

第19回 代数的組合せ論シンポジウム 報告集

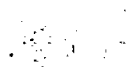
2002年7月1～3日
於 熊本大学 くすの木会館

平成14年度文部科学省科学研究費基盤研究(B)
研究代表者 坂内 英一

まえがき

この報告集は2002年7月1日(月)から3日(水)にわたって熊本大学くすの木会館レセプションルームで行われた「第19回代数的組合せ論シンポジウム」の講演記録です。講演は外国からの6名を含む26名の講演者によって行われ、多数の参加者を得て盛会でした。そのため会場がやや窮屈の感がありご迷惑をおかけしたことをお詫びいたします。この研究集会の講演者の旅費については科学研究費基盤研究B(研究代表者 坂内英・九州大学教授)の援助をいただきましたことを御礼申し上げます。また、講演をお引き受け下さった方々、会場の準備を手伝ってくださった熊本大学自然科学研究科および教育学部数学科の学生有志の方々、そしてこの報告集の作成に助力をお願いした九州大学大学院数理学研究科院生有志の方々に心から感謝致します。

2002年12月
平峰 豊



1950年10月1日，中华人民共和国中央人民政府成立。这一天，是新中国诞生的日子。毛泽东主席在天安门城楼上，向全世界宣告：中华人民共和国中央人民政府今天成立了！

从这一天起，中国人民开始了新的生活。在党的领导下，全国人民团结一心，艰苦奋斗，为国家的独立和民族的解放而斗争。

回首往事，我们不禁感慨万千。正是有了新中国，才有了我们今天的生活。我们要继续发扬革命传统，为实现中华民族伟大复兴而努力奋斗。

1950年10月1日

第19回代数的組合せ論シンポジウム

標記の研究集会を下記の要領で開催しますので、ご案内申し上げます。

世話人：平峰 豊（熊本大学・教育）

日程：2002年7月1日（月） - 3日（水）

場所：熊本大学黒髪キャンパス くすの木会館 レセプションルーム

周辺地図と交通機関

<http://www.kumamoto-u.ac.jp/univ-j.htm> のキャンバスマップ

プログラム

7月1日（月）

9:30-10:20 宗政 昭弘（九大・数理）

Nonexistence of tight spherical designs

10:30-11:30 Christine Bachoc (University of Bordeaux)

Codes and Designs in Grassmannian Spaces

13:00-14:00 Audrey Terras (UCSD)

Artin L-Functions of Graph Coverings

14:05-14:35 名越 弘文（京大数理研）

Spectra of arithmetic infinite graphs

14:40-15:30 坂内 英一（九大・数理）

Character tables of certain association schemes and Ramanujan graphs

15:35-16:15 Hadi Kharaghani (University of Lethbridge)

On a decomposition of complete graphs

16:20-17:00 吉荒 聡（大阪教育大）

高次元の双対弧の構成とその埋めこみ次元

17:00-17:30 藤崎竜也（九大・数理）

有限体上の直交群とその交換子群の external line の集合への作用

7月2日（火）

9:00-9:30 山内 博（筑波大学数学研究科）

ユニタリーヴィラソロ頂点作用素代数の単純カレント拡大

9:30-10:00 佐久間 伸也（筑波大学数学研究科）

二つの宮本 involution が S_3 を生成する頂点作用素代数

10:05-11:05 Keith Conrad(UCSD)

Counting prime power torsion in symmetric groups

11:10-12:10 Harold Stark (UCSD)

Galois theory for covering graphs

- 13:30-14:30 Vladimir D.Tonchev (Michigan Technological University)
Formulas for the number of Steiner triple and quadruple systems of low 2-rank
- 14:35-15:05 Daniel Dalan (九大・数理)
Hadamard matrices of order $2(p+1)$ with automorphisms of odd prime order p
- 15:10-16:00 小谷元子 (東北大・理)
結晶格子のランダム・ウォークの大偏差と空間の収束
- 16:05-16:45 野澤 宗平 (千葉大・理)
共役類の長さとは既約指標の次数

7月3日(水)

- 9:00-9:30 末竹 千博 (福島高専)
位数 16 の自己同型群を持つ位数 12 の射影平面について
- 9:30-10:00 城本 啓介 (龍谷大・理工)
 r -th MDS codes and matroids
- 10:10-10:50 丸田 辰哉 (愛知県立大)
Extendability of linear codes over finite fields
- 10:55-11:25 生田 卓也 (神戸女子学院短大)
On association schemes with A. V. Ivanov's condition
- 11:25-11:55 細谷 利恵 (金沢大・自然科学研究科)
On the association schemes of type II matrices constructed on Paley graphs
- 13:30-14:00 吉田知行 (北大・理)
A note on plethysm composition
- 14:00-14:30 水川 裕司 (北大・理)
 $(r, 2r)$ 型超幾何関数の選点直交多項式
- 14:35-15:05 田上 真 (九大・数理)
Symmetric association schemes attached to finite upper half planes over finite rings
- 15:05-15:35 飯寄 信保 (山口大・教育)
群上の単項式による群の特徴付け
- 15:40-16:00 平峰 豊 (熊大・教育)
 $(2n, 2, 2n, n)$ 差集合について

目次

1.	宗政 昭弘 (九大・数理)	1
	Nonexistence of tight spherical designs	
2.	Christine Bachoc (University of Bordeaux)	11
	Siegel modular forms, Grassmannian Designs, and Unimodular lattices	
3.	Audrey Terras (UCSD)	19
	Artin L-Functions of Graph Coverings	
4.	名越 弘文 (京大数理研)	57
	Spectra of arithmetic infinite graphs	
5.	坂内 英一 (九大・数理)	66
	Character tables of some association schemes, and Ramanujan graphs	
6.	吉荒 聡 (大阪教育大)	77
	高次元の双対弧の構成とその埋めこみ次元	
7.	藤崎竜也 (九大・数理)	87
	Association schemes defined by the action of finite orthogonal groups on the external lines	
8.	山内 博 (筑波大学数学研究科)	100
	ユニタリー-ウィラソロ頂点作用素代数の単純カレント拡大	
9.	佐久間 伸也 (筑波大学数学研究科)	108
	Vertex operator algebras with two Miyamoto involutions generating S_3	
11.	Harold Stark (UCSD)	116
	Galois theory for covering graphs	
12.	Vladimir D. Touchev (Michigan Technological University)	139
	A formula for the number of Steiner triple and quadruple systems on 2^n points of 2-rank $2^n - n$	
13.	Daniel Dalan (九大・数理)	154
	On Hadamard matrices of order $2(p + 1)$ with an automorphism of odd prime order p	

14.	小谷元子 (東北大・理)	165
	Geometric aspects of large deviations on random walks on a crystal lattice	
15.	野澤 宗平 (千葉大・理)	172
	共役類の長さと同約指標の次数	
16.	末竹 千博 (福島高専)	182
	位数 16 の自己同型群を持つ位数 12 の射影平面について	
17.	城本 啓介 (龍谷大・理工)	192
	g -th MDS codes and matroids	
18.	丸田 辰哉 (愛知県立大)	200
	Extendability of linear codes over finite fields	
19.	生田 卓也 (神戸女子学院短大)	207
	On association schemes with A. V. Ivanov's condition	
20.	細谷 利恵 (金沢大・自然科学研究科)	217
	On the association schemes of type II matrices constructed on Paley graphs	
21.	吉田知行 (北大・理)	228
	A note on plethysm composition	
22.	水川 裕司 (北大・理)	243
	$(r, 2r)$ 型超幾何関数の選点直交多項式	
23.	田上 真 (九大・数理)	253
	有限環上の上半平面から得られる symmetric association scheme	
24.	飯寄 信保 (山口大・教育)	261
	群上の単項式について	
25.	平峰 豊 (熊大・教育)	268
	On $(2n, 2, 2n, n)$ RDS's	

Nonexistence of tight spherical designs

Akihiro Munemasa

joint work with
Eiichi Bannai
and
Boris Venkov

1 Introduction and Preliminaries

A spherical design is a finite subset X of the unit sphere $S^{n-1} \subset \mathbb{R}^n$ which approximates S^{n-1} (to a certain degree $t \in \mathbb{N}$, to be defined later). A spherical t -design is called tight if it has the smallest possible number of points among all t -designs in S^{n-1} . Before giving the exact definition, let us list some examples.

- A regular simplex in S^{n-1} is a tight spherical 2-design.
- $X = \frac{1}{\sqrt{2}}E_8$, where $E_8 \subset \mathbb{R}^8$ is the set of 240 roots (vectors of norm 2) of the root system of type E_8 . X is a tight spherical 7-design.
- $X = \frac{1}{2}\Lambda_4 \subset S^{23}$, where $\Lambda \subset \mathbb{R}^{24}$ is the Leech lattice, Λ_4 is the set of the 196560 shortest vectors (of norm 4) in Λ . X is a tight spherical 11-design.

Definition 1. A subset $X \subset S^{n-1}$ is a spherical t -design if

$$\frac{1}{|X|} \sum_{x \in X} f(x) = \frac{1}{\omega_{n-1}} \int_{S^{n-1}} f(x) dS$$

for every polynomial $f(x) = f(x_1, x_2, \dots, x_n)$ of degree $\leq t$, where

$$\omega_{n-1} = \int_{S^{n-1}} 1 dS$$

If $X \subset S^{n-1}$ is a spherical t -design, then

$$|X| \geq \binom{n-1+t/2}{t/2} + \binom{n+t/2-2}{t/2-1}$$

if t is even, and

$$|X| \geq 2 \binom{n-1+(t-1)/2}{(t-1)/2}$$

if t is odd. X is said to be tight if equality holds.

If $X \subset S^{n-1}$ ($n \geq 3$) is a tight spherical t -design, then

- (Bannai-Damerell, 1979-1980) $t \leq 5$, $t = 7$ or $t = 11$.
- (Bannai-Sloane, 1981) $t = 11 \implies$ Leech.
- $t \leq 3 \implies$ classified (trivial for $t = 1$, regular simplex for $t = 2$, generalized octahedron for $t = 3$).
- $t = 5 \implies$ a derived configuration is a tight 4-design in S^{n-2} .
- $t = 4 \implies$ an extended configuration is a tight 5-design in S^n .

So the existence of a tight spherical 4-design in S^{n-2} is equivalent to the existence of a tight spherical 5-design in S^{n-1} . We may restrict our attention to the existence problem of tight spherical 5- and 7-designs.

If $X \subset S^{n-1}$ ($n \geq 3$) is a tight spherical 5-design, then $n = 3$ and X is an icosahedron, or

$$\begin{aligned} n &= d^2 - 2 \quad (d: \text{odd}) \\ &= 7, 23, 47, \dots \end{aligned}$$

$$\{(x, y) \mid x, y \in X\} = \{\pm 1, \pm \frac{1}{d}\}.$$

For $n = 7$, we have the derived E_8 , and for $n = 23$, we have $Co_3 \times 2$ on $276 \cdot 2$.

If $X \subset S^{n-1}$ ($n \geq 3$) is a tight spherical 7-design, then

$$n = 3d^2 - 4 = 8, 23, 44, 71, \dots$$

$$\{(x, y) \mid x, y \in X\} = \{0, \pm 1, \pm \frac{1}{d}\}$$

For $n = 8$, we have E_8 , and for $n = 23$, we have the derived Leech configuration on 4600 points.

2 Nonexistence of Tight Spherical 7-Designs

A tight spherical $(2s + 1)$ -design X is antipodal, i.e., $X = -X$, and an antipodal subset $X \subset S^{n-1}$ is a spherical $(2s + 1)$ -design iff

$$\frac{1}{|X|} \sum_{x \in X} f(x) = \frac{1}{\omega_{n-1}} \int_{S^{n-1}} f(x) dS$$

for every homogeneous polynomial of degree $2, 4, \dots, 2s$. For 7-designs, it suffices to take f to be homogeneous polynomials of degree $2, 4, 6$. Take

$$f(x) = (\alpha, x)^2, (\alpha, x)^4, (\alpha, x)^6$$

where $\alpha \in \mathbb{R}^n$, $x = (x_1, \dots, x_n)$, and $(\alpha, x) = \sum_{i=1}^n \alpha_i x_i$. The conditions derived by taking the above f are called the basic relations, and these are given below [11, 12].

$$\begin{aligned} \frac{1}{|X|} \sum_{x \in X} (\alpha, x)^2 &= \frac{1}{n} (\alpha, \alpha), \\ \frac{1}{|X|} \sum_{x \in X} (\alpha, x)^4 &= \frac{3}{n(n+2)} (\alpha, \alpha)^2, \\ \frac{1}{|X|} \sum_{x \in X} (\alpha, x)^6 &= \frac{15}{n(n+2)(n+4)} (\alpha, \alpha)^3. \end{aligned}$$

Suppose that X is a tight spherical 7-design. If one takes $\alpha \in X$, then one obtains the consequences

$$n = 3d^2 - 4,$$

$$x, y \in X \implies (x, y) = \pm 1, \pm \frac{1}{d}, 0$$

but not more. To derive further restrictions, the key idea is to take α in the dual lattice of the lattice generated by X . Thus, for the convenience, we normalize the set X in such a way that it generates an integral lattice. If $X \subset S^{n-1}$ is a tight spherical 7-design, then $n = 3d^2 - 4$. Put $D = \sqrt{d}X$. Then

$$x, y \in D \implies (x, y) = \pm d, \pm 1, 0.$$

Let Λ be the integral lattice in \mathbb{R}^n generated by D . The basic relations become:

$$\begin{aligned}\frac{1}{|D|} \sum_{x \in D} (\alpha, x)^2 &= \frac{d}{n} (\alpha, \alpha) \\ \frac{1}{|D|} \sum_{x \in D} (\alpha, x)^4 &= \frac{3d^2}{n(n+2)} (\alpha, \alpha)^2 \\ \frac{1}{|D|} \sum_{x \in D} (\alpha, x)^6 &= \frac{15d^3}{n(n+2)(n+4)} (\alpha, \alpha)^3\end{aligned}$$

for any $\alpha \in \mathbb{R}^n$. Also,

$$|D| = |X| = \frac{n(n+1)(n+2)}{3}$$

After simplification, we get

$$\begin{aligned}\sum_{x \in D} (\alpha, x)^2 &= d(3d^2 - 2)(d^2 - 1)(\alpha, \alpha) \\ \sum_{x \in D} (\alpha, x)^4 &= 3d^2(d^2 - 1)(\alpha, \alpha)^2 \\ \sum_{x \in D} (\alpha, x)^6 &= 5d(d^2 - 1)(\alpha, \alpha)^3\end{aligned}$$

for all $\alpha \in \mathbb{R}^n$.

If (α, x) is an integer for all $x \in D$, or equivalently, α belongs to the dual lattice of $\Lambda = \langle D \rangle$, then we can get some congruencial conditions. Assume

$$\begin{aligned}\alpha \in \Lambda^* &= \{\alpha \in \mathbb{R}^n \mid (\alpha, \beta) \in \mathbb{Z}, \forall \beta \in \Lambda\} \\ &= \{\alpha \in \mathbb{R}^n \mid (\alpha, x) \in \mathbb{Z}, \forall x \in D\} \\ &\supset \Lambda \supset D\end{aligned}$$

For each $k = 1, 2, \dots$, define $n_k(\alpha)$ by

$$n_k(\alpha) = \frac{1}{2} |\{x \in D \mid (\alpha, x) = \pm k\}| \in \mathbb{Z}$$

Then the basic relations become:

$$\begin{aligned}\sum_{k=1}^{\infty} k^2 n_k(\alpha) &= \frac{d}{2}(3d^2 - 2)(d^2 - 1)(\alpha, \alpha) \\ \sum_{k=1}^{\infty} k^4 n_k(\alpha) &= \frac{3d^2}{2}(d^2 - 1)(\alpha, \alpha)^2 \\ \sum_{k=1}^{\infty} k^6 n_k(\alpha) &= \frac{5d}{2}(d^2 - 1)(\alpha, \alpha)^3\end{aligned}$$

Example 1. $d = 4$, $n = 44$ (the smallest open case). Since

$$\sum_{k=1}^{\infty} k^2(k^2 - 1)(k^2 - 4)n_k(\alpha) \equiv 0 \pmod{24}$$

we have

$$\frac{5(\alpha, \alpha)(5(\alpha, \alpha)^2 - 60(\alpha, \alpha) + 184)}{4} \in \mathbb{Z}.$$

Similarly,

$$\begin{aligned}k^2(k^2 - 1) &\equiv 0 \pmod{12} \\ k^2(k^4 - 1) &\equiv 0 \pmod{60}\end{aligned}$$

give more divisibility conditions, which imply $(\alpha, \alpha) \in 2\mathbb{Z}$. We therefore obtain

$$\begin{aligned}(\alpha, \alpha) &\in 2\mathbb{Z} \quad \forall \alpha \in \Lambda^* \\ \implies \Lambda^* &\text{ is even} \implies \Lambda^* \text{ is integral} \\ \implies \Lambda = \Lambda^* &\text{ is an even unimodular lattice} \\ &\text{of dimension } n = 44\end{aligned}$$

This is impossible, because an even unimodular lattice exists only when the dimension is a multiple of 8, and it is not the case for 44.

Example 2. $d = 5$. We claim $\min \Lambda = 5$. Suppose

$$\alpha \in \Lambda, (\alpha, \alpha) = \min \Lambda \leq 4.$$

Then for $\forall x \in D$, $\alpha + x \in \Lambda$, so

$$\begin{aligned}(\alpha, \alpha) &\leq (\alpha \pm x, \alpha \pm x) \\ &= (\alpha, \alpha) \pm 2(\alpha, x) + 5\end{aligned}$$

Thus

$$\begin{aligned}|(\alpha, x)| &\leq \frac{5}{2} \\ (\alpha, x) &\in \{0, \pm 1, \pm 2\}\end{aligned}$$

This means

$$\sum_{k=1}^{\infty} k^m n_k(\alpha) \text{ becomes } n_1(\alpha) + 2^m n_2(\alpha)$$

This situation has been investigated by Martinet in a different context [9].

$$\begin{aligned}n_1(\alpha) + 4n_2(\alpha) &= 3880(\alpha, \alpha) \\ n_1(\alpha) + 16n_2(\alpha) &= 900(\alpha, \alpha)^2 \\ n_1(\alpha) + 64n_2(\alpha) &= 300(\alpha, \alpha)^3\end{aligned}$$

Eliminating $n_1(\alpha), n_2(\alpha)$ from these equations, we find a quadratic equation in (α, α) which has only imaginary solutions. This is a contradiction.

Example 3. $d = 6$, $n = 104$ (still open).

- Λ is even unimodular.
- $\min \Lambda = 6$, $\Lambda_6 = D$.
- $\Lambda_8 = \emptyset$.
- $\vartheta_\Lambda = 1 + 385840q^3 + 153139896000q^5 + \dots$ (uniquely determined modular form).

We now state our main result for the nonexistence of tight spherical 7-designs. Let p a prime. For $m \in \mathbb{Z}$, define

$$\nu_p(m) = \text{the largest integer } \nu \text{ such that } p^\nu | m$$

Theorem 1. *Let $d > 1$ be a positive integer, and suppose*

$$\begin{aligned} \nu_2(d) = 2, \quad \nu_3(d(d^2 - 1)) < 4, \\ \nu_p(d(d^2 - 1)) < 3 \quad \forall \text{prime } p \geq 5. \end{aligned}$$

Then a tight spherical 7-design in dimension $n = 3d^2 - 4$ does not exist.

Proof. (Sketch). The lattice Λ becomes an even unimodular lattice of dimension n , but $n \equiv 4 \pmod{8}$, a contradiction. \square

Pétermann pointed out that the set of positive integers d satisfying the hypothesis of Theorem 1 has positive density in \mathbb{N} (in particular, is infinite).

3 Nonexistence of Tight Spherical 5-Designs

For spherical 5-design X , we have

$$\begin{aligned} \frac{1}{|X|} \sum_{x \in X} (\alpha, x)^2 &= \frac{1}{n} (\alpha, \alpha) \\ \frac{1}{|X|} \sum_{x \in X} (\alpha, x)^4 &= \frac{3}{n(n+2)} (\alpha, \alpha)^2 \end{aligned}$$

for any $\alpha \in \mathbb{R}^n$.

