \quad \sum_{k=1}^{d} a_k P_k^n(u) + 2b_{12} + b_{22} + \sum_{k=0}^{d} \langle F_k, 3S_k^n(u,u,1)\rangle \leq -1, \\ & (ii) \quad b_{22} + \sum_{k=0}^{d} \langle F_k, S_k^n(u,v,t)\rangle \leq 0\} \end{aligned}$$

where (i) holds for all $u \in I$ *and (ii) holds for all* $(u,v,t) \in D$.

FIRST STRATEGY: DISCRETIZE THE CONSTRAINTS

- Choose finite discretizations I^*, D^* of I, D.
- Solve the SDP corresponding to (i) for $u \in I^*$ and (ii) for $(u, v, t) \in D^*$.
- Try to prove (i) and (ii) for the feasible solution returned by the algorithm (or a weaker form).

Lemma. *Let U_0 be the $(d+1) \times (d+1)$ matrix with zeroes everywhere except the upper left coefficient equal to* 1.

Let $\{a_k^*, b_{i,j}^*, F_k^*\}$ be a feasible solution to the discretized SDP, with objective value b^*.

Let ϵ_0 be such that

$$b_{22}^* + \sum_k \langle F_k^*, S_k^n(u, v, t) \rangle \leq \epsilon_0 \text{ for all } (u, v, t) \in D$$

and such that $F_0^* - \epsilon_0 U_0 \succeq 0$. Let ϵ_1 be such that

$$\sum_k a_k^* P_k^n(u) + 2b_{12}^* + b_{22}^* + \sum_k \langle F_k^*, 3S_k^n(u, u, 1) \rangle \leq -1 + \epsilon_1 \text{ for all } u \in I.$$

Then we have

$$A(n, \theta) \leq \frac{(1 + b^*) - \epsilon_1 + 2\epsilon_0}{1 - \epsilon_1 + 3\epsilon_0}.$$

Second strategy: use Putinar theorem

- $\sum^2 = \{\sum_{i=1}^k q_i^2 : k \in \mathrm{N}, q_i \in \mathbb{R}[x_1, \ldots, x_n]\}$ denotes the cone of polynomials which can be written as sums of squares (SOS).

  Theorem. *(Putinar Positivstellensatz) Let* $K = \{x \in \mathbb{R}^n : p_1(x) \geq 0, \ldots, p_m(x) \geq 0\}$ *be a compact semialgebraic set. Suppose that there is a polynomial* P *of the form* $P = \sum^2 + p_1 \sum^2 + \cdots + p_m \sum^2$ *so that the set* $\{x : P(x) \geq 0\}$ *is compact. Then, if a polynomial* p *is positive on* K*, it can be written as*

$$p = \sum^2 + p_1 \sum^2 + \cdots + p_m \sum^2.$$

- A polynomial p of degree $2d$ lies in $\sum^2$ iff there is a positive semidefinite matrix Q so that $p = z^t Q z = \langle Q, z^t z \rangle$ where z is the vector of monomials $z = (1, x_1, \ldots, x_n, x_1 x_2, \ldots, x_{d-1} x_d, \ldots, x_n^d)$.

Theorem. *The following semidefinite optimization problem gives an upper bound on* $A(n, \theta) - 1$*:*

$$\begin{aligned}
\min\{ \quad & \sum_{k=1}^{d} a_k + b_{11} + \langle F_0, S_0^n(1,1,1) \rangle : \\
& a_k \geq 0, \quad \begin{pmatrix} b_{11} & b_{12} \\ b_{12} & b_{22} \end{pmatrix} \succeq 0, \quad F_k \succeq 0, \\
& P \succeq 0, \quad P_1 \succeq 0, \quad Q \succeq 0, \quad Q_i \succeq 0 \quad (1 \leq i \leq 4) \\
& (i) \quad \sum_{k=1}^{d} a_k P_k^n(u) + 2b_{12} + b_{22} + \sum_{k=0}^{d} \langle F_k, 3S_k^n(u,u,1) \rangle \\
& \qquad + \langle P, M_N(u) \rangle + \langle P_1, g(u) M_{N-1}(u) \rangle = -1, \\
& (ii) \quad b_{22} + \sum_{k=0}^{d} \langle F_k, S_k^n(u,v,t) \rangle \\
& \qquad + \langle Q, M_N(u,v,t) \rangle + \textstyle\sum_{i=1}^{4} \langle Q_i, g_i(u,v,t) M_{N-1}(u,v,t) \rangle = 0\}
\end{aligned}$$

An analogy between a real field and finite prime fields on six-line arrangements on a projective plane

Jiro Sekiguchi

1 Introduction

A simple six-line arrangement on a projective plane is obtained by a system of labelled six lines $L_1, L_2, \ldots, L_6$ with the conditions; (1) they are mutually different and (2) no three of them intersect at a point. We add the condition that (3) there is no conic tangent to all the lines.

We now explain some results on the real case. There are four types of simple six-line arrangements on a real projective plane (cf. B. Grünbaum [2]). Among the four types, one is characterized by the existence of a hexagon and one is characterized by the condition that the conic tangent to any five lines of the six lines does not intersect the remaining line. The totality of systems of labelled six lines with conditions (1), (2) admits the action of the sixth symmetric group by permutations among six lines. The advantage of the condition (3) is that the action of the sixth symmetric group on the totality of systems of labelled six lines with conditions (1), (2), (3) naturally extends to that of the Weyl group $W(E_6)$ of type E_6. It is shown in J. Sekiguchi and M. Yoshida [7] that $W(E_6)$ acts transitively on the set of six-line arrangements fixed by a group isomorphic to a fifth symmetric group and that this is decomposed into four subsets by the sixth symmetric group action. These four sets are in a one to one correspondence with the four types of simple-six line arrangements mentioned above.

The purpose of this paper is to study what happens when we replace a real projective plane by a projective plane over a finite prime field. Let p be a prime number, $\mathbf{F}_p$ the field consisting of p points and $\mathbf{P}^2(\mathbf{F}_p)$ the projective plane over $\mathbf{F}_p$. Let $L_1, L_2, \ldots, L_6$ be six lines on $\mathbf{P}^2(\mathbf{F}_p)$ with the conditions (1), (2), (3). Then the following two theorems hold.

Theorem 1. If 5 is a quadratic residue mod p, there is a system of labelled six lines on $\mathbf{P}^2(\mathbf{F}_p)$ fixed by a fifth symmetric group.

Theorem 2. Now assume that there is $n \in \mathbf{F}_p$ such that $n^2 \equiv 5\,(p)$. Then there is a system of labelled six-line arrangement fixed by a fifth symmetric group such that the conic tangent to any five lines of the six lines does not intersect the remaining line if and only if $\pm 2n - 5$ is non-quadratic residue mod p.

It is well-known that for a prime p, 5 is quadratic residue mod p if and only if $p = 10k+1$ or $p = 10k - 1$ for a positive integer k. The following theorem was conjectured by the author and later proved by T. Ibukiyama.

Theorem 3. For a prime p with $5 < p$, there is $n \in \mathbf{F}_p$ such that $n^2 \equiv 5\,(p)$ and there is no $m \in \mathbf{F}_p$ such that $m^2 \equiv 2n - 5\,(p)$, if and only if $p = 10k - 1$ for a positive integer k.

The details are shown in [6].

2 Systems of labelled six lines on a projective plane over a prime field

Let p be a prime number and let $\mathbf{F}_p$ be the prime field consisting of p elements. In this section, we study systems of labelled six lines on a projective plane defined over $\mathbf{F}_p$. Let $\mathbf{P}^2(\mathbf{F}_p)$ be a projective plane defined over $\mathbf{F}_p$. As before let $t_1 : t_2 : t_3$ be its homogeneous coordinate system.

First of all, we consider the conic tangent to five lines on $\mathbf{P}^2(\mathbf{F}_p)$. Let

(1) $t_1 = 0, t_2 = 0, t_3 = 0, a_1t_1 + a_2t_2 + a_3t_3 = 0, b_1t_1 + b_2t_2 + b_3t_3 = 0$

be equations of five lines. We assume that no three of them intersect at a point. Then it is easy to show that there is a unique conic tangent to the five lines (1) and it is defined by

(2) $p_1^2t_1^2 + p_2^2t_2^2 + p_3^2t_3^2 - 2p_2p_3t_2t_3 - 2p_3p_1t_3t_1 - 2p_1p_2t_1t_2 = 0.$

where

$$p_1 = a_1b_1(a_2b_3 - a_3b_2),\ p_2 = a_2b_2(a_3b_1 - a_1b_3),\ p_3 = a_3b_3(a_1b_2 - a_2b_1).$$

A system $\mathcal{S}$ of labelled six lines on $\mathbf{P}^2(\mathbf{F}_p)$ consists of labelled six lines $L_1, \ldots, L_6$ on it. We consider conditions (C1), (C2), (C3) on the system:

(C1) $L_1, \ldots, L_6$ are mutually different.

(C2) No three of them intersect at a point.

(C3) There is no conic tangent to all the six lines.

From the systems $\mathcal{S}$ with conditions (C1), (C2), (C3), we are naturally led to define the configuration space $\mathbf{P}_0(2,6)_{\mathbf{F}_p}$ over $\mathbf{F}_p$. The matrices of the form

(3) $$X = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & x_1 & x_2 \\ 0 & 0 & 1 & 1 & y_1 & y_2 \end{pmatrix}$$

with $x_1, x_2, y_1, y_2 \in \mathbf{F}_p$ are regarded as representatives of $\mathbf{P}_0(2,6)_{\mathbf{F}_p}$. Noting this, we may identify $\mathbf{P}_0(2,6)_{\mathbf{F}_p}$ with an affine open subset $S_{\mathbf{F}_p}$ of $\mathbf{F}_p^4$. In order to define $S_{\mathbf{F}_p}$ definitely, we introduce the fifteen polynomials f_j $(j = 1, 2, \ldots, 15)$ by

$$\begin{aligned} &f_1 = x_1,\ f_2 = x_2,\ f_3 = y_1,\ f_4 = y_2,\ f_5 = y_1 - x_1,\ f_6 = y_2 - x_2, \\ &f_7 = 1 - x_1,\ f_8 = 1 - x_2,\ f_9 = 1 - y_1,\ f_{10} = 1 - y_2, \\ &f_{11} = x_1 - x_2,\ f_{12} = y_1 - y_2,\ f_{13} = x_1y_2 - x_2y_1, \\ &f_{14} = x_1y_2 - x_2y_1 - x_1 + x_2 + y_1 - y_2, \\ &f_{15} = x_1y_1y_2 - x_2y_1y_2 + x_1x_2y_2 - x_1x_2y_1 - x_1y2 + x_2y_1. \end{aligned}$$

Then

$$S_{\mathbf{F}_p} = \{(x_1, x_2, y_1, y_2) \in \mathbf{F}_p^4;\ f_j \neq 0\ (j = 1, 2, \ldots, 15)\}.$$

It is easy to show that the Weyl group $W(E_6)$ acts on the space $S_{\mathbf{F}_p} \simeq \mathbf{P}_0(2,6)_{\mathbf{F}_p}$ by the same manner as in the real case (cf. [7]).

Let $\mathcal{S}$ be a system of labelled six lines $L_1, \ldots, L_6$ in $\mathbf{P}^2(\mathbf{F}_p)$. Then as mentioned before, for each j $(j = 1, 2, \ldots, 6)$, there is a unique conic C_j in $\mathbf{P}^2(\mathbf{F}_p)$ tangent to the five lines L_k $(k = 1, \ldots, 6,\ k \neq j)$. Since systems of labelled six lines of type III in the real case play an important role in the study [7], we introduce the notion of systems of labelled six lines of type III.

Definition 1 *A system $\mathcal{S}$ is of type III if $C_j \cap L_j = \emptyset$ for $j = 1, 2, \ldots, 6$.*

Then it is interesting to study the following problems.

Problem 1 *(i) Find a condition for the prime p in order that there exists a system of labelled six lines of type III.*

(ii) Fix a prime p for which there is a system of labelled six lines of type III. For any $(x_1, x_2, y_1, y_2) \in S$, does there exist $w \in W(E_6)$ satisfying the condition that w transforms (x_1, x_2, y_1, y_2) to $(u_1, u_2, v_1, v_2) \in S$ so that the system of labelled six lines corresponding to (u_1, u_2, v_1, v_2) is of type III?

Problem 2 *Find a condition for the prime p in order that there exists a system of labelled six lines fixed by a subgroup H of $W(E_6)$ isomorphic to the symmetric group of degree five.*

In the next section, we shall study topics related to these problems.

3 Systems of labelled six lines fixed by S_5-action over $\mathbf{F}_p$

In this section, we restrict our attention to such systems of labelled six lines that they are fixed by subgroups of $W(E_6)$ isomorphic to S_5.

We begin with this section with defining a subgroup $H(5)$ of $W(E_6)$ generated by $\tau(i\,i+1)'$ $(i = 2, 3, 4, 5)$. Clearly $H(5)$ is isomorphic to S_5. It is shown in [4] that there are forty five involutions in $W(E_6)$ conjugate to $\tau(i\,i+1)'$ $(i = 1, 2, \ldots, 5)$. As actions on $S_{\mathbf{F}_p}$, the explicit forms of $\tau(i\,i+1)'$ $(i = 2, \ldots, 5)$ are given in [7], Lemma 2. For example,

$$\tau(23)' : (x_1, x_2, y_1, y_2) \longrightarrow \left(\frac{x_2}{y_2}, x_2, \frac{x_2 y_1}{x_1 y_2}, \frac{x_2}{x_1}\right)$$

Noting this, we conclude that for $(x_1, x_2, y_1, y_2) \in S_{\mathbf{F}_p}$, (x_1, x_2, y_1, y_2) is fixed by $\tau(23)'$ if and only if $x_2 - x_1 y_2 = 0$. More generally we have the following lemma (cf. [7], Corollary 1 to Lemma 2).

Lemma 1 *For $i = 2, 3, 4, 5$, the fixed point set of $\tau(i\,i+1)'$ is given by $k_{i\,i+1} = 0$, where*

$$(4) \qquad \begin{array}{ll} k_{23} = -x_2 + x_1 y_2, & k_{34} = -(x_1 - x_2 - y_1 + x_2 y_1), \\ k_{45} = x_2 y_1 - y_2, & k_{56} = x_1 - x_2 + y_2 - x_1 y_2. \end{array}$$

Theorem 1 *Let p be a prime number with $p > 5$. Then there is $(x_1, x_2, y_1, y_2) \in S_{\mathbf{F}_p}$ fixed by $H(5)$ if and only if there is $n \in \mathbf{Z}$ such that $n^2 \equiv 5\ (p)$.*

Let p be a prime number with $p > 5$. Then it follows from the reciprocity law for the Legendre symbol that 5 is a quadratic residue mod p if and only if $p+1$ or $p-1$ is divisible by 5. Noting that p is odd, this is equivalent to that there is an integer k such that $p = 10k+1$ or $p = 10k-1$.

In the rest of this section, we always assume that p is a prime number of the form $p = 10k+1$ or $p = 10k-1$. Moreover let n be an integer such that $n^2 \equiv 5\ (p)$ and fix it.

It follows from the computation above that $((-1-n)/2, (1-n)/2, (1-n)/2, (3-n)/2)$ is the fixed point of $H(5)$ in $W(E_6)$. Put $a = (p+1)/2 \cdot (1-n)$. Then we find that

$$(a-1, a, a, a+1) = ((-1-n)/2, (1-n)/2, (1-n)/2, (3-n)/2)$$

and the corresponding matrix is

$$X_{\mathbf{F}_p}(n) = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & a-1 & a \\ 0 & 0 & 1 & 1 & a & a+1 \end{pmatrix}.$$

Then we have the following theorem.

Theorem 2 *Let p be a prime number and suppose that $p = 10k-1$ or $p = 10k+1$ for an integer k. Then the system of labelled six lines defined by the matrix $X_{\mathbf{F}_p}(n)$ is of type III if and only if $\left(\dfrac{2n-5}{p}\right) = -1$.*

It is interesting to determine such prime numbers satisfying the condition in Theorem 2.

Theorem 3 *Let p be a prime number with $5 < p$. Then there is $n \in \mathbf{F}_p$ such that $n^2 \equiv 5\ (p)$ and there is no $m \in \mathbf{F}_p$ such that $m^2 \equiv 2n-5\ (p)$ if and only if $p = 10k-1$ for a positive integer k.*

Remark 1 *The author proved Theorem 3 for such primes that $p < 1000$ by direct computation. Later T. Ibukiyama proved for an arbitrary prime p $(5 < p)$.*

4 Concluding remarks

(1) The condition for a prime number p that there is $n \in \mathbf{Z}$ such that $n^2 \equiv 5\ (p)$ is equivalent to the condition that the twenty seven lines on the Clebsch diagonal surface

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 = 0,\ x_1 + x_2 + x_3 + x_4 + x_5 = 0$$

are defined over the prime number field $\mathbf{F}_p$.

(2) Let p be a prime number such that $\left(\frac{5}{p}\right) = -1$. In this case, we consider a field extension $\mathbf{F}_p(n)$ over $\mathbf{F}_p$ attaching n such that $n^2 = 5$ in $\mathbf{F}_p$. Let $\mathbf{P}^2(\mathbf{F}_p(n))$ be a projective plane over $\mathbf{F}_p(n)$. Then it is possible to define systems of labelled six lines on $\mathbf{P}^2(\mathbf{F}_p(n))$ with conditions (C1), (C2), (C3). In this case, by direct computation, the condition for the existence of a system of labelled six lines of type III and fixed by the group $H(5)$ is equivalent to that there is no pair $(a, b) \in \mathbf{Z}^2$ such that $(an + b)^2 = 2n - 5$ in $\mathbf{F}_p(n)$, which is also equivalent to the condition that there is no pair $(a, b) \in \mathbf{Z}^2$ such that $5a^2 + b^2 \equiv -5$, $ab \equiv 1$ (p). It is easy to show that if $p \not\equiv \pm 1\,(5)$, then there is no pair (a, b) of integers satisfying the conditions $5a^2 + b^2 \equiv -5$, $ab \equiv 1$ (p). As a consequence, we conclude that there is a system of labelled six lines of type III and fixed by the group $H(5)$ on $\mathbf{P}^2(\mathbf{F}_p(n))$.

Acknowledgment The author thanks his colleague Professor H. Maeda for the discussion between them on number theory being very useful to formulate Theorem 3 and Professor T. Ibukiyama for proving it and kindly telling the author its proof.

References

[1] N. Bourbaki, *Groupes et Algèbres de Lie*. Chaps. 4, 5, 6, Herman, Paris (1968).

[2] B. Grünbaum, *Convex Polytopes*. Interscience (1967).

[3] T. Ibukiyama, Sekiguchi's Problem, private communication.

[4] I. Naruki, Cross ratio variety as a moduli space of cubic surfaces. *Proc. London Math. Soc.* **45** (1982), 1-30.

[5] J. Sekiguchi, Cross ratio varieties for root systems. *Kyushu J. Math.* , **48** (1994), 123-168.

[6] J. Sekiguchi, Simple six-line arrangements on a projective plane over a prime field, preprint.

[7] J. Sekiguchi and M. Yoshida, $W(E_6)$-action on the configuration space of 6 points of the real projective plane. *Kyushu J. Math.*, **51** (1997), 297-354.

[8] J. H. Silverman, *Friendly Introduction to Number Theory*.

Jiro SEKIGUCHI
Department of Mathematics
Tokyo University of Agriculture and Technology
Koganei, Tokyo 184-8588, JAPAN

Embeddings of resolvable group divisible designs with block size 3*

Jun Shen, Hao Shen
Department of Mathematics, Shanghai Jiao Tong University
Shanghai 200030, People's Republic of China
(ppshen@gmail.com, haoshen@sjtu.edu.cn)

July 21, 2006

Abstract

In this talk, we give the necessary and sufficient conditions for the embeddings of resolvable group divisible designs with block size 3.

1 Introduction

A *group divisible design* (GDD) of order v and index λ, denoted by GD$(K, \lambda, M; v)$, is an ordered triple $(X, \mathcal{G}, \mathcal{B})$ where

1) X is a set of v *points*,

2) $\mathcal{G}$ is a set of subsets (called *groups*) of X such that $\mathcal{G}$ partitions X and $|G| \in M$ for each $G \in \mathcal{G}$,

3) $\mathcal{B}$ is a collection of subsets (called *blocks*) of X such that $|B| \in K$ for each $B \in \mathcal{B}$, and each pair of points from distinct groups occurs in exactly λ blocks,

4) $|G \cap B| \leq 1$ for each $G \in \mathcal{G}$ and each $B \in \mathcal{B}$.

A GD$(K, \lambda, M; v)$ is also denoted by (K, λ)-GDD of type T where T is the multiset $\{|G| : G \in \mathcal{G}\}$. T is called the *group-type* or *type* of the GDD. We usually use an "exponential" notation to describe group-type: a type $1^i 2^j 3^k \ldots$ means i occurrences of 1, j occurrences of 2, etc.

When $\lambda = 1$, we simply write $GD(K, M; v)$ or K-GDD of type T. When $K = \{k\}$, we simply write k for $\{k\}$. When $M = \{m\}$, we simply write m for $\{m\}$. A (k, λ)-GDD of type m^u is called *uniform*. A (k, λ)-GDD of type m^k is called a *transversal design* and is denoted by TD$(k, \lambda; m)$. When $\lambda = 1$, we simply write TD(k, m).

A GD$(K, \lambda, M; v)$ is called *resolvable* and is denoted by RGD$(K, \lambda, M; v)$ or (K, λ)-RGDD of type T if its blocks can be partitioned into *parallel classes*, each of which

*Research supported by NSFC Grant 10471093

forms a partition of the point set X. A resolvable transversal design is denoted by RTD$(k, \lambda; m)$. When $\lambda = 1$, we simply write RTD(k, m).

An RGD$(3, \lambda, 1; v)$ is called an $RB(3, \lambda; v)$. An RB$(3, 1; v)$ is called a *Kirkman triple system* and denoted by KTS(v). An RGD$(3, 2; v)$ is called a *nearly Kirkman triple system* and denoted by NKTS(v).

The existence problem for resolvable group divisible designs with block size three has been completely solved.

Theorem 1.1 [1, 10, 11, 12] *An RGD$(3, \lambda, g; v)$ exists if and only if $v \geq 3g$, $\lambda(v - g) \equiv 0 \pmod 2$, $v \equiv 0 \pmod 3$, $v \equiv 0 \pmod g$, and $(\lambda, g, v) \neq (1, 2, 12)$, $(1, 6, 18)$, $(2j + 1, 2, 6)$, $(4j + 2, 1, 6)$, $j \geq 0$.*

Now let $(X_1, \mathcal{G}_1, \mathcal{B}_1)$ be an RGD$(K, \lambda, M; v)$, and $(X_2, \mathcal{G}_2, \mathcal{B}_2)$ be an RGD$(K, \lambda, M; u)$. If $X_1 \subset X_2$, $\mathcal{G}_1 \subset \mathcal{G}_2$, $\mathcal{B}_1 \subset \mathcal{B}_2$, and each parallel class of $\mathcal{B}_1$ is a part of some parallel class of $\mathcal{B}_2$, then we say $(X_1, \mathcal{G}_1, \mathcal{B}_1)$ is embedded in $(X_2, \mathcal{G}_2, \mathcal{B}_2)$, or $(X_2, \mathcal{G}_2, \mathcal{B}_2)$ contains $(X_1, \mathcal{G}_1, \mathcal{B}_1)$ as a *subdesign*.

The solution to the embedding problem for $(3, \lambda)$-RGDDs mainly depends on the cases $(\lambda, g) \in \{(1, 1), (1, 2), (1, 6), (1, 12), (2, 1), (2, 3)\}$. The following theorems are the known results.

Theorem 1.2 [13, 14, 18] *A KTS(v) can be embedded in a KTS(u) if and only if $u \equiv v \equiv 3 \pmod 6$, and $u \geq 3v$.*

Theorem 1.3 [3, 4, 5, 19] *An NKTS(v) can be embedded in an NKTS(u) if and only if $u \equiv v \equiv 0 \pmod 6$, $u \geq 3v$, and $v \neq 6, 12$.*

Theorem 1.4 [17] *An $RB(3, \lambda; v)$ can be embedded in an $RB(3, \lambda; u)$ if and only if $\lambda(u - 1) \equiv \lambda(v - 1) \equiv 0 \pmod 2$, $u \equiv v \equiv 0 \pmod 3$, $u \geq 3v$, and $(\lambda, v) \neq (4j + 2, 6)$, $j \geq 0$.*

In this talk, we will solve the embedding problem for $(3, \lambda)$-RGDDs with arbitrary group size g and index λ.

2 Recursive Constructions

To provide constructions for resolvable designs with subdesigns, we need some auxiliary designs.

Let $(X, \mathcal{G}, \mathcal{B})$ be a GD$(K, \lambda, M; v)$. It is called a (K, λ)-*frame* if the blocks of $\mathcal{B}$ can be partitioned into *holey parallel classes* each of which forms a partition of $X \setminus G$ for some $G \in \mathcal{G}$.

An *incomplete group divisible design* (IGDD) of index λ is a quadruple $(X, H, \mathcal{G}, \mathcal{B})$ satisfying the following conditions.

1) X is the point set, H is a subset (called a *hole*) of X,

2) $\mathcal{G}$ is a partition of X into subsets (called *groups*),

3) $\mathcal{B}$ is a collection of subsets (called *blocks*) of X such that each pair of points from distinct groups containing at least one member in $X \setminus H$ occurs in exactly λ blocks,

4) $|B \cap G| \leq 1$ for each $B \in \mathcal{B}$ and each $G \in \mathcal{G}$,

5) no block contains two members of H.

If $|B| \in K$ for each $B \in \mathcal{B}$, then an IGDD is called a (K, λ)-IGDD of type T, where K is a given set of positive integers, and T is the multiset $\{(|G|, |G \cap H|) : G \in \mathcal{G}\}$. T is called the *type* of the IGDD. As with GDDs, we use an "exponential" notation to describe the type. When $\lambda = 1$, we simply write K-IGDD. When $K = \{k\}$, we simply write k for $\{k\}$.

A (K, λ)-IGDD is said to be *resolvable* and is denoted by (K, λ)-IRGDD if its blocks can be partitioned into parallel classes and holey parallel classes, the latter partitioning $X \setminus H$.

In this talk, we will only use IRGDDs of types $(h, 0)^{m-n}(h, h)^n$ where $h > 0$ and $m > n > 0$. So, we will use $h^{(m,n)}$ to denote the types of such IRGDDs. It is easy to show that a (k, λ)-IRGDD of type $h^{(m,n)}$ contains $\lambda h(m-n)/(k-1)$ parallel classes and $\lambda h(n-1)/(k-1)$ holey parallel classes. We note that a (k, λ)-IRGDD of type $h^{(m,1)}$ is just a (k, λ)-RGDD of type h^m as in this case the number of holey parallel classes is 0.

The following lemmas are obvious but very useful in studying the embedding problem.

Lemma 2.1 *Suppose there exists a $(3, \lambda)$-IRGDD of type $g^{(u/g, v/g)}$ and an $RGD(3, \lambda, g; v)$. Then an $RGD(3, \lambda, g; v)$ can be embedded in an $RGD(3, \lambda, g; u)$.*

Lemma 2.2 *Suppose there exists a $(3, \lambda)$-IRGDD of type $g^{(u/g, v/g)}$ and an $RTD(3, m)$. Then there exists a $(3, \lambda)$-IRGDD of type $(mg)^{(u/g, v/g)}$.*

The following "filling in holes" construction is a powerful tool for the construction of IRGDDs. (see [6])

Construction 2.3 *Suppose there is a $(3, \lambda)$-frame of type $T = \{t_i : i = 1, 2, \ldots, n\}$. Let $g | t_i$ and $b > 0$. Suppose there also exists a $(3, \lambda)$-IRGDD of type $g^{(t_i/g+b, b)}$ for $i = 1, 2, \ldots, n-1$, then there exists a $(3, \lambda)$-IRGDD of type $g^{(u/g+b, t_n/g+b)}$ where $u = \sum_{i=1}^{n} t_i$. Furthermore, if there exists a $(3, \lambda)$-IRGDD of type $g^{(t_n/g+b, b)}$, then there exists a $(3, \lambda)$-IRGDD of type $g^{(u/g+b, b)}$.*

An *incomplete* $(3, \lambda)$-*frame* is a $(3, \lambda)$-IGDD $(X, H, \mathcal{G}, \mathcal{B})$ where the blocks of $\mathcal{B}$ can be partitioned into holey parallel classes, each of which forms a partition of $X \setminus G$ for some $G \in \mathcal{G}$, or a partition of $X \setminus (G \cup H)$ for some $G \in \mathcal{G}$.

The following lemma is a generalization of the construction used in [8, Lemma 5.4].

Lemma 2.4 *Suppose there is an incomplete $(3, \lambda)$-frame of type $t_1^x(t_2, t_2)^1(t_3, t_4)^1$, where $g | t_i$ for $i = 1, 2, 3, 4$. Suppose there also exists a $(3, \lambda)$-IRGDD of type $g^{(t_1/g+b, b)}$ and a $(3, \lambda)$-IRGDD of type $g^{(t_2+t_4)/g+b, t_4/g+b)}$, then there exists a $(3, \lambda)$-IRGDD of type $g^{(u/g+b, t_3/g+b)}$ where $u = x \cdot t_1 + t_2 + t_3$.*

3 Main Results

With the above preparations, we can prove the following lemmas and theorem.

Lemma 3.1 *There exists a 3-IRGDD of type* $6^{(u/6,v/6)}$ *if and only if* $u \equiv v \equiv 0 \pmod 6$, $u \geq 3v$, *and* $(u,v) \neq (18,6)$.

Lemma 3.2 *There exists a 3-IRGDD of type* $12^{(u/12,v/12)}$ *if and only if* $u \equiv v \equiv 0 \pmod{12}$, *and* $u \geq 3v$.

Lemma 3.3 *There exists a* $(3,2)$*-IRGDD of type* $3^{(u/3,v/3)}$ *if and only if* $u \equiv v \equiv 0 \pmod 3$, *and* $u \geq 3v$.

Theorem 3.4 *An* $RGD(3,\lambda,g;v)$ *can be embedded in an* $RGD(3,\lambda,g;u)$ *if and only if* $v \geq 3g$, $u \geq 3v$, $u \equiv v \equiv 0 \pmod 3$, $u \equiv v \equiv 0 \pmod g$, $\lambda(u-g) \equiv \lambda(v-g) \equiv 0 \pmod 2$, *and* $(\lambda,g,v) \neq (1,2,12),(1,6,18),(2j+1,2,6),(4j+2,1,6), j \geq 0$.

References

[1] A.M. Assaf, A. Hartman, Resolvable group divisible designs with block size 3, Discrete Math. 77(1989) 5-20.

[2] C.J. Colbourn, J.H. Dinitz(eds.), Handbook of Combinatorial Designs, CRC Press, Boca Raton, Florida 1996. (New results are reported at http://www.emba.uvm.edu/~dinitz/hcd.html)

[3] D. Deng, R. Rees, H. Shen, On the existence and application of incomplete nearly Kirkman triple systems with a hole of size 6 or 12, Discrete Math. 261(2003) 209-233.

[4] D. Deng, R. Rees, H. Shen, Further results on nearly Kirkman triple systems with subsystems, Discrete Math. 270(2003) 99-114.

[5] D. Deng, R. Rees, H. Shen, On the existence of nearly Kirkman triple systems with subsystems, Discrete Math., accepted.

[6] S.C. Furino, Y. Miao, J.X. Yin, Frame and Resolvable Designs: Uses, Constructions and Existence, CRC Press, Boca Raton, FL, 1996.

[7] G. Ge, C.W.H. Lam, Resolvable group divisible designs with block size four and group size six, Discrete Math. 268(2003) 139-151.

[8] G. Ge, R. Rees, On group-divisible designs with block size four and group-type $6^u m^1$, Discrete Math. 279(2004) 247-265.

[9] G. Ge, R. Rees, On group-divisible designs with block size four and group-type $g^u m^1$, Designs, Codes and Cryptography 27(2002) 5-24.

[10] E. Mendelsohn, H. Shen, A construction of resolvable group divisible designs with block size 3, Ars Combin. 24(1987) 39-43.

[11] R. Rees, Two new direct product-type constructions for resolvable group divisible designs, J. Combin. Designs 1(1993) 15-26.

[12] R. Rees, D.R. Stinson, On resolvable group-divisible desings with block size three, Ars Combin. 23(1987) 107-120.

[13] R. Rees, D.R. Stinson, On the existence of Kirkman triple systems containing Kirkman subsystems, Ars Combin. 26(1988) 3-16.

[14] R. Rees, D.R. Stinson, Kirkman triple systems with maximum subsystems, Ars Combin. 25(1988) 125-132.

[15] H. Shen, Constructions and Uses of Labeled Resolvable Designs, in: W.D. Wallis (Ed.), Combinatorial Designs and Applications, Marcel Dekker, New York, 1990, 97-107.

[16] H. Shen, Embeddings of simple triple systems, Sci. China Ser. A 35(1992) 283-291.

[17] H. Shen, Y. Wang, Embeddings of resolvable triple systems, J. Combin. Theory(A) 89(2000) 21-42.

[18] D.R. Stinson, Frames for Kirkman triple systems, Discrete Math. 65(1987) 289-300.

[19] S. Tang, H. Shen, Embeddings of nearly Kirkman triple systems, J. Stat. Plann. and Inference 94(2001) 327-333.

[20] J. Wang, Embeddings of Resolvable Designs, Ph.D. dissertation(in Chinese), Shanghai Jiao Tong University 2004.

A contraction of divisible designs

Yutaka Hiramine
(hiramine@gpo.kumamoto-u.ac.jp)
Department of Mathematics, Faculty of Education, Kumamoto University, Japan

Chihiro Suetake
(suetake@csis.oita-u.ac.jp)
Department of Mathematics, Faculty of Engineering, Oita University, Japan

Algebraic Combinatorics
(An International Conference in honour of Eiichi Bannai's 60$^{\text{th}}$ Birthday)
June 26-30, 2006
Sendai International Center, Sendai, Japan

1. Preliminaries

Definition 1.1
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a finite incidence structure ($v = |\mathcal{P}|, b = |\mathcal{B}|$). $\mathcal{D}$ is called an (m, u, k, λ)-**divisible design** and denoted by $\mathrm{DD}_\lambda[k, u; v]$ if the following conditions are satisfied.
(i) The point set $\mathcal{P}$ is partitioned into m *point classes* $\mathcal{P}_1, \cdots, \mathcal{P}_m$ such that $|\mathcal{P}_1| = \cdots = |\mathcal{P}_m| = u$, where $m = \frac{v}{u}$ and the number $[p_1, p_2]$ of blocks containing any two distinct points p_1, p_2 ($\in \mathcal{P}$) satisfies

$$[p_1, p_2] = \begin{cases} \lambda & \text{if } p_1 \text{and } p_2 \text{are in distinct} \\ & \text{point classes,} \\ 0 & \text{otherwise} \end{cases}$$

(ii) $|B| = k$ for every block $B \in \mathcal{B}$.

• Each point of a $\mathrm{DD}_\lambda[k, u; v]$ $\mathcal{D}$ is on exactly r blocks, where $r = \frac{\lambda(v-u)}{k-1}$.
$b = \frac{\lambda m(m-1)u^2}{k(k-1)}$.

Definition 1.2
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $\mathrm{DD}_\lambda[k, u; v], v = um$. If $|\mathcal{P}| = |\mathcal{B}|$, then $\mathcal{D}$ is called **square**. In this case,
$r = k, \quad b = um, \quad k(k-1) = \lambda(um - u)$.

Definition 1.3
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $\mathrm{DD}_\lambda[k, u; v], v = um$. If the dual structure of $\mathcal{D}$ is also a $\mathrm{DD}_\lambda[k, u; v]$, then $\mathcal{D}$ is called
symmetric and denoted by $\mathrm{SDD}_\lambda[k; u]$. In this case $\mathcal{B}$ is partitioned into m **block classes** $\mathcal{B}_1, \cdots, \mathcal{B}_m$ such that

(i) $|\mathcal{B}_1| = \cdots = |\mathcal{B}_m| = u$ and

(ii) $|B_1 \cap B_2| = \begin{cases} \lambda & \text{if } B_1 \text{ and } B_2 \text{ are in} \\ & \text{distinct block classes,} \\ 0 & \text{otherwise} \end{cases}$

In this case, $\mathcal{D}$ is square.

Definition 1.4
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $\mathrm{DD}_\lambda[k, u; v], v = um$. By definition, $m \geq k$. If $m = k$, $\mathcal{D}$ is called a **transversal design** and denoted by $\mathrm{TD}_\lambda[k, u; v]$.
If a $\mathrm{TD}_\lambda[k, u; v]$ is square, then $k = m = r = u\lambda$, $b = v = u^2\lambda$ and denoted by $\mathrm{TD}_\lambda[k; u]$.
Furthermore, if $\mathrm{TD}_\lambda[k, u; v]$ is symmetric, then it is denoted by $\mathrm{STD}_\lambda[k; u]$.

2. Contraction of $\mathrm{DD}_\lambda[k, u; v]$'s

• Let G be a permutation group on a set Ω. We say that G acts **semiregularly** on a subset Ω' of Ω if G leaves Ω' invariant and each nontrivial element of G has no fixed point on Ω'.
Let $\alpha \in \Omega$. Then we denote by α^G the G-orbit containing α.

Definition 2.1
Let $\mathcal{D}$ be a $\mathrm{DD}_\lambda[k, u; v]$. A subgroup G of $\mathrm{Aut}(\mathcal{D})$ is said to be
class semiregular if G acts on each point class of $\mathcal{D}$ semiregularly.

Lemma 2.2
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $\mathrm{DD}_\lambda[k, u; v], v = mu$. Assume that a subgroup G of $\mathrm{Aut}(\mathcal{D})$ is class semiregular. Then $B \cap B^x = \emptyset$ for any $x \in G \setminus \{1\}$ and $B \in \mathcal{B}$. In particular, G acts semiregularly on $\mathcal{B}$.

Corollary 2.3
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an $\mathrm{SDD}_\lambda[k; u]$. If a subgroup G of $\mathrm{Aut}(\mathcal{D})$ is class semiregular, then G is semiregular on each block class of $\mathcal{D}$.

Definition 2.4
An automorphism g of an $\mathrm{STD}_\lambda[k; u]$, say $\mathcal{D}$ $(= (\mathcal{P}, \mathcal{B}))$, is called
a **generalized elation** if it leaves each point class and each block class of $\mathcal{D}$ invariant.

Remark 2.5
Let $\mathcal{D}$ be as in Definition 2.4 and let $\{\mathcal{P}_1, \cdots, \mathcal{P}_k\}$ be the point classes of $\mathcal{D}$. If $\lambda = 1$ then $u = k$ and the incidence structure $\pi = (\mathcal{P}, \mathcal{B} \cup \{\mathcal{P}_1, \cdots, \mathcal{P}_k\})$ is an affine plane of order k. In this case, the notion of a generalized elation coincides with that of an affine elation of π.

Lemma 2.6
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an $\mathrm{SDD}_\lambda[k; u]$. If G is a group of generalized elations of $\mathcal{D}$, then G acts semiregularly on $\mathcal{P}$ and $\mathcal{B}$. In particular, G is class semiregular and $|G|$ divides u.

In Lemmas 2.8, 2.9 and Theorem 2.10, we assume the following.

2.7 Hypothesis
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a $\mathrm{DD}_\lambda[k, u; v], v = mu$. Assume that a subgroup G of $\mathrm{Aut}(\mathcal{D})$ is class semiregular. By Lemma 2.2, G acts semiregularly on $\mathcal{B}$ and so the length of each G-orbit on $\mathcal{B}$ is $|G|$.
Set $s = |G|, b' = \frac{b}{s}$ and $t = \frac{u}{s}$.
By the semiregularity of G, t and b' are positive integers.
For each i with $1 \leq i \leq m$,
let $\{\Omega_{(i-1)t+1}, \Omega_{(i-1)t+2}, \cdots, \Omega_{it}\}$ be the set of G-orbits on $\mathcal{P}_i$ and
let $\{\Delta_1, \Delta_2, \cdots, \Delta_{b'}\}$ be the set of G-orbits on $\mathcal{B}$.
Set $N_d = \{1, 2 \cdots, d\}$ for a positive integer d.
For each $i \in N_{mt}$ and $j \in N_{b'}$ we fix a point $p_i \in \Omega_i$ and a block $B_j \in \Delta_j$.

Lemma 2.8
If $p_i^x, p_i^y \in B_j$ for some $x, y \in G$, then $x = y$.

• Using Lemma 2.8 we define
$d_{ij} \in G \cup \{0\}$ by
$$d_{ij} = \begin{cases} x & \text{if } p_i{}^x \in B_j \ (\exists x \in G), \\ 0 & \text{otherwise} \end{cases}$$
Let $M = (d_{ij})$ be a $mt \times b'$ matrix with entries in $G \cup \{0\}$. We regard each entries d_{ij} of M as an element of $\mathbf{Z}[G]$.

• For a group ring element
$f = \sum_{x \in G} a_x x \in \mathbf{Z}[G]$ we define
$f^{(-1)} = \sum_{x \in G} a_x x^{-1} (\in \mathbf{Z}[G])$.
Set $M^{(-1)} = (d_{ij}^{(-1)})$ and
$z = \hat{G} \ (= \sum_{x \in G} x \ \in \mathbf{Z}[G])$.

Proposition 2.9
$$M(M^{(-1)})^T = \begin{bmatrix} k'I & \lambda z J & \lambda z I & \cdots & \lambda z J \\ \lambda z J & k'I & \lambda z J & \cdots & \lambda z J \\ \lambda z J & \lambda z J & k'I & \cdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda z J & \lambda z J & \cdots & \cdots & k'I \end{bmatrix},$$
where $k' = \frac{\lambda(v-u)}{k-1}$, I is a $t \times t$ identity matrix and J is a $t \times t$ all-one matrix.

Theorem 2.10
If an automorhism group G of a $GD_\lambda[k,u;v]$ of order s is class semiregular, then there exists a $GD_{\lambda s}[\frac{\lambda(v-u)}{k-1}, \frac{u}{s}; \frac{v}{s}]$.

As an application of Theorem 2.10, we have the following with the aid of compnter.

Theorem 2.11
Any $STD_2[12;6]$ admits no nontrivial generalized elation.

3. Class semiregular automorphisms of $TD_\lambda[k;u]$

Lemma 3.1
If a square transversal design $TD_\lambda[k;u]$ admits a class semiregular abelian automorphism group G of order s, then an equation

$$XX^{(-1)} = -\frac{1}{|G|}k^{\frac{u}{s}}\widehat{G} + k^{\frac{u}{s}}$$

has a solution X in $\mathbf{Z}[G]$.

For a positive integer m and n, we denote by $\mathrm{Ord}_n(m)$ the order of m in the multiplicative group of $\mathbf{Z}_n$. As an application of Lemma 3.1, we have

Theorem 3.2
Let $\mathcal{D}$ be a square transversal design $TD_\lambda[k;u]$ with k odd and let p be a prime which divides the square free part of k. If an automorhism σ of $\mathcal{D}$ of prime order $q(\neq p)$ acts semiregularly on each point class of $\mathcal{D}$, then $\mathrm{Ord}_q(p)$ is odd.

Corollary 3.3
Let p and q be distinct primes dividing an odd integer $n(>0)$. If p divides the square free part n^* of n and $\mathrm{Ord}_q(p)$ is even, then any projective plane of order n admits no elation of order q.

Example 3.4
(i) Since $\mathrm{Ord}_3(p)$ is 2 for an odd prime p with $p \equiv 2 \pmod 3$ $(p \in \{5, 11, 17, 23, \cdots\})$, any projective plane of odd order n such that $p \mid n^*$ and $3 \mid n$ admits no elation of order 3.
(ii) If $\mathrm{Ord}_q(3)$ is even for an odd prime q $(\in \{5, 7, 17, 19, 29, 31, \cdots\})$, any projective plane of odd order n such that $3 \mid n^*$ and $q \mid n$ admits no elation of order q.

References

[1] R. C. Bose and W. S. Connor, Combinatorial properties of group divisible incomplete block designs, *Ann. Math. Stat.* **24** (1952), 367-383.

[2] A. S. Hedayat, N. J. A. Sloane and John Stufken, *Orthogonal Arrays*, Springer-Verlag, Berlin/Heidelberg/New York, (1999).

[3] D. Jungnickel, On difference matrices, resolvable transversal designs and generalized Hadamard matrices, *Math. Z.* **167**(1979), 49-60.

[4] D. Jungnickel, On automorphism groups of divisible designs, *Canad. J. Math.* **34** (1982), 257-297.

[5] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, 2nd Edition. Cambridge University Press, Cambridge (1998).

[6] C. W. H. Lam, G. Kolesova, L. Thiel, A computer search for finite projective planes of order 9, *Discrete Math.* **92** (1991), 187-195.

[7] V. C. Mavron and V. D. Tonchev, On symmetric nets and generalized Hadamard matrices from affine designs, *J. Geom.* **67** (2000), 180-187.

[8] B. Schmidt, *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Mathematics 1797, Springer-Verlag (2002).

[9] C. Suetake, The nonexistence of projective planes of order 12 with a collineation group of order 16, *J. Combin. Theory, Ser. A* **107** (2004), 21-48.

[10] C. Suetake, The classification of symmetric transversal designs $STD_4[12;3]$'s, *Designs, Codes and Cryptography* **37** (2005), 293-304.

[11] J. A. Todd, A combinatorial problem, *J. Math. Phys.* **12** (1933), 321-333.

Gleason's Theorem on Self-Dual Codes and Its Generalizations

N. J. A. Sloane

AT&T Shannon Labs, Florham Park, NJ, USA

September 30, 2006; corrected October 17, 2006

TO EIICHI BANNAI, ON THE OCCASION OF HIS 60TH BIRTHDAY.

Abstract

One of the most remarkable theorems in coding theory is Gleason's 1970 theorem about the weight enumerators of self-dual codes. In the past 36 years there have been hundreds of papers written about generalizations and applications of this theorem to different types of codes, always on a case-by-case basis. In this talk I will state the theorem and then describe the far-reaching generalization that Gabriele Nebe, Eric Rains and I have developed which includes all the earlier generalizations at once. The full proof has just appeared in our book *Self-Dual Codes and Invariant Theory* (Springer, 2006).

This paper is based on my talk at the conference on Algebraic Combinatorics in honor of Eiichi Bannai, held in Sendai, Japan, June 26–30, 2006.

1. Motivation

Self-dual codes are important because they intersect with

- communications
- combinatorics
- block designs, spherical designs
- group theory
- number theory
- sphere packing
- quantum codes
- conformal field theory, string theory

2. Introduction

In classical coding theory (as for example in MacWilliams and Sloane [13]), a *code* C of length N over a field $\mathbb{F}$ is a subspace of $\mathbb{F}^N$. The *dual code* is

$$C^\perp := \{u \in \mathbb{F}^N : \ u \cdot c = 0, \ \ \forall c \in C\}.$$

Example: $C = \{000, 111\}$, $C^\perp = \{000, 011, 101, 110\}$ with $\mathbb{F} = \mathbb{F}_2$. The weight enumerators of these two codes are

$$W_C(x,y) = x^3 + y^3, \ \ W_{C^\perp}(x,y) = x^3 + 3xy^2.$$

A code is *self-dual* if $C = C^\perp$. For example, the binary code $i_2 := \{00, 11\}$ is self-dual, with weight enumerator

$$W_{i_2}(x,y) = x^2 + y^2. \tag{1}$$

Example: The Hamming code h_8 of length 8 is self-dual. This is the binary code with generator matrix:

∞	0	1	2	3	4	5	6
1	1	1	1	1	1	1	1
0	1	1	1	0	1	0	0
0	0	1	1	1	0	1	0
0	0	0	1	1	1	0	1

The second row of the matrix has 1's under the quadratic residues 0, 1, 2 and 4 mod 7. The remaining rows are obtained by fixing the infinity coordinate and cycling the other coordinates. This code has weight enumerator

$$W_{h_8}(x,y) = x^8 + 14x^4y^4 + y^8. \tag{2}$$

As can be seen from the generator matrix, this code is closely related to the incidence matrix of the projective plane of order 2.

If we replace the prime 7 in this construction by 23, we get the binary Golay self-dual code

g_{24} of length 24, with generator matrix as follows:

1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1,	1
0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0,	0,	1,	0,	1,	0,	0,	0,	0
0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0,	0,	1,	0,	1,	0,	0,	0
0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0,	0,	1,	0,	1,	0,	0
0,	0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0,	0,	1,	0,	1,	0
0,	0,	0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0,	0,	1,	0,	1
0,	1,	0,	0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0,	0,	1,	0
0,	0,	1,	0,	0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0,	0,	1
0,	1,	0,	1,	0,	0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0,	0
0,	0,	1,	0,	1,	0,	0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1,	0
0,	0,	0,	1,	0,	1,	0,	0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1,	1
0,	1,	0,	0,	1,	0,	1,	0,	0,	0,	0,	1,	1,	1,	1,	1,	0,	1,	0,	1,	1,	0,	0,	1

This has weight enumerator

$$W_{g_{24}}(x,y) = x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}. \tag{3}$$

3. MacWilliams' Theorem, 1962

In her Ph.D. thesis at Harvard in 1962, Jessie MacWilliams [11] showed that the weight enumerator of the dual of a linear code is determined by the weight enumerator of the code:

Theorem 1. *For a code C over $\mathbb{F}_q$,*

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y). \tag{4}$$

The proof uses the Poisson summation formula, in the form that says that the sum of a function f over a vector space is equal to the average of the appropriate Fourier transform of f over the dual vector space.

Corollary. If C is self-dual, $W_C(x,y)$ is fixed under the "MacWilliams" transformation

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & q-1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \tag{5}$$

4. First there were four types

As can be seen from (2) and (3), for some binary self-dual codes the Hamming weights of all the codewords (the powers of y) are multiples of 4. In other cases (as in (1)) the weights may only be even. Gleason and Pierce showed that there are essentially only four possibilities for this phenomenon to occur with self-dual codes over fields:

Theorem 2. (Gleason-Pierce (1967), see [1], [18]). *If C is a self-dual code over $\mathbf{F}_q$ with Hamming weights divisible by m, then one of the following holds:*

I) $q = 2$ $(\Rightarrow m = 2)$

II) $q = 2$ *and* $m = 4$

III) $q = 3$ $(\Rightarrow m = 3)$

IV) $q = 4$ *and Hermitian* $(\Rightarrow m = 2)$ *or* $q = 4$ *and Euclidean,*

or else $c = 2$, q *is arbitrary,* N *is even and* $W(x, y) = (x^2 + (q-1)y^2)^{N/2}$.

Because of this theorem, self-dual codes falling into one of those four classes came to be known as codes of Types I, II, III and IV, respectively.

Incidentally, the codes with $c = 2$ mentioned in the final clause of the theorem still have not been fully classified (see [18]).

5. Gleason's Theorem (1970, Nice)

At the International Congress of Mathematicians in Nice, 1970, Gleason established the following result.

Theorem 3. (Gleason [8]). *If C is a self-dual code of one of the four types mentioned in Theorem 2 then the weight enumerator of C belongs to the polynomial ring $\mathbb{C}[f, g]$, where:*

Type	f	g
I	$x^2 + y^2$ i_2	$x^2y^2(x^2 - y^2)^2$ Hamming code h_8
II	$x^8 + 14x^4y^4 + y^8$ Hamming code h_8	$x^4y^4(x^4 - y^4)^4$ binary Golay code g_{24}
III	$x^4 + 8xy^3$ tetracode	$y^3(x^3 - y^3)^3$ ternary Golay code
IV*	$x^2 + 3y^2$ $i_2 \otimes \mathbb{F}_4$	$y^2(x^2 - y^2)^2$ hexacode

*In fact Gleason omitted this case, which was first given in [12].

Under each polynomial we have written the name of a code whose weight enumerator leads to that polynomial. For example, the theorem states that the weight enumerator of a Type I

self-dual code belongs to the ring generated by the weight enumerators of the codes i_2 and h_8, that is, by $f = W_{i_2} = x^2 + y^2$ (see (1)) and W_{h_8} (see (2)). It is simpler to replace W_{h_8} as a generator of this ring by

$$g := \frac{1}{4}\left(f^4 - W_{h_8}\right) = x^2y^2(x^2 - y^2)\,,$$

as in the first row of the table.

In the following years many generalizations of Gleason's theorem were published, for example to self-dual codes over other fields ($\mathbb{F}_5, \ldots$), to biweight enumerators, split weight enumerators, codes containing the all-ones vector, etc.

The main applications of these theorems are in the classification of self-dual codes of moderate lengths, and in the determination of the optimal (or *extremal*) codes of the various Types. The book [15] contains an extensive bibliography.

6. $\mathbb{Z}/4\mathbb{Z}$ appears!

In the early 1990's, coding theory changed forever when it was discovered that certain infamous nonlinear binary codes were really *linear* (and in some cases self-dual) codes over the ring $\mathbb{Z}/4\mathbb{Z}$ of integers mod 4. For example, the Nordstrom-Robinson code is a famous nonlinear binary code of length 16 that contains 256 codewords and has minimal distance 6, more than is possible with any linear code of the same length and the same number of codewords (cf. [13]). Although nonlinear, its weight enumerator behaves like that of a linear binary code — it is fixed under (5) (with $q = 2$). In 1992, Forney, Trott and I [7] showed that this code is really a linear self-dual code over $\mathbb{Z}/4\mathbb{Z}$, a code already known as the *octacode* (cf. [5], [6]).

This work was extended by Hammons, Kumar, Calderbank, Solé and me in [9] to cover many other families of binary nonlinear codes, and this in turn was followed by numerous other papers that studied self-dual codes over the rings $\mathbb{Z}/m\mathbb{Z}$ for integers $m \geq 4$ (again see [15] for references).

7. And then there were nine!

In 1998, Eric Rains and I wrote a 120-page survey for the *Handbook of Coding Theory* [17] in which we distinguished nine types of self-dual codes, extending the original four types to include such families as linear codes over $\mathbb{Z}/4\mathbb{Z}$, linear codes over $\mathbb{Z}/m\mathbb{Z}$ for $m \geq 4$, additive codes over $\mathbb{F}_4$, etc. Again each version of Gleason's theorem was treated separately.

8. Higher-genus weight enumerators

In the mid-1990's there was a major breakthrough. As the result of a really amazing coincidence, we were led to investigate a certain family of "Clifford groups" $\mathcal{C}(m)$ with structure $2_+^{1+2m} \cdot O_{2m}^+(2)$. The story of this astonishing coincidence can be found in [4] and [15], so I will not repeat it here. Studying these "Clifford" groups led to breakthroughs in quantum codes [4] and to generalizations of Gleason's theorem to higher-genus or multiple weight enumerators [14].

9. The new book

After writing [14], we realized that the arguments used to handle the invariants of the Clifford groups could be extended to handle other classes of self-dual codes. The result is a far-reaching generalization of Gleason's theorem which defines the "Type" of a self-dual code in such a way that the weight enumerator of any code of that Type belongs to the invariant ring of a certain "Clifford-Weil" group associated with the Type, and furthermore that this invariant ring is spanned by weight enumerators of codes of that Type.

These are the two properties that previously had to be proved for each Type on a case-by-case basis. Now we know that this is automatically true, provided the codes fall into one of certain very general classes.

The proof of the general theorem is not easy, and occupies perhaps 150 pages of the new 400-page book, "Self-Dual Codes and Invariant Theory" [15].

For me, the book represents the culmination of thirty-five years of work.

In the rest of this talk I will give an outline of our approach, omitting all the technical details (and the category theory).

10. Notation: codes over rings

We will use the following notation:

$$\begin{aligned} R &= \text{ground ring} = \text{ring with unit} \\ V &= \text{left } R\text{-module} = \text{alphabet} \\ &\quad (\text{usually we assume } R \text{ and } V \text{ are finite}) \\ C &= \text{code of length } N \\ &= R\text{-submodule of } V^N \\ c \in C,\ r \in R &\Rightarrow rc \in C\,. \end{aligned}$$

Dual code:

$$\beta = \text{nonsingular bilinear form}\,,\quad \beta:\ V \times V \to \mathbb{Q}/\mathbb{Z}$$

$$\text{E.g. } \beta(u,v) = \tfrac{1}{2}uv \text{ (in the binary case)}$$

$$C^\perp := \left\{ u \in V^N :\ \sum_{i=1}^{N} \beta(u_i, c_i) = 0,\ \forall c \in C \right\}$$

11. Weight enumerators

Let $C \leq V^N$ be a code, where the alphabet $V = \{v_0, v_1, \ldots\}$. The *complete weight enumerator* of C is:

$$\mathrm{cwe}(C) \ :=\ \sum_{c \in C} \prod_{i=1}^{N} x_{c_i} \ \in\ \mathbb{C}[x_{v_0}, x_{v_1}, \ldots]\,.$$

Example: $\mathbb{F}_4 = \{0, 1, \omega, \bar{\omega}\}$,

$$\text{codeword } \ c = 0011\omega\bar{\omega} \ \Rightarrow\ x_0^2 x_1^2 x_\omega x_{\bar{\omega}}\,.$$

The *symmetrized weight enumerator* is obtained by identifying x_v and x_w in $\mathrm{cwe}(C)$ if we do not need to distinguish v and w. E.g. we usually set $x_{\bar{\omega}} = x_\omega$ for codes over $\mathbb{F}_4$. The *Hamming weight enumerator* is obtained from $\mathrm{cwe}(C)$ by setting $x_0 = x$ and all other $x_v = y$.

12. Biweight or genus-2 weight enumerator

Take an ordered pair of codewords $b, c \in C$ in all possible ways and write one above the other:

$$\begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & \omega & \bar{\omega} & \cdots \\ 0 & 1 & 0 & 1 & \omega & \bar{\omega} & \cdots \end{bmatrix}.$$

Then the *biweight* or *genus*-2 weight enumerator of C is

$$\mathrm{cwe}_2(C) := \sum_{(b,c)\in C\times C} \prod_{i=1}^{N} x \begin{pmatrix} b_i \\ c_i \end{pmatrix}.$$

Remark:

$$\mathrm{cwe}_2(C) = \mathrm{cwe}(C \otimes R^2).$$

For we have

$$C \otimes R^2 \leq V^N \otimes R^2 \cong V^{2N} \cong (V^2)^N.$$

Note that the ground ring for $C \otimes R^2$ is

$$\mathrm{Mat}_2(R),$$

the ring of 2×2 matrices over R. So, even in the case of classical binary codes, we need to use noncommutative rings when we consider higher-genus weight enumerators!

13. Extra conditions

Often one wants to consider self-dual codes with certain additional properties, for example that the weights are divisible by 4, or the code contains the all-ones vector. Some of these properties can be included in the new notion of Type, provided they can be described in terms of "quadratic mappings". Oversimplifying (see [15, Chapter 1] for the precise definition), a quadratic mapping is a map from V to $\mathbb{Q}/\mathbb{Z}$ which is the sum of a quadratic part and a linear part. If Φ is a collection of quadratic mappings then we say that a code C is *isotropic* with respect to Φ if

$$\sum_{i=1}^{N} \phi(c_i) = 0, \qquad \forall\, c \in C, \ \ \forall \phi \in \Phi.$$

Examples:

- $\phi(x) = \frac{1}{4}x^2$ (to get weights divisible by 4 in the binary case)
- $\phi(x) = \frac{1}{p}x$, p odd (to ensure that $1 \in C$)
- $\phi(x) = \beta(x,x)$ (specialization of β, always present)

14. The new definition of Type

We say that a code $C \leq V^N$ has

$$\text{Type } \rho := (R, V, \beta, \Phi)$$

if C is self-dual with respect to β and isotropic with respect to Φ.

Memo: Many details have been concealed here. See [15] for further information.

We call (R, V, β, Φ) a *form ring*, adapting a term from algebraic K-theory (cf. Bak [2]).

15. Symmetric idempotents

A *symmetric idempotent* $\iota \in R^*$ satisfies $\iota^2 = \iota$ together with certain extra conditions (see [15]), and has the property that there are "left" and "right" elements l_ι and r_ι associated with it such that

$$\iota = l_\iota r_\iota$$

Examples:

- $R = \mathbb{Z}/6\mathbb{Z}$: $\iota = 3 = 3 \cdot 3$ or $\iota = 4 = 4 \cdot 4$
- $R = \mathrm{Mat}_m(R') : \iota = \mathrm{diag}\{1, 0, 0, \ldots, 0\}$

16. The Clifford-Weil group $\mathcal{C}(\rho)$

We associate with the form ring $\rho = (R, V, \beta, \Phi)$ a certain finite subgroup of $GL_{|V|}(\mathbb{C})$ that we call the Clifford-Weil group $\mathcal{C}(\rho)$. This generalizes the familiar group of order 192 generated by

$$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \qquad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

that arises from Gleason's theorem for Type II (or doubly-even) binary codes, and also generalizes the Clifford groups $\mathcal{C}(m)$ mentioned above. The generators for $\mathcal{C}(\rho)$ are:

$$\rho(r): \quad x_v \mapsto x_{rv}, \qquad \forall r \in R^* \quad \text{(because } C \text{ is a code)}$$

$$\rho(\phi): \quad x_v \mapsto e^{2\pi i \phi(v)} x_v, \qquad \forall \phi \in \Phi \quad \text{(because } C \text{ is isotropic)}$$

and the "MacWilliams" transformations (generalizing (5)): for every symmetric idempotent $\iota = l_\iota r_\iota$ the associated MacWilliams transformation is

$$h_{\iota,r} : x_v \mapsto \frac{1}{\sqrt{|\iota V|}} \sum_{v \in V} e^{2\pi i \beta(w, r_\iota v)} x_{w + (1-\iota)v} \,.$$

Example of $h_{\iota,r}$:

$$R = V = \mathbb{Z}/6\mathbb{Z},$$

two symmetric idempotents $3 = 3 \cdot 3$, $4 = 4 \cdot 4$

For $\iota = 3$, $r_\iota = 3$, $|3V| = 2$:

$$h_{3,r_3} = \frac{1}{\sqrt{2}} \begin{bmatrix} + & 0 & 0 & + & 0 & 0 \\ 0 & - & 0 & 0 & + & 0 \\ 0 & 0 & + & 0 & 0 & + \\ + & 0 & 0 & - & 0 & 0 \\ 0 & + & 0 & 0 & + & 0 \\ 0 & 0 & + & 0 & 0 & - \end{bmatrix},$$

where + stands for $+1$ and $-$ for -1.

Our reasons for calling $\mathcal{C}(\rho)$ the Clifford-Weil group are that (i) when the groups $\mathcal{C}(m)$ mentioned in §8 act on the Barnes-Wall lattices, they act as the full orthogonal group $O^+_{2m}(2)$ on the Clifford algebra of the quadratic form, and (ii) in some situations $\mathcal{C}(\rho)$ coincides with the groups studied by Weil in his famous paper "Sur certaines groups d'opérateurs unitaires" [20].

17. Quasi-chain rings

Our main theorems will cover self-dual codes over a very large class of rings.

A *chain ring* is one in which the left ideals are linearly ordered by inclusion.

A *quasi-chain ring* is a direct product of matrix rings over chain rings.

Examples of quasi-chain rings:

- matrix rings over finite fields
- matrix rings over $\mathbb{Z}/m\mathbb{Z}$
- matrix rings over Galois rings

But not all rings are covered by the present theory. Examples of rings that are not (yet) covered:

- the group ring $\mathbb{F}_3$ Sym(3)
- the matrix ring

$$\begin{bmatrix} \mathbb{Z}/4\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \\ 2\mathbb{Z}/4\mathbb{Z} & \mathbb{Z}/4\mathbb{Z} \end{bmatrix}$$

18. The main theorems

Theorem. Let R be a finite chain ring or quasi-chain ring, and let ρ be the form ring

$$\rho = (R, V, \beta, \Phi) .$$

Consider codes $C \leq V^N$ of Type ρ. Then (i) $\mathrm{cwe}(C)$ belongs to the invariant ring $\mathrm{Inv}(\mathcal{C}(\rho))$, and (ii) $\mathrm{Inv}(\mathcal{C}(\rho))$ is spanned by the $\mathrm{cwe}(C)$, where C runs through codes of Type ρ.

The proof, as already mentioned, uses category theory and is long and hard, and takes up a good part of the book [15].

We believe, but have not been able to prove, that the theorem should hold without the restriction to quasi-chain rings. We state this as the:

Weight Enumerator Conjecture: The theorem should hold for any finite ring R.

19. An application

In their 1999 paper "Type II codes, even unimodular lattices and invariant rings" [3], Bannai, Dougherty, Harada and Oura consider codes of (in our new notation) Type $4^{\mathbf{Z}}_{\mathrm{II}}$. The corresponding Clifford-Weil group has order 1536, and the ring to which the complete weight enumerators belong has Molien series

$$\frac{1 + t^8 + 2t^{16} + 2t^{24} + t^{32} + t^{40}}{(1 - t^8)^3(1 - t^{24})} . \tag{6}$$

They remark that "it is not known if the invariant ring is generated by the complete weight enumerators of codes". This now follows immediately from our main theorem.

Incidentally, the nonzero coefficients of the Molien series in (6) form sequence A051462 in [19], where the reader will find references to both [3] and [15]. A great many Molien series arise in studying self-dual codes[1], and [19] provides a convenient way to keep track of them.

[1] The index to [15] lists the sequence numbers for over 100 such Molien series.

20. Example: Hermitian self-dual codes over $\mathbb{F}_9$

The form ring for Hermitian self-dual codes over $\mathbb{F}_9$ is $\rho = (R = V = \mathbb{F}_9, \beta, \Phi)$, where

$$\begin{aligned} \beta(v,w) &= \frac{1}{3}\mathrm{Tr}_{\mathbb{F}_9/\mathbb{F}_3}(v\bar{w}) \\ \Phi &= \{\beta(av,v),\ a \in \mathbb{F}_9\} \\ \mathbb{F}_9 &= \{0,1,\alpha,\alpha^2,\ldots,\alpha^7\}, \end{aligned}$$

with $\alpha^2 + \alpha = 1$, $\alpha^4 = -1$.

Generators for $\mathcal{C}(\rho)$ are:

$$\rho(\alpha) = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} =: M_1 .$$

The isotropic conditions are:

$$\Phi = \{\phi(a) : a \in \mathbb{F}_9\},$$

$$\begin{aligned} \phi(a)(v) &= \frac{1}{3}\,\mathrm{Tr}(av\bar{v}) = \frac{1}{3}\,\mathrm{Tr}(av^4) \\ &= \frac{1}{3}(av^4 + a^3v^4) = \frac{1}{3}(a + a^3)v^4 . \end{aligned}$$

Take $a = \alpha$, $\alpha + \alpha^3 = -1$. Then

$$\rho(\phi(\alpha)) :\ x_v \mapsto e^{2\pi i \cdot \frac{-v^4}{3}} x_v$$

giving the matrix

$$M_2 := \mathrm{diag}\{1,\omega^2,\omega,\omega^2,\omega,\omega^2,\omega,\omega^2,\omega\},$$

where $\omega = e^{2\pi i/3}$.

The MacWilliams transformation:

$$\text{idempotent } \iota = 1$$

$$x_v \mapsto \frac{1}{\sqrt{9}} \sum_{w \in \mathbb{F}_9} e^{2\pi i \frac{1}{3} \operatorname{Tr}(\alpha v \bar{w})} x_w$$

giving the matrix

$$M_3 := \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \bar{\omega} & \omega & 1 & \omega & \omega & \bar{\omega} & 1 & \bar{\omega} \\ 1 & \omega & \omega & \bar{\omega} & 1 & \bar{\omega} & \bar{\omega} & \omega & 1 \\ 1 & 1 & \bar{\omega} & \bar{\omega} & \omega & 1 & \omega & \omega & \bar{\omega} \\ 1 & \omega & 1 & \omega & \omega & \bar{\omega} & 1 & \bar{\omega} & \bar{\omega} \\ 1 & \omega & \bar{\omega} & 1 & \bar{\omega} & \bar{\omega} & \omega & 1 & \omega \\ 1 & \bar{\omega} & \bar{\omega} & \omega & 1 & \omega & \omega & \bar{\omega} & 1 \\ 1 & 1 & \omega & \omega & \bar{\omega} & 1 & \bar{\omega} & \bar{\omega} & \omega \\ 1 & \bar{\omega} & 1 & \bar{\omega} & \bar{\omega} & \omega & 1 & \omega & \omega \end{bmatrix}.$$

Then the Clifford-Weil group is

$$C(\rho) = \langle M_1, M_2, M_3 \rangle,$$

a nine-dimensional group of order 192.

The Molien series for this group is

$$\frac{1 + 3t^4 + 24t^6 + 74t^8 + 156t^{10} + \cdots + 989t^{20} + \cdots + t^{38}}{(1-t^2)^2(1-t^4)^2(1-t^6)^3(1-t^8)(1-t^{12})}$$

Remarks

- The coefficients of the Taylor series expansion form sequence A092354 in [19].
- There are at least 6912 secondary invariants (set $t = 1$ in numerator).
- This complexity is typical of most groups — see Huffman and Sloane [10].
- This ring is spanned by cwe's of codes, by our main theorem.
- It would be hopeless to try to find a corresponding set of codes!
- To get the Hamming weight enumerator theorem, we cannot simply identify $x_1 = x_\alpha = \cdots = x_{\alpha^7} = x$ (this fails because M_2 does not act nicely, and if we ignore the generator M_2 the resulting ring has Molien series $1/(1-t^2)^2$, which is wrong) — this is what we call an "illegal symmetrization".
- The correct way to obtain the Hamming weight enumerator theorem is first to divide up the elements of $\mathbb{F}_9$ into three orbits $\{0\}$, $\{1, \alpha^2, \alpha^4, \alpha^6\}$ (which square to 1) and

$\{\alpha, \alpha^3, \alpha^5, \alpha^7\}$ (which square to -1). The generators now collapse nicely, to

$$\tilde{M}_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \tilde{M}_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{bmatrix}, \quad \tilde{M}_3 = \frac{1}{3}\begin{bmatrix} 1 & 1 & 1 \\ 4 & 1 & -2 \\ 4 & -2 & 1 \end{bmatrix},$$

generating a group of order 48 with Molien series

$$\frac{1}{(1-t^2)(1-t^4)(1-t^5)}.$$

Codes that correspond to the terms in the denominator can be taken to be:

$$[1\ \alpha], \quad \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & \alpha & 2\alpha & 0 & 1 & 2 \end{bmatrix}.$$

If their Hamming weight enumerators are denoted by f_2, f_4, f_6 respectively, then the ring of Hamming weight enumerators is

$$\mathbb{C}[f_2, f_4] \oplus f_6\mathbb{C}[f_2, f_4].$$

This is not the ring of invariants of any finite group of 2×2 matrices.

21. Higher-genus weight enumerators

To handle higher-genus or multiple weight enumerators we use tensor products, as mentioned in §12, and Morita theory. The form ring for genus-m weight enumerators is

$$\rho \otimes R^m = \mathrm{Mat}_m(\rho) := (\mathrm{Mat}_m(R),\ V \otimes R^m,\ \beta^{(m)},\ \Phi_m).$$

Theorem. (1) *The space of homogeneous invariants of degree N of the corresponding Clifford-Weil group $C_m(\rho)$ is spanned by the genus-m weight enumerators $cwe_m(C)$, where C ranges over a set of permutation representatives of codes of Type ρ and length N.* (2) *If every length N code of Type ρ is generated by at most m elements, then these genus-m weight enumerators are a basis for the space of homogeneous invariants of degree N.*

Corollary. *The Molien series of $C_m(\rho)$, $Mol_{C_m(\rho)}(t)$, converges monotonically as m increases:*

$$\lim_{m\to\infty} Mol_{C_m(\rho)}(t) = \sum_{N=0}^{\infty} \nu_N t^N,$$

where ν_N is the number of permutation-equivalence classes of codes of Type ρ and length N.

Example: Binary self-dual (or Type 2_I) codes. The order of $\mathcal{C}_m(\rho)$ and the Molien series for genera 1 to 4 are as follows:

Genus 1: $|\mathcal{C}_1| = 16$ (Gleason [8]):

$$\frac{1}{(1-t^2)(1-t^8)}$$

Genus 2: $|\mathcal{C}_2| = 2304$ (see [12]):

$$\frac{1+t^{18}}{(1-t^2)(1-t^8)(1-t^{12})(1-t^{24})}$$

Genus 3: $|\mathcal{C}_3| = 5160960$ (see [14]):

$$\frac{\text{degree } 154}{(1-t^2)(1-t^{12})\cdots(1-t^{40})}$$

— there are at least 720 secondary invariants

Genus 4: $|\mathcal{C}_4| = 178362777600$ (see Oura [16])

$$\frac{\text{degree } 504}{(1-t^2)\cdots(1-t^{120})}$$

— there are over 10^{10} secondary invariants

The convergence of the Molien series mentioned in the above Corollary can be seen in the following table, which gives the initial terms of the expansion of the Molien series for genera 1–5:

$m \setminus N$	0	2	4	6	8	10	12	14	16	$\cdots$
1	1	1	1	1	2	2	2	2	3	
2	1	1	1	1	2	2	3*	3	4	
3	1	1	1	1	2	2	3	4	6	
4	1	1	1	1	2	2	3	4	7	
5	1	1	1	1	2	2	3	4	7	

*This entry 3 corresponds to the fact that the biweight enumerators of the three codes i_2^6, $h_8 i_2^2$ and d_{12}^+ are linearly independent.