Suppose that X is a tight spherical 5-design. If one takes $\alpha \in X$, then we obtain the consequences

$$\begin{aligned} n &= d^2 - 2, \quad d = 2m + 1 \\ x, y \in X &\implies (x, y) = \pm 1, \pm \frac{1}{d} \end{aligned}$$

As we have done for tight spherical 7-designs, we normalize X to define an integral lattice Λ , and then take α in the dual lattice of Λ . If $X \subset S^{n-1}$ ($n > 3$) is a tight spherical 5-design, then $n = d^2 - 2$, $d = 2m + 1$. Put $D = \sqrt{d}X$. Then

$$x, y \in D \implies (x, y) = \pm d, \pm 1$$

Let Λ be the integral lattice in \mathbb{R}^n generated by D . The basic relations read:

$$\begin{aligned} \frac{1}{|D|} \sum_{x \in D} (\alpha, x)^2 &= \frac{d}{n} (\alpha, \alpha) \\ \frac{1}{|D|} \sum_{x \in D} (\alpha, x)^4 &= \frac{3d^2}{n(n+2)} (\alpha, \alpha)^2 \end{aligned}$$

for any $\alpha \in \mathbb{R}^n$, and

$$|D| = |X| = n(n+1).$$

After simplification, we get

$$\begin{aligned} \sum_{x \in D} (\alpha, x)^2 &= 4m(m+1)(2m+1)(\alpha, \alpha) \\ \sum_{x \in D} (\alpha, x)^4 &= 12m(m+1)(\alpha, \alpha)^2 \end{aligned}$$

If $\alpha \in \Lambda^*$, then

$$\begin{aligned} \sum_{k=1}^{\infty} k^2 n_k(\alpha) &= 2m(m+1)(2m+1)(\alpha, \alpha) \\ \sum_{k=1}^{\infty} k^4 n_k(\alpha) &= 6m(m+1)(\alpha, \alpha)^2 \end{aligned}$$

Since $k^4 - k^2 \equiv 0 \pmod{12}$, we have

$$\frac{m(m+1)(\alpha, \alpha)(3(\alpha, \alpha) - (2m+1))}{6} \in \mathbb{Z}$$

This is much weaker than the divisibility condition for tight 7-designs, but we can get the following consequence:

$$m, m+1 : \text{square-free} \implies (\alpha, \alpha) \in \frac{1}{3}\mathbb{Z}$$

To get more restriction, we consider some other lattices related to Λ .

$$\begin{aligned} \Lambda \supset \Lambda_+ : \text{even sublattice} \\ &= \{\alpha \in \Lambda \mid (\alpha, \alpha) \in 2\mathbb{Z}\} \\ &\text{is a sublattice of index 2 in } \Lambda \\ \Gamma &= \frac{1}{\sqrt{2}}\Lambda_+ \end{aligned}$$

Then Γ is an integral lattice and

$$\det \Gamma = 2 \cdot 3^s \quad (s \in \mathbb{Z}, s \geq 0)$$

Theorem 2. *Suppose*

$$m = 2k, \quad k \equiv 2 \pmod{3},$$

$$k, 2k + 1 \text{ are square-free.}$$

Then there does not exist a tight spherical 5-design in \mathbb{R}^n , where $n = (2m + 1)^2 - 2$.

The proof of this theorem is more complicated than that of Theorem 1, and requires the Milgram–Braun formula [10].

Example 4. The case $m = 3$ ($n = 47$) is not ruled out by Theorem 2. We give an outline of the proof of the nonexistence in this case. Suppose that there exists a tight spherical 5-design in \mathbb{R}^{47} . Then

$$\begin{aligned} \Gamma \subset \mathbb{R}^{47} & \text{ has determinant } 2 \\ \implies \exists \tilde{\Gamma} \subset \mathbb{R}^{48} & : \text{ even unimodular, by gluing} \\ \implies \vartheta_{\tilde{\Gamma}} & \text{ is a modular form of weight } 24 \\ & \text{ with respect to } SL(2, \mathbb{Z}) \end{aligned}$$

But the analysis of the coefficients of $\vartheta_{\tilde{\Gamma}}$ reveals that $\vartheta_{\tilde{\Gamma}}$ can not be expressible as a linear combination of a known basis of the space of modular forms of weight 24. This is a contradiction.

We originally hoped to construct one in \mathbb{R}^{47} . Let X be a tight spherical 5-design in \mathbb{R}^{47} . Then a derived configuration (a hyperplane section of X) is a tight 4-design Y , $|Y| = 1127$. Angles among the elements of Y defines a strongly regular graph:

$$\begin{array}{cc} 1 & 320 \\ & 165 & 320 \\ 1 & 320 \end{array}$$

Then Venkov showed that the subgraph induced by “165” is a generalized quadrangle of order $(4, 8)$.

Could our technique be applied to establish the uniqueness of a generalized quadrangle of order $(4, 8)$?

References

- [1] E. Bannai and E. Bannai, Algebraic Combinatorics on Spheres, Springer-Verlag, Tokyo, 1999 (Japanese).
- [2] E. Bannai and R. Damerell, Tight spherical designs, I, J. Math. Soc. Japan 31 (1979), 199–207.
- [3] E. Bannai and R. Damerell, Tight spherical designs, II, J. London Math. Soc. (2) 21 (1980), 13–30.
- [4] E. Bannai and N. J. A. Sloane, Uniqueness of certain spherical codes, Canad. J. Math. 33 (1981), 437–449.
- [5] J. H. Conway and N. J. A. Sloane, Sphere Packing, Lattices and Groups, 3rd ed., Springer-Verlag, New York, 1999.
- [6] P. Delsarte, J.-M. Goethals and J. J. Seidel, Spherical codes and designs, Geometriae Dedicata 6 (1977), 363–388.
- [7] J.-M. Goethals and J. J. Seidel, Spherical designs, Proc. Sympos. Pure Math., XXXIV, 255–272, Amer. Math. Soc., Providence, R.I., 1979.
- [8] J.-M. Goethals and J. J. Seidel, The regular two-graph on 276 vertices, Discrete Math. 12 (1975), 143–158.
- [9] J. Martinet, Sur certains designs sphériques liés à des réseaux entiers, in: Réseaux Euclidiens, Design Sphériques et Formes Modulaires, Autour des travaux de Boris Venkov, J. Martinet (ed.), 135–146. L'Enseignement Math., Geneve, 2001.
- [10] J. Milnor and D. Husemoller, Symmetric Bilinear Forms, Springer-Verlag, 1973.
- [11] G. Nebe and B. Venkov, The strongly perfect lattices of dimension 10, J. Théor. Nombres Bordeaux 12 (2000), 503–518.
- [12] B. Venkov, Réseaux et designs sphériques, in: Réseaux Euclidiens, Design Sphériques et Formes Modulaires, Autour des travaux de Boris Venkov, J. Martinet (ed.), 10–86. L'Enseignement Math., Geneve, 2001.

SIEGEL MODULAR FORMS, GRASSMANNIAN DESIGNS, AND UNIMODULAR LATTICES

CHRISTINE BACHOC AND GABRIELE NEBE

ABSTRACT. Siegel theta series with harmonic coefficients are vector-valued Siegel modular forms. We use them to show that certain sections of lattices form designs in Grassmannian space.

1. INTRODUCTION

In [2], a notion of t -design on the Grassmann manifold $\mathcal{G}_{m,n}$ is introduced, generalizing the so-called (antipodal) spherical designs. Many examples of such designs arise from lattices, the most famous ones being the designs associated to the root lattice E_8 and the Leech lattice. In both cases, these designs can be explained by properties of the representations afforded by their automorphism groups. In the case of the spherical designs, another proof, due to Boris Venkov, uses the theta series of these lattices as modular forms. Such an argument has been applied successfully to other families of lattices (see [15] and [3]).

In this paper, we prove a similar connection between the Grassmannian designs and certain vector-valued Siegel modular forms associated to a lattice. By using the explicit description of certain spaces of vector-valued Siegel modular forms, we can prove the existence of Grassmannian designs in the family of the extremal even unimodular lattices of dimension 32.

2. GRASSMANNIAN DESIGNS

2.1. Definitions. We briefly recall here the notion of Grassmannian designs. For a more detailed presentation, the reader is referred to [2].

Let $\mathcal{G}_{m,n}$ denote the real Grassmannian space of m -dimensional subspaces of \mathbb{R}^n , together with the transitive action of the real orthogonal group $O(n, \mathbb{R})$. The starting point is the decomposition of the Hilbert-space of complex-valued absolutely squared integrable functions $L^2(\mathcal{G}_{m,n})$ under the action of $O(n, \mathbb{R})$. As an $O(n, \mathbb{R})$ -module:

$$(1) \quad L^2(\mathcal{G}_{m,n}) = \overline{\bigoplus_{\mu} H_{m,n}^{\mu}}$$

where the sum is over the partitions $\mu = \mu_1 \geq \dots \geq \mu_m \geq 0$ with even parts $\mu_i \equiv 0 \pmod{2}$. The spaces $H_{m,n}^{\mu}$ are isomorphic to the irreducible

Date: January 8, 2003.

1991 Mathematics Subject Classification. 11H06,

representation V_n^μ (see [6]) of $O(n, \mathbb{R})$ canonically associated to μ . The degree of the partition μ is by definition $\deg(\mu) := \sum_i \mu_i$.

Definition 2.1. *A finite subset X of $\mathcal{G}_{m,n}$ is called a t -design if one of the following equivalent properties is satisfied:*

1. For all $f \in H_{m,n}^\mu$ and all μ with $0 \leq \deg(\mu) \leq t$,

$$\int_{\mathcal{G}_{m,n}} f(p) dp = \frac{1}{|X|} \sum_{x \in X} f(x).$$
2. For all $f \in H_{m,n}^\mu$ and all μ with $2 \leq \deg(\mu) \leq t$, $\sum_{x \in X} f(x) = 0$.

There is a nice characterization of the designs in terms of the zonal functions of $\mathcal{G}_{m,n}$: It is a classical fact that the orbits under the action of $O(n, \mathbb{R})$ of the pairs (p, p') of elements of $\mathcal{G}_{m,n}$ are characterized by their so-called principal angles $(\theta_1, \dots, \theta_m) \in [0, \pi/2]^m$. We denote $y_i := \cos^2(\theta_i)$. The polynomial functions on $\mathcal{G}_{m,n} \times \mathcal{G}_{m,n}$ which are invariant under the diagonal action of $O(n, \mathbb{R})$ are polynomials in the variables (y_1, \dots, y_m) . They form an algebra isomorphic to the algebra $\mathbb{C}[Y_1, \dots, Y_m]^{S_m}$ of symmetric polynomials in m variables. Moreover, there is a unique sequence of polynomials $p_\mu(Y_1, \dots, Y_m)$ indexed by the partitions into even parts, such that $\mathbb{C}[Y_1, \dots, Y_m]^{S_m} = \sum_\mu \mathbb{C} p_\mu$, $p_\mu(1, \dots, 1) = 1$, and the function : $p \in \mathcal{G}_{m,n} \rightarrow p_\mu(y_1(p, p'), \dots, y_m(p, p'))$ defines, for all $p' \in \mathcal{G}_{m,n}$, an element of $H_{m,n}^\mu$. These polynomials have degree $\deg(\mu)/2$. They are explicitly calculated in [8].

Theorem 2.2. (see [2, Proposition 4.2]) *Let $X \subset \mathcal{G}_{m,n}$ be a finite set. Then,*

1. $\sum_{p, p' \in X} p_\mu(y_1(p, p'), \dots, y_m(p, p')) \geq 0$.
2. *The set $X \subset \mathcal{G}_{m,n}$ is a t -design if and only if for all μ , $2 \leq \deg(\mu) \leq t$,
 $\sum_{p, p' \in X} p_\mu(y_1(p, p'), \dots, y_m(p, p')) = 0$.*

2.2. Some subsets of $\mathcal{G}_{m,n}$ associated to a lattice. Let $L \subset \mathbb{R}^n$ be a lattice. We define certain natural finite subsets of $\mathcal{G}_{m,n}$ associated to L , in the following way. The spaces of $m \times m$ real symmetric, real positive definite, and real positive semi-definite matrices are denoted by $S_m(\mathbb{R})$, $S_m^{>0}(\mathbb{R})$, $S_m^{\geq 0}(\mathbb{R})$, respectively.

Definition 2.3. *Let $S \in S_m^{>0}(\mathbb{R})$. We denote L_S the set of $p \in \mathcal{G}_{m,n}$ such that $p \cap L$ is a lattice, having a basis (v_1, \dots, v_m) with $v_i \cdot v_j = S_{i,j}$.*

Clearly, the sets L_S are finite sets. In the case $m = 1$, the sets L_S are the sets of lines supporting the primitive lattice vectors of fixed norm. It is worth noticing that these sets are unions of orbits under the automorphism group of the lattice.

We introduce a few more notations. An m -tuple of vectors of \mathbb{R}^n is denoted by $v^{(m)}$ and the Gram matrix of its vectors by $\text{gram}(v^{(m)})$. The real vector space spanned by these vectors is $\mathbb{R}v^{(m)}$. If the vectors of $v^{(m)}$ belong to the lattice L , and consist of a \mathbb{Z} -basis of $L \cap \mathbb{R}v^{(m)}$, $v^{(m)}$ is called *primitive*.

One of the aims of this paper is to study the design properties of the sets L_S . Therefore, we have to consider sums of the type $\sum_{p \in L_S} f(p)$ where f runs over the spaces $H_{m,n}^\mu$.

Lemma 2.4. *The following assertions are equivalent:*

1. For all $S \in S_m^{>0}(\mathbb{R})$, $\sum_{p \in L_S} f(p) = 0$
2. For all $S \in S_m^{>0}(\mathbb{R})$, $\sum_{\substack{v^{(m)} \in L^m, \text{primitive} \\ \text{gram}(v^{(m)})=S}} f(\mathbb{R}v^{(m)}) = 0$
3. For all $S \in S_m^{>0}(\mathbb{R})$, $\sum_{\substack{v^{(m)} \in L^m \\ \text{gram}(v^{(m)})=S}} f(\mathbb{R}v^{(m)}) = 0$

Proof. Two bases of the lattice $L \cap p$ with the same Gram matrix are exchanged by an element of the automorphism group of $L \cap p$, so the second sum differs from the first by a multiplicative factor. In the third sum, the non primitive $v^{(m)}$ contribute to subsums of the type $\sum_{p \in L_{S'}} f(p)$ with $\det(S') < \det(S)$ so we can conclude by induction on $\det(S)$. \square

Remark 2.5. *With the help of representation theory of the automorphism group, one finds examples of lattices L such that all the (non empty) sets L_S (with $\text{rank}(S) \leq \frac{\dim(L)}{2}$) are Grassmannian k -designs (see [2]). For the root lattices D_4, E_6, E_7 one can take $k = 4$, for E_8 and the Barnes-Wall lattice BW_{16} , $k = 6$ and even $k = 10$ for the Leech lattice Λ_{24} .*

It turns out that the sums of Lemma 2.4(3) can be interpreted in terms of certain vector-valued modular forms. The next section recalls the basic properties of these modular forms.

3. VECTOR-VALUED SIEGEL MODULAR FORMS

Let H_m denote the Siegel space

$$(2) \quad H_m := \{Z \in M^{m \times m}(\mathbb{C}) \mid Z^t = Z, Z = X + iY \text{ and } Y > 0\}$$

endowed with the usual action of the symplectic group $\text{Sp}(m, \mathbb{R})$. If $M := \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \text{Sp}(m, \mathbb{R})$ and $Z \in H_m$ then $M.Z := (AZ + B)(CZ + D)^{-1}$.

Let (ρ, V_ρ) be a finite dimensional complex representation of $\text{GL}(m, \mathbb{C})$. A V_ρ -valued Siegel modular form for the modular group $\Gamma_m := \text{Sp}(m, \mathbb{Z})$ is a holomorphic function $f : H_m \rightarrow V_\rho$ satisfying the transformation formula $f|_\rho M = f$ for all $M \in \Gamma_m$, where

$$(f|_\rho M)(Z) := \rho(CZ + D)^{-1} f(MZ)$$

(plus a condition on the growth of f in the case $m = 1$). Such a modular form has got a Fourier expansion of the type:

$$(3) \quad f(Z) = \sum_S a_f(S) e(SZ)$$

where $e(SZ) := e^{i\pi \operatorname{trace}(SZ)}$ and S runs over the set of even symmetric positive semi-definite matrices $S_m^{\text{even}} := \{S \in S_m^{\geq 0}(\mathbb{R}) \mid S_{i,j} \in \mathbb{Z} \text{ and } S_{i,i} \equiv 0 \pmod{2}\}$.

One can restrict without loss of generality to the case when the representation ρ is irreducible. Then, it is characterized by its highest weight, an m -tuple $\mu := (\mu_1, \dots, \mu_m)$ with $\mu_1 \geq \dots \geq \mu_m$, and we may denote (ρ_μ, V_μ) this representation.

The vector space $[\Gamma_m, \rho]$ of these modular forms is finite dimensional. The classical case of complex-valued Siegel modular forms corresponds to the one-dimensional representations; the spaces may be denoted $[\Gamma_m, \det^k]$ or more briefly $[\Gamma_m, k]$. The direct sum $A(\Gamma_m) := \bigoplus_{k \equiv 0 \pmod{2}} [\Gamma_m, k]$ is a \mathbb{C} -algebra, the structure of which is completely understood only for $m = 1, 2, 3$. For an arbitrary representation ρ , the sum $A(\Gamma_m, \rho) := \bigoplus_{k \equiv 0 \pmod{2}} [\Gamma_m, \det^k \otimes \rho]$ is a module over the previous algebra. Its structure is completely described in the cases $m = 2$ and $\rho = [2, 0], [4, 0], [6, 0]$ (see [12], [7]).

Such modular forms can be constructed from lattices, in the following way (see [4] and [5] for detailed proofs). Let L be again an n -dimensional lattice contained in \mathbb{R}^n . The theta series of degree $m \leq n/2$ associated to L is:

$$(4) \quad \theta_L^{(m)} := \sum_{\substack{v^{(m)} \in L^m \\ S := \operatorname{gram}(v^{(m)})}} e(SZ) = \sum_{S \in S_m^{\text{even}}} a_L(S) e(SZ)$$

where $a_L(S)$ counts the number of $v^{(m)} \in L^m$ with $\operatorname{gram}(v^{(m)}) = S$. Then $\theta_L^{(m)}$ is a Siegel modular form for some congruence subgroup, which can be taken to be the full modular group $\Gamma_m = \operatorname{Sp}(m, \mathbb{Z})$, if the lattice L is even unimodular. The weight of $\theta_L^{(m)}$ is equal to $n/2$ (i.e. they are modular forms for the representation $\rho = \det^{n/2}$).

More generally, one can construct vector-valued modular forms from a lattice L and some spaces of harmonic polynomials.

Let $\mathbb{C}[\underline{X}]$ denote the polynomial algebra in the matrix variables $(X_{i,j})_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}}$, with the action of $\operatorname{GL}(m, \mathbb{R}) \times \operatorname{GL}(n, \mathbb{R})$ given by $(g, h).P = P(g^t X h)$. The decomposition of this space is well-known to be:

$$(5) \quad \mathbb{C}[\underline{X}] \simeq \bigoplus_{\mu} F_m^{\mu} \otimes F_n^{\mu}$$

where F_m^{μ} denotes the irreducible $\operatorname{GL}(m, \mathbb{R})$ -module canonically associated to the partition $\mu = (\mu_1, \dots, \mu_m)$ with $\mu_1 \geq \dots \geq \mu_m \geq 0$. The harmonic polynomials are the polynomials belonging to the intersection of the kernels of the operators

$$(6) \quad \Delta_{i,j} := \sum_{k=1}^n \frac{\partial^2}{\partial X_{i,k} \partial X_{j,k}}.$$

Their space is denoted $\mathcal{H}_{m,n}$ and is stable under the action of $\operatorname{GL}(m, \mathbb{R}) \times \operatorname{O}(n, \mathbb{R})$. Its decomposition is given by

$$(7) \quad \mathcal{H}_{m,n} \simeq_{\mathrm{GL}(m,\mathbb{R}) \times \mathrm{O}(n,\mathbb{R})} \bigoplus_{\mu} F_m^{\mu} \otimes V_n^{\mu}$$

Equivalently, the polynomial functions: $P : M^{m \times n}(\mathbb{C}) \rightarrow F_m^{\mu}$ satisfying $\rho_{\mu}(u)P(X) = P(u^t X)$ for all $u \in \mathrm{GL}(m, \mathbb{R})$ span a vector space, $\mathrm{O}(n, \mathbb{R})$ -isomorphic to V_n^{μ} . We shall denote it $\mathrm{Harm}_{m,n}^{\mu}$.

Definition 3.1. Let $L \subset \mathbb{R}^n$ be a lattice and $P \in \mathrm{Harm}_{m,n}^{\mu}$. For $m \leq \frac{n}{2}$ let

$$(8) \quad \theta_{L,P}^{(m)} := \sum_{\substack{v^{(m)} \in L^m \\ S := \mathrm{gram}(v^{(m)})}} P(v^{(m)}) e(SZ)$$

where $P(v^{(m)})$ stands for the value of P on the $m \times n$ matrix $X_{v^{(m)}}$, the rows of which are equal to the m vectors of $v^{(m)}$. $\theta_{L,P}^{(m)}$ is called the harmonic Siegel theta series of L with coefficients P .

Proposition 3.2. ([5]) If $L \subset \mathbb{R}^n$ is an even unimodular lattice and $P \in \mathrm{Harm}_{m,n}^{\mu}$, then $\theta_{L,P}^{(m)} \in [\Gamma_m, \det^{n/2} \otimes \rho_{\mu}]$ is a vector valued Siegel modular form for the full modular group.

4. HARMONIC THETA SERIES AND GRASSMANNIAN DESIGNS

In this section we show how harmonic Siegel theta series can be used to show that certain sets L_S of sections of a lattice L provide Grassmannian designs.

Theorem 4.1. Let $L \subset \mathbb{R}^n$ be an even lattice, and let $m \leq n/2$. Assume that, for all $P \in \mathrm{Harm}_{m,n}^{\mu}$ and all even μ with $2 \leq \deg(\mu) \leq t$, $\theta_{L,P}^{(m)} = 0$. Then, for all $m_0 \leq m$ and all $S \in S_{m_0}^{>0}(\mathbb{R})$, the non empty sets L_S are t -designs.

Proof. The space $(F_m^{\mu})^{\mathrm{O}(m,\mathbb{R})}$ of $\mathrm{O}(m, \mathbb{R})$ -invariant elements in F_m^{μ} is one-dimensional if and only if μ is even. We denote v_{μ} an arbitrary non-zero vector of this space. We choose on F_m^{μ} an $\mathrm{O}(m, \mathbb{R})$ -invariant hermitian form, denoted by \langle, \rangle , and we can assume v_{μ} to be of norm 1 for this form. If $P \in \mathrm{Harm}_{m,n}^{\mu}$, let $P_0 : M^{m \times n}(\mathbb{C}) \rightarrow \mathbb{C}$ be defined by: $P_0(X) := \langle P(X), v_{\mu} \rangle$. By construction, the function P_0 is $\mathrm{O}(m, \mathbb{R})$ -invariant and therefore defines an element \tilde{P}_0 of $L^2(\mathcal{G}_{m,n})$ by: $\tilde{P}_0(p) := P_0(X_p)$, where X_p is the matrix of any orthonormal basis of p . The mapping $P \rightarrow \tilde{P}_0$ is an isomorphism of $\mathrm{O}(n, \mathbb{R})$ -modules from $\mathrm{Harm}_{m,n}^{\mu}$ to $H_{m,n}^{\mu}$.

Let $S \in S_m^{\mathrm{even}}$ be of rank m . There exists $U \in \mathrm{GL}(m, \mathbb{R})$ such that $S = UU^t$. From the hypothesis, we have, for all $P \in \mathrm{Harm}_{m,n}^{\mu}$,

$$\sum_{\substack{v^{(m)} \in L^m \\ S := \mathrm{gram}(v^{(m)})}} P(v^{(m)}) = 0.$$

Since $\rho_\mu((U^{-1})^t)P(v^{(m)}) = P(U^{-1}X_{v^{(m)}})$, and since $U^{-1}X_{v^{(m)}}$ is the matrix of an orthonormal basis of the space $\mathbb{R}v^{(m)}$, we conclude that

$$\sum_{\substack{v^{(m)} \in L^m \\ S := \text{gram}(v^{(m)})}} \tilde{P}_0(\mathbb{R}v^{(m)}) = 0.$$

From Lemma 2.4, the set L_S is a t -design. The assertion on the other $m_0 < m$ derives from the same argument applied to the successive images of $\theta_{L,P}^{(m)}$ by the Φ -operator. \square

In order to apply the previous theorem to concrete situations, we need to study the spaces of vector-valued modular forms. The next proposition shows that in general we only need to study the cusp forms. The space of cusp forms is the space of forms $f \in [\Gamma_m, \mu]$ for which $a_f(S) = 0$ for all the matrices S of rank smaller than m , and is denoted $[\Gamma_m, \mu]_0$.

Proposition 4.2. *Assume that, for all $m_0 \leq m$, and for all $S \in S_{m_0}^{>0}(\mathbb{R})$, the non empty sets L_S are t -designs. Then, the modular forms $\theta_{L,P}^{(m+1)}$ are cusp forms, when P is associated to a partition μ with either $\mu_{m+1} > 0$ or $\sum_{i=1}^m \mu_i \leq t$.*

Proof. If $S \in \text{Seven}_{m+1}^{\text{even}}$ is such that $S_{m+1,m+1} = 0$, and if $S = UU^t$, then the last row vector u_{m+1} of U equals 0. One has $AU = U$, with A the diagonal matrix with 1 on the diagonal except the last coefficient equals 0. If $P \in H_{m+1,n}^\mu$, $P(U) = P(AU) = \rho_\mu(A)P(U) = 0$ if $\mu_{m+1} > 0$ (in that case, \det divides ρ_μ). On the other hand, the polynomial P restricted to the matrix variables $X_{i,j}$ with $X_{m+1,j} = 0$ belongs to a subspace isomorphic as a $\text{GL}(m, \mathbb{R})$ -module to $F_m^{(\mu_1, \dots, \mu_m)}$, and is harmonic in these variables. Hence the design property implies that the coefficients of $\theta_{L,P}^{(m+1)}$ corresponding to matrices S with $S_{m+1,m+1} = 0$ and of rank m are equal to zero. We can iterate the same argument to obtain the nullity of the coefficients associated to matrices S of lower rank.

5. EVEN UNIMODULAR EXTREMAL LATTICES

Let L be an even unimodular lattice of dimension $n = 24q + 8r$ ($r = 0, 1, 2$). Since its theta series θ_L belongs to the space $[\Gamma_1, n/2]$, and since, as is well-known, the algebra of modular forms $A(\Gamma_1) = \mathbb{C}[E_4, E_6]$, the following bound holds for the minimum of L :

$$(9) \quad \min(L) \leq 2\lfloor n/24 \rfloor + 2$$

A lattice is called (analytically) *extremal*, if its minimum attains this bound. This notion can be defined for other families of lattices, see the nice survey paper [10]. Extremal even unimodular lattices are only known for $n = 8, 16, 24, 32, 40, 48, 56, 64, 80$ and are completely determined only up to

$n = 24$ (where the unique Leech lattice satisfies this bound). In dimension 32, they form a huge family, among which 5 of them are constructed from extremal binary codes. In dimension 48, which is the first dimension for the minimum 6, only three of them are known. The question of the existence of such a lattice in dimension 72 (hence of minimum 8) is still opened.

Let $S \in S_m^{>0}(\mathbb{R})$, we denote $\min(S) := \min\{xSx^t, x \in \mathbb{Z}^m, x \neq 0\}$. Let f be a non zero cusp form; we define $m(f) := \frac{1}{2} \min\{\min(S) \mid a_f(S) \neq 0\}$. We set $m(0) = +\infty$. For example, if $f = \theta_{L,P}^{(m)}$, clearly $m(f) \geq \min(L)/2$. In the case of degree one, due to the explicit description of $[\Gamma_1, k]$, it is easy to see that:

$$(10) \quad \text{if } f \neq 0, \quad m(f) \leq k/12$$

where k is the weight of f . Applied to the forms $f = \theta_{L,P}^{(1)}$, it leads to the result, due to Boris Venkov, that the sets L_S associated to extremal lattices (here $L_S = L_{(a)}$ is the set of lines supporting lattice vectors of given norm a) support designs of strength $10 - 4r$. We introduce the following notation:

$$(11) \quad \min([\Gamma_m, \mu]_0) := \max\{\min(f) \mid f \in [\Gamma_m, \mu]_0\}.$$

We now consider the question of the generalization of this result to the higher degree Grassmannian designs contained in extremal even unimodular lattices. For the E_8 lattice and the Leech lattice, the properties of their automorphism groups prove that they do contain respectively 6- and 10-Grassmannian designs (see [2]). So, the first interesting case is the case of dimension 32.

We now restrict to the case $m = 2$, and give the numerical results obtained by the explicit calculations of the spaces $[\Gamma_2, \mu]_0$ for $\rho_\mu = \det^{16} \otimes \rho_\nu$, where ν runs over partitions of small degree. A formula for the dimensions of these spaces is given in [13].

$ \nu $	0	2	4	6	8	10
ν	(0)	(2, 0)	(4, 0)	(6, 0)	(8, 0)	(10, 0)
$\dim([\Gamma_m, \mu]_0)$	2	2	3	5	7	8
$\min([\Gamma_m, \mu]_0)$		2	2	2	2(?)	2(?)
ν			(2, 2)	(4, 2)	(6, 2)	(8, 2)
$\dim([\Gamma_m, \mu]_0)$			2	2	4	7
$\min([\Gamma_m, \mu]_0)$			2	2	2	4
ν					(4, 4)	(6, 4)
$\dim([\Gamma_m, \mu]_0)$					3	3
$\min([\Gamma_m, \mu]_0)$					4	2

Corollary 5.1. *For all 32-dimensional even unimodular lattices of minimum 4 and all S of rank ≤ 2 the non-empty sets L_S are 6-designs.*

REFERENCES

- [1] C. Bachoc, E. Bannai, R. Coulangeon, *Codes and designs in Grassmannian spaces*
- [2] C. Bachoc, R. Coulangeon, G. Nebe, *Designs in Grassmannian spaces and lattices*, J. Algebraic Combinatorics **16** (2002), 5-19
- [3] C. Bachoc and B. Venkov, *Modular forms, lattices and spherical designs*, in "Réseaux euclidiens, "designs" sphériques et groupes", J. Martinet, éd., *L'Enseignement Mathématique*, Monographie n° 37", Genève (2001), 87-111.
- [4] E. Freitag, "Siegelsche Modulfunktionen", Springer-Verlag, 1983.
- [5] E. Freitag, *Thetareihen mit harmonischen Koeffizienten zur Siegelschen Modulgruppe*, Math. Ann. **254** (1980), 27-51.
- [6] R. Goodman and N. R. Wallach, *Representations and invariants of the classical groups*, Encyclopedia of Mathematics and its Applications **68**, Cambridge University Press, 1998.
- [7] T. Ibukiyama *Vector valued Siegel modular forms of $\det^k \text{Sym}(4)$ and $\det^k \text{Sym}(6)$* , preprint.
- [8] A.T. James and A.G. Constantine, *Generalized Jacobi polynomials as spherical functions of the Grassmann manifold*, Proc. Loudon Math. Soc. (3) **29** (1974), 174-192.
- [9] C. Poor and D.S. Yuen *Linear dependence among Siegel modular forms* Math. Ann. **318** (2000), 205-234.
- [10] R. Scharlau, R. Schulze-Pillot, *Extremal lattices* In Algorithmic algebra and number theory. edited by B. H. Matzat, G. M. Greuel, G. Hiss. Springer (1999), 139-170. Preprint available under www.matha.mathematik.uni-dortmund.de/preprints/welcome.html
- [11] R. Salvati Manni, *Slope of cusp forms and theta series*, Journal of Number Theory **83** (2000), 282-296.
- [12] T. Satoh, *On certain vector-valued Siegel modular forms of degree two*, Math. Ann. **274** (1986), 335-352.
- [13] R. Tsushima, *An explicit dimension formula for the spaces of generalized Siegel modular forms with respect to $Sp(2, \mathbb{Z})$* , Proc. Japan Acad. Ser. A Math. Sci. (59)4 (1983), 139-142.
- [14] B. Venkov, *Réseaux et designs sphériques*, in "Réseaux euclidiens, "designs" sphériques et groupes, J. Martinet, éd., *L'Enseignement Mathématique*, Monographie n° 37", Genève (2001), to appear.
- [15] B. Venkov, *Even unimodular extremal lattices*, Proc. Steklov Inst. Math. **165** (1984), 47-52.
- [16] R. Weissauer, *Vektorwertige Siegelsche Modulformen kleinen Gewichtes*, Crelle **343** (1983), 184-202.

C. BACHOC, LABORATOIRE A2X, UNIVERSITÉ BORDEAUX I, 351, COURS DE LA LIBÉRATION, 33405 TALENCE FRANCE

E-mail address: bachoc@math.u-bordeaux.fr

G. NEBE, ABTEILUNG REINE MATHEMATIK, UNIVERSITÄT ULM, 89069 ULM, GERMANY

E-mail address: nebe@mathematik.uni-ulm.de

Artin L-Functions of Graph Coverings

Audrey Terras
U.C.S.D.

Summer, 2002

Part 0. Outline.

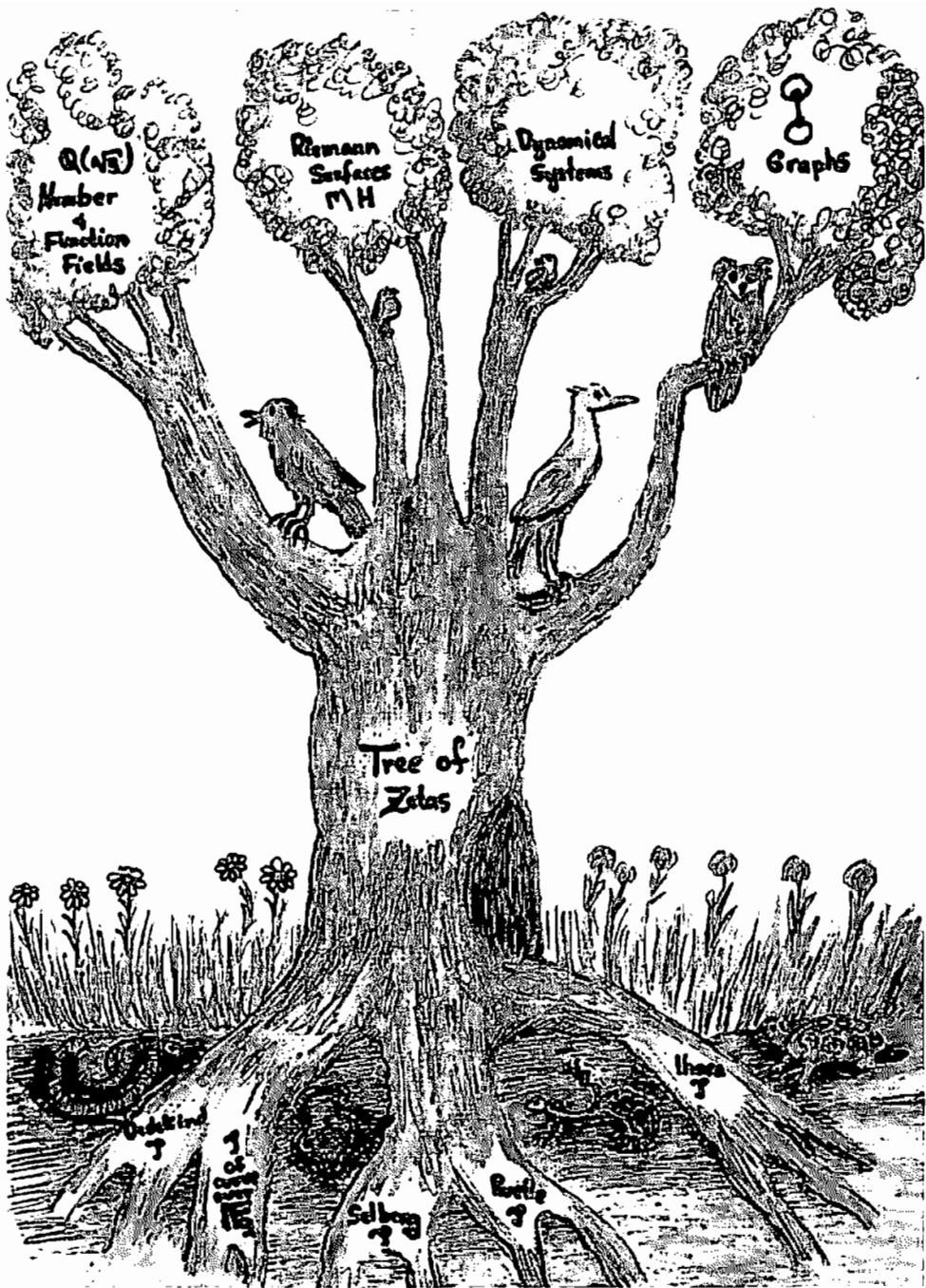
The goal of this talk is to provide an introduction to my joint papers with Harold Stark on zeta and L-functions of graph coverings [*Advances in Math.*, 121 (1996) and 154 (2000)]. The motivation is to treat the graph zeta functions the same way as the number theory analogs. This requires a discussion of the graph theoretic version of Galois theory which is to be found in the 2nd Advances paper. Here we will not discuss the Galois theory but instead focus on examples and computation. The following picture shows the tree of zetas with the zetas appearing as roots of the tree. The branches indicate the parallel fields that benefit from these roots. Here we consider only the 2 fields of algebraic number theory and graph theory. In part 1, we discuss zeta and L-functions of algebraic number fields. More details for part 1 can be found in

H. M. Stark, Galois theory, algebraic number theory & zeta functions, in *From Number Theory to Physics* (editors M. Waldschmidt et al), Springer-Verlag, 1992.

In part 2, the graph theory analogs are to be found. There are actually 3 kinds of graph zetas (vertex, edge and path). We will attempt to extol the computational advantages of the path zetas. The path and edge zetas have many variables and do not appear to have number theory analogs as yet.

Some History.

The theory of zeta functions of algebraic number fields was developed by Riemann (mid 1800s) for the rational number field, then Dedekind, Dirichlet, Hecke, Takagi, and Artin (early 1900s). Graph zeta functions appeared first from the point of view of p-adic groups in work of Ihara in the mid 1960s. Then Serre realized the graph theory interpretation. Papers of Sunada, Hashimoto and Bass further developed the theory. In particular, see Hashimoto, *Adv. Stud. Pure Math.*, 15, Academic, 1989, pages 211-280. More references can be found in the Advances papers mentioned above, as well as my book, *Fourier Analysis on Finite Groups and Applications*, Cambridge, 1999.



Part I. The Algebraic Number Theory Zoo of Zetas.

Riemann zeta, for $\text{Re}(s) > 1$,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p=\text{prime}} (1 - p^{-s})^{-1}.$$

- Riemann extended to all complex s with pole at $s=1$.
- Functional equation relates value at s and $1-s$
- Riemann hypothesis
- duality between primes and complex zeros of zeta
- prime number theorem
- See Davenport, *Multiplicative Number Theory*.

Dedekind zeta of algebraic number field $K=\mathbb{Q}(\theta)$

θ a root of a polynomial with coefficients in \mathbb{Q}

prime = prime ideal \mathfrak{p} in \mathcal{O}_K , ring of integers of K

infinite product of terms $(1 - N_{\mathfrak{p}}^{-s})^{-1}$,

where $N_{\mathfrak{p}} = \text{norm of } \mathfrak{p} = \#(\mathcal{O}_K/\mathfrak{p})$

prime ideal theorem

S

associated to a compact Riemannian manifold $M = \Gamma \backslash H$
 $H =$ upper half plane with $ds^2 = (dx^2 + dy^2)y^{-2}$

$\Gamma =$ discrete subgroup of group of real fractional linear transformations

primes = primitive closed geodesics C in M
of length $v(C)$
(primitive means only go around once)

Duality between spectrum of Laplacian Δ on M & lengths closed geodesics in M

$$Z(s) = \prod_{[C]} \prod_{j \geq 0} (1 - e^{-(s+j)v(C)})$$

Riemann hypothesis known to hold

Prime geodesic theorem

$Z(s+1)/Z(s)$ is a closer analog of $\zeta(s)$

We won't say more about this zeta here.