Incidentally, the 8-dimensional group $\mathcal{C}_3(\rho)$ of order 5160960 is the group whose magical emergence from the computer — leading to the astonishing coincidence mentioned in §8 — indirectly led to our writing the book.

22. There is no time to mention:

- Our new construction for the Barnes-Wall lattices as lattices over $\mathbb{Z}[\sqrt{2}]$ whose automorphism groups are the Clifford-Weil groups $\mathcal{C}_m(2_I)$ (Chapter 6).

- The theorem that the automorphism group of the genus-m weight enumerator of any Type $2_{\rm I}$ code that is not generated by codewords of weight 2 is the Clifford-Weil group $\mathcal{C}_m(2_{\rm I})$. There is an analogous assertion for doubly-even or Type $2_{\rm II}$ codes. (Chapter 6)
- The generalizations to maximal self-orthogonal codes (Chapter 10).
- Quantum codes (Chapter 13).
- The extensive tables giving the classification of all codes and of extremal codes of modest lengths (Chapters 11, 12).
- Applications to spherical designs (Chapters 5,6).
- "Closed codes": What definition of duality guarantees that $C^{\perp\perp} = C$?
- Our attempts at generalizing the theory to handle self-dual *lattices.*

23. Finally, the new list of Types

Chapter 2 of the book ends with a list of the principal Types and the sections in which they are discussed. To entice the reader, but without giving any further details, here is that list:

2_{I} (The old Type I)	$4^{\mathbb{Z}}$ (Codes over $\mathbb{Z}/4\mathbb{Z}$)
2_{II} (The old Type II)	$4_{\mathrm{II}}^{\mathbb{Z}}$
2_S	$m^{\mathbb{Z}}$
$2^{\mathrm{lin}}, 2_1^{\mathrm{lin}}$	$m_1^{\mathbb{Z}}$
$2_{1'}^{\mathrm{lin}}, 2_{1,1'}^{\mathrm{lin}}$	$m_{\mathrm{II}}^{\mathbb{Z}}$
4^E (The old Type IV)	$m_{\mathrm{II},1}^{\mathbb{Z}}$
4_{II}^E	$m_S^{\mathbb{Z}}$
q^E(even)	$GR(p^e, f)^E$
q_{II}^E	$GR(p^e, f)_1^E$
3 (The old Type III)	$GR(p^e, f)_{p^s}^E$
q^E(odd)	$GR(2^e, f)_{2^s}^E$
q_1^E(odd)	$GR(2^e, f)_{\mathrm{II}}^E$
4^H (The old Type IV)	$GF(2^e, f)_{\mathrm{II},2^s}^E$
q^H	$GR(p^e, f)^H$
q_1^H	$GR(p^e, f)_{p^s}^H$
4^{H+}	$GR(p^e, f)^{H+}$
4_{II}^{H+}	$GR(p^e, f)_{p^s}^{H+}$
q^{H+}(even)	$\mathbb{Z}_p$ (Codes over the p-adic integers)
q_1^{H+}(even)	$\mathbb{F}_{q^2} + \mathbb{F}_{q^2} u$
q_{II}^{H+}(even)	
$q_{\mathrm{II},1}^{H+}$(even)	
q^{H+}(odd)	
q_1^{H+}(odd)	
$q^{\mathrm{lin}}, q_1^{\mathrm{lin}}$	
$q_{1'}^{\mathrm{lin}}, q_{1,1'}^{\mathrm{lin}}$	

References

[1] E. F. Assmus, Jr., H. F. Mattson, Jr. and R. J. Turyn, Research to develop the algebraic theory of codes, *Report AFCRL-67-0365*, Air Force Cambridge Res. Labs., Bedford, MA, June 1967.

[2] A. Bak, *K-Theory of Forms*, Princeton Univ. Press, 1981.

[3] E. Bannai, S. T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices and invariant rings, *IEEE Trans. Information Theory* **45** (1999), 1194–1205.

[4] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over GF(4), *IEEE Trans. Information Theory* **44** (1998), 1369–1387 [arXiv: quant-ph/9608006].

[5] J. H. Conway and N. J. A. Sloane, Self-dual codes over the integers modulo 4, *J. Combinat. Theory* **A62** (1993), 30–45.

[6] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer, 1998, 3rd. ed., 1998.

[7] G. D. Forney, Jr., N. J. A. Sloane and M. D. Trott, The Nordstrom-Robinson code is the binary image of the octacode, in *Coding and Quantization: DIMACS/IEEE Workshop October 19–21, 1992*, ed. R. Calderbank, G. D. Forney, Jr. and and N. Moayeri, Amer. Math. Soc. (1993), pp. 19–26.

[8] A. M. Gleason, Weight polynomials of self-dual codes and the MacWilliams identities, in *Actes, Congrés International de Mathématiques (Nice, 1970)*, Gauthiers-Villars, Paris, 1971, Vol. 3, pp. 211–215.

[9] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Information Theory* **40** (1994), 301–319 [arXiv: math.CO/0207208].

[10] W. C. Huffman and N. J. A. Sloane, Most primitive groups have messy invariants, *Advances in Math.* **32** (1979), 118–127.

[11] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell Syst. Tech. J.* **42** (1963), 79–94.

[12] F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane, Generalizations of Gleason's theorem on weight enumerators of self-dual codes, *IEEE Trans. Information Theory* **18** (1972), 794–805.

[13] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977; 11th impression 2003.

[14] G. Nebe, E. M. Rains and N. J. A. Sloane, The invariants of the Clifford groups, *Designs, Codes and Cryptography* **24** (2001), 99–121 [arXiv: math.CO/0001038].

[15] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Springer-Verlag, 2006.

[16] M. Oura, The dimension formula for the ring of code polynomials in genus 4, *Osaka J. Math.* **34** (1997), 53–72.

[17] E. M. Rains and N. J. A. Sloane, Self-dual codes, Chapter 3 of ed. V. S. Pless and W. C. Huffman, Elsevier, Amsterdam, 1998, pp. 177–294 [arXiv: math.CO/0208001].

[18] N. J. A. Sloane, Self-dual codes and lattices, in *Relations Between Combinatorics and Other Parts of Mathematics*, Proc. Symp. Pure Math., Vol 34, Amer. Math. Soc., Providence, RI, 1979, pp. 273–308.

[19] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/~njas/sequences/.

[20] A. Weil, Sur certaines groupes d'opérateurs unitaires, *Acta Math.* **111** (1964), 143–211: *Oeuvres Scientifiques* III, Springer, 1979, pp. 1–69.

$(1-u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$

Maria Carmen V. Amarra
Fidel R. Nemenzo
Department of Mathematics
University of the Philippines, Diliman

Abstract

We extend the results of [5] to the commutative ring $R = \mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, where p is prime, $k \in \mathbb{N}$ and $u^2 = 0$. In particular, we prove that the Gray image of a linear $(1-u)$-cyclic code over R of length n is a distance-invariant quasicyclic code of index p^{k-1} and length $p^k n$ over $\mathbb{F}_{p^k}$. We also prove that if $(n,p) = 1$, then every code of length $p^k n$ over $\mathbb{F}_{p^k}$ which is the Gray image of a linear cyclic code of length n over R is permutation-equivalent to a quasicyclic code of index p^{k-1}.

1 Preliminaries

Let p be prime and $k \in \mathbb{N}$. Let R be the ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$, where $u^2 = 0$ and $\mathbb{F}_{p^k} = GF(p^k)$. Then R is a finite chain ring with maximal ideal uR and residue field $\mathbb{F}_{p^k}$. Let $\mathcal{C}$ be a code of length n over R, and $P(\mathcal{C})$ be its polynomial representation, i.e.,

$$P(\mathcal{C}) = \left\{ \sum_{i=0}^{n-1} r_i x^i \mid (r_0, \ldots, r_{n-1}) \in \mathcal{C} \right\}.$$

Let σ and ν be maps from R^n to R^n given by

$$\sigma(r_0, r_1, \ldots, r_{n-1}) = (r_{n-1}, r_0, \ldots, r_{n-2})$$

and

$$\nu(r_0, r_1, \ldots, r_{n-1}) = ((1-u)r_{n-1}, r_0, \ldots, r_{n-2}).$$

Then $\mathcal{C}$ is said to be *cyclic* if $\sigma(\mathcal{C}) = \mathcal{C}$, and $(1-u)$-*cyclic* if $\nu(\mathcal{C}) = \mathcal{C}$. It is known that:

Theorem 1.1 *A code $\mathcal{C}$ of length n over R is cyclic if and only if $P(\mathcal{C})$ is an ideal of $R[x]/\langle x^n - 1\rangle$.*

Theorem 1.2 *A code C of length n over R is $(1-u)$-cyclic if and only if $P(C)$ is an ideal of $R[x]/\langle x^n-1\rangle$.*

Let $\mathbf{a} \in \mathbb{F}_{p^k}^{p^k n}$, with $\mathbf{a} = (a_0, \ldots, a_{p^k n-1}) = \left(a^{(0)} \mid \ldots \mid a^{(p^{k-1}-1)}\right)$, $a^{(i)} \in \mathbb{F}_{p^k}^{pn}$ for all $i = 0, \ldots, p^{k-1}-1$. Let $\sigma^{\otimes p^{k-1}}$ be the map from $\mathbb{F}_{p^k}^{p^k n}$ to $\mathbb{F}_{p^k}^{p^k n}$ given by

$$\sigma^{\otimes p^{k-1}}(\mathbf{a}) = \left(\tilde{\sigma}\left(a^{(0)}\right) \mid \ldots \mid \tilde{\sigma}\left(a^{(p^{k-1}-1)}\right)\right),$$

where $\tilde{\sigma}$ is the usual cyclic shift $(c_0, c_1, \ldots c_{pn-1}) \mapsto (c_{pn-1}, c_0, \ldots, c_{pn-2})$ on $\mathbb{F}_{p^k}^{pn}$. A code $\tilde{C}$ of length $p^k n$ over $\mathbb{F}_{p^k}$ is said to be *quasicyclic of index* p^{k-1} if $\sigma^{\otimes p^{k-1}}(\tilde{C}) = \tilde{C}$.

In [3], a homogeneous weight on arbitrary finite chain rings is defined; we give it here for the case of the ring $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$. The homogeneous weight $w_{\text{hom}}(\mathbf{r})$ of $\mathbf{r} = (r_0, \ldots, r_{n-1})$ is given by

$$w_{\text{hom}}(\mathbf{r}) = \sum_{i=0}^{n-1} w_{\text{hom}}(r_i),$$

where, for all $i = 0, 1, \ldots, n-1$,

$$w_{\text{hom}}(r_i) = \begin{cases} p^k - 1 & \text{if } r \in R \backslash Ru \\ p^k & \text{if } r \in Ru \backslash \{0\} \\ 0 & \text{otherwise} \end{cases}$$

The homogeneous distance $d_{\text{hom}}(\mathbf{x}, \mathbf{y})$ between any distinct $\mathbf{x}, \mathbf{y} \in R^n$ is defined to be $w_{\text{hom}}(\mathbf{x} - \mathbf{y})$.

2 Gray images of $(1-u)$-cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$

Let α be a fixed primitive kth root of unity in some extension of $\mathbb{F}_p$. Let $\alpha_\epsilon \in \mathbb{F}_{p^k}$ be given by

$$\alpha_\epsilon := \gamma_{0,\epsilon} + \gamma_{1,\epsilon}\,\alpha + \ldots + \gamma_{(k-1),\epsilon}\,\alpha^{k-1},$$

where $\epsilon \in \{0, 1, \ldots, p^k - 1\}$ with p-adic representation

$$\gamma_{0,\epsilon} + \gamma_{1,\epsilon}\,p + \ldots + \gamma_{(k-1),\epsilon}\,p^{k-1}.$$

The *Gray map* Φ on R, which is a special case of the Gray map defined in [3], is given by

$$\begin{aligned} \Phi \;:\; R^n &\longrightarrow \mathbb{F}_{p^k}^{p^k n} \\ x + yu &\longmapsto (y, \alpha_1 x \oplus y, \ldots, \alpha_{p^k-1} x \oplus y), \end{aligned}$$

where $\oplus$ is componentwise addition in $\mathbb{F}_{p^k}$. It is shown in [3] that Φ is an isometry from R^n under the homogeneous distance to $\mathbb{F}_{p^k}^{p^k n}$ under the Hamming distance.

From the above definitions, we have

Proposition 2.1

$$\Phi \circ \nu = \sigma^{\otimes p^{k-1}} \circ \Phi$$

As a consequence, we obtain

Theorem 2.2 *A code $\mathcal{C}$ of length n over R is $(1-u)$-cyclic if and only if $\Phi(\mathcal{C})$ is quasicyclic of index p^{k-1} over $\mathbb{F}_{p^k}$.*

3 Gray images of cyclic codes over $\mathbb{F}_{p^k} + u\mathbb{F}_{p^k}$

Supose that $(n,p) = 1$. Following [2], let $n' \in \{0, 1, \ldots, p-1\}$ such that $nn' \equiv 1 \bmod p$ and $\beta = 1 + n'u$. The map μ defined by

$$\begin{aligned} \mu \; : \; R[x]/(x^n - 1) &\longrightarrow R[x]/\left(x^n - (1-u)\right) \\ r(x) &\longmapsto r(\beta x) \end{aligned}$$

is a ring isomorphism. Hence I is an ideal of $R[x]/\langle x^n - 1\rangle$ if and only if $\mu(I)$ is an ideal of $R[x]/\langle x^n - (1-u)\rangle$. Let $\overline{\mu}$ be the map

$$\begin{aligned} \overline{\mu} \; : \; R^n &\longrightarrow R^n \\ r &\longmapsto \left(r_0, \beta r_1, \beta^2 r_2, \ldots, \beta^{n-1} r_{n-1}\right). \end{aligned}$$

Then

Proposition 3.1 *The set $\mathcal{C} \subseteq R^n$ is a linear cyclic code if and only if $\overline{\mu}(\mathcal{C})$ is a linear $(1-u)$-cyclic code.*

Moreover

Proposition 3.2 *There is a permutation $\pi^{\otimes p^{k-1}}$ on $\mathbb{F}_{p^k}^{p^k n}$ such that*

$$\Phi \circ \overline{\mu} = \pi^{\otimes p^{k-1}} \circ \Phi.$$

Here the permutation $\pi^{\otimes p^{k-1}}$, which is an extension of the Nechaev permutation introduced in [4], is defined as follows:

For $\mathbf{c} = \left(c^{(0)} | \ldots | c^{\left(p^{k-1}-1\right)}\right) \in \mathbb{F}_{p^k}^{p^k n}$,

$$\pi^{\otimes p^{k-1}}(\mathbf{c}) := \left(\pi\left(c^{(0)}\right) \mid \ldots \mid \pi\left(c^{\left(p^{k-1}-1\right)}\right)\right),$$

where

$$\pi(\mathbf{a}) = \left(a_{\tau(0)}, \ldots, a_{\tau(pn-1)}\right)$$

for $\mathbf{a} = (a_0, \ldots, a_{pn-1}) \in \mathbb{F}_{p^k}^{pn}$, where

$$\tau(\gamma n + j) = (\gamma + jn')_p n + j,$$

$0 \leq \gamma \leq p-1$, $0 \leq j \leq n-1$, and $(\gamma + jn')_p$ is the unique number in $\{0, 1, \ldots, p-1\}$ with $(\gamma + jn')_p \equiv (\gamma + jn') \bmod p$.

Thus we obtain

Corollary 3.3 *If $\tilde{C}$ is the Gray image of a linear cyclic code of length n over R, then $\tilde{C}$ is equivalent to a quasicyclic code of index p^{k-1} and length $p^k n$ over $\mathbb{F}_{p^k}$.*

References

[1] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and Patrick Solé, The $\mathbb{Z}_4$-Linearity of Kerdock, Preparata, Goethals and Related Codes, *IEEE Trans. Inform. Theory* 40 (1999), 301-309.

[2] S. Ling and J. Blackford, $\mathbb{Z}_{p^{k+1}}$-linear codes, *IEEE Trans. Inform. Theory* 48 (2002), 2592-2605.

[3] M. Greferath and S. E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. *IEEE Trans. Inform. Theory* 45 (1999), 2522-2524.

[4] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* 45 (1999), 2527-2532.

[5] J. F. Qian, L. N. Zhang and S. X. Zhu, $(1+u)$-constacyclic and cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *Appl. Math. Lett.* 19 (2006), 820-823.

Codes that attain minimum distance in all possible directions

Gyula O.H. Katona[1], Attila Sali[1], Klaus-Dieter Schewe[2]

[1] Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences
Budapest, P.O.B.127, H-1364 Hungary
ohkatona@renyi.hu, sali@renyi.hu
[2] Massey University, Information Science Research Centre
& Department of Information Systems
Private Bag 11 222, Palmerston North, New Zealand
k.d.schewe@massey.ac.nz

Abstract. Let $\mathcal{K}$ be the system of minimal keys in a relational database schema R with respect some collection of functional dependencies Σ. Then $\mathcal{K}$ is a Sperner system, or antichain, that is for $K_1 \neq K_2 \in \mathcal{K}$ $K_1 \not\subset K_2$ holds. Armstrong (and independently Demetrovics) proved that for each nonempty Sperner system of attribute sets there exists an instance of the scheme such that if the complete set of functional dependencies are considered that hold in that instance, then exactly the given Sperner system is the collection of minimal key sets. However, the constructions use unbounded domains for each attribute.
In the study of key systems in higher-order datamodels with counter attributes the case of bounded domains come up naturally. In the present paper we investigate the following problem. Assume that a relational scheme of n attributes is given, where each attribute's domain is of q elements. Furthermore, suppose that the minimal key sets are exactly all the k-element subsets of the set of attributes. Let $f(q,k)$ be the maximum n such that an Armstrong instance with the above properties exists. Considering the records or rows of the Armstrong instance as codewords of length n, the key property means that no two codewords can agree on k or more coordinates, that is the minimum distance is at least $n-k+1$. The minimal key property tells that for any $k-1$-set of coordinates there are two codewords that agree exactly there. We give lower and upper bounds for $f(q,k)$. In particular, we show that $f(q,k)$ is bounded by linear functions of k and q, and determine the exact values for special k and q.

1 Introduction

Arguably the most important database constraint is the collection of functional dependencies a relational schema satisfies, in particular the key dependencies. If R denotes the set of attributes, then $K \subseteq R$ is a *key*, if the functional dependency $K \rightarrow R$ holds. In what follows we use the terminology of the book [1].

It is interesting from the point of view of schema design that given a collection Σ of functional dependencies, what other dependencies hold in a database

instance that satisfies Σ. A way of solving this problem is the construction of *Armstrong instance* for Σ, that is a database that satisfies a functional dependency $X \to Y$ if and only if $\Sigma \models X \to Y$. Silva and Melkanoff [16] developed a design aid that for a collection of functional and multivalued dependencies as input prsents an Armstrong instance for that set. The existence of Armstrong instance for a set of functional dependencies was proved by Armstrong [2] and Demetrovics [3]. Later Fagin [10] gave a necessary and sufficient condition for general dependencies.

Further investigations concentrated on the minimal size of an Armstrong instance, since it is a good measure of the complexity of the collection of dependencies or system of minimal keys in question [4–9, 11].

All papers cited above assumed that the *domain* of each attribute is unbounded, countably infinite. However, in the study of *Higher Order Datamodel* [12–15] the question of bounded domains arises naturally. In fact, if a minimal key system contains only *counter attributes*, then the possible number of tuples in an Armstrong instance is bounded from above. Another reason to consider bounded domains comes from real life databases. In many cases the domain of an attribute is a well defined finite set, for example in car rental, the class of cars can take values from the set {subcompact, compact, mid-size, full-size, SUV, sportscar, van}. Same kind finiteness may occur in case of job assignments, schedules, etc.

It is natural to ask what can be said about Armstrong instances if attribute A_i has a domain of size ℓ_i. The main question investigated in this paper was introduced in [15]. Let $\mathcal{K}_n^k$ denote the collection of all k-subsets of an n-element attribute set R.

Definition 1. *Let $q > 1$ and $k > 1$ be given natural numbers. Let $f(q,k)$ be the maximum such n that there exists an Armstrong instance for $\mathcal{K}_n^k$ being the system of minmal keys.*

It is clear that for a meaningful Armstrong instance we need at least two distinct symbols, so $q > 1$ is necesary. On the other hand the minimal Armstrong instance for $\mathcal{K}_n^1$ uses only two symbols for arbitrary n [6], hence $f(q,k)$ is well defined only for $k > 1$. We give lower bounds for $f(q,k)$ in Section 2, while upper bounds are presented in Section 3. In particular, it is shown in Section 3 that Definition 1 is meaningful. finally, in Section 4 further research directions and problems are discussed.

2 Lower bounds

For lower bounds we need constructions. It is helpful to view an Armstrong instance for $\mathcal{K}_n^k$ as minimal key system using q symbols as a q-ary code of length n, where codewords are the tuples, or rows of the instance. Since all k-element attribute sets are keys, any two codewords could agree in at most $k-1$ positions, that is the code has minimum distance at least $n-k+1$. On the other hand, no $k-1$-element attribute set is a key, so for any $k-1$ positions there must

exist two codewords that agree (exactly) there, that is the minimum distance is *attained in all directions.*

Our construction is greedy. That is pick a pair of codewords for a given $k-1$ subset of positions such that they agree exactly at that $k-1$ positions. Then rule out the balls of radii $n-k$ around the two codewords. If enough codewords are left, then we can pick a pair for the next $k-1$ subset of positions, etc. In order to complete the plan above we need the following lemma.

Lemma 1. *Let Q be the set of q^n q-ary codewords of length n, furthermore let K be a $k-1$-subset of coordinate positions. Then Q can be partitioned into q^{n-1} classes of size q each, that any two codewords of the same class agree exactly on the positions of K.*

Proof. Use induction on n. The first interesting case is $n = k$ is trivial, since fixing the $k-1$ coordinate positions there is one position left, and a partition class contains the q codewords with the given fixed value on the positions in K. Now assume that the partition exists for codewords of length n, and consider a class of q codewords. Each one of them has to be extended by one coordinate that takes values $1, 2, \ldots, q$. We want to do so that q new classes are formed of the codewords of length $n+1$. That requires that in each new class the "extension coordinates" are all distinct. This could best represented by a *bipartite graph* $G(A, B, E)$, where A is the set of q codewords to be extended and $B = \{1, 2, \ldots, q\}$ and E consists of all possible edges between A and B. Now, one good extension is a *complete matching* in this bipartite graph. It is an easy exercise that $G(A, B, E)$, that is a complete bipartite graph, can be partitioned into q complete matchings. This partition into matchings gives the q new partiton classes of codewords of length $n+1$. □

Lemma 1 tells us that as long as we have more codewrds than the number of partition classes, i.e., q^{n-1} available, then for any given $k-1$ subset of the coordinates we can find two codewords that agree in exatly those positions. This implies that the greedy construction works if

$$\left[\binom{n}{k-1} - 1\right]\left[2\sum_{i=0}^{n-k}\binom{n}{i}(q-1)^i - B\right] < q^n - q^{n-1} \tag{1}$$

where B is the intersection of the two balls of radii $n-k$ around two codewords of distance $n-k+1$.

$$B = \sum_{\substack{a+b\geq k \\ a+b'\geq k \\ b+b'\leq n-k+1}} \binom{k-1}{a}(q-1)^{k-1-a}\binom{n-k+1}{b}\binom{n-k+1-b}{b'}(q-2)^{n-k+1-b-b'} \tag{2}$$

The expression for B in (2) is quiet complicated, so to obtain a simple lower bound for n we may use that if

$$\left[\binom{n}{k-1} - 1\right]\left[2\sum_{i=0}^{n-k}\binom{n}{i}(q-1)^i\right] < q^n - q^{n-1} \tag{3}$$

holds, then (1) holds, as well.

Theorem 1. *There exists k_0 such that if $k > k_0$, and $n \leq \frac{1}{2}k \log q$, then there exists an Armstrong instance for $\mathcal{K}_n^k$ as minimal key system using q symbols.*

The proof of Theorem 1 using (3) is in the Appendix. The bound in Theorem 1 is rather trivial for $q = 2$. For that case we can get some better estimates. (3) can be written as

$$\left[\binom{n}{k-1} - 1\right]\left[2\sum_{i=0}^{n-k}\binom{n}{i}\right] < 2^{n-1}. \tag{4}$$

Now, if $n < 2k$, then the left hand side of (4) can be bounded by $2\binom{n}{k}^2(n-k)$. That is if

$$2\binom{n}{k}^2(n-k) \leq 2^{n-1}, \tag{5}$$

then (4) holds. The binomial coefficient in (5) can be estimated using the *entropy function* $H(x) = -x\log x - (1-x)\log(1-x)$ as $\log\binom{n}{k} = nH(\frac{k}{n}) + O(\log n)$. Taking the logarithm of both sides of (5) and substituting the previous estimate for $\log\binom{n}{k}$

$$2nH(\frac{k}{n}) + O(\log n) \leq n - 1 \tag{6}$$

is obtained. Putting $n = ck$, (6) holds for $k > k_0$ if $H(\frac{1}{c}) < \frac{1}{2}$, which is certainly true for $c = 1.12$. Thus, we have proved

Theorem 2. *There exists k_0 and $c > 1$ constants, that for $k > k_0$, and $n = \lfloor ck \rfloor$, there exists an Armstrong instance for the minimal key system $\mathcal{K}_n^k$ using only two symbols.*

The main point of Theorem 2 is that constant c is *strictly* larger than one. To conclude this section we show a lower bound that turns out to be sharp.

Proposition 1.

$$f(q,2) \geq \binom{q+1}{2} \tag{7}$$

Proof. The lower bound is given by construction. Relation R has $q+1$ rows and *binom*$q+12$ columns (attributes). Since q symbols are allowed in each column we have eactly one pair of equal symbols and we do so that these pairs are all distinct. Since each column has a pair of rows that agree there, no single attribute forms a key. However, no two rows agree in two columns, so any pair of attributes form a key, that is R is an Armstrong instance for $\mathcal{K}^2_{\binom{q+1}{2}}$, hence $f(q,2) \geq \binom{q+1}{2}$. □

3 Upper bounds

Here we assume that an Armstrong instance for the minimal key system $\mathcal{K}_n^k$ exists containing m tuples. Also, we may assume without loss of generality that $q < m$.

Lemma 2. *If s is a sequence of length m containing elements from the set $\{1, 2, \ldots, q\}$, then the number of equal pairs in s is at least*

$$\frac{m}{2}\left(\frac{m}{q} - 1\right) \tag{8}$$

Proof. Extend the concept of the binomial coefficient $\binom{m}{2}$ for real values x as $\binom{x}{2} = \frac{x(x-1)}{2}$. Since $f(x) = \frac{x(x-1)}{2}$ is a convex function (from below), the Jensen inequality

$$f\left(\frac{\sum_{i=1}^{q} x_i}{q}\right) \leq \frac{\sum_{i=1}^{q} f(x_i)}{q} \tag{9}$$

implies

$$\binom{\frac{\sum_{i=1}^{q} x_i}{q}}{2} \leq \frac{\sum_{i=1}^{q} \binom{x_i}{2}}{q}. \tag{10}$$

Let m_i denote the number of digits i in s. Then the number of equal pairs is

$$\sum_{i=1}^{q} \binom{m_i}{2}. \tag{11}$$

On the other hand, $\sum_{i=1}^{q} m_i = m$. Substituting these into (10), we obtain

$$\binom{\frac{m}{q}}{2} \leq \frac{\sum_{i=1}^{q} \binom{m_i}{2}}{q} \tag{12}$$

and the desired (8). □

The following slight improvement of Lemma 2 will also be used.

Lemma 3. *If s is a sequence of lenght m containing elements from the set $\{1, 2, \ldots, q\}$, where $q < m$, then the number of equal pairs in s is at least*

$$q\binom{h}{2} + rh, \tag{13}$$

where $m = qh + r$ with $(0 \leq h < q)$.

Its proof is in the appendix.

Theorem 3. *Let M be an Armstrong instance for the minimal key system $\mathcal{K}_n^k$ where $k > 2$, that consists of m tuples. Then*

$$n \leq q(k-1)\left(1 + \frac{q-1}{\sqrt{\frac{2(qk-q-k+2)^{k-1}}{(k-1)!}} - q}\right) \tag{14}$$

holds.

Proof. The number of pairs of equal entries in each column is at least (8). Altogether:

$$n\frac{m}{2}\left(\frac{m}{q}-1\right). \tag{15}$$

In one pair of rows at most $k-1$ of them can appear, otherwise the two rows had k equal entries in contradiction with the assumption that every k-element subset of columns is a key. Hence we have the inequality

$$n\frac{m}{2}\left(\frac{m}{q}-1\right) \leq (k-1)\binom{m}{2}. \tag{16}$$

For any choice of $k-1$ columns there must exist two (distinct) rows such that they have equal entries in these columns. It is easy to see that this pair of rows must be different for different choices of $k-1$ columns, otherwise the union of these two $k-1$-element sets would be an at least k element non-key, in contradiction with our assumptions. Hence the following inequality is obtained:

$$\binom{n}{k-1} \leq \binom{m}{2}. \tag{17}$$

(16) can be easily rewritten as an upper bound on n for fixed m:

$$n \leq \frac{(k-1)\binom{m}{2}}{\frac{m}{2}\left(\frac{m}{q}-1\right)} = q(k-1)\left(1+\frac{q-1}{m-q}\right) = a_{q,k}(m). \tag{18}$$

(17) gives another, but implicit upper bound, a somewhat weaker explicit bound will be formed. (17) implies

$$\frac{(n-k+2)^{k-1}}{(k-1)!} \leq \frac{m^2}{2}, \tag{19}$$

hence we obtain

$$n \leq \left(\frac{(k-1)!}{2}m^2\right)^{\frac{1}{k-1}} + k - 2 = b_{q,k}(m). \tag{20}$$

Notice that $a_{q,k}(m)$ is a decreasing, while $b_{q,k}(m)$ is an increasing function of m. Therefore, if α is the solution of the equation

$$a_{q,k}(m) = b_{q,k}(m) \tag{21}$$

in m then $a_{q,k}(\alpha) = b_{q,k}(\alpha)$ is a universal (indpendent of m) upper bound for n. Such a solution must exist if $a_{q,k}(q+1) \geq b_{q,k}(q+1)$ holds (at the smallest value where $a_{q,k}(m)$ is defined). That is, we have to show

$$q(k-1)\left(1+\frac{q-1}{q+1-q}\right) \geq \left(\frac{(k-1)!}{2}(q+1)^2\right)^{\frac{1}{k-1}} + k - 2, \tag{22}$$

or equivalently

$$q^2(k-1) \geq \left(\frac{(k-1)!}{2}(q+1)^2\right)^{\frac{1}{k-1}} + k - 2. \tag{23}$$

Inequality (23) reduces to following in case of $q = 2$

$$4(k-1) \geq \left(\frac{(k-1)!}{2}9\right)^{\frac{1}{k-1}} + k - 2 \tag{24}$$

Using the inequality between geometric and arithmetic means (24) follows from

$$3k - 2 \geq \left(\frac{9}{2}\right)^{\frac{1}{k-1}} \frac{k}{2} \tag{25}$$

that holds trivially for $k > 2$. Considering the differnce of the left and right hand sides of (23) for fixed k as a function of q one can realize that it is a monotone increasing function by observing that the derivative with respect of q is non-negative.

Since it is difficult to find the explicit solution of equation (21), we solve the easier equation

$$q(k-1) = \left(\frac{(k-1)!}{2}m^2\right)^{\frac{1}{k-1}} + k - 2, \tag{26}$$

replacing $a_{q,k}$ by a smaller function (what is actually a constant). Its solution β satisfies $\beta \leq \alpha$ by the monotonity of $b_{q,k}(m)$. We have

$$\beta = \sqrt{\frac{2(qk-q-k+2)^{k-1}}{(k-1)!}}. \tag{27}$$

Let us see that $q + 1 \leq \beta$ if $2 < k$. what we need is

$$(k-1)!(q+1)^2 \leq 2(qk-q-k+2)^{k-1} \tag{28}$$

or equivalently,

$$\left(\frac{(k-1)!}{2}\right)^{\frac{1}{k-1}} (q+1)^{\frac{2}{k-1}} \leq qk - q - k + 2. \tag{29}$$

(29) holds with equality for $q = 2$ and $k = 3$. Keeping $q = 2$, easy induction on k shows that (29) holds for $q = 2$, $k \geq 3$. Now fixing k, we find that the differnce of the right hand side and the left hand side of (29) is a monotone increasing function of q, since its derivative with respect to q

$$k - 1 - \frac{2}{k-1}(q+1)^{\frac{2}{k-1}-1} \tag{30}$$

is nonnegative.

Then $a_{q,k}(\beta)$ is defined and is a universal upper bound on n and this is actually the bound formulated in the theorem. □

In the case $k = 2$ our theorem is not valid. However, the method works. We only have to use somewhat better estimates rather than $a_{q,2}(m)$ and $b_{q,2}(m)$. These improved bounds lead to a better estimate for $k = 3$, too. If Lemma 2 is replaced by Lemma 3 then

$$n \leq a^*_{q,k}(m) = \frac{(k-1)\binom{m}{2}}{q\binom{h}{2} + rh} \tag{31}$$

is obtained instead of (18). To be able to use this bound we have to see that it is a decreasing function of m.

Lemma 4.

$$a^*_{q,k}(m) = \frac{(k-1)\binom{m}{2}}{q\binom{h}{2} + rh} \tag{32}$$

is decreasing in m for $q < m$.

(Its proof is in the Appendix.)

In the cases $k = 2, 3$ formula (17) has a nice form, there is no need to rewrite in the weaker form of (20). When $k = 2$, it is simply

$$n \leq b^*_{q,2}(m) = \binom{m}{2}. \tag{33}$$

The solution of

$$a^*_{q,2}(m) = b^*_{q,2}(m) \tag{34}$$

that is of

$$\frac{\binom{m}{2}}{q\binom{h}{2} + rh} = \binom{m}{2} \tag{35}$$

is simply $q + 1$ as it can be seen by substitution since here $h = 0, r = 1$. The universal bound on n is $\binom{q+1}{2}$, which is sharp by Proposition 1

If $k = 3$ then (17) reduces to $n \leq m$, that is $b^*_{q,3}(m) = m$. By (31) we have to solve the equation

$$a^*_{q,3}(m) = \frac{2\binom{m}{2}}{q\binom{h}{2} + rh} = m = b^*_{q,3}(m). \tag{36}$$

The solution is $3q-1$. Indeed, $h = 2, r = q-1$ implies $q\binom{h}{2}+rh = q\binom{2}{2}+(q-1)2 = 3q - 2$. The left hand side of (36) is really $3q - 1$.

Theorem 4. *If k is 2 then $n \leq \binom{q+1}{2}$, if $k = 3$ then $n \leq 3q - 1$.*

One can feel that if k and/or q are large then the remainder term in Theorem 3 is less than 1, that is the main term is the upper bound. Indeed, we can prove the following theorem.

Theorem 5. *If $5 \leq k$ and $2 \leq q$ then the upper bound in Theorem 3 can be improved to*

$$n \leq q(k-1) \tag{37}$$

with the following exceptions: $(k, q) = (5, 2), (5, 3), (5, 4), (5, 5), (6, 2)$.

4 Appendix

Proof (Theorem 1). Write $n = \alpha k$. The the binomial coefficients in (3) can be bounded from above by $\frac{2^{\alpha k}}{\sqrt{\alpha k}}$, while the powers of $(q-1)$ can be replaced with the highest one to obtain

$$\frac{2^{\alpha k}}{\sqrt{\alpha k}}\left(2[(\alpha-1)k]\frac{2^{\alpha k}}{\sqrt{\alpha k}}(q-1)^{(\alpha-1)k}\right) < q^{(\alpha k-1)}(q-1) \tag{38}$$

that implies (3). (38) in turn is implied by

$$2^{2\alpha k+1} < q^k \tag{39}$$

that holds for $k > k_0$ if $\alpha < \frac{1}{2}\log q$ □

Proof (of Lemma 3). Let m_i be the number of digits i in s. Suppose that $m_1 < m_2 - 1$. Replace m_1 by $m_1' = m_1 + 1$ and m_2 by $m_2' = m_1 - 1$. This change does not change the sum of ms. The sum of the equal entries before the change is

$$\sum_{i=1}^{q}\binom{m_i}{2} \tag{40}$$

and it is

$$\binom{m_1+1}{2} + \binom{m_2-1}{2} + \sum_{i=3}^{q}\binom{m_i}{2} \tag{41}$$

after the changes. It is easy to see that the number of equal entries was decreased by $m_2 - 1 - m_1 > 0$. The same can be said in every case when the difference of any two m_i's is at least 2. Otherwise, when the differences are 0 and 1 then r of them is $h+1$, on the other hand $q-r$ of them is h. The number of equal digits is

$$r\binom{h+1}{2} + (q-r)\binom{h}{2} = q\binom{h}{2} + rh. \tag{42}$$

□

Proof (of Lemma 4). Here $m = qh + r, 0 \le r < q$ inplies $m = qh + r + 1$, we have to verify

$$\frac{(k-1)\binom{m}{2}}{q\binom{h}{2} + rh} \ge \frac{(k-1)\binom{m+1}{2}}{q\binom{h}{2} + (r+1)h} \tag{43}$$

when $r + 1 < q$. This leads to the following inequality after carrying out the obvious cancellations.

$$(m - r - 1)h \ge 2q\binom{h}{2} = qh^2 - qh \tag{44}$$

or equivalently: $qh - 1 \ge qh - q$ what is trivially true.

The above proof does not perfectly work when $r = q - 1$ since then $m + 1$ is obtained in the form $qh + q$. However, as it is easy to see, the formula for the minimum number of equal digits works in this case, too:

$$q\binom{h}{2} + qh = q\binom{h+1}{2}. \tag{45}$$

□

Proof (of Theorem 5). We have to prove

$$\frac{q(q-1)(k-1)}{\sqrt{\frac{2(qk-q-k+2)^{k-1}}{(k-1)!}} - q} < 1 \tag{46}$$

for the desired cases. More precisely it is sufficient to prove $\leq$ since the denumerator is a result of a non-sharp estimation. The inequality is equivalent to

$$q(q-1)(k-1) + q = q(qk-q-k+2) \leq \sqrt{\frac{2(qk-q-k+2)^{k-1}}{(k-1)!}}, \tag{47}$$

that is

$$q^2(k-1)! \leq 2(qk-q-k+2)^{k-3}. \tag{48}$$

Replacing $qk - q - k + 2$ by $(q-1)(k-1)$ a somewhat stronger inequality is obtained:

$$q^2(k-1)! \leq 2(q-1)^{k-3}(k-1)^{k-3}. \tag{49}$$

Suppose that $5 \leq k$. Then $(k-1)! \leq 2(k-1)^{k-3}$ (induction), (49) reduces to

$$q^2 \leq (q-1)^{k-3}. \tag{50}$$

Our strategy is to prove the statement of (50) or (49). If they are not true for some values then we go back to the original (48).

If $k = 6$ then (50) becomes $q2 \leq (q-1)3$. Analizing this equation one can see that it holds for $4 \leq q$. Since the right hand side of (50) is increasing in k, our statement is proved for the the values $6 \leq k, 4 \leq q$.

Consider now the case $k = 5$. Then (49) has the form $q^2 24 \leq 2(q-1)24^2$. Solving the quadratic equation we obtain that it holds for $8 \leq q$. The smaller values of q, namely $q = 4, 5, 6, 7$ can be checked for (48). It holds for $q = 6, 7$ but not for $q = 4, 5$.

The remaining cases are $q = 2, 3$ for all k. Fix first $q = 2$ and find the smallest k satisfying (49) for this case:

$$4(k-1)! \leq 2(k-1)^{k-3}. \tag{51}$$

It holds with $k = 8$, therefore (49) is true for $q = 2$, $9 \leq k$ as it can be seen by easy induction. The smaller cases of k can be checked in the original (48). It holds for $k = 7$ and does not hold for $k = 5, 6$.

Let now $q = 3$. (49) reduces to $9(k-1)! \leq 2^{k-2}(k-1)^{k-3}$. It holds with $k = 6$, the larger values of k can be obtained by induction. The case $(q = 3,)k = 5$ is not true in (48). □

The estimates we used to show that the gredy construction works are rather coarse, nevertheless we believe that the order of the magnitude of the upper bound is not the right one. The problem has a coding theory flavour, since Armstrong databases are in fact codes with given large minmum distance, combined with design theoretic ideas as the minimum distance must be attained in all directions.

References

1. ABITEBOUL, S., HULL, R., AND VIANU, V. *Foundations of Databases.* Addison-Wesley, 1995.
2. ARMSTRONG, W. W. Dependency structures of database relationships. *Information Processing* (1974), 580–583.
3. DEMETROVICS, J. On the equivalence of candidate keys with Sperner systems. *Acta Cybernetica 4* (1979), 247–252.
4. DEMETROVICS, J., FÜREDI, Z., AND KATONA, G. O. H. Minimum matrix reperesentation of closure operetions. *Discrete Applied Mathematics 11* (1985), 115–128.
5. DEMETROVICS, J., AND GYEPESI, G. A note on minimum matrix reperesentation of closure operetions. *Combinatorica 3* (1983), 177–180.
6. DEMETROVICS, J., AND KATONA, G. Extremal combinatorial problems in relational data base. In *Fundamentals of Computing Theory (FCT 1981)*, no. 117 in LNCS. Springer-Verlag, Berlin, 1981, pp. 110–119.
7. DEMETROVICS, J., KATONA, G., AND SALI, A. The characterization of branching dependencies. *Discrete Applied Mathematics 40* (1992), 139–153.
8. DEMETROVICS, J., KATONA, G., AND SALI, A. Design type problems motivated by database theory. *Journal of Statistical Planning and Inference 72* (1998), 149–164.
9. DEMETROVICS, J., AND KATONA, G. O. H. A survey of some combinatorial results concerning functional dependencies in databaseperfect error-correcting databases. *Annals of Mathematics and Artificial Intelligence 7* (1993), 63–82.
10. FAGIN, R. Horn clauses and database dependencies. *Journal of the Association for Computing Machinery 29*, 4 (1982), 952–985.
11. FÜREDI, Z. Perfect error-correcting databases. *Discrete Applied Mathematics 28* (1990), 171–176.
12. HARTMANN, S., LINK, S., AND SCHEWE, K.-D. Weak functional dependencies in higher-order datamodels. In *Foundations of Information and Knowledge Systems* (2004), D. Seipel and J. M. Turull Torres, Eds., vol. 2942 of *Springer LNCS*, Springer Verlag.
13. SALI, A. Minimal keys in higher-order datamodels. In *Foundations of Information and Knowledge Systems* (2004), D. Seipel and J. M. Turull Torres, Eds., vol. 2942 of *Springer LNCS*, Springer Verlag.
14. SALI, A., AND SCHEWE, K.-D. Counter-free keys and functional dependencies in higher-order datamodels. *Fundamenta Informaticae 70* (2006), 277–301.
15. SALI, A., AND SCHEWE, K.-D. Keys and armstrong databases in trees with restructuring. *preprint* (2006).
16. SILVA, A., AND MELKANOFF, M. A method for helping discover the dependencies of a relation. In *Advances in Data Base Theory* (1981), H. Gallaire, J. Minker, and J.-M. Nicolas, Eds., vol. 1, Plenum Publishing, New York.

Hilbert Series and Free Distance Bounds for Quaternary Convolutional Codes

Romar B. dela Cruz
Jose Maria P. Balmaceda
Department of Mathematics
University of the Philippines, Diliman

Virgilio P. Sison
Institute of Mathematical Sciences and Physics
University of the Philippines Los Baños

Abstract

A quaternary convolutional code is a $\mathbb{Z}_4(D)$-submodule of $\mathbb{Z}_4(D)^n$, where $\mathbb{Z}_4(D)$ is the ring of rational functions in D over $\mathbb{Z}_4$. Let C be a quaternary convolutional code with a basic polynomial generator matrix $G(D)$ satisfying the predictable degree property. We study the polynomial subcodes of C and define the Hilbert series for C. The Hilbert series will then be used to compute the rank of the polynomial subcodes. An upper bound for the Lee free distance of C is obtained in terms of the maximum possible minimum distances of the polynomial subcodes. We also investigate the residue and torsion binary convolutional codes associated with C. We also show how to construct a quaternary convolutional code from two binary convolutional codes in such a way that the two binary codes will be the residue and torsion codes of the quaternary code. Another upper bound for the Lee free distance of C is given.

1 Preliminaries

We begin by discussing some concepts about convolutional codes over rings. For a detailed discussion, the reader is referred to [2], [3] and [6]. Let R be a commutative ring with identity and D an indeterminate. We denote by $R((D))$ the ring of formal Laurent series in D over the ring R. The ring of rational functions in D, a subring of $R((D))$, is denoted by $R(D)$. A rate-k/n ***convolutional code*** C over R is an $R(D)$-submodule of $R(D)^n$ given by

$$C = \{v(D) \in R(D)^n \mid v(D) = u(D)G(D), u(D) \in R(D)^k\}$$

where $G(D)$ is a $k \times n$ matrix over $R(D)$ whose rows are free over $R(D)$. The matrix $G(D)$ is a ***generator matrix*** for C if all its entries are realizable functions. If $R = \mathbb{Z}_4$ then C is called a ***quaternary*** convolutional code.

Let $v(D) = [v_1(D), v_2(D), \ldots, v_n(D)]$ be a codeword of C. The weight of $v_i(D)$ is the sum of the weights (Hamming, Lee, etc.) of the Laurent series coefficients of $v_i(D)$. The weight of $v(D)$ is the sum of the weights of its components. The *free distance* of C, $d_{\text{free}}(C)$, is the minimum among the weights of the nonzero codewords. The free distance is a measure of the ability of the code to correct errors. For a fixed k and n, the higher the free distance, the better is the ability to correct

errors. In most cases, it is difficult to compute the free distance and so free distance bounds are important.

If the entries of $G(D)$ are polynomials then $G(D)$ is called a *polynomial generator matrix* (PGM) for C. We now present some properties of polynomial generator matrices. The matrix $G(D)$ is *basic* if it is a PGM and it has a polynomial right inverse. If $v(D) = [v_1(D), v_2(D), \ldots, v_n(D)]$ is a polynomial codeword then we define the *degree* of $v(D)$ as

$$\deg v(D) = \max_i \{\deg v_i(D)\}.$$

Suppose $G(D)$ is a PGM and

$$G(D) = (g_{ij}(D)), \ 1 \leq i \leq k, \ 1 \leq j \leq n.$$

Denote the ith row of $G(D)$ by $g_i(D) = [g_{i1}(D), \ldots, g_{in}(D)]$. The ith-*constraint length*, denoted by ν_i, is the maximum among the degrees of the components of $g_i(D)$. The *overall constraint length* ν of $G(D)$ is given by

$$\nu = \sum_{i=1}^{k} \nu_i.$$

The *memory* μ of $G(D)$ is the maximum among the constraint lengths. Let $u(D)$ be a polynomial input such that $u(D) = [u_1(D), u_2(D), \ldots, u_k(D)]$ and suppose $v(D) = u(D)G(D)$. Then

$$\deg v(D) \leq \max_i \{\deg u_i(D)g_i(D)\} = \max_i \{\deg u_i(D) + \nu_i\}.$$

For each polynomial input $u(D)$, if $\deg v(D) = \max_i \{\deg u_i(D) + \nu_i\}$ then $G(D)$ is said to satisfy the *predictable degree property* (PDP).

In this paper, we present the main results of our study. The details will appear in a forthcoming article.

2 Hilbert series

In this section, we are following the approach by McEliece and Stanley [4] who introduced the Hilbert series for a rate-k/n binary convolutional code. They used the series to obtain a useful family of upper bounds on the Hamming free distance of the code.

Throughout this section, we assume that C is a rate-k/n quaternary convolutional code with generator matrix $G(D)$. A polynomial codeword is an element of C whose components are all polynomials. Define C_L to be the set of polynomial codewords in C of degree less than or equal to L where $L \geq 0$. Then C_L is a module over $\mathbb{Z}_4$ and it can be viewed as a linear block code of length $n(L+1)$.

Theorem 2.1. *If $G(D)$ is basic and satisfies the PDP then C_L is a finitely generated free module over $\mathbb{Z}_4$ and the length of C_L as a $\mathbb{Z}_4$-module, denoted by $l_{\mathbb{Z}_4}(C_L)$, is finite. In addition, $l_{\mathbb{Z}_4}(C_L) = 2\rho_L$ where ρ_L is the rank of C_L.*

Consider the power series $\sum_{L \geq 0} l_{\mathbb{Z}_4}(C_L) t^L$. By Theorem 2.1, we have

$$\sum_{L \geq 0} l_{\mathbb{Z}_4}(C_L) t^L = \sum_{L \geq 0} 2\rho_L t^L.$$

Theorem 2.2. *Let C be a quaternary convolutional code and let ρ_L be the rank of its polynomial subcode C_L. Let $G(D)$ be a PGM with constraint lengths $\nu_1, \nu_2, \ldots, \nu_k$. If $G(D)$ is basic and satisfies the PDP then*

$$\sum_{L\geq 0} 2\rho_L t^L = \frac{2(t^{\nu_1} + t^{\nu_2} + \ldots + t^{\nu_k})}{(1-t)^2}.$$

Since the power series is in $\mathbb{Z}((t))$, then

$$\sum_{L\geq 0} 2\rho_L t^L = 2\sum_{L\geq 0} \rho_L t^L.$$

We will call the series $\sum_{L\geq 0} \rho_L t^L$ the *Hilbert series for C*.

The following corollary shows that the rank ρ_L can be computed from the constraint lengths $\nu_1, \nu_2, \ldots, \nu_k$.

Corollary 2.3.

$$\rho_L = \sum_{i=1}^{k} \max\,(L + 1 - \nu_i, 0).$$

If C_L is a free module over $\mathbb{Z}_4$ then it is a quaternary linear block code of length $n(L+1)$ with parameters $k_1 = \rho_L$ and $k_2 = 0$. Since each C_L is a polynomial subcode of C then the Lee free distance of C, $d^L_{\text{free}}(C)$, cannot exceed the minimum Lee distance of C_L, for $L \geq 0$. We then have the following theorem:

Theorem 2.4. *Let C be a quaternary convolutional code and let ρ_L be the rank of its polynomial subcode C_L. Let $G(D)$ be a PGM with constraint lengths $\nu_1, \nu_2, \ldots, \nu_k$. If $G(D)$ is basic and satisfies the PDP then*

$$d^L_{free}(C) \leq \min_{L\geq 0}\{\Delta[n(L+1), \rho_L]\},$$

where $\Delta[n(L+1), \rho_L]$ denotes the maximum possible minimum Lee distance of a rate-$\rho_L/n(L+1)$ linear block code over $\mathbb{Z}_4$ of type $\{\rho_L, 0\}$.

Example. Consider the rate-1/2 quaternary convolutional code, constructed by R. Johannesson and E. Wittenmark [6], generated by the basic encoder

$$G(D) = \begin{bmatrix} 3 + 3D + D^2 & 2 + D + 2D^2 \end{bmatrix}.$$

There is only one constraint length which is 2. $G(D)$ satisfies the PDP since the indicator matrix

$$[G(D)]_h = [1 \quad 2]$$

is of full rank. It follows from Theorem 2.2 that the Hilbert series for this code is

$$\sum_{L\geq 0} \rho_L t^L = \frac{t^2}{(1-t)^2} = t^2 + 2t^3 + 3t^4 + \ldots$$

So, $\rho_0 = 0$ and $\rho_L = L - 1$ for all $L \geq 1$.

The Lee free distance of this code satisfies

$$d^L_{\text{free}}(C) \leq \min_{L\geq 1}\{\Delta[2(L+1), L-1]\}.$$

For $L = 2$, we have $d^L_{\text{free}}(C) \leq \Delta[6, 1] = 8$. In fact, the Lee free distance of this code is 8.

3 Residue and Torsion codes

Given a quaternary convolutional code $\mathcal{C}$, there are two binary codes associated with it. To obtain these codes, we first consider the mappings from $\mathbb{Z}_4$ to $\mathbb{Z}_2$ denoted by α and β:

$x \in \mathbb{Z}_4$	$\alpha(x)$	$\beta(x)$
0	0	0
1	1	0
2	0	1
3	1	1

Note that α is a ring homomorphism. We extend these mappings to $\mathbb{Z}_4(D)$ as follows: if $a(D) \in \mathbb{Z}_4(D)$ and $a(D) = \sum a_i D^i$ then define $\alpha[a(D)] = \sum \alpha(a_i)D^i$ and $\beta[a(D)] = \sum \beta(a_i)D^i$. Now for any element of $\mathbb{Z}_4(D)^n$, we apply α and β componentwise.

The *residue code* of $\mathcal{C}$ is defined as

$$\mathrm{Res}(\mathcal{C}) = \{\alpha[v(D)] \mid v(D) \in \mathcal{C}\}$$

and the *torsion code* of $\mathcal{C}$ is given by

$$\mathrm{Tor}(\mathcal{C}) = \{\beta[v(D)] \mid v(D) \in \mathcal{C}, \alpha[v(D)] = 0\}.$$

Theorem 3.1. $\mathrm{Res}(\mathcal{C})$ *and* $\mathrm{Tor}(\mathcal{C})$ *are binary convolutional codes, that is, subspaces of* $\mathbb{Z}_2(D)^n$ *over* $\mathbb{Z}_2(D)$.

Let $G(D)$ be a generator matrix of a quaternary convolutional code $\mathcal{C}$. Then we have the following generator matrices for $\mathrm{Res}(\mathcal{C})$ and $\mathrm{Tor}(\mathcal{C})$:

Theorem 3.2. *A generator matrix for* $\mathrm{Res}(\mathcal{C})$ *is* $G(D)$ mod 2 *and a generator matrix for* $\mathrm{Tor}(\mathcal{C})$ *is* $\beta[2G(D)]$.

If $\mathcal{B}$ is a linear block code over $\mathbb{Z}_4$, $\mathrm{Res}(\mathcal{B}) = \mathrm{Tor}(\mathcal{B})$ if and only if $\mathcal{B}$ is a free module (see [5]). Using the assumption that $\mathcal{C}$ is a free module, we have shown that a generator matrix for $\mathrm{Res}(\mathcal{C})$ is $G(D)$ mod 2 and a generator matrix for $\mathrm{Tor}(\mathcal{C})$ is $\beta[2G(D)]$. Now, $\beta[2G(D)] = G(D)$ mod 2, and therefore we have the following theorem:

Theorem 3.3. *If* $\mathcal{C}$ *is a rate-*k/n *quaternary convolutional code then*

$$\mathrm{Res}(\mathcal{C}) = \mathrm{Tor}(\mathcal{C}).$$

4 Construction of a quaternary convolutional code

Let $f(D), g(D) \in \mathbb{Z}_4(D)$ such that $f(D) = \sum f_i D^i$ and $g(D) = \sum g_i D^i$. Define

$$f(D) * g(D) := \sum (f_i \cdot g_i) D^i,$$

where $\cdot$ is multiplication modulo 4. Thus, $*$ is coefficient-wise multiplication. If $v(D), w(D) \in \mathbb{Z}_4(D)^n$ where $v(D) = [v_1(D), v_2(D), \ldots, v_n(D)]$ and $w(D) = [w_1(D), w_2(D), \ldots, w_n(D)]$, then define $v(D) * w(D) = [v_1(D) * w_1(D), \ldots, v_n(D) * w_n(D)]$.

If $b(D) \in \mathbb{Z}_2(D)^n$ and $b(D) = \sum b_i D^i$ then we define $2b(D) = \sum 2b_i D^i$. We also denote by $+$ the addition in $\mathbb{Z}_4$.

Theorem 4.1. *Let C' and C'' be binary convolutional codes, that is, C' and C'' are subspaces of $\mathbb{Z}_2(D)^n$, with $C' \subseteq C''$. Then*

$$C = C' + 2C'' = \{a(D) + 2b(D) \mid a(D) \in C', b(D) \in C''\}$$

is a quaternary convolutional code if and only if

$$a_1(D), a_2(D) \in C' \Rightarrow a_1(D) * a_2(D) \in C''.$$

In this case, $\mathrm{Res}(C) = C'$ *and* $\mathrm{Tor}(C) = C''$.

This construction is analogous to the construction in [1] for the case of linear block codes. Since we have $\mathrm{Res}(C) = \mathrm{Tor}(C)$ then $C = C' + 2C' = C'' + 2C''$. In the theorem, it is clear that C' and $2C''$ are subcodes of C. Thus, we have

Corollary 4.2.

$$d^L_{free}(C) \leq \min\{d^H_{free}(C'), 2d^H_{free}(C'')\}.$$

Acknowledgments. We thank the University of the Philippines Diliman for a Research Dissemination Grant and the Kyushu Graduate School of Mathematics COE Program for support to participate in the conference.

References

[1] A. Bonnecaze, P. Solé and A. Calderbank, "Quaternary quadratic residue codes and unimodular lattices," *IEEE Trans. Inform. Theory*, vol. 41, pp. 366-367, 1995.

[2] F. Fagnani and S. Zampieri, "System-theoretic properties of convolutional codes over rings," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2256-2274, 2001.

[3] R. Johannesson, Z. Wan and E. Wittenmark, "Some structural properties of convolutional codes over rings," *IEEE Trans. Inform. Theory*, vol. 44, pp. 839-845, 1998.

[4] R. McEliece, "The Algebraic Theory of Convolutional Codes," in *Handbook of Coding Theory*, W.C. Huffman and V. Pless, Eds., North Holland, 1998, vol. 1, ch. 12.

[5] Z. Wan, *Quaternary Codes*, World Scientific, 1997.

[6] E. Wittenmark, "An Encounter with Convolutional Codes over Rings," *Ph.D. dissertation*, Lund University, 1998.

A family of Higmanian association schemes on 40 points: A computer algebra approach

Mikhail Klin[1]
Matan Ziv-Av[1]

Dedicated to Eiichi Bannai on the occasion of his 60th birthday

1 Introduction

In this paper we describe a family of imprimitive rank 5 association schemes on 40 points which are called Higmanian (they belong to class II association schemes with 4 classes according to the classification introduced by D. G. Higman in [9]). The first example of such schemes was given by Y. Chang and T. Huang in [2] based on a previous construction by A. and M. Deza [3].

A scheme $\mathfrak{M}$ considered in [2] is presented in evident form via basis matrices which are described in a block form, intersection numbers and eigenmatrices are computed, but there is no information about the automorphism group $Aut(\mathfrak{M})$. It is also shown that one of the basis graphs of $\mathfrak{M}$ is the point graph of a generalized quadrangle $Q(4,3)$. In the course of computer algebra experimentation using total graph coherent configuration with two fibers, we constructed such configuration starting from the triangular graph $T(5)$ and described all mergings of it which provide association schemes. One of the resulting fusion schemes was isomorphic to the scheme $\mathfrak{M}$ (this was first established with the aid of a computer, though later on we obtained a computer-free proof). We also found the group $G = Aut(\mathfrak{M})$ to be a certain transitive permutation group of degree 40 and order 1920. Playing with this group we have managed to establish a few nice properties of $\mathfrak{M}$ and related structures. In particular, we discovered a new partial linear space on 40 points and 40 lines of size 4 which in a sense is a "geometric generator" of all scheme $\mathfrak{M}$.

Understanding of these properties of $\mathfrak{M}$ allowed us to elaborate a nice, simple though very efficient, algorithmic approach to the constructive enumeration of all association schemes sharing with $\mathfrak{M}$ the same tensor of structure constants (algebraically isomorphic in our terminology). This approach is based on a computer inspection of the catalogue of all 28 strongly regular graphs with the parameters $(40, 12, 2, 4)$. This catalogue belongs to ES and is available from his home page.

Finally we proved that there exists precisely 15 association schemes, algebraically isomorphic to $\mathfrak{M}$. Only one of them, namely $\mathfrak{M}$ is Schurian while all the remaining schemes have intransitive automorphism group. Four of the discovered schemes, including $\mathfrak{M}$, are geometric in the sense which was explained above.

[1]Department of Mathematics, Ben-Gurion University of the Negev, 84105 Beer Sheva, Israel

Our results are based on use of a few computer algebra packages, namely COCO [6], GAP [17], GRAPE [18], and nauty [15], although we finally managed to provide computer-free proofs for the most important (and beautiful in our eyes) results.

2 Preliminaries

Association schemes

A *coherent algebra* is a matrix algebra which is closed with respect to SH (elementwise) multiplication and transposition, and contains the matrices I and J. The rank of a coherent algebra is its dimension. A *coherent configuration* is a relational reformulation of coherent algebra. That is, a coherent configuration can be defined as a set of relations such that their adjacency matrices form a basis of a coherent algebra. We refer to [5], [8], [13] for more information about coherent configurations (algebras) and association schemes. An *association scheme* is a coherent configuration for which all basis relations are regular.

Generalized quadrangles of order 3

A generalized quadrangle is a partial geometry $PG(s,t,1)$, i.e., an incidence structure for which every block has $s+1$ points, every point lies on $t+1$ blocks, two blocks intersect in at most one point, and for every block b and every point P not in b, there is exactly one block c such that P is in c, and b intersects c.

A generalized quadrangle of order 3 is $PG(3,3,1)$, denoted by $GQ(3)$. A $GQ(3)$ has 40 points and 40 blocks.

In [16] it is shown that up to isomorphism there are two generalized quadrangles of order 3, $W(3)$ and $Q(4,3)$.

3 Imprimitive association schemes of low rank

The smallest rank for which non-trivial imprimitive association schemes exist is equal to 4. The paper [20] provides a nice survey of various classes of such schemes.

Rank 5 imprimitive schemes have been investigated with less attention. A general program was outlined by Higman in [9].

Let E be an equivalence relation in an association scheme $\mathfrak{M}$ (closed subset in Zieschang's terms, parabolic in terms of Higman). Then $rank(E)$ is the rank of the association scheme induced by $\mathfrak{M}$ on one (any) of the equivalence classes of E, while $corank(E)$ is the rank of the quotient association scheme $\mathfrak{M}/E$.

It is easy to see that $rank(E) + corank(E) \leq rank(\mathfrak{M}) + 1$, with equality if and only if $\mathfrak{M}$ is the wreath product of E and $\mathfrak{M}/E$.

This makes it reasonable to consider the following classes (due to Higman) of rank 5 imprimitive symmetric association schemes with a parabolic E which are not decomposable into a wreath product:

class of $\mathfrak{M}$	I	II	III
rank of E	3	2	2
corank of E	2	3	2

In [9] examples are given, which show that classes I and II may have non-trivial intersection, while class III is distinct from classes I and II. Class I was investigated extensively by Higman.

Let E have n equivalence classes of size v, and suppose that one of two associate classes of $\mathfrak{M}/E$ is a strongly regular graph with the parameters (n, k, l, λ, μ). Then the whole scheme $\mathfrak{M}$ has nv points and valencies $k_0 = 1$, $k_1 = v - 1$, $k_2 = kS$, $k_3 = (v - S)k$, $k_4 = lv$ for a suitable parameter S. Corresponding intersection matrices and character tables are provided in [9], as well as for a particular case, which corresponds to the intersection of classes I and II. Higman refers to examples of distance regular imprimitive graphs of diameter 4 (see, e.g. [1]), briefly discussing when these graphs also belong to class I.

We are interested in rank 5 schemes which belong properly to class II. Such an example was provided in [2]. It has 40 points and corresponds to the following Higman parameters: $n = 10$, $k = 6$, $l = 3$, $\lambda = 3$, $\mu = 4$ (that is the complement of the Petersen graph), $v = 4$, $S = 2$, thus resulting in four classes with the valencies 3, 12, 12, 12.

In this paper we provide detailed investigation of this example and classify all association schemes which are algebraically isomorphic to it.

4 Starting point: Total configuration of $T(5)$.

Let $\Sigma = (V, E)$ be a graph. The total graph $T(\Sigma)$ is the graph with the vertex set $V \cup E$, two such vertices in $T(\Sigma)$ are adjacent if and only if they are adjacent or incident in Σ (here edges of Σ are incident if they have a joint vertex).

A coherent closure of $T(\Sigma)$ will be called a *total coherent configuration* of Σ.

We are interested in the total coherent configuration $\mathfrak{T}(m)$ of the triangular graph $T(m)$ (recall that $T(m)$ is the line graph $L(K_m)$ of the complete graph K_m). Clearly, $\mathfrak{T}(m)$ is a coherent configuration with 2 fibers on $\frac{m(m-1)^2}{2}$ points.

The first non-trivial case corresponds to $m = 4$. Here (according to COCO) we get a coherent configuration of rank 18 which has a few Schurian mergings of rank 3 and 4. All these mergings are quite predictable.

The first surprises appear in the case $m = 5$. Here we get a coherent configuration of rank 24 with 2 fibers of size 10 and 30.

COCO returns 9 mergings, all Schurian, among them 4 association schemes of rank 5 and one primitive strongly regular graph with the parameters $(40, 12, 2, 4)$ and rank 3 automorphism group of order 51840.

Two of the above association schemes with 4 classes have valencies 1, 3, 12, 12, 12. With the aid of GAP we prove that they are both isomorphic to the Higmanian association scheme from [2].

For these schemes one of the classes of valency 12 provides the above rank 3 graph, which should be the point graph of a generalized quadrangle $GQ(3)$. According to [2], this graph is the polar graph $O_5(3)$, in other words the point graph of $Q(4,3)$.

As was mentioned, the story of our association scheme with 4 classes goes back to the paper [3], in which the ridge graph Γ_5 was defined. (Note that one more description of Γ_5 with correction of some misprints in [3] appears in [4].) This ridge graph has valency 15 and is easily described via the union of one relation of valency 12 with the relation of valency 3 in the Higmanian association scheme.

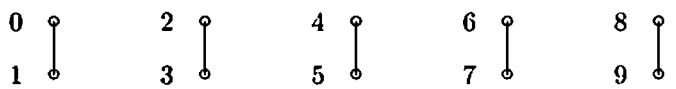
5 The group of order 1920 and its actions

One of the main paradigms in our vision of computer algebra experimentation in algebraic combinatorics may be formulated as follows:

In order to understand properly a combinatorial object O in consideration, describe its automorphism group $G = Aut(O)$ and reveal all actions of G which should be naturally attributed to O. Sometimes it may be very helpful to start from a certain auxiliary structure Δ and to define the action of G on this structure.

In this text we are following the formulated paradigm.

Let us consider graph $\Delta = 5 \circ K_2$ as follows:



The automorphism group $Aut(\Delta)$ is isomorphic to the wreath product $S_5 \wr S_2$ of order $5! \cdot 25 = 3840$. We refer to [5] and [13], where the operation of the wreath product of groups is treated in notation and style consistent with our current presentation.

The group $Aut(\Delta)$ clearly contains odd permutations. This is why the group $G = (S_5 \wr S_2)^{pos}$ which consists of all even permutations from $Aut(\Delta)$ has index 2 in $Aut(\Delta)$. It is, in a sense, our master group in this paper.

For the sake of convenience (especially using COCO) in what follows we will consider G defined with the aid of the following generators:

$$G =< (0,6,4,1,7,5)(8,9), (0,7,1,6)(2,5,8,3,4,9) > .$$

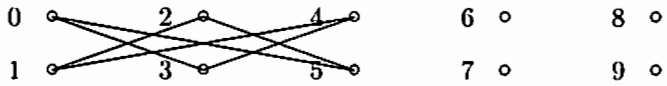
We now wish to describe in terms of Δ the action of G on the points of a new model of $Q(4,3)$ (to be presented in Section 6), as well as on the points of the Higmanian association scheme $\mathfrak{M}$. The fact that G is indeed isomorphic to the group $Aut(\mathfrak{M})$ can be confirmed by GAP. GAP returns also the description of a point stabilizer in this transitive action, namely a group H_1 of order 48 isomorphic to $D_6 \times E_4$, that is the direct product of dihedral group D_6 of order 12 and the elementary abelian group of order 4.

We get the following set of generators for H_1:

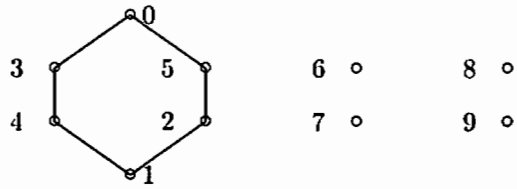
$$H_1 = \left\langle \begin{matrix} (6,7)(8,9), (0,1)(2,3)(4,5)(8,9), \\ (6,8)(7,9), (0,2,4)(1,3,5), (2,4)(3,5) \end{matrix} \right\rangle.$$

In fact, COCO requires to interpret H_1 as the intersection of the group G with the automorphism group of a suitable structure (or string), say $S^{(1)}$, which is defined in terms of auxiliary structure Δ. Then the required set Ω of points of the model for $\mathfrak{M}$ will be obtained via induced action of G on the images of $S^{(1)}$.

Let us take as the role of $S^{(1)}$ the following hexagon:



or, in a more beautiful form:



Clearly our group H_1 stabilizes $S^{(1)}$. On the other hand stabilizer of $S^{(1)}$ in $Aut(\Delta)$ has order $12 \cdot 8 = 96$ and contains odd permutations, for example $(6,7)$. Therefore $Aut(S^{(1)}) \cap G = H_1$. Define $\Omega = {S^{(1)}}^G$ and obtain that $|\Omega| = [G : H_1] = \frac{1920}{48} = 40$. (List of elements of Ω is attached in archive file which may be provided by authors.)

It is easy to see also that the complementary graph $\overline{\Delta} = \overline{5 \circ K_5}$ has $\binom{5}{2}4 = 40$ inscribed subgraphs which are isomorphic to the hexagon $S^{(1)}$. Therefore the required set Ω may also be described purely combinatorially.

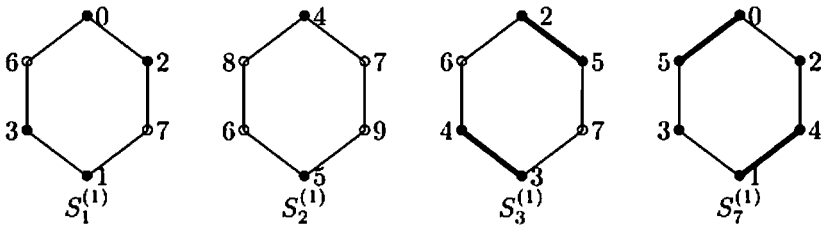
We use COCO and get a Schurian association scheme $(\Omega, 2 - orb(G, \Omega))$. It has rank 5 with classes of valency 12, 12, 12, 3. The group G is its full automorphism group. (Labeling of classes is produced by COCO.) We also get a description of structure constants and of all fusion schemes. GAP confirms that $(\Omega, 2 - orb(G, \Omega))$ is isomorphic to the original Higmanian association scheme. Thus from now we simply write

$$\mathfrak{M} = (\Omega, 2 - orb(G, \Omega)).$$

Let us describe this scheme in a more friendly form providing computer-free proofs of some of its properties, when this seems to be reasonable and productive.

Therefore from now we attribute the label $S_0^{(1)}$ to the above copy of the hexagon (for brevity, four isolated points are omitted), and following COCO, depict a few

other requested copies of structure $S^{(1)}$:



With the aid of these representatives of Ω we define basis relations on $\mathfrak{M}$ as follows: R_0, R_1, R_2, R_3, R_4, where $R_i = (S_0^{(1)}, S_{j_i}^{(1)})^G$, $j_i = 0, 1, 2, 3, 7$ respectively.

We now give more formal description of the relations in which we regard $S_0^{(0)}$ as the reference copy. Then black vertices and bold edges on other hexagons reveal their intersection with the reference copy. Using the methodology of subsequent splitting of relations (see [5]) we may easily distinguish basis relations of $\mathfrak{M}$ via two invariants of pairs of hexagons:

R_i	R_0	R_1	R_2	R_3	R_4
Nr. of joint points	6	4	2	4	6
Nr. of joint edges	6	0	0	2	2

It is immediately clear from the description that $E = R_0 \cup R_4$ is an equivalence relation with 10 classes of size 4 parametrized by 2-element subsets of the edges of Δ. Thus we may define quotient graphs for all the remaining basis graphs Γ_1, Γ_2, Γ_3. Simple combinatorial arguments show that Γ_2/E is isomorphic to the Petersen graph, while Γ_1/E and Γ_3/E are isomorphic to its complement. Γ_1 is the point graph of $Q(4,3)$ (a computer-free proof of this result will be discussed in next section).

From this information it follows that Γ_2 is the wreath product graph.

COCO also returns the following complete list of mergings:

$\mathfrak{M}_1 = (\Omega, \{R_0, R_1 \cup R_3, R_2, R_4\})$,

$\mathfrak{M}_2 = (\Omega, \{R_0, R_1 \cup R_2 \cup R_3, R_4\})$,

$\mathfrak{M}_3 = (\Omega, \{R_0, R_1, R_2 \cup R_3 \cup R_4\})$.

Analyzing this list we detect that the only subalgebra of the adjacency algebra $\mathfrak{A}$ of $\mathfrak{M}$, which contains the basis matrix A_3 is $\mathfrak{A}$ itself. In other words, $\mathfrak{A}$ is generated by A_3. We denote this fact as $\mathfrak{A} =<< A_3 >>$, where $<< A_3 >>$ stands for the coherent closure of A_3 (see references in section 2).