References:

D. Hejhal, *Duke Math. J.*, 43 (1976); A. Terras, *Harmonic Analysis on Symmetric Spaces & Applics.*, I, Springer, 1985

Example 1. Quadratic Extension

field	ring	prime ideal	finite field
		$g = \# \text{ of such } p$	
$K = \mathbb{Q}(\sqrt{2})$	$O_K = \mathbb{Z}[\sqrt{2}]$	$\mathfrak{p} \supset \mathfrak{p}O_K$	O_K / \mathfrak{p}
2			$f = \text{degree}$
F = \mathbb{Q}	\mathbb{Z}	$\mathfrak{p}\mathbb{Z}$	$\mathbb{Z}/\mathfrak{p}\mathbb{Z}$

3 CASES

1) **p inert:** $f=2$. $\mathfrak{p}O_K = \text{prime ideal}$, $2 \not\equiv x^2 \pmod{p}$

2) **p splits:** $g=2$. $\mathfrak{p}O_K = \mathfrak{p}\mathfrak{p}'$, $2 \equiv x^2 \pmod{p}$

3) **p ramifies:** $e=2$. $\mathfrak{p} = \mathfrak{p}^2$, $\mathfrak{p} = 2$

$\text{Gal}(K/F) = \{1, -1\}$,

Frobenius automorphism = Legendre Symbol =

$$\left(\frac{2}{p}\right) = \begin{cases} -1, & \text{in case 1} \\ 1, & \text{in case 2} \\ 0, & \text{in case 3} \end{cases}$$

p odd implies p has 50% chance of being in Case 1

Zeta and L-Functions for Example 1

Dedekind Zeta

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1} \quad \text{product over prime ideals in } O_K$$

Riemann Zeta

$$\zeta_{\mathbb{Q}}(s) = \prod_p (1 - Np^{-s})^{-1} \quad \text{product over primes in } \mathbb{Z}$$

Dirichlet L-Function

$$L(s, \chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}, \quad \text{where } \chi(p) = \left(\frac{2}{p}\right)$$

product over primes in \mathbb{Z}

Factorization

$$\zeta_{\mathbb{Q}(\sqrt{2})}(s) = \zeta_{\mathbb{Q}}(s)L(s, \chi)$$

Functional Equations: $\zeta_K(s)$ related to $\zeta_K(1-s)$
Hecke

Values at 0: $\zeta_{\mathbb{Q}}(0) = -1/2, \quad \zeta_K(0) = -hR/w$

h = class number (measures how far O_K is from having unique factorization) = 1 for $\mathbb{Z}[\sqrt{2}]$

R = regulator (determinant of logs of units)
= $\log(1+\sqrt{2})$ when $K=\mathbb{Q}(\sqrt{2})$

w = number of roots of unity in K is 2, when $K=\mathbb{Q}(\sqrt{2})$

Statistics of Prime Ideals and Zeros

- ✱ from information on zeros of $\zeta_K(s)$ obtain
prime ideal theorem

$$\#\{\mathfrak{p} \text{ prime ideal in } \mathcal{O}_K \mid N\mathfrak{p} \leq x\} \sim \frac{x}{\log x}, \text{ as } x \rightarrow \infty$$

- ✱ there are an infinite number of primes such that $\left(\frac{2}{p}\right)=1$.
- ✱ Dirichlet theorem: there are an infinite number of primes p in the progression $a, a+d, a+2d, a+3d, \dots$, when $\text{g.c.d.}(a,d)=1$.
- ✱ **Riemann hypothesis still open:**
GRH or ERH: $\zeta_K(s)=0$ implies $\text{Re}(s)=1/2$,
assuming s is not real.

References: Lang or Neukirch, *Algebraic Number Theory*

See the **pulchritudinous primes** website for some interesting pictures made using programs involving primes, including prime island. The site belongs to Adrian J. F. Leatherland and the address is:

yoyo.cc.monash.edu.au/~bunyip/primes

Artin L-Functions

$K \supset F \supset \mathbb{Q}$ number fields with K/\mathbb{Q} Galois

$\mathcal{O}_K \supset \mathcal{O}_F \supset \mathbb{Z}$ rings of integers

$\mathcal{P} \supset \mathfrak{p} \supset \mathfrak{p}\mathbb{Z}$ prime ideals (\mathfrak{p} unramified,
i.e., \mathcal{P}^2 does not contain \mathfrak{p})

Frobenius Automorphism $\left(\frac{K/F}{\mathcal{P}}\right) = \sigma \in \text{Gal}(K/F)$

$$\sigma_{\mathcal{P}}(x) \equiv x^{N_{\mathfrak{p}}} \pmod{\mathcal{P}}, \text{ for } x \in \mathcal{O}_K,$$

when \mathfrak{p} is unramified.

$\sigma_{\mathcal{P}}$ determined by \mathfrak{p} up to conjugation if \mathcal{P}/\mathfrak{p} unramified
 $f(\mathcal{P}/\mathfrak{p}) = \text{order of } \sigma_{\mathcal{P}} = [\mathcal{O}_K/\mathcal{P} : \mathcal{O}_F/\mathfrak{p}]$

Artin L-Function for $s \in \mathbb{C}$, π is a representation of $\text{Gal}(K/F)$

$$L(s, \pi) = \prod_{\mathcal{P}} \left(1 - \pi \left(\frac{K/F}{\mathcal{P}} \right) N_{\mathcal{P}}^{-s} \right)^{-1}$$

where “=” means we only give the formula for unramified primes \mathfrak{p} of F . Here we pick \mathcal{P} a prime in \mathcal{O}_K dividing \mathfrak{p} ,

Applications

⌘ Factorization

$$\zeta_K(s) = \prod_{\substack{\pi \\ \text{irreducible} \\ \text{degree } d_\pi}} L(s, \pi)^{d_\pi}$$

⌘ Chebotarev Density Theorem

$\forall \sigma$ in $\text{Gal}(K/F)$, $\exists \infty$ -ly many prime ideals \mathfrak{p} of \mathcal{O}_F such that $\exists \mathfrak{P}$ in \mathcal{O}_K dividing \mathfrak{p} with Frobenius

$$\left(\frac{K/F}{\mathfrak{P}} \right) = \sigma$$

⌘ Artin Conjecture: $L(s, \pi)$ entire for non-trivial irreducible rep π

⌘ Stark Conjectures: π not containing trivial rep



$$\lim_{s \rightarrow 0} s^a L(s, \pi) = \Theta(\pi) * R(\pi)$$

= algebraic number * determinant of $a \times a$ matrix in linear forms with alg. coeffs. of logs of units of K and its conjugate fields $/\mathbb{Q}$.

References:

Stark's paper in *From Number Theory to Physics*, edited by Waldschmidt et al

Stark, Adv. in Math., *Advances in Math.*, 17 (1975), 60-92

Lang or Neukirch, *Algebraic Number Theory*

Chebotarev Density Theorem for K/\mathbb{Q} normal.

For a set S of rational primes, define the analytic density of S


$\lim_{s \rightarrow 1^+} \left(\frac{\sum_{p \in S} p^{-s}}{\log \frac{1}{s-1}} \right)$. In the following proof, one needs to know that

$L(s, \pi)$ continues to $s=1$ with no pole or zero if $\pi \neq 1$, while $L(s, 1) = \zeta(s)$ = Riemann zeta.

Theorem. For every conjugacy class C in $G = \text{Gal}(K/\mathbb{Q})$, the analytic density of the set of rational primes p such that $C(p)$ = the conjugacy class of the Frobenius auto of a prime ideal \mathfrak{P} of K dividing p is $|C|/|G|$.

Proof. Sum the logs of the Artin L -functions \times conjugate of characters χ_π over all irreducible reps π of G . As $s \rightarrow 1^+$,

$$\begin{aligned} \log \frac{1}{s-1} &\sim \sum_{\pi} \log L(s, \pi) \overline{\chi_{\pi}(C)} \\ &\sim \sum_{\pi} \sum_p \chi_{\pi}(C(p)) p^{-s} \overline{\chi_{\pi}(C)} \\ &\sim \frac{|G|}{|C|} \sum_{\substack{p \\ C(p)=C}} p^{-s} \end{aligned}$$

by the orthogonality relations of the characters of the irreducible representations π of G . Here $C(p)$ denotes the conjugacy class of the Frobenius auto of the prime of K above p . 

Example 2. Galois Extension of Non-normal Cubic

field	ring	prime ideal	finite field
$g(P/\mathfrak{p}) = \# \text{ of such } P$			
$K = \mathbb{F}(e^{2\pi i/3})$	\mathcal{O}_K	\mathfrak{P}	$\mathcal{O}_K/\mathfrak{P}$
3			
$F = \mathbb{Q}(\sqrt[3]{2})$	\mathcal{O}_F	\mathfrak{p}	$\mathcal{O}_F/\mathfrak{p}$
2			
\mathbb{Q}	\mathbb{Z}	$\mathfrak{p}\mathbb{Z}$	$\mathbb{Z}/\mathfrak{p}\mathbb{Z}$
$f(P/\mathfrak{p}) = \text{degree}(\mathcal{O}_K/\mathfrak{P} : \mathcal{O}_F/\mathfrak{p})$			

More details are in Stark's article in *From Number Theory to Physics*, edited by Waldschmidt et al

Splitting of Rational Primes in \mathcal{O}_F

Type 1. $\mathfrak{p}\mathcal{O}_F = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$, with distinct \mathfrak{p}_i of degree 1 ($\mathfrak{p}=31$ is 1st example), Frobenius of prime P above \mathfrak{p}_i has order 1
density 1/6 by Chebotarev

Type 2. $\mathfrak{p}\mathcal{O}_F = \mathfrak{p}_1 \mathfrak{p}_2$, with \mathfrak{p}_1 of degree 1, \mathfrak{p}_2 of degree 2 ($\mathfrak{p}=5$ is 1st example), Frobenius of prime P above \mathfrak{p}_1 has order 2
density 1/2 by Chebotarev

Type 3. $\mathfrak{p}\mathcal{O}_F = \mathfrak{p}$, with \mathfrak{p} of degree 3, ($\mathfrak{p}=7$ is 1st example), Frobenius of P above \mathfrak{p}_i has order 3
density 1/3 by Chebotarev

Part II. The Graph Theory Zoo of Zetas

References:

- Harold M. Stark and Audrey Terras, *Adv. in Math.*, Vol. 121 (1996); Vol. 154 (2000)
- K. Hashimoto, *Internatl. J. Math.*, 1992, Vol.3.

Definitions.

Graph Y an unramified covering of Graph X
means (assuming no loops or multiple edges)
 $\pi: Y \rightarrow X$ is an onto graph map such that
for every $x \in X$ & for every $y \in \pi^{-1}(x)$,
 π maps the points $z \in Y$ adjacent to y
1-1, onto the points $w \in X$ adjacent to x .

Normal d -sheeted Covering means:

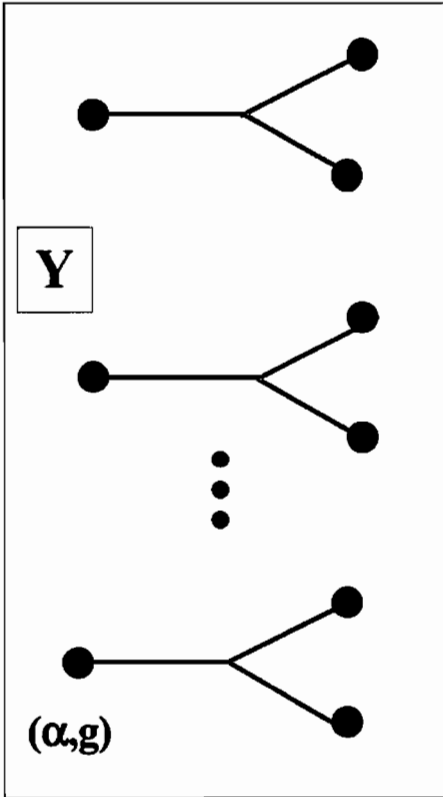
$\exists d$ graph isomorphisms

g_1, \dots, g_d mapping $Y \rightarrow Y$

such that $\pi g_j(y) = \pi(y)$ for all $y \in Y$

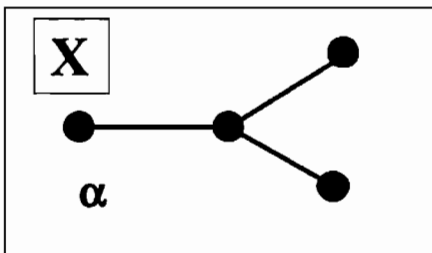
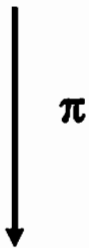
The Galois group $G(Y/X) = \{g_1, \dots, g_d\}$.

Note: We do not assume graphs are regular!



How to label points on Y covering X with Galois group $G = \text{Gal}(Y/X)$

Second make $n = |G|$ copies of the tree in X. These are the sheets of Y. Label the sheets with $g \in G$. Then
 $g(\text{sheet } h) = \text{sheet}(gh)$
 $g(\alpha, h) = (\alpha, gh)$
 $g(\text{path from } (\alpha, h) \text{ to } (\beta, j)) = \text{path from } (\alpha, gh) \text{ to } (\beta, gj)$

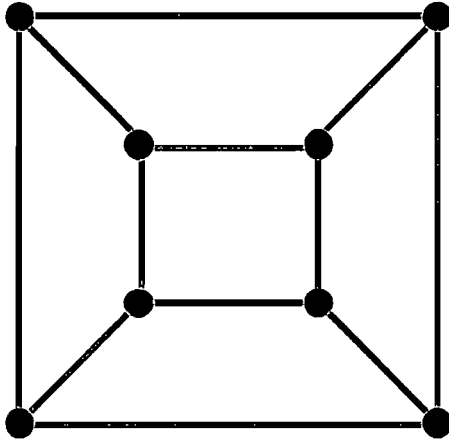


First pick a spanning tree in X (no cycles, connected, includes all vertices of X).

Example 1. Quadratic Cover

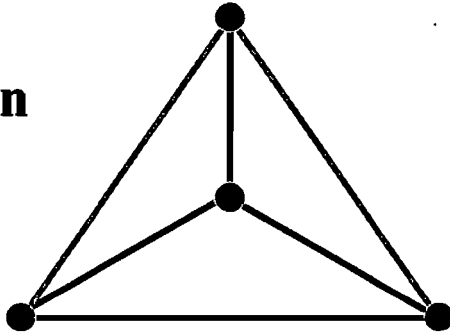
This is analogous to Example 1 in Part 1.

Cube



covers

Tetrahedron



Spanning Tree in X is red.
Corresponding sheets of Y are also red

**"PRIMES in GRAPHS" are
equivalence classes of closed backtrackless
tailless primitive paths**

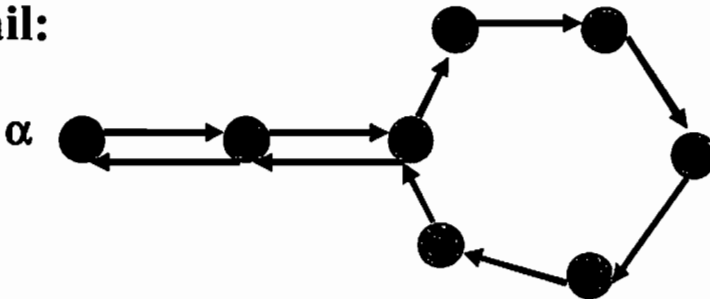
DEFINITIONS

backtrack



equivalence class: change starting point

tail:

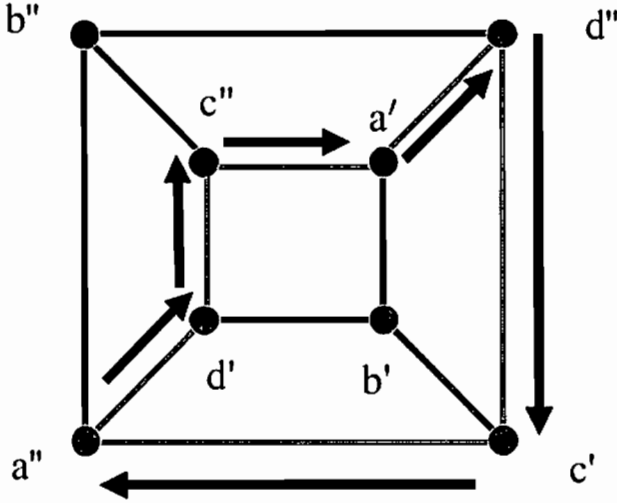


Here α is the start of the path

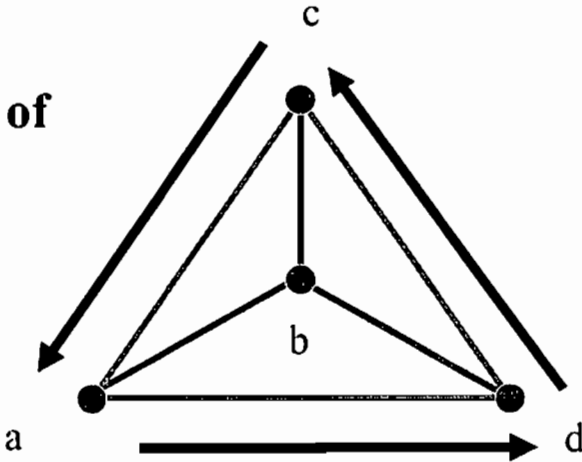
**non-primitive: go around path more than
once**

Example of Splitting of Primes in Quadratic Cover, $f=2$

D
prime
above
C of
length 6

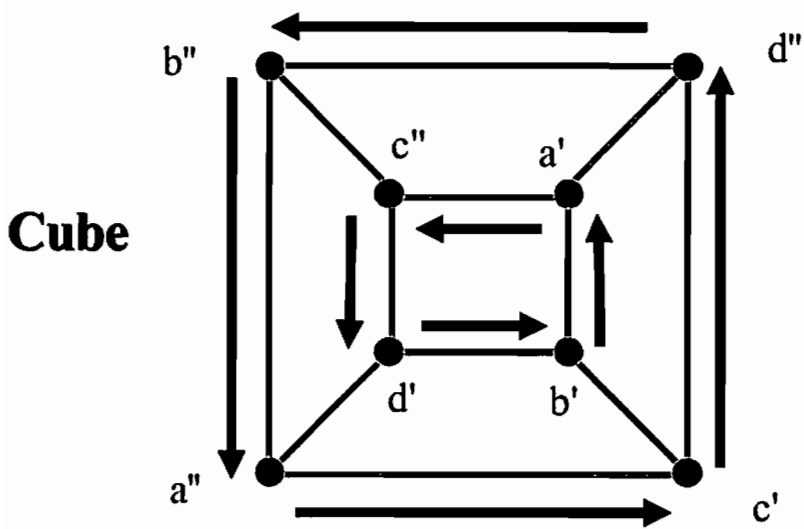


C prime of
length 3

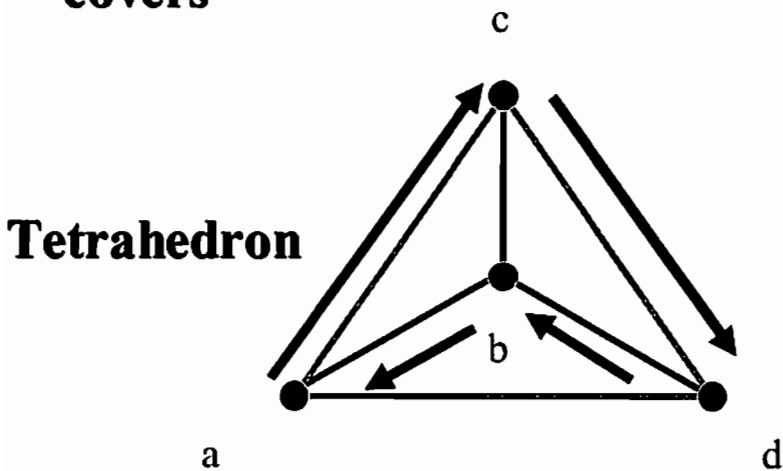


Picture of Splitting of Prime
which is inert; i.e., $f=2$, $g=1$, $e=1$
1 prime cycle **D** above, & **D** is lift of C^2 .

**Example of Splitting of Primes
in Quadratic Cover, $g=2$**



covers



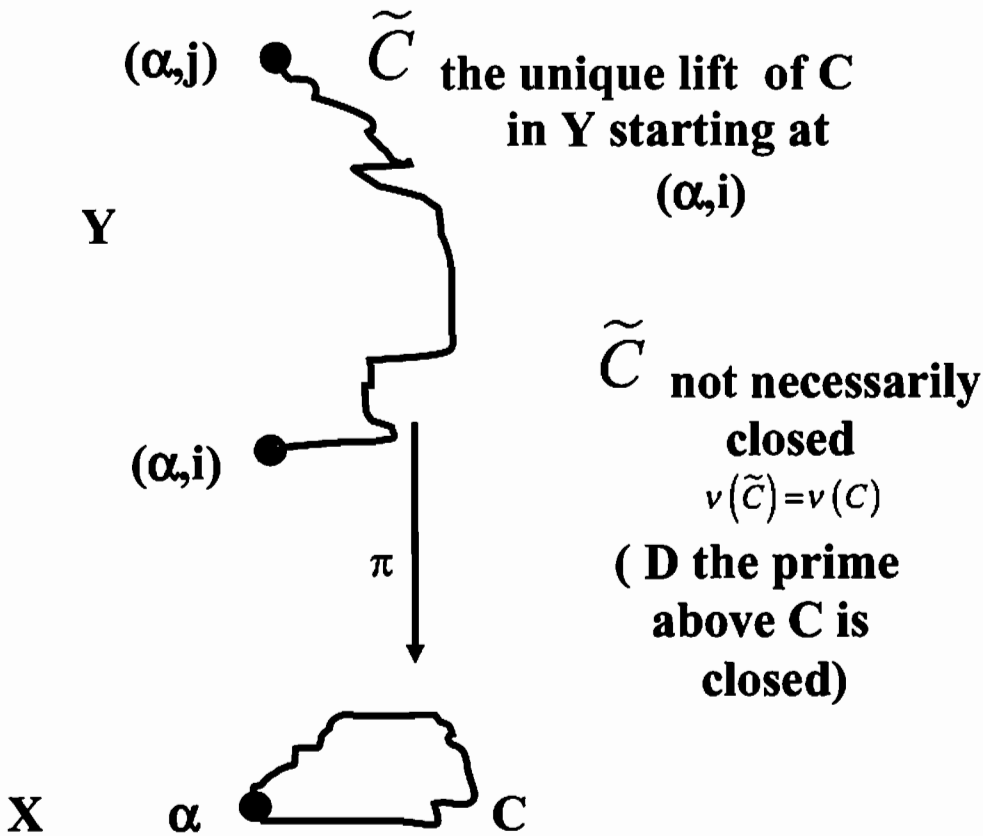
Picture of Splitting of Prime which splits
completely; i.e., $f=1$, $g=2$, $e=1$
2 primes cycles above

FROBENIUS AUTOMORPHISM

C a “prime” in X , D a prime over C in Y

$$\text{Frob}(D) = \left(\frac{Y/X}{D} \right) = ji^{-1} \in G = \text{Gal}(Y/X)$$

where ji^{-1} maps sheet i to sheet j



Exercise: Compute $\text{Frob}(D)$ on preceding pages, $G = \{1, g\}$.

Answers:
 preceding page: 1.
 page before that: g

Properties of Frobenius

- 1) Replace (α, i) with (α, hi) . Then $\text{Frob}(D) = ji^{-1}$ is replaced with $hji^{-1}h^{-1}$. Conjugacy class of $\text{Frob}(D) \in \text{Gal}(Y/X)$ does not change.
- 2) Varying α does not change $\text{Frob}(D)$.
- 3) $\text{Frob}(D)^j = \text{Frob}(D)^j$.

Artin L-Function

ρ = representation of $G = \text{Gal}(Y/X)$, $u \in \mathbb{C}$, $|u|$ small

$$L(u, \rho, Y/X) = \prod_{[C]} \det \left(1 - \rho \left(\frac{Y/X}{D} \right) u^{v(C)} \right)^{-1}$$

$[C]$ = equivalence class of primes of X

$v(C)$ = length C , D a prime in Y over C

Properties of Artin L-Functions

Copy from Lang, *Algebraic Number Theory*

1) $L(u, 1, Y/X) = \zeta(u, X)$
= Ihara zeta function of X
(our analogue of the Dedekind zeta
function, also Selberg zeta function)

2)

$$\zeta(u, Y) = \prod_{\rho \in \widehat{G}} L(u, \rho, Y/X)^{d_\rho}$$

product over all irred. reps of G ,

$d_\rho = \text{degree } \rho$

3) You can prove $\zeta(u, X)^{-1}$ divides $\zeta(u, Y)^{-1}$
directly and you don't need to assume
 Y/X Galois.

Thus the analog of the Dedekind
conjecture for zetas of algebraic number
fields is proved easily for graph zetas.

Ihara Theorem for L-Functions

$$L(u, \rho, Y / X)^{-1}$$

$$= (1 - u^2)^{(r-1)d_\rho} \det(I' - A'_\rho u + Q' u^2)$$

r = rank fundamental group of $X = |E| - |V| + 1$

ρ = representation of $G = \text{Gal}(Y/X)$, $d = d_\rho = \text{degree } \rho$

Definitions. $n \times n$ matrices A', Q', I' , $n = |X|$

$n \times n$ matrix $A(g)$, $g \in \text{Gal}(Y/X)$,

has entry for $\alpha, \beta \in X$ given by

$$(A(g))_{\alpha, \beta} = \# \{ \text{edges in } Y \text{ from } (\alpha, e) \text{ to } (\beta, g) \}$$

Here $e = \text{identity of } G$.

$$A'_\rho = \sum_{g \in G} A(g) \otimes \rho(g)$$

$Q = \text{diagonal matrix, } j\text{th diagonal entry}$

$= q_j = (\text{degree of } j\text{th vertex in } X) - 1,$

$$Q' = Q \otimes I_d,$$

$I' = I_{nd} = \text{identity matrix.}$

Proof can be found in Stark and Terras, *Advances in Math.*, Vol. 154 (2000)

NOTES FOR REGULAR GRAPHS mostly

✚ Another proof uses Selberg trace formula on tree to prove Ihara's theorem. For case of trivial representation, see A.T., *Fourier Analysis on Finite Groups & Applies*; for general case, see and Venkov & Nikitin, *St. Petersburg Math. J.*, 5 (1994)

✚ $\left(\frac{1}{\zeta_X}\right)^{(r)}(0) = (-1)^{r+1} 2^r (r-1) \kappa(X)$, where $\kappa(X)$ = the number of spanning trees of X, the complexity

✚ Ihara zeta has functional equations relating value at u and $1/(qu)$, $q = \text{degree} - 1$

✚ Riemann Hypothesis, for case of trivial representation (poles), means graph is Ramanujan i.e., non-trivial spectrum of adjacency matrix is contained in the spectrum for the universal covering tree which is the interval $(-2\sqrt{q}, 2\sqrt{q})$ [see Lubotzky, Phillips & Sarnak, *Combinatorica*, 8 (1988)]

✚ RH is true for most graphs but it can be false

✚ Hashimoto [Adv. Stud. Pure Math., 15 (1989)] proves Ihara ζ for certain graphs is essentially the ζ function of a Shimura curve over a finite field

The Prime Number Theorem

Let $\pi_X(m)$ denote the number of prime path equivalence classes $[C]$ in X where the length of C is m . Assume X is finite connected $(q+1)$ -regular. Since $1/q$ is the absolute value of the closest pole(s) of $\zeta(u, X)$ to 0, then

$$\pi_X(m) \sim q^m/m \text{ as } m \rightarrow \infty.$$

The proof comes from the method of generating functions (See Wilf, *generatingfunctionology*) and the fact that (as in Stark & Terras, *Advances in Math*, 121 & 154):

$$u \frac{d}{du} \log \zeta(u, X) = \sum_{m=1}^{\infty} n_X(m) u^m$$

Here $n_X(m)$ is the number of closed paths C in X of length m without backtracking or tails.

Note: When X is not regular, we could define q to be the reciprocal of the absolute value of the closest pole(s) of zeta to 0.

EXAMPLE 1. Y=cube, X=tetrahedron

$$|X|=4, \quad |Y|=8, \quad r=3, \quad G = \{e, g\}$$

representations of G are 1 and ρ : $\rho(e) = 1, \rho(g) = -1$

$$I' = I_4, \quad Q' = 2I_4,$$

$$A(e)_{u,v} = \#\{\text{length 1 paths } u' \text{ to } v' \text{ in } Y\}$$

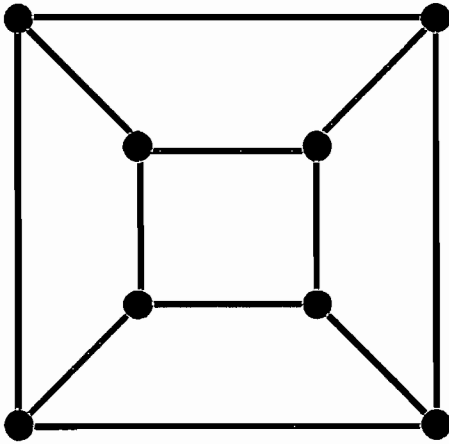
$$A(g)_{u,v} = \#\{\text{length 1 paths } u' \text{ to } v'' \text{ in } Y\}$$

$$A(e) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \quad A(g) = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

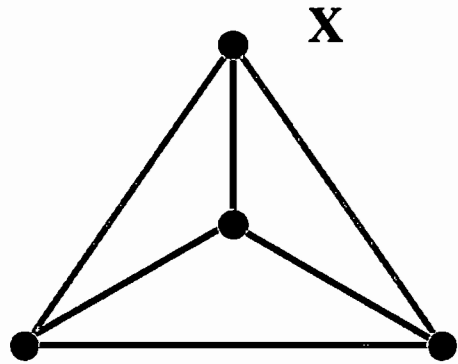
$A'_1 = A =$ adjacency matrix of X

$$A'_\rho = A(e) - A(g) = \begin{pmatrix} 0 & 1 & -1 & -1 \\ 1 & 0 & 1 & 1 \\ -1 & 1 & 0 & -1 \\ -1 & 1 & -1 & 0 \end{pmatrix}$$

Zeta and L-Functions of Cube & Tetrahedron



Y



X

$$\ast \zeta(u, Y)^{-1} = L(u, \rho, Y/X)^{-1} \zeta(u, X)^{-1}$$

$$\ast L(u, \rho, Y/X)^{-1} = (1-u^2)(1+u)(1+2u)(1-u+2u^2)^3$$

$$\ast \zeta(u, X)^{-1} = (1-u^2)^2(1-u)(1-2u)(1+u+2u^2)^3$$

$$\ast \text{roots of } \zeta(u, X)^{-1} \text{ are } 1, 1, 1, \frac{1}{2}, r, r, r$$

where $r = (-1 \pm \sqrt{-7})/4$ and $|r| = 1/\sqrt{2}$

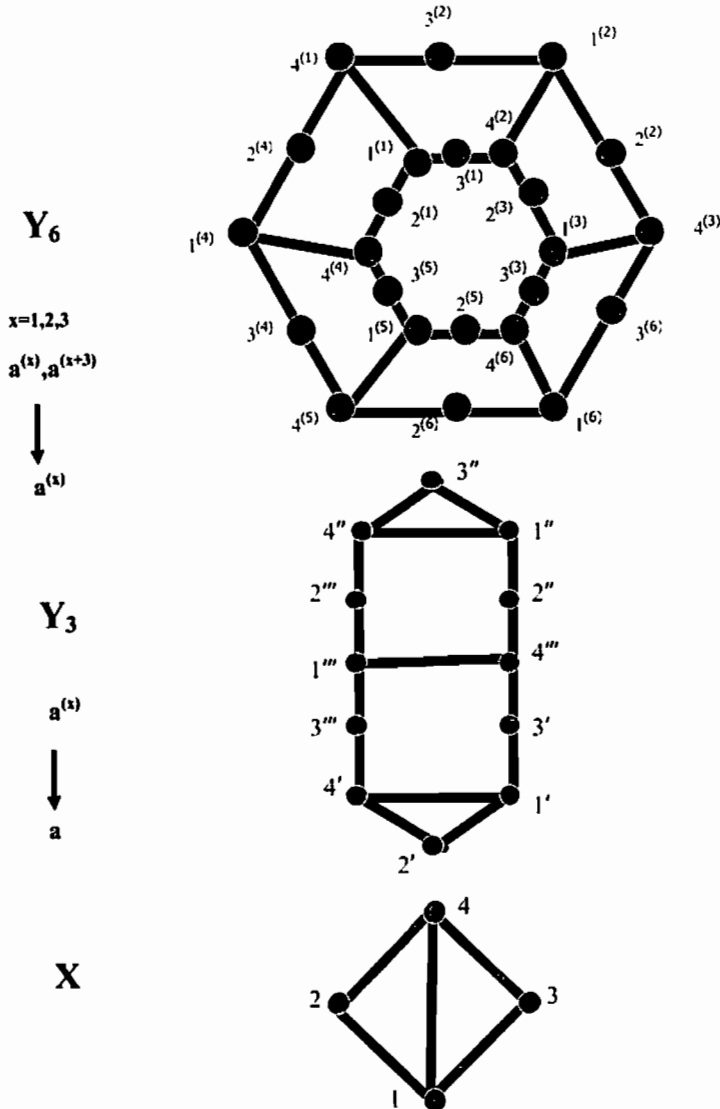
\ast The pole of $\zeta(u, X)$ closest to 0 governs the prime number theorem discussed a few pages back. It is $1/q=1/2$. The coefficients of the following generating function are the numbers of closed paths without backtracking or tails of the indicated length

$$u \frac{d}{du} \log \zeta(u, X) = 24u^3 + 24u^4 + 96u^6 + 168u^7 + 168u^8 + 528u^9 + 1200u^{10} + 1848u^{11} + O(u^{12})$$

So there are 8 primes of length 3 in X, for example.

Example 2. Galois Cover of Non-Normal Cubic

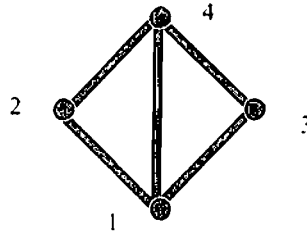
This example is analogous to example 2 in part 1.



$G=S_3$, $H=\{(1),(23)\}$ fixes Y_3 . $a^{(1)}=(a,(1))$, $a^{(2)}=(a,(13))$, $a^{(3)}=(a,(132))$,
 $a^{(4)}=(a,(23))$, $a^{(5)}=(a,(123))$, $a^{(6)}=(a,(23))$

Here we use the standard cycle notation for elements of the symmetric group.

**3 classes of primes
in base graph X
from preceding
page**



✚ **Class C1** path in X (list vertices)
14312412431

$f=1, g=3$ 3 lifts to Y_3

1'4'3'''1'''2'''4'1''2''4'''3'1'

1''4''3''1''2''4'''1'''2'''4''3''1''

1'''4'''3'1'2'4'1'2'4'3'''1'''

Frobenius trivial \Rightarrow density $1/6$

✚ **Class C2** path in X (list vertices) 1241
2 lifts to Y_3

1'2'4'1' $f=1$

1''2''4'''1'''2'''4'1'' $f=2$

Frobenius order 2 \Rightarrow density $1/2$

✚ **Class C3** path in X (list vertices)
12431

$f=3$ 1 lift to Y_3

1'2'4'3'''1'''2'''4''3''1''2''4'''3'1'

Frobenius order 3 \Rightarrow density $1/3$

Ihara Zeta Functions

$$\boxtimes \zeta(u, X)^{-1} = (1-u^2)(1-u)(1+u^2)(1+u+2u^2)(1-u^2-2u^3)$$

$$\boxtimes \zeta(u, Y_3)^{-1} = \zeta(u, X)^{-1} (1-u^2)^2(1-u-u^3+2u^4) \\ \times (1-u+2u^2-u^3+2u^4)(1+u+u^3+2u^4) \\ \times (1+u+2u^2+u^3+2u^4)$$

$$\boxtimes \zeta(u, Y_6)^{-1} = \zeta(u, Y_3)^{-1} (1-u^2)^8(1+u)(1+u^2)(1-u+2u^2) \\ \times (1-u^2+2u^3)(1-u-u^3+2u^4)(1-u+2u^2-u^3+2u^4) \\ \times (1+u+u^3+2u^4)(1+u+2u^2+u^3+2u^4)$$

It follows that, as in the number theory analog,

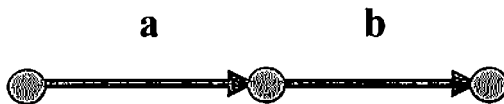
$$\zeta(u, X)^2 \zeta(u, Y_6) = \zeta(u, Y_2) \zeta(u, Y_3)^2$$

Here Y_2 is an intermediate quadratic extension between Y_6 and X . See Stark and Terras, *Adv. in Math.*, 154 (2000), Figure 13, for a discussion.

The poles of $\zeta(u, X)$ are $u=1, 1, -1, \pm i, (-1 \pm \sqrt{7}i)/4, w, w, 1/q$ Where $w, 1/q$ are roots of the cubic. The closest pole to 0 is $1/q$. And q is approximately 1.5214. So the prime number theorem gives a considerably smaller main term, q^m/m , for this graph X than for K_4 , where $q=2$.

Multiedge Artin L-Functions

Orient the edges of the graph. Multiedge matrix W has ab entry $w(a,b)=w_{ab}$ in C , if the edges a and b look like



Otherwise set $w_{ab}=0$ Define for closed path $C=a_1a_2\dots a_s$,

$$N_E(C)=w(a_s,a_1)w(a_1,a_2)\dots w(a_{s-1},a_s)$$

$$L_E(W, \rho, Y/X) = \prod_{[C]} \left(1 - \rho \left(\frac{Y/X}{D} \right) N_E(C) \right)^{-1}$$

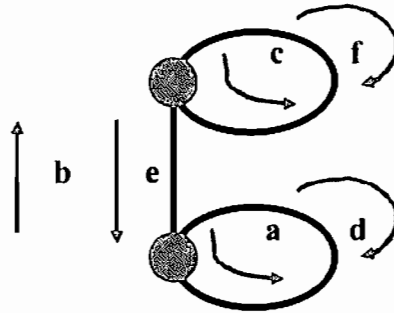
where the product is over primes $[C]$ of X and $[D]$ is any prime of Y over $[C]$

Properties

- $L_E(W, 1, Y/X) = \zeta_E(W, X)$, the edge zeta function
- $L_E(W, \rho)^{-1} = \det(I - W_\rho)$, where W_ρ is a $2|E| \times 2|E|$ block matrix with ij block given by $(w_{ij} \rho(\text{Frob}(e_i)))$
- Induction property
- Factorization of edge zeta as a product of edge L-functions
- specialize all $w_{ij}=u$ and get the Artin-Ihara vertex L function

$E \square \square \square \square \square$

**X=Dumbbell Graph
and Fission of an
Edge**



$$\zeta_E(W, X)^{-1} = \det \begin{pmatrix} w_{aa} - 1 & w_{ab} & 0 & 0 & 0 & 0 \\ 0 & -1 & w_{bc} & 0 & 0 & w_{bf} \\ 0 & 0 & w_{cc} - 1 & 0 & w_{ce} & 0 \\ 0 & w_{db} & 0 & w_{dd} - 1 & 0 & 0 \\ w_{ea} & 0 & 0 & w_{ed} & -1 & 0 \\ 0 & 0 & 0 & 0 & w_{fe} & w_{ff} - 1 \end{pmatrix}$$

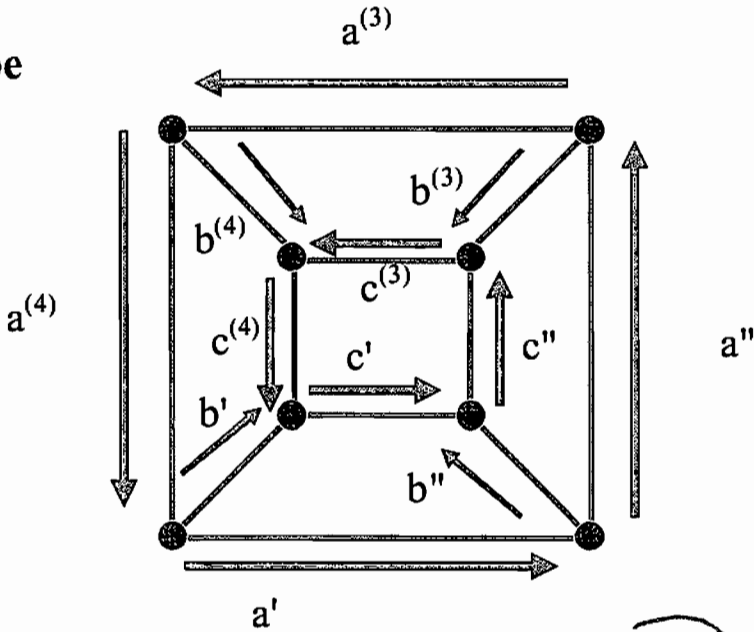
Here **b** and **e** are the vertical edges.

Specialize all variables with **b** and **e** to be 0 and get zeta function of subgraph with vertical edge removed - **Fission**

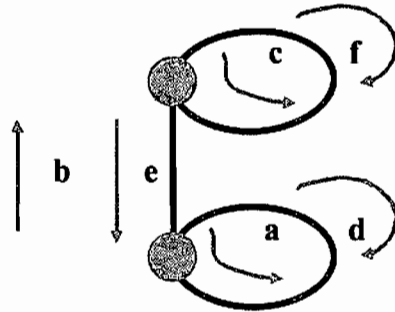
This gives the graph with just 2 disconnected loops.