Summing up all detected information we obtain:

Proposition 5.1. *a)* $\mathfrak{M} = (\Omega, 2 - orb(G, \Omega))$ *is an association scheme of rank 5 with valencies 1, 12, 12, 12, 3;*

b) $Aut(\mathfrak{M}) = G$;

c) $E = R_0 \cup R_4$ *is the unique closed subset in* $\mathfrak{M}$;

d) The quotient scheme $\mathfrak{M}/E$ is isomorphic to the rank 3 association scheme $\mathfrak{J}(5,2)$;

e) $\mathfrak{M}_1 \cong \mathfrak{J}(5,2) \wr W(K_4)$ ($W(K_4)$ is coherent closure of K_4);

f) $\mathfrak{M}_3$ is 2-class association scheme corresponding to $Q(4,3)$;

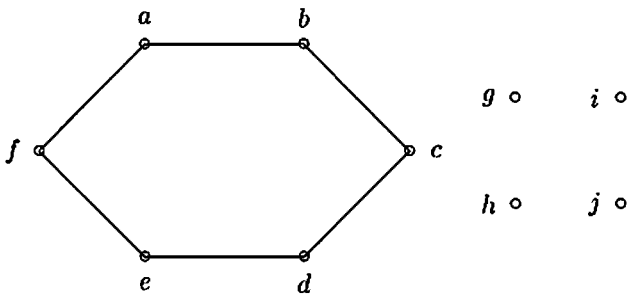
g) $\mathfrak{M}$ belongs to class II of association schemes of rank 5 in notation of Higman;

h) Up to isomorphism, $\mathfrak{M}$ is the scheme which was introduced in [2].

In what follows we will call the basis graph Γ_3 of $\mathfrak{M}$ the *classical Higmanian graph* of valency 12 on 40 points.

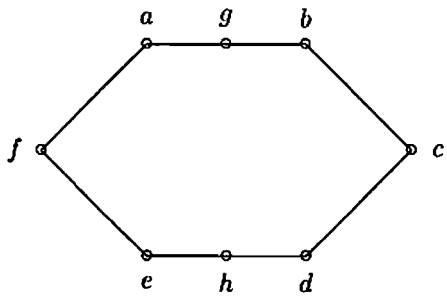
We want to give to this graph a more transparent description, because in a sense description of Γ_3 implies description of the whole scheme $\mathfrak{M}$. For this purpose we will use methodology of so-called reaction graphs, see e.g. [14], [12], [11].

Let $S \in \Omega$ be an arbitrary hexagon, described as follows:

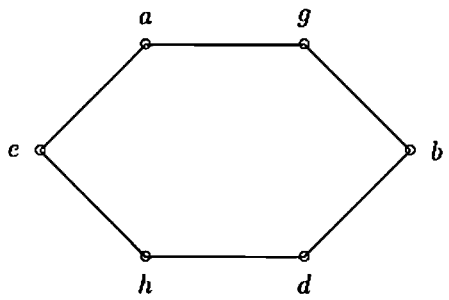


Let us consider the following transformation of S:

- select a pair of opposite edges;
- put on each edge one of the vertices g and h;
- get auxiliary graph S' with 8 vertices;



- get a homeomorphic image S'' of S' contracting vertices f and c.



We will call *reaction on* S an operation of transformation from S to S''. Clearly such reaction can be arranged by $3 \cdot 4 = 12$ different opportunities.

We now define the *reaction graph* Γ with the vertex set Ω'. Here Ω' is the set of all hexagons which may be obtained in a few reaction steps from a prescribed copy S of hexagon, say from $S_0^{(1)}$. Two hexagons from Ω' are joined by an edge if the second is obtained from the first via a reaction as above. The following lemma may be proved with the aid of (slightly routine) hand or computer considerations.

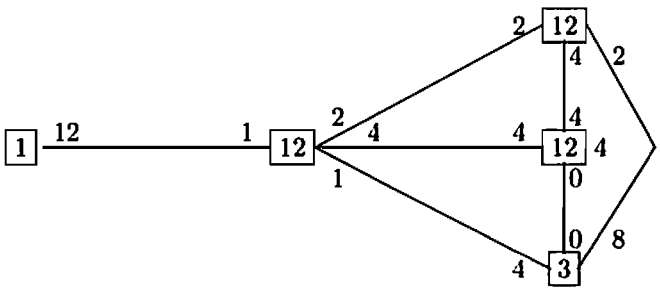
Lemma 5.2. *a) For each* $S \in \Omega$, $S'' \in \Omega$;

b) $\Omega' = \Omega$;

c) Γ *is connected graph of valency 12;*

d) Γ *has diameter 2 and girth 3;*

e) the intersection diagram of Γ *looks as*



f) Γ *is isomorphic to the Higmanian graph* Γ_3 *as above;*

g) $Aut(\Gamma) = G$;

h) Γ *is locally* $2 \circ P_6$, *the disjoint union of two prisms* P_6 *with 6 vertices.*

In what follows we will exploit various consequences of this lemma. In particular, knowledge of the intersection diagram allows us to calculate for $A = A(\Gamma)$ its square A^2 and cube A^3 and to describe the multiplication table in the adjacency algebra $\mathfrak{A}$.

Another approach to the investigation of $\mathfrak{M}$ concerns the consideration of certain incidence structures. For this purpose we need to get more information about certain subgroups of G.

Using GAP we describe all (up to conjugacy) subgroups of G. Among them we reveal 14 conjugacy classes of subgroups of order 48. One of these classes with the representative H_1 was already submitted earlier. This is stabilizer of a point in the transitive action (G, Ω).

Using GAP, we describe all orbits of (G, Ω) on the set $\begin{Bmatrix} \Omega \\ 4 \end{Bmatrix}$ of the 4-element subsets of Ω. It turns out that there are 94 such orbits with lengths from 10 (it corresponds to spread, that is graph Γ_4) to 1920. Two of these orbits are of a special interest, because they have the desired length 40. In other words, the stabilizer of a corresponding 4-subset is a subgroup of order 48 in G.

Let us now describe these selected subgroups. Subgroup H_2 as an abstract group is isomorphic to the group $GL(2,3)$. It can be defined as

$$H_2 = \left\langle \begin{matrix} (2,3)(4,5)(6,7)(8,9), & (4,6,8)(5,7,9), \\ (2,8,3,9)(4,6,5,7), & (0,1)(4,5)(6,9)(7,8) \\ (2,4,3,5)(6,8,7,9) & \end{matrix} \right\rangle.$$

Let us now consider the following structure M:

$$M = \begin{Bmatrix} \{2,4,7\}, & \{2,6,9\}, & \{2,5,8\}, & \{4,6,8\}, \\ \{3,5,6\}, & \{3,7,8\}, & \{3,4,9\}, & \{5,7,9\} \end{Bmatrix}.$$

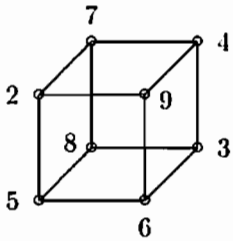
It is easy to see that M is a partial linear space with the point set $\{2,3,4,5,6,7,8,9\}$ (in fact this is a copy of a classical configuration 8_3.) Also we can check that the stabilizer of the set M in the group G coincides with the group H_2.

We also introduce the group H_3, which as an abstract group is isomorphic to $S_4 \times S_2$. Namely

$$H_3 = \left\langle \begin{matrix} (2,3)(4,5)(6,7)(8,9), & (4,6,8)(5,7,9), \\ (2,4)(3,5)(6,8)(7,9), & (6,8)(7,9), \\ (2,6)(3,7)(4,8)(5,9) & \end{matrix} \right\rangle.$$

Again we can easily check that H_3 is the automorphism group of the cube Q_3 below. Moreover this cube is an inscribed subgraph of $\overline{\Delta}$, and the stabilizer of Q_3 in G

coincides exactly with H_3.



Groups H_1, H_2 and H_3 play a significant role in the next section.

6 Two partial linear spaces on 40 points

First, we will discuss our new model for the generalized quadrangle $Q(4,3)$.

Let us consider an incidence structure $\mathfrak{I}_1 = (P, \mathfrak{L}_1)$, where $P = \Omega$ is the set of 40 inscribed hexagons of $\overline{\Delta}$, as it is defined in the previous section. We define $\mathfrak{L}_1 = M^G$ as the orbit of a copy of a partial linear space M under the action of G.

Incidence is defined in the following manner: Each copy $M_i \in \mathfrak{L}_1$ contains 4 pairs of opposite triangles. A hexagon from P is matched to a pair of opposite triangles, if they both have the same 6 vertices, and no shared edges (so in a sense, their union, together with the edges from the original Δ, is the complete graph). For example, a pair of opposite triangles of M: $\{2,4,7\}, \{3,5,6\}$ matches the hexagon $(2,5,7,3,4,6)$. A hexagon from P is incident to M_i if it matches a pair of opposite triangles of M_i.

Proposition 6.1. *a) The incidence structure $\mathfrak{I}_1$ has $v = 40$ points, $b = 40$ lines, each line has $k = 4$ points and each point is on $r = 4$ lines;*

b) $\mathfrak{I}_1$ is a partial linear space;

c) $\mathfrak{I}_1$ is a model of a generalized quadrangle $GQ(3)$;

d) $\mathfrak{I}_1$ is isomorphic to $Q(4,3)$;

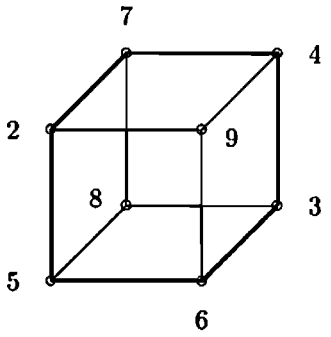
e) $Aut(\mathfrak{I}_1)$ has order 51840.

We refer to [22] for a proof of this proposition.

Now we intend to consider a model for another incidence structure formed by vertices and 4-cliques of Γ_3.

We have the same point set $P = \Omega$. The set of lines $\mathfrak{L}_2$ is the orbit Q_3^G of a selected copy of Q_3 under the action of group G.

Let us look at this copy from a different point of view. Namely, consider the following diagram of the same Q_3:



It shows a hexagon from Ω, $(2,5,6,3,4,7)$ inscribed into this copy of Q_3.

Formal definition: remove a pair of antipodal vertices $\{8,9\}$ from Q_3 and consider the subgraph induced by the remaining vertices. This is a copy of hexagon. Note that this hexagon is the *automorphic subgraph* of Q_3 (see [10]), that is the stabilizer of the hexagon in $Aut(Q_3)$ is equal to the full automorphism group D_6 (of order 12) of the hexagon.

Clearly for a fixed copy of Q_3 the incidence just introduced may be established in precisely 4 different ways, that is removing different antipodal pairs of vertices.

Proposition 6.2. *a)* $v = b = 40$, $k = r = 4$;

b) $\mathfrak{I}_2$ *is a partial linear space;*

c) Γ_3 *is the point graph of* $\mathfrak{I}_2$;

d) $\mathfrak{I}_2$ *is uniquely reconstructed from* Γ_3;

e) $Aut(\Gamma_3) = Aut(\mathfrak{I}_2) = G$;

f) for each line $l \in \mathfrak{L}$ *there are precisely:*

- *12 points* $P \notin l$ *through which there are 0 lines intersecting* l;
- *12 points* $P \notin l$ *through which there are 1 lines intersecting* l;
- *12 points* $P \notin l$ *through which there are 2 lines intersecting* l;

7 Search for all schemes algebraically isomorphic to $\mathfrak{M}$

The problem posed in the title of the section was solved with the aid of a computer.

The starting point was a catalogue of all strongly regular graphs with the parameters $(40,12,2,4)$, which was produced by ES, see [19]. There are precisely

28 non-isomorphic such graphs. Note that significant portion of those graphs was already described by W. H. Haemers in [7]. Haemers was using methodology developed in Moscow by V. L. Arlazarov et al (see [21]).

The computer search was organized as follows:

- Consider each strongly regular graph $\overline{\Gamma}$ from the catalogue ($\overline{\Gamma}$ has valency 27).
- Describe all orbits of cliques of size 8 in $\overline{\Gamma}$.
- Use detected cliques as possible "hyperedges" in a wreath product $W = Petersen\ wr\ K_1$ (this is a regular graph of valency 15). Classify all (up to automorphisms from $Aut(\Gamma)$) possible embeddings of W into $\overline{\Gamma}$.
- Consider difference $\overline{\Gamma}\backslash W$, which is a regular graph of valency 12 (candidate to be an analogue of classical Higmanian graph). Find coherent closure of $\overline{\Gamma}\backslash W$. Disregard result if it has rank larger than 5.
- In case when coherent closure has rank 5 check if it is algebraically isomorphic to the Higmanian scheme $\mathfrak{M}$.

This algorithm was programmed in GAP with the aid of GRAPE.

In what follows we are using labeling of strongly regular graphs as in [19].

It turns out that precisely first 11 graphs have cliques of size 8. All these graphs admit at least one Higmanian association scheme. Altogether we get 15 schemes.

8 Survey of computer results

The main results of computation are presented in table form below. Here we show for each graph order of its automorphism group and lengths of its orbits, similar information is provided for automorphism group of each association scheme.

Note that now the classical Higmanian association scheme coincides with the scheme $\mathfrak{M}_{6.1}$.

We provide also information about the number of 4-cliques in each of 15 Higmanian graphs. An interesting correlation appears with the property to be geometric. Only those (4) Higmanian graphs are the point graphs of a suitable partial linear space, which admit (like classical Higmanian graph) precisely 40 cliques of size 4.

Γ_i	$\mathfrak{M}_j$	$\lvert Aut(\Gamma)\rvert$	$\lvert orb(Aut(\Gamma))\rvert$	$\lvert Aut(\mathfrak{M})\rvert$	$\lvert orb(Aut(\mathfrak{M}))\rvert$	Geometric	Nr. of 4-cliques
Γ_1	1.1	48	4, 123	48	same	no	32
Γ_2	2.1	384	16, 24	384	same	no	8
Γ_2	2.2	384	16, 24	192	same	yes	40
Γ_3	3.1	8	28, 42, 82	8	same	no	20
Γ_4	4.1	12	1, 33, 63, 12	12	same	no	24
Γ_5	5.1	64	8, 162	64	same	yes	40
Γ_5	5.2	64	8, 162	32	42, 82, 16	no	24
Γ_6	6.1	51840	40	1920	same	yes	40
Γ_7	7.1	192	4, 12, 24	192	same	no	24
Γ_7	7.2	192	4, 12, 24	32	42, 82, 16	yes	40
Γ_8	8.1	8	28, 42, 82	8	same	no	28
Γ_9	9.1	48	2, 4, 6, 12, 16	16	24, 44, 16	no	32
Γ_{10}	10.1	16	42, 84	16	same	no	32
Γ_{10}	10.2	16	42, 84	8	48, 8	no	32
Γ_{11}	11.1	144	4, 12, 24	48	same	no	32

Acknowledgements

We thank E. Bannai, A. Deza, M. Deza, T. Huang and A. Woldar for helpful discussions and information.

As we have mentioned, our paper makes essential use of the catalogue of srg's on 40 points created by Ted Spence. For this reason we regard him as our "invisible" coauthor. Moreover, Ted looked carefully over this text and suggesting many helpful inprovements. Thus it is our pleasure to thank him for this job, and to extend our hope for his more essential involvement in the preparation of an advanced, self-contained paper concerning the introduced family of Higmanian schemes.

References

[1] **A. E. Brouwer, A. M. Cohen, A. Neumaier.** *Distance-regular graphs.* Springer-Verlag, Berlin, 1989.

[2] **Y. Chang, T. Huang.** *Imprimitive association schemes of low ranks and Higmanian graphs.* Conference on Combinatorics and Physics (Los Alamos, NM, 1998), Ann. Comb. 4 (2000), no. 3-4, 317–326.

[3] **A. Deza, M. Deza.** *The ridge graph of the metric polytope and some relatives.* Polytopes: abstract, convex and computational (Scarborough, ON, 1993), pp. 359–372, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 440, Kluwer Acad. Publ., Dordrecht, 1994.

[4] **M. Deza, T. Huang.** *A generalization of strongly regular graphs.* Southeast Asian Bull. of Math. 26, 2002, 205–213.

[5] **I. A. Faradžev, M. H. Klin, M. E. Muzichuk.** *Cellular rings and groups of automorphisms of graphs.* In: I. A. Faradžev et al. (eds.): *Investigations in algebraic theory of combinatorial objects.* Kluwer Acad. Publ., Dordrecht, 1994, 1–152.

[6] **I. A. Faradžev, M. H. Klin.** *Computer package for computations with coherent configurations.* Proc. ISSAC-91, pp. 219–223, Bonn, 1991. ACM Press.

[7] **W. H. Haemers.** *Eigenvalue techniques in design and graph theory.* Math. Centre Tracts 121. Mathematisch Centrum, Amsterdam, 1980.

[8] **D. G. Higman.** *Coherent algebras.* Linear Algebra Appl. 93, 1987, 209–239.

[9] **D. G. Higman.** *Rank 5 association schemes and triality.* Linear Algebra Appl. 226-228, 1995, 197–222.

[10] **G. Jones, M. Klin, F. Lazebnik.** *Automorphic subsets of the n-dimensional cube.* Beiträge Algebra Geom 41, 2000, 303–323.

[11] **M. Klin, M. Meszka, S. Reichard, A. Rosa.** *The smallest non-rank 3 strongly regular graphs which satisfy the 4-vertex condition.* Bayreuther Math. Schriften 74, 2005, 145–205.

[12] **M. Klin, S. Reichard.** *A partial linear space on 96 points, the icosahedron, and other related combinatorial structures.* Congr. Numer. 161, 2003, 195–209.

[13] **M. Klin, C. Rücker, G. Rücker, G. Tinhofer.**, *Algebraic combinatorics in mathematical chemistry. Methods and algorithms. I. Permutation groups and coherent (cellular) algebras.* MATCH (Communications in mathematical and in computer chemistry) 40, 1999, 7–138.

[14] **M. H. Klin, N. S. Zefirov.** *Group theoretical approach to the investigation of reaction graphs for highly degenerate rearrangements of chemical compounds. II Fundamental concepts.* MATCH (Communications in mathematical and in computer chemistry) 26, 1991, 171–190.

[15] **B. D. McKay.** *nauty User's Guide (Version 1.5).* Technical Report TR-CS-90-02, Computer Science Department, Australian National University, 1990.

[16] **S. E. Payne.** *All generalized quadrangles of order 3 are known.* J. Combin. Theory (A) 18, 1975, 203–206.

[17] **M. Schönert et al.** *GAP – Groups, Algorithms, and Programming.* Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, Germany, fifth edition, 1995.

[18] **L. H. Soicher.** *GRAPE: a system for computing with graphs and groups.* In: L. Finkelstein and W.M. Kantor, editors, *Groups and Computation*, volume 11 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pp. 287–291, A.M.S., 1993.

[19] **E. Spence.** *The strongly regular* $(40, 12, 2, 4)$ *graphs.* Electron. Journal of Combin. 7, 2000, R22.

[20] **E. R. van Dam.** *Three-class association schemes.* J. Algebraic. Combin. 10, 1999, 69–107.

[21] **B. Weisfeiler (ed.).** *On construction and identification of graphs.* Lecture Notes in Math. 558, Springer, Berlin, 1976.

[22] **M. Ziv-Av.** *Two assiciation schemes on 40 and 64 points: A supplement to the paper by Bannai-Bannai-Bannai.* Poster presentation (jointly with M. Klin), Linz, 2006.
`http://www.ricam.oeaw.ac.at/specsem/srs/groeb/download/ZivAv_poster.pdf`

Group-Case Commutative Association Schemes and Their Character Tables

Sung Y. Song
Department of Mathematics, Iowa State University, Ames, Iowa, 50011, U. S. A.

Hajime Tanaka
Graduate School of Information Sciences, Tohoku University, Sendai, 980-8579, Japan

Abstract

Leading towards the classification of primitive commutative association schemes as the ultimate goal, Bannai and some of his school have been trying to

- identify the major sources of (primitive) commutative association schemes,
- collect known group-case primitive commutative association schemes, and
- compute their character tables

over the last twenty years. The construction of their character tables are important first step for a systematic study of such association schemes and towards the classification of those schemes. In this talk, we briefly survey the progress made in this direction of research, and list some open problems.

Dedicated to Eiichi Bannai on the occasion of his 60th birthday

1 Introduction

Let a finite group G act on a finite set X transitively. Then G naturally acts on $X \times X$ by $(x,y)^g = (x^g, y^g)$. Let $R_0, R_1, \ldots, R_d$ be the orbits of G on $X \times X$ with $R_0 = \{(x,x) : x \in X\}$. Then $\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$ is an association scheme, called a *group-case* (or *Schurian*) association scheme, and denoted by $\mathcal{X}(G,X)$.

Let G be a finite group, and let H be a subgroup of G. Let $X = H\backslash G$ be the set of the cosets of H in G. Then G acts transitively on X under the action $(Hx)^g = H(xg)$. The group-case scheme $\mathcal{X}(G, H\backslash G)$ is commutative if and only if the permutation character of G on $H\backslash G$ is multiplicity-free. Any group-case scheme $\mathcal{X}(G,X)$ can be viewed as $\mathcal{X}(G, H\backslash G)$ with the point stabilizer $H = G_x$ for an $x \in X$. The condition that the group-case association scheme is primitive is equivalent to that of the permutation group acts on the cosets by a maximal subgroup.

In early nineteen eighties, Bannai had a conviction that the works by many group theorists on the classification of maximal subgroups of finite simple groups (by using

the classification of finite simple groups) would eventually lead to the complete list of group-case primitive commutative association schemes. He seemed to believe that the calculations of parameters and character tables of known association schemes of such kind were to be feasible. He began to investigate the major sources of group-case primitive commutative association schemes, collect examples, and calculate their character tables.

The major sources of group-case (primitive) commutative association schemes of large class which Bannai (cf. [2]) has considered were as follows.

1. The actions of classical groups (or Chevalley groups) G on appropriate subspaces X of vector spaces over finite fields. (If the subspaces are isotropic, they are well understood because then the groups act on the cosets by parabolic subgroups. The cases of non-isotropic subspaces require further study. See examples in Table 1 below.)

2. The actions of classical groups (or Chevalley groups) G on the cosets $X = H\backslash G$ of multiplicity-free (maximal) subgroups H. (A pair (G, H) of a finite group G and a subgroup H whose permutation character 1_H^G is multiplicity-free, is often called a Gelfand pair. See examples in Tables 2 and 3 below.)

3. Finite (simple) groups, loops, and quasigroups G. (Commutative association schemes obtained from these algebraic structures by using their conjugacy classes as we will see in the sequel.)

4. The n-dimensional vector spaces V over $GF(q)$ and subgroups H of $GL(n, q)$; for example, the action of the semidirect product $G = V \rtimes H$ on V, in other words, G acts on $X = H\backslash G$.

We note that the items in this list are not necessarily mutually exclusive nor cover all primitive commutative association schemes. Character tables of many commutative association schemes coming from the permutation groups in the above list have been investigated by many people including, Bannai-Song [8, 9, 10], Bannai-Shen-Song [6], Bannai-Kawanaka-Song [4], Bannai-Kwok-Song [5], Bannai-Shen-Song-Wei [7], Kwok [25, 26], Henderson [18, 19, 20, 21], Tanaka [29, 30], Bannai-Tanaka [12], Fujisaki [14, 15], and Bannai-Song-Yamada [11].

In Section 2, we briefly recall the definition of character tables of commutative association schemes and related basic facts. In Section 3, we discuss Paige's simple Moufang loops and their character tables. In Section 4, we give a list of known examples of group-case association schemes whose character tables are either calculated or conjectured. Some open cases coming from Gelfand pairs are listed. In Section 5, we illustrate another example that is constructed in a different way from the previous ones. The character tables illustrated in this note are happened to be closely related to each other in an interesting way.

Our aim is to review the progress that has been made in the construction of character tables by paying attention to the construction methods employed. In doing this we would like to point out some connections between association schemes and classical groups and geometries. Experts in algebraic combinatorics, groups and geometry will hopefully find some useful information and sufficient pointers in this note.

2 The character tables

Let $\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$ be a commutative association scheme. Let $A_0, A_1, \ldots, A_d$ be the adjacency matrices and let $E_0, E_1, \ldots, E_d$ be the primitive idempotents of $\mathcal{X}$. The Bose-Mesner algebra $\mathcal{A} = \langle A_0, A_1, \ldots, A_d \rangle = \langle E_0, E_1, \ldots, E_d \rangle$ of $\mathcal{X}$ over the field $\mathbb{C}$ of complex numbers, satisfies

$$A_j = \sum_{i=0}^{d} p_j(i) E_i.$$

Equivalently, with the character table $P = [p_j(i)]$ of $\mathcal{X}$, we have

$$[A_0\ A_1\ \cdots\ A_d] = [E_0\ E_1\ \cdots\ E_d] \begin{bmatrix} 1 & k_1 & k_2 & \cdots & k_d \\ 1 & p_1(1) & p_2(1) & \cdots & p_d(1) \\ 1 & p_1(2) & p_2(2) & \cdots & p_d(2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & p_1(d) & p_2(d) & \cdots & p_d(d) \end{bmatrix}.$$

The character table P of the association scheme satisfies the (i) row and (ii) column orthogonality relations [3, Theorem 3.5]. For $i, j \in \{0, 1, \ldots, d\}$,

$$\text{(i)} \quad \sum_{l=0}^{d} \frac{1}{k_l} p_l(i)\overline{p_l(j)} = \frac{|X|}{m_i}\delta_{ij}, \qquad \text{(ii)} \quad \sum_{l=0}^{d} m_l p_i(l)\overline{p_j(l)} = |X| k_i \delta_{ij},$$

where $m_l = \operatorname{rank}(E_l) = \operatorname{trace}(E_l)$ $(0 \le l \le d)$, δ_{ij} is the Kronecker delta, and $\overline{a}$ denotes the complex conjugate of a. The numbers m_l are the multiplicities of the scheme.

Let G be a finite (simple) group, and let $C_0, C_1, \ldots, C_d$ be the conjugacy classes of G. Then by defining the associate classes R_i by

$$(x, y) \in R_i \quad \text{iff} \quad yx^{-1} \in C_i,$$

we obtain a (primitive) commutative scheme $\mathcal{X}(G) = (G, \{R_i\}_{0 \le i \le d})$ which is often referred to as the *group scheme*. Given a finite (simple) quasigroup, we also obtain a (primitive) commutative association scheme by defining the associate relations as above. For $i = 0, 1, \ldots, d$, let k_i and f_i denote the sizes of conjugacy classes C_i and the degrees of the irreducible characters of G, respectively. Then $f_i = \sqrt{\operatorname{rank}(E_i)}$ and the character table P of $\mathcal{X}(G)$ and the group character table T has the following relation:

$$T = \begin{bmatrix} f_0 & & & 0 \\ & f_1 & & \\ & & \ddots & \\ 0 & & & f_d \end{bmatrix} \cdot P \cdot \begin{bmatrix} 1/k_0 & & & 0 \\ & 1/k_1 & & \\ & & \ddots & \\ 0 & & & 1/k_d \end{bmatrix}.$$

3 Character tables of Paige's Moufang loops

A set Q with one binary operation is a *quasigroup* if the equation $xy = z$ has a unique solution in Q whenever two of $x, y, z \in Q$ are specified. A *loop* is a quasigroup with a neutral element 1 satisfying $1x = x = x1$ for every $x \in Q$.

A *Moufang loop* is a loop in which any of the following (equivalent) Moufang identities holds: $((xy)x)z = x(y(xz))$, $x(y(zy)) = ((xy)z)y$, $(xy)(zx) = x((yz)x)$, or $(xy)(zx) = (x(yz))x$.

Paige (1956) [28] introduced a class of finite simple Moufang loops which we are referring to as Paige's simple Moufang loops. Liebeck (1987) [27] proved that there are no other finite (non-associative) simple Moufang loops besides these Moufang loops. For every finite field $\mathbb{F}_q$, there is exactly one simple Moufang loop $\mathcal{M}^* = \mathcal{M}^*(q)$ of order $q^3(q^4-1)/(q-1,2)$. Bannai and Song (1989) [9] calculated the character tables of $\mathcal{M}^*(q)$. We now recall the definition of $\mathcal{M}^*(q)$.

On the set

$$\left\{ \begin{bmatrix} a & \alpha \\ \beta & b \end{bmatrix} : \ a,b \in \mathbb{F}_q, \ \alpha,\beta \in \mathbb{F}_q^3 \right\}$$

where $\mathbb{F}_q^3 := \{(x,y,z) : \ x,y,z \in \mathbb{F}_q\}$, using the dot product $\alpha \cdot \beta$ and vector product $\alpha \times \beta$ in $\mathbb{F}_q^3$, define the Zorn's multiplication

$$\begin{bmatrix} a & \alpha \\ \beta & b \end{bmatrix} \begin{bmatrix} c & \gamma \\ \delta & d \end{bmatrix} := \begin{bmatrix} ac + \alpha \cdot \delta & a\gamma + d\alpha - \beta \times \delta \\ c\beta + b\delta + \alpha \times \gamma & \beta \cdot \gamma + bd \end{bmatrix}.$$

Given $M = \begin{bmatrix} a & \alpha \\ \beta & b \end{bmatrix}$, we define its determinant by

$$\det(M) := ab - \alpha \cdot \beta.$$

Then both sets $\mathcal{L} := \{M : \ \det(M) \neq 0\}$ and $\mathcal{M} := \{M : \ \det(M) = 1\}$ are (non-associative) Moufang loops. The center of $\mathcal{L}$ is

$$Z(\mathcal{L}) = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} : \ a \in \mathbb{F}_q^* \right\}.$$

We see that $|Z(\mathcal{M})| = 1$ if the characteristic of $\mathbb{F}_q$ is 2, otherwise, $|Z(\mathcal{M})| = 2$. The quotient loop $\mathcal{M}^* := \mathcal{M}/Z(\mathcal{M})$ is referred to as the *Paige's simple Moufang loop.*

The conjugacy classes and character tables of $\mathcal{M}^*(q)$ were calculated in [9]. Here we recall the case with $q = 2^r$.

Theorem 1. [9, Table 5] *The character table of $\mathcal{X}(\mathcal{M}^*)$, $q = 2^r$ is given by*

$$\left[\begin{array}{cc|ccc|ccc} 1 & (q^6-1) & q^6-q^3 & \cdots & q^6-q^3 & q^6+q^3 & \cdots & q^6+q^3 \\ 1 & q^2-1 & -q^3+q^2 & \cdots & -q^3+q^2 & q^3+q^2 & \cdots & q^3+q^2 \\ \hline 1 & -q^3-1 & & & & & & \\ \vdots & \vdots & & q^2\,[a_{kl}] & & & 0 & \\ 1 & -q^3-1 & & & & & & \\ \hline 1 & q^3-1 & & & & & & \\ \vdots & \vdots & & 0 & & & q^2\,[b_{mn}] & \\ 1 & q^3-1 & & & & & & \end{array}\right]$$

where

$$a_{kl} = -q(\sigma^{kl} + \sigma^{-kl}), \ 1 \leq k,l \leq q/2; \ \sigma = \exp(2\pi i/(q+1))$$

$$b_{mn} = q(\rho^{mn} + \rho^{-mn}), \ 1 \leq m,n \leq (q-2)/2: \ \rho = \exp(2\pi i/(q-1)).$$

This character table resembles the following table of $\mathcal{X}(PSL(2,q))$, $q = 2^r$ which is derived from the group character table of $PSL(2,2^r)$ found in [13].

Proposition 1. [13, §38] *The character table of $\mathcal{X}(PSL(2,q))$, $q = 2^r$ is given by*

$$\left[\begin{array}{cc|ccc|ccc}
1 & (q^2-1) & q^2-q & \cdots & q^2-q & q^2+q & \cdots & q^2+q \\
1 & 0 & -q+1 & \cdots & -q+1 & q+1 & \cdots & q+1 \\
\hline
1 & -q-1 & & & & & & \\
\vdots & \vdots & & [a_{kl}] & & & 0 & \\
1 & -q-1 & & & & & & \\
\hline
1 & q-1 & & & & & & \\
\vdots & \vdots & & 0 & & & [b_{mn}] & \\
1 & q-1 & & & & & &
\end{array}\right]$$

where a_{kl} and b_{mn} as in the above theorem.

So, it is evident how the character table of $\mathcal{X}(\mathcal{M}^*)$ can be expressed in terms of $\mathcal{X}(PSL(2,q))$, and vice versa. It is also shown that the corresponding result for odd q is very similar to the above. Namely, if we replace all q^3 by q and q^2 by 1 in the character table of $\mathcal{X}(\mathcal{M}(q)^*)$ for $q = p^r$ with p an odd prime, then the resulting table is the character table of the fusion scheme $\tilde{\mathcal{X}}(PSL(2,q))$ obtained from that of $\mathcal{X}(PSL(2,q))$ by combining two conjugacy classes of order p of $PSL(2,q)$, which are conjugate in $PGL(2,q)$, into a single class. (See [9, Theorem 2.3.3].)

Construction A. The character table of $\mathcal{X}(\mathcal{M}(q)^*)$ was constructed as follows.
(1) We calculated the parameters p_{ij}^h of $\mathcal{X}(\mathcal{M}(q)^*)$ and expressed them in terms of parameters of $\mathcal{X}(PSL(2,q))$ as in [9, Lemma 2.2.2].
(2) Using the relationship $\sum_{h=0}^{d} p_{ij}^h p_h(r) = p_i(r)p_j(r)$ between the parameters and the characters for $\mathcal{X}(PSL(2,q))$, and the relationship between the two sets of parameters obtained in (1), we found the relations between the parameters and entries of the character table of $\mathcal{X}(\mathcal{M}(q)^*)$.
(3) Finally, we examined if the table satisfied the orthogonality conditions of rows and columns to be a character table.

Of course, this method only works when two schemes are intimately related so that the relations in (1) are simple enough to figure out the relations in (2). The construction of the character tables of Paige's Moufang loops has led us to be able to construct those for many other association schemes via this method. Despite the 'intimacy' requirement, it has been used effectively in many cases where one scheme 'controls' many others. See, for example [6, 7, 29].

4 Group-case association schemes

All association schemes coming from the major sources listed in Introduction are essentially coming from either a finite simple groups or quasigroups, Gelfand pairs, the primitive permutation groups and the suitable subgroups that can be the point stabilizers of the actions of groups. All group schemes $\mathcal{X}(G)$ can be viewed as groups $G \times G$

acting on G by $x \mapsto g^{-1}xh$. For given a quasigroup Q and $x \in Q$, Suppose G is the multiplicative group $Gr(Q)$ of Q generated by all permutations $L(x)$ and $R(x)$ of Q defined by

$$L(x): \ y \mapsto xy; \quad R(x): \ y \mapsto yx.$$

Then the association scheme defined by the orbits of $Gr(Q)$ on $Q \times Q$ as the associate relations, is isomorphic to the quasigroup association scheme $\mathcal{X}(Q)$ defined by its conjugacy classes.

The class of group schemes and quasigroup schemes contain all finite simple groups and quasigroups. All finite simple groups have been classified (cf. [16]), but quasigroups seems to require a lot more work. Many maximal subgroups of finite simple groups have been discovered by the work of many group theorists (cf., [22, 23]). So there are a lot of group-case primitive commutative association schemes to be studied. The character tables of some of these association schemes have been calculated. In doing so, the following facts play an important role.

Construction B. Let G be a group and H be a subgroup of G. Let $c_0, c_1, \ldots, c_d$ be class representatives of the conjugacy classes $C_0, C_1, \ldots, C_d$. Let $\{Hg_jH : \ 0 \le j \le d\}$ be the set of all double cosets of H. Suppose

$$1_H^G = \rho_0 + \rho_1 + \cdots + \rho_d$$

is the decomposition of 1_H^G into irreducible characters $\rho_0, \rho_1, \ldots, \rho_d$ of G. Then by [3, Corollary 11.7], the entries $p_j(i)$ of the character table of $\mathcal{X}(G, H\backslash G)$ are given by

$$\begin{aligned} p_{j'}(i) &= \frac{1}{|H|} \sum_{c \in Hg_jH} \rho_i(c) \\ &= \frac{1}{|H|} \sum_k |Hg_jH \cap C_k| \cdot \rho_i(c_k). \end{aligned}$$

So, in order to calculate $p_j(i)$ for $\mathcal{X}(G, H\backslash G)$, we need to know

- the conjugacy classes and group characters of G,
- the set of double cosets of H in G,
- the size of the intersection of each conjugacy class and each double coset, and
- the decomposition of 1_H^G into irreducible characters.

This procedure has been employed when W. Kwok (1991) [25] calculated the character table of $\mathcal{X}(O_3(q), O_2^+(q)\backslash O_3(q))$, the scheme obtained from the action of the general orthogonal group $O_3(q)$ acting on the sets of hyperplanes (for odd q; see [30] for even q). This character table controls the character tables of association schemes coming from the orthogonal groups on the sets of hyperplanes in the corresponding orthogonal geometries. We remark that the character tables of the association schemes coming from the action of $O_{2m}^+(q)$ on the set of non-isotropic points are obtained by modifying the character tables of the group $PSL(2, q)$ in exactly the same way as that of $\mathcal{X}(\mathcal{M}^*)$ is obtained from that of $\mathcal{X}(PSL(2, q))$. The reason for this may be explained as follows. Let V be a $2m$-dimensional vector space over $GF(q)$. Let X be the set

of non-isotropic points corresponding to a non-singular quadratic form of Witt index m. Then $|X| = q^{m-1}(q^m - 1)$. The group $G = O^+_{2m}(q)$ acts transitively on X if q is even, and it acts transitively on each half of X if q is odd. Any of these transitive permutation groups gives a symmetric association scheme of class q if q is even, and class $(q+1)/2$ if q is odd. It is shown that when $m = 4$ this permutation group $O^+_8(q)$ on X (or the half of X) is isomorphic to the permutation group $Gr(\mathcal{M}^*(q))$ on $\mathcal{M}^*(q)$.

The following table summarizes the results from [6, 7, 10, 25, 29]. In every case, the character tables of association schemes corresponding to permutation groups G on corresponding geometries are controlled by the character table of a 'canonical' one. This happens to almost all cases (cf. [5]).

Table 1. Examples of schemes from source group 1.

Groups	Geometries	Controlled by
$O^{\pm}_{2m}(q)$, q even	nonisotropic points (or lines)	$PGL(2,q)$
$O^{\pm}_{2m}(q)$, q odd	each half of nonisotropic points	$PSL(2,q)$
$O_{2m+1}(q)$, q even	$\pm$-type hyperplanes	$PGL(2,q)/D_{2(q\mp1)}$
$O_{2m+1}(q)$, q odd	$\pm$-type nonisotropic points	$PGL(2,q)/D_{2(q\mp1)}$
$U_m(q)$	nonisotropic points	$PGL(2,q)/Z_{q+1}$
$Sp_{2m}(q)$	nonisotropic lines	$PGL(2,q)/Z_{q-1}$
$P\Gamma L(n,q)$	non-incident point-hyperplane pairs	$PGL(2,q)/Z_{q-1}$

The following table includes some examples of known Gelfand pairs for which corresponding association schemes have been investigated. However, the character tables of the associated commutative association schemes are not yet known for (4).

Table 2. Examples of Gelfand pairs from the source group 2.

Labels	Groups G	Subgroups H	References
(1)	$GL(2n,q)$	$Sp(2n,q)$	Klyachko [24]; Bannai-Kawanaka-Song [4]
(2)	$GL(n,q^2)$	$GL(n,q)$	Gow [17]; Henderson [18, 19]
(3)	$GL(n,q^2)$	$GU(n,q)$	Gow [17]; Henderson [18, 19]
(4)	$GL(2n,q)$	$GL(n,q^2)$	Inglis-Liebeck-Saxl [23]; Terras [31]; Bannai-Tanaka [12]; Henderson [20]
(5)	$GU(2n,q^2)$	$Sp(2n,q)$	Inglis [22]; Henderson [20, 21]
(6)	$Sp(4,q)$	$Sz(q)$	Inglis [22]; Bagchi-Sastry [1]; Bannai-Song [8]

There are many instances where the knowledge of all ingredients in Construction B does not automatically determine the character tables. Still there are many other examples of known Gelfand pairs, and character tables of their corresponding association schemes need to be determined. For example, among the association schemes $\mathcal{X}(G, H\backslash G)$ coming from the Gelfand pairs G and H that appeared in the Arjeh

Cohen's "Tables of Possible Classical Distance-Transitive Groups" (found at URL: http://www.win.tue.nl/~amc/oz/dtg/classic.html), the character tables of the following cases need to be calculated. Here in the table instead of an almost simple group G and its maximal subgroup H, socle S of G and H are listed.

Table 3. Examples of Gelfand pairs whose character tables need to be determined.

S	type H	Comment
$PSU_6(q)$	$SU_3(q) \times SU_3(q)$	[20]: 1_H^G decomposed
$PSU_4(q)$	$SU_2(q) \times SU_2(q)$	[20]: 1_H^G decomposed
$PSU_4(q)$	$O_4^-(q)$, q: odd	[20]: 1_H^G decomposed
$P\Omega_{2n}^+(q)$	stabilizer of an $O_2^-(q)$ space	[14, 15]: double cosets described
$P\Omega_{2n}^-(q)$	stabilizer of an $O_2^-(q)$ space	[14, 15]: double cosets described
$P\Omega_n(q)$	stabilizer of an $O_2^-(q)$ space, nq: odd	?

Using the classification of finite simple groups, multiplicity-free maximal subgroups of almost simple groups are getting well understood. This will eventually lead to the complete list of association schemes of this type which we are looking for.

5 Character tables of $\mathcal{X}(G_2(q), O_6^\epsilon(q))$

This is an example that we determine the character table by using fission relations together with orthogonality conditions of the character table.

Let q be odd, and let $G = G_2(q)$ be the Chevalley group of type G_2. Let Ω_1 and Ω_2 denote the sets of hyperplanes of type $O_6^+(q)$ and $O_6^-(q)$ in the 7-dimensional orthogonal space over $\mathbb{F}_q$. G acts transitively on Ω_1 and Ω_2. Let H_1 and H_2 be the one-point stabilizers of G on Ω_1 and Ω_2, respectively. Then $H_1 \simeq SL_3(q).2$ and $H_2 \simeq SU_3(q).2$. The corresponding ranks of the permutation group are $\frac{1}{2}(q+5)$ and $\frac{1}{2}(q+3)$, respectively. It is shown that $\mathcal{X}(G_2(q), \Omega_2) \simeq \mathcal{X}(O_7(q), \Omega_2)$. The character table of $\mathcal{X}(O_7(q), \Omega_2)$ has been constructed in [6]. However, the character table of $\mathcal{X}(G_2(q), H_1\backslash G_2(q))$ is not isomorphic to $\mathcal{X}(O_7(q), \Omega_1)$ but to its fission table. We note that $|G| = q^6(q^2-1)(q^6-1)$, and $|\Omega_1| = [G : H_1] = \frac{1}{2}q^3(q^3+1)$ with $\mathrm{rank}(G, \Omega_1) = \frac{1}{2}(q+5) = 1 + \mathrm{rank}(O_7(q), \Omega_1)$.

The character table of $\mathcal{X}(G_2(q), SL_3(q).2\backslash G_2(q))$ and that of $\mathcal{X}(O_7(q), \Omega_1)$ are, respectively, given as follows

$$\begin{bmatrix}
1 & 2(q^3-1) & (q^2-1)(q^3-1) & q^2(q^3-1) & \cdots\cdots & q^2(q^3-1) & \frac{1}{2}q^2(q^3-1) \\
1 & -q^2+q-2 & q^3-q^2-q+1 & -2q^2 & \cdots\cdots & -2q^2 & -q^2 \\
1 & 2q^2-2q-2 & q^3-4q^2+2q+1 & -2q^2 & \cdots\cdots & -2q^2 & -q^2 \\
1 & -2 & -q^2+1 & & & & \\
\vdots & \vdots & \vdots & & (q^2\chi_{ij}) & {\scriptstyle 1\le i\le \frac{1}{2}(q-1)} & \\
 & & & & & {\scriptstyle 1\le j\le \frac{1}{2}(q-1)} & \\
1 & -2 & -q^2+1 & & & &
\end{bmatrix}$$

$$\begin{bmatrix} 1 & (q^2+1)(q^3-1) & q^2(q^3-1) & \dots & q^2(q^3-1) & \frac{1}{2}q^2(q^3-1) \\ 1 & q^3-2q^2-1 & -2q^2 & \dots & -2q^2 & -q^2 \\ 1 & -q^2-1 & & & & \\ \vdots & \vdots & & (q^2\chi_{ij}) & {\scriptstyle 1\le i\le \frac{1}{2}(q-1)} & \\ & & & & {\scriptstyle 1\le j\le \frac{1}{2}(q-1)} & \\ 1 & -q^2-1 & & & & \end{bmatrix}$$

where $\chi_{ij} \in \mathbb{Q}(\theta) \cup \mathbb{Q}(\rho)$, θ and ρ are the $(q+1)$th- and $(q-1)$th- root of unity, are the entries of the character table of $\mathcal{X}(O_3(q), \Omega_1)$ described by Kwok [25] and can be calculated from the result in [6, §6].

References

[1] B. Bagchi and N. S. N. Sastry, Intersection pattern of the classical ovoids in symplectic 3-space of even order, J. Algebra 126 (1989) 147–160.

[2] E. Bannai, Character tables of commutative association schemes, in: finite geometries, buildings, and related topics (Pingree Park, CO, 1988), Oxford University Press, New York, 1990, pp. 105–128.

[3] E. Bannai and T. Ito, Algebraic combinatorics I: Association schemes, Benjamin/Cummings, Menlo Park, CA, 1984.

[4] E. Bannai, N. Kawanaka and S.-Y. Song, The character table of the Hecke algebra $\mathcal{H}(GL_{2n}(F_q), Sp_{2n}(F_q))$, J. Algebra 129 (1990) 320–366.

[5] E. Bannai, W. M. Kwok and S.-Y. Song, Ennola type dualities in the character tables of some association schemes, Mem. Fac. Sci. Kyushu Univ. Ser. A 44 (1990) 129–143.

[6] E. Bannai, H. Shen and S.-Y. Song, Character tables of the association schemes of finite orthogonal groups acting on the nonisotropic points, J. Combin. Theory Ser. A 54 (1990) 164–200.

[7] E. Bannai, H. Shen, S.-Y. Song and H. Wei, Character tables of certain association schemes coming from finite unitary and symplectic groups, J. Algebra 144 (1991) 189–213.

[8] E. Bannai and S.-Y. Song, On the character table of the association scheme $Sp(4,q)/Sz(q)$, Graphs Combin. 5 (1989) 291–293.

[9] E. Bannai and S.-Y. Song, The character tables of Paige's simple Moufang loops and their relationship to the character tables of $PSL(2,q)$, Proc. London Math. Soc. (3) 58 (1989) 209–236.

[10] E. Bannai and S.-Y. Song, The character table of the commutative association scheme coming from the action of $GL(n,q)$ on nonincident point-hyperplane pairs, Hokkaido Math. J. 19 (1990) 417–429.

[11] E. Bannai, S.-Y. Song and H. Yamada, Character tables of the association schemes coming from the action of $G_2(q)$ on hyperplanes of type $O_6^\epsilon(q)$, preprint.

[12] E. Bannai and H. Tanaka, The decomposition of the permutation character $1_{GL(n,q^2)}^{GL(2n,q)}$, J. Algebra 265 (2003) 496–512.

[13] L. Dornhoff, Group representation theory, Part A: Ordinary representation theory, Marcel Dekker, New York, 1971.

[14] T. Fujisaki, The action of finite orthogonal groups in characteristic 2 on the set of anisotropic lines, Ph.D. Thesis, Kyushu University, 2003.

[15] T. Fujisaki, The action of finite orthogonal groups in characteristic 2 on the set of anisotropic lines, J. London Math. Soc. (2) 73 (2006) 287–303.

[16] D. Gorenstein, R. Lyons and R. Solomon, The classification of the finite simple groups, American Mathematical Society, Providence, RI, 1994.

[17] R. Gow, Two multiplicity-free permutation representations of the general linear group $GL(n, q^2)$, Math. Z. 188 (1984) 45–54.

[18] A. Henderson, Character sheaves on symmetric spaces, Ph.D. Thesis, Massachusetts Institute of Technology, 2001.

[19] A. Henderson, Spherical functions of the symmetric space $G(\mathbb{F}_{q^2})/G(\mathbb{F}_q)$, Represent. Theory 5 (2001) 581–614.

[20] A. Henderson, Symmetric subgroup invariants in irreducible representations of G^F, when $G = GL_n$, J. Algebra 261 (2003) 102–144.

[21] A. Henderson, Spherical functions and character sheaves, unpublished.

[22] N. F. J. Inglis, Multiplicity-free permutation characters, distance-transitive graphs and classical groups, Ph.D. thesis, Cambridge University, 1988.

[23] N. F. J. Inglis, M. W. Liebeck and J. Saxl, Multiplicity-free permutation representations of finite linear groups, Math. Z. 192 (1986) 329–337.

[24] A. A. Klyachko, Models for the complex representations of the groups $GL(n, q)$, Math. USSR-Sb. 48 (1984) 365–379.

[25] W. M. Kwok, Character table of a controlling association scheme defined by the general orthogonal group $O(3, q)$, Graphs Combin. 7 (1991) 39–52.

[26] W. M. Kwok, Character tables of association schemes of affine type, European J. Combin. 13 (1992) 167–185.

[27] M. W. Liebeck, The classification of finite simple Moufang loops, Math. Proc. Cambridge Philos. Soc. 102 (1987) 33–47.

[28] L. J. Paige, A class of simple Moufang loops, Proc. Amer. Math. Soc. 7 (1956) 471–482.

[29] H. Tanaka, On some relationships among the association schemes of the orthogonal groups acting on hyperplanes, Master Thesis, Kyushu University, 2001.

[30] H. Tanaka, A four-class subscheme of the association scheme coming from the action of $PGL(2, 4^f)$, European J. Combin. 23 (2002) 121–129.

[31] A. Terras, Fourier analysis on finite groups and applications, Cambridge University Press, Cambridge, 1999.

Association schemes related to universally optimal configurations

Kanat Abdukhalikov
Institute of Mathematics,
Pushkin Str 125, Almaty 480100, Kazakhstan
abdukhalikov@math.kz
and
Eiichi Bannai
Graduate School of Mathematics, Kyushu University,
Hakozaki 6-10-1, Higashi-ku, Fukuoka 812-8581, Japan
bannai@math.kyushu-u.ac.jp

In [4] two association schemes were considered and it was conjectured that these schemes determine universally optimal configurations in $\mathbb{R}^{10}$ and $\mathbb{R}^{14}$. It is known that these schemes are uniquely determined by there parameters [2].

The scheme on 40 points is a 4 class association scheme with automorphism group $2^4 : S_5$ (split extension). The stabilizer of a point is isomorphic to $2.S_4$ (nonsplit extension). The scheme generates a configuration of 40 points on unit sphere in $\mathbb{R}^{10}$. Rescaling these vectors we can suppose that they lie on a sphere of squared radius 6. Then they generate integral isodual lattice Q_{10} [5] with automorphism group $2^{10} : S_6$. This lattice can be obtained by construction A from binary quadratic residue [10,5,4] code. Theta series of the lattice Q_{10} is $\theta(q) = 1 + 260q^4 + 960q^6 + 3060q^8 + \cdots$. So 40 vectors from the configuration are not minimal vectors of the lattice.

The first and the second eigenmatrices are given by

$$P = \begin{pmatrix} 1 & 3 & 4 & 8 & 24 \\ 1 & -1 & 0 & -4 & 4 \\ 1 & -1 & 0 & 2 & -4 \\ 1 & 3 & 4 & -2 & -6 \\ 1 & 3 & -4 & 0 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 1 & 10 & 20 & 4 & 5 \\ 1 & -\frac{10}{3} & -\frac{20}{3} & 4 & 5 \\ 1 & 0 & 0 & 4 & -5 \\ 1 & -5 & 5 & -1 & 0 \\ 1 & \frac{5}{3} & -\frac{5}{3} & -1 & 0 \end{pmatrix}.$$

The scheme on 64 points is a 3 class association scheme [3] with automorphism group $4^3 : (2 \times L_3(2))$, where $2 \times L_3(2)$ is the stabilizer of a point.

It has the following first and second eigenmatrices:

$$P = Q = \begin{pmatrix} 1 & 14 & 42 & 7 \\ 1 & -6 & 6 & -1 \\ 1 & 2 & -2 & -1 \\ 1 & -2 & -6 & 7 \end{pmatrix}.$$

The scheme generates a configuration of 64 vectors on a sphere of squared radius 7 in $\mathbb{R}^{14}$. These vectors generate integral lattice with automorphism group $2^{14} : (2^3 : L_3(2))$. The lattice can be obtained by construction A from binary shortened projective [14,4,7] code. Theta series of the lattice is equal to $\theta(q) = 1 + 28q^4 + 1024q^7 + 2156q^8 + \cdots$. As in the previous case, 64 vectors are not minimal vectors of the lattice.

The latter scheme has a following generalization in terms of quaternary Kerdock and Preparata codes. Recall that $\mathbb{Z}_4$-Kerdock code K and $\mathbb{Z}_4$-Preparata code P are linear codes over $\mathbb{Z}_4$ of length $q = 2^m$, m odd:

$$0 \subset K \subseteq P \subset \mathbb{Z}_4^q.$$

They are dual codes: $K^\perp = P$. Moreover, $K = P$ for $m = 3$ and $K \neq P$ for $m > 3$. The image under the Gray map of the quaternary Kerdock (resp. Preparata) code is binary nonlinear Kerdock (resp. "Preparata") code. For $m = 3$ the Gray image of $K = P$ is the famous binary nonlinear Nordstrom-Robinson code of length 16. Consider shortened Kerdock and punctured Preparata codes:

$$0 \subset K_{\text{short}} \subseteq P_{\text{punct}} \subset \mathbb{Z}_4^{q-1} = A.$$

Since the automorphism group of the Kerdock code acts transitively on coordinates we can consider shortening and puncturing at any fixed (same) position. Note that $K_{\text{short}}^\perp = P_{\text{punct}}$. Therefore, one has nondegenerate bilinear pairing

$$(K_{\text{short}}, A/P_{\text{punct}}) \to \mathbb{Z}_4,$$

which gives us duality between K_{short} and A/P_{punct}. We have $|K_{\text{short}}| = |A/P_{\text{punct}}| = q^2 = 4^m$. We can consider A/P_{punct} as character group of K_{short} or vice versa. Therefore, an abelian association scheme on K_{short} defines dual abelian scheme on A/P_{punct} (cosets of P_{punct}).

Shortened $\mathbb{Z}_4$-Kerdock code [6] is a code of length $2^m - 1$, m odd. It has 4^m codewords and nonzero codewords have Lee weights $2^m - 2^{(m-1)/2}$, 2^m and $2^m + 2^{(m-1)/2}$. The following relations on the shortened Kerdock code will determine an abelian 3 class association scheme:

$$(x,y) = \begin{cases} R_0, & \text{if } x-y \text{ has weight } 0, \\ R_1, & \text{if } x-y \text{ has weight } 2^m + 2^{(m-1)/2}, \\ R_2, & \text{if } x-y \text{ has weight } 2^m - 2^{(m-1)/2}, \\ R_3, & \text{if } x-y \text{ has weight } 2^m. \end{cases}$$

The scheme has automorphism group $4^m : Aut(K_{\text{short}})$. Recall that $Aut(K_{\text{short}}) \cong 2 \times L_3(2)$ for $m = 3$ and $Aut(K_{\text{short}}) \cong 2 \times (\mathbb{F}_{2^m}^* : Aut(\mathbb{F}_{2^m}))$ for $m > 3$.

Cosets of punctured $\mathbb{Z}_4$-Preparata code $C = P_{\text{punct}}$ have Lee weights 0, 1 and 2. Furthermore, for cosets $a+C$ we can choose $a = (0,\dots,0,\pm 1,0,\dots,0)$, $a = (0,\dots,0,\pm 1,\dots,\pm 1,0,\dots,0)$ or $a = (0,\dots,0,2,0,\dots,0)$. The following relations on A/C

$$(x,y) = \begin{cases} R_0', & \text{if } x-y = C, \\ R_1', & \text{if } x-y = (0,\dots,0,\pm 1,0,\dots,0) + C, \\ R_2', & \text{if } x-y = (0,\dots,0,\pm 1,\dots,\pm 1,0,\dots,0) + C, \\ R_3', & \text{if } x-y = (0,\dots,0,2,0,\dots,0) + C \end{cases}$$

define a three class association scheme which is dual to the previous scheme.

Shortened $\mathbb{Z}_4$-Kerdock code scheme has the following first and second eigenmatrices:

$$P = \begin{pmatrix} 1 & 2q-2 & (q-1)(q-2) & q-1 \\ 1 & -\sqrt{2q}-2 & \sqrt{2q}+2 & -1 \\ 1 & \sqrt{2q}-2 & -\sqrt{2q}+2 & -1 \\ 1 & -2 & -q+2 & q-1 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & \frac{(q-\sqrt{2q})(q-1)}{2} & \frac{(q+\sqrt{2q})(q-1)}{2} & q-1 \\ 1 & -\frac{\sqrt{2q}(q-2)}{4} & \frac{\sqrt{2q}(q-2)}{4} & -1 \\ 1 & \frac{\sqrt{2q}}{2} & -\frac{\sqrt{2q}}{2} & -1 \\ 1 & -\frac{q-\sqrt{2q}}{2} & -\frac{q+\sqrt{2q}}{2} & q-1 \end{pmatrix}.$$

Abelian scheme defined on cosets A/P_{punct} has the following first and second eigenmatrices: $P' = Q$, $Q' = P$.

We also note that abelian group K_{short} is isomorphic to the Galois ring $GR(4,m) = \mathbb{Z}_4[\xi]$, $\xi^{q-1} = 1$, $q = 2^m$. Isomorphism is given by map $\gamma \mapsto (Tr(\gamma\xi^0), Tr(\gamma\xi^1), \dots, Tr(\gamma\xi^{q-2}))$, where $\gamma \in GR(4,m)$ (see for details [6]).

It seems that the schemes on shortened Kerdock codes also might be candidates for being universally optimal (or optimal) configurations in $\mathbb{R}^{2(2^m-1)}$.

We note that in $\mathbb{R}^{14}$ for θ-code, $\theta = \frac{1}{7}$, Levenshtein's bound is 69.6 (corresponding scheme has 64 points). Similarly, in $\mathbb{R}^{62}$ for θ-code, $\theta = \frac{3}{31}$, Levenshtein's bound is 1081 (corresponding scheme has 1024 points).

References

[1] K. Abdukhalikov, Projective Generalized Reed-Muller Codes over p-adic Numbers and Finite Rings. In: Jungnickel, Dieter (ed.) et al., Finite fields and applications. Proceedings of the fifth international conference on finite fields and applications F_{q^5}, 1–13, University of Augsburg, Germany, August 2-6, 1999. Berlin: Springer. 1–13 (2001).

[2] E. Bannai, E. Bannai and H. Bannai, Uniqueness of certain association schemes. Preprint.

[3] D. de Caen and E. R. van Dam, Association schemes related to Kasami codes and Kerdock sets, Designs and codes - a memorial tribute to Ed Assmus. *Des. Codes Cryptogr.* **18** (1999), no. 1–3, 89–102.

[4] H. Cohn, Sphere packings, energy minimization, and linear programming bounds, in The Proceedings of Second COE Workshop on Sphere Packings, (2005), 1–42.

[5] J. H. Conway and N. J. A. Sloane, On lattices equivalent to their duals. *J. Number Theory* **48** (1994) 373–382.

[6] R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* 40, No. 2 (1994), 301–319.

Rediscovered Theorems

By Koichiro Harada, Ohio State University

The classification of all simple groups of finite order was declared to be complete early in 1980's. It did not mean, however, that all relevant papers had actually been published at the time. One important paper had not been published for more than ten year after its announcement when Aschbaher and Smith took up the work of doing it from scratch in the latter half of 1990's. Their work was completed in 2004, thus completing the classification of all finite simple groups. Recently, a group of people (Aschbacher, Lyons, Smith, and Solomon) have been rechecking if indeed all relevant papers, minor or major, have been published. They discovered several missing papers. To my surprise, one of them is mine:

*) Finite groups having a component of type $2M_{22}$.

Roughly speaking what I claimed was that there is no simple groups having an involution z such that the centralizer of z in G is isomorphic to the double cover of M_{22} or of $Aut(M_{22})$. I remember that I wrote such a paper and searched for it in my file. I found several typed copies of it. The paper was written in the late 1970's but obviously it has not been submitted. At the Santa Cruz AMS Summer School for Group Theory held in 1979, it was reported that the Schur multiplier of M_{22} is a cyclic group of order 12, but not of order 6 as was believed previously. I must have put off the publication of my result on the double cover of M_{22} until the issue settled. Then, it was all forgotten and the copies began accumulating dust. This 'rediscovered theorem' will now be written jointly with Solomon in which the quadruple cover of M_{22} and the standard subgroup problem of type $2M_{12}$ will also be treated. Aschbacher, Lyons, Smith, and Solomon found other 'rediscovered theorems'. Those are:

*) Aschbacher, M., Standard components of alternating type centralized by a 4-group.

*) Egawa, Y., Standard components of type M_{24} or $\Omega_8^+(2)$.

*) Goldschmidt, D., On the 2-exponent of a finite group.

These four rediscovered theorems were briefly discussed in my talk and its rather faithful notes, also very brief, presented by OHP format in the conference will be reproduced below.

(#1) Aschbacher (early1970's)
Standard components of alternating type centralized by a 4-group.

Assume :

t : involution.

$C_G(t) \simeq 2 \times 2 \times A_n \subset G$.

Then what can you say about G = ?

Examples.

* $G = A_{10}$.

$t = (12)(34)$.

$C_G(t) = (2 \times 2 \times A_6)2$. Here $(2 \times 2 \times A_6)2$ is an extension of the group $2 \times 2 \times A_6$ by an involutive automorphism.

** $G = Janko_2$.

t = noncentral involution.

$C_G(t) = 2 \times 2 \times A_5$.

*** $G = Aut(Janko_2)$.

t = same involution as in **.

$C_G(t) = (2 \times 2 \times A_5)2$.

**** $G = Aut(M_{12})$.

t = outside involution.

$C_G(t) = (2 \times 2 \times A_5)2$.

Theorem (Aschbacher, 2006)

Assume:

G : finite simple.
A : standard component.
$C_G(A)$: 2-rank > 1.
$A/Z(A) = A_n$.

Then,

(1). $A = A_5$ with $G = J_2$ or,

(2). $G = A_{n+4}$. ♦

A subgroup A of G is <u>standard,</u> if
(1). A is quasisimple,
(2). $K = C_G(A)$ is <u>tightly embedded,</u>
(3). $N_G(K) = N_G(A)$,
(4). $[A, A^g] \neq 1$.

A subgroup K of a finite group G is <u>tightly embedded</u> if $|K|$ = even, and $|K \cap K^g|$= odd unless $K = K^g$.

<u>Remark</u>. In general, cases like

$C_G(t) \approx 2 \times 2 \times L \subset G$

L = (almost, quasi) simple
G = simple

do not occur often.

<u>One more example</u>.

$C_G(t) \approx (2 \times 2 \times F_4(2))2 \subset \text{Fischer}_4 = B$.

Finkelstein's theorem (will be discussed later) eliminates most such cases.

(#2) Egawa (1980, Thesis)
Standard components of type M_{24} or $\Omega_8^+(2)$.

<u>Theorem</u>. Assume:

G : finite.
$L = M_{24}$ or $\Omega_8^+(2)$: standard subgroup and Sylow 2 subgroups of $C_G(L)$ cyclic.

Then $G = M_{24}, M_{24} \times M_{24}$;
$\Omega_8^+(2), \Omega_8^+(2) \times \Omega_8^+(2), \Omega_8^+(4), \text{Fischer}_1 = M(22)$. ♦

<u>Remark.</u>

Case : $L = M_{24}$ (1981, Comm. Algebra).

Case : $L = \Omega_8^+(2)$. No complete paper exists. Some related results appeared in Hokkaido Jouranl of Mathematics.

Pick $L \supset A = 2 \times 2 \times 2 \times 2 \times 2 \times 2 = E_{64}$ such that $N_L(A)/A = \Omega_6^+(2)$.

Put $B = \langle z, A \rangle = E_{128}$.

Then $N_G(B)/B \approx$
(1) $\Omega_6^+(2)$,
(2) $Sp_6(2)$, or
(3) $E_{64}\Omega_6^+(2)$.

(1) $\Rightarrow G \approx L = \Omega_8^+(2)$,
(2) $\Rightarrow G = M(22)$ = Fischer's 1st simple group, and
(3) $\Rightarrow G \approx (\Omega_8^+(2) \times \Omega_8^+(2))2$, $\Omega_8^+(4)$??? This part (3) is not completely written. Egawa intends to complete it this summer.

(#3) Goldschmidt (late 1960's) On the 2-exponent of a finite group.

Theorem. Gorenstein-Gilman (1975).

Assume:

G: finite group.
Syow 2-subgroup of class 2.

Then G is $L_2(q)$, A_7, $Sz(2^n)$, $U_3(2^n)$, $L_3(2^n)$, or $PSp_4(2^n)$, $n>1$. ♦

For the proof of the result of Gorenstein-Gilman, the following result of Goldschmidt was used (then unpublished).

Goldschmidt (1968).

Assume :

G : finite group.
S : Sylow 2-subgroup of class two.

Then, the center of S, Z(S), is elementary. ♦

Using this theorem of Goldschmidt, one can show easily that the exponent of S is 4. He was able to extend to the following:

Goldschmidt (2006, to appear)

Assume :

G : finite simple.
S : Sylow 2-subgroup of class $n > 1$.

Then, the exponent of Z(S) is at most 2^{n-1}. ♦

The following example shows that the theorem gives the best possible bound.

Example. S = a Sylow 2-subgroup of $L_3(q)$, $q \equiv 1 \pmod{2^n}$.

Then cl(S) = n +1 and exp(Z(S)) = n.

(#4) Harada (late 1970's) Finite groups having a component of type $2M_{22}$.

Theorem. No simple groups has centralizer of involution $\cong 2M_{22}$ or $2M_{22}2$. ♦

Here the notation such as $2M_{22}$ denotes the non-splitting central extension of the group of order 2 by M_{22}. A new paper will be written jointly with Ronald Solomon which includes a treatment of the standard component problem of type $2M_{12}$.

Schur multiplier of M_{22} changed its value as follows.

1966 Z_3.
1968 Z_6.
1979 Z_{12}.

Therefore $4M_{22}$ case must be treated.

Finkelstein (1977).

G : simple.
A : standard component.
Then, under some hypothesis, $|C_G(A)|_2 = 2$ must hold. ♦

The hypothesis mentioned in Finkelstein's theorem is:

A: quasisimple.
For any L where $A/Z(A) \subset L \subset Aut(A/Z(A))$, no involution t such that $C_L(t)$ has normal Z_4 or normal $Z_2 \times Z_4$.

If $A = 4M_{22}$, then, $A/Z(A) = M_{22}$. We need some information about the structure of the centralizer of an involution in $L = M_{22}$ or $Aut(M_{22})$.

$L = M_{22}$. Only one conjugate class of involutions in L.

$L = Aut(M_{22})$. Three conjugate classes of involutions in L.

It is easy to check that Finkelstein's criteria hold. Therefore, $4M_{22}$ case does not occur.

Next : $2M_{22}$, $Aut(2M_{22})$ cases.

Let T : Sylow 2-subgroup of $2M_{22}$ or $Aut(2M_{22})$.

Then $Z(T) = 2 \times 2$, the Klein's four group.

Therefore, it is possible that a Sylow 2-subgroup of G may be larger than T.
But we can argue that $|G|_2 = |C_G(t)|_2 = |T| = 2^8$ or 2^9.

Next consider $N_G(A)$,
$A = 2 \times 2 \times 2 \times 2 \times 2 \times 2 = E_{128}$, elementary abelian of order 2^6.

The structure forced on $N_G(A)$ contradicts the following result.

Harada-Yamaki (written in late 1970's but unpublished, to be submitted).

The classification of all irreducible subgroups of $GL_n(2)$, $n \leq 6$.

64 possible cases if n = 6,
18 cases if n = 4,
3 if n = 5.

Let X be an irreducible subgroup of $GL_6(2)$. Then, listing only 10 of 64 possible structures, we have:

(1). $X \cong Z_9$,
(2). $X \cong D_{18}$,
(3). $X \cong Q$, an extra special group of order 27 and of exponent 9,
(4). $X \cong Q \cdot Z_2$,
(5). $X \cong P$, an extra special group of order 27 and of exponent 3,
.....
(60). $X \cong G_2(2)) \cong Aut(U_3(3))$,
(61). $X \cong U_4(2))$,
(62). $X \cong Aut(U_4(2))$,
(63). $X \cong Sp_6(2)$, and
(64). $X \cong GL_6(2)$.

ON THE ZEROS OF HECKE TYPE FABER POLYNOMIALS

EIICHI BANNAI, KOJI KOJIMA AND TSUYOSHI MIEZAKI

Graduate School of Mathematics Kyushu University
Hakozaki 6-10-1 Higashi- ku, Fukuoka, 812-8581 Japan

Abstract. For any McKay-Thompson series which appear in Moonshine, the Hecke type Faber polynomial[1] $P_n(X)$ of degree n is defined . The Hecke type Faber polynomials are of course special cases of the Faber polynomials introduced by Faber a century ago. We first study the locations of the zeros of the Hecke type Faber polynomials of the 171 monstrous types, as well as those of the 157 non-monstrous types. We have calculated, by using computer, the zeros for all $n \leq 50$. These results suggest that in many (about 13 percent) of the cases, we can expect all the zeros of $P_n(x)$ are real numbers. In particular, we prove rigorously that the zeros of the Hecke type Faber polynomials (of any degree) for the McKay-Thompson series of type 2A are real numbers. We alse discuss the effect of the existence of harmonics, and the effect of so called dash operator. We remark that by the dash operators, we get many replicable functions (with rational integer coefficients) which are not necessarily completely replicable functions. Finally we study more closely, the curves on which the zeros of the Hecke type Faber polynomials for type 5B lie in particular in connection with the fundamental domain (on the upper half plane) of the group $\Gamma_0(5)$, which was studied by Shigezumi and Tsutumi. At the end, we conclude this paper by stating several observations and speculations.

Key Words and Phrases. McKay-Thompson series, Monster, Moonshine, Hauptmodul, modular group, twisted Hecke operator, replicable function, Faber polynomial, locating zeros.

2000 *Mathematics Subject Classification.* Primary 11F03; Secondary 20D08; Tertiary 30C15.

1. Introduction

Let $\mathbb{M}$ be the Monster group. Then, for each element $g \in \mathbb{M}$, a modular function $T_g(z)$, which is called a McKay-Thompson series, $T_g(z)$, is defined. It is known that

$$T_g(z) = \frac{1}{q} + \sum_{i=0}^{\infty} a_i(g)\, q^i,$$

where $q = e^{2\pi i z}$. The coefficients a_i are known empiricaly in conjunction with the following conjectures (i), (ii), which were first conjectured by McKay and Thompson [T1] from the similarity between the degrees of irreducible representations of the Monster and the coefficients of the elliptic modular function j.

(i)There exists a module $V = \bigoplus_{i \geq -1} V_i$ such that V_i are $\mathbb{M}$-invariant, $V_0 = 0$ and $j(q) - 744 = \sum_{i=-1}^{\infty} \dim V_i q^i$.

(ii)$T_g(z) = 1/q + \sum_{i=1}^{\infty} \chi_i(g)\, q^i$, where χ_i are the characters of $\mathbb{M}$ acting on V_i, is a modular function for some genus 0 subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{R})$, and is a generator of the function field of $\mathbb{H}^*/\Gamma$ (Hauptmodul).

Moreover, Conway and Norton gave the genus 0 subgroups concretely for each $g \in \mathbb{M}$. So, the above (i) and (ii) are called "Conway-Norton conjectures" also [CN], [TH].

[1]We originally called them Hecke polynomials, but since there already exists a concept with the same name (see e.g. Ihara[I]), we choose to call them Hecke type Faber polynomials.

Frenkel-Lepowsky-Meurman constructed V satisfying (i). And Richard Borcherds finally proved the Conway-Norton conjecture [B]. So the McKay-Thompson series is expressed as follows:

$$T_g(z) = \frac{1}{q} + \sum_{i=1}^{\infty} \chi_i(g)\, q^i,$$

where $\chi_i (i = 1, 2, \cdots)$ are called the head characters of $\mathbb{M}$.

$\mathbb{M}$ has 194 conjugacy classes, so 194 McKay-Thompson series exist. The character values of χ_i are integers. Namely, the V_i are rational representations. So χ_i are determined by the values on the conjugacy classes of the cyclic subgroups of $\mathbb{M}$. There are 172 cyclic subgroups in $\mathbb{M}$ up to conjugation. Moreover, 27A and 27B are non conjugate cyclic subgroups but give the same McKay-Thompson series. So, there are 171 McKay-Thompson series that are different from each other.