Example 3. Cube Covering Dumbbell

Y=Cube



X=Dumbbell



$$\text{Gal}(Y/X) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\} \approx \mathbb{Z}/4\mathbb{Z}.$$

Identification sends σ_j to $j - 1 \pmod{4}$

The representations are 1-dimensional: $\pi_a(b) = i^{a(b-1)}$.

Galois group elements associated to edges a, b, c are

$$\text{Frob}(a) = \sigma_2, \quad \text{Frob}(b) = \sigma_1, \quad \text{Frob}(c) = \sigma_2.$$

Edge L-Functions for Example 3.

$$\zeta(W, X)^{-1} = L(W, 1, Y/X)^{-1} = \det \begin{pmatrix} w_{aa}-1 & w_{ab} & 0 & 0 & 0 & 0 \\ 0 & -1 & w_{bc} & 0 & 0 & w_{bf} \\ 0 & 0 & w_{cc}-1 & 0 & w_{ce} & 0 \\ 0 & w_{db} & 0 & w_{dd}-1 & 0 & 0 \\ w_{ca} & 0 & 0 & w_{cd} & -1 & 0 \\ 0 & 0 & 0 & 0 & w_{fe} & w_{ff}-1 \end{pmatrix}$$

$$L_{\varepsilon}(W, \pi_1, Y/X)^{-1} = \det \begin{pmatrix} iw_{aa}-1 & iw_{ab} & 0 & 0 & 0 & 0 \\ 0 & -1 & w_{bc} & 0 & 0 & w_{bf} \\ 0 & 0 & iw_{cc}-1 & 0 & iw_{ce} & 0 \\ 0 & -iw_{db} & 0 & -iw_{dd}-1 & 0 & 0 \\ w_{ca} & 0 & 0 & w_{cd} & -1 & 0 \\ 0 & 0 & 0 & 0 & -iw_{fe} & -iw_{ff}-1 \end{pmatrix}$$

$$L(W, \pi_2, Y/X)^{-1} = \det \begin{pmatrix} -w_{aa}-1 & -w_{ab} & 0 & 0 & 0 & 0 \\ 0 & -1 & w_{bc} & 0 & 0 & w_{bf} \\ 0 & 0 & -w_{cc}-1 & 0 & -w_{ce} & 0 \\ 0 & -w_{db} & 0 & -w_{dd}-1 & 0 & 0 \\ w_{ca} & 0 & 0 & w_{cd} & -1 & 0 \\ 0 & 0 & 0 & 0 & -w_{fe} & -w_{ff}-1 \end{pmatrix}$$

$$L(W, \pi_3, Y/X)^{-1} = \det \begin{pmatrix} -iw_{aa}-1 & -iw_{ab} & 0 & 0 & 0 & 0 \\ 0 & -1 & w_{bc} & 0 & 0 & w_{bf} \\ 0 & 0 & -iw_{cc}-1 & 0 & -iw_{ce} & 0 \\ 0 & iw_{db} & 0 & iw_{dd}-1 & 0 & 0 \\ w_{ca} & 0 & 0 & w_{cd} & -1 & 0 \\ 0 & 0 & 0 & 0 & iw_{fe} & iw_{ff}-1 \end{pmatrix}$$

Note that the product of these 6x6 determinants is the 24x24 determinant whose reciprocal is the multiedge zeta function of Y, the cube.

Path L-Functions

Here we discuss a new kind of L-function with smaller sized matrix determinants.

Fundamental Group of X can be identified with group generated by edges left out of a spanning tree

$$e_1, \dots, e_r, e_1^{-1}, \dots, e_r^{-1}$$

$2r \times 2r$ **multipath matrix** Z has ij entry

z_{ij} in C if $e_j \neq e_i^{-1}$ and $z_{ij} = 0$, otherwise.

Imitate the definition of the edge Artin L-functions.

Write a prime path as a reduced word in a conjugacy class

$$C = a_1 \cdots a_s, \text{ where } a_j \in \{e_1^{\pm 1}, \dots, e_r^{\pm 1}\}$$

and define the **path norm**

$$N_p(C) = z(a_s, a_1) \prod_{i=1}^{s-1} z(a_i, a_{i+1})$$

where $z(e_i, e_j) = z_{ij}$.

Define the **path zeta L-function**

$$L_p(Z, \pi, Y/X) = \prod_{[C]} \det \left(1 - \pi \left(\frac{Y/X}{D} \right) N_p(C) \right)^{-1}$$

Product is over prime cycles [C] in X

[D] is any prime of Y over [C]

Specializing Path L-Functions to Edge L-Functions

The path L-functions have analogous properties to the edge L-functions.

- * They are reciprocals of polynomials.
- * They provide factorizations of the path zeta functions.
- * The most important property is that of

Specialization to Path L-functions.

- edges left out of a spanning tree T of X: e_1, \dots, e_r
generate fundamental group of X
- inverse edges are $e_{r+1} = e_1^{-1}, \dots, e_{2r} = e_r^{-1}$
- edges of the spanning tree T are $t_1, \dots, t_{|X|-1}$
- with inverse edges $t_{|X|}, \dots, t_{2|X|-2}$

If $e_i \neq e_j^{-1}$, write the part of the path between e_i and e_j as the (unique) product $t_{k_1} \cdots t_{k_n}$

C is 1st a product of e_j (generators of the fundamental group), then a product of actual edges e_j and t_k .

Specialize the multipath matrix Z to $Z(W)$ with entries

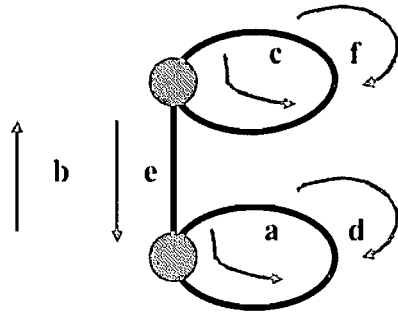
$$z_{ij} = w(e_i, t_{k_1}) w(t_{k_2}, e_j) \prod_{v=1}^{n-1} w(t_{k_v}, t_{k_{v+1}})$$

Then

$$L_P(Z(W), X) = L_E(W, X)$$

Example - the Dumbbell

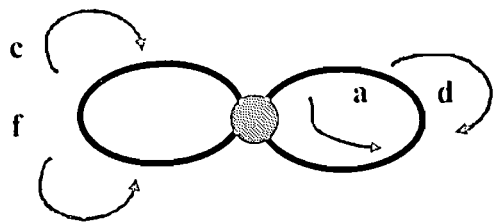
Recall the edge zeta was a 6x6 determinant.
 The specialized path zeta is only 4x4.
 Maple computes it much faster than the 6x6.



$$\zeta_E(W, X)^{-1} = \det \begin{pmatrix} w_{aa} - 1 & w_{ab} w_{bc} & 0 & w_{ab} w_{bf} \\ w_{ce} w_{ea} & w_{cc} - 1 & w_{ce} w_{ed} & 0 \\ 0 & w_{db} w_{bc} & w_{dd} - 1 & w_{db} w_{bf} \\ w_{fe} w_{ea} & 0 & w_{fe} w_{ed} & w_{ff} - 1 \end{pmatrix}$$

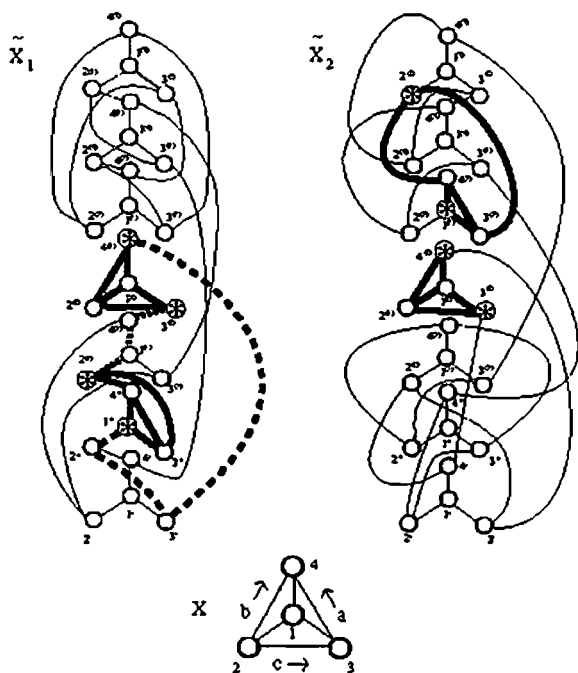
Fusion of an edge is now easy to do in the path zeta.

To obtain edge zeta of graph obtained from dumbbell graph, by fusing edges b and e,



Replace $w_{xb}w_{by}$ with w_{xy}

Replace $w_{xe}w_{ey}$ with w_{xy}

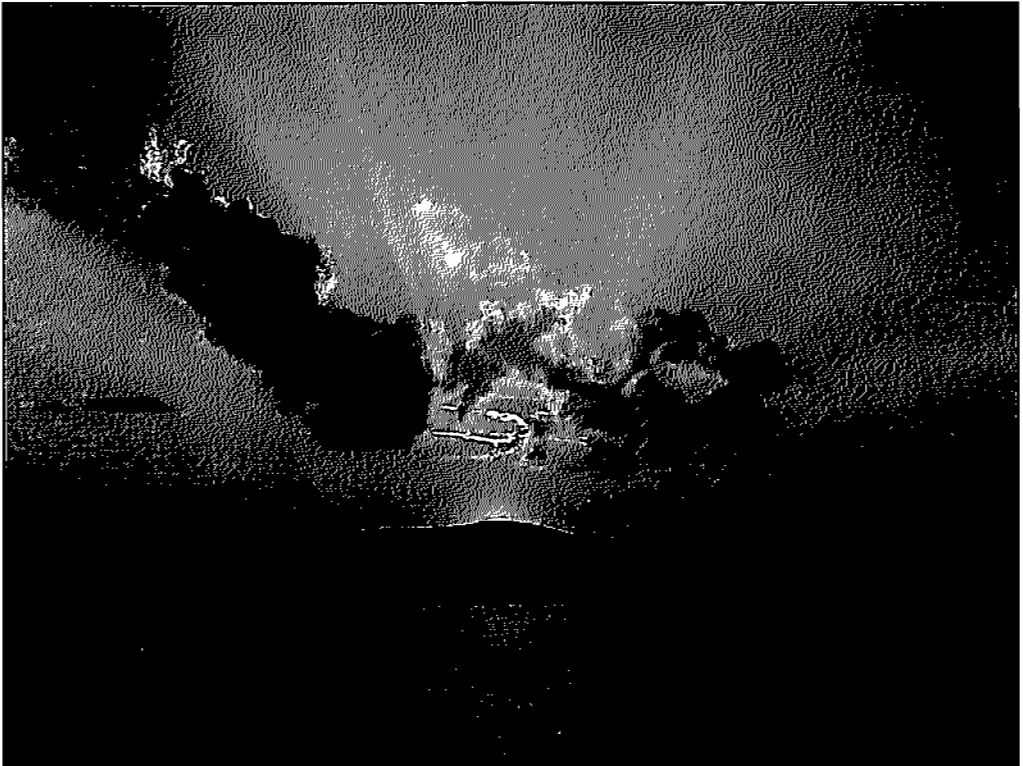


Application of Galois Theory of Graph Coverings. You can't hear the shape of a graph.

Find 2 regular graphs (without loops and multiple edges) which are isospectral but not isomorphic.

See A.T. & Stark in *Adv. in Math.*, Vol. 154 (2000) for the details. The method goes back to algebraic number theorists who found number fields K_i which are non isomorphic but have the same Dedekind zeta. See Perlis, *J. Number Theory*, 9 (1977).

THE END



Spectra of arithmetic infinite graphs

名越弘文 (Hirofumi Nagoshi)

京都大学数理解析研究所

1. はじめに

本稿では、関数体上の数論的離散群から作られるある無限グラフを考察する。それに対する明確な跡公式を構成し、またその応用として、付随する Ihara-Selberg ゼータ関数や隣接作用素の固有値の分布に対する結果を述べる。

$SL(2, \mathbb{R})$ は、上半平面 $H = \{z \in \mathbb{C} | \text{Im } z > 0\}$ に一次分数変換で作用する。そのとき、例えば $SL(2, \mathbb{Z})$ などの離散部分群による商 $SL(2, \mathbb{Z}) \backslash H$ を考えると、あるリーマン面が出来る。このような適当な離散部分群に対して、いわゆる跡公式や Selberg ゼータ関数などの理論が Selberg により構築された [S1][S2][He]。

その後、この Selberg の理論は、様々な方面への一般化や類似が考え出されたが、また一方でまだ研究されていないことも沢山ある。本稿の結果に関連するものとして、正則有限グラフの場合の Selberg の理論が Ahumada[Ah] によって知られている。

2. 設定

次に、本稿で扱う対象の設定を述べる。以下では、 q は奇素数 p の冪 p^r とし、 $\mathbb{F}_q[t]$ を有限体 \mathbb{F}_q 上の多項式環、 $\mathbb{F}_q(t)$ をその商体とする。体 $\mathbb{F}_q(t)$ には、 $a = f(t)/g(t) \in \mathbb{F}_q(t)$ ($f(t), g(t) \in \mathbb{F}_q[t]$) に対し $|a|_\infty := q^{-(\deg g - \deg f)}$ と定めることによりノルム $|\cdot|_\infty$ が入る。このノルムに関して $\mathbb{F}_q(t)$ を完備化した体、つまり結局、 $1/t$ のローラン級数全体で出来る体 $\mathbb{F}_q((1/t)) = \{\sum_{i=n}^{\infty} a_i t^{-i} | n \in \mathbb{Z}, a_i \in \mathbb{F}_q\}$ のことであるが、それを以下、 k_∞ と書くことにする。この体 k_∞ は、有理数体 \mathbb{Q} を“無限遠点”で完備化して出来る体 \mathbb{R} (実数体) の類似である。体 k_∞ の元 $a = \sum_{i=n}^{\infty} a_i t^{-i}$ ($a_n \neq 0$) に対し、そのノルムは $|a|_\infty = q^{-n}$ となる。また r_∞ で、 $1/t$ のテーラー級数全体で出来る環 $\mathbb{F}_q[[1/t]] = \{\sum_{i=n}^{\infty} a_i t^{-i} | n \in \mathbb{N}_{\geq 0}, a_i \in \mathbb{F}_q\}$ を表すことにする。

この先、

$$G := PGL(2, k_\infty) = GL(2, k_\infty)/k_\infty^\times,$$

$$K := PGL(2, r_\infty) = GL(2, r_\infty)/r_\infty^\times$$

と置く。 K は G の極大コンパクト部分群である。そのとき、 $G \backslash K$ は $(q+1)$ -正則木 $X = X_q$ とみなせれることが知られている。それに関して、少し述べる。

まず explicit な表示を述べたい (see e.g. [Li]). 商 G/K の完全代表系の一つとして、

$$\left\{ \begin{pmatrix} t^n & x \\ 0 & 1 \end{pmatrix} \in G \mid n \in \mathbb{Z}, x \in k_\infty/t^n r_\infty \right\}$$

が取れるが、これら各 coset を“頂点”と思い、一つの頂点 $gK \in G/K$ には、 $q+1$ 個の頂点 gs_iK ($i = 1, \dots, q+1$) (ただし、

$$(2.1) \quad \{s_1, \dots, s_{q+1}\} = \left\{ \begin{pmatrix} \frac{1}{t} & \alpha \\ 0 & 1 \end{pmatrix} \mid \alpha \in \mathbb{F}_q \right\} \cup \left\{ \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

とする) がつながっていることと定める。こうして作ったものが、木 (tree) になることが実は分かり、 $(q+1)$ -正則木 X が出来上がる。今は、 G の具体的な表示を使って X を構成したが、より intrinsic な形式で、一般に k_∞ のような非アルキメデスな局所体の上の適当な行列群に対して、このような combinatorial な幾何的対象 (building と呼ばれる) が定義できる。 X のそのような作り方や building については、例えば、[Se] や [St] を見ると良い。

一般にグラフ Y に対して、 $V(Y)$ でその頂点全体、 $E(Y)$ でその辺全体を表すとする。 $V(Y)$ のことを、単に Y と書くこともある。木 X には、自然な距離 d ($u, v \in X$ が隣接していたら $d(u, v) = 1$) がある。

以下、本稿では、主合同部分群と呼ばれる次の数論的離散部分群を考察する。

$$\Gamma = \Gamma(A) = \left\{ \gamma \in PGL(2, \mathbb{F}_q[t]) \mid \gamma \text{ のある代表元 } \tilde{\gamma} \text{ が, } \tilde{\gamma} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{A} \right\},$$

$A \in \mathbb{F}_q[t]$ 。この Γ に対して、商グラフ $\Gamma \backslash X$ は、 $\Gamma(A)$ は反転の元を持たないことに注意し、自然に定義される。この $\Gamma \backslash X$ は、無限グラフで、ある有限グラフに半直線 (end 部分と言うことにする) が有限個くつついた形をしている。特に、 $\Gamma = \Gamma(1) = PGL(2, \mathbb{F}_q[t])$ による商グラフは、頂点たち $\sigma_n := \begin{pmatrix} t^n & 0 \\ 0 & 1 \end{pmatrix} \in V(X)$, $n \in \mathbb{N}_{\geq 0}$ を結んでできる半直線与えられる。それら、詳しくは、[Se, II.1.6] [M2] などに載っている。有限個 (μ 個とする) の end 部分をたどった先 ($\in \partial X$) の全体を非同値な cusps と呼び、これらを $\kappa_1, \kappa_2, \dots, \kappa_\mu \in \partial X = P^1(k_\infty)$ と表す。

また、 $\Gamma(1)$ は、 G 上の Haar 測度に関して商 $\Gamma(1) \backslash G$ の体積が有限であるような離散部分群である (see [Se, II.1.6])。よって、 $\Gamma(A)$ もそうである。商グラフ $\Gamma \backslash X$ には、 K の測度を 1 と正規化しておくとし、 $v \in V(\Gamma \backslash X)$ に対し

$$m(v) = |\Gamma_v|^{-1}$$

(ここで、 $\Gamma_v \subset \Gamma$ は v の固定部分群) なる測度が入る (see [Se, II.1.5])。また、辺上に重み $m(e)$, $e \in E(\Gamma \backslash X)$ を $m(e) := |\Gamma_e|^{-1}$ (ここで、 $\Gamma_e \subset \Gamma$ は e の固定部分群) で定義する。

本稿では、 $V(X)$ 上の関数は \mathbb{C} 値なものを考える。隣接作用素と呼ばれる作用素 T を

$$(Tf)(v) := \sum_{u:d(v,u)=1} f(u) = \sum_{i=1}^{q+1} f(vs_i), \quad f: V(X) \rightarrow \mathbb{C}$$

として定義する。これは $\Gamma \backslash X$ 上の関数に誘導されるが、今の $\Gamma \backslash X$ の場合には、

$$(Tf)(v) = \sum_{e=(v,u) \in E(\Gamma \backslash X)} \frac{m(e)}{m(v)} f(u), \quad f: V(\Gamma \backslash X) \rightarrow \mathbb{C}$$

(ここで、 $e = (v, u)$ は頂点 v と u とが辺 e で結ばれていることを示す) と表すことができる。

以下、扱う関数空間は、 $L^2(\Gamma \backslash X) :=$

$$\left\{ f: V(X) \rightarrow \mathbb{C} \mid f(\gamma g) = f(g) \text{ for } \gamma \in \Gamma, g \in V(X), \int_{\Gamma \backslash X} |f(v)|^2 dm(v) < \infty \right\}$$

である。この $L^2(\Gamma \backslash X)$ には、内積

$$\langle f_1, f_2 \rangle := \int_{\Gamma \backslash X} f_1(g) \overline{f_2(g)} dm(g)$$

を入れる。

Lubotzky-Phillips-Sarnak[LPS] によって、隣接作用素の固有値の大きさの条件から、Ramanujan graph と呼ばれる正則有限グラフが定義されている。Morgenstern [M1] は、これを有限グラフとは限らないものに一般化して Ramanujan diagram と呼ばれるものを定義した。そして、Drinfeld の結果を使うことにより、彼は次を示した。

Theorem 2.1. [M2, Theorem 2.1] グラフ $\Gamma(A) \backslash X$ は、*Ramanujan diagram* である。

3. EISENSTEIN 級数

この節では、Eisenstein 級数と呼ばれるものを導入する。実はこれを使うことにより、 $L^2(\Gamma \backslash X)$ での T の連続スペクトルの部分を表せれることが知られている。はじめに、関数 $\psi_s(g)$ ($g \in G, s \in \mathbb{C}$) を

$$\psi_s(g) := |\det g|_\infty^s h((0, 1)g)^{-2s}$$

と定義する。ここで、 $(0, 1)g$ は、 1×2 -行列 $(0, 1)$ と 2×2 -行列 g の積を表し、 $h((x, y)) := \sup\{|x|_\infty, |y|_\infty\}$ である。実は、 $\psi_s(g) = |g$ の y 座標 $|_\infty^s$ となっている。関数 ψ_s は、右 K 不変かつ左 N 不変 ($N := \{ \begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix} \in G \}$) である。また、

$$(T\psi_s)(g) = (q^s + q^{1-s}) \psi_s(g)$$

を満たすことが容易に確かめれる。そのとき、各カスプ κ_i に対して、Eisenstein 級数 $E_{\kappa_i}(g, s), g \in G, s \in \mathbb{C}$ が定義される。簡単のために、カスプ ∞ に対する Eisenstein 級数のみを定義するが、それは

$$E_{\infty}(g, s) = \sum_{\gamma \in \Gamma_{\infty} \backslash \Gamma} \psi_s(\gamma g), \quad \operatorname{Re}(s) > 1$$

というものである。ここで、 $\Gamma_{\infty} \subset \Gamma$ は $\infty \in \partial X$ の固定部分群を表す。級数 $E_{\kappa_i}(g, s)$ は、 \mathbb{C} 全体に解析接続され、

$$\begin{aligned} E_{\kappa_i}(\gamma g, s) &= E_{\kappa_i}(g, s), \quad \gamma \in \Gamma, \\ (TE_{\kappa_i})(g, s) &= (q^s + q^{1-s})E_{\kappa_i}(g, s) \end{aligned}$$

を満たすことが分かる。

$E_i(g, s)$ は、各カスプ κ_j ($j = 1, \dots, \mu$) にて、体 κ_{∞} におけるフーリエ展開が出来、その定数項から $\varphi_{ij}(s)$ と表す重要なある関数が定まる。Li [Li] は $\Gamma(A)$ に対して $\varphi_{ij}(s)$ を、 $\mathbb{F}_q[t] \bmod A$ の指標に付随する Dirichlet L 関数を使って表し、次を示した。

Proposition 3.1. [Li, p. 241, p. 242, p. 249] $\Gamma = \Gamma(A)$ とするとき、

- $\varphi_{ij}(s)$ は q^{-2s} の有理関数。頂点 $g \in X$ を固定したとき、 $E_{\kappa_i}(g, s)$ は q^{-s} の有理関数である。
- $\varphi_{ij}(s)$ と $E_{\kappa_i}(g, s)$ (g は固定) は、 $\operatorname{Re}(s) \geq \frac{1}{2}$ において、 $s = 1 + n \frac{\pi i}{\log q}$ ($n \in \mathbb{Z}$) での 1 位の極を除いて、正則。
- $\mu \times \mu$ -行列 $\Phi(s) := (\varphi_{ij}(s))$ は対称行列で、関数等式 $\Phi(s)\Phi(1-s) = I$ を満たす。($s = \frac{1}{2} + it$ では、 $\Phi(s)$ はユニタリ-)。

行列 $\Phi(s)$ のことを散乱行列式といい、その行列式 $\varphi(s) := \det \Phi(s)$ を散乱行列式と呼ぶ。行列式 $\varphi(s)$ は、後々、跡公式や Ihara-Selberg ゼータ関数の行列式表示で重要となる。論文 [N2] において [Li] とは違うやり方で、 $\varphi_{ij}(s)$ の表示を得て、次を示した。

Proposition 3.2. $A^{\times} := (\mathbb{F}_q[t]/A\mathbb{F}_q[t])^{\times} / \mathbb{F}_q^{\times}$ とし、 \hat{A}^{\times} を A^{\times} の指標全体とする。関数 $L(s, \chi)$ を $\chi \in \hat{A}^{\times}$ に付随する Dirichlet L 関数とする。そのとき、 $\varphi(s)$ の極たちは、関数

$$(q^{2s} - q^2) \prod_{\chi \in \hat{A}^{\times}} L(2s, \chi)^h$$

(ここで、 $h := \mu/r, r := \phi(A)/(q-1)$ 、 $\phi(A)$ は Euler の totient function) の零点たちに、重複度込みで、含まれる。

後のために、

$$(3.1) \quad \varphi(s) = c \frac{(q^{2s} - qa_1)(q^{2s} - qa_2) \cdots (q^{2s} - qa_m)}{(q^{2s} - qb_1)(q^{2s} - qb_2) \cdots (q^{2s} - qb_n)}$$

(ここで、 $c, a_i (i = 1, \dots, m), b_j (j = 1, \dots, n)$ は定数で、右辺は既約とする) と置いておく。

4. 跡公式

Selberg 跡公式とは、 Γ に関するスペクトルの情報 (表現論的な情報) に渡る和と Γ の共役類 (幾何的情報) に渡る和を結ぶ公式である。積分核 $k(g, g')$ を point pair invariant とし $K(g, g') = \sum_{\gamma \in \Gamma} k(g, \gamma g')$ を作ると、これは $K(\gamma g, g') = K(g, g') = K(g, \gamma g'), \gamma \in \Gamma$ であるから $\Gamma \backslash X$ 上の関数 f (つまり、 $f(\gamma g) = f(g)$ for $\gamma \in \Gamma, g \in V(X)$ を満たす) に対する積分作用素

$$(Lf)(g) := \int_{\Gamma \backslash X} K(g, g') f(g') dm(g')$$

であるが、 k が適当な条件を満たすときこの L について 2 通りに跡が取れ、それらを計算することによって跡公式は得られる。

以下、 $\Gamma = \Gamma(A)$ の双曲的な元 P に対して

$$N(P) = \sup\{|\lambda_i|_\infty^2 \mid \lambda_i \text{ は行列 } P \text{ の固有値}\}$$

とおき、 $\deg P := \log_q N(P)$ とする。また、双曲的な元 P は素双曲的な元 (Γ の他の元の exponent > 1 なるべきではないもの) P_0 を用いて、 $P = P_0^k (k \geq 1)$ と表される。 Γ の素双曲共役類全体を \mathfrak{P}_Γ で表し、 D を T の $L^2(\Gamma \backslash X)$ -固有値全体 (有限個) とする。そのとき、 $\Gamma = \Gamma(A)$ に対する explicit な跡公式は次のようになる [N1]。

Theorem 4.1. 固有値 $\lambda_j \in D$ に対して $\lambda_j = q^{s_j} + q^{1-s_j}, s_j = 1/2 + ir_j$ と置く。数列 $c(n) \in \mathbb{C}, n \in \mathbb{Z}$ が、 $c(n) = c(-n)$ と $\sum_{n \geq m} q^{n/2} |c(n)| = O(q^{-m}), m \rightarrow \infty$ を満たしているとする。すると、 $\Gamma = \Gamma(1)$ のとき

$$\begin{aligned} & h\left(\frac{i}{2}\right) + h\left(\frac{i}{2} + \frac{\pi}{\log q}\right) = \text{vol}(\Gamma \backslash X) k(0) \\ & + \left(-\frac{q}{q^2 - 1} k(0) + \frac{q}{2(q-1)} c(0)\right) + \sum_{\{P_0\} \in \mathfrak{P}_\Gamma} \sum_{l=1}^{\infty} \frac{\deg P_0}{q^{\frac{l \deg P_0}{2}}} c(l \deg P_0) \\ & + 2 \sum_{m=1}^{\infty} (q^{-m} + 1) c(2m) + \frac{q-2}{(q-1)^2} k(0) + \frac{3q-4}{2(q-1)} c(0) \end{aligned}$$

が成立し、 $\Gamma = \Gamma(A)$ ($a = \deg A \geq 1$) のとき

$$\begin{aligned} \sum_{j=1}^{|D|} h(r_j) &= \text{vol}(\Gamma \backslash X) k(0) + \sum_{\{P_0\} \in \mathfrak{P}_\Gamma} \sum_{l=1}^{\infty} \frac{\deg P_0}{q^{\frac{l \deg P_0}{2}}} c(l \deg P_0) \\ &+ \left(\mu - \text{Tr} \Phi \left(\frac{1}{2} \right) \right) \left(\frac{1}{2} c(0) + \sum_{m=1}^{\infty} c(2m) \right) \\ &+ \frac{1}{4\pi} \int_{-\frac{\pi}{\log q}}^{\frac{\pi}{\log q}} h(r) \frac{\varphi' \left(\frac{1}{2} + ir \right)}{\varphi \left(\frac{1}{2} + ir \right)} dr - \mu \left(a + \frac{1}{q-1} \right) c(0). \end{aligned}$$

が成立する。

5. IHARA-SELBERG ゼータ関数

この節では、グラフ $\Gamma(A) \backslash X$ に対する Ihara-Selberg ゼータ関数について考察する。まず、その定義であるが、素双曲共役類 \mathfrak{P}_Γ を用いて次のようにする。

$$\zeta_\Gamma(u) := \prod_{\{P_0\} \in \mathfrak{P}_\Gamma} (1 - u^{\deg P_0})^{-1} = \prod_{\{P_0\} \in \mathfrak{P}_\Gamma} (1 - N(P_0)^{-s})^{-1}, \quad u = q^{-s}.$$

今、

$$(5.1) \quad N_m = \sum_{\substack{\{P_0\} \in \mathfrak{P}_\Gamma \\ \deg P_0 | m}} \deg P_0, \quad m \geq 1$$

とおくと、 $\zeta_\Gamma(u)$ は

$$(5.2) \quad \zeta_\Gamma(u) = \exp \left(\sum_{m=1}^{\infty} \frac{N_m}{m} u^m \right)$$

と表せれる。

Theorem 4.1 において、 $c(n)$ を

$$c(n) = \begin{cases} -(\log q) q^{-|n|(s-\frac{1}{2})} & n \neq 0 \\ 0 & n = 0, \end{cases}$$

($s \in \mathbb{C}$ は $\text{Re}(s) \geq 2$ とし固定) と取ることにより、Ihara-Selberg ゼータ関数 $\zeta_\Gamma(u)$ に対し、次のような T のスペクトルによる行列式表示が得られる [N1]。

Theorem 5.1. $\Gamma = \Gamma(A)$ ($\deg A \geq 1$) とし、

$$\det(T_\Gamma, s) := \det_D(T_\Gamma, s) \cdot \det_C(T_\Gamma, s),$$

$$\det_D(T_\Gamma, s) := \prod_{n=1}^{|D|} (1 - \lambda_n q^{-s} + q^{1-2s}),$$

$$\det_C(T_\Gamma, s) := \prod_{|b_j| < 1} (1 - q^{-2s+1} b_j) \prod_{|b_j| > 1} (1 - q^{-2s+1} b_j^{-1})^{-1}$$

(ここで、 b_j は (3.1) 中のもの) と置くと、

$$(5.3) \quad \zeta_\Gamma(u)^{-1} = (1 - q^{-2s})^\chi (1 - q^{-2s+1})^{-\rho} \det(T_\Gamma, s)$$

が成立する。ここで、 $\chi := \text{vol}(\Gamma \backslash X) \frac{q-1}{2}$, $\rho := \frac{1}{2} (\mu - \text{Tr} \Phi(\frac{1}{2}))$ である。そして、 $\zeta_{\Gamma(A)}(u)$ は u の有理関数である。

より具体的には、例えば、

$$\begin{aligned} \zeta_{\Gamma(1)}(u)^{-1} &= \frac{1 - q^2 u^2}{1 - q u^2}, \\ \zeta_{\Gamma(u)}(u)^{-1} &= \frac{(1 - u^2)^q (1 - q^2 u^2)}{(1 - q u^2)^{q+1}} \end{aligned}$$

である。散乱行列式の計算を要する。

有限グラフの Ihara-Selberg ゼータ関数については、例えば、[StTe] [Te] [Ah] を見ると良い。それらについては、Theorem 5.1 における $\det_C(T, s)$ が無い形をしている。

連続スペクトルの貢献分の行列式を担っている $\det_C(T, s)$ は、 $\varphi(s)$ の極 (または、Proposition 3.1 にある関数等式を使えば、 $\varphi(s)$ の零点) を用いて定義していることに注意。散乱行列式 $\varphi(s)$ を (3.1) のように書いたとき、 $|b_i| > 1$ (resp. $|b_i| < 1$) なる因子 $q^{2s} - q b_i$ は、 $\varphi(s)$ の $\text{Re}(s) > \frac{1}{2}$ (resp. $\text{Re}(s) < \frac{1}{2}$) にある極に対応している。この $\det_C(T, s)$ は、 $\varphi(s)$ の極を渡る。

本稿では、解析的に跡公式を作ってから、それを使って Ihara-Selberg ゼータ関数 $\zeta_{\Gamma(A)}(u)$ の行列式表示を得た。ところで [N1] の内容の作成時には筆者は知らなかったのだが、Scheja [Sc] が組み合わせ的な議論より同じ $\zeta_{\Gamma(A)}(u)$ について Theorem 5.1 とは異なるある行列式表示を得ているので、そのことを注意しておく。Theorem 5.1 に出てきた $V(\Gamma \backslash X)$ における作用素 $\Delta(u) = 1 - Tu + qu^2$ の変形で、 $\Gamma \backslash X$ から end 部分を除いた残りの有限グラフにおける作用素 $\Delta^*(u)$ を考えている。

6. 固有値の分布

グラフ $\Gamma(A) \backslash X_q$ に対する T/\sqrt{q} の非自明な固有値 λ 全体を $D(A, q)$ とすると、Theorem 2.1 より、 $D(A, q) \subset \Omega := [-2, 2]$ である。この節では、パラメータ A, q について $\deg A \rightarrow \infty, q \rightarrow$ としたときの $D(A, q)$ の極限分布について調べる。

そのために、 Ω 上の確率測度を 2 つ用意する。1 つは、Wigner semi-circle または Sato-Tate 測度と呼ばれるもので、

$$d\mu_\infty(x) = \frac{1}{\pi} \sqrt{1 - \frac{x^2}{4}} dx.$$

である。もう 1 つは、

$$d\mu_q(x) = \frac{q+1}{(q^{1/2} + q^{-1/2})^2 - x^2} d\mu_\infty(x).$$

である。測度 μ_q は、 $(q+1)$ -正則木 X 上の T のスペクトル測度として知られている。

そのとき、次が得られる [N2]。

Theorem 6.1. (1) q を固定し、 $\deg A_i \rightarrow \infty$ ($as i \rightarrow \infty$) なる任意の多項式の列 $\{A_i\}$ ($i = 1, 2, \dots; A_i \in \mathbb{F}_q[t]$) を取ってくる。すると、 $i \rightarrow \infty$ のとき $D(A_i, q)$ は Ω 上で測度 μ_q に関して一様分布する。すなわち、 Ω 上の任意の連続関数 $f(x)$ に対し

$$(6.1) \quad \lim_{i \rightarrow \infty} \frac{1}{\#D(A_i, q)} \sum_{\lambda \in D(A_i, q)} f(\lambda) = \int_{\Omega} f(x) d\mu_q(x)$$

が成立する。

(2) $q_i \rightarrow \infty$ かつ $\deg A_i \rightarrow \infty$ ($as i \rightarrow \infty$) なる組 $\{q_i, A_i\}$ ($i = 1, 2, \dots; A_i \in \mathbb{F}_{q_i}[t]$) を任意に取ってくる。すると、 $i \rightarrow \infty$ のとき $D(A_i, q_i)$ は Ω 上で測度 μ_∞ に関して一様分布する。すなわち、 Ω 上の任意の連続関数 $f(x)$ に対し

$$(6.2) \quad \lim_{i \rightarrow \infty} \frac{1}{\#D(A_i, q_i)} \sum_{\lambda \in D(A_i, q_i)} f(\lambda) = \int_{\Omega} f(x) d\mu_\infty(x)$$

が成立する。

この定理の証明の概略は、次のようになっている。今は (1) のみについて述べる。まず、 $X_m(x)$ を第二種の Chebychev 多項式とし、 $X_{m,q}(x) := X_m(x) - q^{-1}X_{m-2}(x)$ とおくと、集合 $\{X_{m,q}(x) | m = 0, 1, 2, \dots\}$ は測度 μ_q の直交多項式系となっている。また、集合 $\{X_{m,q}(x) | m = 0, 1, 2, \dots\}$ は Ω 上の連続関数全体で稠密なので、これらについて (6.1) を調べれば十分である。 $f(x) = X_{m,q}(x)$ とおき、 $\text{Tr } T_m$ で $\Gamma(A)$ に対する T_m の固有値の和を表すとすると (ここで $V(X)$ 上の関数 $\phi(v)$ に対し $T_m \phi(v) := \sum_{d(v,u)=m} \phi(u)$ とする)、 $\sum_{\lambda \in D(A,q)} f(\lambda) = q^{-m/2} \text{Tr } T_m$ であることが分かる。次に、(5.2) と (5.3) を u について \log 微分を取ることにより、 $\text{Tr } T_m$ と N_m を結びつけるある式が得られる。そのうち、連続スペクトルの貢献分は、Proposition 3.2 を使って、処理できる。また、主合同部分群 $\Gamma(A)$ に対して $\deg A \rightarrow \infty$ とするとき、各 m

に対して $N_m \rightarrow 0$ である。以上のことを組み合わせると、各 $m \neq 0$ に対して $\#D(A_i, q)^{-1} \sum_{\lambda \in D(A_i, q)} f(\lambda) \rightarrow 0$ (as $i \rightarrow \infty$) となり、証明が終わる。

REFERENCES

- [Ah] G. Ahumada, Fonctions periodiques et formule des traces de Selberg sur les arbres, C. R. Acad. Sci. Paris, 305 (1987), 709-712.
- [He] D. Hejhal, The Selberg trace formula for $PSL(2, \mathbb{R})$, Vol. 2, Lecture Notes in Math. 1001, Springer.
- [Li] W. Li, On modular functions in characteristic p , Trans. Amer. Math. Soc. 246 (1978), 231-259.
- [LPS] A. Lubotzky, R. Phillips and P. Sarnak, Ramanujan graphs, Combinatorica, 8 (1988), 261-277.
- [M1] M. Morgenstern, Ramanujan diagrams, SIAM J. Discrete Math. 7 (1994), 560-570.
- [M2] M. Morgenstern, Natural bounded concentrators, Combinatorica, 15 (1995), 111-122.
- [N1] H. Nagoshi, Selberg zeta functions over function fields, J. Number Theory, 90 (2001), 207-238.
- [N2] H. Nagoshi, The distribution of eigenvalues of arithmetic infinite graphs, to appear in Forum Math.
- [N3] H. Nagoshi, Spectra of arithmetic infinite graphs and their application, Interdisciplinary Info. Sciences, 7 (2001), 67-76.
- [Sc] O. Scheja: Zetafunktionen arithmetisch definierter Graphen. Ph.D. Thesis, Saarbrücken, 1998
- [S1] A. Selberg, Harmonic analysis and discontinuous groups in weakly symmetric Riemannian spaces with applications to Dirichlet series, J. Indian Math. Soc. B. 20 (1956), 47-87; Collected papers, Vol. 1, 423-463, Springer-Verlag.
- [S2] A. Selberg, Harmonic analysis, Collected papers, Vol. 1, 626-674, Springer-Verlag.
- [Se] J. P. Serre, Trees, Springer-Verlag, 1980.
- [StTe] H. M. Stark and A. A. Terras, Zeta functions of finite graphs and covering, Adv. Math. 121 (1996), 124-165.
- [St] T. Steger, Local fields and buildings, Contemp. Math. 206 (1997), 79-107.
- [Te] A. A. Terras, Fourier analysis on finite groups and applications, London Math. Soc. Student Texts 43, Cambridge, 1999.
- [VeNi] A. B. Venkov and A. M. Nikitin, The Selberg trace formula, Ramanujan graphs and some problems in mathematical physics, St. Petersburg Math. J. 5 (1993), 419-484.

Character tables of some association schemes, and Ramanujan graphs

Eiichi Bannai, Osamu Shimabukuro and Hajime Tanaka

Graduate School of Mathematics
Kyushu University

In Kumamoto the first author (Eiichi Bannai) gave the talk with the above title. This talk was based on the following two papers written jointly with Osamu Shimabukuro and Hajime Tanaka, both at Kyushu University.

1. Finite Euclidean graphs and Ramanujan graphs, preprint, submitted to the Proceedings of the Fourth Shanghai Conference on Combinatorics, a special issue of *Discrete Mathematics*.

2. Finite analogues of non-Euclidean spaces and Ramanujan graphs, preprint, to appear in Seidel memorial issue of *European Journal of Combinatorics*.