For example, the McKay-Thompson series for 1A and 2A are given as follows:

$$T_{1A}(z) = \frac{1}{q} + 196884q + 21493760q^2 + \cdots = j(q) - 744,$$

$$T_{2A}(z) = \frac{1}{q} + 4372q + 96256q^2 + \cdots,$$

where T_{1A} is equal to the elliptic modular function $j(z)$ whose constant term vanished. The genus 0 subgroup corresponding 2A is the Fricke group $\Gamma_0^*(2)$.

Now, there is an operator that acts on the McKay-Thompson series, called the twisted Hecke operator. For any McKay-Thompson series $T_g(z)$, it acts as follows, where the twisted Hecke operator $\widehat{T}$ is defined in §2 Definition 2.3. Then for each positive integer n the polynomial $P_n(X)$ is defined by

$$T_g(z)|\widehat{T}_n = \frac{1}{n} \sum_{\substack{ad=n \\ 0 \le b < d}} T_m^{(a)}\left(\frac{az+b}{d}\right) = \frac{1}{n} P_n(T_g(z)), \tag{1}$$

From now on, we call this polynomial $P_n(X)$ (or more precisely $P_{n,g}(X)$) the Hecke type Faber polynomial of degree n associated to $T_g(z)$. It is also characterized by the following relation.

$$P_n(T_m(z)) \equiv q^{-n} \pmod{q\mathbb{Z}[[q]]}. \tag{2}$$

A function $f = \sum_{i=-1}^{\infty} a_i q^i$ is called replicable if there exist a family of functions $\{f^{(a)} = \sum_{i=-1}^{\infty} a_i^{(a)} q^i\}_{a \in \mathbb{N}}$ called replicate functions of f satisfying the following equations:

$$f(z)|\widehat{T}_n = \frac{1}{n} \sum_{\substack{ad=n \\ 0 \le b < d}} f^{(a)}\left(\frac{az+b}{d}\right) = \frac{1}{n} P_n(f(z)). \tag{1'}$$

$$P_n(f(z)) \equiv q^{-n} \pmod{q\mathbb{Z}[[q]]}. \tag{2'}$$

Moreover, a replicable function whose replicate functions $f^{(a)} (a \in \mathbb{N})$ are all replicable is called a completely replicable function. It is known that all the McKay-Thompson series related to the Monster are completely replicable functions. On the other hand, it is known ([ACMS]) that there exist completely replicable functions which are not related to the Monster. We call them non monstrous McKay-Thompson series. All the non monstrous McKay-Thompson series whose coefficients are integers were determined in [ACMS]. The number of the non monstrous McKay-Thompson series are 157 including the ghost elements 25Z(=25a), 49Z(=49a), 50Z(=50a). The non monstrous McKay-Thompson series are also Hauptmoduls for some genus 0 subgroups of $SL_2(\mathbb{R})$.

Remark 1.1. *We explain some notation. If $T_g(z)$ is a monstrous McKay-Thompson series then g represents the conjugacy class of $\mathbb{M}$. We use the ATLAS notation of conjugacy classes which is used in* [CN]. *If $T_g(z)$ is non monstrous we use the notation which is used in* [ACMS], *that is,* 1a, 2a, $\cdots$. *Moreover, the Hecke type Faber polynomial of degree n related to $T_g(z)$ is denoted by $P_{n,g}(X)$.*

We have calculated, for all $n \le 50$, the zeros of Hecke type Faber polynomials. Since the space is limited, we illustrate them only for $n = 30$ in the APPENDIX of the present paper. In about 13% of the cases, all the zeros are real roots, and the other cases give interesting figures. More concretely, we have the following observation.

Observation 2.1.
(i) *Let $P_n(X)$ be a Hecke type Faber polynomial of the following type* : 1A, 2A, 2B, 3A, 3B, 4A, 4B, 4C, 5A, 6A, 6B, 6C, 6E, 7A, 8A, 8B, 8E, 9A, 10B, 12A, 12B, 12C, 12I, 14A, 18B, 21A, 28A, 30B, 40B, 60A.

1a, 1b, 6b, 6d, 8b, 9b, 12c, 12e, 16b, 18g, 24g, 24i, 27a, 32c. *Then the zeros of* $P_n(X)$ *for all* $n \leq 50$ *are real. Moreover, it is expected that the roots of* $P_n(X)$ *are all real for* $n \geq 50$.
(ii) *Let* $P_n(X)$ *be a Hecke type Faber polynomial of the following type* : 10D, 12H. 13A, 15C, 16C, 18C, 25A, 32B, 34A, 36A, 39A, 14c, 15a. *Then the zeros of* $P_n(X)$ *for all* $n \leq 50$ *are real except for some small* n. *Moreover, it is expected that the roots of* $P_n(X)$ *are all real for* $n \geq 50$.

In §3 we recall the properties of "harmonics" and "dash operator" for McKay-Thompson series. We first study the effect of the existence of harmonics to the location of the zeros of Hecke type Faber polynomials. Then, we study the effect of dash operators. An interesting thing is that the dash operator rotates the locations of the zeros of Hecke type Faber polynomials. In some cases, by applying the dash operator, a Hecke type Faber polynomial moves to a Hecke type Faber polynomial of another type, as is explained in ([FMN]) (we call these of completely replicable function type (c.r.f.)) Another interesting thing is that by applying the dash operator, we do not necessarily get a completely replicable function, but only a replicable function. Actually, we get many such replicable functions, which are not completely replicable functions (we call these of replicable function type (r.f.)) (It is expected that they also correspond to genus 0 subgroups of $SL_2(\mathbb{R})$.) We list all such cases in the following.

Observation 3.2. *The following table is the list of c.r.f. type polynomials, namely the image of the function under the dash operator is again a completely replicable function. (This list is due to* [FMN]. *A minor correction should be made in the list of* [FMN], *that is,* (40e, 80a) *should be* (40d, 80a).)

n=1:	(2B, 4A)	(6C, 12A)	(6E, 12B)	(10B, 20A)	(10E, 20C)	(14B, 28B)	(18C, 36A)
	(22B, 44A)	(30C, 60B)	(30G, 60C)				
n=2:	(1a, 2b)	(4C, 8a)	(4D, 8B)	(8D, 8E)	(8b, 8c)	(12E, 24b)	(12I, 24c)
	(12c, 24a)	(12d, 24A)	(16b, 16c)	(16c, 16f)	(16g, 16h)	(20D, 40B)	(20d, 40a)
	(24D, 24h)	(24d, 24e)	(24f, 24g)	(24i, 24j)	(28C, 56a)	(32c, 32d)	(36f, 72a)
	(40b, 40c)	(44b, 88A)	(48a, 48b)	(48c, 48d)	(48e, 48f)	(56b, 56c)	(60a, 120a)
	(72c, 72d)						
n=3:	(6F, 12D)	(18D, 36B)	(18e, 36b)	(42C, 84C)			
n=4:	(8F, 16a)	(16B, 16d)	(40d, 80a)				
n=6:	(12J, 24E)	(36e, 72b)					
n=8:	(32c, 64a)						
n=12:	(24J, 48g),						

where n *is the level of dash operator (defined later). If* (g, h) *is level* n *then the zeros of* $P_{m,g}$ *and* $P_{m,h}$ *are transformed to each other by the rotation of* π/n. □

Observation 3.3. *The following table is the list of r.f. type, namely the image of the function under the dash operator is not completely replicable function. In other words,* $T_g|'$ *is not a McKay-Thompson series of one of the 171+157 completely replicable functions.*

n=1:	(1A)	(2A)	(3A)	(3B)	(5A)	(5B)	(5a)
	(6A)	(6B)	(6D)	(6d)	(7A)	(7B)	(8A)
	(9A)	(9b)	(9d)	(10A)	(10C)	(10D)	(10b)
	(11A)	(12H)	(13A)	(13B)	(14A)	(14C)	(15A)
	(15B)	(15C)	(15a)	(15b)	(16C)	(17A)	(18A)
	(18B)	(18E)	(18a)	(18h)	(18j)	(19A)	(20F)
	(21A)	(21B)	(21D)	(22A)	(23A)	(24B)	(24C)
	(24I)	(25A)	(25a)	(26A)	(26B)	(27A)	(27a)
	(29A)	(30A)	(30B)	(30D)	(30F)	(30b)	(30e)
	(31A)	(32A)	(33A)	(33B)	(34A)	(35A)	(35B)
	(35a)	(36D)	(38A)	(39A)	(39C)	(41A)	(42A)
	(42B)	(42D)	(42c)	(45A)	(45a)	(46A)	(46C)
	(47A)	(49a)	(50A)	(50a)	(51A)	(54A)	(54a)
	(55A)	(56A)	(59A)	(60D)	(62A)	(66A)	(66B)
	(69A)	(70A)	(70B)	(71A)	(78A)	(78B)	(87A)
	(90a)	(92A)	(94A)	(95A)	(105A)	(110A)	(119A)
n=2:	(2a)	(4B)	(4a)	(6a)	(6b)	(6c)	(10a)
	(10c)	(12C)	(12F)	(12G)	(12a)	(12b)	(12e)
	(12f)	(14a)	(14b)	(14c)	(16A)	(18c)	(18f)
	(18g)	(20B)	(20E)	(20a)	(20b)	(20c)	(20e)

	(22a)	(24H)	(26a)	(28A)	(28D)	(28a)	(30a)
	(30c)	(30d)	(30f)	(32B)	(34a)	(36C)	(36a)
	(36c)	(36d)	(36h)	(36i)	(38a)	(40C)	(42a)
	(42b)	(42d)	(44a)	(44c)	(48A)	(52A)	(52B)
	(52a)	(58a)	(60A)	(60E)	(60b)	(60c)	(60d)
	(60e)	(66a)	(68A)	(70a)	(76a)	(82a)	(84A)
	(84B)	(84a)	(102a)	(132a)	(140a)		
n=3:	(3C)	(9B)	(9a)	(9c)	(15D)	(18d)	(21C)
	(27b)	(27c)	(27d)	(27e)	(30E)	(39B)	(45b)
	(45c)	(54b)	(57A)	(63a)	(90b)	(93A)	(117a)
n=4:	(8C)	(24F)	(24G)	(32b)	(40A)	(40c)	(48h)
	(56B)	(104A)					
n=6:	(18b)	(18i)	(36g)	(54c)	(54d)	(60F)	(126a)
n=8:	(32a)						
n=12:	(72c)						
n=24:	(96a)						

where n is the level of the dash operator (defined later). If the type g is in the above list (for example 1A), $T_g|'$ is not a completely replicable function but a replicable function in most of the cases. However, if $n = 8$ or 24 (i.e., a multiple of 8), they are not even replicable functions. In other words, $T_g|'$ is not a McKay-Thompson series of one of the 171+157 completely replicable functions. But the following facts hold. If (g) is level n then the zeros of $P_{m,g}$ and $P_{m,g|'}$ are transformed each other by the rotation π/n. (This ensures the construction of many new replicable functions with rational integral coefficients.)

In §4, following the method of [AKN], where they showed that all the zeroes of Hecke type Faber polynomials related to 1A$\in \mathbb{M}$ are real, we show that the following result for 2A$\in \mathbb{M}$. That is,

Theorem 4.1. *For each n, all the zeros of the Hecke type Faber polynomial $P_{n,2A}(X)$ are real.*

In §5 we treat the case of 5B $\in \mathbb{M}$ more carefully since 5B is the first case where the curve on which the zeros of Hecke type Faber polynomials lie is a delicate shape. The modular forms and related topics of $\Gamma_0(5)$ are studied by Sigezumi [S2] and Tsutsumi [T2]. We observe that this curve is the image by the map T_{5B} of the boundary of the fundamental region considered by them. In §6, we state some speculations and conjectures.

2. Zeros of Hecke type Faber polynomial

2.1. Preliminaries.

Definition 2.1 (Hecke operator, see [S1]). *The Hecke oprators $T_n(= 1, 2, 3, \cdots)$ related to $\mathrm{SL}_2(\mathbb{Z})$ are defined as follows: for any $f(z) \in M_k(\mathrm{SL}_2(\mathbb{Z}))$,*

$$(f|_k T(n))(z) := n^{k-1} \sum_{\substack{ad=n, d>0 \\ 0\le b\le d-1}} d^{-k} f\left(\frac{az+b}{d}\right)$$

$$= \sum_{m\in\mathbb{Z}} \left(\sum_{0<d|(m,n)} d^{k-1} a\left(\frac{mn}{d^2}\right)\right) q^m. \tag{3}$$

Example 2.1 (1A). *By the q-expansion (3),*

$$(T_{1A}|_0 T(n))(z) = \frac{1}{n} \sum_{\substack{ad=n, d>0 \\ 0\le b\le d-1}} T_{1A}\left(\frac{az+b}{d}\right) \equiv \frac{1}{q^n} \pmod{q\mathbb{Z}[[q]]}.$$

Because the middle term is $\mathrm{SL}_2(\mathbb{Z})$-invariant (since $\mathrm{SL}_2(\mathbb{Z})$ acts as permutation of elements of summation). $(T_{1A}|_0 T(n))(z)$ is expressed by a polynomial of $T_{1A}(z)$.

$$(T_{1A}|_0 T(n))(z) = \frac{1}{n} P_{n,1A}((T_{1A}(z))).$$

Next, we define replicable functions.

Definition 2.2 (replicable function, replicate level, see [ACMS]). *A McKay-Thompson series*

$$T_m(z) = \frac{1}{q} + \sum_{i=1}^{\infty} a_i q^i$$

is a replicable function if and only if there exists a family of functions $T_m^{(a)}$ for $a \in \mathbb{N}$ of the following form :

$$T_m^{(a)}(z) = \frac{1}{q} + \sum_{i=1}^{\infty} a_i^{(a)} q^i, \quad a \in \mathbb{N}$$

such that

$$\sum_{\substack{ad=n \\ 0 \le b < d}} T_m^{(a)}\left(\frac{az+b}{d}\right) = P_n(T_m(z)), \tag{4}$$

$$\equiv q^{-n} \pmod{q\mathbb{Z}[[q]]}. \tag{5}$$

$T_m^{(a)}$ is called the a-th replicate function.

When there exists an $n \in \mathbb{N}$ which satisfies the equation,

$$T_m^{(\gcd(n,k))} = T_m^{(k)} \quad (\forall k \ge 1),$$

n is called the replicate level. □

Definition 2.3 (twisted Hecke operator, Hecke type Faber polynomial, see [ACMS]). *We define for each n, the left side of (4) as $n(T_m|\widehat{T})$, and call $\widehat{T}$ twisted Hecke operator. We call P_n in (4) Hecke type Faber polynomial. Especially, if $f(z)$ is $T_m(z)$, then we write $P_{n,m}$.*

If all the replicate functions $f^{(a)}(z)$ are replicable, then $f(z)$ is called a completely replicable function. It is known that for every $m \in \mathbb{M}$, $T_m(z)$ are completely replicable functions, that is, their replicate functions are also replicable functions.

Next lemma is useful to calculate the replicate functions.

Lemma 2.1. [ACMS] *Let p be a prime number and let f be a replicable function. Then the following equation holds.*

$$f^{(p)}(pz) = P_{p,m}(f(z)) - pf(z)|U_p.$$

where U_p is the operator, $U_p : a_n q^n \mapsto a_{pn} q^n$.

Example 2.2. *When $p = 2$,*

$$\begin{aligned} T_{2A}^{(2)}(2z) &= P_{2,2A}(T_{2A}(z)) - 2T_{2A}(z)|U_2 \\ &= \frac{1}{q^2} + 196884q^2 + 21493760q^4 + \cdots \\ &= T_{1A}(2z) \end{aligned}$$

Therefore, $T_{2A}^{(2)} = T_{1A}$. The replicate level of 2A is 2, that is, the replicate functions are as follows:

$$T_{2A}^{(n)} = \begin{cases} T_{1A}. & n : \text{even} \\ T_{2A}. & n : \text{odd} \end{cases}$$

2.2. **Method of Calculation of the zeros of Hecke type Faber polynomials $P_n(X)$.** We calculated the Hecke type Faber polynomial and their zeros by two methods.

(i) The first 50(resp. 23) q-coefficients of monstrous (resp. non monstrous) McKay-Thompson series are caluculated in [MS](resp. [FMN]). We caluculated the Hecke type Faber polynomials using (5). More concretely, for Hecke type Faber polynomial $P_n(X) = X^n + a_1 X^{n-1} + \cdots + a_n$, we put b_n as follows,

$$P_n(T_g(q)) = \frac{1}{q} + \frac{b_{-(n-1)}}{q} + \frac{b_{-(n-2)}}{q} + \cdots + \frac{b_{-1}}{q} + b_0 + b_1 q + b_2 q^2 + \cdots,$$

where b_n are linear sums of the coefficients a_i, $1 \leq i \leq n$ of Hecke type Faber polynomial. Then we solve the following linear equations :

$$\begin{cases} b_{-(n-1)} = 0 \\ b_{-(n-2)} = 0 \\ \vdots \\ b_0 = 0. \end{cases}$$

Next we caluculated their zeros by Maple (the command "solve"). By this method, we caluculated the zeros of monstrous (resp. non monstrous) Hecke type Faber polynomial for $n \leq 50$ (resp. 23)

(ii) We use the following facts [ACMS]: For McKay-Thompson series $T_g^{(a)}(q) = \sum_{i=1}^{\infty} a_i^{(a)}(q)$, $k \geq 1$,

$$a_{4k} = a_{2k+1} + \sum_{j=1}^{k-1} a_j a_{2k-j} + \frac{1}{2}(a_k^2 - a_k^{(2)}),$$

$$a_{4k+1} = a_{2k+3} + \sum_{j=1}^{k} a_j a_{2k+2-j} + \frac{1}{2}(a_{k+1}^2 - a_{k+1}^{(2)}) + \frac{1}{2}(a_{2k}^2 + a_{2k}^{(2)})$$
$$- a_2 a_{2k} + \sum_{j=1}^{k-1} a_j^{(2)} a_{4k-4j} + \sum_{j=1}^{2k-1} (-1)^j a_j a_{4k-j},$$

$$a_{4k+2} = a_{2k+2} + \sum_{j=1}^{k} a_j a_{2k+1-j},$$

$$a_{4k+3} = a_{2k+4} + \sum_{j=1}^{k+1} a_j a_{2k+3-j} - \frac{1}{2}(a_{2k+1}^2 - a_{2k+1}^{(2)})$$
$$- a_2 a_{2k+1} + \sum_{j=1}^{k} a_j^{(2)} a_{4k+2-4j} + \sum_{j=1}^{2k} (-1)^j a_j a_{4k+2-j}.$$

These equations are generalizations of Mahler recurrence relations [M1]. The above facts imply that if we know a_1, a_2, a_3, a_5 and the coefficients of $T_g^{(2)}(q)$ then the McKay-Thompson series are calculable. In [CN](resp. [ACMS]), the 2nd replicate function of monstrous (resp. non monstrous) type are explicitly given. So all the McKay-Thompson series are calculable. Morever, the coefficients of the McKay-Thompson series are calculable by 12 coefficients $(a_1, a_2, a_3, a_4, a_5, a_7, a_8, a_9, a_{11}, a_{17}, a_{19}, a_{23})$(See [FMN]) recursively. Finally, we check on these calculations. Using these equation, we calculate the Hecke type Faber polynomial using (5) and their zeros by Mathematica (for all $n \leq 50$).

The Hecke type Faber polynomial $P_n(X)$ have the following recurrence relations(See [ACMS]):

$$P_0(X) = 1, \quad ra_{r-1} + \sum_{k=-1}^{r-2} a_k P_{r-k-1}(X) = X P_{r-1}(X), \quad r = 1, 2, \cdots \tag{6}$$

In addition, we compared the coefficients of the McKay-Thompson series calculated by the two methods above with the coefficients obtained by other methods, say in [CN], [K3], which give other expressions using the η function and theta series of certain lattices as much as possible and check the Hecke type Faber polynomial calculated by above two methods with that of calculated by recurrence relations (6). Thus, we are convinced that the results of these calculations are correct.

In the appendix, we show the pictures of the location of the zeros for $n = 30$.

2.3. **Classification.** We classified the graphics of zeros of $P_{n,m}(X)$ into the following types, All real, All imaginary, 2 lines, 3 arrows, 3 lines, Almost real and Others. We remark that when the cases All real we checked that the observations here are completely rigorous (for $n \leq 50$) by Sturm's theorem. But some of the observations here are not completely rigorous, in particular when the cases of 3 arrows or 3 lines, say. In these cases, we concluded the results only by our human eyevision. Note that the 3 arrows or 3 lines means that the 3 arrows or 3 lines may be straight or may be curved.

Monstrous type:

Type	*Number of types*	*Name*
All real	30	1A, 2A, 2B, 3A, 3B, 4A, 4B, 4C, 5A, 6A, 6B, 6C, 6E, 7A, 8A 8B, 8E, 9A, 10B, 12A, 12B, 12C, 12I, 14A, 18B, 21A, 28A, 30B 40B, 60A
All imaginary	3	4D, 8D, 20D
2 lines	8	8C, 8F, 12E, 12F, 16A, 16B, 20B, 36C
3 arrows	8	3C, 5B, 6D, 6F, 7B, 9B, 10C, 12D
3 lines (Hexagonal)	5	12J, 24E, 48A, 52B, 60E
Almost real	11	10D, 12H, 13A, 15C, 16C, 18C, 25A, 32B, 34A, 36A, 39A
Others	106	

Non monstrous type:

Type	*Number of types*	*Name*
All real	15	1a, 1b, 6b, 6d, 8b, 9b, 12c, 12e, 16b, 18g, 20b, 24g, 24i, 27a, 32c
All imaginary	19	2a, 2b, 4a, 6a, 6c, 8a, 8c, 12a, 12d, 12f, 14a, 16c, 18f, 20a, 24a 24c, 24f, 24j, 32d
2 lines	24	10a, 12b, 16a, 16d, 16g, 16h, 18c, 20d, 24b, 24d, 24e, 28a, 40a 40d, 42a, 42b, 48a, 48b, 48c, 48d, 56b, 56c, 60b, 80a
3 arrows	14	5a, 9a, 9c, 15b, 18a, 18d, 18e, 27d, 30b, 30e, 36b, 54a, 90a, 90b
3 lines (Hexagonal)	5	18b, 18i, 36e, 54d, 72b
Almost real	2	14c, 15a
Others	78	

3. Harmonic. Dash operator

3.1. **Harmonic.** Let t_m be $T_m + C$, where C is a constant. The appropriate constant term is defined by [CN].

Remark 3.1. *We remark that the zeros of a Hecke type Faber polynomial with the constant term C added to T_m are shifted by $-C$. So the figure of zeros does not changed essentially.* □

Definition 3.1. (Harmonic, [CN]) *t_m is called the d-th harmonic of $t_{m'}$, if the following equation holds,*

$$t_{m'}(z) = (t_m(dz))^{1/d}. \tag{7}$$

□

Example 3.1 (1A⟶3C). *t_{1A} and t_{3C} are given as follows :*

$$t_{1A}(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$
$$t_{3C}(z) = \frac{1}{q} + 248q^2 + 4124q^5 + 34752q^8 + \cdots.$$

Since the following relation

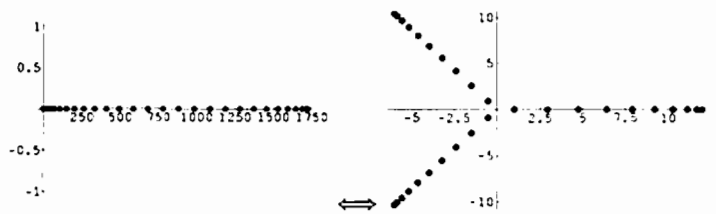
$$t_{3C}(z) = (t_{1A}(3z))^{1/3} \tag{8}$$

holds, t_{3C} is the 3-rd harmonic of t_{1A}.

We give the Hecke type Faber polynomials of t_{1A} and t_{3C} for the first 6 degrees.

$$P_{1,1A}(X) = X - 744$$
$$P_{2,1A}(X) = X^2 - 1488X + 159768$$
$$P_{3,1A}(X) = X^3 - 2232X^2 + 1069956X - 36866976$$
$$P_{4,1A}(X) = X^4 - 2976X^3 + 2533680X^2 - 561444608X + 8507424792$$
$$P_{5,1A}(X) = X^5 - 3720X^4 + 4550940X^3 - 2028551200X^2 + 246683410950X - 1963211493744$$
$$P_{6,1A}(X) = X^6 - 4464X^5 + 7121736X^4 - 4850017536X^3 + 1304194222980X^2 - 96687754014528X + 453039686271072$$
$$P_{1,3C}(X) = X$$
$$P_{2,3C}(X) = X^2$$
$$P_{3,3C}(X) = X^3 - 744$$
$$P_{4,3C}(X) = X^4 - 992X$$
$$P_{5,3C}(X) = X^5 - 1240X^2$$
$$P_{6,3C}(X) = X^6 - 1488X^3 + 159768$$

From (8), *it is easy to prove that for* $n \equiv 0 \pmod 3$ *the relation* $P_{n/3,1A}(X^3) = P_{n,3C}(X)$ *holds. So for* $n \equiv 0 \pmod 3$ *the roots of* $P_{n,3C}(X)$ *are the cubic roots of the roots of* $P_{n/3,1A}(X)$. *The following figures are the roots of* $P_{30,1A}(X)$ *and* $P_{30,3C}(X)$.



1A 3C

For $n \not\equiv 0 \pmod 3$, it seems that the relation between the roots of $P_{n,3C}(X)$ and those of $P_{n,1A}(X)$ is not so simple. But it is conjectured that the roots of $P_{n,3C}(X)$ are all located on the 3 lines through the origin with argument $0, (2/3)\pi, (4/3)\pi$, respectively.

Example 3.2 (2A⟶4B). *t_{2A} and t_{4B} are given as follows*:

$$t_{2A}(z) = \frac{1}{q} + 104 + 4372q + 96256q^2 + \cdots,$$
$$t_{4B}(z) = \frac{1}{q} + 52q^1 + 834q^3 + 4760q^5 + \cdots,$$

Since the following relation

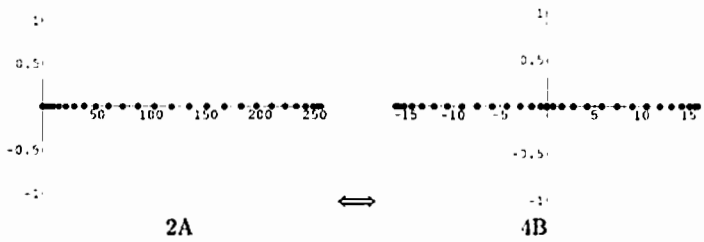
$$t_{4B}(z) = (t_{2A}(2z))^{1/2} \tag{9}$$

holds, t_{4B} is the 2-nd harmonic of t_{2A}.

We give the Hecke type Faber polynomials of t_{2A} and t_{4B} for the first 6 degrees.

$$
\begin{aligned}
P_{1,2A}(X) &= X - 104\\
P_{2,2A}(X) &= X^2 - 208X + 2072\\
P_{3,2A}(X) &= X^3 - 312X^2 + 19332X - 49568\\
P_{4,2A}(X) &= X^4 - 416X^3 + 47408X^2 - 1246976X + 1146904\\
P_{5,2A}(X) &= X^5 - 520X^4 + 86300X^3 - 4909600X^2 + 65094150X - 26542704\\
P_{6,2A}(X) &= X^6 - 624X^5 + 136008X^4 - 12162304X^3 + 397216644X^2 - 2958154560X\\
&\quad + 614211680\\
P_{1,4B}(X) &= X\\
P_{2,4B}(X) &= X^2 - 104\\
P_{3,4B}(X) &= X^3 - 156X\\
P_{4,4B}(X) &= X^4 - 208X^2 + 2072\\
P_{5,4B}(X) &= X^5 - 260X^3 + 9350X\\
P_{6,4B}(X) &= X^6 - 312X^4 + 19332X^2 - 45968
\end{aligned}
$$

From (9), *it is easy to prove that for* $n \equiv 0 \pmod 2$ *the relation* $P_{n/2,2A}(X^2) = P_{n,4B}(X)$ *holds. So for* $n \equiv 0 \pmod 2$ *the roots of* $P_{n,4B}(X)$ *are the square roots of the roots of* $P_{n/2,2A}(X)$. *The following figures are the roots of* $P_{30,2A}(X)$ *and* $P_{30,4B}(X)$.



For $n \not\equiv 0 \pmod 2$, it seems that the relation between the roots of $P_{n,4B}(X)$ and those of $P_{n,2A}(X)$ is not so simple. But it is conjectured that the roots of $P_{n,4B}(X)$ are all located on the real interval $[-16, 16]$ i.e., equivalently the 2 lines through the origin with argument $0, \pi$, respectively.

Example 3.3 (2A⟶8C). t_{2A} *and* t_{8C} *are given as follows* :

$$
\begin{aligned}
t_{2A}(z) &= \frac{1}{q} + 104 + 4372q + 96256q^2 + \cdots,\\
t_{8C}(z) &= \frac{1}{q} + 26q^3 + 79q^7 + 326q^{11} + \cdots,
\end{aligned}
$$

Since the following relation

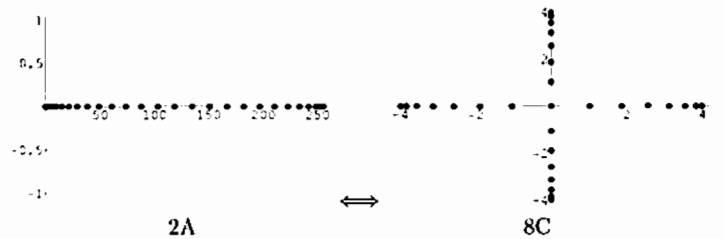
$$t_{8C}(z) = (t_{2A}(4z))^{1/4} \tag{10}$$

holds, t_{8C} *is the 4-th harmonic of* t_{2A}.

We give the Hecke type Faber polynomials of t_{2A} and t_{8C} for the first 6 degrees.

$$
\begin{aligned}
P_{1,2A}(X) &= X - 104 \\
P_{2,2A}(X) &= X^2 - 208X + 2072 \\
P_{3,2A}(X) &= X^3 - 312X^2 + 19332X - 49568 \\
P_{4,2A}(X) &= X^4 - 416X^3 + 47408X^2 - 1246976X + 1146904 \\
P_{5,2A}(X) &= X^5 - 520X^4 + 86300X^3 - 4909600X^2 + 65094150X - 26542704 \\
P_{6,2A}(X) &= X^6 - 624X^5 + 136008X^4 - 12162304X^3 + 397216644X^2 - 2958154560X \\
&\quad + 614211680 \\
P_{1,8C}(X) &= X \\
P_{2,8C}(X) &= X^2 \\
P_{3,8C}(X) &= X^3 \\
P_{4,8C}(X) &= X^4 - 104 \\
P_{5,8C}(X) &= X^5 - 130X \\
P_{6,8C}(X) &= X^6 - 156X^2
\end{aligned}
$$

From (10), *it is easy to prove that for* $n \equiv 0 \pmod 4$ *the relation* $P_{n/4,2A}(X^4) = P_{n,8C}(X)$ *holds. So for* $n \equiv 0 \pmod 4$ *the roots of* $P_{n,8C}(X)$ *are the quartic roots of the roots of* $P_{n/4,2A}(X)$. *The following figures are the roots of* $P_{30,2A}(X)$ *and* $P_{30,8C}(X)$.



For $n \not\equiv 0 \pmod 4$, it seems that the relation between the roots of $P_{n,8C}(X)$ and those of $P_{n,2A}(X)$ is not so simple. But it is conjectured that the roots of $P_{n,8C}(X)$ are all located on the 4 lines through the origin with argument $0, (1/2)\pi, \pi, (3/2)\pi$, respectively.

By the figure of the zeros, it is conjectured that if t_m is the d-th harmonic of $t_{m'}$ the roots of $P_{n,m'}(X)$ are the d-th root of the roots of $P_{n/d,m}(X)$. If $n \equiv 0 \pmod d$, it is easy to prove from (7). If $n \not\equiv 0 \pmod d$, it is not correct. But supposing the roots of $P_{n/d,m}(X)$ are in $\mathbb{R}$, it is conjectured that the roots of $P_{n,m'}(X)$ are the d-th roots of some real numbers.

Conjecture 3.1. *If t_m is the d-th harmonic of $t_{m'}$ and the roots of $P_{n/d,m}(X)$ are all in $\mathbb{R}$, then all the roots of $P_{n,m'}(X)$ are the d-th root of some real numbers.*

3.2. Dash operator.

Definition 3.2. (Dash operator, [FMN]) *The dash operator are change the sign of every 2n-th term starting with the coefficient of q^{n-1}, where n is the largest number such that all coefficients other than those of q^{kn-1} are zero. We call such n the level of the dash operator.*

By the form of Hecke type Faber polynomials, it is easily proved that, by the action of the dash operator, the roots of $P_{n,m}(X)$ are rotated in the complex plane around the origin by the following

angle.

$$\begin{aligned} n = 1 &\longleftarrow \pi \\ n = 2 &\longleftarrow \pi/2 \\ n = 3 &\longleftarrow \pi/3 \\ n = 4 &\longleftarrow \pi/4 \\ n = 6 &\longleftarrow \pi/6 \\ n = 8 &\longleftarrow \pi/8 \\ n = 12 &\longleftarrow \pi/12 \\ n = 24 &\longleftarrow \pi/24 \end{aligned}$$

Remark 3.2. *By the definition of the dash operator, for any McKay-Thompson series $T_g(z)$, the following equation holds : $(T_g(z)|')|' = T_g(z)$. So, the zeros of the Hecke type of Faber polynomial of $(T_g(z)|')|'$ are equal to those of $(T_g(z)$.*

Example 3.4. *$T_{2B}(z)$ is given as follows :*

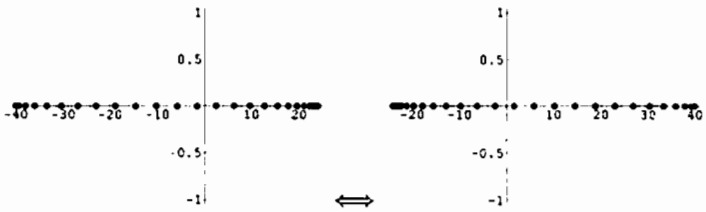
$$T_{2B}(z) = \frac{1}{q} + 276q - 2048q^2 + 11202q^3 - 49152q^4 + 184024q^5 - \cdots .$$

Since the level of T_{2B} is 1, $T_{2B}(z)|'$ is given as follows :

$$T_{2B}(z)|' = \frac{1}{q} + 276q + 2048q^2 + 11202q^3 + 49152q^4 + 184024q^5 + \cdots .$$

So the next relation holds.

$$T_{2B}(z)|' = T_{4A}(z).$$



2B $\Longleftrightarrow$ 4A

Example 3.5. *$T_{4D}(z)$ is given as follows :*

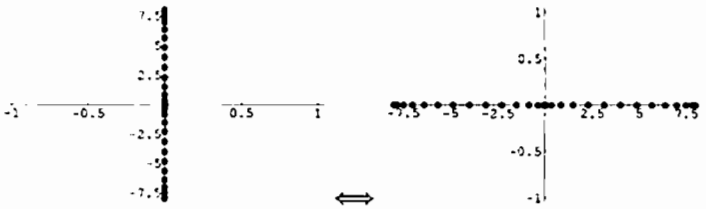
$$T_{4D}(z) = \frac{1}{q} - 12q + 66q^3 - 232q^5 + \cdots .$$

Since the level of T_{4D} is 2, $T_{4D}(z)|'$ is given as follows :

$$T_{4D}(z)|' = \frac{1}{q} + 12q + 66q^3 + 232q^5 + \cdots .$$

So the next relation holds.

$$T_{4D}(z)|' = T_{8B}(z).$$



4D $\Longleftrightarrow$ 8B

Example 3.6. *$T_{12J}(z)$ is given as follows :*

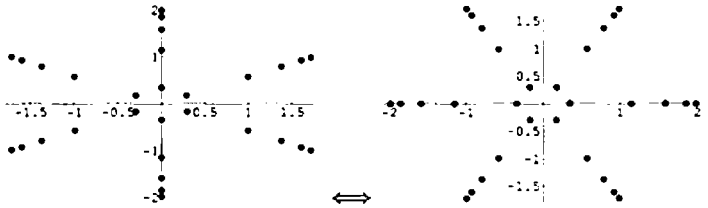
$$T_{12J}(z) = \frac{1}{q} - 4q^5 + 6q^{11} - 8q^{17} + \cdots .$$

Since the level of T_{12J} *is 6, the* $T_{12J}(z)|'$ *is given as follows* :

$$T_{12J}(z)|' = \frac{1}{q} + 4q^5 + 6q^{11} + 8q^{17} + \cdots .$$

So the next relation holds.

$$T_{12J}(z)|' = T_{24E}(z).$$



12J ⟺ 24E

4. 2A

Definition 4.1 (Fricke group). *The Fricke group is defined by the following : for any prime p,*

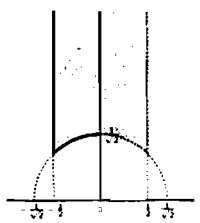
$$\Gamma_0^*(p) := \Gamma_0(p) \cup \Gamma_0(p) W_p,$$

where

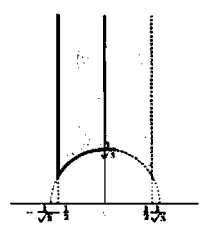
$$\Gamma_0^*(p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) ; c \equiv 0 \pmod{p} \right\}, \ W_p := \begin{pmatrix} 0 & -1/\sqrt{p} \\ \sqrt{p} & 0 \end{pmatrix}$$

The following figures are the fundamental domains of $\mathrm{SL}_2(\mathbb{Z})$, Fricke group $\Gamma_0^*(2)$ and $\Gamma_0^*(3)$, respectively.

$\mathrm{SL}_2(\mathbb{Z})$
FIGURE 1



$\Gamma_0^*(2)$
FIGURE 2



$\Gamma_0^*(3)$
FIGURE 3

Let C be the following part of the boundary of the fundamental domain of $\Gamma_0^*(2)$,

$$C = \left\{ z \in \mathbb{H} \,\middle|\, |z| = \frac{1}{\sqrt{2}}, 0 \le \Re(z) \le \frac{1}{2} \right\}.$$

We consider the next function :

$$F_n(z) = P_{n,2A}(T_{2A}(z)).$$

The map $z \mapsto T_{2A}(z)$ gives a bijection from the fundamental domain to $\mathbb{C}$. Moreover, this map moves the curve C to the interval $[-104, 152]$. In paticular, $F_n(z)$ is real on C, because the coefficients of

$P_{n,2A}(T_{2A}(z))$ are rational numbers. Since $P_{n,2A}$ is a polynomial, in order to prove Theorem 4.1, it is sufficient to show that the $F_n(z)$ has at least $n-1$ zeros on C.

So, we show the following lemma.

Lemma 4.1. *Let $z_0 = x_0 + y_0 \in C$. Then we have*

$$\left|F_n(z_0)e^{-2\pi n y_0} - 2\cos(2\pi n x_0)\right| < 2.$$

This lemma means that the sign of $F_n(z)$ changes in each part of

$$\frac{\nu-1}{2n} < \Re(z) < \frac{\nu}{2n}, \quad \nu = 1, 2, \ldots, n-1,$$

so, $F_n(z)$ has at least $n-1$ zeros on C.

Proof of Lemma 4.1. The fundamental domain of $\Gamma_0^*(2)$ is

$$D = \left\{ z \in \mathbb{H} \;\middle|\; |z| \geq \frac{1}{\sqrt{2}}, |\Re(z)| \leq \frac{1}{2} \right\}.$$

By the left hand side of (4),

$$F_n(z) = \sum_{\substack{ad=n \\ 0 \leq b < d}} T_m^{(a)}\left(\frac{az+b}{d}\right).$$

However, by Example 2.2, we have

$$F_n(z) = \sum_{\substack{ad=n \\ 0 \leq b < d \\ n:odd}} T_{2A}\left(\frac{az+b}{d}\right) + \sum_{\substack{ad=n \\ 0 \leq b < d \\ n:even}} T_{1A}\left(\frac{az+b}{d}\right). \tag{11}$$

Let M be the maximum of $\left|T_m^{(a)}((az+b)/d) - e^{2\pi i z}\right|$ in $\bar{D}$, i.e.,

$$M := \max\left\{ \max_{z \in D}\left|T_{2A}\left(\frac{az+b}{d}\right) - e^{2\pi i z}\right|, \max_{z \in D}\left|T_{1A}\left(\frac{az+b}{d}\right) - e^{2\pi i z}\right| \right\}.$$

Because the Fourier coefficients of T_{1A}, T_{2A} are positive, the following estimate provides $M < 286729$.

$$\begin{aligned}
\left|T_{2A}\left(\frac{az+b}{d}\right) - e^{2\pi i z}\right| &\leq \sum_{n \geq 1} c_n |q|^n \\
&= \sum_{n \geq 1} c_n e^{-2\pi \Im(z) n} \\
&\leq \sum_{n \geq 1} c_n e^{-2\pi \frac{1}{2} n} \\
&= \left|T_{2A}\left(\frac{i}{2}\right) - e^{-2\pi i \frac{1}{2}}\right| \\
&= 520.858\cdots < 521.
\end{aligned}$$

$$\left|T_{1A}\left(\frac{az+b}{d}\right) - e^{2\pi i z}\right| \leq 286728.859\cdots < 286729.$$

For any $z \in \mathbb{H}$, let $z^* \in D$ denote the equivalent point under the action of the corresponding group. From now on, for each term of (11), $z_0 = x_0 + y_0 \in C$ and $n \geq 2$, we show the following inequalities.

(i) $\left|T_{1A}(nz_0) - e^{-2\pi i n z_0}\right| \leq M.$

(ii) $\left|T_{2A}\left(\frac{z_0}{n}\right) - e^{-2\pi i n z_0}\right| \leq M.$

(iii) $\frac{az_0+b}{d}$ is different from, nz_0, $\frac{z_0}{n}$, $\frac{z_0+n-1}{n}$, then,
$\left|T_{1A}\left(\frac{az_0+b}{d}\right)\right| \leq e^{\pi n y_0} + M.$

The next estimate which is based on $nz_0 - (nz_0)^* \in \mathbb{Z}$, proves inequality (i).

$$\left|T_{1A}(nz_0) - e^{-2\pi i n z_0}\right| = \left|T_{1A}((nz_0)^*) - e^{-2\pi i (nz_0)^*}\right| \leq M.$$

For (ii), we note that

$$\begin{pmatrix} 0 & -1/\sqrt{2} \\ \sqrt{2} & 0 \end{pmatrix} \frac{z_0}{n} = -\frac{n}{2z_0} \text{ and } \frac{1}{z_0} = 2\bar{z}_0.$$

By $-n/(2z_0) - (z_0/n)^* \in \mathbb{Z}$,

$$\begin{aligned} \left| T_{2A}\left(\frac{z_0}{n}\right) - e^{2\pi i n \bar{z}_0} \right| &= \left| T_{2A}\left(-\frac{n}{2z_0}\right) - e^{-2\pi i(-n/2z_0)} \right| \\ &= \left| T_{2A}\left(\left(\frac{z_0}{n}\right)^*\right) - e^{-2\pi i(z_0/n)^*} \right| \leq M. \end{aligned}$$

So inequality (ii) holds. For the proof of (iii), we set

$$z = \frac{az_0 + b}{d} \text{ and } z^* = \frac{\alpha z + \beta}{\gamma z + \delta}.$$

By

$$\Im(z^*) = \frac{n y_0}{|\gamma a z_0 + \gamma b + \delta d|^2},$$

and the triangle inequality, we get inequality:

$$\left| T_{1A}\left(\frac{az_0 + b}{d}\right) \right| \leq e^{2\pi \Im(z^*)} + M. \tag{12}$$

So it is sufficient to show that

$$L \geq \sqrt{2}, \ L := |\gamma a z_0 + \gamma b + \delta d|.$$

The elements of $\Gamma_0^*(2)$ are uniquely expressed by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} or \begin{pmatrix} \sqrt{2}b & -a/\sqrt{2} \\ \sqrt{2}d & -c/\sqrt{2} \end{pmatrix}, where \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(2).$$

Without loss of generality, we can assume $\gamma \geq 0$. For $\gamma = 0$, we have

$$\delta = \pm 1, \ \pm\frac{1}{\sqrt{2}}.$$

If $\delta = \pm 1$, then $L = |d| \geq 2$. On the other hand, $\delta = \pm 1/\sqrt{2}$ contradicts $c \equiv 2 \pmod 2$. For $a \geq 2\sqrt{2}$ or $\gamma \geq 2\sqrt{2}$, $L \geq \sqrt{2}$ holds by the definition of L. By classification of (a, γ), the remaining cases are the following two cases:

$$(a, \gamma) = (1, 2), \ (1, \sqrt{2}).$$

For the case of $(a, \gamma) = (1, 2)$ and $d = n$,

$$L = |2z_0 + 2b + \delta n|,$$

we have $L \geq \sqrt{2}$ unless $2b + \delta n = -1$. For the case $2b + \delta n = -1$, $\delta = -1$ and $2b = n - 1$, we consider the tight estimation of (12). The point which provide the minimum of L is

$$z_0 = \left(\frac{n-1}{2n}, \frac{\sqrt{n^2 + 2n - 1}}{2n}\right).$$

So the following inequalities hold :

$$L \geq 1 + \frac{2}{n},$$

$$\left| T_{1A}\left(\frac{az_0 + b}{d}\right) \right| \leq e^{2\pi n y_0/(1+2/n)} + M.$$

For the case of $(a, \gamma) = (1, \sqrt{2})$, we have

$$L = \left| \sqrt{2} z_0 + \sqrt{2} b + \delta n \right|.$$

Similarly, we have $L \geq \sqrt{2}$ unless $\sqrt{2}b + \delta n = -\sqrt{2}$. For the case of $\sqrt{2}b + \delta n = -\sqrt{2}$, $\delta = -\sqrt{2}$ and $b = n - 1$, we get the trivial estimation:

$$\left| T_{2A}\left(\frac{z_0 + n - 1}{n}\right) \right| \leq e^{2\pi n y_0} + M.$$

So we have,

$$\begin{aligned}
|F_n(z_0) - (e^{-2\pi i n z_0} + e^{2\pi i n \bar{z}_0})| &\leq \sigma_1(n)M + (\sigma_1(n) - 4)e^{\pi n y_0} + e^{2\pi n y_0} + e^{2\pi n y_0/(1+2/n)} \\
|F_n(z_0)e^{-2\pi n y_0} - 2\cos(2\pi n x_0)| &\leq n^2(Me^{-\pi n} + e^{-\pi n(1/2)}) + 1 + e^{(2\pi n/(1+2/n)-2\pi n)(1/2)} \\
&\leq 6^2(Me^{-6\pi} + e^{-6\pi(1/2)}) + 1 + e^{(2\pi 6/(1+2/6)-2\pi 6)(1/2)} \\
&= 1.07091\cdots .
\end{aligned}$$

Thus, the proof of Lemma 4.1 is completed. Theorem 4.1 follows Lemma 4.1 immediately. □

Although we were unable to eliminate the possibility that there might exist one real root outside the interval $[-104, 152]$, we suspect that there is no such root. We note that if the coefficients in (14) below are alternating in sign, then we can show that all the zeros of $P_{n,2A}(X)$ are in the interval $[-104, 152]$.

Using the following lemma, we prove the Proposition 4.1. The proof is similar to [AKN].

Lemma 4.2. *Any meromorphic modular form on $\Gamma_0^*(2)$ of weight 2 which is holomorphic in $\mathbb{H}$ is the derivative (with respect to z) of a polynomial in T_{2A}.*

Proposition 4.1. *Let $P_{n,2A}(X)$ be a Hecke type Faber polynomial. Then*

$$\frac{E_{10,2}^*(q)}{\Delta_2(q)(T_{2A}(q) - X)} = \sum_{n=0}^{\infty} P_{n,2A}(X)q^n, \tag{13}$$

where the $E_{k,p}^*(q)$ is the Eisenstein series of weight k of $\Gamma_0^*(p)$, $\Delta_2(q) = (\eta(z)\eta(2z))^8$, and $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ which is called Dedekind η-function.

Remark 4.1. *In Theorem 4.1, we see that the $n-1$ zeros are in $(-104, 152)$. If we set $X = T_{2A}(1/2 + i/2) = -104$ in (13), then*

$$\begin{aligned}
\frac{E_{6,2}^*(z)}{E_{4,2}^*(z)} &= \sum_{n=0}^{\infty} p_{n,2A}(-104)q^n \\
&= 1 - 104q + 2072q^2 - 49568q^3 + 1146904q^4 - 26542704q^5 + \cdots . \qquad (14)
\end{aligned}$$

If we could show that the coefficients of (14) are alternative, then we can show that all the zeros lie in $(-104, 152)$ by the intermediate value theorem. (Can you prove that the coefficients of (14) are alternating?)

We note that the following generating function for $P_{n,2A}(X)$ can be obtained, by a similar argument as in Kaneko [K1], which give a proof for type 1A. These formulae are obtained for all types (not just 1A or 2A). These formulae might be useful for further study on this subject.

Proposition 4.2.

$$-q\frac{\partial}{\partial q}\log(T_m(q) - X) = \sum_{n=0}^{\infty} P_{n,m}(X)\,q^n. \tag{15}$$

Remark 4.2. *Since relation (15) is equivalent to*

$$\left\{-q\frac{\partial}{\partial q}(T_m(q))\right\}\frac{1}{T_m(q) - X} = \sum_{n=0}^{\infty} P_{n,m}(X)\,q^n,$$

we note that Proposition.4.1 can also be proved by the following fact :

$$-q\frac{\partial}{\partial q}(T_{2A}(q)) = \frac{E_{10,2}^*(q)}{\Delta_2(q)}.$$

5. 5B

All the zeros of the Hecke type Faber polynomial for 1A, 2A$\in \mathbb{M}$ (except possibly at most one zero for 2A, i.e. for $\Gamma_0^*(2)$) exist in $[-744, 984]$, $[-104, 152]$ respectively. For the possible remaining one zero of 2A, we expect that it also exists in $[-104, 152]$ as it is supported numerically by a computer calculation. The intervals correspond to the images of the boundaries $\{e^{i\theta} \in \mathbb{H} | \pi/2 \leq \theta \leq 2\pi/3\}$ and $\{e^{i\theta}/\sqrt{2} \in \mathbb{H} | \pi/2 \leq \theta \leq 3\pi/4\}$ of the fundamental domains by the mappings $z \mapsto T_{1A}(z)$, $z \mapsto T_{2A}(z)$ respectively (see FIGURE 1, 2 and APPENDIX). These imply that the zeros of the Hecke type Faber

polynomial of 1A and 2A exist in the image of the boundaries of the fundamental domains. The theme of this section is that this may hold for more general cases. Namely, we can discuss which are the most natural choice of the fundamental domains for the discrete subgroups $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$.

Now, we consider the case 5B. The group corresponding to 5B is $\Gamma_0(5)$. One of the choices of a fundamental domain of $\Gamma_0(5)$ is

$$\left\{-\frac{1}{2} \leq |\Re(z)| < \frac{1}{2}\right\} \bigcap \left\{\left|e^{i\theta} + \frac{2}{5}\right| \geq \frac{1}{5}, \frac{\pi}{2} \leq \theta \leq \frac{2\pi}{3}\right\} \bigcap \left\{\left|e^{i\theta} + \frac{2}{5}\right| > \frac{1}{5}, \frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}\right\} \bigcap$$
$$\left\{\left|e^{i\theta} + \frac{1}{5}\right| \geq \frac{1}{5}, 0 < \theta \leq \frac{2\pi}{3}\right\} \bigcap \left\{\left|e^{i\theta} - \frac{1}{5}\right| > \frac{1}{5}, \frac{\pi}{3} \leq \theta < 0\right\} \bigcap \left\{\left|e^{i\theta} - \frac{2}{5}\right| \geq \frac{1}{5}, \frac{\pi}{2} \leq \theta \leq \frac{\pi}{3}\right\} \bigcap$$
$$\left\{\left|e^{i\theta} - \frac{2}{5}\right| > \frac{1}{5}, \frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}\right\} \bigcap \mathbb{H}.$$

The following figures show the fundamental domain of $\Gamma_0(5)$ and the image of the boundaries BC, DEO, FG by $T_{5\mathrm{B}}$. We note that the method which gives these choices of the fundamental domain of $\mathrm{SL}_2(\mathbb{Z})$, $\Gamma_0^*(2)$ and $\Gamma_0(5)$ is given in Y. Kawada[K2], H. Shimizu [S3]. (See also [T2], [S2].) We want to claim that this choice of the fundamental domain is the most natural one, at least from the view point of the location of the zeros of Hecke type Faber polynomials $P_{n,5\mathrm{B}}(X)$.

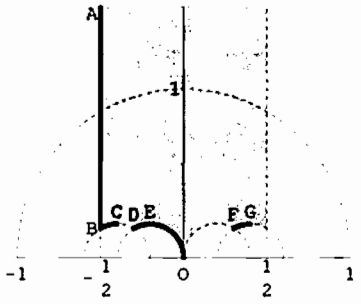


FIGURE 4, $\Gamma_0(5)$

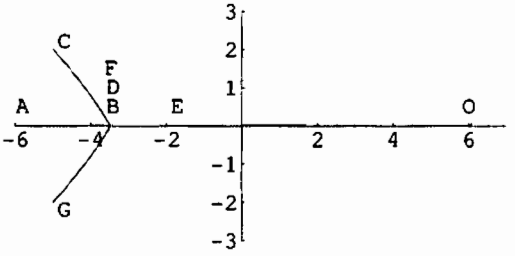


FIGURE 5, $T_{5\mathrm{B}}(BC, DEO, FG)$

In FIGURE 5, we have $\lim_{\Im(A)\to\infty} T_{5\mathrm{B}}(A) = -\infty, T_{5\mathrm{B}}(B) \approx -3.47214, T_{5\mathrm{B}}(C) \approx -5 + 2i, T_{5\mathrm{B}}(D) \approx -3.47214, T_{5\mathrm{B}}(E) \approx 1.76393, T_{5\mathrm{B}}(F) \approx -3.47214, T_{5\mathrm{B}}(G) \approx -5 - 2i, T_{5\mathrm{B}}(O) \approx 6$.

The next figure is the union of FIGURE 5 and the zoros of $P_{n,5\mathrm{B}}$, where $1 \leq n \leq 15$.

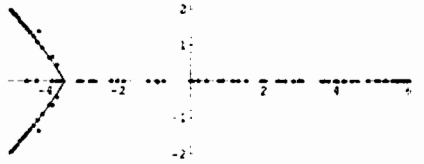
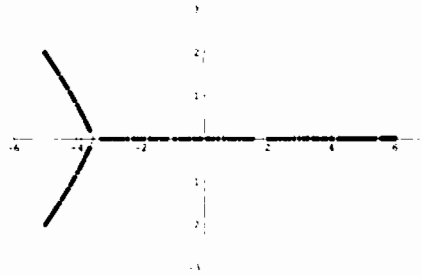
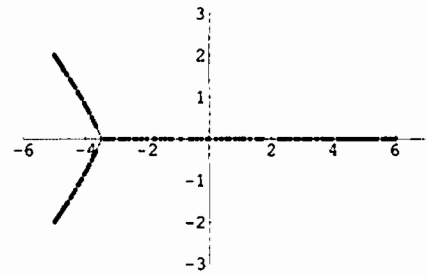


FIGURE 6

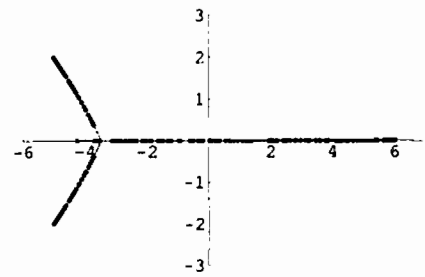
FIGURE 6 implies that some zeros of $P_{n,5\mathrm{B}}$ do not lie on the boundary of the fundamental domain, although many of them actually do. So we examine the zeros for some cases by dividing the cases into the degree n modulo 5 in detail. Next figures are union of FIGURE 5 and the zoros of $P_{n,5\mathrm{B}}$, where $n \equiv 0, 1, 2, 3, 4 \pmod 5$, $1 \leq n \leq 50$.



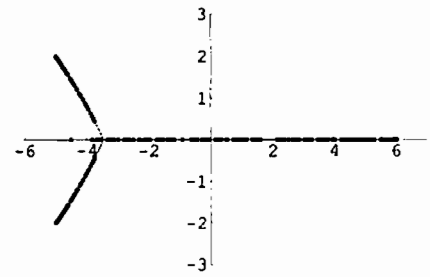
$n \equiv 0 \pmod 5$
FIGURE7



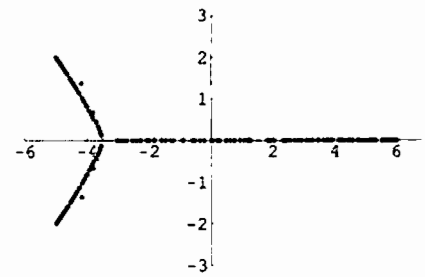
$n \equiv 1 \pmod 5$
FIGURE8



$n \equiv 2 \pmod 5$
FIGURE9



$n \equiv 3 \pmod 5$
FIGURE10



$n \equiv 4 \pmod 5$
FIGURE 11

We can see that for each degree $n \leq 104$ with $n \equiv 4 \pmod 5$ only two zeros do not lie on the boundary of the fundamental domain by a computer calculation. (Moreover, these two zeros seem to approach the point $T_{5B}(B) = T_{5B}(D) = T_{5B}(F) \sim -3.47214$ as n get larger. It would be interesting to know what the curves on which these exceptional zeros lie is. These curevs are not straight lines.) However, for $n \not\equiv 4 \pmod 5$, it is expected that the zeros always lie on the boundary of the fundamental domain. Moreover, for $n \equiv 0, 1 \pmod 5$, it is expected that the zeros lie on the boundary of the fundamental domain except for the line AB, i.e., $x = -1/2$. For the cases $n \equiv 2, 3 \pmod 5$, some zeros of Hecke type Faber polynomials exist in the line AB, i.e., $x = -1/2$.

6. Speculation

Let Γ be a genus 0 subgroup of $\mathrm{SL}_2(\mathbb{R})$. Let $\Gamma_\infty = \{\left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma\}$, and let $r = \mathrm{Min}\{x > 0 | \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_\infty\}$. Define F as follows :

$$F := \left\{ z \in \mathbb{H} \middle| -\frac{r}{2} < \Re(z) < \frac{r}{2} \right\} \bigcap \left(\bigcap_{x=\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma \backslash \Gamma_\infty} \{ z \in \mathbb{H} \, | \, |cz + d| > 1 \} \right).$$

Then there exists a fundamental domain D of Γ such that

$$F \subset D \subset \bar{F},$$

where $\bar{F}$ is the topological closure of F. Note that the fundamental domain D of $\Gamma_0(5)$ (= the group corresponding to 5B) described in the previous section is a special case of this. Also, note that this choice of the fundamental domain is in various books and papers, including [K2], [S3], [T2]. (We would like to know what the oldest source for this is.)

Speculation 6.1. *Most of the zeros of $P_{n,m}(X)$ are on the curve C which is the image of the boundaries of the fundamemtal domain D (described above) by the map $T_m(z)$. Equivalently, most of the zeros of $P_{n,m}(T_m(z))$ as a function of z are on the boundaries of D.*

We checked this speculation for some types of m, including 2B, 3B, 5B, 7B, 13B (where the corresponding gronp are $\Gamma_0(p)$ with genus 0, p is a prime, $p|\,|\mathbb{M}|$) and 2A, 3A, 5A, 7A, 11A, 13A, 17A, 19A, 23A, 29A, 31A, 41A, 47A, 59A, 71A (where the corresponding group are $\Gamma_0(p)$ with genus 0, p is a prime, $p|\,|\mathbb{M}|$).

Remark 6.1. *It would be very nice, if this speculation or something similar, is true for general $T_m(z)$. At least, this speculation will give a criterion of which choice of the fundamental domain is the best (natural) among many (arbitrary) choices. (Note that our check mentioned above, of this speculation is not very rigorous, i.e., we verified visually by drawing the curve C and plotting the zeros of the Hecke type polynomials $P_{n,m}(X)$.)*

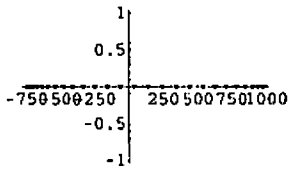
Remark 6.2. *Ken Ono informed us that the paper of Heekyoung Hahn* [H] *proves a similar type of phenomenon for the zeros of Eisenstein series, although in the examples treated there, the curve C is in the real axis. Anyway, we speculate that the choice of the fundamental domain described above is a natural (and perhaps most interesting) choice of fundamental domain, and we expect that a similar phenomenon might be true also for the zeros of Eisenstein series.*

Acknowledgement

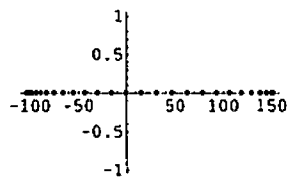
The authors thank Professors Masanobu Kaneko, Yuji Kodama, Masao Koike, John McKay, Simon Norton and Ken Ono, for their comments to the present work and providing us useful informations. We thank Junichi Shigezumi and Hiroshi Nozaki for their helpful discussions on this research. We also thank David Sevilla for pointing out some of incorrect statements made in an earlier version of our manuscript, especially in Observation 2.1 and Tables in §2.3. These previous mistakes by us were not of the calculation themselves, but were made when tabulation the results using our human eyevision.

Appendix A. Graphics of Zeros

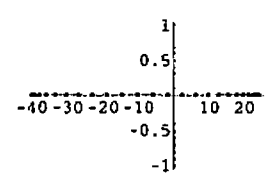
1 A



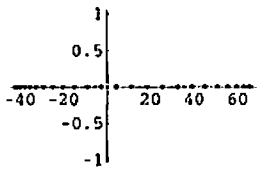
2 A



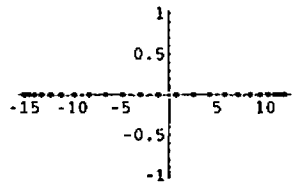
2 B



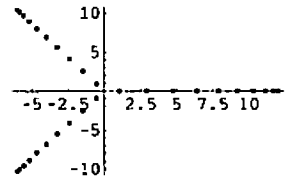
3 A



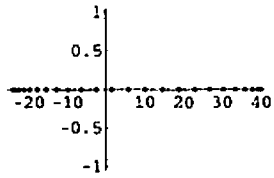
3 B



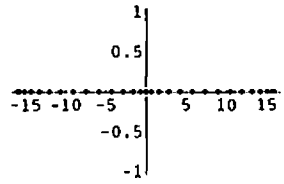
3 C



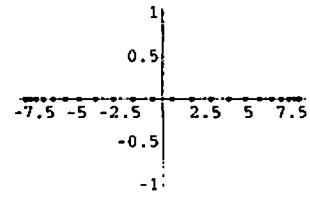
4 A



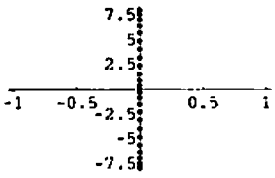
4 B



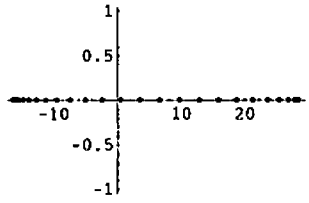
4 C



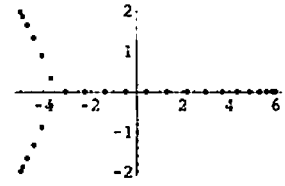
4 D



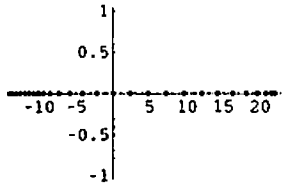
5 A



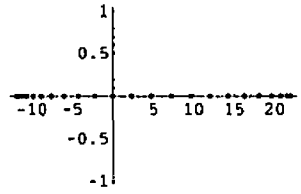
5 B



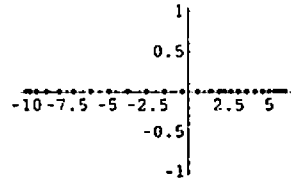
6 A



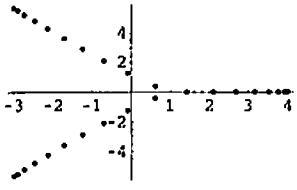
6 B



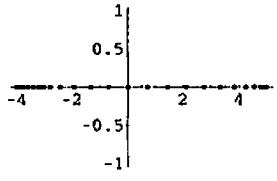
6 C



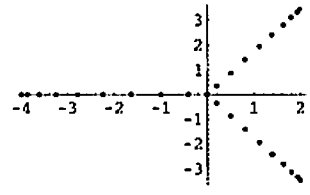
6 D



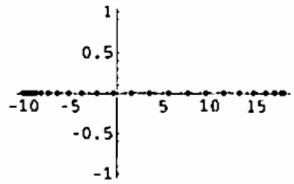
6 E



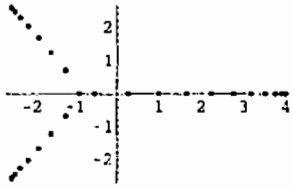
6 F



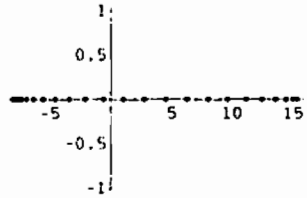
7 A



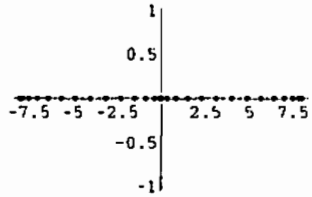
7 B



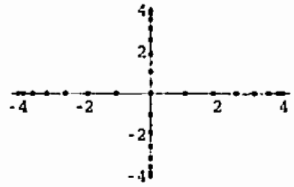
8 A



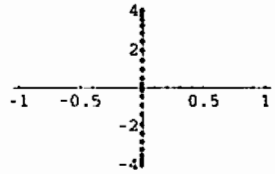
8 B



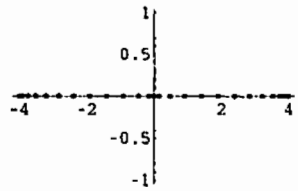
8 C



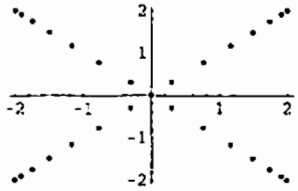
8 D



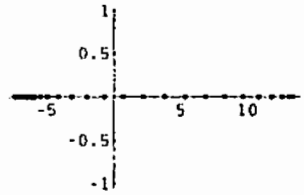
8 E



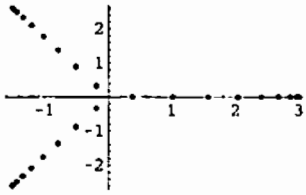
8 F



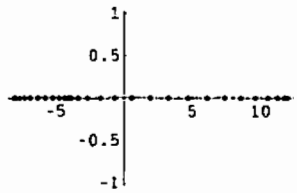
9 A



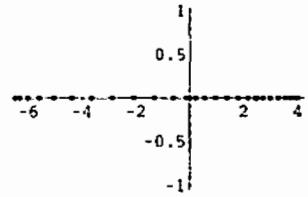
9 B



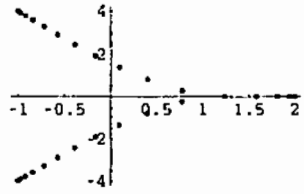
10 A



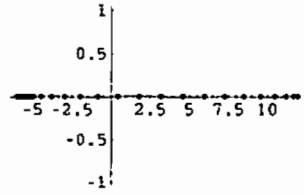
10 B



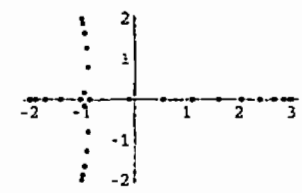
10 C



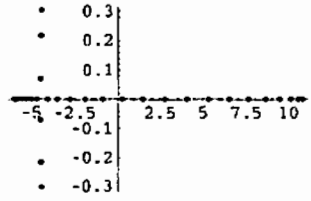
10 D



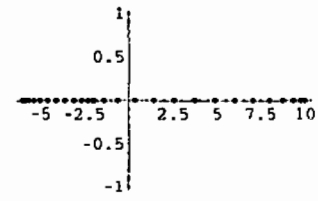
10 E



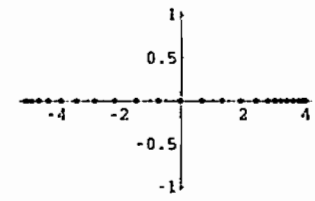
11 A

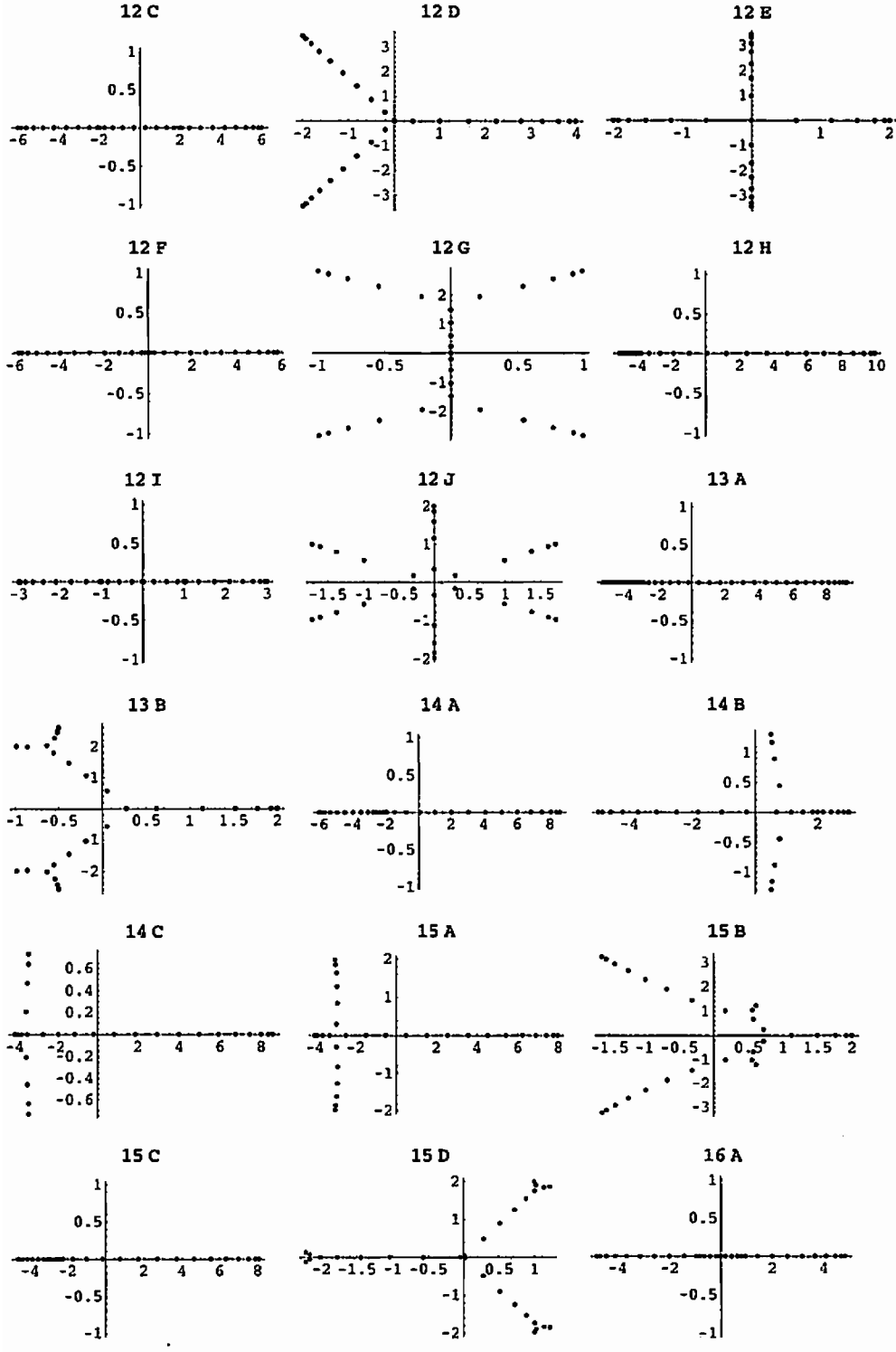


12 A

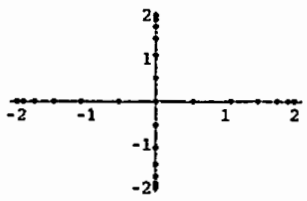


12 B

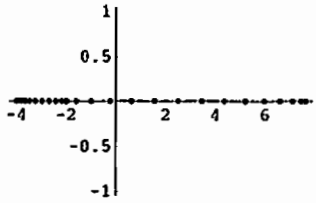



12 C
12 D
12 E
12 F
12 G
12 H
12 I
12 J
13 A
13 B
14 A
14 B
14 C
15 A
15 B
15 C
15 D
16 A

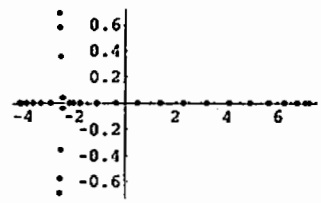
16 B



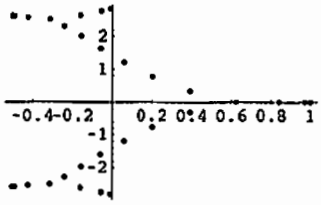
16 C



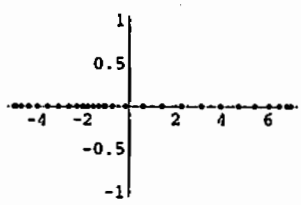
17 A



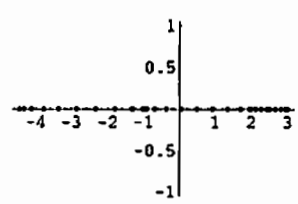
18 A



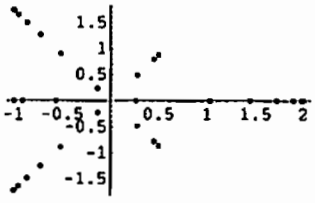
18 B



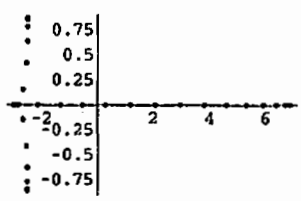
18 C



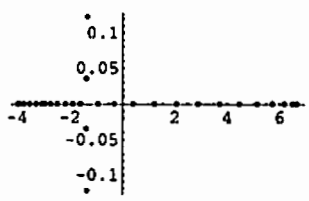
18 D



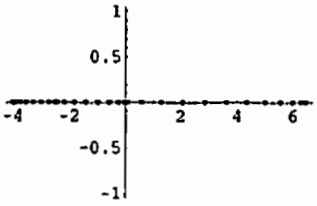
18 E



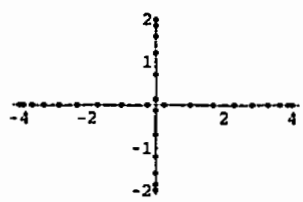
19 A



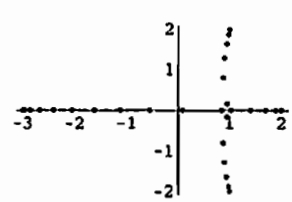
20 A



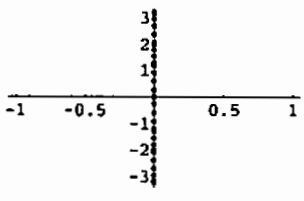
20 B



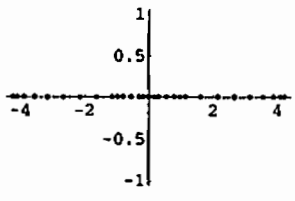
20 C



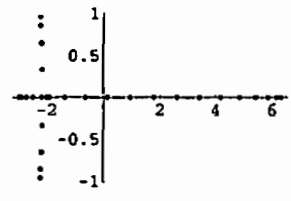
20 D



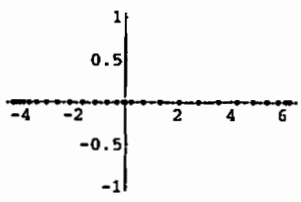
20 E



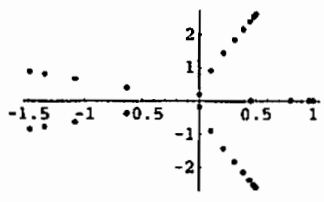
20 F



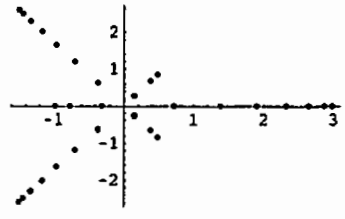
21 A

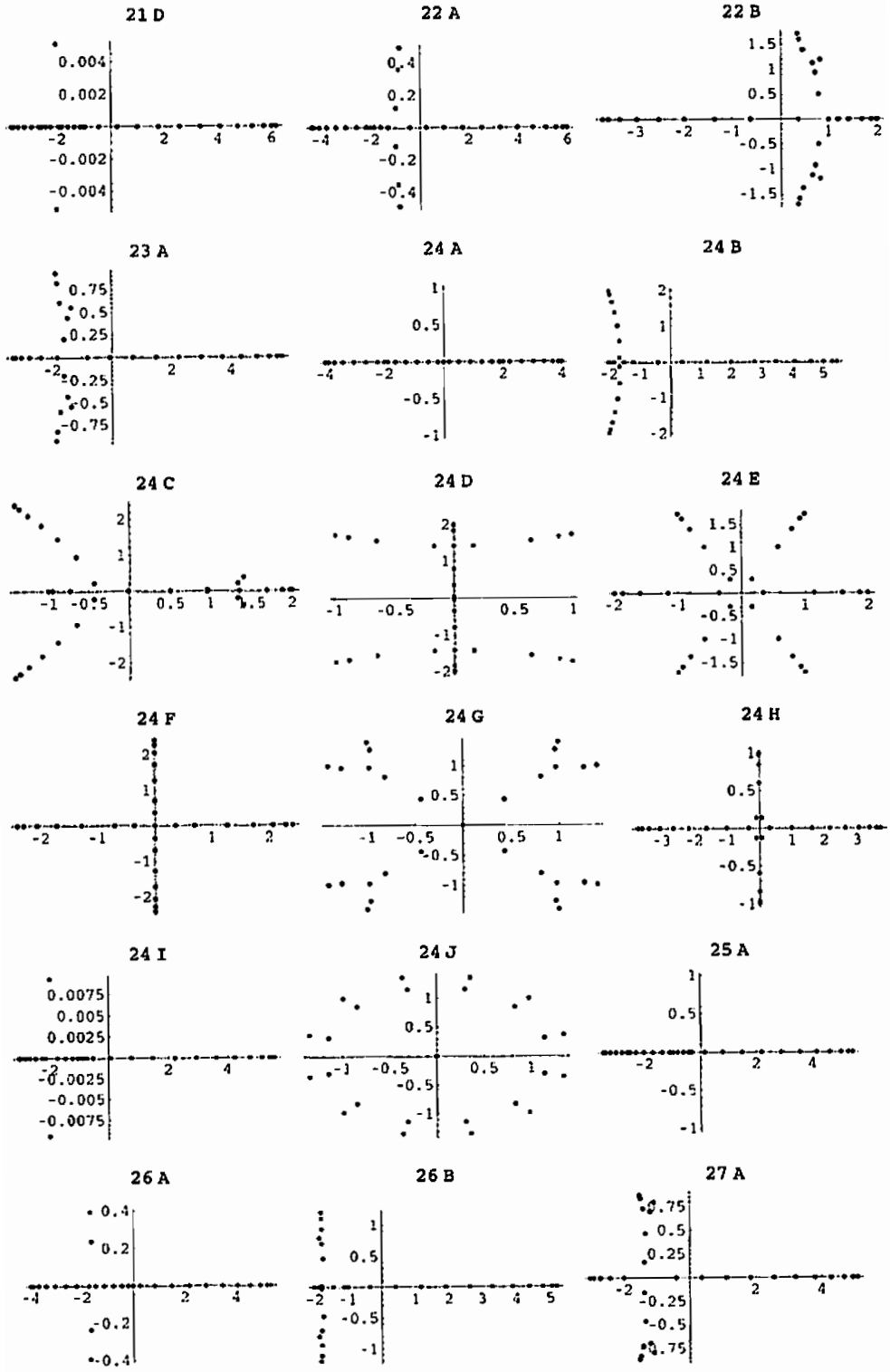


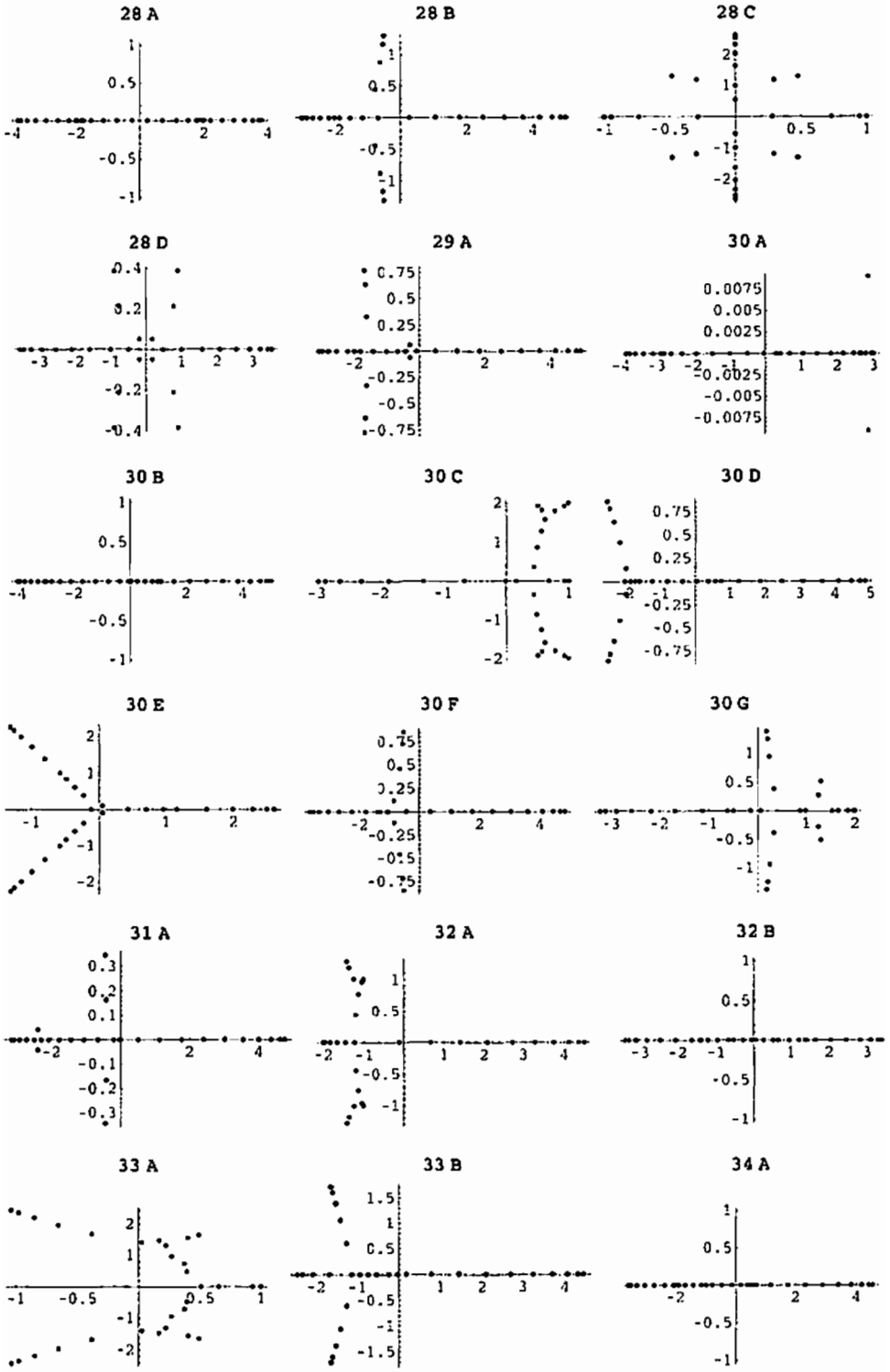
21 B

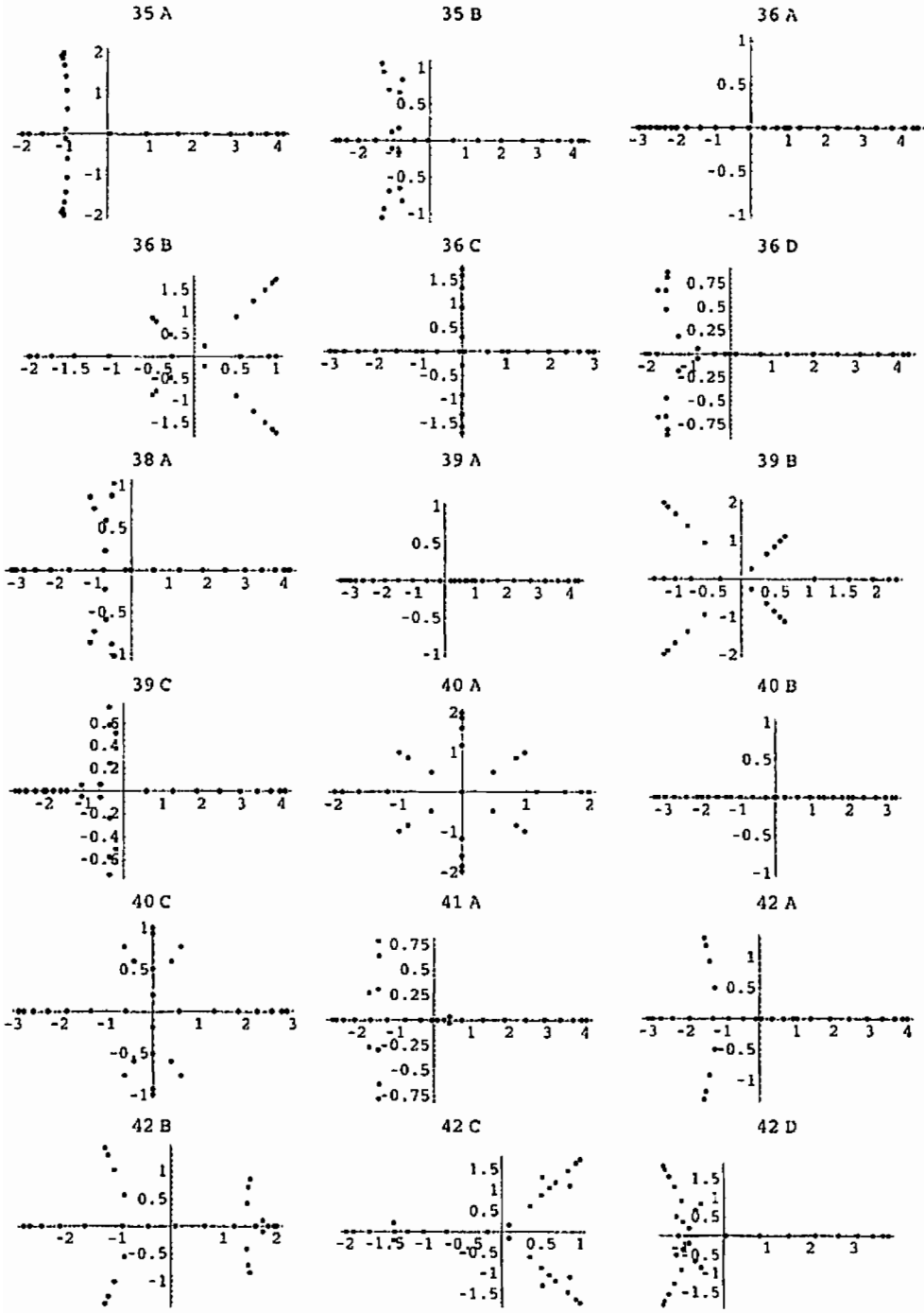


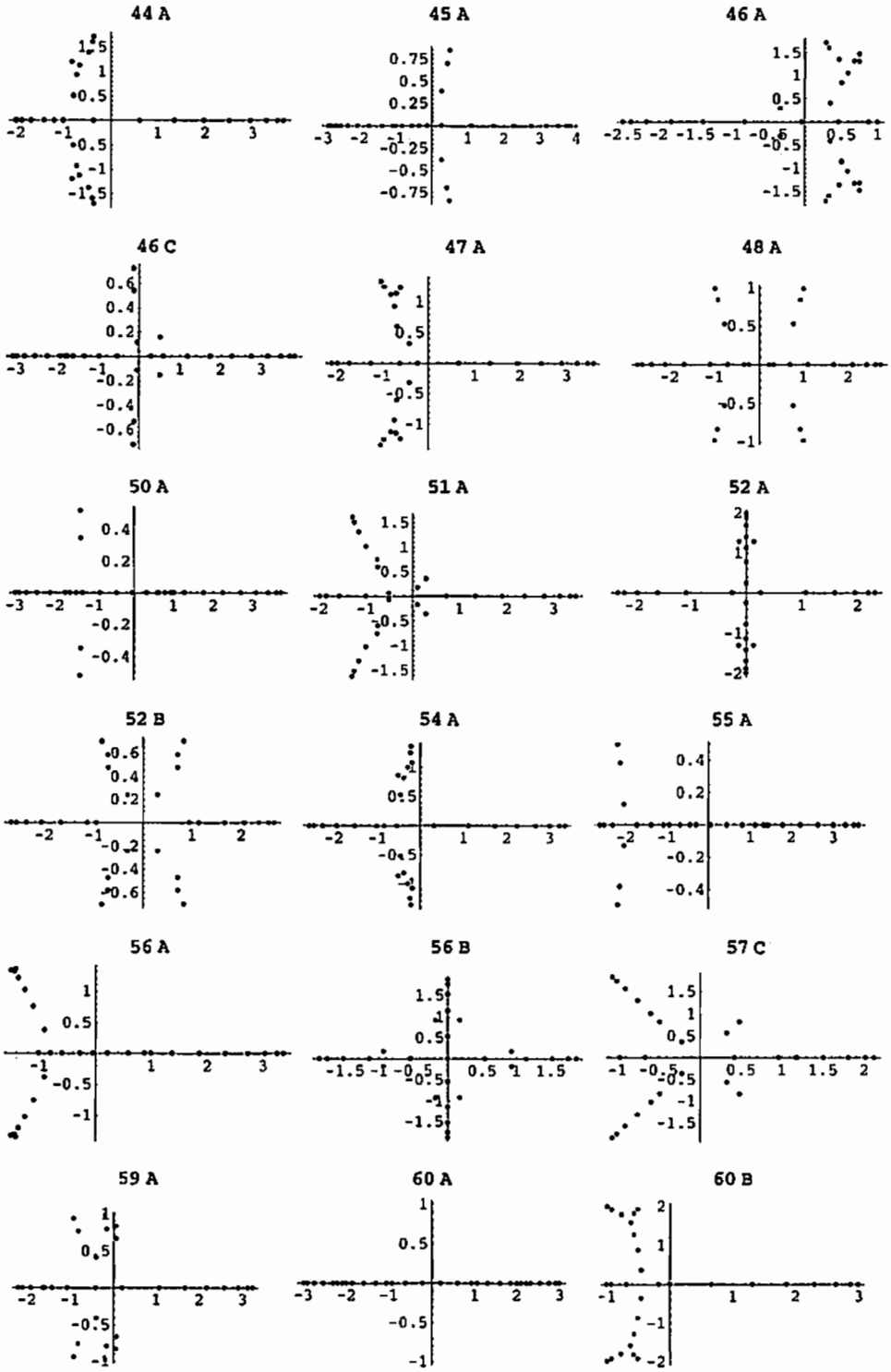
21 C



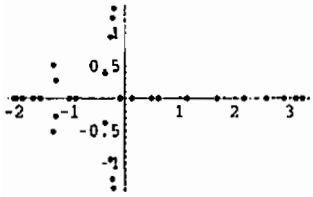

21 D
22 A
22 B
23 A
24 A
24 B
24 C
24 D
24 E
24 F
24 G
24 H
24 I
24 J
25 A
26 A
26 B
27 A


28 A
28 B
28 C
28 D
29 A
30 A
30 B
30 C
30 D
30 E
30 F
30 G
31 A
32 A
32 B
33 A
33 B
34 A

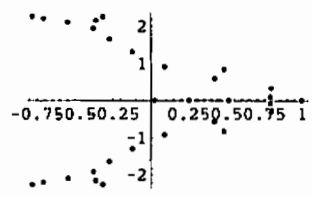

35 A
35 B
36 A
36 B
36 C
36 D
38 A
39 A
39 B
39 C
40 A
40 B
40 C
41 A
42 A
42 B
42 C
42 D


44 A
45 A
46 A
46 C
47 A
48 A
50 A
51 A
52 A
52 B
54 A
55 A
56 A
56 B
57 C
59 A
60 A
60 B

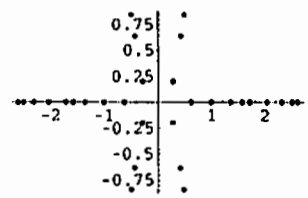
60 C



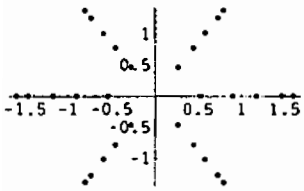
60 D



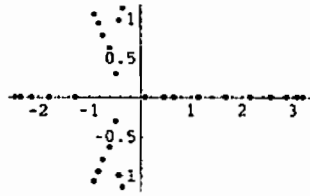
60 E



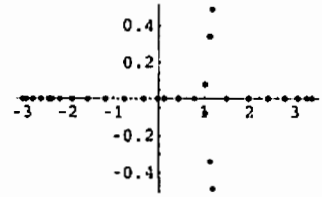
60 F



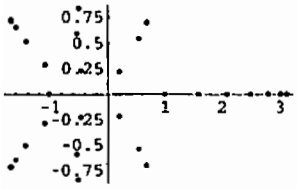
62 A



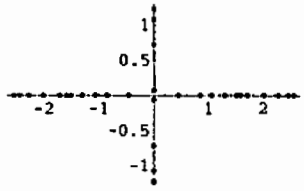
66 A



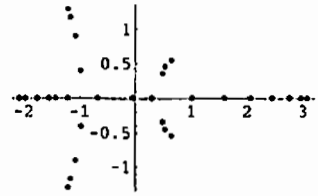
66 B



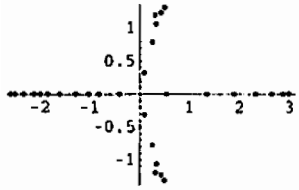
68 A



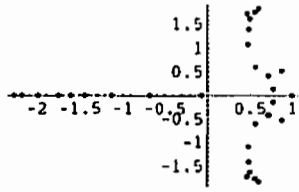
69 A



70 A

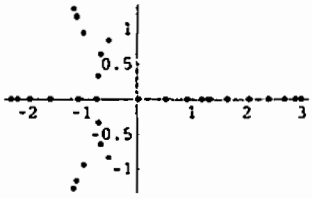


70 B

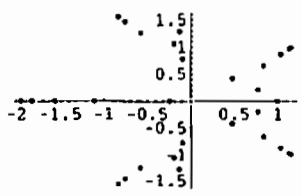


71 A

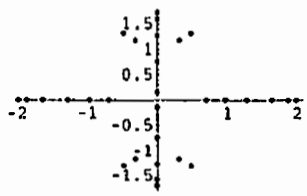
78 A



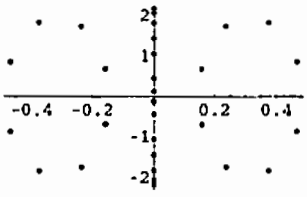
78 B



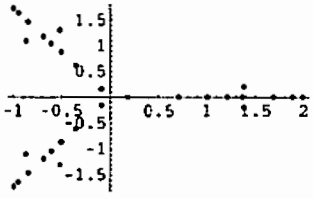
84 A



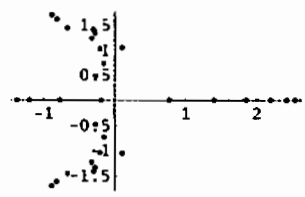
84 B

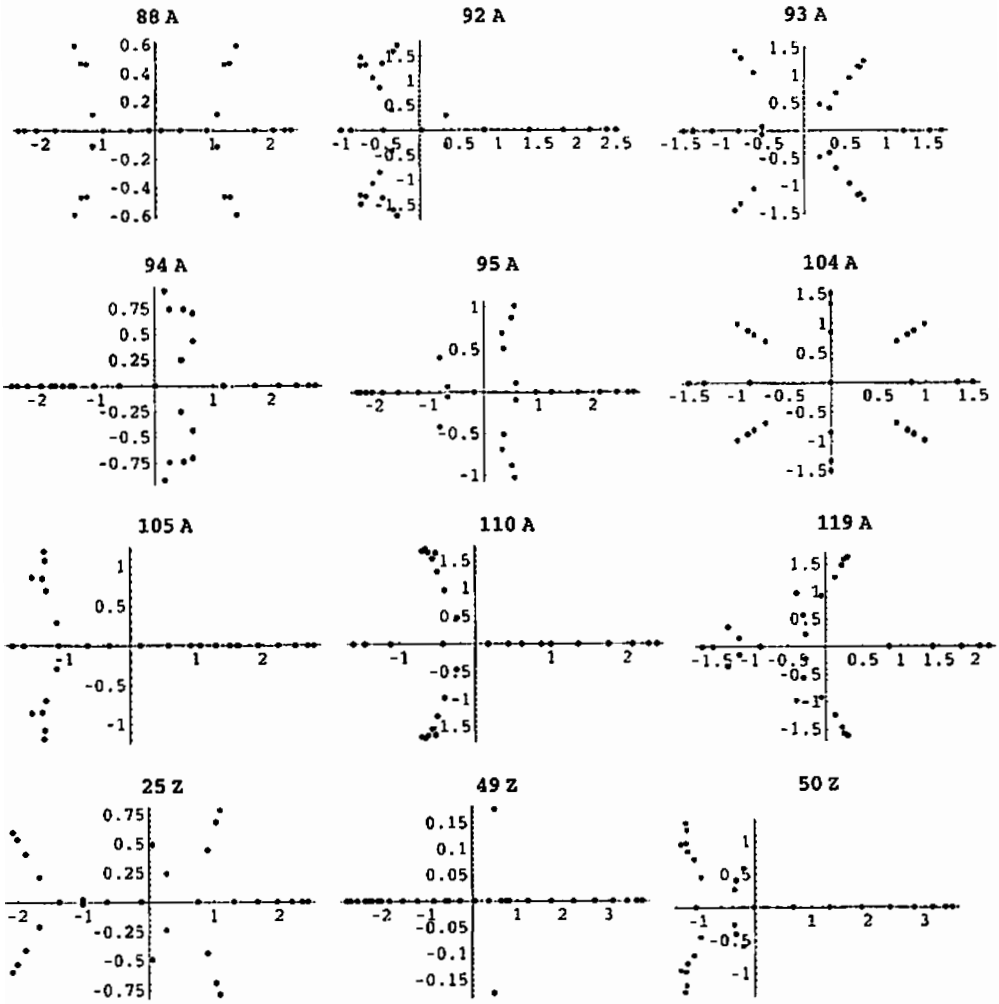


84 C

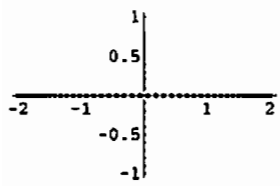


87 A

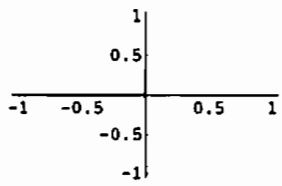



88 A
92 A
93 A
94 A
95 A
104 A
105 A
110 A
119 A
25 Z
49 Z
50 Z

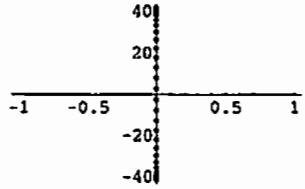
1 a



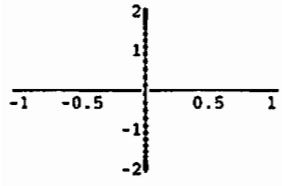
1 b



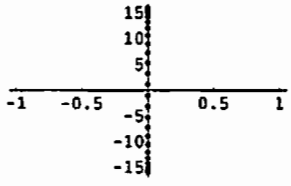
2 a



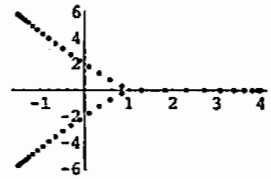
2 b



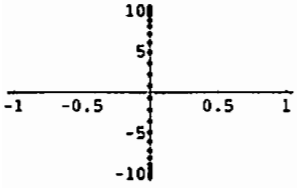
4 a



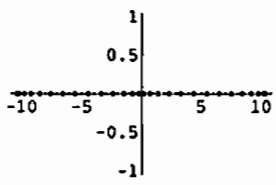
5 a



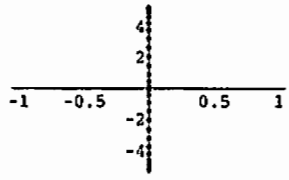
6 a



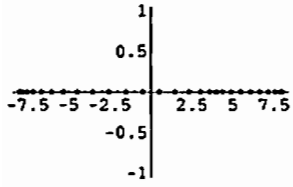
6 b



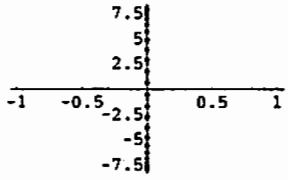
6 c



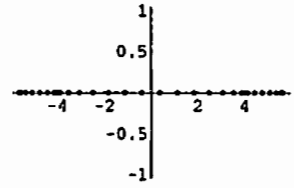
6 d



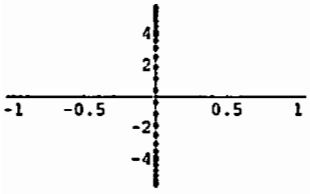
8 a



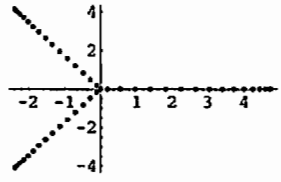
8 b



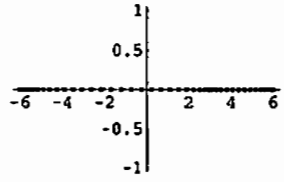
8 c



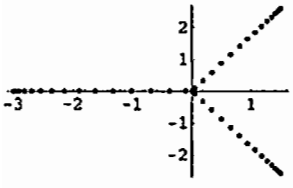
9 a



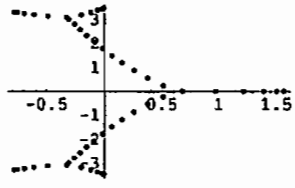
9 b



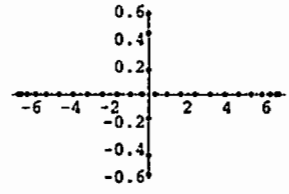
9 c

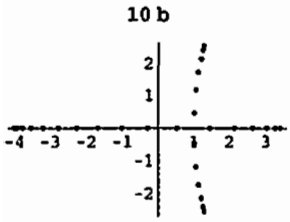


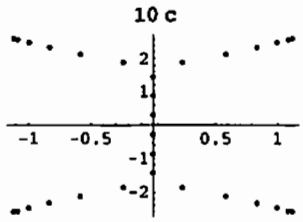
9 d

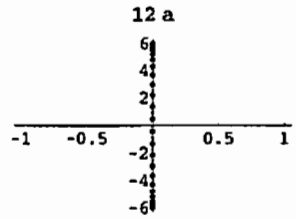


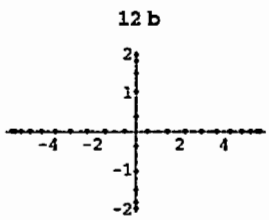
10 a

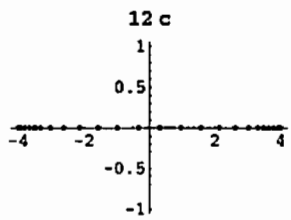


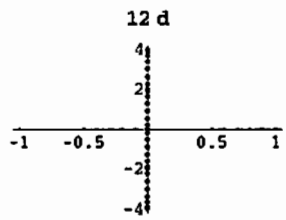

10 b

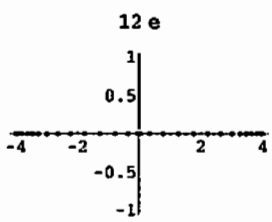

10 c

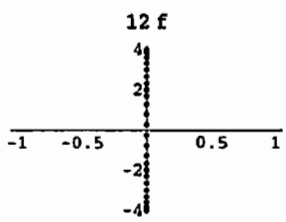

12 a

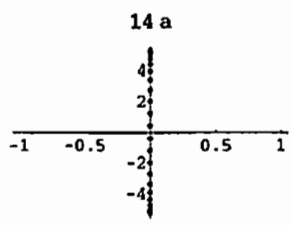

12 b

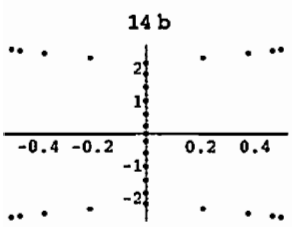

12 c

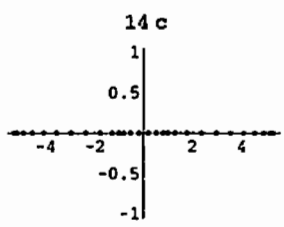

12 d

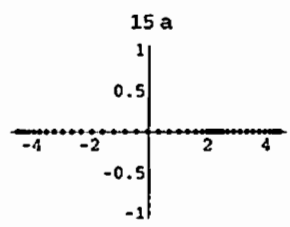

12 e

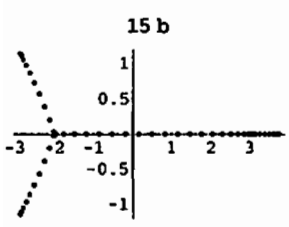

12 f

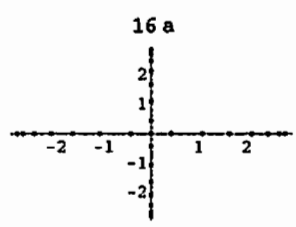

14 a

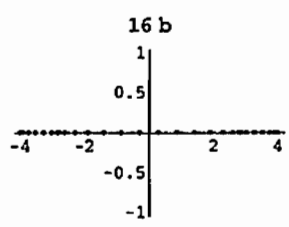

14 b

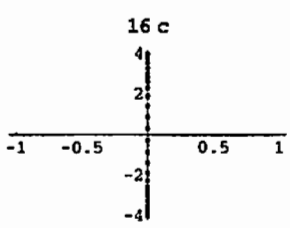

14 c

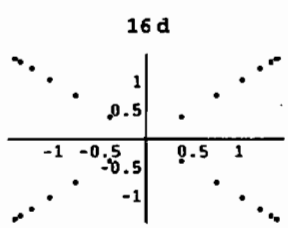

15 a

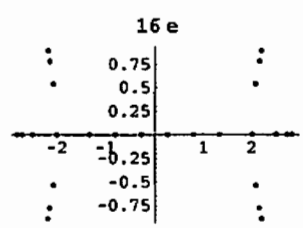

15 b


16 a

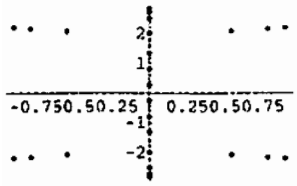

16 b


16 c

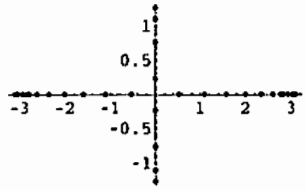

16 d


16 e

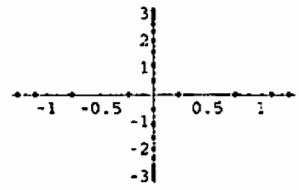
16 f



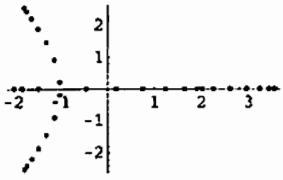
16 g



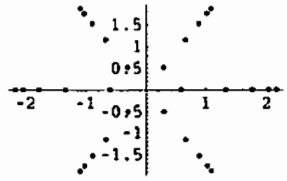
16 h



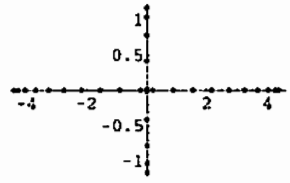
18 a



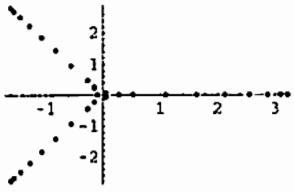
18 b



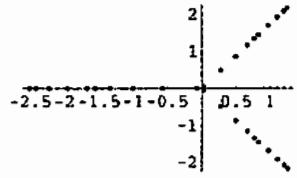
18 c



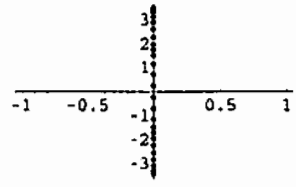
18 d



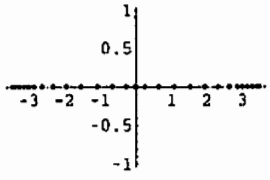
18 e



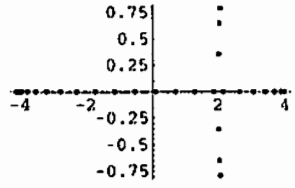
18 f



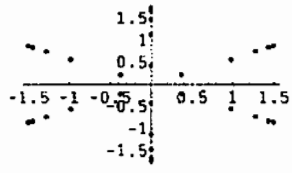
18 g



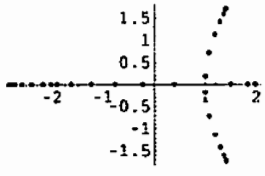
18 h



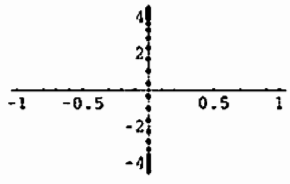
18 i



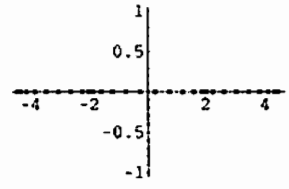
18 j



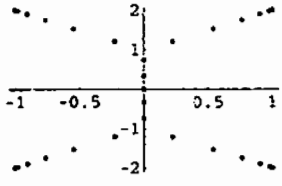
20 a



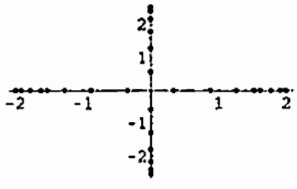
20 b



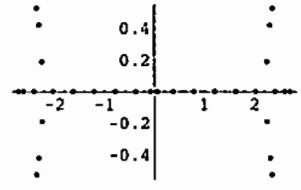
20 c

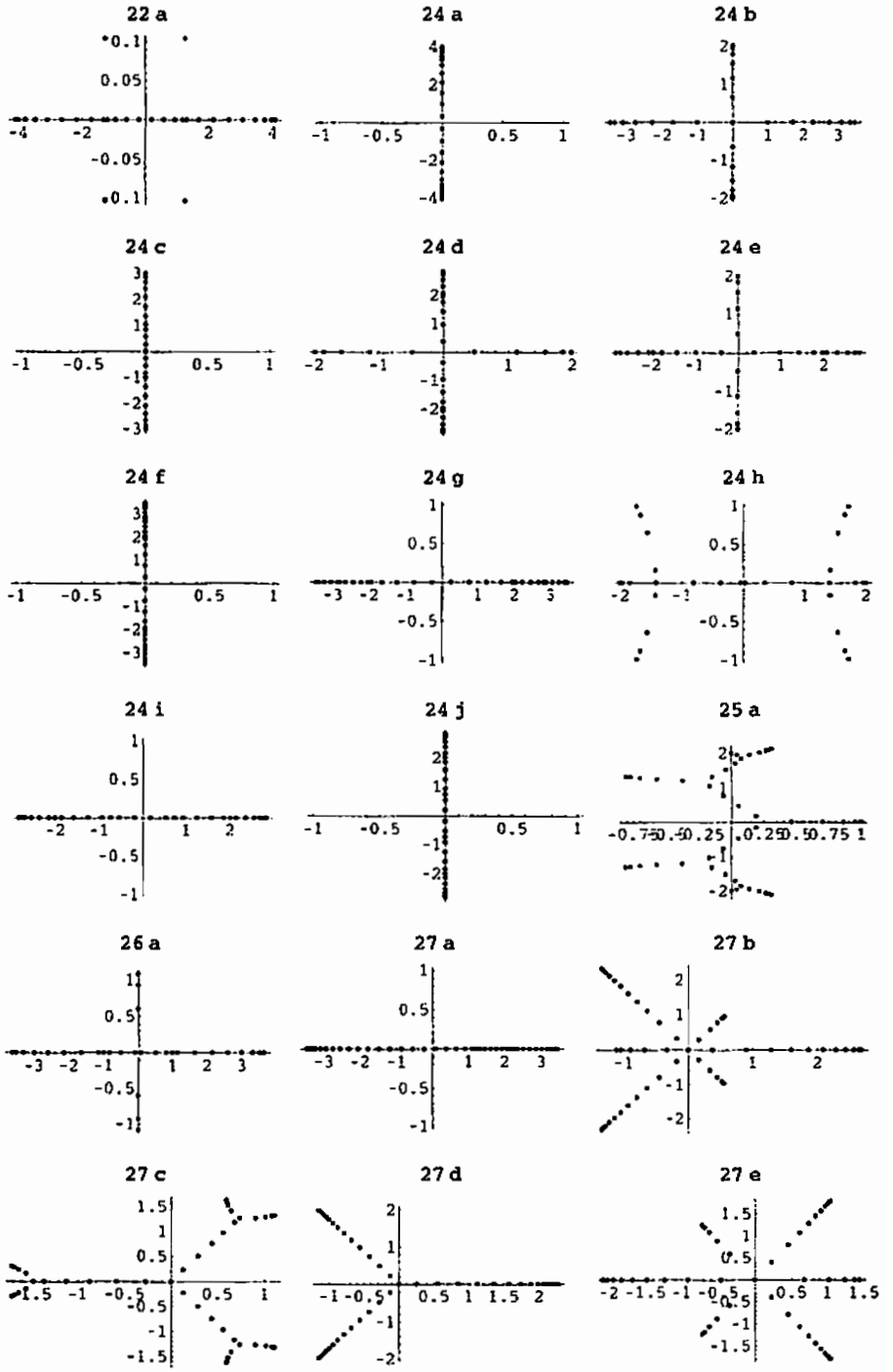


20 d

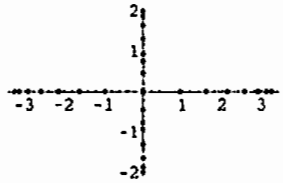


20 e

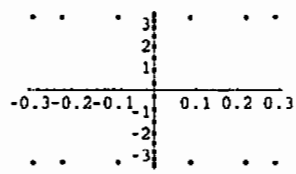



22 a
24 a
24 b
24 c
24 d
24 e
24 f
24 g
24 h
24 i
24 j
25 a
26 a
27 a
27 b
27 c
27 d
27 e

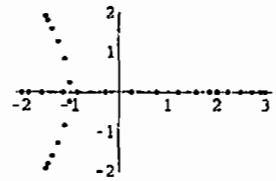
28 a



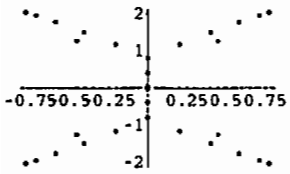
30 a



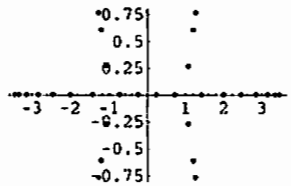
30 b



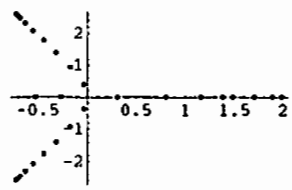
30 c



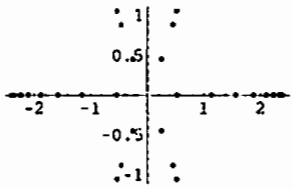
30 d



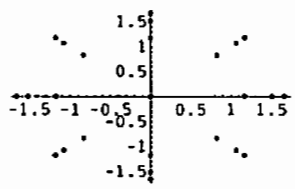
30 e



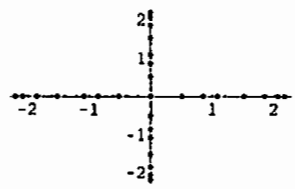
30 f



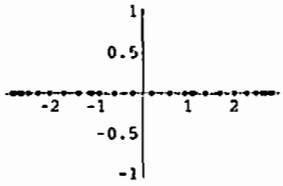
32 a



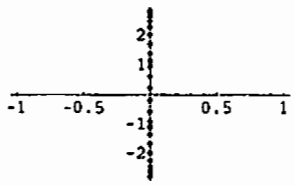
32 b



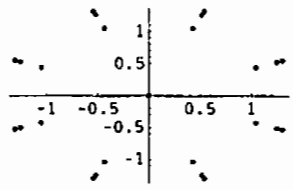
32 c



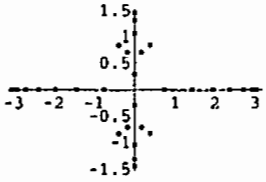
32 d



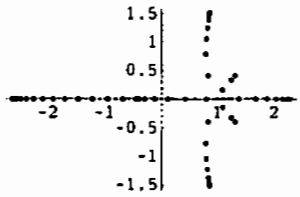
32 e



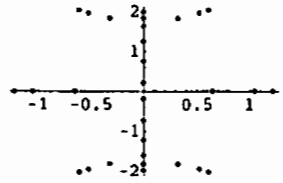
34 a



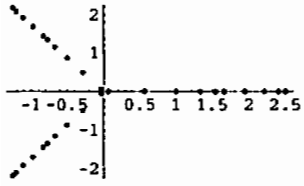
35 a



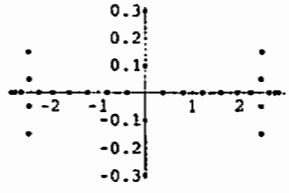
36 a



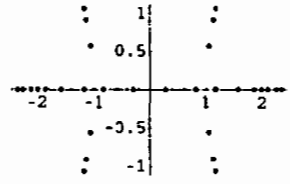
36 b

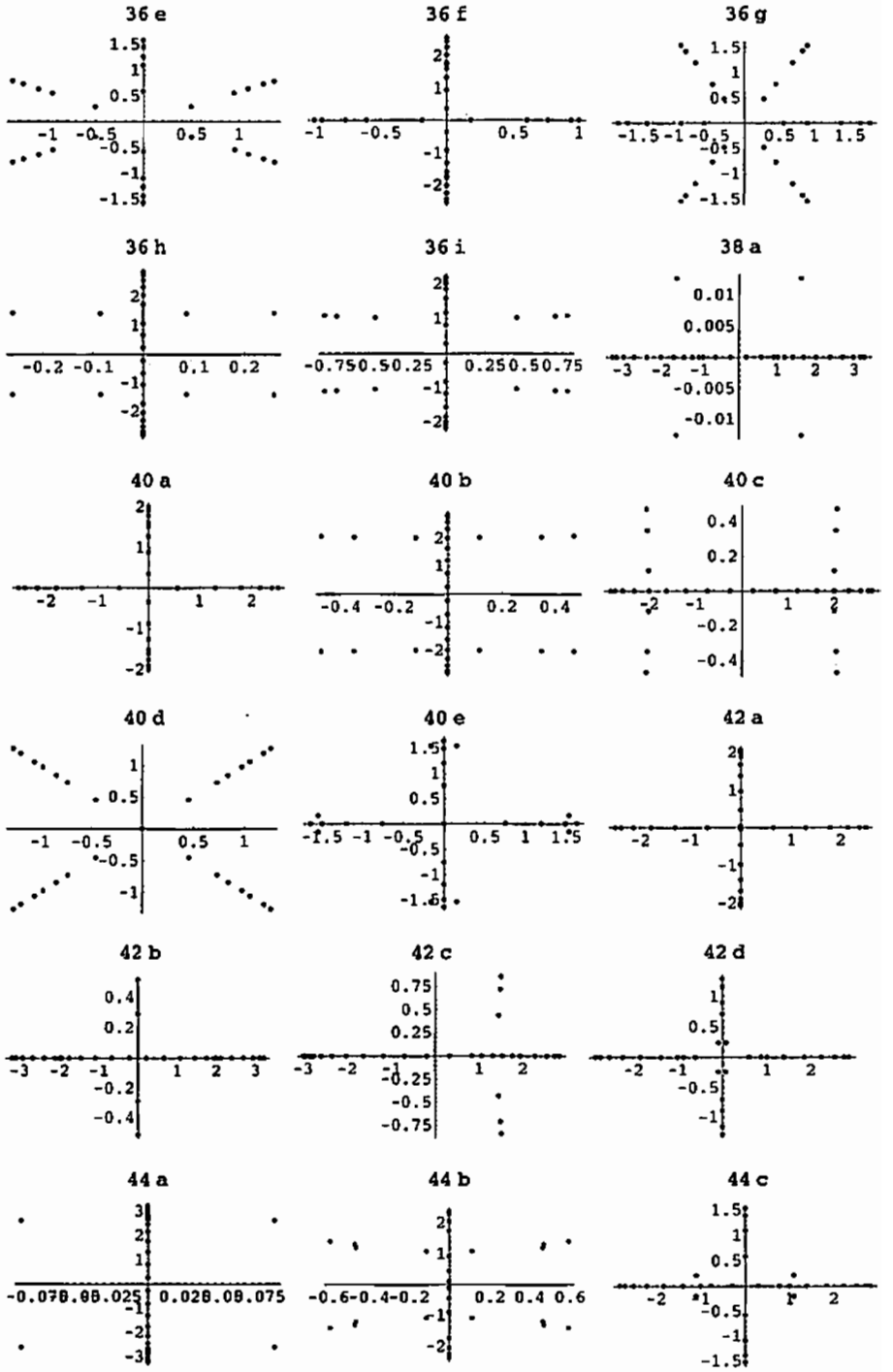


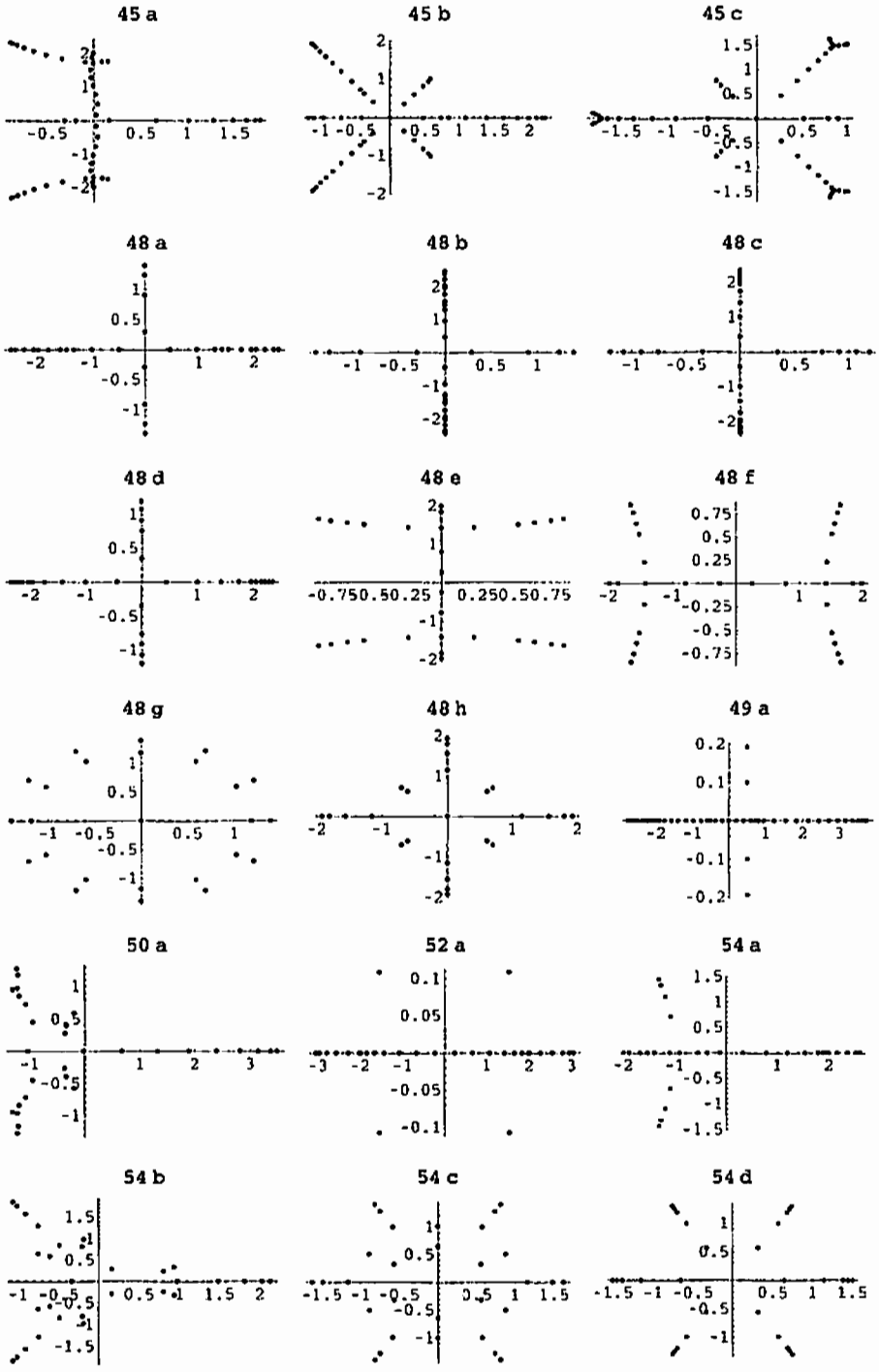
36 c

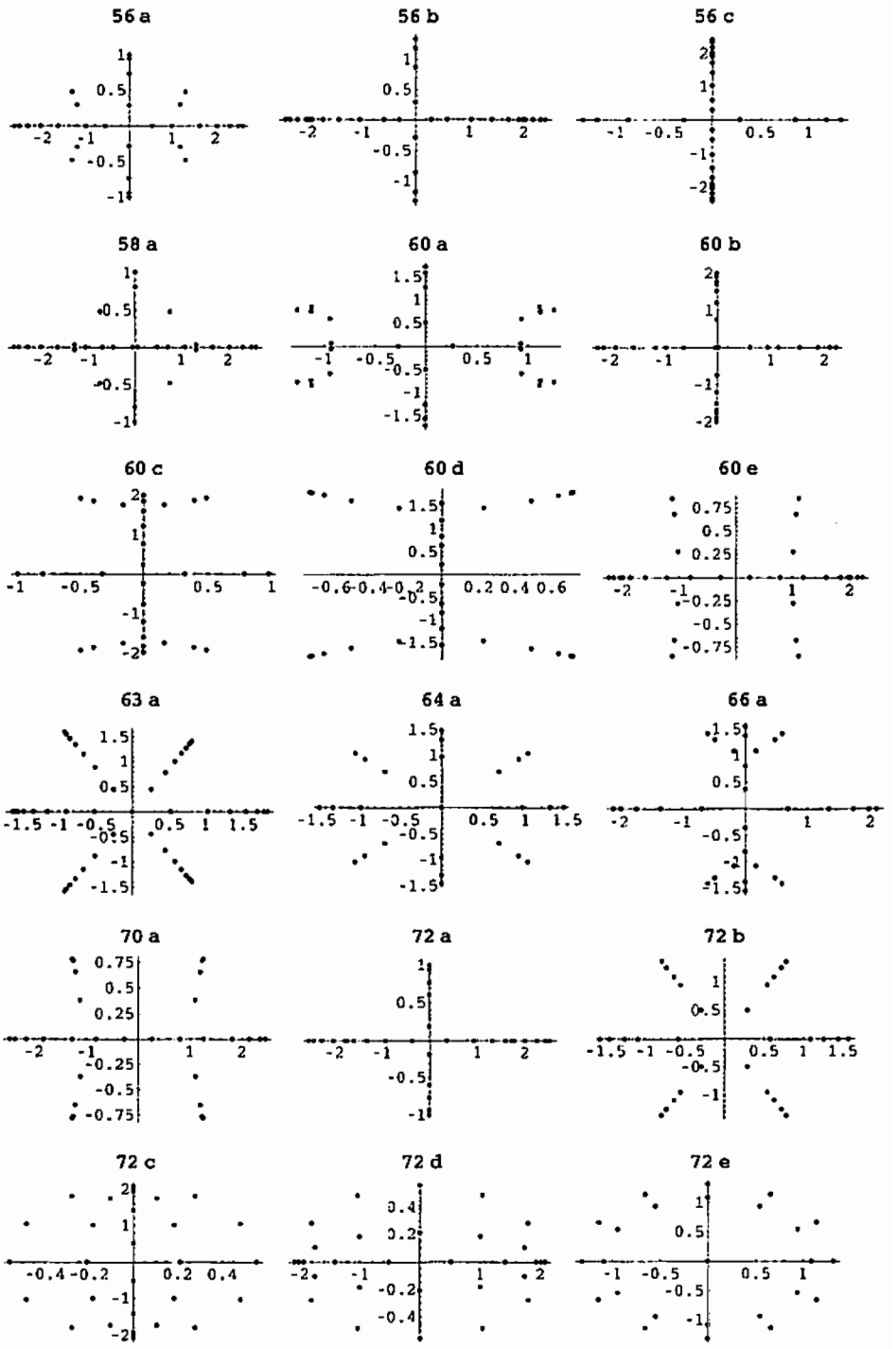


36 d

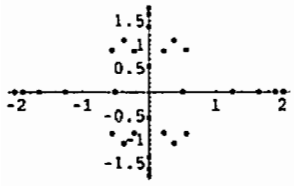



36 e
36 f
36 g
36 h
36 i
38 a
40 a
40 b
40 c
40 d
40 e
42 a
42 b
42 c
42 d
44 a
44 b
44 c

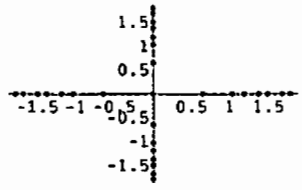

45 a
45 b
45 c
48 a
48 b
48 c
48 d
48 e
48 f
48 g
48 h
49 a
50 a
52 a
54 a
54 b
54 c
54 d


56 a
56 b
56 c
58 a
60 a
60 b
60 c
60 d
60 e
63 a
64 a
66 a
70 a
72 a
72 b
72 c
72 d
72 e

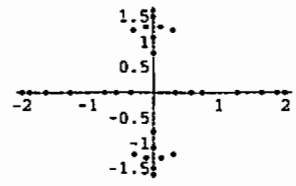
76 a



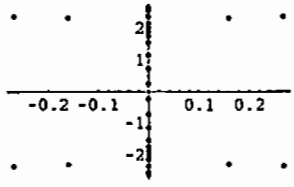
80 a



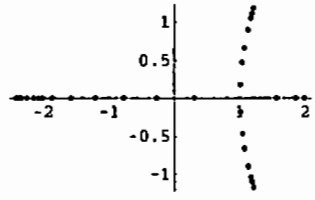
82 a



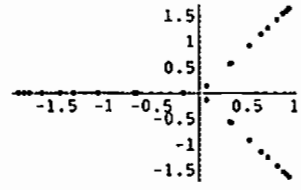
84 a



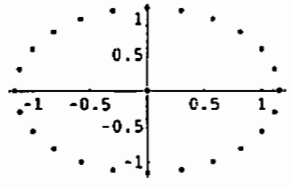
90 a



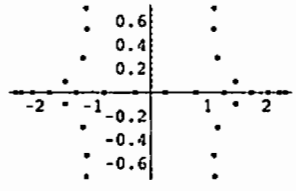
90 b



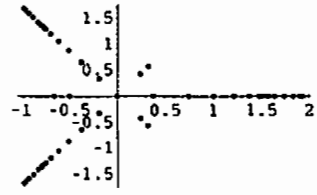
96 a



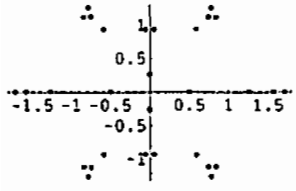
102 a



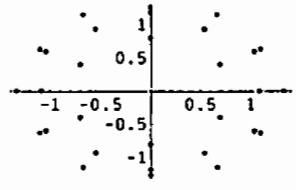
117 a



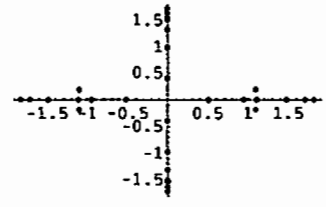
120 a



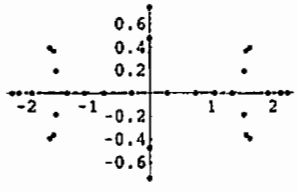
126 a



132 a



140 a



REFERENCES

[ACMS] D. Alexander, C. Cummins, J. McKay, C. Simons, *Completely Replicable Functions.*, Groups, Combinatorics and Geometry (M. W. Liebeck and j. Saxl, eds.), LMS Lecture Note Series, vol.165, Cambridge University Press, 1992, pp.87-98.

[AKN] T. Asai, M. Kaneko, H. Ninomiya, *Zeros of Certain Modular Functions and Applocation.*, Comment. Math. Univ. St Pauli, **46-1**(1997), 93-101.

[B] R. E. Borcherds, *Monstrous moonshine and monstrous Lie superalgebras.*, Invent. Math. **109** (1992), no. 2, 405–444.

[CN] J. H. Conway, S. P. Norton, *Monstrous Moonshine.*, Bull. Lond. Math. Soc. **11**(1979), 308-339.

[F] G. Faber, *Über polynomische Entwickelungen.*, Math. Ann., **57**(1903), 389-408.

[FMN] D. Ford, J. McKay, S. Norton, *More on replicable functions.*, Comm. Algebra, **22**(1994), 5175-5193.

[H] H. Hahn, *On zeros of Eisenstein series for genus zero Fuchsian groups.*, Proceedings of the AMS, to appear.

[I] Y. Ihara, *Hecke Polynomials as congruence ζ functions in elliptic modular case.*, Ann. of Math. (2) **85**(1967), 267-295.

[K1] M. Kaneko, *Fourier coefficient of elliptic modular function $j(\tau)$.*, Lecture Note, (Japanese).

[K2] Y. Kawada, *Theory of modular functions of one variable (I).*, Seminary note, no. 4, University of Tokyo, (1963), (in Japanese).

[K3] M. Koike, *Modular forms and the automorphism group of the Leech lattice.*, Nagoya. Math. J.,**112** (1988), 63-79.

[K4] A. Krieg, *Modular Forms on the Fricke Group.*, Abh. Math. Sem. Univ. Hamburg, **65**(1995), 293-299.

[L] M.-L. Lang, *On a question raised by Conway-Norton.*, J. Math. Soc. Japan. **41** (1989), 263-284.

[M1] K. Mahler, *On a class of non-linear functional equations connected with modular functions.*, J. Austral. Math. Soc. **22A** (1976), 65-118.

[M2] J. McKay, *The essentials of Monstrous Moonshine.*, Adv. Stud. Pure Math. **32**(2001), 347-353.

[MNS] T. Miezaki, H. Nozaki, J. Shigezumi, *On the Zeros of Eisenstein Series for $\Gamma_0^*(2)$ and $\Gamma_0^*(3)$.*, submitted.

[MS] J. McKay, H. Strauß, *The q-series of monstrous moonshine & the decomposition of the head characters.*, Comm. in Alg. **18**(1990), 253-278.

[RSD] F. K. C. Rankin, H. P. F. Swinnerton-Dyer, *On the zeros of Eisenstein Series*, Bull. London Math. Soc., **2**(1970), 169-170.

[S1] J. -P. Serre, *A Corse in Arithmetic.*, Graduate Texts in Mathematics, No.7, Springer-Verlag, New York-Heidelberg, 1973. (Translation of *Cours d'arithmétique.*, Presses Univ. French, Paris, 1970.)

[S2] J. Shigezumi, *On the zeros of Eisenstein series for $\Gamma_0^*(5)$ and $\Gamma_0^*(7)$.*, submitted.

[S3] H. Shimizu, *Hokei kansu. I-III.* (*in Japanese*) *[Automorphic functions. I-III].*, Iwanami Shoten Kiso Sūgaku [Iwanami Lectures on Fundamental Mathematics], 8. Daisū [Algebra], vii, Iwanami Shoten, Tokyo, (1984).

[T1] J. G. Thompson, *Some numerology between the Fischer-Griess Monster and the elliptic modular function.*, Bull. London Math. Soc., **11**(1979), 352-353.

[T2] H. Tsutsumi, *The Atkin inner product for $\Gamma_0(N)$.* , J. Math. Kyoto Univ., **40**(2000), no. 4, 751-773.

[TH] I. Terada, K. Harada, *group theory.*(*in Japanese*), Iwanami Shoten.

Double Circulant Codes from Two Class Association Schemes

Patrick Solé[a]

I3S-CNRS, Université de Nice - Sophia Antipolis, France

[a]joint work with S. Dougherty, J-L. Kim

1

Quadratic residues

Let q be an odd prime power, and $\mathbb{F}_q$ the finite field of order q.
Define the matrix Q with rows and columns indexed by $\mathbb{F}_q$ by the rule
$Q_{x,y} = 1$, if $y - x$ is a nonzero square in $\mathbb{F}_q$ and zero otherwise.
For instance, for $q = 5$,

$$Q = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

Same definition for matrix N and nonsquares in $\mathbb{F}_q$
But where have we seen these matrices before in Algebraic Combinatorics?

;=))

2

Hadamard matrices

Assume $q = 4k + 3$ and let $H' = Q - N$. Note that H' is skew symmetric.
Then adding a row,a column, and a diagonal of ± 1 yields a Hadamard matrix H

$$H = \begin{bmatrix} + & + & + & + \\ - & + & + & + \\ - & - & + & + \\ - & + & - & + \end{bmatrix}.$$

In symbols

$$HH^t = (q+1)I.$$

3

Doubly regular tournaments

A tournament is a digraph: an orientation of the complete graph.
Models a sport tournament with no ties (unlike the (soccer) World Cup!):
vertex=team; arc from x to y=win of x on y
A tournament is regular iff every team has the same score (same out-degree).
It is doubly regular iff every pair of teams defeats the same number of common opponents.
Then Q is the adjacency matrix of a DRT of $q = 4k + 3$ teams:

- every team scores $2k + 1$
- every pair of teams defeats k common opponents

Result: (Brown, 1972) There is a DRT of $4k + 3$ teams iff there is a Hadamard matrix of order $4k + 4$.

4

Matrix Equations for $q = 4k + 3$

In this case $Q^t = N$ and $Q + N + I = J$.

$$QQ^t = (k+1)I + kJ.$$

For a general DRT of parameters $(v, \kappa, \lambda, \mu)$ with adjacency matrix A one would have

$$AA^T = \kappa I + (\kappa - 1 - \lambda)A + (\kappa - \mu)\overline{A}.$$

5

Strongly Regular Graphs

If $q = 4k + 1$ then -1 is a quadratic residue in $\mathbb{F}_q$.
The matrix $A := Q + N$ is symmetric.
It is the adjacency matrix of $2k-$regular graph with the following properties

- every pair of adjacent vertices has $(q-5)/4$ common neighbors
- every pair of non adjacent vertices has $(q-1)/4$ common neighbors

Matrix equation (counting paths of length 2)

$$AA^t = qI - J$$

(with I=identity and J=all-one matrix)

6

Matrix Equations for $q = 4k + 1$

In this case $Q^t = Q$ and $N^t = N$, and $Q + N + I = J$.

$$QQ^t = 2kI + (k-1)Q + kN.$$

For a general SRG of parameters $(v, \kappa, \lambda, \mu)$ one would have

$$AA^T = A^2 = \kappa I + \lambda A + \mu(J - I - A)$$

7

Gaborit Quadratic Double Circulant Codes

For scalars r, s, t of your favorite alphabet let $Q_q(r, s, t) := rI + sQ + tN$.
Define a pure double circulant code by its generator matrix

$$\mathcal{P}_R(r, s, t) = (I \mid Q_R(r, s, t)).$$

The generator matrix of the bordered double circulant code

$$\mathcal{B}_R(r, s, t) = \left(\begin{array}{c|c|c|c} 1 & 0 \ldots 0 & \alpha & \beta \ldots \beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_R(r, s, t) \\ 0 & & \gamma & \end{array}\right).$$

See Gaborit (2001) for fields and Gaborit, Natividad, S. (2006) for $GR(4, 2)$

8

Karlin double circulant Codes

When $q = 8k + 3$ and $r = s = 1; t = 0$ the bordered construction over $\mathbb{F}_2$ yields a Type II code

The special case $q = p$ is Karlin (1969) construction

In particular $q = 11$ yields the extended Golay code

9

Pless symmetry codes Codes

When $q = 6k + 5$ and $r = 0; s = 1; t = 2$
the bordered construction over $\mathbb{F}_3$ yields (with $\alpha = 0, \beta = 1, \gamma = \pm 1$) a Type III code

The special case $q = p$ is Pless (1969) construction

In particular $q = 5$ yields the extended Golay code

10

Two class association schemes

Let X be a set of size v.
A two class association scheme on X is a partition of $X \times X$ into three relations R_0, R_1, R_2 such that

1. $R_0 = \{(x,x) | \ x \in X\}$
2. $R_i^T = R_j$ for some $j = 0, 1, 2$
3. for any triple $i, j. k$ the number of $z \in X$ such that $(x,z) \in R_i$ and $(z,y) \in R_j$ is a constant p_{ij}^k which does not depend on the choice of x and y that satisfy $(x,y) \in R_k$.

By Higman (1975) such a scheme is commutative:
i.e. $p_{ij}^k = p_{ji}^k$ for any triple of indices i, j, k.

11

Two class association schemes=SRG+DRT

The Bose-Mesner algebra of a 2-class association scheme is spanned over $\mathbf{C}$ by the adjacency matrices $A_0 = I, A_1, A_2$ of the relations R_i.
Either $A_1^T = A_1, A_2^T = A_2$ and then the undirected graph (X, R_1) is a SRG with parameters $(v, \kappa := p_{11}^0, \lambda := p_{11}^1, \mu := p_{11}^2)$;

$$A^2 = \kappa I + \lambda A + \mu(J - I - A),$$

or $A_1^T = A_2, A_2^T = A_1$ and the directed graph (X, R_1) is a DRT with parameters $(v, \kappa := p_{12}^0, \lambda := p_{11}^1, \mu := p_{11}^2)$.

$$A^2 = \lambda A + \mu(J - I - A)$$

12

DC codes from 2-class association schemes

For arbitrary scalars $r, s, t \in R$ the code alphabet let

$$Q_R(r,s,t) = (rI + sA + t(J - I - A)).$$

The pure construction is

$$\mathcal{P}_R(r,s,t) = (I \mid Q_R(r,s,t)).$$

The bordered construction is

$$\mathcal{B}_R(r,s,t) = \left(\begin{array}{c|c|c|c} 1 & 0\ldots0 & \alpha & \beta\ldots\beta \\ \hline 0 & & \gamma & \\ \vdots & I & \vdots & Q_R(r,s,t) \\ 0 & & \gamma & \end{array}\right).$$

13

Parameters

The code $P_R(r,s,t)$ is a code over R of length $2v$ and the code $B_R(r,s,t)$ is a code over R of length $2v+2$.

The code $P_R(r,s,t)$ is a free code over any ring R with $|R|^v$ elements and the code $B_R(r,s,t)$ is a free code over any ring R with $|R|^{v+1}$ elements.

14

Our contribution

For the five alphabets $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{Z}_4$ we give general conditions on r, s, t and α, β, γ (using matrix equations for SRG s and DRTs) for the pure and bordered constructions to yield self-dual Type I,II, III, IV codes.

- We thus generalize Gaborit's QDC and some double circulant constructions over $\mathbb{Z}_4$
- We construct self dual codes invariant under finite sporadic simple groups
- When we have enough DRT or SRG s with the same parameters we construct some codes with high minimum distance

15

The octacode

The code of length 8 over $\mathbb{Z}_4$ obtained from the bordered construction with $r = 1, s = 1, t = -1$ and $\alpha = 2, \beta = 1, \gamma = 3$ is
a Type II code of length 8 the octacode
related to the holey construction of the Leech lattice
and the Gray map construction of the Nordstrom Robinson code

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 3 & 0 & 1 & 3 \\ 0 & 0 & 1 & 0 & 3 & 3 & 0 & 1 \\ 0 & 0 & 0 & 1 & 3 & 1 & 3 & 0 \end{bmatrix}.$$

Conway & Sloane construction (1993)
$(I, H + I)$ where H is skew Hadamard matrix

16

Lifting Karlin binary construction (I)

Calderbank and Sloane (1997) consider for $q = p \equiv 3 \pmod 8$

$$\left(\begin{array}{c|c|c|c} 1 & 1\ldots1 & 1 & 1\ldots1 \\ \hline 0 & & 0 & \\ \vdots & I & \vdots & b(I+Q) \\ 0 & & 0 & \end{array}\right).$$

This generator matrix is equivalent (up to top row reduction)
to our bordered case $B_{\mathbb{Z}_4}(b, b, 0)$, (with $b = \pm 1$)

17

Lifting Karlin binary construction (II)

Calderbank and Sloane (1997) consider for $q = p \equiv 11 \pmod{16}$

$$\left(\begin{array}{c|c|c|c} 1 & 1\ldots1 & 1 & 1\ldots1 \\ \hline 0 & & 0 & \\ \vdots & I & \vdots & I+3Q+2N \\ 0 & & 0 & \end{array}\right).$$

This is our $B_{\mathbb{Z}_4}(2, 1, 3)$, for suitable α, β, γ.
The code of length 24 over $\mathbb{Z}_4$ obtained in that way with $\alpha = 2, \beta = 1, \gamma = 3$ has $d_E = 16$,
according to Bell Labs Cray
Construction A therefore yields the Leech lattice.
Chapman (2000) gave a computer free proof of that.

18

Some special SRGs

The Petersen graph with parameters $(10,3,0,1)$ yields by bordered construction $(4,3,0)$ with $\alpha=3,\beta=4,\gamma=1$ a [22,11,6] self-dual code over $\mathbb{F}_5$, with automorphism group S_5.
The Shrikhande graph with parameters $(16,6,2,2)$ yields by pure construction $(1,1,0)$ an extremal Type II $[32,16,8]$ code.
The Clebsch graph with parameters $(16,10,6,6)$ yields by pure construction $(1,0,1)$ an extremal Type II $[32,16,8]$ code.
The three Chang graphs with parameters $(28,12,6,4)$ yield by pure construction $(0,0,1)$ three Type II $[56,28,8]$ code.
The Hoffman-Singleton graph with parameters $(50,7,0,1)$ yields by pure construction $(1,0,\omega)$ a $[100,50,14]$ hermitian self-dual code over $\mathbb{F}_4$.
The Gewirtz graph with parameters $(56,10,0,2)$ yields by pure construction $(1,1,0)$ a Type II $[112,56,12]$ code.

19

General constructions of SRGs (I)

The Hamming graph $H(2,q)$ (a.k.a. $L(K_{q,q})$, a.k.a. Square Lattice Graph) is a $(q^2,2q-2,q-2,2)$ SRG.
If q is even then $P_{\mathbb{F}_2}(0,0,1)$ is a Type I code and $P_{\mathbb{F}_2}(1,1,0)$ is a Type II code.
Example: For $q=4$ the code $P_{\mathbb{F}_2}(1,1,0)$ is an extremal Type II $[32,16,8]$ code.

The graph Johnson graph $J(q,2)$ (a.k.a. $L(K_q)$,a.k.a. Triangular Graph) is a $(\binom{q}{2},2q-4,q-2,4)$ SRG.

- If $q\equiv 0 \pmod 4$ then $P_{\mathbb{F}_2}(0,0,1)$ is self-dual.
- If q is even then $P_{\mathbb{F}_2}(1,1,0)$ is a self-dual code.

Example: For $q=6$ the code $P_{\mathbb{F}_2}(1,1,0)$ is an optimal Type I $[30,15,6]$ code.

20

General constructions of SRGs (II)

An Orthogonal array $OA(h,n)$ is a system of $h-2$ mutually orthogonal Latin squares.
The vertices of the SRG are the cells of the squares.
Two cells are adjacent if they share a row or column or an entry in one of the squares.
This forms an SRG of parameters $(n^2, h(n-1), n-2+(h-1)(h-2), h(h-1))$.
Depending on the parity of n and h the pure construction yields self dual binary codes for suitable r, s, t.

21

General constructions of SRGs (III)

A Steiner triple system on N points is a $2-(N,3,1)$ design.
The vertices of the SRG are the blocks. Declare two block adjacent if they intersect in at least one point.
This yields an SRG with parameters $(N(N-1)/6, 3(N-3)/2, (N+3)/2, 9)$.
If $n \equiv 7 \pmod 8$ then $P_{\mathbb{F}_2}(1,0,1)$ is self-dual.

22

Rank three groups

Historically, the concept of SRGs was motivated by the action of sporadic simple groups on certain graphs
The Higman Sims graph a $(100, 36, 14, 12)$ SRG produces two binary [200,100,12] codes (Type I and Type II, respectively).
The Hall Janko Wales graph a $(100, 22, 0, 6)$ SRG produces two binary [200,100,16] codes (Type I and Type II, respectively).
The codes constructed from SRG's invariant under
Suzuki, Conway2, Rudvalis, Fischer22, Fischer23, Fischer24,
are too long for their minimum distance to be computed.

23

Magma database

There are *exactly* 32 548 SRGs with parameters $(36, 15, 6, 6)$ (Spence and McKay)
By pure construction $(1, 0, 1)$ we obtain at least 4 non equivalent $[72, 36, 12]$ Type I codes.
By pure construction $(0, 1, 0)$ we obtain at least 29 $[72, 36, 12]$ Type II codes
They seem to be different from the codes constructed so far in the literature.
(Doncheva 2001, Dougherty, Gulliver, Harada 1997)
Novelty and non equivalence are proved by comparing kissing numbers.
Since $35 = 5 \times 7$ we are not using quadratic residues!

24

Conclusion and Open Problems

To obtain good codes one needs to sieve thru large databases: success rate is one per thousand!

- extend Magma SRG database to higher v's
- Magma DRT database?
- Good (long) codes from "prolific" infinite families of SRG
- three class association schemes ?

25

Designs from Subcode Supports of Linear Codes

Keisuke SHIROMOTO*
Department of Information Systems
Aichi Prefectural University
Nagakute, Aichi 480-1198, Japan
keisuke@ist.aichi-pu.ac.jp

Abstract

The purpose of this work is to study designs which are constructed from subcode supports for a linear code over a finite field. In particular, we obtain the strengthening of the two celebrated methods for the constructions of designs from linear codes, the automorphism characterization and the Assmus-Mattson theorem.

1 Introduction

One of the important problems in design theory is to consider the existence of a design with given parameters and give a construction of a design. There are a large number of researches in the constructions of designs from linear codes (see Chapter V.1 in [3], also Chapter 15 in [12]). For instance, the Assmus-Mattson theorem ([1]) gives a sufficient condition for which the set of supports for all codewords of a certain weight in a linear code forms a t-design. And a lot of new designs have been constructed from the theorem. Moreover it is known that the automorphism group of a linear code is t-transitive, then the set of codeword supports forms a t-design.

The generalized Hamming weights for a linear code over a finite field were introduced by Wei as an application in keyless cryptography ([16]). He also gave the characterization of the performance of a linear code on the wire-tap channel II from its weight hierarchy. The support and the support weight of a subcode are exactly generalizations of the support and the Hamming weight of a codeword in a linear code. And so the generalized Hamming weight is the minimum support weight among all subcodes of a certain dimension and is precisely a generalization of the minimum Hamming weight of a linear code. The support weight enumerator for a linear code over a finite field was first introduced in [5] as a generalization of the Hamming weight enumerators. Currently, many researchers have investigated the

*This work is a part of the joint work with Thomas Britz, University of New South Wales, Australia

generalized Hamming weights for various classes of linear codes and their applications (e.g. [15]).

The purpose of this work is to find an application of the generalized Hamming weights to the constructions of t-designs from linear codes.

2 Definitions and Notation

Throughout this paper, we let $\mathbb{F}_q$ denote the finite field of q elements. For each vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ and each subset $D \subseteq \mathbb{F}_q^n$, we define the *supports* and *weights* of $\boldsymbol{x}$ and D respectively as follows:

$$\begin{aligned} \mathrm{supp}(\boldsymbol{x}) &:= \{i \mid x_i \neq 0\}; \\ \mathrm{Supp}(D) &:= \bigcup_{\boldsymbol{x} \in D} \mathrm{supp}(\boldsymbol{x}); \\ \mathrm{wt}(\boldsymbol{x}) &:= |\mathrm{supp}(\boldsymbol{x})|; \\ \mathrm{wt}(D) &:= |\mathrm{Supp}(D)|. \end{aligned}$$

Let C be an $[n, k]$ code over $\mathbb{F}_q$, let $r, i \geq 1$ be integers with $r \leq k$ and $i \leq n$, and define

$$\begin{aligned} \mathcal{D}_r(C) &:= \{D \ : \ D \text{ is an } [n, r] \text{ subcode of } C\}; \\ \mathcal{S}_r(C) &:= \{\mathrm{Supp}(D) \ : \ D \in \mathcal{D}_r(C)\} \quad \text{(multiset)}; \\ \mathcal{S}_{r,i}(C) &:= \{X \in \mathcal{S}_r(C) \ : \ |X| = i\} \quad \text{(multiset)}; \\ d_r(C) &:= d_r = \min\{|X| \ : \ X \in \mathcal{S}_r(C)\}. \end{aligned}$$

Note that $\mathcal{S}_1(C)$ is the multiset of supports of all codewords in C and $d_1 = d$ is the minimum Hamming weight of C. The *weight hierarchy* of C is the set of integers $\{d_r(C) : 1 \leq r \leq k\}$. The following inequalities are well-known ([16]):

$$\begin{aligned} &1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n; \\ &(q^r - 1)d_{r-1}(C) \leq (q^r - q)d_r(C). \end{aligned}$$

For each integer r with $1 \leq r \leq k$, the *r-th support weight enumerator* $SW_C^{(r)}(x, y)$ of C is defined as follows:

$$SW_C^{(r)}(x, y) := \sum_{i=0}^{n} A_i^{(r)} x^{n-i} y^i,$$

where

$$A_i^{(r)} = A_i^{(r)}(C) := |\{D \in \mathcal{D}_r(C) \ : \ \mathrm{wt}(D) = i\}|.$$

We note that $W_C(x, y) = x^n + (q-1)SW_C^{(1)}(x, y)$ is the Hamming weight enumerator of C.

A t-(v, k, λ) *design* is a collection $\mathcal{B}$ of k-subsets (called *blocks*) of a set V with v *points*, such that any t-subset of V is contained in exactly λ blocks. A design is called *simple* if all the blocks are distinct, otherwise the design is said to have *repeated blocks* (cf. [3]). The following lemma is easy to prove.

Lemma 2.1 *Let $(V, \mathcal{B})$ be a simple t-(v, k, λ) design and let $\mathcal{B}'$ be a multiset of $\mathcal{B}$. If $(V, \mathcal{B}')$ is a t-(v, k, λ') design with repeated blocks, then $(V, \mathcal{B}' \setminus \mathcal{B})$ is also a t-$(v, k, \lambda' - \lambda)$ design possibly with repeated blocks.*

In [1], E. F. Assmus, Jr. and H. F. Mattson, Jr. found a sufficient condition for the codewords of a certain weight in a linear code over a finite field to form a t-design:

Theorem 2.2 (The Assmus-Mattson theorem) *Let C be an $[n, k, d]$ code over $\mathbb{F}_q$, and let $d^\perp$ denote the minimum nonzero weight of the dual code $C^\perp$. Let $w = n$ when $q = 2$ and otherwise let w be the largest integer satisfying*

$$w - \left\lfloor \frac{w + q - 2}{q - 1} \right\rfloor < d,$$

defining $w^\perp$ similarly. Suppose there is an integer t with $0 < t < d$ that satisfies the following condition: the number of indices i $(1 \le i \le n - t)$ such that $A_i^{(1)}(C^\perp) \neq 0$ is at most $d - t$. Then for each i with $d \le i \le w$, the set of supports of codewords in C of weight i, provided there are any, yield a simple t-design. Similarly, for each j with $d^\perp \le j \le \min\{w^\perp, n - t\}$, the set of supports of codewords in $C^\perp$ of weight j, provided there are any, form a simple t-design.

3 Codes With t-transitive Automorphism Groups

Let C be an $[n, k]$ code over $\mathbb{F}_q$ with coordinates E. A *field automorphism* σ on $\mathbb{F}_q$ is a bijection on $\mathbb{F}_q$ such that $(a+b)\sigma = a\sigma + b\sigma$ and $(ab)\sigma = (a\sigma)(b\sigma)$ for all $a, b \in \mathbb{F}_q$. Consider maps of the form $v \mapsto vPD_1D_2$, where P is an $n \times n$ permutation matrix and $D_1 = \mathrm{diag}(a_1, \ldots, a_n)$ and $D_2 = \mathrm{diag}(\sigma_1, \ldots, \sigma_n)$ are diagonal matrices such that $a_1, \ldots, a_n \in \mathbb{F}_q$ are non-zero scalars and $\sigma_1, \ldots, \sigma_n$ are field automorphisms of $\mathbb{F}_q$. The set of such maps that map C onto itself may be called the *general automorphism group* of C and is denoted by $\Delta\mathrm{Aut}(C)$. It is said to be *t-transitive* if, for each pair of t-subsets $T_1, T_2 \subseteq E$, there exists an element $\delta = P'D_1'D_2' \in \Delta\mathrm{Aut}(C)$ for which the permutation π' on E associated to P' maps T_1 to T_2, i.e., $T_1\pi' = T_2$. Note that each element $g \in \Delta\mathrm{Aut}(C)$ maps the set of r-dimensional subcodes of C with weight i onto itself for all $r, i \ge 1$. Then we have the following result:

Theorem 3.1 *If $\Delta\mathrm{Aut}(C)$ is t-transitive, then $\mathcal{S}_{r,i}(C)$ forms a t-design possibly with repeated blocks for all $r \ge 1$, $i \ge t$.*

A related result, on automorphism groups of matroids associated to C, was proved in [2].

4 Designs from Subcodes

In this section, we investigate designs from subcode supports by considering the support weight enumerator. In particular, we give a generalization of the Assmus-Mattson theorem for subcode supports.

Let C be an $[n,k,d]$ code over $\mathbb{F}_q$ with coordinates E. For a positive integer m, we define the *m-ply weight enumerator* of C by

$$W_C^{[m]}(x,y) := \sum_{i=0}^{n} P_i^{[m]}(C) x^{n-i} y^i ,$$

where

$$P_i^{[m]}(C) = \left| \{ (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m) \in C \times \cdots \times C \ : \ |\mathrm{supp}(\boldsymbol{x}_1) \cup \cdots \cup \mathrm{supp}(\boldsymbol{x}_m)| = i \} \right| .$$

Shiromoto [13] proved the following MacWilliams-type identity.

Theorem 4.1 $W_{C^\perp}^{[m]}(x,y) = q^{-km} W_C^{[m]}(x + (q^m - 1)y, x - y)$.

In [14], it was proved that if G is a generator matrix of C, then the enumerator is consistent with the Hamming weight enumerator of *the code* $C^{(m)}$ having generator matrix G over the extended field $\mathbb{F}_{q^m}$. Then we immediately obtain the following lemma (cf. [6]).

Lemma 4.2 *For each subset* $S \subseteq \{1, \ldots, n\}$, *the coefficients* $P_i^{[m]}(C^\perp), i < |S|$ *and* $P_j^{[m]}(C)$, $j \notin S$ *together uniquely determine the coefficients* $P_i^{[m]}(C^\perp)$, $i \geq |S|$ *and* $P_j^{[m]}(C)$, $j \in S$.

By identities proved in [4, 7, 14], we also have the following equations:

$$P_i^{[m]}(C) = \sum_{r=0}^{m} [m]_r A_i^{(r)}(C) ; \tag{4.1}$$

$$A_i^{(r)}(C) = \sum_{j=0}^{r} (-1)^{r-j} \frac{[r]_j}{[r]_r [j]_j} q^{\binom{r-j}{2}} P_i^{[j]}(C) , \tag{4.2}$$

where $[a]_b = \prod_{i=0}^{b-1} (q^a - q^i)$.

For each positive integer m, set

$$\mathcal{L}_{m,t} := \left\{ i \in \{ d_m^\perp, \ldots, n - t \} \ : \ P_i^{[m]}(C^\perp) \neq 0 \right\} .$$

Then the following result generalizes the Assmus-Mattson Theorem for subcode supports.

Theorem 4.3 *Let* C *be an* $[n,k,d]$ *code over* $\mathbb{F}_q$ *and suppose that* $m, t \geq 1$ *are integers with* $t < d$ *such that* $|\mathcal{L}_{\mu,t}| \leq d_\mu - t$ *for each* μ *with* $1 \leq \mu \leq m$. *Then for all* $i \geq d_m$ *and* $j \geq d_m^\perp$ $\mathcal{S}_{m,i}(C)$ *and* $\mathcal{S}_{m,j}(C^\perp)$ *each form a* t*-design possibly with repeated blocks.*

Remark 4.4 The t-design obtained from a multiset $\mathcal{S}_{m,i}(C)$ in Theorem 4.3 is guaranteed not to have repeated blocks (i.e., $\mathcal{S}_{m,i}(C)$ is a set) if

$$m = 1 \quad \text{and} \quad i \leq w, \qquad \text{or} \qquad m \geq 1 \quad \text{and} \quad d_m \leq i < d_{m+1},$$

where w is as defined in the Assmus-Mattson Theorem. Note that these are not necessary conditions. Analogue remarks hold for the t-designs obtained from the multisets $\mathcal{S}_{m,j}(C^\perp)$ in Theorem 4.3.

For each positive integer m, set

$$\mathcal{T}_{m,i}(C) := \{\, \mathrm{supp}(\boldsymbol{x}) \ : \ \boldsymbol{x} \in C^{(m)},\ \mathrm{wt}(\boldsymbol{x}) = i \,\} \ \text{(multiset)}.$$

Corollary 4.5 *If an $[n,k,d]$ code C over $\mathbb{F}_q$ satisfies the same conditions as in Theorem 4.3, then for all $d \le i$ and $d^\perp \le j$ $\mathcal{T}_{m,i}(C)$ and $\mathcal{T}_{m,j}(C^\perp)$ each form a simple t-design.*

5 Examples

In this section, we shall give several examples of t-designs obtained from binary codes by using Theorem 3.1, Theorem 4.3 and Corollary 4.5.

5.1 The Binary Golay Codes

Let G_{22}, G_{23} and G_{24} be the binary shortened Golay $[22,11,6]$ code, the binary Golay $[23,11,8]$ code and the binary extended Golay $[24,12,8]$ code, respectively. Since $\Delta\mathrm{Aut}(G_{22})$ is 3-transitive, both of $\Delta\mathrm{Aut}(G_{23})$ and $\Delta\mathrm{Aut}(G_{23}^\perp)$ are 4-transitive and $\Delta\mathrm{Aut}(G_{24})$ is 5-transitive (eg. [9]), all of $\mathcal{S}_{r,i}(G_{22}), \mathcal{S}_{r,j}(G_{23}), \mathcal{S}_{r,l}(G_{23}^\perp)$ and $\mathcal{S}_{r,w}(G_{24})$ form a 3-, 4- and 5-designs possibly with repeated blocks, respectively, for all $r \ge 1$, $i \ge 6, j \ge 8, l \ge 7, w \ge 8$, from Theorem 3.1. Then Figure 1, 2, 3 and 4 below present the r-th support weight distributions $A_i^{(r)}(C)$ for each $C \in \{G_{22}, G_{23}, G_{23}^\perp, G_{24}\}$ and all $r \ge 1$, by displaying the values of the non-zero coefficients $A_i^{(r)}$, empty entries for zero-coefficients and the values of λ for all obtained designs. And the character $*$ denotes a simple design from Remark 4.4. For instance, the second support weight enumerator $A_{G_{22}}^{(2)}(1,y)$ of C is

$$A_{G_{22}}^{(2)}(1,y) = 2984y^{22} + 62370y^{20} + 228690y^{18} + 251867y^{16} + 122430y^{14} + 27566y^{12} + 2310y^{10},$$

and $\mathcal{S}_{2,10}(G_{22})$ forms a simple 3-$(22,10,180)$ design.

5.2 The Extremal Doubly-Even Self-Dual $[32,16,8]$ Codes

It is well-known that there are only 5 inequivalent codes RM(2,5), QR, F, G and U (cf. [8]) and $d_2 = 12, d_3 = 14$ (see [11]). For any $C \in \{\mathrm{RM}(2,5), \mathrm{QR}, \mathrm{F}, \mathrm{G}, \mathrm{U}\}$, we have

$$A_C^{(1)}(1,y) = y^{32} + 620y^{24} + 13888y^{20} + 36518y^{16} + 13888y^{12} + 620y^8$$

$$A_C^{(2)}(1,y) = 163897y^{32} + 7805056y^{30} + 64101800y^{28} + 178655232y^{26} + 230100600y^{24} + 158045440y^{22} + 60326000y^{20} + 14443520y^{18} + 2006010y^{16} + 138880y^{14} + 8680y^{12}$$

$$W_C^{[2]}(1,y) = 983385y^{32} + 46830336y^{30} + 384610800y^{28} + 1071931392y^{26} + 1380605460y^{24} + 948272640y^{22} + 361997664y^{20} + 86661120y^{18} + 12145614y^{16} + 833280y^{14} + 93744y^{12} + 1860y^8 + 1$$

Since $\mathcal{L}_{1,3} = \{8,12,16,20,24\}$ and $\mathcal{L}_{2,3} = \{12,14,16,18,20,22,24,26,28\}$, it follows from Theorem 4.3 and Corollary 4.5 that each of $\mathcal{S}_{1,i}(C)$, $\mathcal{S}_{2,j}(C)$ and $\mathcal{T}_{2,l}(C)$ forms a 3-design for each $i \in \{8,12,16,20,24\}, j \in \{12,14,16,18,20,22,24,26,28,30,32\}, l \in \{8,12,14,16,18,20,22,24,26,28,30,32\}$.

We list the obtained 3-designs below.

Remark 5.1 We find that the set $\mathrm{Set}(\mathcal{S}_{2,16}(C))$ of the multiset $\mathcal{S}_{2,16}(C)$ forms a simple 3-$(32,16,225995)$ design having 2001670 blocks by calculation. By Lemma 2.1, we have that $\mathcal{S}_{2,16}(C) \setminus \mathrm{Set}(\mathcal{S}_{2,16}(C))$ forms a 3-$(32,16,490)$ design possibly with repeated blocks.

set of blocks	3-$(32,k,\lambda)$designs	set of blocks	3-$(32,k,\lambda)$designs	set of blocks	3-$(32,k,\lambda)$designs
$\mathcal{S}_{1,8}(C)$	(8, 7)	$\mathcal{S}_{1,12}(C)$	(12, 616)	$\mathcal{S}_{1,16}(C)$	(16, 4123)
$\mathcal{S}_{1,20}(C)$	(20, 3192)	$\mathcal{S}_{1,24}(C)$	(24, 253)	$\mathcal{S}_{2,12}(C)$	(12, 385)
$\mathcal{S}_{2,14}(C)$	(14, 10192)	$\mathcal{S}_{2,16}(C)$	(16, 226485)	$\mathcal{S}_{2,18}(C)$	(18, 2376192)
$\mathcal{S}_{2,20}(C)$	(16, 13865250)	$\mathcal{S}_{2,22}(C)$	(22, 49070560)	$\mathcal{S}_{2,24}(C)$	(24, 93895890)
$\mathcal{S}_{2,26}(C)$	(26, 93649920)	$\mathcal{S}_{2,28}(C)$	(28, 42338205)	$\mathcal{S}_{2,30}(C)$	(30, 6388816)
$\mathcal{S}_{2,32}(C)$	(32, 163897)	$\mathcal{T}_{2,8}(C)$	(8, 21)	$\mathcal{T}_{2,12}(C)$	(12, 4158)
$\mathcal{T}_{2,14}(C)$	(14, 61152)	$\mathcal{T}_{2,16}(C)$	(16, 1371279)	$\mathcal{T}_{2,18}(C)$	(18, 14257152)
$\mathcal{T}_{2,20}(C)$	(16, 83201076)	$\mathcal{T}_{2,22}(C)$	(22, 294423360)	$\mathcal{T}_{2,24}(C)$	(24, 563376099)
$\mathcal{T}_{2,26}(C)$	(26, 561899520)	$\mathcal{T}_{2,28}(C)$	(28, 254029230)	$\mathcal{T}_{2,30}(C)$	(30, 38332896)
$\mathcal{T}_{2,32}(C)$	(32, 983385)				

Table 1: 3-designs from subcode supports for the five $[32, 16, 8]$ codes

5.3 The Extremal Doubly-Even Self-Dual $[48, 24, 12]$ Codes

It is well-known that there is only one code and $d_2 = 18, d_3 \geq 21$.

$$A_C^{(1)}(1,y) = y^{48} + 17296y^{36} + 535095y^{32} + 3995376y^{28} + 7681680y^{24} + 3995376y^{20} + 535095y^{16} + 17296y^{12}$$

$$\begin{aligned} A_C^{(2)}(1,y) = {} & 99273682y^{48} + 11795491488y^{46} + 227081475720y^{44} + 1589848008672y^{42} + 5432928694380y^{40} \\ & + 10464210515616y^{38} + 12381654787320y^{36} + 9527550547680y^{34} + 4947166777905y^{32} + 1782244008160y^{30} \\ & + 453764840760y^{28} + 82241961120y^{26} + 10803665340y^{24} + 1030807008y^{22} + 64211400y^{20} + 2663584y^{18} \end{aligned}$$

$$\begin{aligned} W_C^{(2)}(1,y) = {} & 595642095y^{48} + 70772948928y^{46} + 1362488854320y^{44} + 9539088052032y^{42} + 32597572166280y^{40} \\ & + 62785263093696y^{38} + 74289928775808y^{36} + 57165303286080y^{34} + 29683002272715y^{32} + 10693464048960y^{30} \\ & + 2722601030688y^{28} + 493451766720y^{26} + 64845037080y^{24} + 6184842048y^{22} + 397254528y^{20} + 15981504y^{18} \\ & + 1605285y^{16} + 51888y^{12} + 1 \end{aligned}$$

Since $\mathcal{L}_{1,5} = \{12, 16, 20, 24, 28, 32, 36\}$ and $\mathcal{L}_{2,5} = \{18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42\}$, it follows from Theorem 4.3 and Corollary 4.5 that each of $\mathcal{S}_{1,i}(C)$, $\mathcal{S}_{2,j}(C)$ and $\mathcal{T}_{2,l}(C)$ forms a 3-design for each $i \in \{12, 16, 20, 24, 28, 32, 36\}$, $j \in \{18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48\}$, $l \in \{12, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42\}$.

We list the obtained 5-designs below.

set of blocks	5-$(48,k,\lambda)$designs	set of blocks	5-$(48,k,\lambda)$designs	set of blocks	5-$(48,k,\lambda)$designs
$\mathcal{S}_{1,12}(C)$	(12, 8)	$\mathcal{S}_{1,16}(C)$	(16, 1365)	$\mathcal{S}_{1,20}(C)$	(20, 36176)
$\mathcal{S}_{1,24}(C)$	(24, 190680)	$\mathcal{S}_{1,28}(C)$	(28, 229320)	$\mathcal{S}_{1,32}(C)$	(32, 62930)
$\mathcal{S}_{1,36}(C)$	(36, 3808)	$\mathcal{S}_{2,18}(C)$	(18, 13328)	$\mathcal{S}_{2,20}(C)$	(20, 581400)
$\mathcal{S}_{2,22}(C)$	(22, 15853068)	$\mathcal{S}_{2,24}(C)$	(24, 268176090)	$\mathcal{S}_{2,26}(C)$	(26, 3159413400)
$\mathcal{S}_{2,28}(C)$	(28, 26044445700)	$\mathcal{S}_{2,30}(C)$	(30, 148326736740)	$\mathcal{S}_{2,32}(C)$	(32, 581812959070)
$\mathcal{S}_{2,34}(C)$	(34, 1548263687520)	$\mathcal{S}_{2,36}(C)$	(36, 2726025753360)	$\mathcal{S}_{2,38}(C)$	(38, 3067461592468)
$\mathcal{S}_{2,40}(C)$	(40, 2087777955510)	$\mathcal{S}_{2,42}(C)$	(42, 789832194424)	$\mathcal{S}_{2,44}(C)$	(44, 144023665940)
$\mathcal{S}_{2,46}(C)$	(46, 9442667388)	$\mathcal{S}_{2,48}(C)$	(48, 99273682)	$\mathcal{T}_{2,12}(C)$	(12, 24)
$\mathcal{T}_{2,16}(C)$	(16, 4095)	$\mathcal{T}_{2,18}(C)$	(18, 79968)	$\mathcal{T}_{2,28}(C)$	(20, 3596928)
$\mathcal{T}_{2,22}(C)$	(22, 95118408)	$\mathcal{T}_{2,24}(C)$	(24, 1609628580)	$\mathcal{T}_{2,26}(C)$	(26, 18956480400)
$\mathcal{T}_{2,28}(C)$	(28, 156267362160)	$\mathcal{T}_{2,30}(C)$	(30, 889960420440)	$\mathcal{T}_{2,32}(C)$	(32, 3490877943210)
$\mathcal{T}_{2,34}(C)$	(34, 9289582125120)	$\mathcal{T}_{2,36}(C)$	(36, 16356154531584)	$\mathcal{T}_{2,38}(C)$	(38, 18404769554808)
$\mathcal{T}_{2,40}(C)$	(40, 12526667733060)	$\mathcal{T}_{2,42}(C)$	(42, 4738993166544)	$\mathcal{T}_{2,44}(C)$	(44, 864141995640)
$\mathcal{T}_{2,46}(C)$	(46, 56656004328)	$\mathcal{T}_{2,48}(C)$	(48, 595642095)		

Table 2: 5-designs from subcode supports for the $[48, 24, 12]$ code

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combinatorial Theory* **6** (1969), 122–151.

[2] T. Britz and K. Shiromoto, An Assmus-Mattson theorem for matroids, Preprint (2005).

[3] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton, 1996.

[4] T. A. Dowling, Codes, packings and the critical problem, in: *Applicazioni (Univ. Perugia, Perugia, 1970)*, (Ist. Mat., Univ. Perugia, Perugia, 1971), 209–224.

[5] T. Helleseth, T. Kløve and J. Mykkeltveit, The weight distribution of irreducible cyclic codes with block length $n_1((q^l-1)/N)$, *Discrete Mathematics* **18** (1977), pp. 179–211.

[6] W. C. Huffman and V. S. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge, 2003.

[7] T. Kløve, The weight distribution of linear codes over $GF(q^l)$ having generator matrix over $GF(q)$, *Discrete Math.* **106/107** (1992), 311–316.

[8] H. Koch, On self-dual, doubly-even codes of length 32, *J. Combin. Theory, Ser. A* **51** (1989), 63–76.

[9] The Magma Computational Algebra System for Algebra, Number Theory and Geometry, Version 2.12, University of Sydney, 2005.

[10] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, 16., North-Holland Publishing Company, Amsterdam, 1978.

[11] O. Milenkovic, The third support weight enumerators of the doubly-even, self-dual $[32, 16, 8]$ codes, *IEEE Trans. Inform. Theory* **49** (2003), 741–746.

[12] V. S. Pless and W. C. Huffman (editors), *Handbook of Coding Theory II*, Elsevier Science B.V., 1998.

[13] K. Shiromoto, A new MacWilliams type identity for linear codes, *Hokkaido Math. J.* **25** (1996), 651–656.

[14] K. Shiromoto, The weight enumerator of linear codes over $GF(q^m)$ having generator matrix over $GF(q)$, *Des. Codes Cryptogr.* **16** (1999), 87–92.

[15] M. A. Tsfasman and S. G. Vlădut, Geometric approach to higher weights, *IEEE Trans. Inform. Theory* **41** (1995) pp. 1564–1588.

[16] V.K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37** (1991) pp. 1412–1418.

i\r	1	2	3	4	5	6	7	8	9	10	11
22	1	2704	2723336	210640210	1778821572	2532783638	736249877	47238930	675752	2025	1
	(1)*	(2704)	(2723336)	(210640210)	(1778821572)	(2532783638)	(736249877)	(47238930)	(675752)	(2025)	(1)
21			8451520	308230360	1252420400	884583632	120731600	3603060	22044	22	
			(7299040)	(286208720)	(1081635800)	(746685864)	(104268200)	(3110870)	(19038)	(19)	
20		62370	12859770	215187588	417324600	137475030	8809275	113421	231		
		(46170)	(9510570)	(150294708)	(308028600)	(101707230)	(6587775)	(83961)	(171)		
19			12073600	94588320	86028080	13170090	303440	1540			
			(7090960)	(59504352)	(54508186)	(8286888)	(228684)	(969)			
18		228690	8285200	29498700	12361580	708490	7315				
		(121176)	(4900080)	(15630480)	(6550032)	(423096)	(3876)				
17			4139520	6800640	1208592	25872					
			(1827840)	(3002880)	(533664)	(11424)					
16	77	251867	1725955	1176175	70763	77					
	(28)*	(91588)	(627620)	(427700)	(25732)	(28)					
15			542080	130944	1232						
			(160160)	(38688)	(364)						
14	330	122430	128040	9570							
	(78)*	(28938)	(30264)	(2262)							
13			24640								
			(4570)								
12	616	27566	2310								
	(88)*	(3938)	(330)								
11											
10	616	2310									
	(48)*	(180)									
9											
8	330										
	(12)*										
7											
6	77										
	(1)*										

Figure 1: $\{A_i^{(r)}(G_{22})\}$ and the obtained 3-designs

i\r	1	2	3	4	5	6	7	8	9	10	11
23			2366056	197474090	1723640424	2494070964	730800367	47075710	674751	2024	1
			(2366056)	(197474090)	(1723640424)	(2494070964)	(730800367)	(47075710)	(674751)	(2024)	(1)
22		14168	7810110	302209580	1269080890	890380731	125338730	3754520	23023	23	
		(11704)	(6451830)	(249725740)	(1048371170)	(735530345)	(103540600)	(3101560)	(19010)	(19)	
21			12184480	220898280	443189208	148430040	9687370	123970	253		
			(8235360)	(149241060)	(299540856)	(100322280)	(6547590)	(83790)	(171)		
20		123970	12200740	102307128	90785150	14056005	416185	1771			
		(67830)	(6724860)	(55977192)	(52955850)	(8183205)	(227715)	(969)			
19			8642480	33471900	14532200	956340	8855				
			(3782976)	(14651280)	(6356640)	(418608)	(3876)				
18		255024	4781700	8182020	1519518	33649					
		(88128)	(1652400)	(2827440)	(525096)	(11628)					
17			1083520	1487640	99176						
			(533120)	(390840)	(26656)						
16	253	216315	646415	216315	253						
	(52)	(44460)	(132860)	(44460)	(52)						
15			212520	4554							
			(32760)	(702)							
14		70840	37050								
		(8008)	(4290)								
13											
12	1288	17710									
	(72)	(990)									
11											
10											
0											
8	506										
	(4)										

Figure 2: $\{A_i^{(r)}(G_{23})\}$ and the obtained 4-designs

i\r	1	2	3	4	5	6	7	8	9	10	11	12
23	1	5842	18976518	3162017276	553539979296	161344182373	96036517940	12782182127	302548222	2747327	4072	1
	(1)	(5842)	(18976518)	(3162017276)	(553539979296)	(161344182373)	(96036517940)	(12782182127)	(302548222)	(2747327)	(4072)	(1)
22		14168	62229308	4844203650	409128610642	58254021903	16033747171	1086405850	15542206	46575	23	
		(11704)	(51406804)	(4001723450)	(337975330226)	(48122887650)	(13088747663)	(897540050)	(12830288)	(38475)	(19)	
21		155848	98095690	3546103660	144039378998	9042717081	1388413400	81423690	253506	263		
		(105336)	(66301830)	(2306773020)	(9734887386)	(6720176367)	(938113800)	(270078630)	(171342)	(171)		
20		123970	97582100	1047965088	3190109606	1053966375	68227775	860561	1771			
		(67830)	(53391900)	(901681632)	(1750388034)	(576676125)	(373307725)	(475779)	(969)			
19		619850	70096180	545007540	498447950	75736815	2039780	6855				
		(271320)	(30682416)	(238560048)	(218180040)	(33151428)	(914736)	(3876)				
18		255024	37623124	135375240	56703878	3667741	33649					
		(88128)	(13001328)	(46781280)	(19595016)	(1267452)	(11628)					
17		765072	16326620	26033700	4657730	100947						
		(205632)	(4388720)	(6997200)	(1251880)	(27132)						
16	253	218315	5465535	3820165	241109							
	(52)	(44460)	(1122940)	(787020)	(49556)							
15	506	432630	1505350	437184	506							
	(78)	(66690)	(232050)	(67392)	(78)							
14		70840	392150	7590								
		(8008)	(44330)	(858)								
13		99176	53130									
		(8008)	(4290)									
12	1288	17710										
	(72)	(990)										
11	1288	17710										
	(48)	(660)										
10												
9												
8	506											
	(4)											
7	253											
	(1)											

Figure 3: The $\{A_i^{(r)}(G_{23}^{\perp})\}$ and the obtained 4-designs

i\r	1	2	3	4	5	6	7	8	9	10	11	12
24	1	5842	10010462	2984643186	536308388872	158850111409	95305717573	12735106417	391673471	2745303	4071	1
	(1)	(5842)	(10010462)	(2984643186)	(536308388872)	(158850111409)	(95305717573)	(12735106417)	(391673471)	(2745303)	(4071)	(1)
23			50785344	4739378160	413673701776	59857703136	17530208808	1129817040	16194024	48576	24	
			(44955064)	(3752007710)	(327491685058)	(47387348316)	(13885206973)	(894438400)	(12820269)	(38456)	(19)	
22		170016	93721320	3627594960	152289706830	10684676772	1504064760	45054240	276276	276		
		(105336)	(58066470)	(2247531660)	(94355340530)	(6619854067)	(931866219)	(27914040)	(171171)	(171)		
21			97475840	1766466240	3545513664	1167440320	77493960	991760	2024			
			(46667040)	(845704440)	(1697432184)	(568492020)	(37103010)	(474810)	(969)			
20		743820	73744440	613842768	580710900	89736570	2497110	10626				
		(271320)	(26890440)	(223908768)	(211623400)	(32732820)	(910860)	(3876)				
19			41483904	166566120	69706560	4500432	42504					
			(11348928)	(43953840)	(19060920)	(1255824)	(11628)					
18		1020096	19126800	3272808O	6078072	134596						
		(205632)	(3855600)	(6597360)	(1225224)	(27132)						
17			6800640	5100480	340032							
			(990050)	(742560)	(49504)							
16	759	648045	1039245	648945	759							
	(78)	(66690)	(199290)	(66690)	(78)							
15			566720	12144								
			(40040)	(858)								
14		170016	91080									
		(8008)	(4200)									
13												
12	2576	35420										
	(48)	(660)										
11												
10												
9												
8	759											
	(1)											

Figure 4: The $\{A_i^{(r)}(G_{24})\}$ and the obtained 5-designs

A new proof of the Assmus-Mattson theorem based on the Terwilliger algebra

Hajime Tanaka

Division of Mathematics, Graduate School of Information Sciences,
Tohoku University, Sendai, Japan
E-mail: htanaka@ims.is.tohoku.ac.jp

Dedicated to Professor Eiichi Bannai on the occasion of his 60th birthday

Abstract

We use the Terwilliger algebra to provide a new approach to the Assmus-Mattson theorem.

1 Introduction

The Terwilliger algebra [25, 26, 27] is an active area of research. See [28] and the references therein. The purpose of the present paper is to demonstrate how the theory of the Terwilliger algebra can also be applied to problems in coding theory.

The *Assmus-Mattson theorem* is a very famous theorem relating linear codes and combinatorial designs:

Theorem 1.1 (Assmus-Mattson [1]). *Let Y denote a linear code of length D over $\mathbb{F}_q$ with minimum weight δ. Let $Y^\perp$ denote the dual code of Y, with minimum weight δ^*. Suppose $t \in \{1, 2, \ldots, D\}$ is such that there are at most $\delta - t$ weights of $Y^\perp$ in $\{1, 2, \ldots, D-t\}$, or such that there are at most $\delta^* - t$ weights of Y in $\{1, 2, \ldots, D-t\}$. Then the supports of the words of any fixed weight in Y form a t-design.*

There are several proofs and strengthenings of this theorem. See [7, 6, 21, 2, 22] for instance. Delsarte [11] proved an Assmus-Mattson-type theorem for general cometric schemes, and Martin [15] studied the Assmus-Mattson theorem for Johnson schemes based on Delsarte's algebraic version. Theorem 1.1 has also been generalized to $\mathbb{Z}_4$-linear codes. See e.g., [23].

In this paper, we use the Terwilliger algebra to provide a new approach to Theorem 1.1. In fact, we prove three versions of the Assmus-Mattson theorem (Theorems 3.2, 4.3, 5.2) and two corollaries (Corollaries 3.5, 4.6). Theorem 4.3 coincides with Delsarte's version whereas Theorem 3.2 seems new and is the dual to Theorem 4.3 for general metric schemes. Both theorems are proved by using only the basic properties of the irreducible modules of the Terwilliger algebra. Corollaries 3.5 and 4.6 may improve these theorems assuming sufficient thinness and dual thinness, respectively. Section 5 deals with metric and cometric schemes. The main theorem in this section is Theorem 5.2, and we apply recent results of Terwilliger on the displacement and split decompositions [28]. An interesting consequence is that Theorem 1.1 still holds for nonlinear codes as well (with an appropriate interpretation of the "weights of the dual code"; see Example 2.3). This is explained in Example 5.5.

The approach presented in this paper can also be used to give another proof of the minimum distance bound shown by W. J. Martin [16] as well as its dual. See [24].

2 Preliminaries

Throughout this paper, let $(X, \boldsymbol{R})$ denote a symmetric association scheme with D classes. Thus X is the vertex set and $\boldsymbol{R} = \{R_0, R_1, \ldots, R_D\}$ is the set of associate classes. We refer the reader to [3, 5, 25] for terminology and background materials on association schemes and the Terwilliger algebra.

Let V denote a vector space over $\mathbb{C}$ with a distinguished basis $\{\hat{x} : x \in X\}$ and a Hermitian inner product $\langle \hat{x}, \hat{y} \rangle = \delta_{xy}$ $(x, y \in X)$. For every $\chi \in V$ and a subspace $W \subseteq V$, $\chi|_W$ will denote the orthogonal projection of χ on W. Let $\mathrm{Mat}_X(\mathbb{C})$ denote the $\mathbb{C}$-algebra of all matrices over $\mathbb{C}$ with

rows and columns indexed by X. Then $\mathrm{Mat}_X(\mathbb{C})$ acts on V from the left in an obvious manner. Let $A_0 = I, A_1, \ldots, A_D \in \mathrm{Mat}_X(\mathbb{C})$ denote the associate matrices and let $E_0 = |X|^{-1}J, E_1, \ldots, E_D$ denote the primitive idempotents for the Bose-Mesner algebra $M = \langle A_0, A_1, \ldots, A_D \rangle$, where J denotes the all ones matrix.

Pick any $x \in X$. For each $0 \leqslant i \leqslant D$, $R_i(x) = \{y \in X : (x,y) \in R_i\}$ will denote the ith subconstituent of (X, R) with respect to x. Let $E_i^*(x), A_i^*(x) \in \mathrm{Mat}_X(\mathbb{C})$ denote the ith *dual idempotent* and the ith *dual associate matrix with respect to* x, respectively $(0 \leqslant i \leqslant D)$. They span the *dual Bose-Mesner algebra* $M^*(x)$ *with respect to* x. We recall $E_i^*(x)$, $A_i^*(x)$ are the diagonal matrices with (y,y)-entries $(E_i^*(x))_{yy} = (A_i)_{xy}$, $(A_i^*(x))_{yy} = |X|(E_i)_{xy}$. The *Terwilliger algebra* $T(x)$ *of* (X, R) *with respect to* x is the subalgebra of $\mathrm{Mat}_X(\mathbb{C})$ generated by M and $M^*(x)$. We remark $T(x)$ is semisimple and any two nonisomorphic irreducible $T(x)$-modules in V are orthogonal.

For the remainder of this section, fix $x \in X$ and write $E_i^* = E_i^*(x)$ $(0 \leqslant i \leqslant D)$, $T = T(x)$. Let $W \subseteq V$ denote an irreducible T-module. Set

$$W_s = \{0 \leqslant i \leqslant D : E_i^* W \neq 0\}, \quad W_s^* = \{0 \leqslant j \leqslant D : E_j W \neq 0\}.$$

We call W_s, W_s^* the *support* and the *dual support* of W, respectively. The *diameter* (resp. the *dual diameter*) of W is defined by $d(W) = |W_s| - 1$ (resp. $d^*(W) = |W_s^*| - 1$). We say W is *thin* whenever $\dim E_i^* W \leqslant 1$ for all i, and we say W is *dual thin* whenever $\dim E_j W \leqslant 1$ for all j.

Suppose for the moment that (X, R) is metric with respect to the ordering $A_0, A_1, \ldots, A_D$. The *endpoint* of an irreducible T-module $W \subseteq V$ is $r(W) = \min\{0 \leqslant i \leqslant D : E_i^* W \neq 0\}$. We remark that the primary module $M\hat{x}$ is a unique irreducible T-module with endpoint zero. We shall freely use the following basic fact:

Lemma 2.1 ([25, Lemma 3.9]). *Suppose (X, R) is metric with respect to the ordering $A_0, A_1, \ldots, A_D$ and write $A = A_1$. Let $W \subseteq V$ denote an irreducible T-module and set $r = r(W)$, $d = d(W)$. Then the following hold:*

(i) $AE_i^* W \subseteq E_{i-1}^* W + E_i^* W + E_{i+1}^* W$ $(0 \leqslant i \leqslant D)$, *where* $E_{-1}^* = E_{D+1}^* = 0$.

(ii) $W_s = \{r, r+1, \ldots, r+d\}$.

(iii) $E_i^* A E_k^* W \neq 0$ *if* $|i-k| = 1$ $(r \leqslant i, k \leqslant r+d)$.

(iv) If W is thin, then W is dual thin.

Next suppose (X, R) is cometric with respect to the ordering $E_0, E_1, \ldots, E_D$. The *dual endpoint* of an irreducible T-module $W \subseteq V$ is $r^*(W) = \min\{0 \leqslant j \leqslant D : E_j W \neq 0\}$. We remark that $M\hat{x}$ is a unique irreducible T-module with dual endpoint zero.

Lemma 2.2 ([25, Lemma 3.12]). *Suppose (X, R) is cometric with respect to the ordering $E_0, E_1, \ldots, E_D$ and write $A^* = A_1^*(x)$. Let $W \subseteq V$ denote an irreducible T-module and set $r^* = r^*(W)$, $d^* = d^*(W)$. Then the following hold:*

(i) $A^* E_j W \subseteq E_{j-1} W + E_j W + E_{j+1} W$ $(0 \leqslant j \leqslant D)$, *where* $E_{-1} = E_{D+1} = 0$.

(ii) $W_s^* = \{r^*, r^*+1, \ldots, r^*+d^*\}$.

(iii) $E_j A^* E_\ell W \neq 0$ *if* $|j-\ell| = 1$ $(r^* \leqslant j, \ell \leqslant r^*+d^*)$.

(iv) If W is dual thin, then W is thin.

To avoid triviality, we say a vector $\chi \in V$ is a *code* whenever $\chi \notin E_0 V$ and $\chi \notin E_0^*(z)V$ for every $z \in X$. We also say a subset $Y \subseteq X$ is a *code* provided its *characteristic vector* $\chi_Y = \sum_{y \in Y} \hat{y}$ is a code; in other words, Y is a code whenever $1 < |Y| < |X|$. To each code χ in V we associate four fundamental parameters (with respect to the base vertex $x \in X$ and given orderings of the associate matrices and the primitive idempotents):

$$\delta_x(\chi) = \min\{i \neq 0 : E_i^* \chi \neq 0\}, \quad s_x(\chi) = |\{i \neq 0 : E_i^* \chi \neq 0\}|,$$
$$\delta^*(\chi) = \min\{j \neq 0 : E_j \chi \neq 0\}, \quad s^*(\chi) = |\{j \neq 0 : E_j \chi \neq 0\}|.$$

When $\chi = \chi_Y$ for a code $Y \subseteq X$, we write $\delta_x(Y)$, $s_x(Y)$, and so on. In this case, we also set

$$\delta(Y) = \min\{i \neq 0 : \langle \chi, A_i \chi \rangle \neq 0\}, \quad s(Y) = |\{i \neq 0 : \langle \chi, A_i \chi \rangle \neq 0\}|.$$

We call $\delta(Y)$, $\delta^*(Y)$, $s(Y)$, $s^*(Y)$ the *minimum distance*, *dual distance*, *degree* and *dual degree* of Y, respectively.

Some of the most important families of association schemes are associated with *regular semilattices* (see [10] for the definition). Below we give two examples:

Example 2.3. Let $Q = \{0, 1, \ldots, q-1\}$ $(q \geqslant 2)$. Introduce a new symbol "$\cdot$", and let $\mathscr{L}$ denote the set of words of length D over $Q \cup \{\cdot\}$. For $u = (u_1, \ldots, u_D), v = (v_1, \ldots, v_D) \in \mathscr{L}$, we set $u \preccurlyeq v$ if and only if $u_i = \cdot$ or $u_i = v_i$, for all i. Then $(\mathscr{L}, \preccurlyeq)$ defines a regular semilattice (*Hamming lattice*) with rank function $\mathrm{rank}(u) = |\{i : u_i \neq \cdot\}|$, and the top fiber induces the Hamming scheme $\mathrm{H}(D, q)$. It is both metric and cometric. Every irreducible T-module $W \subseteq V$ is thin (thus dual thin) and satisfies $r(W) = r^*(W)$. Moreover, if $q = 2$ then $d(W)(= d^*(W)) = D - 2r(W)$. More detailed information on the irreducible T-modules of the Hamming scheme can be found in [27, Section 6], [13]. See also [20, 12]. We remark that if Y denotes a code in $\mathrm{H}(D, q)$ then $\delta^*(Y) - 1$ coincides with the (maximum) strength of Y as an orthogonal array [9, Theorem 4.4]. If moreover Q is the finite field $\mathbb{F}_q$, Y is linear with dual code $Y^\perp$ and the base vertex x is the zero vector $(0, 0, \ldots, 0)$, then $E_j \chi_Y \neq 0$ if and only if $E_j^* \chi_{Y^\perp} \neq 0$ $(0 \leqslant j \leqslant D)$ [9, Chapter 6]. See also [5, Section 2.10].

Example 2.4. Let $\Omega = \{1, 2, \ldots, N\}$ and set $\mathscr{L} = \{u \subseteq \Omega : |u| \leqslant D\}$, where $D \leqslant \lfloor N/2 \rfloor$. Then $(\mathscr{L}, \preccurlyeq)$, where the partial order $\preccurlyeq$ is given by inclusion, forms a regular semilattice (*truncated Boolean lattice*) with rank function $\mathrm{rank}(u) = |u|$. The top fiber induces the Johnson scheme $\mathrm{J}(N, D)$. It is both metric and cometric. Every irreducible T-module $W \subseteq V$ is thin (thus dual thin) and satisfies $r(W) \leqslant r^*(W)$. Information on the irreducible T-modules of the Johnson scheme can be found in [27, Section 6]. See also [20, Section III]. We remark that if Y denotes a code in $\mathrm{J}(N, D)$ then $\delta^*(Y) - 1$ coincides with the (maximum) strength of Y as a t-(N, D, λ) design [9, Theorem 4.7].

3 Assmus-Mattson theorem for metric schemes

In this section, we assume that (X, R) is metric with respect to the ordering $A_0, A_1, \ldots, A_D$. Thus $\Gamma = (X, R_1)$ is a distance-regular graph and $\partial(\cdot, \cdot)$ will denote the graph distance in Γ. We fix $x \in X$ and write $E_i^* = E_i^*(x)$ $(0 \leqslant i \leqslant D)$, $T = T(x)$.

Definition 3.1. For convenience, we say a vector $\chi \in V$ is a *relative t-codesign with respect to x* if $E_i^* \chi$ and $A_i \hat{x}$ are linearly dependent for all $1 \leqslant i \leqslant t$.

The first version of our Assmus-Mattson theorems is a variant of Delsarte's result (see the remark below):

Theorem 3.2 (Assmus-Mattson, Version 1). *Let χ denote a code in V. Set $\delta_x = \delta_x(\chi)$, $s^* = s^*(\chi)$. Then $A_\ell \chi$ is a relative $(\delta_x - s^*)$-codesign with respect to x for $0 \leqslant \ell \leqslant D$.*

Proof. Set $A = A_1$ and $U = (M\hat{x})^\perp$ (the orthogonal complement in V). We observe U is the linear span of all irreducible T-modules $W \subseteq V$ with $r(W) > 0$. Set $S = \{j \neq 0 : E_j \chi \neq 0\}$. Then

$$\chi|_U \in \left(\sum_{i=\delta_x}^{D} E_i^* U \right) \cap \left(\sum_{j \in S} E_j U \right).$$

Since A generates M and takes $s^* (= |S|)$ distinct eigenvalues on $\sum_{j \in S} E_j U$, we find $M\chi|_U$ is spanned by $\chi|_U, A\chi|_U, \ldots, A^{s^*-1}\chi|_U$ and thus (cf. Lemma 2.1 (i))

$$M\chi|_U \subseteq \sum_{i=\delta_x - s^* + 1}^{D} E_i^* U.$$

This proves $E_i^* M\chi \subseteq \mathbb{C} A_i \hat{x}$ for all $1 \leqslant i \leqslant \delta_x - s^*$. In particular, $E_i^* A_\ell \chi \in \mathbb{C} A_i \hat{x}$ for $0 \leqslant \ell \leqslant D$. □

Remark 3.3. Let Y denote a code in X. Set $\delta = \delta(Y)$, $s^* = s^*(Y)$. Delsarte [9, Theorem 5.11] showed that Y is $(\delta - s^*)$-regular (i.e., $|Y \cap R_\ell(z)|$ depends only on ℓ and $\partial(z, Y) = \min\{\partial(z, y) : y \in Y\}$ whenever $0 \leqslant \partial(z, Y) \leqslant \delta - s^*$). See also [5, Theorem 11.1.1].

The following lemma shows that the code χ in Theorem 3.2 exhibits far stronger regularity if irreducible T-modules with small endpoints are thin, and validates the term "Assmus-Mattson" above:

Lemma 3.4. *Let χ denote a vector in V. Then the following are equivalent:*

(i) χ is orthogonal to every irreducible T-module $W \subseteq V$ with $1 \leqslant r(W) \leqslant t$.

(ii) $F\chi$ is a relative t-codesign with respect to x for any $F \in T$. In particular, $A_\ell \chi$ is a relative t-codesign with respect to x for $0 \leqslant \ell \leqslant D$.

Suppose every irreducible T-module with endpoint at most t is thin. Then the second part of (ii) implies (i) (and thus (ii)).

Proof. With the same notation as in the proof of Theorem 3.2, (ii) is equivalent to $T\chi|_U \subseteq \sum_{i=\ell+1}^{D} E_i^* U$; in other words,

$$T\chi|_W \subseteq \sum_{i=\ell+1}^{r(W)+d(W)} E_i^* W$$

for every irreducible T-module $W \subseteq V$ with $r(W) > 0$. Since $T\chi|_W$ equals 0 or W according to whether $\chi|_W$ is zero or not, the equivalence of (i) and (ii) follows immediately from this comment.

Let $W \subseteq V$ denote an irreducible T-module with $1 \leqslant r(W) \leqslant t$ and suppose W is thin. Then $M\chi|_W$ cannot be a subspace of $\sum_{i=t+1}^{r(W)+d(W)} E_i^* W$ unless $\chi|_W = 0$ (cf. Lemma 2.1 (iii)). This completes the proof. □

As an application of the technique discussed above, we may improve Theorem 3.2 assuming sufficient thinness:

Corollary 3.5. *Let χ denote a code in V. Set $\delta_x = \delta_x(\chi)$. Suppose $t \in \{1, 2, \ldots, D\}$ is such that*

$$|\{j \in W_x^* : E_j \chi \neq 0\}| \leqslant \delta_x - r(W)$$

for each irreducible T-module $W \subseteq V$ with $1 \leqslant r(W) \leqslant t$. If every irreducible T-module with endpoint at most t is thin, then $F\chi$ is a relative t-codesign with respect to x for any $F \in T$.

Proof. Let $W \subseteq V$ denote an irreducible T-module with $1 \leqslant r(W) \leqslant t$ and set $S = \{j \in W_x^* : E_j \chi \neq 0\}$. Then as in the proof of Theorem 3.2 we find

$$M\chi|_W \subseteq \sum_{i=\delta_x - |S|+1}^{r(W)+d(W)} E_i^* W.$$

However since W is thin and $r(W) \leqslant \delta_x - |S|$, this forces $\chi|_W = 0$ (cf. Lemma 2.1 (iii)). Now the result follows from Lemma 3.4. □

Example 3.6. Suppose (X, R) is the Hamming scheme $\mathrm{H}(D, q)$. Let Y denote a code in X and assume χ_Y satisfies the equivalent conditions (i), (ii) in Lemma 3.4. Then setting $F = A_\ell E_k^*$ $(0 \leqslant k, \ell \leqslant D)$ we find $|Y \cap R_k(x) \cap R_\ell(z)|$ is independent of $z \in R_\ell(x)$. In particular, when $x = (0, 0, \ldots, 0)$ the supports of the codewords of fixed weight k form a t-design (in $\mathrm{J}(D, k)$). We remark that for $q = 2$, (half of) Theorem 1.1 follows from Corollary 3.5.

Example 3.7. Again suppose (X, R) is the Hamming scheme $\mathrm{H}(D, q)$. When q is a prime power, there are many nonlinear single-error-correcting perfect codes (containing $(0, 0, \ldots, 0)$; see e.g., [19]). They have minimum distance three and dual degree one. Thus Theorem 3.2, together with Lemma 3.4, shows that these codes support 2-designs.

Example 3.8. The $[24, 12, 8]$ extended binary Golay code has covering radius four and is self-dual with weight enumerator $x^{24} + 759x^{16}y^8 + 2576x^{12}y^{12} + 759x^8y^{16} + y^{24}$ (where x, y are indeterminates). Thus Corollary 3.5 shows that a coset of weight four supports 1-designs. On the other hand, it is well-known that the codewords of a fixed weight form a 5-design.

Example 3.9. Suppose (X, R) is the Johnson scheme $\mathrm{J}(N, D)$. Let Y denote a code in X and assume χ_Y satisfies the equivalent conditions (i), (ii) in Lemma 3.4. Then for every $0 \leqslant k \leqslant D$, $\{(x - y, y - x) : y \in Y \cap R_k(x)\}$ (which is a subset of $\mathrm{J}(D, k) \otimes \mathrm{J}(N - D, k)$) has the following property: there exists a constant λ such that for any t-subsets $\xi \subseteq x$ and $\eta \subseteq \Omega - x$, the number of elements $y \in Y \cap R_k(x)$ satisfying $\xi \subseteq x - y$ and $\eta \subseteq y - x$ is exactly λ. Such combinatorial objects are (among other things) studied in detail in [16].

Example 3.10. The 5-$(24, 8, 1)$ large Witt design has block intersection numbers 4, 2 and 0 so that the minimum distance is four, and it can be checked that this design has dual degree two (more precisely, it is a $\{1, 2, 3, 4, 5, 7\}$-design; see [7]). Thus if the base vertex x is chosen from the design, then by Theorem 3.2 we can take $t = 2$ in the previous example.

4 Assmus-Mattson theorem for cometric schemes

In this section, we assume that $(X, \boldsymbol{R})$ is cometric with respect to the ordering $E_0, E_1, \ldots, E_D$. We fix $x \in X$ and write $E_i^* = E_i^*(x)$ $(0 \leqslant i \leqslant D)$, $M^* = M^*(x)$, $T = T(x)$.

Definition 4.1 ([11]). A vector $\chi \in V$ is said to be a *relative t-design with respect to x* if $E_j\chi$ and $E_j\hat{x}$ are linearly dependent for all $1 \leqslant j \leqslant t$.

The notion of relative t-designs has a geometric interpretation when the scheme is associated with a regular semilattice:

Example 4.2. Suppose $(X, \boldsymbol{R})$ is induced on the top fiber X of a short regular semilattice $(\mathscr{L}, \preccurlyeq)$. (A semilattice $(\mathscr{L}, \preccurlyeq)$ is *short* if $X \wedge X = \mathscr{L}$.) In this case, Delsarte [11, Theorem 9.8] showed that $\chi \in V$ is a relative t-design with respect to x if and only if for each object $u \in \mathscr{L}$ such that $\mathrm{rank}(u) = t$, $\sum_{y \in X, u \preccurlyeq y} \langle \chi, \hat{y} \rangle$ depends only on $\mathrm{rank}(x \wedge u)$.

We may also use the Terwilliger algebra to give a new proof of Delsarte's algebraic version of the Assmus-Mattson theorem (cf. [5, Theorem 2.8.1]):

Theorem 4.3 (Assmus-Mattson, Version 2 [11, Theorem 8.4]). *Let χ denote a code in V. Set $\delta^* = \delta^*(\chi)$, $s_x = s_x(\chi)$. Then $E_k^*\chi$ is a relative $(\delta^* - s_x)$-design with respect to x for $0 \leqslant k \leqslant D$.*

Proof. By an argument similar to the proof of Theorem 3.2, we find $E_jM^*\chi \subseteq \mathbb{C}E_j\hat{x}$ for all $1 \leqslant j \leqslant \delta^* - s_x$. In particular, $E_jE_k^*\chi \in \mathbb{C}E_j\hat{x}$ for $0 \leqslant k \leqslant D$. □

Remark 4.4. Let Y denote a code in X. Set $\delta^* = \delta^*(Y)$, $s = s(Y)$. Delsarte [9, Theorem 5.24] also showed that if $\delta^* \geqslant s$ then Y is regular (i.e., 0-regular; for each k, $|Y \cap R_k(y)|$ does not depend on the choice of $y \in Y$).

The following lemma is the counterpart to Lemma 3.4:

Lemma 4.5. *Let χ denote a vector in V. Then the following are equivalent:*

(i) χ is orthogonal to every irreducible T-module $W \subseteq V$ with $1 \leqslant r^*(W) \leqslant t$.

(ii) $F\chi$ is a relative t-design with respect to x for any $F \in T$. In particular, $E_k^*\chi$ is a relative t-design with respect to x for $0 \leqslant k \leqslant D$.

Suppose every irreducible T-module with dual endpoint at most t is dual thin. Then the second part of (ii) implies (i) (and thus (ii)).

Proof. Similar to the proof of Lemma 3.4. □

Assuming sufficient dual-thinness, we may improve Theorem 4.3 as follows:

Corollary 4.6. *Let χ denote a code in V. Set $\delta^* = \delta^*(\chi)$. Suppose $t \in \{1, 2, \ldots, D\}$ is such that*

$$|\{i \in W_s : E_i^*\chi \neq 0\}| \leqslant \delta^* - r^*(W)$$

for each irreducible T-module $W \subseteq V$ with $1 \leqslant r^*(W) \leqslant t$. If every irreducible T-module with dual endpoint at most t is dual thin, then $F\chi$ is a relative t-design with respect to x for any $F \in T$.

Proof. Similar to the proof of Corollary 3.5. □

Example 4.7. Suppose $(X, \boldsymbol{R})$ is the Hamming scheme $\mathrm{H}(D, q)$. We remark that in this case the equivalent conditions (i), (ii) in Lemma 4.5 are also equivalent to the conditions (i), (ii) in Lemma 3.4. For $q = 2$, (half of) Theorem 1.1 follows from Corollary 4.6.

Example 4.8. Relative t-designs as well as the Assmus-Mattson theorem in the Johnson scheme $\mathrm{J}(N, D)$ are studied in detail in [15] in the context of *mixed block designs*. (Mixed 2-designs form a subclass of *balanced bipartite block designs*.)

Example 4.9. As observed in [11, Example 10.2] and [15, Example 9], the 5-$(24, 8, 1)$ large Witt design provides two relative 3-designs. See Example 3.10.

5 Assmus-Mattson theorem for metric and cometric schemes

In this section, we assume that $(X, \boldsymbol{R})$ is metric with respect to the ordering $A_0, A_1, \ldots, A_D$ and cometric with respect to the ordering $E_0, E_1, \ldots, E_D$. We fix $x \in X$ and write $E_i^* = E_i^*(x)$ $(0 \leqslant i \leqslant D)$, $T = T(x)$. The third version of our Assmus-Mattson theorems is related to the displacement and split decompositions for $(X, \boldsymbol{R})$ [28].

Let $W \subseteq V$ denote an irreducible T-module. Then $d(W) = d^*(W)$ by [18, Corollary 3.3] and moreover [8, Lemmas 5.1, 7.1]

$$2r(W) + d(W) \geqslant D, \quad 2r^*(W) + d(W) \geqslant D.$$

The *displacement* of W is

$$\eta(W) = r(W) + r^*(W) + d(W) - D.$$

Then $0 \leqslant \eta(W) \leqslant D$ [28, Lemma 4.2] and it follows from the above inequalities that $\eta(W) = 0$ if and only if $r(W) = r^*(W) = (D - d(W))/2$. Note that the primary module $M\hat{x}$ has displacement zero. For each $0 \leqslant \eta \leqslant D$, we let V_η denote the subspace of V spanned by the irreducible T-modules with displacement η. Then $V = \sum_{\eta=0}^{D} V_\eta$ (orthogonal direct sum) [28, Lemma 4.4]. This is the *displacement decomposition of V with respect to x.*

On the other hand, for $0 \leqslant i, j \leqslant D$ we define

$$V_{ij} = \left(\sum_{k=0}^{i} E_k^* V\right) \cap \left(\sum_{\ell=0}^{j} E_\ell V\right).$$

Obviously $V_{i-1,j}, V_{i,j-1} \subseteq V_{ij}$, and we let $\tilde{V}_{ij}$ denote the orthogonal complement of $V_{i,j-1} + V_{i-1,j}$ in V_{ij}. Then for $0 \leqslant k, \ell \leqslant D$, we have [28, Theorem 5.7]

$$V_{k\ell} = \sum_{i=0}^{k} \sum_{j=0}^{\ell} \tilde{V}_{ij} \quad \text{(direct sum)},$$

and in particular, $V = \sum_{i=0}^{D} \sum_{j=0}^{D} \tilde{V}_{ij}$ [28, Corollary 5.8]. We call the latter sum the *split decomposition of V with respect to x*. This decomposition is not orthogonal in general.

Moreover, Terwilliger [28, Theorem 6.2] showed that for each $0 \leqslant \eta \leqslant D$ we have $V_\eta = \sum_{i,j} \tilde{V}_{ij}$, where the sum is over $0 \leqslant i, j \leqslant D$ such that $i + j = D + \eta$, and thus comparing the displacement and split decompositions he found $\tilde{V}_{ij} = V_{ij} = 0$ if $i + j < D$.

Lemma 5.1. *We have $V_0 = \sum_{i=0}^{D} V_{i,D-i}$ (direct sum). Moreover the following hold.*

(i) $\sum_{k=0}^{i} V_{k,D-k} = \sum_{k=0}^{i} E_k^* V_0$ $(0 \leqslant i \leqslant D)$.

(ii) $\sum_{\ell=0}^{j} V_{D-\ell,\ell} = \sum_{\ell=0}^{j} E_\ell V_0$ $(0 \leqslant j \leqslant D)$.

Proof. As $V_{i-1,D-i} = V_{i,D-i-1} = 0$, we find $V_{i,D-i} = \tilde{V}_{i,D-i}$ and the first line follows.

(i) Clearly it suffices to show $\sum_{k=0}^{i} E_k^* V_0 \subseteq \sum_{k=0}^{i} V_{k,D-k}$. Set $A^* = A_1^*(x)$ and let θ_k^* denote the eigenvalue of A^* associated with $E_k^* V$ $(0 \leqslant k \leqslant D)$. Then it is easy to see that $(A^* - \theta_k^* I)V_{k,D-k} \subseteq V_{k-1,D-k+1}$ for $0 < k \leqslant D$ and $(A^* - \theta_0^* I)V_{0D} = 0$ (cf. [28, Theorem 7.1]). Thus setting $F = \prod_{k=i+1}^{D} (A^* - \theta_k^* I)$, we obtain

$$\sum_{k=0}^{i} E_k^* V_0 = F V_0 = \sum_{k=0}^{D} F V_{k,D-k} \subseteq \sum_{k=0}^{i} V_{k,D-k}.$$

See also [14, Theorem 4.6].

(ii) Similar to the proof of (i) above. □

Theorem 5.2 (Assmus-Mattson, Version 3). *Let χ denote a code in V. Set $\delta_x = \delta_x(\chi)$, $\delta^* = \delta^*(\chi)$. Suppose $t \in \{1, 2, \ldots, D\}$ is such that for every $1 \leqslant r \leqslant t$ at least one of the following holds:*

$$|\{r \leqslant j \leqslant D - r : E_j \chi \neq 0\}| \leqslant \delta_x - r,$$
$$|\{r \leqslant i \leqslant D - r : E_i^* \chi \neq 0\}| \leqslant \delta^* - r.$$

If every irreducible T-module with displacement zero and endpoint at most t is thin (thus dual thin), then the following hold.

(i) For any $F \in T$, $F\chi$ is orthogonal to $V_{i,D-i} \cap (M\hat{x})^{\perp}$ whenever $1 \leqslant i \leqslant t$.

(ii) For any $F \in T$, $F\chi$ is orthogonal to $V_{D-j,j} \cap (M\hat{x})^{\perp}$ whenever $1 \leqslant j \leqslant t$.

Proof. First, by the hypothesis we find $\chi|_W = 0$ for any irreducible T-module $W \subseteq V$ with $\eta(W) = 0$ and $1 \leqslant r(W)(= r^*(W)) \leqslant t$, as in the proofs of Corollaries 3.5, 4.6.

(i) Set $U_0 = V_0 \cap (M\hat{x})^{\perp}$. We observe U_0 is the linear span of all irreducible T-modules $W \subseteq V$ with $\eta(W) = 0$ and $r(W) > 0$. Then, in view of Lemma 5.1 it suffices to show $T\chi|_{U_0} \subseteq \sum_{i=t+1}^{D} E_i^* U_0$, or equivalently $T\chi|_W \subseteq \sum_{i=t+1}^{r(W)+d(W)} E_i^* W$ for every irreducible T-module $W \subseteq V$ with $\eta(W) = 0$ and $r(W) > 0$, but this follows immediately from the above comment.

(ii) Similar to the proof of (i) above. □

Remark 5.3. The assumption on thinness in Theorem 5.2 is redundant. In fact, P. Terwilliger (private communication) pointed out that the irreducible T-modules with displacement zero are always thin for any metric and cometric schemes. This (among other things) will be discussed in a future paper.

Example 5.4. With the same hypothesis as in Theorem 5.2, assume moreover (X, R) is induced on the top fiber X of a short regular semilattice $(\mathscr{L}, \preccurlyeq)$. For each object $u \in \mathscr{L}$, let $\chi_{\succcurlyeq u} = \sum_{y \in X, u \preccurlyeq y} \hat{y}$ denote the characteristic vector of $\{y \in X : u \preccurlyeq y\}$. It is a standard fact that $\chi_{\succcurlyeq u} \in V_{D-\mathrm{rank}(u),\mathrm{rank}(u)}$ whenever $u \preccurlyeq x$ [10]. We remark that each $A_k\hat{x}$ is obviously a relative D-design with respect to x and thus also a relative t-design with respect to x (cf. [11, Corollary 9.9] and the remark that follows it). Therefore, if $u, v \in \mathscr{L}$ are two objects of rank t such that $u, v \preccurlyeq x$, then in view of the geometric interpretation of relative t-designs given in Example 4.2, $\chi_{\succcurlyeq u} - \chi_{\succcurlyeq v}$ is orthogonal to $A_k\hat{x}$ for every $0 \leqslant k \leqslant D$; in other words, $\chi_{\succcurlyeq u} - \chi_{\succcurlyeq v} \in V_{D-t,t} \cap (M\hat{x})^{\perp}$. Now the second part of Theorem 5.2 implies that for each $F \in T$, $\langle F\chi, \chi_{\succcurlyeq u}\rangle$ is independent of $u \preccurlyeq x$ with rank t.

Example 5.5. Suppose (X, R) is the Hamming scheme $\mathrm{H}(D, q)$ and set $x = (0, 0, \ldots, 0)$. Let Y denote a code in X and set $\chi = \chi_Y$ in the previous example. Then we find that (the complements of) the supports of the words of fixed weight k in Y form a t-design (in $\mathrm{J}(D, k) \cong \mathrm{J}(D, D-k)$) for every k. In particular, the conclusion of the original Assmus-Mattson theorem (Theorem 1.1) is also true for nonlinear codes as well.

Example 5.6. The $[12, 6, 6]$ extended ternary Golay code has covering radius three and is self-dual with weight enumerator $x^{12}+264x^6y^6+440x^3y^9+24y^{12}$ (where x, y are indeterminates). Thus Theorem 5.2 shows that a coset of weight three supports 1-designs. On the other hand, it is well-known that the codewords of a fixed weight form a 5-design.

Example 5.7. Suppose (X, R) is the Johnson scheme $\mathrm{J}(N, D)$. Let Y denote a code in X and set $\chi = \chi_Y$ in Example 5.4. Then, in this case we find that the multiset $\{x \cap y : y \in Y \cap R_k(x)\}$ (counting repeats) forms a t-design (in $\mathrm{J}(D, D-k)$) for every k.

Example 5.8. The 2-$(56, 12, 3)$ design constructed in [4] has intersection numbers 3, 2 and 0, and thus Theorem 5.2 provides two 1-designs.

6 Remarks

Remark 6.1. We proved our Assmus-Mattson theorems (Theorems 3.2, 4.3, 5.2) and their corollaries (Corollaries 3.5, 4.6) by projecting the code χ to the orthogonal complement U of the primary module $M\hat{x}$. Thus everything still works, for instance, even if we replace $s_x(\chi)$ by $\hat{s}_x(\chi) = |\{i \neq 0 : E_i^*(x)\chi \notin \mathbb{C}A_i\hat{x}\}|$ and/or $s^*(\chi)$ by $\hat{s}^*(\chi) = |\{j \neq 0 : E_j\chi \notin \mathbb{C}E_j\hat{x}\}|$. This (slight) improvement seems particularly effective for codes in the binary Hamming scheme $\mathrm{H}(D, 2)$ (in which case $\dim E_D^*(x)V = \dim E_D V = 1$). See also [5, Section 2.8].

Remark 6.2. Recently, Schrijver [20] established the *semidefinite programming bound* on the sizes of codes in the binary Hamming schemes and Johnson schemes, which is shown to be at least as good as Delsarte's bound based on the linear programming method [9]. This provides a remarkable application of the Terwilliger algebra. See also [12].

Acknowledgements. The author would like to thank Jack Koolen, Bill Martin, Akihiro Munemasa and Paul Terwilliger for helpful discussions and comments. In particular, Paul Terwilliger drastically simplified the initial proof of Corollaries 3.5 and 4.6 presented at the conference, which ultimately led to the whole results in this paper.

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, J. Combin. Theory 6 (1969) 122-151.

[2] C. Bachoc, On harmonic weight enumerators of binary codes, Des. Codes Cryptogr. 18 (1999) 11-28.

[3] E. Bannai and T. Ito, Algebraic combinatorics I, Benjamin/Cummings, Menlo Park, 1984.

[4] H. Beker and W. Haemers, 2-designs having an intersection number $k - n$, J. Combin. Theory Ser. A 28 (1980) 64-81.

[5] A. E. Brouwer, A. M. Cohen and A. Neumaier, Distance-regular graphs, Springer-Verlag, Berlin, 1989.

[6] A. R. Calderbank and P. Delsarte, On error-correcting codes and invariant linear forms, SIAM J. Discrete Math. 6 (1993) 1-23.

[7] A. R. Calderbank, P. Delsarte and N. J. A. Sloane, A strengthening of the Assmus-Mattson theorem, IEEE Trans. Inform. Theory 37 (1991) 1261-1268.

[8] J. S. Caughman, IV, The Terwilliger algebras of bipartite P- and Q-polynomial schemes, Discrete Math. 196 (1999) 65-95.

[9] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. No. 10 (1973).

[10] P. Delsarte, Association schemes and t-designs in regular semilattices, J. Combinatorial Theory Ser. A 20 (1976) 230-243.

[11] P. Delsarte, Pairs of vectors in the space of an association scheme, Philips Res. Rep. 32 (1977) 373-411.

[12] D. Gijswijt, A. Schrijver and H. Tanaka, New upper bounds for nonbinary codes based on the Terwilliger algebra and semidefinite programming, J. Combin. Theory Ser. A 113 (2006) 1719-1731.

[13] J. T. Go, The Terwilliger algebra of the hypercube, European J. Combin. 23 (2002) 399-429.

[14] T. Ito, K. Tanabe and P. Terwilliger, Some algebra related to P- and Q-polynomial association schemes, Codes and association schemes (Piscataway, NJ, 1999), Amer. Math. Soc., Providence, RI (2001), pp. 167-192.

[15] W. J. Martin, Mixed block designs, J. Combin. Des. 6 (1998) 151-163.

[16] W. J. Martin, Designs in product association schemes, Des. Codes Cryptogr. 16 (1999) 271-289.

[17] W. J. Martin, Minimum distance bounds for s-regular codes, Des. Codes Cryptogr. 21 (2000) 181-187.

[18] A. A. Pascasio, On the multiplicities of the primitive idempotents of a Q-polynomial distance-regular graph, European J. Combin. 23 (2002) 1073-1078.

[19] K. T. Phelps, J. Rifà and M. Villanueva, Kernels and p-kernels of p^r-ary 1-perfect codes, Des. Codes Cryptogr. 37 (2005) 243-261.

[20] A. Schrijver, New code upper bounds from the Terwilliger algebra and semidefinite programming, IEEE Trans. Inform. Theory 51 (2005) 2859-2866.

[21] J. Simonis, MacWilliams identities and coordinate partitions, Linear Algebra Appl. 216 (1995) 81-91.

[22] K. Tanabe, A new proof of the Assmus-Mattson theorem for non-binary codes, Des. Codes Cryptogr. 22 (2001) 149-155.

[23] K. Tanabe, A criterion for designs in $\mathbb{Z}_4$-codes on the symmetrized weight enumerator, Des. Codes Cryptogr. 30 (2003) 169-185.

[24] H. Tanaka, New proofs of the Assmus-Mattson theorem based on the Terwilliger algebra, submitted.

[25] P. Terwilliger, The subconstituent algebra of an association scheme I, J. Algebraic Combin. 1 (1992) 363-388.

[26] P. Terwilliger, The subconstituent algebra of an association scheme II, J. Algebraic Combin. 2 (1993) 73-103.

[27] P. Terwilliger, The subconstituent algebra of an association scheme III, J. Algebraic Combin. 2 (1993) 177-210.

[28] P. Terwilliger, The displacement and split decompositions for a Q-polynomial distance-regular graph, Graphs Combin. 21 (2005) 263-276.

New Examples of Euclidean Tight 4-designs

— 還暦おめでとう —

Etsuko Bannai
Faculty of Mathematics, Graduate School,
Kyushu University

1 Introduction

The concept of Euclidean design was defined by Neumaier and Seidel in 1988 ([15]) as a generalization of spherical designs. Delsarte and Seidel ([10]) proved the Fisher type lower bounds for the cardinality of a Euclidean $2e$-design and that of an antipodal Euclidean $(2e+1)$-design, and they gave definitions of Euclidean tight designs. They conjectured that only Euclidean tight designs are trivial ones such as regular simplices. Recently, Eiichi Bannai-Etsuko Bannai, Etsuko Bannai and Bajnok constructed interesting Euclidean tight designs. In this talk we consider Euclidean tight 4-designs supported by 2 concentric spheres. In this case tight 4-designs must have 2 layers and each layer must be a strongly regular graph.

In this talk we give new examples of Euclidean tight 4-designs in $\mathbb{R}^n$ for $n = 4,\ 5,\ 6$ and 22. Some of the examples have the structures of tight 4-designs in Johnson schemes and Hamming schemes. The combinatorial tight 4-designs are equivalent to the tight 4-designs in Johnson schemes. In 1979, H.Enomoto, N. Ito and R. Noda ([11]) proved that there are only two nontrivial combinatorial tight 4-design, 4-$(23, 7, 1)$ design, and its complimentary design 4-$(23, 16, 52)$. The classification of tight 4-designs in the Hamming schemes is also known and it is proved that only $H(11, 3)$ and $H(5, 2)$ have tight 4-designs (see [13, 14]). We constructed 2 kinds of new examples of Euclidean tight 4-designs in $\mathbb{R}^{22}$. One of them corresponds to the classical tight 4-$(23, 7, 1)$ design and the other one corresponds to the tight 4-design in the Hamming scheme $H(11, 3)$. For more information about the designs in Q-polynomial association schemes please refer to [8].

Originally, the concept of spherical designs was defined as a generalization of the classical designs (see [9]). It is interesting to know that Euclidean tight 4-designs are related to classical tight 4-designs or tight 4-designs in certain association schemes. Also, as Prof. Klin mentioned at the conference, it is interesting to know whether the concept of coherent configurations can explain all these phenomena.

2 Definitions and basic facts

X is a finite set in $\mathbb{R}^n$. Let $\{\|\boldsymbol{x}\| \mid \boldsymbol{x} \in X\} = \{r_1, \ldots, r_p\}$ be the set of the lengths of the vectors in X. Let $S^{n-1} = \{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x}\| = 1\}$ be the unit sphere centered at the origin.

For $i = 1, \ldots, p$, let $S_i = \{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x}\| = r_i\}$ be the sphere of radius r_i centered at the origin. Let $X_i = S_i \cap X$ for $i = 1, \ldots, p$. Let σ, σ_i $(1 \leq i \leq p)$ be the Haar measure on S^{n-1} and S_i $(1 \leq i \leq p)$ respectively. We normalize the measures so that $|S^{n-1}| = \int_{S^{n-1}} d\sigma(\boldsymbol{x})$, $|S_i| = \int_{S_i} d\sigma_i(\boldsymbol{x}) = r_i^{n-1}|S^{n-1}|$ hold. If $r_i = 0$, then we define $\frac{1}{|S_i|}\int_{S_i} f(\boldsymbol{x})d\sigma_i(\boldsymbol{x}) = f(0)$. Let $w : X \longrightarrow \mathbb{R}_{>0}$ be a positive weight function defined on X. Let $S = \cup_{i=1}^{p} S_i$. Let $\mathcal{P}(\mathbb{R}^n) = \mathbb{R}[x_1, \ldots, x_n]$ be the vector space of polynomials of n variables over the field of real numbers. $\mathrm{Hom}_i(\mathbb{R}^n)$ be the subspace or $\mathcal{P}(\mathbb{R}^n)$ consists of homogeneous polynomials of degree i. Let $\mathcal{P}_l(\mathbb{R}^n) = \bigoplus_{i=0}^{l} \mathrm{Hom}_i(\mathbb{R}^n)$ and $\mathcal{P}_l^*(\mathbb{R}^n) = \bigoplus_{i \equiv l \pmod 2, \atop 0 \leq i \leq l} \mathrm{Hom}_i(\mathbb{R}^n)$. $\mathcal{P}_l(S)$, $\mathcal{P}_l^*(S)$, etc., mean the restriction of the polynomials to the union of concentric p concentric spheres S. If X is antipodal, then X^* is the antipodal half of X, i.e., $X = X^* \cup (-X^*)$, $X^* \cap (-X^*) = \emptyset$ or $\{0\}$.

Definition 2.1 (Neumaier-Seidel, 1988 [15]) *Let X be a finite subset in $\mathbb{R}^n$, w be a positive weight function on X and t be a natural number. If the following condition holds then X is a Euclidean t-design:*

$$\sum_{i=1}^{p} \frac{w(X_i)}{|S_i|} \int_{S_i} f(\boldsymbol{x}) d\sigma_i(\boldsymbol{x}) = \sum_{\boldsymbol{x} \in X} w(\boldsymbol{x}) f(\boldsymbol{x})$$

for any $f \in \mathcal{P}_t(\mathbb{R}^n)$.

The following lower bounds of the cardinalities of the t-designs are known.

Theorem 2.2 (Delsarte-Seidel, 1989 [10])
(i) *Let X be a Euclidean $2e$-design. Then*

$$|X| \geq \dim(\mathcal{P}_e(S))$$

holds.
(ii) *Let X be an antipodal Euclidean $(2e+1)$-design. Assume $w(-\boldsymbol{x}) = w(\boldsymbol{x})$ for $\boldsymbol{x} \in X$. Then*

$$|X^*| \geq \dim(\mathcal{P}_e^*(S))$$

holds.

Definition 2.3 ([5])
(i) *If equality holds in Theorem 2.2* (i), *then X is a tight $2e$-design on S. Moreover if* $\dim(\mathcal{P}_e(S)) = \dim(\mathcal{P}_e(\mathbb{R}^n))$ *holds, then X is a tight Euclidean $2e$-design.*
(ii) *If equality holds in Theorem 2.2* (ii), *then X is an antipodap tight $(2e+1)$-design on S. Moreover if* $\dim(\mathcal{P}_e^*(S)) = \dim(\mathcal{P}_e^*(\mathbb{R}^n))$ *holds, then X is an antipodal tight Euclidean $(2e+1)$-design.*

For the tight $2e$-designs on S and antipodal tight $(2e+1)$-designs on S we have the following lemma ([5, 2]).

Lemma 2.4 (Ei. Bannai, Et. Bannai)
(1) *Let X be a tight $2e$-design on S. Then the following hold:*
  (i) *w is constant on each X_i $(1 \leq i \leq p)$.*
  (ii) *Each X_i $(1 \leq i \leq p)$ is an at most e-distance set.*
(2) *Let X be an antipodal $(2e+1)$-design on S. Then the following hold:*
  (i) *w is constant on each X_i $(1 \leq i \leq p)$.*
  (ii) *Each X_i^* $(1 \leq i \leq p)$ is an at most e-distance set.*
  (iii) *Each X_i $(1 \leq i \leq p)$ is an at most $(e+1)$-distance set.*

The following examples are known:
• A Euclidean tight 4-design in $\mathbb{R}^2$ with $p = 2$ was constructed in [5].
• An antipodal Euclidean tight 5-design in $\mathbb{R}^3$ with $p = 2$ and an antipodal Euclidean tight 7-design in $\mathbb{R}^3$ with $p = 3$ were constructed by Bajnok [1].
• The Euclidean tight 2-designs in $\mathbb{R}^n$ were classified in [6].
• The antipodal Euclidean tight 3-designs in $\mathbb{R}^n$ were classified in [2].
• Existence of a Euclidean tight 4-design in $\mathbb{R}^n$ with constant weight is equivalent to the existence of a spherical tight 4-design on S^{n-1} [5].
• The antipodal Euclidean tight 5-designs in $\mathbb{R}^n$ with $p = 2$ were classified in [2]. It is proved that if $0 \notin X$ and $p = 2$, then we must have $n = 2, 3, 5, 6$ and all the antipodal Euclidean tight 5-designs are given in [2]. If $0 \in X$ and $p = 2$, then the classification is equivalent to that of spherical tight 5-designs.

In the following we consider Euclidean tight 4-designs with $p = 2$ and $r_1, r_2 > 0$. For a Euclidean t-design X with a weight function w, it is known that $X' = \{\lambda \boldsymbol{x} \mid \boldsymbol{x} \in X\}$ with $w'(\lambda \boldsymbol{x}) = w(\boldsymbol{x})$, $\boldsymbol{x} \in X$ and X with $w'(\boldsymbol{x}) = \lambda w(\boldsymbol{x})$ are Euclidean t-designs. With this fact and Lemma 2.4 we may assume $|X_1| \leq |X_2|$, $r_1 = 1$, $r_2 = r$ (a positive constant), $w(\boldsymbol{x}) = 1$ for $\boldsymbol{x} \in X_1$, and $w(\boldsymbol{x}) = w$ (a positive constant) for $\boldsymbol{x} \in X_2$. We note that $|X| = \binom{n+2}{2}$ holds. Since $p = 2$, each X_i $(1 \leq i \leq 2)$ is a spherical 2-design (see [2]). Hence we have $n + 1 \leq |X_1| \leq |X_2|$. If $n = 2$, then $|X| = 6$, $|X_1| = |X_2| = 3$ hold. Hence $X = X_1 \cup X_2$ is similar to the following:

$$X_1 = \left\{ (1,0),\ (-\frac{1}{2}, \frac{\sqrt{3}}{2}),\ (-\frac{1}{2}, -\frac{\sqrt{3}}{2}) \right\},\ X_2 = \left\{ (-r,\ 0),\ (\frac{r}{2}, \frac{\sqrt{3}\,r}{2}),\ (\frac{r}{2}, -\frac{\sqrt{3}\,r}{2}) \right\}$$

with $w(\boldsymbol{x})$ defined by $w(\boldsymbol{x}) = \begin{cases} 1 & \text{for } \boldsymbol{x} \in X_1 \\ \frac{1}{r^3} & \text{for } \boldsymbol{x} \in X_2. \end{cases}$

In the following we assume $n \geq 3$. If $|X_1| = n + 1$, then X_1 is a regular simplex. If $|X_i| \geq n + 2$, then Lemma 2.2 implies that X_i is a 2-distance set. Since X_i is a spherical 2-design, X_i must be a strongly regular graph (see [9]). Assume that X_i is not a conference graph. Let a_1 and a_2 be the 2 distances between the distinct two points in X_i. Assume $a_1 < a_2$. Then there exists a natural number $k \geq 2$ satisfying $\left(\frac{a_1}{a_2}\right)^2 = \frac{k-1}{k}$ (see [4, 12]).

For $n \geq 3$, if $|X_1| = n + 1$, then X_1 is a regular simplex and X_2 is a strongly regular graph. If $|X_1| \geq n + 2$, then both X_1 and X_2 are strongly regular graphs. Hence X_1 and X_2 have the structure of association schemes, that is, X_1 and X_2 are images of spherical

embeddings of association schemes. Let $E^{(1)}$ and $E^{(2)}$ be the idempotents which give the spherical embeddings of X_1 and X_2 respectively. Let $J^{(i)}$ $(1 \leq i \leq 2)$ be the matrix of the same size with $E^{(i)}$ whose entries are all 1. Then we have $E^{(i)}J^{(i)} = 0$ for $i = 1, 2$ (see [7, 3]). This implies the following:

$$\sum_{\boldsymbol{u} \in X_1} \boldsymbol{u} = 0, \quad \sum_{\boldsymbol{x} \in X_2} \boldsymbol{x} = 0.$$

We can also prove

$$\langle \boldsymbol{u}_i, \boldsymbol{x}_j \rangle = \gamma_1 + \varepsilon_{i,j}\gamma_2$$

holds for any $\boldsymbol{u}_i \in X_1, \boldsymbol{x}_j \in X_2$ with $\varepsilon_{i,j} \in \{1, -1\}$ and constant real numbers $\gamma_1 < 0$ and $\gamma_2 > 0$. Let $N_i = |X_i|$, for $i = 1, 2$. Then we have

$$0 = \sum_{i=1}^{N_1} \langle \boldsymbol{u}_i, \boldsymbol{x}_j \rangle = N_1\gamma_1 + \gamma_2 \sum_{i=1}^{N_1} \varepsilon_{i,j}.$$

Since $\gamma_1 < 0$ and $\gamma_2 > 0$, we have $m_1 = \sum_{i=1}^{N_1} \varepsilon_{i,j} > 0$. Thus we have

$$\frac{\gamma_1}{\gamma_2} = -\frac{m_1}{N_1}.$$

Similarly we have

$$\frac{\gamma_1}{\gamma_2} = -\frac{m_2}{N_2},$$

where $m_2 = \sum_{j=1}^{N_2} \varepsilon_{i,j} > 0$. Summarize the above arguments we obtain the following proposition:

Proposition 2.5
(i) *There exist positive integers m_1 and m_2 satisfying*

$$\frac{m_1}{N_1} = \frac{m_2}{N_2} = -\frac{\gamma_1}{\gamma_2}.$$

(ii) *For any fixed $\boldsymbol{x} \in X_2$*

$$|\{\boldsymbol{u} \in X_1 \mid \langle \boldsymbol{u}, \boldsymbol{x} \rangle = \gamma_1 + \gamma_2\}| = \frac{N_1 + m_1}{2}$$

and

$$|\{\boldsymbol{u} \in X_1 \mid \langle \boldsymbol{u}, \boldsymbol{x} \rangle = \gamma_1 - \gamma_2\}| = \frac{N_1 - m_1}{2}$$

(iii) *For any fixed $\boldsymbol{u} \in X_1$*

$$|\{\boldsymbol{x} \in X_2 \mid \langle \boldsymbol{u}, \boldsymbol{x} \rangle = \gamma_1 + \gamma_2\}| = \frac{N_2 + m_2}{2}$$

and

$$|\{\boldsymbol{x} \in X_2 \mid \langle \boldsymbol{u}, \boldsymbol{x} \rangle = \gamma_1 - \gamma_2\}| = \frac{N_2 - m_2}{2}.$$

Since X_1 and X_2 have the structure of association schemes, Proposition 2.5 implies that the Euclidean tight 4-design X with $p = 2$ is a distance invariant set.

As for the basic fact about the association schemes, spherical embedding of association schemes please refer to [7, 3].

Using these integral conditions we have the classification for the case $|X_1| = n+1$ and $n+2$.

3 Classification for the case $|X_1| = n+1$ and $n+2$.

Case $|X_1| = n+1$

Since $|X_1| = n+1$, X_1 must be a regular simplex. We may assume $X_1 = \{u_1, \ldots, u_{n+1}\}$ where for $1 \leq i \leq n$, the j-th coordinate of u_i equals $\frac{-1+\sqrt{n+1}}{n\sqrt{n}}$ for $j \neq i$, the i-th coordinate of u_i equals $-\frac{1+(n-1)\sqrt{n+1}}{n\sqrt{n}}$ and $u_{n+1} = \frac{1}{\sqrt{n}}(1, 1, \ldots, 1)$. In this case we must have $n = 4$, 5, 6, and 22. and X is similar to the one of the followings:

$n = 4$
$|X_1| = 5$, $|X_2| = 10$, $r_1 = 1$, $r_2 = \frac{1}{\sqrt{6}}$. X_2 consists of 10 points determined uniquely by the following way:

$$X_2 = \left\{ x \mid \langle x, u_i \rangle = -\frac{1}{24} + \frac{5}{24}\varepsilon_i,\ \varepsilon_i \in \{1, -1\},\ 1 \leq i \leq 5,\ \text{and } |\{i \mid \varepsilon_i = -1\}| = 2 \right\}.$$

$w(x) = 27$ for $x \in X_2$. Thus X_2 has the structure of Johnson scjeme $J(5,2)$ or $J(5,3)$. Let $\varepsilon_i, 1 \leq i \leq 5$ and $\varepsilon'_i, 1 \leq i \leq 5$ coresspond to the points x, $x' \in X_2$ respectively. Then $\sum_{i=1}^{5} \varepsilon_i \varepsilon'_i = 1$ or -3.

$n = 5$
$|X_1| = 6$, $|X_2| = 15$, $r_1 = 1$, $r_2 = \sqrt{\frac{8}{5}}$. X_2 consists of 15 points determined uniquely by the following way:

$$X_2 = \left\{ x \mid \langle x, u_i \rangle = -\frac{1}{5} + \frac{3}{5}\varepsilon_i,\ \varepsilon_i \in \{1, -1\},,\ 1 \leq i \leq 6,\ \text{and } |\{i \mid \varepsilon_i = -1\}| = 2 \right\}.$$

$w(x) = \frac{1}{2}$ for $x \in X_2$. Thus X_2 has the structure of $J(6,2)$ or $J(6,4)$.

Let $\varepsilon_i, 1 \leq i \leq 6$ and $\varepsilon'_i, 1 \leq i \leq 6$ coresspond to the points x, $x' \in X_2$ respectively. Then $\sum_{i=1}^{6} \varepsilon_i \varepsilon'_i = -2$ or -2.

$n = 6$
$|X_1| = 7$, $|X_2| = 21$, $r_1 = 1$, $r_2 = \sqrt{15}$. X_2 consists of 21 points determined uniquely by the following way:

$$X_2 = \left\{ x \mid \langle x, u_i \rangle = -\frac{3}{4} + \frac{7}{4}\varepsilon_i,\ \varepsilon_i \in \{1, -1\},,\ 1 \leq i \leq 7,\ \text{and } |\{i \mid \varepsilon_i = -1\}| = 2 \right\}.$$

$w(\boldsymbol{x}) = \frac{1}{81}$ for $\boldsymbol{x} \in X_2$. Thus X_2 has the structure of $J(7,2)$ or $J(7,5)$.

Let $\varepsilon_i, 1 \leq i \leq 7$ and $\varepsilon'_i, 1 \leq i \leq 7$ coresspond to the points $\boldsymbol{x}$, $\boldsymbol{x}' \in X_2$ respectively. Then $\sum_{i=1}^{7} \varepsilon_i \varepsilon'_i = 3$ or -1.

$n = 22$

$|X_1| = 23$, $|X_2| = 253$, $r_1 = 1$, $r_2 = \sqrt{\frac{126}{11}}$. X_2 consists of 253 points determined uniquely, up to orthogonal transformation, by the following way:

$$X_2 \subset \left\{ \boldsymbol{x} \mid \langle \boldsymbol{x}, \boldsymbol{u}_i \rangle = -\frac{27}{88} + \frac{69}{88}\varepsilon_i,\ \varepsilon_i \in \{1,-1\},\ 1 \leq i \leq 23, \text{ and } |\{i \mid \varepsilon_i = -1\}| = 7 \right\}.$$

Let $\varepsilon_i, 1 \leq i \leq 23$ and $\varepsilon'_i, 1 \leq i \leq 23$ coresspond to the points $\boldsymbol{x}$, $\boldsymbol{x}' \in X_2$ respectively. Then $\sum_{i=1}^{23} \varepsilon_i \varepsilon'_i = 7$ or -1. Hence X_2 must be a 2-distance set in $J(23,7)$ with maximum cardinality $\binom{23}{2} = 253$. The weight function is given by $w(\boldsymbol{x}) = \frac{1}{81}$ for $\boldsymbol{x} \in X_2$.

In above examples, we can define conbinatorial designs in the following manner. Let X_1 be the point set and let X_2 be the block set and define the incidence relation $\boldsymbol{x}\mathcal{I}\boldsymbol{u}_i$ by $\varepsilon_i = 1$ for $\boldsymbol{x} \in X_2$ and $\boldsymbol{u}_i \in X_1$ for $n = 4,\ 5,\ 6$. Then, we can regards X_2 as a 2-distance set with respect to the distance in the Johnson scheme $J(n+1, n-1)$ for $n = 4,\ 5,\ 6$. Since $|X_2| = \binom{n+2}{2} - (n+1) = \binom{n+1}{2}$ holds, X_2 attains the maximum cardinality of 2-distance set. Hence if $n = 5,\ 6$, then the theorem by Ray-chauhuri and Wilson (see [16]) implies $(X_1, X_2, \mathcal{I})$ is a combinatorial tight 4-$(n+1, n-1, n-4)$ design. For $n = 22$, we define the incidence relation $\boldsymbol{x}\mathcal{I}\boldsymbol{u}_i$ by $\varepsilon_i = -1$ for $\boldsymbol{x} \in X_2$ and $\boldsymbol{u}_i \in X_1$. Then $(X_1, X_2, \mathcal{I})$ is the combinatorial tight 4-(23, 7, 1) design (see[11]).

Case $|X_1| = n + 2$

In this case we must have $n = 4$. Then $|X_1| = 6$ and $|X_2| = 9$ and $r = \sqrt{2}$. $X = X_1 \cup X_2$ is similar to the following set:

$$X_1 = \left\{ \begin{array}{lll} \boldsymbol{u}_1 = (a,b,0,0), & \boldsymbol{u}_2 = (b,a,0,0), & \boldsymbol{u}_3 = \frac{1}{\sqrt{2}}(1,1,0,0) \\ \boldsymbol{u}_4 = (0,0,a,b), & \boldsymbol{u}_5 = (0,0,b,a), & \boldsymbol{u}_6 = \frac{1}{\sqrt{2}}(0,0,1,1), \end{array} \right\}$$

where $a = -\frac{1+\sqrt{3}}{2\sqrt{2}}$ and $b = \frac{-1+\sqrt{3}}{2\sqrt{2}}$. X_2 is determined uniquely by the following way:

$$X_2 = \left\{ \boldsymbol{x} \;\middle|\; \begin{array}{l} \langle \boldsymbol{x}, \boldsymbol{u}_i \rangle = -\frac{1}{4} + \frac{3}{4}\varepsilon_i,\ \langle \boldsymbol{x}, \boldsymbol{u}_{i+3} \rangle = -\frac{1}{4} + \frac{3}{4}\eta_i, \varepsilon_i, \eta_i \in \{1,-1\},\ 1 \leq i \leq 3, \\ \sum_{i=1}^{3} \varepsilon_i = \sum_{i=1}^{3} \eta_i = 1 \end{array} \right\}.$$

Let F be a set with 3 elements. Then X_2 is combinatorially considered as Hamming scheme $H(2,3)$ on $F \times F$. Actually we can prove that X_2 is the spherical embedding of $H(2,3)$ into $\mathbb{R}^4$.

4 One more example and a Conjecture for the case $|X_1| \geq n + 3$

We have the following conjecture:

Conjecture

If $|X_1| \geq n+3$, *then there exists a natural number* k *satisfying* $n+3=(2k-1)^2$. *Moreover*

$$\left(\frac{a_1}{a_2}\right)^2=\left(\frac{b_1}{b_2}\right)^2=\frac{k-1}{k}$$

holds, where a_1 *and* a_2 *are the 2 distances of* X_1 *and* b_1 *and* b_2 *are the 2 distances of* X_2.

Case $n=22$, $|X_1|=33$

In this case we can show that only possibility is the following Euclidean tight 4-design.

X_1 is a union of 11 regular triangles on the unit circle in $\mathbb{R}^2 \subset \mathbb{R}^{22}$.

$$X_1=\{u_1,\ldots,u_{33}\},$$

where $\{u_{3i+1},u_{3i+2},u_{3i+3}\}$ $(0\leq i\leq 10)$ is a regular triangle consists of the following unit vectors

$$\begin{aligned}
u_{3i+1}&=(0,0,\ldots,0,\ \tfrac{-1+\sqrt{3}}{2\sqrt{2}},\ -\tfrac{1+\sqrt{3}}{2\sqrt{2}},\ 0,\ldots,0)\\
u_{3i+2}&=(0,0,\ldots,0,\ -\tfrac{1+\sqrt{3}}{2\sqrt{2}},\ \tfrac{-1+\sqrt{3}}{2\sqrt{2}},\ 0,\ldots,0)\\
u_{3i+3}&=(0,0,\ldots,0,\ \tfrac{1}{\sqrt{2}},\ \tfrac{1}{\sqrt{2}},\ 0,\ldots,0),
\end{aligned}$$

where j-th coordinate of u_{3i+l} is 0 for $j\neq 2i+1, 2i+2$.

$r_1=1$, $r_2=\sqrt{11}$. $w(x)=\frac{1}{81}$ on X_2. X_2 is determined uniquely, up to orthogonal transformation, by the following way:

$$X_2\subset\left\{x\in\mathbb{R}^{22}\ \middle|\ \langle x,u_j\rangle=-\frac{1}{4}+\frac{3}{4}\varepsilon_j,\ \varepsilon_j\in\{1,-1\},\ \sum_{l=1}^{3}\varepsilon_{3i+l}=1,\ 0\leq i\leq 10\right\}.$$

Then, combinatorially, we can consider X_2 as a 243-point 2-distance subset of F^{11}, where F is a finite set with 3 elements and F^{11} has the structure of Hamming scheme $H(11,3)$. $H(11,3)$ has a tight 4-design Y with 243 points (see [13, 14]). We can prove that the spherical embedding of Y equals X_2. Moreover X_2 itself is a strongly regular graph whose character table is given by

$$P=\begin{bmatrix}1&132&110\\1&24&-25\\1&-3&2\end{bmatrix},\quad Q=\begin{bmatrix}1&22&220\\1&4&-5\\1&-5&4\end{bmatrix}.$$

Here we give one more conjecture.

Conjecture *Any Euclidean tight 4-design with* $p=2$ *has the structure of coherent configuration.*

We note that all the examples we obtained satisfy the conjecture.

5 Next possible parameters with $n+3=(2k-1)^2$.

In this section we looked for the next possible n satisfying $n+3=(2k-1)^2$.

$n=78$ and $|X_1|=1027$, then $|X_2|=2133$. $r_1=1$, $r_2=\frac{\sqrt{30381}}{19}$, $w_2=\frac{1}{6561}$. Then $\alpha=\frac{13}{171}$ or $-\frac{53}{342}$, and $\frac{\beta}{r_2^2}=\frac{59}{533}$ or $-\frac{119}{1066}$. $\gamma_1=-\frac{3}{76}$, $\gamma_2=\frac{79}{76}$, $m_1=39$ and $m_2=81$.
Possible character tables for X_1:

$$P=\begin{bmatrix} 1 & 684 & 342 \\ 1 & 52 & -53 \\ 1 & -5 & 4 \end{bmatrix},\quad Q=\begin{bmatrix} 1 & 78 & 948 \\ 1 & \frac{338}{57} & -\frac{395}{57} \\ 1 & -\frac{689}{57} & \frac{632}{57} \end{bmatrix}.$$

Possible character tables for X_2:

$$P=\begin{bmatrix} 1 & 1066 & 1066 \\ 1 & 118 & -119 \\ 1 & -5 & 4 \end{bmatrix},\quad Q=\begin{bmatrix} 1 & 78 & 2054 \\ 1 & \frac{354}{41} & -\frac{395}{41} \\ 1 & -\frac{357}{41} & \frac{316}{41} \end{bmatrix}.$$

References

[1] B. Bajnok, *On Euclidean t-designs*, to appear in Advances in Geometry, .

[2] Et. Bannai *On Antipodal Euclidean Tight (2e+1)-Designs*, to appear in J. Algebraic Combinatorics.

[3] Ei. Bannai and Et. Bannai, *Algebraic Combinatorics on Spheres* (in Japanese) Springer Tokyo 1999.

[4] Ei. Bannai and Et. Bannai, *A note on the spherical embeddings of strongly regular graphs*, European J. Combin. 26 (2005) 1177-1179.

[5] Ei. Bannai and Et. Bannai, *On Euclidean tight 4-designs*, J. Math. Soc. Japan 58 (2006), 775-804.

[6] Ei. Bannai, Et. Bannai and D. Suprijanto, *On the strong non-rigidity of certain tight Euclidean designs*, to appear in European J. Combin.

[7] Ei. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schmes*, Benjamin/Cummings, Menlo Park, CA (1984).

[8] P. Delsarte, *An algebraic approsch to the association schemes of coding theory*, Philips Res. Rep. Suppl. 10 (1973).

[9] P. Delsarte, J. M. Goethals, and J. J. Seidel, *Spherical codes and designs*, Geom. Dedicata 6 (1977), 363-388.

[10] P. Delsarte and J. J. Seidel, *Fisher type inequalities for Euclidean t-designs*, Linear Algebra Appl. 114-115 (1989), 213-230.

[11] H. ENOMOTO, N. ITO AND R. NODA, *Tight 4-designs*, Osaka J. Math. 16 (1979) 39-43.

[12] D. G. Larman, C. A. Rogers and J. J. Seidel, *On two-distance sets in Euclidean space*, Bull London Math. Soc. 9 (1977) 261-267.

[13] R. NODA, On orthogonal arrays of strength 4 achieving Rao's bound, J. London Math. Soc. (2) 19 (1979) 385-390.

[14] R. NODA, On orthogonal arrays of strength 3 and 5 achieving Rao's bound, Graphs and Combinatorics 2 (1986) 277-282.

[15] A. NEUMAIER AND J. J. SEIDEL, *Discrete measures for spherical designs, eutactic stars and lattices*, Nederl. Akad. Wetensch. Proc. Ser. A 91=Indag. Math. 50 (1988), 321-334.

[16] D. K. RAY-CHAUHURI AND R. M. WILSON, *On t-designs*, Osaka J. Math. 12 (1975) 737-744.

On three-distance sets in the three-dimensional Euclidean Space

Masashi Shinohara (Kyushu University)

Abstract

A subset X in the d-dimensional Euclidean space $\mathbb{R}^d$ is called a k-distance set if there are exactly k distances between two distinct points in X. Einhorn and Schoenberg conjectured that the vertices of the regular icosahedron is the only 12-point three-distance set in $\mathbb{R}^3$ up to isomorphism. In this note we prove the uniqueness of 12-point three-distance sets in the two-dimensional sphere S^2 and prove the nonexistence of a 14-point three-distance set in $\mathbb{R}^3$.

1 Introduction

Let $\mathbb{R}^d$ be the d-dimensional Euclidean space. For $X \subset \mathbb{R}^d$, let $A(X) = \{PQ | P, Q \in X, P \neq Q\}$ where PQ is the Euclidean distance between P and Q in $\mathbb{R}^d$. We call X a k-distance set if $|A(X)| = k$. For two subsets in $\mathbb{R}^d$, we say that they are isomorphic if there exists a similar transformation from one to the other. An interesting problem on k-distance sets is to determine the largest possible cardinality of k-distance sets in $\mathbb{R}^d$. We denote this number by $g_d(k)$. E. Bannai-E. Bannai-D. Stanton [2] and A. Blokhuis [3] gave an upper bound $g_d(k) \leq \binom{d+k}{k}$. A k-distance sets X in $\mathbb{R}^d$ is maximum if $|X| = g_d(k)$. For $k = 2$, the numbers $g_d(2)$ are known for $d \leq 8$ (L. M. Kelly [9], H. T. Croft [4] and P. Lisoněk [11]). For $d = 2$, the numbers $g_2(k)$ are known and maximum k-distance sets are classified for $k \leq 5$ (P. Erdős-P. Fishburn [7], [8], M. Shinohara [12], [13]). However, for $d \geq 3$ and $k \geq 3$, even the smallest case $g_3(3)$ have not been determined. In this case, S. J. Einhorn-I. J. Schoenberg [6] conjectured the following:

Conjecture 1.1. *The vertices of the regular icosahedron is the only 12-point three-distance set in* $\mathbb{R}^3$.

The followings are the main results of this note.

Theorem 1.1. *(i) There are no 14-point three-distance sets in* $\mathbb{R}^3$. *Thus* $g_3(3) = 12$ *or* 13. *(ii) The vertices of the regular icosahedron is the only 12-point three-distance set in* S^2.

In section 2, we introduce diameter graphs and characterize the diameter graphs for finite subsets in three-dimensional Euclidean space. Our goal of section 2 is to prove the following:

Theorem 1.2. *(i) Every 14-point three-distance set in $\mathbb{R}^3$ contains a five-point two-distance set in $\mathbb{R}^3$.*
(ii) Every 12-point three-distance set in S^2 contains a five-point two-distance set in S^2 or a four-point two-distance set in S^1.

Since five-point two-distance sets in $\mathbb{R}^3$ and four-point two-distance sets in S^1 have been classified, we have Theorem 1.1 by using computer calculations. We give the details of these calculations in section 3.

2 Diameter graphs

Let $G = (V, E)$ be a simple graph, where $V = V(G)$ and $E = E(G)$ are the vertex set and the edge set of G, respectively. We denote a path and a cycle with n vertices by P_n and C_n, respectively. We denote a complete graph of order n by K_n. A subset H of $V(G)$ is an **independent set** of $V(G)$ if no two vertices in H are adjacent. The **independence number** $\alpha(G)$ of a graph G is the maximum cardinality among the independent sets of G. The **Ramsey number** $R(s,t)$ is the smallest value of n for which every red-blue coloring of K_n yields a red K_s or a blue K_t. For example, Ramsey numbers $R(3,t)$ are known as $R(3,3) = 6$, $R(3,4) = 9$, $R(3,5) = 14$.

For $X \subset \mathbb{R}^d$, the diameter of X is defined by $D(X) = \max A(X)$. Diameters give us important information when we study distance sets in particular in few dimensional space. The diameter graph $DG(X)$ for $X \subset \mathbb{R}^d$ is the graph with X as its vertices and where two vertices $P, Q \in X$ are adjacent if $PQ = D(X)$. Let R_n be the set of the vertices of a regular n-gon. Clearly $DG(R_{2n+1}) = C_{2n+1}$ and $DG(R_{2n}) = n \cdot P_2$. Note that if $\alpha(DG(X)) = n'$ for a k-distance set X, then X contains an n'-point k'-distance set for some $k' < k$.

The diameter graph $G = DG(X)$ of $X \subset \mathbb{R}^2$ does not contain C_4 and if G contains C_3, then any two vertices in $V(G) \setminus V(C_3)$ are not adjacent. For diameter graphs for $\mathbb{R}^2$, we have the following propositions ([13]).

Proposition 2.1. *Let $G = DG(X)$ for $X \subset \mathbb{R}^2$. Then*
(i) G contains no C_{2k} for any $k \geq 2$;
(ii) if G contains C_{2k+1}, then any two vertices in $V(G) \setminus V(C_{2k+1})$ are not adjacent and every vertex not in the cycle is adjacent to at most one vertex of the cycle.
In particular, G contains at most one cycle.

Proposition 2.2. *Let $G = DG(X)$ be the diameter graph of $X \subset \mathbb{R}^2$ with $|X| = n$. If $G \neq C_n$, then we have $\alpha(G) \geq \lceil \frac{n}{2} \rceil$.*

The above propositions are implied from the fact that two segments with the diameter must cross if they do not share an end point. We consider an analogue of this fact for three dimensional Euclidean space.

Lemma 2.1. *Let $P_1P_2 = P_2P_3 = P_3P_1 = c$ for $P_1, P_2, P_3 \in \mathbb{R}^3$ and $c \in \mathbb{R}_{>0}$. Π be the plane determined by $\{P_1, P_2, P_3\}$ and R^+ and R^- be the division of $\mathbb{R}^3$ by Π. Here let Π be contained in R^+. Let $S^+ = \{Q \in R^+ | P_iQ \leq c$ for any $i = 1, 2, 3\}$ and $S^- = \{Q \in$*

$R^-|P_iQ \leq c$ *for any* $i = 1,2,3\}$. *Then* $Q_1Q_2 \leq c$ *for any* $Q_1, Q_2 \in S^+$ *and equality holds only if* Q_1 *or* Q_2 *coincides* P_i *for some* $i = 1,2,3$. *Moreover* $Q_1Q_2 < c$ *for any* $Q_1, Q_2 \in S^-$.

In Lemma 2.1, let $c = D(X)$ for any $X \subset \mathbb{R}^3$. Then we have the following proposition.

Proposition 2.3. *Let* $G = DG(X)$ *for* $X \subset \mathbb{R}^3$ *with* $|X| = n$. *Let* G *contains a triangle* G'. *Then the graph* $G - G'$ *is a bipartite graph. In particular* $\alpha(G) \geq \lceil \frac{n-3}{2} \rceil$.

By Proposition 2.3, for 12-point three-distance set $X \subset \mathbb{R}^3$, if $G = DG(X)$ contains K_3, then $\alpha(G) \geq 5$. Therefore to prove the uniqueness of 12-point three-distance sets in $\mathbb{R}^3$, we want to know more information about 12-point three-distance sets in $\mathbb{R}^3$ with $\alpha(G) \geq 5$ and K_3-free for their diameter graphs G. The following is useful to prove the uniqueness of 12-point three-distance sets in S^2.

Proposition 2.4. *Let* G *be a* K_3*-free graph of order 12 with* $\alpha(G) < 5$. *Then there exists a vertex* $v \in V(G)$ *with* $deg(v) = 4$.

Proof of Theorem 1.2
(i) Let X be a 14-point three-distance set in $\mathbb{R}^3$ and $G = DG(X)$. If G contains K_3, then X contains a six-point two-distance set in $\mathbb{R}^3$ by Proposition 2.3. Otherwise, $\alpha(G) \geq 5$ since $R(3,5) = 14$.
(ii) Let X be a 12-point three-distance set in S^2 and $G = DG(X)$. We may assume G is K_3-free and $\alpha(G) < 5$. By Proposition 2.4, there exists a vertex O with $deg(O) = 4$. Then the neighbors of O consists of a four-point two-distance set in S^1, otherwise G contains K_3 and then $\alpha(G) \geq 5$.

3 Calculations

In this section, we prove Theorem 1.1 from Theorem 1.2. To complete the proof, it is sufficient to classify 12-point three-distance sets $X \subset \mathbb{R}^3$ containing a five-point two-distance set $Y \subset \mathbb{R}^3$ with $D(Y) < D(X)$ and 12-point three-distance sets $X \subset S^2$ containing a four-point two-distance set $Y \subset S^1$ with $D(Y) < D(X)$.

I. 12-point three-distance sets containing a five-point two-distance set Y.

Five-point two-distance sets in $\mathbb{R}^3$ are classified ([6]). We give coordinates of these sets in table 1. For any sets Y in table 1, $1 \in A(Y)$. Let d be the other distance in $A(Y)$.
We divide into following two cases: Case 1: $Y \neq R_5$, Case 2: $Y = R_5$

Case 1: Let $Y = \{Q_1, Q_2, \cdots, Q_5\}$ be a five-point two-distance set in $\mathbb{R}^3$ except R_5. Let

$$Candi(Y) = \{P \in \mathbb{R}^3 | Y \cup \{P\} \textit{is a } k\textit{-distance set with six points, } k \leq 3\}.$$

Lemma 3.1. *Let* Y *be a five-point two-distance set in* $\mathbb{R}^3$ *except* R_5. *Then* $|Candi(Y)| < +\infty$.

Proof. For $P \in Candi(Y)$, let $Old(P) = \{Q \in Y | PQ \in A(Y)\}$, $New(P) = \{Q \in Y | PQ \notin A(Y)\}$ and $Type(P) = |New(P)|$. We consider three cases. First we consider the case where $Type(P) \leq 2$. Suppose $\{Q_1, Q_2, Q_3\} \subset Old(P)$. Since $PQ_i \in A(Y)$ and no three points in Y is colinear, the possibility of P is at most $2 \cdot 2^3$. Next we consider the case where $Type(P) = 3, 4$. Suppose $\{Q_1, Q_2, Q_3\} \subset New(P)$ and $Q' \in Old(P)$. Let L be the perpendicular of the plane determined by Q_1, Q_2, Q_3 which pass through the center of Q_1, Q_2, Q_3. Since P lies on L and $PQ' \in A(Y)$, the possibility of P is at most 4. Finally we consider the case where $Type(P) = 5$. Since the points in Y are noncoplanar, the possibility of P is at most 1. Therefore $|Candi(Y)| \leq \binom{5}{3} \cdot 16 + \binom{5}{3} \cdot \binom{2}{1} \cdot 4 + 1$. □

By the proof of Lemma 3.1, we can find all point in $Candi(Y)$ for any five-point two-distance set Y except R_5. We can check that vertices of the regular icosahedron is the only 12-point three-distance set containing five-point two-distance sets under the assumption in case 1.

Case 2: Let $R_5 = \{Q_1, Q_2, \cdots, Q_5\}$ be labeled by cyclic order and $A(R_5) = \{1, \frac{1+\sqrt{5}}{2}\}$ Let X be a 12-point three-distance set in $\mathbb{R}^3$ containing R_5 and $d_3 = D(X) \notin A(R_5)$. Let L be the perpendicular of the plane determined by R_5 which pass through the center of R_5. Suppose $P_0 \in X$ is on L. We may assume $P_0Q_1 = d_3$, otherwise $R_5 \cup \{P\}$ containing another five-point two-distance set and such X is actually Case 1. If $P_0' \neq P_0$ is also on L, then $P_0P_0' > d_3$. Therefore other points $P \in X' = X \setminus (R_5 \cup \{P_0\})$ satisfy one of the following:

$$Type(1) = \{P \in X' | PQ_{i-1} = PQ_i = 1, PQ_{i-2} = PQ_{i+1} = \tfrac{1+\sqrt{5}}{2}, PQ_{i+2} = d_3\};$$
$$Type(2) = \{P \in X' | PQ_i = 1, PQ_{i-1} = PQ_{i+1} = \tfrac{1+\sqrt{5}}{2}, PQ_{i-2} = PQ_{i+2} = d_3\}.$$

Suppose $P \in Type(1)$. Then $R_5 \cup \{P\}$ contains a five-point two-distance set different from R_5. Next suppose $P \in Type(2)$. Then $R_5 \cup \{P\}$ is a subset of the vertices of a dodecahedron. Since $|X'| \geq 6$, X must contain an 8-point subset of the vertices of a dodecahedron. However this can not be a three-distance set.

II. 12-point three-distance sets in S^2 containing a four-point two-distance set in S^1

In this part, we prove the nonexistence of 12-point three-distance set X in S^2 which have a point O such that $deg(O) = 4$ in its diameter graph. Let $X_i = \{Q \in X | OQ = d_i\}$ for $i = 1, 2, 3$. Clearly X_3 is R_4 or a four point subset of R_5. Since $|X_1 \cup X_2| = 7$, we take $X' \subset X_i$ for some $i = 1, 2$ such that $|X'| = 4$. For each case, we can prove that $X_3 \cup X' \cup \{O\}$ can not be a three-distance set.

References

1 E. Bannai and E. Bannai, Algebraic Combinatorics on Spheres(in Japanese), Springer Tokyo, 1999.

2 E. Bannai, E. Bannai and D. Stanton, An upper bound for the cardinality of an s-distance subset in real Euclidean space, II, Combinatorica 3 (1983), 147-152.

3 A. Blokhuis, Few-distance sets, Ph. D. thesis, Eindhoven Univ. of Technology (1983), (CWI Tract (7) 1984).

4 H. T. Croft, 9-point and 7-point configuration in 3-space, Proc. London Math. Soc. (3), 12 (1962), 400-424.

5 S. J. Einhorn and I. J. Schoenberg, On Euclidean sets having only two distances between points I, Nederl Akad. Wetensch. Proc. Ser. A69=Indag. Math. 28 (1966), 479-488.

6 S. J. Einhorn and I. J. Schoenberg, On Euclidean sets having only two distances between points II, Nederl Akad. Wetensch. Proc. Ser. A69=Indag. Math. 28 (1966), 489-504.

7 P. Erdős and P. Fishburn, Convex nonagons with five intervertex distance, Geometriae Dedicata 60 (1996) 317-332.

8 P. Erdős and P. Fishburn, Maximum planar sets that determine k distances, Discrete Math. , 160 (1996) 115-125.

9 L. M. Kelly, Elementary Problems and Solutions. Isosceles n-points, Amer. Math. Monthly, 54 (1947), 227-229.

10 D. G. Larman, C. A. Rogers,and J. J. Seidel, On two-disatance sets in Euclidean space, Bull. London Math. Soc. , 9 (1977), 261-267.

11 P. Lisoněk, New maximal two-distance sets, J. Combin. Theory, Ser. A77 (1997), 318-338.

12 M. Shinohara, Classification of three-distance sets in two dimensional Euclidean space, Europ. J. Combinatorics, 25 (2004) 1039-1058.

13 M. Shinohara, Uniqueness of maximum planar five-distance sets, submitted

Trees and spanning trees on m-uniform hypergraphs

Tatsuya Fujisaki
Graduate School of Mathematics
Kyushu University

Abstract

An original graph consists of a vertex set and an edge set. Each edge is a 2-subset of the vertex set. An m-uniform hypergraph consists of a vertex set and an edge set but each edge is an m-subset of the vertex set. Similar to the case of original graphs, we can define a tree of m-uniform hypergraph. In original graph, it is well-known that the number of trees on a vertex set of size N is N^{N-2}. In this paper, as a generalization, we compute the number of trees on a vertex set of size N and related topics.

1 Introduction

Suppose $m \geq 2$. For a set V and a set E of m-subsets of V, the pair (V, E) is called an *m-uniform hypergraph*. So we can say that graphs are 2-uniform hypergraphs. For an m-uniform hypergraph $G = (V, E)$, consider a bipartite graph whose vertex set is $V \cup E$ and edge set is $\{ \{v, e\} : v \in V, e \in E, v \in e\}$. If the bipartite graph forms a tree, we say that G is a *tree* (as m-uniform hypergraph.) We note that every path in the bipartite graph is a sequence appearing vertices and edges alternatively. If a subset E' of E satisfies that (V, E') forms a tree, we say that the hypergraph (V, E') is a *spanning tree* of G. We say that an m-uniform hypergraph is *complete* if E consists of all m-subsets of V.

For 2-uniform hypergraphs, that is, graphs, a notation of spanning trees in a graph (V, E) is shown.

Theorem 1.1. (cf. [1, §2.2], [4]) *Let $V = \{v_1, v_2, \cdots, v_N\}$ and x_{ij} $(i \neq j)$ be a variable with a condition that $x_{ij} = x_{ji}$ for any i and j. For a 2-uniform hypergraph $G = (V, E)$, let M be an $N \times N$ matrix such that*

$$M_{ij} = \begin{cases} \sum_{\{v_i, v_k\} \in E} x_{ik} & \text{if } i = j, \\ -x_{ij} & \text{if } \{v_i, v_j\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

Then a matrix $M^{(N)}$ obtained by removing the N-th row and column from M satisfies

$$Det(M^{(N)}) = \sum_{\substack{E' \subseteq E \\ (V, E'):\ tree}} \left(\prod_{\{v_i, v_j\} \in E'} x_{ij} \right).$$

We can see that for any index i, a determinant of a matrix obtained by removing the i-th row and column from M is equal to $Det(M^{(N)})$. From this theorem, we can get the numbers of trees on a fixed vertex set and that of spanning trees of a complete bipartite graph.

Corollary 1.2. (i) *The number of trees on a vertex set of size N is N^{N-2}.*
(ii) *The number of spanning trees of a complete bipartite graph between an N_1-set and an Nforming$_2$-set is $N_1^{N_2-1}N_2^{N_1-1}$.*

For 3-uniform hypergraph, we can easily see that if a 3-uniform hypergraph has a tree, then the number of vertices is odd. G. Masbaum and A. Vaintrob [3] showed a notation of all trees in a 3-uniform hypergraph. Later S. Hirschman and V. Reiner [2] showed another proof of this theorem.

Theorem 1.3. *Suppose that N is an odd integer. Let $V = \{v_1, v_2, \cdots, v_N\}$ and y_{ijk} $(1 \leq i, j, k \leq N)$ be a variable with a condition $y_{\sigma(i)\sigma(j)\sigma(k)} = \mathrm{sgn}(\sigma) y_{ijk}$ where σ is a permutation on $\{i, j, k\}$. For a 3-uniform hypergraph $G = (V, E)$, let M be a $N \times N$ matrix such that*

$$M_{ij} = \begin{cases} \sum_{\{v_i, v_j, v_k\} \in E} y_{ijk} & \text{if } i \neq j. \\ 0 & \text{if } i = j \end{cases}$$

(M is skew-symmetric.) Then a matrix $M^{(N)}$ obtained by removing the N-th row and column from M satisfies

$$\mathrm{Pf}(M^{(N)}) = \sum_{\substack{E' \subseteq E \\ (V, E'): \text{ tree}}} \mathrm{sgn}(\sigma_{E'}) \left(\prod_{\{i,j,k\} \in E'} x_{ijk} \right).$$

where $\sigma_{E'}$ is a permutation on $\{1, 2, \cdots, N\}$ satisfying

$$\sigma_{E'}^{-1}(1, 2, \cdots, N)\sigma_{E'} = \prod_{\substack{\{v_i, v_j, v_k\} \in E' \\ i<j<k}} (i, j, k)$$

Remark that the permutation $\sigma_{E'}$ depends on arrangements of (i, j, k)'s but $\mathrm{sgn}(\sigma_{E'})$ is independent of them. We can see that for any index i, a Pfaffian of a matrix obtained from removing the i-th row and column from M is equal to $\mathrm{Pf}(M^{(N)})$.

It is hard to compute the number of trees in a 3-uniform hypergraph from the above result. So, in general case, we compute the number of trees of an m-uniform hypergraph on a vertex set of size N where $m \geq 2$. Similarly we compute the number of spanning trees of an complete m-partite m-uniform hypergraph, which is a generalization of complete bipartite graph.

2 Preliminaries

Suppose $m \geq 2$. Let V be a set of size N and E be a set of m-subsets of V. We call a pair (V, E) be an *m-uniform hypergraph*. We call an element of V a *vertex* and an element of E an *edge*. Consider a graph $B(V, E)$ with vertex set $V \cup E$ and edge set $\{(v, e) \mid v \in V, e \in E, v \in e\}$. Note that the graph is bipartite. If $B(V, E)$ forms a tree, we say that (V, E) is a *tree* on V. For s subset E' of E, if (V, E') forms a tree, we call (V, E') *spanning tree* of (V, E). For an edge $e \in E$ is called a *leaf* if e has a unique vertex contained in other edge of E. We call the vertex a *leafstalk* of e in E and denote the leafstalk v_e. We can see that $e \in E$ is a leaf with a leafstalk v if and only if $\bigcup_{e' \in E \setminus \{e\}} (e \cap e') = \{v\}$. For a leaf e with a leafstalk v_e, put $\pi_e = e \setminus \{v_e\}$. For example, when $m = 3$ and $V = \{1, 2, \cdots, 13\}$, a set $\{\{1, 6, 11\}, \{1, 7, 12\}, \{2, 8, 13\}, \{3, 7, 10\}, \{4, 8, 12\}, \{5, 9, 12\}\}$ forms a tree. In this tree, $\{1, 6, 11\}$, $\{3, 7, 10\}$ and $\{5, 9, 12\}$ are leaves. We can see the following propositions.

Proposition 2.1. (i). *There exists a set of m-subsets of V forming a tree if and only if* $N-1 \equiv 0 \pmod{m-1}$. *Moreover the number of edges of a tree is* $(N-1)/(m-1)$.
(ii). *Suppose* $N-1 \equiv 0 \pmod{m-1}$. *An edgeset E is a tree if and only if* $|E| = (N-1)/(m-1)$ *and* (V,E) *is connected.*

Hence we assume that $N = k(m-1)+1$ for some integer $k \geq 1$. Let $A_0, A_1, \cdots, A_{m-1}$ be mutually disjoint (non-empty) sets satisfying $\sum_{i=0}^{m-1} |A_i| = N$. Put $V = A_0 \cup A_1 \cup \cdots \cup A_{m-1}$ and $E = \{\{v_0, v_1, \cdots, v_{m-1}\} \mid v_i \in A_i\}$. Then we say that a m-uniform hypergraph (V,E) a *complete m-partite m-uniform hypergraph* and denote the hypergraph as $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$ where $a_i = |A_i|$ for each $i \in \{0,1,\cdots,m-1\}$.

Proposition 2.2. *A hypergraph $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$ has a spanning tree if and only if* $\sum_{i=0}^{m-1} a_i = k(m-1)+1$ *and each a_i is at most k.*

From this lemma, we have

$$\sum_{i=1}^{m}(k-a_i) = km - (k(m-1)+1) = k-1,$$

Hence the number of sequences $(a_0, a_1, \cdots, a_{m-1})$, up to permutation, such that $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$ has a spanning tree is equal to the number of partitions of $k-1$ into at most m positive integers.

3 A computation of trees

In this section, we show that the number of trees on a vertex set of size $N = k(m-1)+1$ is equal to

$$\frac{(k(n-1))!}{k!((n-1)!)^k}(k(n-1)+1)^{k-1}.$$

Let V be a finite set of positive integers with size $k(m-1)+1$ and $M(V)$ be the greatest integer of V. Denote $P(V, m-1)$ as the set of partitions of $V \setminus \{M(V)\}$ into k subsets whose size are all $m-1$. Let $S(V,k)$ be the set of sequences of V with k entries such that the first entry is $M(V)$. Then the above number is equal to the size of a set $P(V,m-1) \times S(V,k)$. For a leaf e of an m-uniform hypergraph, let v_e be the leafstalk of e and $\pi_e = e \setminus \{v_e\}$. Note that each π_e is an $(m-1)$-subsets of V. For a subset π of V, let $m(\pi)$ be the smallest vertex in π.

First, for each tree $\mathcal{T} = (V,T)$, construct a partition $\Pi_{\mathcal{T}}$ in $P(V,m-1)$ and a sequence $S_{\mathcal{T}}$ in $S(V,k)$ by using induction of $|V|$. When $k=1$, the edge set T is just V. In this case, we put $\Pi_{\mathcal{T}} = \{V \setminus \{M(V)\}\}$ and $S_{\mathcal{T}} = (M(V)) \in S(V,1)$. When $k \geq 2$, we can see that there exists at least two leaves in $\mathcal{T}$ and any two leaves have no common vertex except their leafstalks. So there exists a leaf e_0 of $\mathcal{T}$ such that $M(V) \notin \pi_{e_0}$ and $m(\pi_{e_0}) < m(\pi_e)$ for any other leaf e of $\mathcal{T}$ satisfying $M(V) \notin \pi_e$. Then an m-uniform hypergraph $\mathcal{T}_0 = (V \setminus \pi_{e_0}, T \setminus \{e_0\})$ is a tree. Since $|V \setminus \pi_{e_0}| = (k-1)(m-1)+1$ and $M(V) \in V \setminus \pi_{e_0}$, by using induction, we can construct $\Pi_{\mathcal{T}_0} \in P(V \setminus \pi_{e_0}, m-1)$ and $S_{\mathcal{T}_0} = (v_1 = M(V), v_2, \cdots, v_{k-1}) \in S(V \setminus \pi_{e_0}, k-1)$ to $\mathcal{T}_0$. From them, we put $\Pi_{\mathcal{T}} = \Pi_{\mathcal{T}_0} \cup \{\{\pi_{e_0}\}\} \in P(V, m-1)$ and $S_{\mathcal{T}} = (v_1, v_2, \cdots, v_{k-1}, v_{e_0}) \in S(V,k)$ to $\mathcal{T}$.

Example. When $m=3$ and $V = \{1,2,\cdots,11\}$ (then $k=5$), an edge set

$$T = \{\{1,10,11\},\{2,4,8\},\{2,7,10\},\{3,7,9\},\{5,6,9\}\}$$

forms a spanning tree with leaves $\{1,10,11\}$, $\{2,4,8\}$ and $\{5,6,9\}$. Then

$$\{\pi_e \mid e:\ \text{a leaf of } T\} = \{\{1,11\},\{4,8\},\{5,6\}\}.$$

Since a leaf $\{1,10,11\}$ contains $M(V)=11$, which is not its leafstalk, we put $e_0=\{2,4,8\}$. Then $v_{e_0}=2$. For a tree $\mathcal{T}_0=(V\setminus\{4,8\},T\setminus\{e_0\})$, we can see that

$$\begin{aligned}\Pi_{\mathcal{T}_0} &= \{\{1,10\},\{2,7\},\{3,9\},\{5,6\}\}\in P(V\setminus\{2,11\},2)\\ S_{\mathcal{T}_0} &= (11,10,7,9)\in S(V\setminus\{2,11\},4)\end{aligned}$$

So we construct the following partition and sequence:

$$\begin{aligned}\Pi_{\mathcal{T}} &= \{\{1,10\},\{2,7\},\{3,9\},\{4,8\},\{5,6\}\}\in P(V,2)\\ S_{\mathcal{T}} &= (11,10,7,9,2)\in S(V,5).\end{aligned}$$

Remark that for a suitable ordering $\pi_1,\pi_2,\cdots,\pi_k$ of $\Pi_{\mathcal{T}}$, we have that

$$\{\pi_i\cup\{v_i\}\mid 1\le i\le k\}=T. \tag{1}$$

We can see that the above mapping $\mathcal{T}\mapsto(\Pi_{\mathcal{T}},S_{\mathcal{T}})$ is bijection.

Theorem 3.1. *Let $N=k(m-1)+1$. The number of trees on a vertex set of size $k(m-1)+1$ is equal to* $\dfrac{(k(m-1))!}{k!((m-1)!)^k}(k(m-1)+1)^{k-1}$.

4 Spanning trees in some hypergraphs

In this section, we consider the number of spanning trees of hypergraphs obtained by deleting one or two edges from a complete m-uniform hypergraph $K_N^{(m)}=(V,T)$ where $V=\{1,2,\cdots,N\}$ and T is the set of all m-subsets of V.

4.1

For an m-subset e of V, compute the number of spanning trees of a hypergraph $K_N^{(m)}\setminus e=(V,T\setminus\{e\})$. It is clear that the number is equal to

$$|P(V,m-1)|N^{k-1}-|\{(V,T'):\text{tree}\mid e\in T'\}|.$$

We may suppose that $e=\{N,N-1,\cdots,N-m+1\}$. Then the following lemma can be proved easily.

Lemma 4.1. *For a tree $T'=(V,T')$, it contains $e=\{N,N-1,\cdots,N-m+1\}$ if and only if corresponding pair $(\Pi_{T'},S_{T'})$ satisfies that $e\setminus\{N\}\in\Pi_{T'}$ and k-th entry of $S_{T'}$ is in e.*

From this lemma, we can compute the number of spanning trees containing e, which is equal to $|P(V\setminus(e\setminus\{N\}),m-1)|\times mN^{k-2}$.

Theorem 4.2. *The number of spanning trees in $K_N^{(m)}\setminus e$ is equal to*

$$\begin{aligned}&|P(V,m-1)|N^{k-1}-|P(V\setminus(e\setminus\{N\}),m-1)|mN^{k-2}\\ =\ &\frac{N^{k-2}}{k!((m-1)!)^k}(N!-k(N-m)!m!).\end{aligned}$$

Denote $\overline{T}$ as the set of trees with an edge $\{N,N-1,\cdots,N-m+1\}$

4.2

For two distinct m-subsets e_1 and e_2, compute the number of spanning trees of $K_N^{(m)} \setminus \{e_1, e_2\} = (V, T \setminus \{e_1, e_2\})$. The number is equal to

$$|P(V, m-1)|N^{k-1} - 2|P(V \setminus (e_1 \setminus \{N\}), m-1)|mN^{k-2} + |\{(V, T') : \text{tree} \mid e_1, e_2 \in T'\}|.$$

It is clear that if $|e_1 \cap e_2| \geq 2$, there is no tree containing e_1 and e_2. Suppose that $|e_1 \cap e_2| = 1$. Then we may assume that $e_1 = \{N, N-1, \cdots, N-m+1\}$ and $e_2 = \{N, N-m, \cdots, N-2m+2\}$. Clearly if $k = 2$ there is only one tree containing e_1 and e_2 whose edgeset is just $\{e_1, e_2\}$. We can easily prove following lemma

Lemma 4.3. *Suppose that $k \geq 3$ and let $T' = (V, T') \in \overline{T}$. Then T' contains $e_2 = \{N, N-m, \cdots, N-2m+2\}$ if and only if corresponding pair $(\Pi_{T'}, S_{T'})$ satisfies that $e_2 \setminus \{N\} \in \Pi_{T'}$. $(k-1)$-entry of $S_{T'}$ is in $e_1 \cup e_2$ and k-entry of $S_{T'}$ is N.*

From this lemma, for $k \geq 3$,

$$\begin{aligned} |\{(V, T') : \text{tree} \mid e_1, e_2 \in T'\}| &= |P(V \setminus (e_1 \cup e_2 \setminus \{N\}), m-1)| \times (2m-1)N^{k-3} \\ &= \frac{(k-2)(m-1)}{(k-2)!((m-1)!)^{k-2}} \times (2m-1)N^{k-3}. \end{aligned}$$

Suppose that $|e_1 \cap e_2| = 0$. It is clear that when $k = 2$, there is no tree containing e_1 and e_2. For $k \geq 3$, we may assume that $e_1 = \{N, N-1, \cdots, N-m+1\}$ and $e_2 = \{1, 2, \cdots, m\}$. We can easily prove following lemma:

Lemma 4.4. *Suppose that $k \geq 3$ and let $T' = (V, T') \in \overline{T}$. Then T' contains $e_2 = \{N, N-m, \cdots, N-2m+2\}$ if and only if corresponding pair $(\Pi_{T'}, S_{T'})$ satisfies that that there exists a vertex $v \in e_2$ such that $e_2 \setminus \{v\} \in \Pi_{T'}$ and one of the following holds:*
(1) Second entry of $S_{T'}$ is v and for $j > 2$, j-th entry of $S_{T'}$ is not in e_2.
(2) For some $i \geq 3$, $(i-1)$-th entry of $S_{T'}$ is in $e_2 \setminus \{v\}$, i-th entry of $S_{T'}$ is v and for $j > i$, j-th entry of $S_{T'}$ is not in e_2.

From this lemma, for $k \geq 3$,

$$\begin{aligned} & |\{(V, T') : \text{tree} \mid e_1, e_2 \in T'\}| \\ = \; & |P(V \setminus (e_1 \cup e_2 \setminus \{N\}), m-1)| \times m \\ & \quad \times \left\{ (N-m+1)^{k-3} \times m + \sum_{i=0}^{k-3} N^i \times (m-1) \times (N-m+1)^{k-4-i} \times m \right\} \\ = \; & |P(V \setminus (e_1 \cup e_2 \setminus \{N\}), m-1)| \times m \\ & \quad \times \left\{ m(N-m+1)^{k-3} + m(m-1)\frac{N^{k-3} - (N-m+1)^{k-3}}{N - (N-m+1)} \right\} \\ = \; & |P(V \setminus (e_1 \cup e_2 \setminus \{N\}), m-1)| \times m^2 N^{k-3} \\ = \; & \frac{(k-2)(m-1)}{(k-2)!((m-1)!)^{k-2}} \times m^2 N^{k-3}. \end{aligned}$$

From above results, we can compute the number of spanning trees in $K_N^{(m)} \setminus \{e_1, e_2\}$

5 Computing the number of spanning trees of $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$

We suppose each A_i is in the integer set and let M be the maximal number of $V = A_0 \cup A_1 \cup \cdots \cup A_{m-1}$, which is in A_0. For $i \in \{0, 1, \cdots, m-1\}$, let $b_i = k - a_i$ and

$$\Lambda = \{(0,0)\} \cup \{(i,j) \mid 0 \le i \le m-1, 1 \le b_i, 1 \le j \le b_i\}.$$

Let $\mathcal{T} = (V, T)$ be a spanning tree of $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$. By using induction of k, we construct a partition $\Pi_{\mathcal{T}}$ of $V \setminus \{M\}$ into k subsets with size $m-1$ and a sequence $S_{\mathcal{T}} = (S_{(i,j)})_{(i,j)\in\Lambda}$ with a condition $S_{(0,0)} = M$ and $S_{(i,j)} \in A_i$, equivalently, $S_{\mathcal{T}} \in \{M\} \times A_0^{b_0} \times A_1^{b_1} \times \cdots A_{m-1}^{b_{m-1}}$. For a subset π of V, let $m(\pi)$ be the smallest element of π.

When $k = 1$, $\Lambda = \{(0,0)\}$ and the edge set T is same to V. In this case, we assign $\Pi_{\mathcal{T}} = V \setminus \{M\}$ and $S_{\mathcal{T}} = (S_{(0,0)} = M)$. When $k \ge 2$, there exists a leaf e_0 such that $M \notin \pi_{e_0}$ and $m(\pi_{e_0}) < m(\pi)$ for any other leaf e of T such that $M \notin \pi_e$. Suppose that $v_{e_0} \in A_l$. Then $b_l \ge 1$, hence $(l, b_l) \in \Lambda$. Then $\mathcal{T}_0 = (V \setminus \pi_{e_0}, T \setminus \{e_0\})$ is a spanning tree of $K^{(m)}_{a'_1,a'_2,\cdots,a'_m}$ where $a'_l = a_l$ and $a'_i = a_i - 1$ for other i. For a partition $\Pi_{\mathcal{T}_0}$, we define $\Pi_{\mathcal{T}} = \Pi_{\mathcal{T}_0} \cup \{\pi_{e_0}\}$, which is a partition of $V \setminus \{M\}$ into k subsets with size $m-1$. A sequence $S_{\mathcal{T}_0} = (S_{(i,j)})$ is indexed by $\Lambda \setminus \{(l, b_l)\}$. Define $S_{\mathcal{T}}$ by adding v_{e_0} as $S_{(l,b_l)}$.

Example. Let $A_0 = \{13, 12, 11, 10\}$, $A_1 = \{9, 8, 7, 6\}$ and $A_2 = \{5, 4, 3, 2, 1\}$, that is, $(a_0, a_1, a_2) = (4, 4, 5)$. Then a 3-uniform hypergraph $K^{(3)}_{4,4,5}$ has a spanning tree $\mathcal{T} = (V = A_0 \cup A_1 \cup A_2, T)$ where

$$T = \{\{11, 6, 1\}, \{12, 7, 1\}, \{13, 8, 2\}, \{10, 7, 3\}, \{12, 8, 4\}, \{12, 9, 5\}\}.$$

A leaf $e_0 = \{10, 7, 3\}$ satisfies $M = 13 \notin \pi_{e_0} = \{10, 3\}$ and $m(\pi_{e_0}) < m(\pi_e)$ for any other leaf e of T such that $M \notin \pi_e$. For a spanning tree $\mathcal{T}_0 = (V \setminus \{10, 3\}, T \setminus \{e_0\})$ of $K^{(3)}_{3,4,4}$,

$$\begin{aligned} \Pi_{\mathcal{T}_0} &= \{\{7, 1\}, \{8, 2\}, \{12, 4\}, \{9, 5\}, \{11, 6\}\} \\ S_{\mathcal{T}_0} &= (13, 12, 12, 8, 1) \end{aligned}$$

Since $v_{e_0} = 7 \in A_1$,

$$\begin{aligned} \Pi_{\mathcal{T}} &= \{\{7, 1\}, \{8, 2\}, \{10, 3\}, \{12, 4\}, \{9, 5\}, \{11, 6\}\} \\ S_{\mathcal{T}} &= (13, 12, 12, 8, 7, 1) \end{aligned}$$

For $i \in \{1, \cdots, m\}$, let

$$A'_i = \{\{v, \cdots, w\} \mid (v, \cdots, w) \in A_1 \times \cdots \times A_{i-1} \times A_{i+1} \times \cdots \times A_m\}.$$

Then we have

$$|\Pi_{\mathcal{T}} \cap A'_i| = \begin{cases} b_i & \text{if } i \ne 0 \\ b_0 + 1 & \text{if } i = 0 \end{cases}$$

Denote $P(A_0, A_1, \cdots, A_{m-1})$ be the set of paritions of $V \setminus \{M\}$ with the above condition. Now we can define a mapping $\mathcal{T} = (V, T) \mapsto (\Pi_{\mathcal{T}}, S_{\mathcal{T}})$ from the set of spanning trees of $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$ to $P(A_0, A_1, \cdots, A_{m-1}) \times \{M\} \times A_0^{b_0} \times A_1^{b_1} \times \cdots \times A_{m-1}^{b_{m-1}}$.

We can see that the above mapping $\mathcal{T} = (V, T) \mapsto (\Pi_{\mathcal{T}}, S_{\mathcal{T}})$ is an injection but not an surjection. For $\Pi \in P(A_0, A_1, \cdots, A_{m-1})$ and a mapping p from $[m-1] := \{1, 2, \cdots, m-1\}$ to Π, let

$$\begin{aligned} B_1 &= \{\{i, p(i)\} \mid 1 \leq i \leq m-1\}. \\ B_2 &= \{\{i, \pi\} \mid \pi \in \Pi \cap A_i'\}. \end{aligned}$$

Let $B(\Pi, p)$ be a bipartite graph between Π and $[m-1]$ whose edge set is $B_1 \cup B_2$. It is clear that for any $i \in [m-1]$, there exists a unique element $\pi \in \Pi$ such that $\{i, \pi\} \in B_1$ and for any $\pi \in \Pi$, there exists a unique element $i \in [m-1]$ such that $\{i, \pi\} \in B_2$. For $S \in \{M\} \times A_0^{b_0} \times A_1^{b_1} \times \cdots \times A_{m-1}^{b_{m-1}}$, let $p_{\Pi,S}$ be a mapping from $[m-1] = \{1, 2, \cdots, m-1\}$ to Π defined by $p_{\Pi,S}(i)$ is an element of Π containing $S_{(i,1)}$, that is, the first entry of S which is in A_i. Then we have the following lemma.

Lemma 5.1. *Let $\Pi \in P(A_0, A_1, \cdots, A_{m-1})$ and $S = (S_{(i,j)})_{(i,j) \in \Lambda}$ be such that $S_{(0,0)} = M$ and $S_{(i,j)} \in A_i$ for any $(i,j) \neq (0,0)$. Then $\Pi = \Pi_{\mathcal{T}}$, $S = S_{\mathcal{T}}$ for some spanning tree $\mathcal{T}$ of $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$ if and only if Π and S satisfy $B(\Pi, p_{\Pi,S})$ has no cycle.*

Example. For $A_0 = \{13, 12, 11, 10\}$, $A_1 = \{9, 8, 7\}$, $A_2 = \{6, 5, 4\}$ and $A_1 = \{3, 2, 1\}$, let $\Pi = \{\{9, 5, 1\}, \{10, 6, 2\}, \{11, 7, 3\}, \{12, 8, 4\}\} \in P(A_0, A_1, A_2, A_3)$. For a sequence $S = (13, 9, 5, 2)$, a bipartite graph $B(\Pi, p_{\Pi,S})$ has no cycle, so the pair (Π, S) is an image of a spanning tree of $K^{(m)}_{4,3,3,3}$. Indeed, a tree with edge set

$$\{\{13, 9, 5, 1\}, \{12, 8, 4, 2\}, \{10, 9, 6, 2\}, \{11, 7, 5, 3\}\}$$

is mapped to (Π, S). For a sequence $S = (13, 8, 5, 2)$, a graph $B(\Pi, p_{\Pi,S})$ has a cycle obtained by a sequence $2, \{10, 6, 2\}, 8, \{12, 8, 4\}$. Hence there exists no spanning tree whose image is (Π, S).

So the number of spanning trees of $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$ is equal to that of pairs (Π, S) such that $B(\Pi, p_{\Pi,S})$ has no cycle.

Lemma 5.2. *For each $\Pi \in P(A_0, A_1, \cdots, A_{m-1})$, the number of mapping p from $[m-1]$ to Π such that $B(\Pi, p)$ has no cycle is equal to $(b_m + 1)k^{m-2}$.*

From this lemma, we can see that the number of $S \in A_1^{b_1} \times A_2^{b_2} \times \cdots \times A_m^{b_m+1}$ such that $B(\Pi, p_{\Pi,S})$ has no cycle, equivalently (Π, S) is an image of a spanning tree of $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$, is equal to $(b_m + 1)k^{m-2}a_m^{b_m} \prod_{i=1}^{m-1} a_i^{b_i-1}$. Since

$$|P(A_0, A_1, \cdots, A_{m-1})| = \frac{\prod_{i=1}^{m-1} a_i!}{\prod_{i=1}^{m-1} b_i!} \times \frac{(a_m - 1)!}{(b_m + 1)!},$$

we can compute the number of spanning trees of $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$.

Theorem 5.3. *The number of spanning trees of $K^{(m)}_{a_0,a_1,\cdots,a_{m-1}}$ is equal to*

$$k^{m-2} \prod_{i=1}^{m} \left(a_i^{b_i-1} \frac{a_i!}{b_i!} \right).$$

References

[1] C. Godsil, G. Royle, Algebraic graph theory. Graduate Texts in Mathematics, 207. Springer-Verlag, New York, 2001.

[2] S. Hirschman, V. Reiner, Note on the Pfaffian matrix-tree theorem. Graphs Combin. 20 (2004), no. 1, 59–63.

[3] G. Masbaum, A. Vaintrob, A new matrix-tree theorem, Int. Math. Res. Not. 2002, no 27, 1397–1426.

[4] W. T. Tutte, Graph theory, With a foreword by C. St. J. A. Nash-Williams, Encyclopedia of Mathematics and its Applications, 21.

A CENTER OF THE GROTHENDIECK RING GREEN FUNCTOR

FUMIHITO ODA AND TOMOYUKI YOSHIDA

1. Introduction

This note is a preliminary draft of our research presented in our talk. It is well known that there exists an isomorphism of commutative rings between the evaluation $\zeta_A(\bullet)$ at the one point G-set $\bullet = G/G$ of the center ζ_A of a Green functor A for a finite group G over a commutative ring $\mathcal{O}$ and the center $Z(A(\Omega^2))$ of the evaluation $A(\Omega^2)$ at the G-set $\Omega^2 = \Omega \times \Omega$ of A, where $\Omega = \cup_{H \leq G} G/H$ (see [Bo97] 12.2.2). If A is the fixed point functor $FP_{\mathcal{O}}$, then the above isomorphism induces an isomorphism between the center of group ring $\mathcal{O}G$ and the center of the Hecke algebra $\mathrm{End}_{\mathcal{O}G}(\oplus_{H \leq G}(\mathrm{Ind}_H^G \mathcal{O}))$ used in [Yo83] (see [Bo97] 4.5.2). If A is the Burnside ring Green functor B, $Z(B(\Omega^2))$ is the center of the Mackey algebra $\mu_{\mathcal{O}}(G)$ (see [TW95]).

The Dress construction for a Green functor in terms of G-sets is as follows: let G^c denote the group G, on which G acts by conjugation. Then the Mackey functor A_{G^c} obtained from A by Dress construction has a natural structure of Green functor (see [Bo03a] for the details.) In particular $A_{G^c}(\bullet)$ is a ring. If A is $FP_{\mathcal{O}}$, then the ring $A_{G^c}(\bullet)$ is the center $Z(\mathcal{O}G)$ of $\mathcal{O}G$. If A is B for G over $\mathcal{O}$, then the ring $A_{G^c}(\bullet)$ is the crossed Burnside ring of G over $\mathcal{O}$ ([OY01],[Bo03a],[Bo03b],[OY04]). If A is the cohomology functor with trivial coefficients $\mathcal{O}$, then the ring $A_{G^c}(\bullet)$ is the Hochschild cohomology ring of G over $\mathcal{O}$ ([Bo03a]). If A is the Grothendieck ring of the representations for $\mathcal{O}G$, then the ring $A_{G^c}(\bullet)$ is the Grothendieck ring of the Drinfeld double $D(\mathcal{O}G)$ ([OY04]). There exists a morphism Z_A of Green functors from the commutant Green functor $C(A, G^c)$ of A in A_{G^c} to the center ζ_A of the Green functor A (Theorem 9.2 of [Bo03a]). This theorem provides in particular a natural ring homomorphism $Z_A(\bullet)$ from $C(A, G^c)(\bullet)$ to the center $\zeta_A(\bullet)$ of the category A-mod of left A-modules (Mackey functors M, endowed for any G-sets X and Y with $\mathcal{O}$-bilinear maps $A(X) \times M(Y) \to M(X \times Y)$ which are bifunctorial, associative, and unitarity in the sense of 2.2 of [Bo97]). If A is $FP_{\mathcal{O}}$, then $\zeta_A(\bullet)$ is the isomorphism of rings from $Z(\mathcal{O}G)$ to the center of the Heeck algebra we

mention above. If A is B, then $\zeta_A(\bullet)$ is the injective homomorphism of rings from the crossed Burnside ring to the center of the Mackey algebra (see [Bo03b] 4.3). So, a natural problem is to study $\zeta_A(\bullet)$ for a Green functor A.

It is well known that there is an isomorphism of algebras

$$\mathbb{C}R_{\mathbb{C}}(D(\mathbb{C}G)) \cong \prod_{g\in[G\backslash G^c]} Z(\mathbb{C}[C_G(g)])$$

[Wi96]. In Seattle conference in 1996, Yoshida pointed out that the center $\mathbb{C}\otimes Z(R_{\mathbb{C}}, G)$ of the span (or Mackey) category (see [Yo83] and [Yo85]) of the Grothendieck ring Green functor $R_{\mathbb{C}}$ for G over the field $\mathbb{C}$ of the complex numbers is very similar to the Grothendieck algebra $\mathbb{C}R_{\mathbb{C}}(D(\mathbb{C}G))$ of the Drinfeld double of the group algebra $\mathbb{C}G$. The first purpose of this note is to present the following result.

Theorem 2.15 *There is an algebra isomorphism*

$$Z(\mathcal{C}_{R_{\mathbb{C}}}) \longrightarrow \prod_{g\in[G\backslash G^c]} Z(\mathbb{C}[C_G(g)/\langle g\rangle]).$$

The second purpose of this note is to give an answer to the reason why $\mathbb{C}\otimes Z(R_{\mathbb{C}}, G) = Z(\mathcal{C}_{R_{\mathbb{C}}})$ is similar to $\mathbb{C}R_{\mathbb{C}}(D(\mathbb{C}G))$ and to the problem we mention above, for the Grothendieck ring Green functor R for G over $\mathbb{C}$.

Theorem 3.6 *There exists a homomorphism Z_R of Green functors from $C(R, G^c)$ to ζ_R. The homomorphism Z_R induces a commutative ring homomorphism f from the Grothendieck ring $R_{\mathbb{C}}(D(\mathbb{C}G))$ to the center $Z(R_{\mathbb{C}}(\Omega^2))$. Moreover f induces a homomorphism*

$$\prod_{g\in[G\backslash G^c]} Z(\mathbb{C}[C_G(g)]) \longrightarrow \prod_{g\in[G\backslash G^c]} Z(\mathbb{C}[C_G(g)/\langle g\rangle]).$$

2. Green functor R

2.1. The Grothendieck ring Green functor. Let k be a commutative ring and $R_k(G)$ denote the Grothendieck group of the category of finitely generated left kG-modules, for relations given by direct sum decompositions. Induction, restriction, and conjugation of modules endow R_k with a structure of Mackey functor, and the tensor product of k-modules gives a structure of Green functor on R_k for G over $\mathbb{Z}$. We recall that the corresponding Mackey functor in the sense of Dress is

defined for a finite G-set X by

$$R_k(X) = \left(\bigoplus_{x\in X} R_k(G_x)\right)^G := \left\{(v(x)) \in \bigoplus_{x\in X} R_k(G_x) \middle| {}^g(v(x)) = v(gx) \forall g \in G\right\},$$

where G_x is the stabilizer of x in G. If Y is another finite G-set, define a product map (see [Bo97] 2.2) $R_k(X) \times R_k(Y) \to R_k(X \times Y)$ in the following way : if $u = (u(x))_{x\in X} \in R_k(X)$ and $v = (v(y))_{y\in Y} \in R_k(Y)$, then the product $u \times v$ is defined by

$$(u \times v)(x, y) = r^{G_x}_{G_{x,y}}(u(x)) r^{G_y}_{G_{x,y}}(v(y)),$$

for $x \in X$ and $y \in Y$, where $G_{x,y} = G_x \cap G_y$. The identity element ε of R_k is the identity element of the ring $R_K(G) = R_k(\bullet)$. Then R_k is a Green functor in terms of G-sets (see [Bo97] 2.2).

2.2. Remark. Let X be a G-set and R_k the Green functor discussed above. Then any element $u = (u(x)) \in R_k(X)$ may be identified with a G-equivariant k-vector bundle on X (see [Wi96] Section 2).

2.3. The category $\mathcal{C}_A$. Let A be a Green functor for G over $\mathcal{O}$. Bouc introduced the category $\mathcal{C}_A$ (see [Bo97] 3.2) defined as follows:

- The object of $\mathcal{C}_A$ are the finite G-sets.
- If X and Y are G-sets, then

$$\mathrm{Hom}_{\mathcal{C}_A}(X, Y) = A(Y \times X)$$

- If X, Y, and Z are G-sets, if $a \in A(Y \times X) = \mathrm{Hom}_{\mathcal{C}_A}(X, Y)$ and if $a' \in A(Z \times Y) = \mathrm{Hom}_{\mathcal{C}_A}(Y, Z)$, then the composite morphism $a' \circ a \in \mathrm{Hom}_{\mathcal{C}_A}(X, Z)$ is defined by

$$a' \circ a = a' \circ_Y a := A_*\begin{pmatrix} x, y, z \\ \downarrow \\ x, z \end{pmatrix} A^*\begin{pmatrix} x, y, z \\ \downarrow \\ x, y, y, z \end{pmatrix}(a' \times a).$$

Lemma 2.4. *Let X, Y, and Z be G-sets. Let $b = (b(z, y_2))$ be an element of $R_k(Z \times Y)$ and $a = (a(y_1, x))$ an element of $R_k(Y \times X)$. Then we have the composition $b \circ a \in R_k(Z \times X)$ by*

$$(b \circ a)(z, x) = \bigoplus_{y\in Y} b(z, y) \otimes_k a(y, x)$$

as k-modules.

2.5. The character ring Green functor.

Let $\mathbb{C}$ be the field of the complex numbers and $C_{\mathbb{C}}(G)$ denote the character ring of a finite group G. Induction, restriction, and conjugation of characters endow $C_{\mathbb{C}}$ with a structure of Mackey functor, and

the product gives a structure of Green functor on $C_{\mathbb{C}}$ for G over $\mathbb{Z}$. We set

$$C_{\mathbb{C}}(X) = \left(\bigoplus_{x\in X} C_{\mathbb{C}}(G_x)\right)^G := \left\{(\alpha(x)) \in \bigoplus_{x\in X} R_k(G_x) \,\middle|\, {}^g(\alpha(x)) = \alpha(gx) \forall g \in G\right\}$$

for a finite G-set X. Then $C_{\mathbb{C}}$ is a Green functor in terms of G-sets (see 2.1).

Lemma 2.6. *Let X, Y, and Z be G-sets. Let $\beta = (\beta(z, y_1))$ be an element of $C_{\mathbb{C}}(Z \times Y)$ and $\alpha = (\alpha(y_2, z))$ an element of $C_{\mathbb{C}}(Y \times X)$. Then we have the composition $\beta \circ \alpha \in C_{\mathbb{C}}(Z \times X)$ by*

$$(\beta\circ\alpha)(z,x) = \sum_{y\in[G_z,x\backslash Y]} \mathrm{ind}_{G_{x,y,z}}^{G_{x,z}} \left(\mathrm{res}_{G_{x,y,z}}^{G_{y,z}}(\beta(z,y_1)) \cdot \mathrm{res}_{G_{x,y,z}}^{G_{y,x}}(\alpha(y_2,x))\right)$$

$$(\beta\circ\alpha)(z,x)(g) = \sum_{y\in Y^{<g>}} \beta(z,y)(g)\cdot\alpha(y,x)(g)$$

for $g \in G$.

2.7. The Hecke category. Yoshida introduced the Hecke category in [Yo83]. The *Hecke category* $\mathcal{H}_{kG}$ of G over a commutative ring k is the category in which objects are finite G-sets and a morphism of Y to X is a matrix $(\alpha_{xy})_{x\in X, y\in Y}$ of size $|X| \times |Y|$ with $\alpha_{gx,gy} = \alpha_{x,y} \in k$ for any $x \in X$, $y \in Y$, and $g \in G$. Compositions are defined by the product of matrices. The category $\mathcal{H}_{\mathcal{O}G}$ is self-dual (by the transpositions of matrices) and equivalent to the category $\mathcal{P}(kG)$ of permutation kG-modules and kG-homomorphims by the functor

$$\begin{aligned} X &\longmapsto kX, \\ ((\alpha_{x,y}) : Y \to X) &\longmapsto (kY \to kX; y \mapsto \sum_{x\in X} \alpha_{xy} y). \end{aligned}$$

If FP_k is the fixed point Green functor (see [Bo97] 4.5.2), then the category $\mathcal{P}(kG)$ may be identified with the category $\mathcal{C}_{FP_k}$.

2.8. The functor Ψ_t. If t is an element of G and X is a G-set, we set $\Psi_t(X) = \mathbb{C}X^{\langle t\rangle}$ and

$$\Psi_t\left((A(x,y))_{x\in X, y\in Y}\right) = \left(\mathrm{Tr}(A(x,y)(t))\right)_{x\in X^{\langle t\rangle}, y\in Y^{\langle t\rangle}},$$

where $\langle t\rangle$ is the cyclic group generated by t and $X^{\langle t\rangle}$ is the $\langle t\rangle$-fixed point in X, for $(A(x,y))_{x\in X, y\in Y} \in R_{\mathbb{C}}(XY)$. Let $(\alpha_{xy}) \in C_{\mathbb{C}}(XY)$ be the corresponding characters. Then we have

$$\Psi_t\left((A(x,y))_{x\in X, y\in Y}\right) = (\alpha_{xy}(t))_{x\in X^{\langle t\rangle}, y\in Y^{\langle t\rangle}}.$$

Lemma 2.9. *The correspondence* $\Psi_t : \mathcal{C}_{R_C} \to \mathcal{H}_{\mathbb{C}[C_G(t)/\langle t\rangle]}$ *is an additive functor.*

Lemma 2.10. *If* $s \in G$ *and* $t \in G$ *are conjugate in* G*, then there is a natural equivalence between* Ψ_s *and* Ψ_t*.*

We obtain an additive functor

$$\Psi := (\Psi_t)_{t\in[G^c]} : \mathcal{C}_{R_C} \longrightarrow \prod_{t\in[G^c]} \mathcal{H}(\mathcal{O}[C_G(t)/\langle t\rangle]),$$

where $[G\backslash G^c]$ is the set of representatives of G-conjugacy classes of G.

Theorem 2.11. *The functor* $\mathbb{C}\otimes_{\mathbb{Z}}\Psi$ *is a fully faithful of additive categories from* $\mathbb{C}\otimes_{\mathbb{Z}}\mathcal{C}_{R_C}$ *to* $\prod_{t\in[G\backslash G^c]}\mathcal{H}(\mathbb{C}[C_G(t)/\langle t\rangle])$*. In particular,*

$$\psi := (\psi_t) : \mathbb{C}\otimes_{\mathbb{Z}} R(X\times Y) \longrightarrow \bigoplus_{t\in[G\backslash G^c]} \mathrm{Hom}_{\mathbb{C}C_G(t)}\left(\mathbb{C}[X^{\langle t\rangle}], \mathbb{C}[Y^{\langle t\rangle}]\right)$$

in an isomorphism of $\mathbb{C}$*-modules.*

2.12. The center of the category. Let C be an additive category. The center $Z(C)$ of C is a collection $\mathrm{Nat}(Id_C, Id_C)$ of the endonatural transformations of the identity functor $Id_C : C \to C$. The center $Z(C)$ has a structure of commutative ring using the composite of natural transformation.

Lemma 2.13. *Let* k *be a commutative ring. Then the center* $Z(\mathcal{H}_{kG})$ *of the Hecke category of* G *and the center* $Z(kG)$ *of the group ring* kG *are isomorphic.*

Lemma 2.14. *Let* A *be a Green functor for* G *over a commutative ring* k*. Then*

$$Z(\mathcal{C}_A) \cong Z(A(\Omega^2)),$$

where $\Omega = \coprod_{H\leq G} G/H$*.*

Theorem 2.15. *There is an ring isomorphism*

$$Z\left(\mathcal{C}_{R_C}\right) \longrightarrow \prod_{t\in[G\backslash G^c]} Z\left(\mathbb{C}[C_G(g)/\langle g\rangle]\right).$$

3. The Dress construction

3.1. Crossed G-monoid. In [Bo03a], Bouc defined the crossed G-monoid as follows. A *crossed G-monoid* (Γ, φ) is a pair consisting of a finite monoid Γ with a left action of G by monoid automorphisms (denoted by $(g,\gamma)\mapsto g\gamma$ or $(g,\gamma)\mapsto {}^g\gamma$, for $g\in G$ and $\gamma\in\Gamma$), and a map of G-monoids φ from Γ to a G-set G^c with G-action defined by conjugation (i.e. a map φ which is both a map of monoids and a map of G-sets). In this note, we use only the crossed G-monoid $G^c = (G, Id)$.

Theorem 3.2. *(Bouc* [Bo03a] *5.1). Let A be a Green functor for G over a commutative ring $\mathcal{O}$, Γ a crossed G-monoid, and ε_A an element of $A(\bullet)$ such that for any G-set X and for any $a \in A(X)$*

$$A_*(p_X)(a \times \varepsilon_A) = a = A_*(q_X)(\varepsilon_A \times a)$$

denoting by p_x (resp. q_x) the bijective projection from $X \times \bullet$ (resp. from $\bullet \times X$) to X (see 1.2.1 of [Bo03a]*). Then the functor A_Γ is a Green functor for G over $\mathcal{O}$, with unit ε_{A_Γ}, where ε_{A_Γ} is the element $A_*\left(\begin{array}{c}\bullet\\ \downarrow \\ 1_G\end{array}\right)(\varepsilon_A)$ of $A(\Gamma) = A(\bullet)$.*

3.3. Commutant. Let A be a Green functor for G. If X and Y are finite G-sets, if $a \in A(X)$ and $b \in A(Y)$, set

$$a \times^{op} b = A_*\left(\begin{array}{c} y, x \\ \downarrow \\ x, y \end{array}\right)(b \times a) \in A(X \times Y).$$

If M is a Mackey subfunctor of A, define the *commutant* of M in A by

$$C_A(M)(X) = \{a \in A(X) | \forall Y, \forall m \in M(Y),\ a \times m = a \times^{op} m\}$$

The commutant of M in A is a Green subfunctor of A (see [Bo97] 6.5.7). A Green functor A is called *commutative* if $C_A(A)(X) = A(X)$ for a finite G-set X. In other words $a \times b = a \times^{op} b$ if $a \in A(X)$ and $b \in A(Y)$ for G-sets X, Y.

3.4. A split injective map ι. Let Γ be a crossed G-monoid. For any finite G-set X, denote by ι_X the map $A(X)$ to $A(X \times \Gamma) = A_\Gamma(X)$. Then Bouc showed that ι_X is a split injective map of $\mathcal{O}$-modules, and the maps ι_X define an injective morphism of Green functors from A to A_Γ (see [Bo03a] 5.10). We denote by $\iota(A)$ the Green subfunctor of A_Γ.

Lemma 3.5. *Let A be a commutative Green functor and Γ the trivial crossed G-monoid G^c. Let $C(A, \Gamma)$ be the commutant of $\iota(A)$ in A_Γ. Then $C(A, \Gamma)(\bullet) = A(\Gamma)$.*

Theorem 3.6. *There exists a homomorphism Z_R of Green functors from $C(R, G^c)$ to ζ_R. The homomorphism Z_R induces a commutative ring homomorphism f from the Grothendieck ring $R_{\mathbb{C}}(D(\mathbb{C}G))$ to the center $Z(R_{\mathbb{C}}(\Omega^2))$. Moreover f induces a homomorphism*

$$\prod_{g \in [G \backslash G^c]} Z(\mathbb{C}[C_G(g)]) \longrightarrow \prod_{g \in [G \backslash G^c]} Z(\mathbb{C}[C_G(g)/\langle g \rangle]).$$

REFERENCES

[Bo97] S. BOUC, *Green functors and G-sets*, Lecture Notes in Mathematics, vol. 1671, Springer, 1997.

[Bo00] S. BOUC, Burnside rings, In *Handbook of Algebra*, Vol. 2, Elsevier Science B.V. (2000), 439–804.

[Bo03a] S. BOUC, Hochschild constructions for Green functors, *Communications in Algebra*, **31** (2003), 419–453.

[Bo03b] S. BOUC, The p-blocks of the Mackey algebra, *Algebras and Representation Theory*, **6** (2003), 515–543.

[OY01] F. ODA AND T. YOSHIDA, Crossed Burnside rings I. The Fundamental Theorem, *J. Algebra* **236** (2001), 29–79.

[OY04] F. ODA AND T. YOSHIDA, Crossed Burnside rings II. The Dress construction of a Green functor, *J. Algebra* **282** (2004), 58–82.

[TW95] J. THÉVENAZ AND P. WEBB, The structure of Mackey functors, *Trans. Amer. Math. soc.* **347 (6)** (1995), 1865–1961.

[Wc00] P. WEBB, A guide to Mackey functor, In *Handbook of Algebra* Vol. 2, Elsevier Science B.V. (2000), 805–836.

[Wi96] S.J.WITHERSPOON, The representation ring of the quantum double of a finite group, *J. Algebra* **179** (1996), 305–329.

[Yo83] T. Yoshida, On G-functors (II) : Hecke operators and G-functors, *J. Math. Soc. Japan* **35**, No. 1, (1983), 179–190.

[Yo85] T. YOSHIDA, *Idempotents and transfer theorems of Burnside rings, character rings and span rings*, Algebraic and Topological Theories (to the memory of T. Miyata) (1985), 589-615.

[Yo87] T.Yoshida, Fisher's inequality for block desings with finite group action, *Journal of the Faculty of Science, Tokyo Univ.*, Sec. IA, **34** (1987), 513–544.

(F. Oda) DEPARTMENT OF LIBERAL ARTS, TOYAMA NATIONAL COLLEGE OF TECHNOLOGY, TOYAMA 939-8630, JAPAN

E-mail address: oda@toyama-nct.ac.jp

(T. Yoshida) DEPARTMENT OF MATHEMATICS, HOKKAIDO UNIVERSITY, SAPPORO 060-0810 , JAPAN

E-mail address: yoshidat@math.sci.hokudai.ac.jp

Isomorphisms and Homomorphisms of Graphs

BRIAN CURTIN
Department of Mathematics
University of South Florida
4202 E. Fowler Ave., PHY114
Tampa, FL 33620
bcurtin@math.usf.edu

We discuss the use of graph homomorphisms to determine the isomorphism class of a graph. In fact, we consider a more general problem which allows us to use some tools of invariant theory. As special case we see how graph homomorphisms can be used to decide graph isomorphism.

Throughout this note X shall denote a finite, non-empty set. Given a ring $\mathcal{R}$, we write $\mathcal{M}_X(\mathcal{R})$ to denote the set of matrices over $\mathcal{R}$ whose rows and columns are indexed by X. We shall study a matrix $W \in \mathcal{M}_X(\mathcal{R})$ by using various multi-digraphs $H = (V, E)$, where V and E are the vertex set and edge multi-set of H, respectively.

For $\phi : V \to X$, write

$$w_W(\phi) = \prod_{\{u,v\} \in E} W(\phi(u), \phi(v)).$$

In this setting, W is called the *Boltzmann weight matrix*, and the maps ϕ are called *states*. The *partition function of H with respect W* is

$$Z^W(H) = \sum_{\phi : V \to X} w_W(\phi).$$

Although they have their origins in physics (statistical mechanics), partition functions have applications and interpretations in discrete math, including the following.

- In studying ensemble of atoms such as the Ising and Potts models, where $Z^W(H)$ determines many properties of system. (See [1, 13])
- In producing graph invariants, such as the chromatic polynomial (see [5, 6]).
- In planar algebras, they provide a fundamental invariant (see [10]). Some combinatorial planar algebras are considered in [3].

- This is the construction of the actual link invariant from spin models for link invariants (see [9]).

We focus on their connection to graph homomorphisms (see [4]). Let $G = (X, R)$ be finite simple graph, and let A denote the adjacency matrix of G. A map $\phi : V \to X$ is a *graph homomorphism* whenever $(u, v) \in E$ implies $(\phi(u), \phi(v)) \in R$.

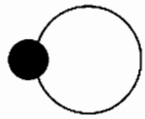
Theorem 1 *$Z^A(H)$ equals the number of graph homomorphisms from H into G.*

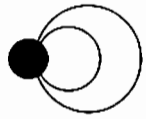
Proof. Summand is $w_A(\phi) = 1$ if each edge of H map to edges of G, and zero otherwise. □

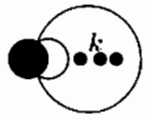
This gives a nice combinatorial interpretation of the partition function. We note that computing the number of graph homomorphisms from H into G is in general an NP-sharp problem, so computing partition functions is as well (see [8]).

We consider what can be deduced about a matrix W from $Z^W(H)$ as H varies. In the theory of graph homomorphism, one usually fixes H and considers graphs into which it maps. Here are a few examples.

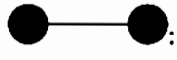
$H =$  : $Z^W(H) = |X|$

$H =$  : $Z^W(H) = \sum_{x \in X} W(x, x)$

$H =$  : $Z^W(H) = \sum_{x \in X} (W(x, x))^2$

$H =$ 

: $Z^W(H) = \sum_{x \in X} (W(x, x))^k$

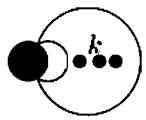
$H =$  : $Z^W(H) = \sum_{x,y \in X} W(x, y)$

$H =$ 

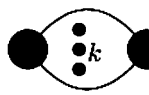
: $Z^W(H) = \sum_{x,y \in X} (W(x, y))^k$

To capture the process of computing the partition function generically, we introduce indeterminates $\lambda_{x,y}$ $(x, y \in X)$, and work in the ring of polynomials $\mathcal{L} = \mathbb{C}[\lambda_{x,y} \,|\, x, y \in X]$. Let $\Lambda \in \mathcal{M}_X(\mathcal{L})$ denote matrix (x,y)-entry $\lambda_{x,y}$. Observe that $Z^\Lambda(H)$ is a polynomial in $\mathcal{L}$. The polynomial $Z^\Lambda(H)$ describes how the partition function of H is computed as a function of the entries of a matrix.

Observe that we may evaluate $p \in \mathcal{L}$ over $\mathcal{M}_X(\mathbb{C})$ in the natural fashion, where $p(M)$ is given by setting $\lambda_{x,y} = M(x,y)$. Thus we may compute $Z^W(H)$ by evaluating $Z^\Lambda(H)$ at $\Lambda = W$. Let us consider the polynomials which arise from partition functions.

$H =$  $: Z^\Lambda(H) = \sum_{x \in X} \lambda_{x,x}^k$

Observe that these are the power symmetric functions in $\{\lambda_{x,x} | x \in X\}$.

$H =$  $: Z^\Lambda(H) = \sum_{x,y \in X} \lambda_{x,y}^k$

Observe that these are the power symmetric functions in $\{\lambda_{x,y} | x, y \in X\}$.

This symmetry noted above is a bit misleading, as it is in part due to the symmetry of the graphs H. We investigate the symmetry of the $Z^\Lambda(H)$. Write $\mathcal{S} = \mathrm{Sym}(X)$. Then $\sigma \in \mathcal{S}$ acts on $\mathcal{L}$ by $\sigma(\lambda_{x,y}) = \lambda_{\sigma^{-1}(x),\sigma^{-1}(y)}$. We consider the ring $\mathcal{L}^\mathcal{S}$ of polynomial invariants for $\mathcal{S}$ in $\mathcal{L}$.

Theorem 2 $Z^\Lambda(H) \in \mathcal{L}^\mathcal{S}$.

Proof. The sum defining $Z^\Lambda(H)$ runs over all $\phi : V \to X$. Permuting X only changes order of summands. □

Theorem 3 $\mathcal{L}^\mathcal{S}$ *is spanned by* $\{Z^\Lambda(H) \,|\, H =$ *multi-digraph*$\}$.

Proof. For $p \in \mathcal{L}^\mathcal{S}$, say one of the maximal degree monomials in p is (ignoring its coefficient) $m = \lambda_{x_1,y_1}^{k_1} \lambda_{x_2,y_2}^{k_2} \cdots \lambda_{x_n,y_n}^{k_n}$. Define $H = (V, E)$ by $V = \{x_i\}_{i=1}^n \cup \{y_i\}_{i=1}^n$, $E = \{(x_i, y_i) \times k_i\}_{i=1}^n$.

Since m is a maximal degree monomial in $Z^\Lambda(H)$, and for some scalar α, $Z^\Lambda(H) - \alpha \mathcal{S} \cdot m$ has fewer monomials with the same degree as m (and no new monomial terms were introduced in this process). By induction, we find that p is in span of the $Z^\Lambda(H)$. □

Note that $\sigma \in \mathcal{S}$ acts on $\mathcal{M}$ by $\sigma(M)(x,y) = M(\sigma(x),\sigma(y))$. For $W \in \mathcal{M}_X(\mathbb{C})$, write $\mathcal{S} \cdot W$ to denote the orbit of W. This set is just the set of matrices permutation equivalent to W.

Consider the polynomial equations $\{Z^\Lambda(H) = Z^W(H) | H \text{ multi-digraph}\}$. They define an affine variety (via their simultaneous zeros). These simultaneous zeros include $\mathcal{S} \cdot W$. In fact, the following result implies equality.

Lemma 4 *(See [2, 12]) Let $\mathcal{G}$ be a finite matrix group. Let $\mathcal{L}^\mathcal{G}$ be the ring of $\mathcal{G}$-invariants. Let $M \in \mathcal{M}_X(\mathbb{C})$. Then $\mathcal{G} \cdot M$ is the set of the simultaneous zeros of $\{p = p(M) \,|\, p \in \mathcal{L}^\mathcal{G}\}$.*

Proof. Take $M' \notin \mathcal{G} \cdot M$. Now $\mathcal{G} \cdot M'$ and $\mathcal{G} \cdot M$ are disjoint finite sets, so there is a polynomial $h \in \mathcal{L}$ s.t. $h(\sigma(M)) = 0$, $h(\sigma(M')) = 1$ for all $\sigma \in \mathcal{G}$. Now $f = \prod_{\sigma \in \mathcal{G}} \sigma(h) \in \mathcal{L}^\mathcal{G}$ is s.t. $f(M) = 0$, $f(M') = 1$. Thus M' is not a simultaneous zeros of $\{p = p(M) \,|\, p \in \mathcal{L}^\mathcal{G}\}$. □

With this we may state our main results.

Theorem 5 *The permutation equivalence class of a complex matrix W is uniquely determined by the invariants $Z^W(H)$ as H runs over all multi-digraphs.*

Proof. The partition function defines an affine variety via $\{Z^\Lambda(H) = Z^W(H) | H \text{ multi-digraph}\}$. By the previous lemma, this affine variety is exactly the permutation equivalence class of W. □

Theorem 6 *The isomorphism class of a simple finite graph G is uniquely determined by the number of homorphisms from H into G as H runs over all graphs.*

Using considerations of invariant theory ([11]), one can conclude that the multi-digraphs H may be assumed to be connected, and a (far too large a) bound on the number of edges of H deduced.

References

[1] R.J. Baxter, *Exactly solved models in statistical mechanics*, Academic Press, London-New York, 1982.

[2] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms, Springer, New York, 1992.

[3] B. Curtin, Some planar algebras related to graphs, *Pacific J. Math.*, **209** (2003), 231–248.

[4] G. Hahn and C. Tardif, Graph homomorphisms: structure and symmetry, *in* "Graph symmetry (Montreal, PQ, 1996)," 107–166, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 497, Kluwer Acad. Publ., Dordrecht, 1997.

[5] P. de la Harpe and F. Jaeger, Chromatic invariants for finite graphs: theme and polynomial variations. *Linear Algebra Appl.* **226/228** (1995), 687–722.

[6] P. de la Harpe and V.F.R. Jones, Graph invariants related to statistical mechanical models: examples and problems. *J. Combin. Theory Ser. B* **57** (1993), no. 2, 207–227.

[7] P. Hell, An introduction to the category of graphs, *in* "Topics in graph theory (New York, 1977)," pp. 120–136, Ann. New York Acad. Sci., 328, New York Acad. Sci., New York, 1979.

[8] P. Hell and J. Nešetřil, *On the complexity of H-coloring.* J. Combin. Theory Ser. B **48** (1990), 92–110.

[9] V.F.R. Jones, On knot invariants related to some statistical mechanical models, *Pacific J. Math.* **137** (1989), 311–224.

[10] V.F.R. Jones Planar algebras, I, *NZ J. Math*, to appear.

[11] E. Noether, Der Endlichkeitssatz der Invarianten endlicher Gruppen, *Math. Ann.* **77** (1916), 89–92.

[12] B. Sturmfels *Algorithms in invariant theory*, Springer-Verlag, Vienna, 1993.

[13] H.N.V. Temperley, *Lattice models in discrete statistical mechanics*, in *Applications of graph theory*, R.J. Wilson and L.W. Beineke, Eds. Academic Press, London-New York, 1979.

An Infinite Class of Non-Symmetric Spin Models, Potts Models, and Hadamard Matrices

TAKUYA IKUTA
Faculty of Law, Kobe Gakuin University, Arise, Ikawadani-cho, Nishi-ku, Kobe, 651-2180 Japan
ikuta@law.kobegakuin.ac.jp

Abstract. A spin model (for link invariants) is a square matrix W with non-zero complex entries which satisfies certain axioms. In [5] it was shown that ${}^tWW^{-1}$ is a permutation matrix (the order of this permutation matrix is called the "index" of W), and a general form was given for spin models of index 2. Moreover, new spin models, called non-symmetric Hadamard models, were constructed. In this paper, we consider certain spin models of index 4, and construct a new infinite class of spin models of index 4 which contains Potts models and Hadamard matrices. Moreover, these results are generalized to the cases of index $4g$ or $4g+2$ for $g \geq 1$.

1 Introduction

The notion of spin model was introduced by Vaughan Jones [6] to construct invariants of knots and links. A spin model is essentially defined by a square matrix W with nonzero entries which satisfies two conditions (type II and type III). Jones restricted his consideration to symmetric matrices. The notion of spin model was generalized to non-symmetric case by Kawagoe-Munemasa-Watatani [7], and it was further generalized by Bannai-Bannai [1].

In [5] Jaeger-Nomura proved that, for every spin model W, its transpose ${}^tW$ is obtained from W by permutation of rows, and called the order of this permutation "index" of W. Moreover, it was shown that every spin model of index 2 takes the following form:

$$W = \begin{pmatrix} A & A & B & -B \\ A & A & -B & B \\ -{}^tB & {}^tB & C & C \\ {}^tB & -{}^tB & C & C \end{pmatrix}, \tag{1}$$

where A, B, C are square matrices of equal sizes. Using this form, a new infinite class of spin models of inex 2, called the non-symmetric Hadamard models, was constructed.

In [10] Nomura classified spin models of the form (1) when A is a Potts model. Then, three spin models appear, that is, as the shape of B in the form (1), a Potts model, a Hadamard matrix, and a certain square matrix of size 4. This results play an important role in this paper.

Nomura and the author [3] determined the general form of spin models for any index m. By [3], if index 4, we obtain two kinds of the general form of spin models. We may regard one of them as a generalization of the from (1) of index 2. In fact, some type III equations of index 4 perfectly coincide with all type III equations of index 2.

In the present paper, using the results of [10] and [3], we consider a special general form of spin models of index 4, and construct a new infinite class of spin models of index 4 which contains Potts models and Hadamard matrices as like the non-symmetric Hadamard models. Moreover, we show that we can construct a more generalized infinite class of spin models of index $4g$ or $4g+2$ for $g \geq 1$.

Starting from a special general form of spin models of index 4, we can construct the following infinite class of spin models.

See Sections 2 for terminology.

Theorem 1.1. We put

$$W = \begin{array}{c} \\ X_0 \\ X_1 \\ X_2 \\ X_3 \end{array} \begin{array}{c} \begin{array}{cccc} X_0 & X_1 & X_2 & X_3 \end{array} \\ \begin{pmatrix} W_{00} & W_{01} & W_{02} & W_{03} \\ W_{10} & W_{00} & W_{12} & W_{02} \\ W_{12} & W_{01} & W_{00} & W_{01} \\ W_{30} & W_{12} & W_{10} & W_{00} \end{pmatrix} \end{array},$$

where,

$$W_{00} = \begin{pmatrix} A & A & A & A \\ A & A & A & A \\ A & A & A & A \\ A & A & A & A \end{pmatrix}.$$

$$W_{01} = \begin{pmatrix} \xi A & -\xi A & \xi A & -\xi A \\ -\xi A & \xi A & -\xi A & \xi A \\ \xi A & -\xi A & \xi A & -\xi A \\ -\xi A & \xi A & -\xi A & \xi A \end{pmatrix}, \quad W_{10} = \begin{pmatrix} -\xi A & \xi A & -\xi A & \xi A \\ \xi A & -\xi A & \xi A & -\xi A \\ -\xi A & \xi A & -\xi A & \xi A \\ \xi A & -\xi A & \xi A & -\xi A \end{pmatrix}.$$

$$W_{02} = \begin{pmatrix} \tau_1 H & \eta^3\tau_1 H & -\tau_1 H & \eta\tau_1 H \\ \eta\tau_1 H & \tau_1 H & \eta^3\tau_1 H & -\tau_1 H \\ -\tau_1 H & \eta\tau_1 H & \tau_1 H & \eta^3\tau_1 H \\ \eta^3\tau_1 H & -\tau_1 H & \eta\tau_1 H & \tau_1 H \end{pmatrix}, \quad W_{03} = \begin{pmatrix} \tau_2 H & \eta\tau_2 H & -\tau_2 H & \eta^3\tau_2 H \\ \eta^3\tau_2 H & \tau_2 H & \eta\tau_2 H & -\tau_2 H \\ -\tau_2 H & \eta^3\tau_2 H & \tau_2 H & \eta\tau_2 H \\ \eta\tau_2 H & -\tau_2 H & \eta^3\tau_2 H & \tau_2 H \end{pmatrix}.$$

$$W_{12} = \begin{pmatrix} \eta\tau_1 H & -\tau_1 H & \eta^3\tau_1 H & \tau_1 H \\ \tau_1 H & \eta\tau_1 H & -\tau_1 H & \eta^3\tau_1 H \\ \eta^3\tau_1 H & \tau_1 H & \eta\tau_1 H & -\tau_1 H \\ -\tau_1 H & \eta^3\tau_1 H & \tau_1 H & \eta\tau_1 H \end{pmatrix}, \quad W_{30} = \begin{pmatrix} \eta^3\tau_2 H & -\tau_2 H & \eta\tau_2 H & \tau_2 H \\ \tau_2 H & \eta^3\tau_2 H & -\tau_2 H & \eta\tau_2 H \\ \eta\tau_2 H & \tau_2 H & \eta^3\tau_2 H & -\tau_2 H \\ -\tau_2 H & \eta\tau_2 H & \tau_2 H & \eta^3\tau_2 H \end{pmatrix}.$$

A is a Potts model. H is a symmetric Hadamard matrix. $\tau_2 \in \{\tau_1, -\tau_1\}$, ${\tau_1}^{16} = \xi^4 = -1$. η is a primitive m-root of unity. Then, W is a spin model.

In Section 2, we review basic terminology for spin models, and describe some known facts concerning non-symmetric spin models. The proof of Theorem 1.1 will be given in Section 4. In Section 5, we give a generalized infinite class of spin models of Theorem 1.1.

2 Preliminaries

In this section, we give some basic materials concerning spin models. For more details the reader can refer to [2, 6, 4, 5].

Let X be a finite non-empty set with n elements. We denote by $Mat_X(\mathbb{C})$ the set of square matrices with complex entries whose rows and columns are indexed by X. For $W \in Mat_X(\mathbb{C})$ and $x, y \in X$, the (x, y)-entry of W is denoted by $W(x, y)$.

A *type II matrix* on X is a matrix $W \in Mat_X(\mathbb{C})$ with nonzero entries which satisfies the *type II condition*:

$$\sum_{x \in X} \frac{W(\alpha, x)}{W(\beta, x)} = n\delta_{\alpha,\beta} \qquad (\text{for all } a, b \in X). \tag{2}$$

Let $W^- \in Mat_X(\mathbb{C})$ be defined by $W^-(x, y) = W(y, x)^{-1}$. Then type II condition is written as $WW^- = nI$ (I denotes the identity matrix). Hence, if W is a type II matrix, then W is non-singular with $W^{-1} = n^{-1}W^-$. It is clear that W^{-1} and ${}^tW$ are also type II matrices.

A type II matrix W is called a *spin model* on X if W satisfies *type III condition*:

$$\sum_{x \in X} \frac{W(\alpha, x)W(\beta, x)}{W(\gamma, x)} = D\frac{W(\alpha, \beta)}{W(\alpha, \gamma)W(\gamma, \beta)} \qquad (\text{for all } \alpha, \beta, \gamma \in X) \tag{3}$$

for some nonzero complex number D. The number D is called the *loop variable* of W. Setting $\beta = \gamma$ in (3), $\sum_{x \in X} W(\alpha, x) = DW(\beta, \beta)^{-1}$ holds, so that the diagonal entries $W(\beta, \beta)$ is a constant, which is called the *modulus* of W.

We recall some results of [5] and [3] which we need in the proof of Theorem 1.1.

Let $W \in Mat_X(\mathbb{C})$ be a spin model. By [5] Proposition 2, ${}^tWW^{-1}$ is a permutation matrix. So, there is a permutation σ of X such that ${}^tW(x, y) = W(\sigma(x), y)$ for all $x, y \in X$. The order of σ is called the *index* of W.

By [5] Proposition 7, when W has index m, there is a partition $X = X_0 \cup \cdots \cup X_{m-1}$ such that (for all $i, j \in \{0, \ldots, m-1\}$)

$$W(x, y) = \eta^{i-j}W(y, x) \quad (\text{for all } x \in X_i, y \in X_j). \tag{4}$$

where η denotes a primitive m-root of unity.

By [5], when W has index 2, X can be ordered and split into 4 blocks Y_1, Y_2, Y_3, Y_4 of equal sizes, so that W takes the following form:

$$W = \begin{array}{c} \\ Y_1 \\ Y_2 \\ Y_3 \\ Y_4 \end{array} \begin{array}{c} \begin{array}{cccc} Y_1 & Y_2 & Y_3 & Y_4 \end{array} \\ \begin{pmatrix} A & A & B & -B \\ A & A & -B & B \\ -{}^tB & {}^tB & C & C \\ {}^tB & -{}^tB & C & C \end{pmatrix} \end{array} \qquad \text{with } A, C \text{ symmetric.} \tag{5}$$

We may regard Y_i $(i = 1, 2, 3, 4)$ as copies of a set Y, and A, B, C as matrices in $Mat_Y(\mathbb{C})$.

Now let W be any matrix of the form (5). By [5] Proposition 8, W is a spin model with loop variable $2D$, where $D^2 = |Y|$, if and only if the following (i), (ii) hold.

(i) A, C are spin models with loop variable D and B is a type II matrix.

(ii) The following identities hold for all α, β, γ in Y:

$$\sum_{y \in Y} \frac{A(\alpha, y)B(y, \beta)}{B(y, \gamma)} = D\frac{B(\alpha, \beta)}{C(\beta, \gamma)B(\alpha, \gamma)}, \tag{6}$$

$$\sum_{y \in Y} \frac{C(\alpha, y)B(\beta, y)}{B(\gamma, y)} = D\frac{B(\beta, \alpha)}{A(\beta, \gamma)B(\gamma, \alpha)}, \tag{7}$$

$$\sum_{y \in Y} \frac{B(y, \beta)B(y, \gamma)}{A(\alpha, y)} = -D\frac{C(\beta, \gamma)}{B(\alpha, \beta)B(\alpha, \gamma)}, \tag{8}$$

$$\sum_{y \in Y} \frac{B(\beta, y)B(\gamma, y)}{C(\alpha, y)} = -D\frac{A(\beta, \gamma)}{B(\beta, \alpha)B(\gamma, \alpha)}. \tag{9}$$

A *Potts model* takes the form $aI + b(J - I)$ for some constants a, b, where I denotes the identity and J the all 1's matrix. It is known that $a = -u^3$, $b = u^{-1}$ for some complex number u satisfying $-u^2 - u^{-2} = D$, where D denotes the loop variable.

A non-symmetric *Hadamard model* takes the form (5) with $A = C$ a Potts model and $B = \xi H$, where H is a Hadamard matrix (i.e., a type II matrix with entries ± 1) and $\xi^4 = -1$.

In [10] Nomura classified spin models of the form (5) when A is a Potts model. The following result is due to [10].

Theorem 2.1. Let W be a spin model having the form (1) with A a Potts model. We get $A = C$. Then B is equivalent to at least one of the followings:

(i) $B = \xi H$ (H is a Hadamard matrix, $\xi^4 = -1$), that is, W is the non-symmetric Hadamard model.

(ii) $B = \xi A$, that is,

$$W = \begin{pmatrix} 1 & 1 & \xi & -\xi \\ 1 & 1 & -\xi & \xi \\ -\xi & \xi & 1 & 1 \\ \xi & -\xi & 1 & 1 \end{pmatrix} \otimes A, \qquad \text{where } \xi^4 = -1.$$

(iii)

$$B = \begin{pmatrix} r & r & ir^{-1} & -ir^{-1} \\ r & r & -ir^{-1} & ir^{-1} \\ ir^{-1} & -ir^{-1} & r & r \\ -ir^{-1} & ir^{-1} & r & r \end{pmatrix},$$

where r is an arbitrary nonzero complex number, and $i^2 = -1$.

By [3] Proposition 6.2, we consider a special form of spin models of index m. X can be ordered and split into m blocks $X_0, X_1, \ldots, X_{m-1}$ with the same size. The (X_i, X_j)-block of W is given by

$$W|_{X_i \times X_j} = S_{ij} \otimes T_{ij} \qquad (i, j = 0, 1, \ldots, m-1). \tag{10}$$

and

$$S_{ij}(\ell, \ell') = \eta^{-(\ell-\ell')(i-j)} \qquad (\ell, \ell' = 0, \ldots, m-1). \tag{11}$$

The matrices $T_{ij} \in Mat_Y(\mathbb{C})$ are type II matrices. Y is a subset of X with size $r = n/(m^2)$. Moreover the following equation holds for all i_1, i_2, $i_3 \in \{0, \ldots, m-1\}$ and for all α_1, α_2, $\alpha_3 \in Y$:

$$\sum_{y \in Y} \frac{T_{i_1,i}(\alpha, y) T_{i_2,i}(\beta, y)}{T_{i_3,i}(\gamma, y)} = D \frac{T_{i_1,i_2}(\alpha, \beta)}{T_{i_1,i_3}(\alpha, c) T_{i_3,i_2}(\gamma, \beta)}, \tag{12}$$

where i denotes the integer in $\{0, \ldots, m-1\}$ such that $i \equiv i_1 + i_2 - i_3 \pmod m$. $D^2 = r$.

3 Spin models of index 4

In the present section, based on the results in Section 2, we consider a special form of spin models of index 4. By (10) and (11), we get the following general form of spin models of index 4.

$$W = \begin{array}{c} \\ X_0 \\ X_1 \\ X_2 \\ X_3 \end{array} \begin{array}{c} \begin{array}{cccc} X_0 & X_1 & X_2 & X_3 \end{array} \\ \begin{pmatrix} W_{00} & W_{01} & W_{02} & W_{03} \\ W_{10} & W_{11} & W_{12} & W_{13} \\ W_{20} & W_{21} & W_{22} & W_{23} \\ W_{30} & W_{31} & W_{32} & W_{33} \end{pmatrix} \end{array}. \tag{13}$$

We denote ℓ the integer in $\{0, 1, 2, 3\}$. We regard the integers $\ell+1, \ell+2, \ell+3$ as mod 4. The shapes of W_{ij} $(i, j \in \{0, 1, 2, 3\})$ are calculated by

$$W_{\ell,\ell} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \otimes T_{\ell,\ell}, \quad W_{\ell,\ell+1} = \begin{pmatrix} 1 & \eta^3 & -1 & \eta \\ \eta & 1 & \eta^3 & -1 \\ -1 & \eta & 1 & \eta^3 \\ \eta^3 & -1 & \eta & 1 \end{pmatrix} \otimes T_{\ell,\ell+1},$$

$$W_{\ell,\ell+2} = \begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix} \otimes T_{\ell,\ell+2}, \quad W_{\ell,\ell+3} = \begin{pmatrix} 1 & \eta & -1 & \eta^3 \\ \eta^3 & 1 & \eta & -1 \\ -1 & \eta^3 & 1 & \eta \\ \eta & -1 & \eta^3 & 1 \end{pmatrix} \otimes T_{\ell,\ell+3},$$

where η denotes a primitive m-root of unity. $T_{ij} \in Mat_Y(\mathbb{C})$.

Using (4), for $j > i$, T_{ji} is given by T_{ij} as the followings:

$$T_{10} = \eta\, {}^tT_{01},\ T_{21} = \eta\, {}^tT_{12},\ T_{32} = \eta\, {}^tT_{23},\ T_{20} = -{}^tT_{02},\ T_{31} = -{}^tT_{13},\ T_{30} = \eta^3\, {}^tT_{03}. \tag{14}$$

Now let W be any matrix of the form (13). By (12), we have the $4^3 (= 64)$ type III equations with respect to the integers i_1, i_2, i_3 in $\{0, 1, 2, 3\}$. We denote the integer i in $\{0, 1, 2, 3\}$ such that $i \equiv i_1 + i_2 - i_3 \pmod 4$ as the symbol $[i_1, i_2, i_3][i]$. W is a spin model with loop variable $4D$, where $D^2 = |Y|$, if and only if the following (i), (ii) hold.

(i) T_{ij} are a type II matrix.

(ii) the 64 type III identities with respect to i_1, i_2, and i_3 hold for all α, β, γ in Y.

By $[0,0,0][0]$, $[1,1,1,][1]$, $[2,2,2][2]$, $[3,3,3][3]$, T_{00}, T_{11}, T_{22}, and T_{33} are symmetric spin models.

4 Proof of Theorem 1.1

We take notice of the type III equations with respect to $\{T_{00}, T_{02}, T_{22}\}$ among the 64 equations. Then, $[0,0,2][2]$, $[0,2,0][2](=[2,0,0][2])$, $[0,2,2][0](=[2,0,2][0])$, $[2,2,0][0]$ are the same as the type III equations (6), (7), (8), and (9) which appear in spin models of index 2. By Theorem 2.1, T_{02} is one of the followings:

$$T_{02} = \begin{cases} \xi A & (A \text{ is a Potts model, } \xi^4 = -1), \\ \xi H & (H \text{ is a Hadamard matrix, } \xi^4 = -1), \\ \text{the matrix of size } 4 \times 4. \end{cases}$$

Similarly, we take notice of the type III equations with respect to $\{T_{11}, T_{13}, T_{33}\}$ among the 64 equations. Then, $[1,1,3][3]$, $[1,3,1][3](=[3,1,1][3])$, $[1,3,3][1](=[3,1,3][1])$, $[3,3,1][1]$ are the same as the type III equations (6), (7), (8), and (9) which appear in spin models of index 2. By Theorem 2.1, T_{13} is one of the followings:

$$T_{13} = \begin{cases} \xi A & (A \text{ is a Potts model, } \xi^4 = -1), \\ \xi H & (H \text{ is a Hadamard matrix, } \xi^4 = -1), \\ \text{the matrix of size } 4 \times 4. \end{cases}$$

We put T_{00}, T_{11}, T_{22}, and T_{33} a Potts model A, that is,

$$T_{00} = T_{11} = T_{22} = T_{33} = A.$$

If we take $T_{02} = T_{13} = \xi H$, then we can not construct a spin model. So, we put $T_{02} = T_{13} = \xi A$.

Then, by [10] Lemma 4.2, when T_{ii} is a Potts model, the following type III equations ($i, j \in \{0,1,2,3\}$)

$$\sum_{y \in Y} \frac{T_{ii}(\alpha, y) T_{ij}(y, \beta)}{T_{ij}(y, \gamma)} = D \frac{T_{ij}(\alpha, \beta)}{T_{ij}(\alpha, \gamma) T_{jj}(\gamma, \beta)}.$$

automatically holds for any type II matrices T_{ij}. Therefore, the 16 type III equations $[0,1,0][1]$, $[0,1,1][0]$, $[0,3,0][3]$, $[0,3,3][0]$, $[1,0,0][1]$, $[1,0,1][0]$, $[1,2,1][2]$, $[1,2,2][1]$, $[2,1,1][2]$, $[2,1,2][1]$, $[2,3,2][3]$, $[2,3,3][2]$, $[3,0,0][3]$, $[3,0,3][0]$, $[3,2,2][3]$, $[3,2,3][2]$ hold.

We assume that

$$T_{01} = T_{12} = T_{23} = \tau_1 H, \quad T_{03} = \tau_2 H. \tag{15}$$

H is a Hadamard matrix.

Calcutating the remaing $32(= 64 - 4 - 6 - 6 - 16)$ type III equations using the condition (15), we get the followings:

$$[0,0,1][3] \qquad \eta\xi^{-1}\tau_1{}^2\tau_2{}^2 \sum_{y\in Y} \frac{H(\alpha,y)H(\beta,y)}{A(\gamma,y)} = D\frac{A(\alpha,\beta)}{H(\alpha,\gamma)H(\beta,\gamma)},$$

$$[0,0,3][1] \qquad \eta\xi^{-1}\tau_1{}^2\tau_2{}^2 \sum_{y\in Y} \frac{H(\alpha,y)H(\beta,y)}{A(y,\gamma)} = D\frac{A(\alpha,\beta)}{H(\alpha,\gamma)H(\beta,\gamma)},$$

$$[0,1,2][3] \qquad \eta\xi^{2}\tau_1{}^{-1}\tau_2 \sum_{y\in Y} \frac{H(\alpha,y)A(\beta,y)}{H(\gamma,y)} = D\frac{H(\alpha,\beta)}{A(\alpha,\gamma)H(\beta,\gamma)},$$

$$[0,1,3][2] \qquad \eta\xi^{2}\tau_1{}^{-1}\tau_2 \sum_{y\in Y} \frac{A(\alpha,y)H(\beta,y)}{H(y,\gamma)} = D\frac{H(\alpha,\beta)}{H(\alpha,\gamma)A(\beta,\gamma)},$$

$$[0,2,1][1] \qquad \eta\xi^{-1}\tau_1{}^{4} \sum_{y\in Y} \frac{H(\alpha,y)H(y,\beta)}{A(\gamma,y)} = D\frac{A(\alpha,\beta)}{H(\alpha,\gamma)H(\gamma,\beta)},$$

$$[0,2,3][3] \qquad \eta\xi^{-1}\tau_1{}^2\tau_2{}^2 \sum_{y\in Y} \frac{H(\alpha,y)H(\beta,y)}{A(\gamma,y)} = D\frac{A(\alpha,\beta)}{H(\alpha,\gamma)H(\beta,\gamma)},$$

$$[0,3,1][2] \qquad \eta\xi^{2}\tau_1\tau_2{}^{-1} \sum_{y\in Y} \frac{A(\alpha,y)H(y,\beta)}{H(\gamma,y)} = D\frac{H(\alpha,\beta)}{H(\alpha,\gamma)A(\gamma,\beta)},$$

$$[0,3,2][1] \qquad \eta\xi^{2}\tau_1\tau_2{}^{-1} \sum_{y\in Y} \frac{H(\alpha,y)A(y,\beta)}{H(y,\gamma)} = D\frac{H(\alpha,\beta)}{A(\alpha,\gamma)H(\gamma,\beta)},$$

$$[1,0,2][3] \qquad \eta\xi^{2}\tau_1{}^{-1}\tau_2 \sum_{y\in Y} \frac{A(\alpha,y)H(\beta,y)}{H(\gamma,y)} = D\frac{H(\beta,\alpha)}{H(\alpha,\gamma)A(\beta,\gamma)},$$

$$[1,0,3][2] \qquad \eta\xi^{2}\tau_1{}^{-1}\tau_2 \sum_{y\in Y} \frac{H(\alpha,y)A(\beta,y)}{H(y,\gamma)} = D\frac{H(\beta,\alpha)}{A(\alpha,\gamma)H(\beta,\gamma)},$$

$$[1,1,0][2] \qquad \eta\xi^{-1}\tau_1^{4} \sum_{y\in Y} \frac{H(\alpha,y)H(\beta,y)}{A(\gamma,y)} = D\frac{A(\alpha,\beta)}{H(\gamma,\alpha)H(\gamma,\beta)},$$

$$[1,1,2][0] \qquad \eta\xi^{-1}\tau_1^{4} \sum_{y\in Y} \frac{H(y,\alpha)H(y,\beta)}{A(y,\gamma)} = D\frac{A(\alpha,\beta)}{H(\alpha,\gamma)H(\beta,\gamma)},$$

$$[1,2,0][3] \qquad \eta\xi^{2}\tau_1\tau_2{}^{-1} \sum_{y\in Y} \frac{A(\alpha,y)H(\beta,y)}{H(\gamma,y)} = D\frac{H(\alpha,\beta)}{H(\gamma,\alpha)A(\gamma,\beta)},$$

$$[1,2,3][0] \qquad \eta\xi^{2}\tau_1\tau_2{}^{-1} \sum_{y\in Y} \frac{H(y,\alpha)A(y,\beta)}{H(y,\gamma)} = D\frac{H(\alpha,\beta)}{A(\alpha,\gamma)H(\beta,\gamma)},$$

$$[1,3,0][0] \qquad \eta\xi^{-1}\tau_1{}^2\tau_2{}^2 \sum_{y\in Y} \frac{H(y,\alpha)H(y,\beta)}{A(\gamma,y)} = D\frac{A(\alpha,\beta)}{H(\gamma,\alpha)H(\gamma,\beta)},$$

$$[1,3,2][2] \qquad \eta\xi^{-1}\tau_1{}^{4} \sum_{y\in Y} \frac{H(\alpha,y)H(y,\beta)}{A(\gamma,y)} = D\frac{A(\alpha,\beta)}{H(\alpha,\gamma)H(\gamma,\beta)},$$

$$[2,0,1][1] \qquad \eta\xi^{-1}\tau_1{}^{4} \sum_{y\in Y} \frac{H(y,\alpha)H(\beta,y)}{A(\gamma,y)} = D\frac{A(\beta,\alpha)}{H(\gamma,\alpha)H(\beta,\gamma)},$$

$$[2,0,3][3] \qquad \eta\xi^{-1}\tau_1{}^2\tau_2{}^2 \sum_{y\in Y} \frac{H(\alpha,y)H(\beta,y)}{A(\gamma,y)} = D\frac{A(\beta,\alpha)}{H(\alpha,\gamma)H(\beta,\gamma)},$$

$$[2,1,0][3] \qquad \eta\xi^{2}\tau_1\tau_2{}^{-1} \sum_{y\in Y} \frac{H(\alpha,y)A(\beta,y)}{H(\gamma,y)} = D\frac{H(\beta,\alpha)}{A(\gamma,\alpha)H(\gamma,\beta)},$$

$$[2,1,3][0] \qquad \eta\xi^{2}\tau_1\tau_2{}^{-1} \sum_{y\in Y} \frac{A(y,\alpha)H(y,\beta)}{H(y,\gamma)} = D\frac{H(\beta,\alpha)}{H(\alpha,\gamma)A(\beta,\gamma)},$$

$$[2,2,1][3] \qquad \eta\xi^{-1}\tau_1^{-1}\sum_{y\in Y}\frac{H(\alpha,y)H(\beta,y)}{A(\gamma,y)} = D\frac{A(\alpha,\beta)}{H(\gamma,\alpha)H(\gamma,\beta)},$$

$$[2,2,3][1] \qquad \eta\xi^{-1}\tau_1^{-1}\sum_{y\in Y}\frac{H(y,\alpha)H(y,\beta)}{A(y,\gamma)} = D\frac{A(\alpha,\beta)}{H(\alpha,\gamma)H(\beta,\gamma)},$$

$$[2,3,0][1] \qquad \eta\xi^{2}\tau_1^{-1}\tau_2\sum_{y\in Y}\frac{H(y,\alpha)A(y,\beta)}{H(\gamma,y)} = D\frac{H(\alpha,\beta)}{A(\gamma,\alpha)H(\gamma,\beta)},$$

$$[2,3,1][0] \qquad \eta\xi^{2}\tau_1^{-1}\tau_2\sum_{y\in Y}\frac{A(y,\alpha)H(y,\beta)}{H(y,\gamma)} = D\frac{H(\alpha,\beta)}{H(\gamma,\alpha)A(\gamma,\beta)},$$

$$[3,0,1][2] \qquad \eta\xi^{2}\tau_1^{-1}\tau_2\sum_{y\in Y}\frac{H(y,\alpha)A(\beta,y)}{H(\gamma,y)} = D\frac{H(\beta,\alpha)}{A(\gamma,\alpha)H(\beta,\gamma)},$$

$$[3,0,2][1] \qquad \eta\xi^{2}\tau_1^{-1}\tau_2\sum_{y\in Y}\frac{A(y,\alpha)H(\beta,y)}{H(y,\gamma)} = D\frac{H(\beta,\alpha)}{H(\gamma,\alpha)A(\beta,\gamma)},$$

$$[3,1,0][0] \qquad \eta\xi^{-1}\tau_1^{2}\tau_2^{2}\sum_{y\in Y}\frac{H(y,\alpha)H(y,\beta)}{A(\gamma,y)} = D\frac{A(\beta,\alpha)}{H(\gamma,\alpha)H(\gamma,\beta)},$$

$$[3,1,2][2] \qquad \eta\xi^{-1}\tau_1^{-1}\sum_{y\in Y}\frac{H(y,\alpha)H(\beta,y)}{A(\gamma,y)} = D\frac{A(\beta,\alpha)}{H(\gamma,\alpha)H(\beta,\gamma)},$$

$$[3,2,0][1] \qquad \eta\xi^{2}\tau_1^{-1}\tau_2\sum_{y\in Y}\frac{A(y,\alpha)H(y,\beta)}{H(\gamma,y)} = D\frac{H(\beta,\alpha)}{H(\gamma,\alpha)A(\gamma,\beta)},$$

$$[3,2,1][0] \qquad \eta\xi^{2}\tau_1^{-1}\tau_2\sum_{y\in Y}\frac{H(y,\alpha)A(y,\beta)}{H(y,\gamma)} = D\frac{H(\beta,\alpha)}{A(\gamma,\alpha)H(\gamma,\beta)},$$

$$[3,3,0][0] \qquad \eta\xi^{-1}\tau_1^{2}\tau_2^{2}\sum_{y\in Y}\frac{H(y,\alpha)H(y,\beta)}{A(\gamma,y)} = D\frac{A(\alpha,\beta)}{H(\gamma,\alpha)H(\gamma,\beta)},$$

$$[3,3,2][0] \qquad \eta\xi^{-1}\tau_1^{2}\tau_2^{2}\sum_{y\in Y}\frac{H(y,\alpha)H(y,\beta)}{A(y,\gamma)} = D\frac{A(\alpha,\beta)}{H(\gamma,\alpha)H(\gamma,\beta)}.$$

We want to return these equations to (6), (7), (8), and (9). The coefficients of the left hand side of the above equations are

$$\eta\xi^{-1}\tau_1^{2}\tau_2^{2}, \quad \eta\xi^{2}\tau_1^{-1}\tau_2, \quad \eta\xi^{-1}\tau_1^{-1}, \quad \eta\xi^{2}\tau_1\tau_2^{-1}.$$

We assume that these values are 1. Then, we get

$$\tau_2 = \eta\xi^{2}\tau_1, \qquad \tau_1^{4} = \eta^{-1}\xi.$$

Since the left hand sides of $[1,0,2][3]$ and $[1,2,0][3]$ are equal, we get

$$\begin{aligned}\frac{H(\beta,\alpha)}{H(\alpha,\gamma)} &= \frac{H(\alpha,\beta)}{H(\gamma,\alpha)},\\ H(\alpha,\beta)H(\alpha,\gamma) &= H(\beta,\alpha)H(\gamma,\alpha).\end{aligned}$$

Since this equation holds for any $\alpha,\beta,\gamma \in Y$, we put

$$H(y,\beta)H(y,\gamma) = H(\beta,y)H(\gamma,y) \quad \text{for any } y \in Y.$$

Exchanging γ and α, we get

$$\begin{aligned}H(y,\beta)H(y,\alpha) &= H(\beta,y)H(\alpha,y),\\ H(\beta,y) &= \frac{H(\alpha,y)}{H(y,\alpha)}H(\beta,y).\end{aligned}$$

The left hand side of $[0,2,1][1]$, since the coefficient is 1, we get

$$\begin{aligned}\sum_{y\in Y}\frac{H(\alpha,y)}{A(\gamma,y)}\cdot\frac{H(\alpha,y)}{H(y,\alpha)}H(\beta,y) &= \sum_{y\in Y}\frac{H(y,\alpha)H(\beta,y)}{A(\gamma,y)}\\ &= \frac{H(\gamma,\alpha)H(\beta,\gamma)}{-u^3}+u\sum_{y\in Y-\{\gamma\}}H(y,\alpha)H(\beta,y)\\ &= -\frac{H(\gamma,\alpha)H(\beta,\gamma)}{u^3}+u\Big(\sum_{y\in Y}H(y,\alpha)H(\beta,y)-H(\gamma,\alpha)H(\beta,\gamma)\Big)\\ &= -(u^{-3}+u)H(\gamma,\alpha)H(\beta,\gamma)+u\sum_{y\in Y}H(y,\alpha)H(\beta,y).\end{aligned}$$

If $\alpha=\beta$, the left hand side of $[0,2,1][1]$ is

$$(1+u^4)uH(\alpha,\gamma)H(\gamma,\alpha).$$

Using $D=-u^2-u^{-2}$, we get

$$u\sum_{y\in Y}H(\alpha,y)H(y,\alpha)=-\frac{(1+u^4)^2}{u^3}H(\alpha,\gamma)H(\gamma,\alpha).$$

From the definition of Hadamard matrix, we know

$$\sum_{y\in Y}H(\alpha,y)H(y,\alpha)=n.$$

Therefore, we get $H(\alpha,\gamma)H(\gamma,\alpha)=1$. H is a symmetric Hadamard matrix.

5 A generalized infinite class of spin models of Theorem 1.1

In this section, we give a generealized infinite class of spin models in Theorem 1.1. We only treat a special general form of spin models mentioned in Section 2.

Theorem 5.1. Let W be a general form of (10) and (11) with $m=4g$ $(g\geq 1)$. For $i,j\in\{0,1,\ldots,4g-1\}$ and $i>j$, we put

$$T_{ij}=\begin{cases}a_{j-i}A & \text{if } |i-j|=\text{even},\\ a_{j-i}H & \text{if } |i-j|=\text{odd}.\end{cases}$$

A is a Potts model and H is a symmetric Hadamard matrix.

Then, we can construct a infinite class of spin models with

$$a_i=\eta^{\frac{i(i-1)}{2}}{a_1}^{i^2},\qquad {a_1}^{16g^2}=-1,$$

where $\eta=\exp(2\pi\sqrt{-1}/(4g))$.

Theorem 5.2. Let W be a general form of (10) and (11) with $m=4g+2$ $(g\geq 1)$. For $i,j\in\{0,1,\ldots,4g+1\}$ and $i>j$, we put

$$T_{ij}=\begin{cases}a_{j-i}H & \text{if } |i-j|=\text{even},\\ a_{j-i}A & \text{if } |i-j|=\text{odd}.\end{cases}$$

A is a Potts model and H is a symmetric Hadamard matrix.

Then, we can construct a infinite class of spin models with

$$a_i=\eta^{\frac{i(i-1)}{2}}{a_1}^{i^2},\qquad {a_1}^{4(2g+1)^2}=-1.$$

where $\eta=\exp(2\pi\sqrt{-1}/(4g+2))$.

References

[1] E. Bannai and Et. Bannai, *Generalized generalized spin models (four-weight spin models)*, Pac. J. Math. **170** (1995), 1–16.

[2] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin/Cummings, Menlo Park, 1984.

[3] T. Ikuta and K. Nomura, *General Form of Non-Symmetric Spin Models*, J. Alg. Combin. **12** (2000), 59–72.

[4] F. Jaeger, M. Matsumoto, and K. Nomura, *Bose-Mesner algebras related to type II matrices and spin models*, J. Alg. Combin. **8** (1998), 39–72.

[5] F. Jaeger and K. Nomura, *Symmetric versus non-symmetric spin models for link invariants*, J. Alg. Combin. **10** (1999), 241–278.

[6] V.F.R. Jones, *On knot invariants related to some statistical mechanical models*, *Pac. J. Math.* **137** (1989), 311–336.

[7] K. Kawagoe, A. Munemasa, and Y. Watatani, *Generalized spin models*, J. of Knot Th. and its Ramific. **3** (1994), 465–475.

[8] K. Nomura, *Spin models constructed from Hadamard matrices*, J. Combin. Th. (A) **68** (1994), 251–261.

[9] K. Nomura, *An algebra associated with a spin model*, J. Alg. Combin. **6** (1997), 53–58.

[10] K. Nomura, *Spin models of index 2 and Hadmard models*, J. Alg. Combin. **17** (2003), 5–17.

Index

Abdukhalikov, Kanat, 214
Amarra, Maria Carmen V., 170

Bachoc, Christine, 119
Bannai, Eiichi, 224
Bannai, Etsuko, 292
Brouwer, Andries, 17

Cerzo, Diana, 32
Curtin, Brian, 321

dela Cruz, Romar B., 185

Evdokimov, Sergei, 72

Fujisaki, Tatsuya, 306

Giudici, Michael, 67

Harada, Koichiro, 218
Hiraki, Akira, 47
Hoshino, Ayumu, 92
Huang, Tayuan, 107

Ikuta, Takuya, 326

Kim, Jon-Lark, 57
Klin, Mikhail, 190
Koolen, Jack, 13

Maklnev, Alexandre A., 53
Manickam, Nachimuthu, 113
Martin, William J., 19

Oda, Fumihito,, 314

Sali, Attila, 174
Sekiguchi, Jiro, 136
Shen, Hao, 141
Shinohara, Masashi, 301
Shiromoto, Keisuke, 275
Sloane, Neil J. A., 151
Solé, Patrick, 262
Song, Sung Y., 204
Suetake, Chihiro, 146

Tanabe, Kenichiro, 98
Tanaka, Hajime, 284
Terwilliger, Paul, 76

Weng, Chih-wen, 37