These papers are available upon request to the authors. In this proceedings, we give an abbreviated version of the first paper, and an abstract and the introduction of the second paper.

Finite Euclidean graphs and Ramanujan graphs

Eiichi Bannai, Osamu Shimabukuro and Hajime Tanaka

Abstract

We consider finite analogues of Euclidean graphs in a more general setting than the one considered in Medrano-Myers-Stark-Terras [13] and we obtain many new examples of Ramanujan graphs. In order to prove these results, we use the previous work of W.M. Kwok [9] calculating the character tables of certain association schemes of affine type. A key observation is that we can obtain better estimates for the ordinary Kloosterman sum $K(a, b; q)$. In particular, we always achieve $|K(a, b; q)| < 2\sqrt{q}$, and $|K(a, b; q)| \leq 2\sqrt{q-2}$ in many (but not all) of the cases, instead of the well known $|K(a, b; q)| \leq 2\sqrt{q}$. Also, we use the ideas of controlling association schemes, and the Ennola type dualities, in our previous work on the character tables of commutative association schemes. The method in this paper will be used to construct many more new examples of families of Ramanujan graphs in the subsequent paper.

Introduction

The purpose of this paper is to continue the study on finite analogues of Euclidean graphs which was started in Medrano *et al.* [13].

In [13], they considered the following finite Euclidean graphs. Let $V = V_n(q) = \mathbb{F}_q^n$ be the n -dimensional vector space over the finite field \mathbb{F}_q where $q = p^r$ with p a prime number. (In [13], p was assumed to be an odd prime.) For $x, y \in \mathbb{F}_q^n$, the Euclidean distance $d(x, y) \in \mathbb{F}_q$ is defined by

$$d(x, y) = (x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2.$$

The Euclidean graph $E_q(n, a)$ was defined as the graph with the vertex set V and the edge set

$$E = \{(x, y) \in V \times V \mid x \neq y, d(x, y) = a\}.$$

Then they considered the spectra of the graph $E_q(n, a)$ and discussed when these graphs are Ramanujan graphs. As is well known, a regular (undirected) graph of valency k is called a Ramanujan graph if any eigenvalue θ of the graph with $|\theta| \neq k$ satisfies

$$|\theta| \leq 2\sqrt{k-1}. \quad (1)$$

However, we remark that it is more natural to define finite analogues of Euclidean graphs for each non-degenerate quadratic form on V , instead of considering only the above distance $d(x, y) = (x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2$. That is, let Q be a non-degenerate quadratic form on V . Then the graph $E_q(n, Q, a)$ is defined as the graph with the vertex set V and the edge set

$$E = \{(x, y) \in V \times V \mid x \neq y, Q(x - y) = a\}. \quad (2)$$

The advantage of using this new definition is twofold. First, note that if $n = 2m$ is even, there are two inequivalent non-degenerate quadratic forms $Q = Q_{2m}^{\pm}$ on $V = \mathbb{F}_q^n$ (see §1). If $q \equiv 3 \pmod{4}$, the quadratic form $d(x, 0) = x_1^2 + x_2^2 + \cdots + x_n^2$ is equivalent to Q_{2m}^{\mp} depending on whether m is odd or even, while it is always equivalent to Q_{2m}^{\pm} if $q \equiv 1 \pmod{4}$. Therefore we obtain more examples of interesting graphs in a unified manner. Second, this allows us to consider finite analogues of Euclidean graphs when q is even. (In this case, $d(\cdot, 0)$ is degenerate. It is remarked in Medrano *et al.* [13] and Terras [15] that finite analogues of Euclidean graphs for \mathbb{F}_q , with q even, had not been studied.) Moreover, we will be able to see that the previous work of W.M. Kwok [9] is readily applicable when this new viewpoint is introduced. In fact, using the character tables of certain association schemes of affine type obtained in Kwok [9], we can obtain many new examples of Ramanujan graphs among the graphs $E_q(n, Q, a)$. (The reader is referred to Bannai-Ito [2], Bannai [1] for the basic concept of commutative association schemes and their character tables.) We also remark that this phenomenon is closely connected with the previous work of Ennola type dualities in some association schemes given in Bannai-Kwok-Song [3], as we will discuss more in the subsequent papers.

The content of this paper is as follows. In §1, we review basic materials on the character tables of association schemes which give the framework for the study of finite Euclidean graphs $E_q(n, Q, a)$. In particular, we will review the work of Kwok [9]. In §2, we consider certain Kloosterman sums (which are essentially Gaussian periods) and the well known inequality $|K(a, b; q)| \leq 2\sqrt{q}$ due to A. Weil [16]. Then we will discuss when the equality $|K(a, b; q)| = 2\sqrt{q}$ is attained. (We will show that this is never attained for the Kloosterman sums $K(a, b; q)$ we are considering.) Then, in §3, this result will be applied to discuss which of the finite Euclidean graphs $E_q(n, Q, a)$ are Ramanujan graphs. Our main results in this paper are Theorems 3.1-3.4 in §3. In addition, in §4, we will give some results of calculations by computer for some small parameters m and q , implementing the earlier work of Medrano *et al.* [13].

In order to keep this paper concise, we confined our discussions to the finite Euclidean graphs $E_q(n, Q, a)$. However, it is possible to obtain similar kinds of results for other many association schemes considered in the papers Bannai-Shen-Song [4], Bannai-Shen-Song-Wei [5], etc. (i.e., finite analogues of non-euclidean graphs in the sense of [15, Chapter 19]). That study will be treated in the subsequent papers.

Acknowledgement. The authors would like to thank Dr. Koji Chinen for giving us a help in finding the idea of the proof of Lemma 2.2, as well as informing us of the references Chinen-Hiramatsu [7], Lachaud-Wolfmann [10], Wolfmann [17]. We are also indebted to Professor Masanobu Kaneko

and Ms. Akane Katamoto. Prof. Kaneko kindly retested some of the computer calculations given in §4, and Ms. Katamoto transformed the formula for Gaussian periods ((3) below) into a more explicit formula using only cosine functions, which enabled us to improve the accuracy of these calculations.

1 Orthogonal groups, association schemes of certain affine types and their character tables

Let $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be a commutative association scheme of class d (see Bannai [1] or Bannai-Ito [2] for instance). Let A_i be the adjacency matrix with respect to the relation R_i . Then A_0, A_1, \dots, A_d generate a semisimple algebra \mathcal{A} over the complex number field, called the Bose-Mesner algebra of \mathfrak{X} . Let $E_0 = \frac{1}{|X|}J, E_1, \dots, E_d$ be a unique set of primitive idempotents of \mathcal{A} , where J is the matrix whose entries are all 1, and write

$$A_i = \sum_{j=0}^d p_i(j)E_j,$$

for $0 \leq i \leq d$ (in particular, $k_i = p_i(0)$ is the valency of the regular graph (X, R_i)). The $(d+1) \times (d+1)$ matrix P whose (j, i) -entry is $p_i(j)$, is called the character table of the commutative association scheme \mathfrak{X} .

Many examples of association schemes are obtained as follows. Let G be a finite group acting transitively on a finite set X , and let $\mathcal{O}_0 = \{(x, x) | x \in X\}, \mathcal{O}_1, \dots, \mathcal{O}_d$ be the orbits of G acting on the set $X \times X$. Define the relation R_i on X by

$$(x, y) \in R_i \Leftrightarrow (x, y) \in \mathcal{O}_i,$$

for $0 \leq i \leq d$, then it is easily seen that the pair $(X, \{R_i\}_{0 \leq i \leq d})$ is an association scheme.

Now, let Q be a non-degenerate quadratic form on the vector space $V = V_n(q) = \mathbb{F}_q^n$. Then the group of all linear transformations on V that fix Q , is called the orthogonal group associated with the quadratic form Q , and is denoted by $O(V, Q)$. More precisely,

$$O(V, Q) = \{\sigma \in GL(V) | Q(\sigma(x)) = Q(x) \text{ for all } x \in V\}.$$

The non-degenerate quadratic forms over \mathbb{F}_q are classified as follows:

(i) Suppose $n = 2m$ is even. If q is odd, then there are two inequivalent non-degenerate quadratic forms Q^+ and Q^- :

$$\begin{aligned} Q^+(x) &= 2x_1x_2 + \cdots + 2x_{2m-1}x_{2m}, \\ Q^-(x) &= 2x_1x_2 + \cdots + 2x_{2m-3}x_{2m-2} + x_{2m-1}^2 - \alpha x_{2m}^2, \end{aligned}$$

where α is a non-square element in \mathbb{F}_q . If q is even, then there are also two inequivalent non-degenerate quadratic forms Q^+ and Q^- :

$$\begin{aligned} Q^+(x) &= x_1x_2 + \cdots + x_{2m-1}x_{2m}, \\ Q^-(x) &= x_1x_2 + \cdots + x_{2m-3}x_{2m-2} + x_{2m-1}^2 + x_{2m-1}x_{2m} + \beta x_{2m}^2, \end{aligned}$$

where β is an element in \mathbb{F}_q such that the polynomial $t^2 + t + \beta$ is irreducible over \mathbb{F}_q . We write $GO_{2m}^+(q) = O(V, Q^+)$ and $GO_{2m}^-(q) = O(V, Q^-)$.

(ii) Suppose $n = 2m + 1$ is odd. If q is odd, then there are two inequivalent non-degenerate quadratic forms Q and Q' :

$$\begin{aligned} Q(x) &= 2x_1x_2 + \cdots + 2x_{2m-1}x_{2m} + x_{2m+1}^2, \\ Q'(x) &= 2x_1x_2 + \cdots + 2x_{2m-1}x_{2m} + \alpha x_{2m+1}^2, \end{aligned}$$

where α is a non-square element in \mathbb{F}_q , however the groups $O(V, Q)$ and $O(V, Q')$ are isomorphic. If q is even, then there exists exactly one inequivalent non-degenerate quadratic form Q :

$$Q(x) = x_1x_2 + \cdots + x_{2m-1}x_{2m} + x_{2m+1}^2.$$

We write $GO_{2m+1}(q) = O(V, Q)$.

Let $G = O(V, Q)$ be the orthogonal group associated with a non-degenerate quadratic form Q on V . Then the group $\tilde{G} = V \cdot G$, the semi-direct product of V (translations) and G , acts on the set V transitively. Since V is abelian, we get the commutative association scheme from this permutation group. Kwok [9] called this association scheme as one of the association schemes of affine type, and studied very carefully their properties together with their character tables. Here, we recall some of the main results obtained by Kwok [9].

In what follows, we denote this association scheme by $\mathfrak{X}(G, V)$. The character table $P = P(G, V)$ of $\mathfrak{X}(G, V)$ is expressed as follows. (Since some of the tables in Kwok [9] contain misprints which are sometimes very difficult to detect, we write down them explicitly here. For the notation, we will basically follow Kwok [9]. Also, see the explanation below.)

Kwok [9] separates the discussion into the following four cases. (Discussions of Case 3 and Case 4 are omitted here.)

Let ρ be a primitive element of \mathbb{F}_q .

Case 1. $\mathfrak{X}(GO_{2m}^-(q), V_{2m}(q))$: The relations are given by

$$\begin{aligned} R_0 &= \{(x, x) | x \in V\}, \\ R_i &= \{(x, y) \in V \times V | Q^-(x - y) = \rho^i\}, \quad \text{for } 1 \leq i \leq q - 1, \\ R_q &= \{(x, y) \in V \times V | x \neq y, Q^-(x - y) = 0\}. \end{aligned}$$

Thus $(V, R_i) = E_q(2m, Q^-, \rho^i)$ for $1 \leq i \leq q - 1$, and $(V, R_q) = E_q(2m, Q^-, 0)$. Notice that R_q is empty if $m = 1$. We have

$$P(GO_{2m}^-(q), V_{2m}(q)) = \begin{bmatrix} 1 & q^{2m-1} + q^{m-1} \dots q^{2m-1} + q^{m-1} & q^{2m-1} - (q-1)q^{m-1} - 1 \\ 1 & & q^{m-1} - 1 \\ \vdots & q^{m-1} \cdot \Psi(2, q, q-1) & \vdots \\ 1 & & q^{m-1} - 1 \\ 1 & q^{m-1} \dots q^{m-1} & -(q-1)q^{m-1} - 1 \end{bmatrix}$$

for $m > 1$ (the last column and the last row are empty if $m = 1$). The explicit definition of the submatrix $\Psi(2, q, q-1)$ is given later.

Case 2. $\mathfrak{X}(GO_{2m}^+(q), V_{2m}(q))$: The relations are given by

$$\begin{aligned} R_0 &= \{(x, x) | x \in V\}, \\ R_i &= \{(x, y) \in V \times V | Q^+(x - y) = \rho^i\}, \quad \text{for } 1 \leq i \leq q - 1, \\ R_q &= \{(x, y) \in V \times V | x \neq y, Q^+(x - y) = 0\}. \end{aligned}$$

Thus $(V, R_i) = E_q(2m, Q^+, \rho^i)$ for $1 \leq i \leq q - 1$, and $(V, R_q) = E_q(2m, Q^+, 0)$. We have

$$P(GO_{2m}^+(q), V_{2m}(q)) = \begin{bmatrix} 1 & q^{2m-1} - q^{m-1} \dots q^{2m-1} - q^{m-1} & q^{2m-1} + (q-1)q^{m-1} - 1 \\ 1 & & -q^{m-1} - 1 \\ \vdots & -q^{m-1} \cdot \Psi(2, q, q-1) & \vdots \\ 1 & & -q^{m-1} - 1 \\ 1 & -q^{m-1} \dots - q^{m-1} & (q-1)q^{m-1} - 1 \end{bmatrix}$$

for $m \geq 1$.

In the above tables, the matrix $\Psi = \Psi(n, q, e)$ with $ef = q^n - 1$ is defined as the following $e \times e$ matrix:

$$\Psi = \begin{bmatrix} \eta_0 & \eta_1 & \cdots & \eta_{e-1} \\ \eta_1 & \eta_2 & \cdots & \eta_0 \\ \vdots & \vdots & \ddots & \vdots \\ \eta_{e-1} & \eta_0 & \cdots & \eta_{e-2} \end{bmatrix}$$

where $\eta_i = \eta_i(n, q, e)$ ($0 \leq i \leq e-1$) are the Gaussian periods for the field \mathbb{F}_{q^n} defined by

$$\eta_i = \sum_{\substack{i' \equiv i \pmod{e} \\ 0 \leq i' \leq q^n - 2}} e(\text{Tr}_{q^n, p}(\rho_n^{i'})) \quad (3)$$

with $e(x) = \exp(2\pi i x/p)$, ρ_n being a primitive element of \mathbb{F}_{q^n} , and $\text{Tr}_{q^n, p} : \mathbb{F}_{q^n} \rightarrow \mathbb{F}_p$ being the trace map from \mathbb{F}_{q^n} onto \mathbb{F}_p . Note that the matrix

$$\begin{bmatrix} 1 & f & f & \cdots & f \\ 1 & \eta_0 & \eta_1 & \cdots & \eta_{e-1} \\ 1 & \eta_1 & \eta_2 & \cdots & \eta_0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \eta_{e-1} & \eta_0 & \cdots & \eta_{e-2} \end{bmatrix}$$

is the character table of the cyclotomic association scheme of class e obtained by the action of $\mathbb{F}_{q^n} \cdot Z_f$ on \mathbb{F}_{q^n} ($\cong V_n(q)$), where $Z_f \subset \mathbb{F}_{q^n}^*$ is the cyclic subgroup of order f .

Remark. The same submatrix $\Psi(2, q, q-1)$ of size $(q-1) \times (q-1)$ appears in both $P(GO_{2m}^-(q), V_{2m}(q))$ and $P(GO_{2m}^+(q), V_{2m}(q))$. This is not an accident, but is an example of the Ennola type dualities which was mentioned in Bannai-Kwok-Song [3], and this observation is crucial for showing that many graphs in Case 2 are Ramanujan graphs.

2 Kloosterman sums

As it is mentioned in Medrano *et al.* [13, p.232], the values of $\eta_i = \eta_i(2, q, q-1)$ ($0 \leq i \leq q-2$) in $P(GO_{2m}^-(q), V_{2m}(q))$ and $P(GO_{2m}^+(q), V_{2m}(q))$ are expressed by using usual Kloosterman sums defined by

$$K(a, b; q) = \sum_{r \in \mathbb{F}_q^*} e(\text{Tr}_{q, p}(ar + br^{-1})). \quad (4)$$

for $a, b \in \mathbb{F}_q$. Namely, we have the following:

Lemma 2.1. *For $0 \leq i \leq q-2$, we have*

$$\eta_i = \eta_i(2, q, q-1) = -K(\rho^i, 1; q), \quad (5)$$

where $\rho = \rho_2^{q+1}$ is a primitive element of \mathbb{F}_q .

(Proof is omitted here.)

It is well known that the Kloosterman sum is bounded above by $2\sqrt{q}$ by Weil [16] (see also Schmidt [14], Li [11]):

$$|K(a, b; q)| \leq 2\sqrt{q}, \quad (6)$$

for all $a, b \in \mathbb{F}_q^*$. The following lemma is a slight strengthening of this result.

Lemma 2.2. *Suppose a, b are nonzero elements of \mathbb{F}_q . Then we have*

$$|K(a, b; q)| < 2\sqrt{q}.$$

Proof. Our proof of Lemma 2.2 is inspired by [7, Theorem 7.1]. By virtue of (6), it is enough to show the following:

$$|K(a, b; q)| \neq 2\sqrt{q}. \quad (7)$$

First, notice that $K(a, b; q)$ is an algebraic integer in the cyclotomic field

$$K = \mathbb{Q}(\zeta_p),$$

where $\zeta_p = \exp(2\pi i/p)$. We denote the ring of integers in K by \mathcal{O}_K . Let $\pi_p = 1 - \zeta_p$, then π_p is a prime in \mathcal{O}_K and π_p divides p . Since

$$e(\mathrm{Tr}_{q,p}(a)) = \zeta_p^{\mathrm{Tr}_{q,p}(a)} = (1 - \pi_p)^{\mathrm{Tr}_{q,p}(a)} \equiv 1 \pmod{\pi_p},$$

for all $a \in \mathbb{F}_q$, we have

$$K(a, b; q) \equiv \overline{K(a, b; q)} \equiv q - 1 \equiv -1 \pmod{\pi_p},$$

from which it follows that

$$|K(a, b; q)|^2 = K(a, b; q)\overline{K(a, b; q)} \equiv 1 \pmod{\pi_p},$$

in \mathcal{O}_K . Therefore, $|K(a, b; q)|$ cannot be equal to $2\sqrt{q}$, since $(2\sqrt{q})^2 = 4q \equiv 0 \pmod{\pi_p}$. \square

3 Ramanujan graphs

We prove the following theorems (Theorem 3.1-3.4). (We omit Theorems 3.3 and 3.4 here.) Here we note that we use Lemma 2.2 crucially, in the proof of the claim in Theorem 3.2, when m becomes large.

Theorem 3.1. *In Case 1, i.e., in the association scheme $\mathfrak{X}(GO_{2m}(Q^-), V_{2m}(q))$, the graph $(V, R_i) = E_q(2m, Q^-, \rho^i)$ is Ramanujan for $1 \leq i \leq q - 1$.*

Proof. For $1 \leq i \leq q - 1$, the valency k_i of the graph (V, R_i) is equal to $q^{2m-1} + q^{m-1}$. From Lemma 2.1 and (6) (or Lemma 2.2) we have

$$|q^{m-1}\eta_j|^2 \leq 4q^{2m-1} \leq (2\sqrt{k_i - 1})^2,$$

for all $\eta_j = \eta_j(2, q, q - 1)$ ($0 \leq j \leq q - 2$). Hence the eigenvalues of the graph (V, R_i) satisfy the Ramanujan bound (1). \square

Remark 3.1. It is not difficult to see that the graph $(V, R_q) = E_q(2m, Q^-, 0)$ is not Ramanujan if and only if $q \geq 7$, or $(q, m) = (5, 2)$.

Theorem 3.2. *We fix q . Then in Case 2, i.e., in the association scheme $\mathfrak{X}(GO_{2m}(Q^+), V_{2m}(q))$, the graphs $(V, R_i) = E_q(2m, Q^+, \rho^i)$ ($1 \leq i \leq q - 1$) are Ramanujan, if m is sufficiently large (i.e., larger than a certain number which is determined by q).*

Proof. The valencies k_i ($1 \leq i \leq q - 1$) are $q^{2m-1} - q^{m-1}$. Let $|\eta_j| = |\eta_j(2, q, q - 1)| = C_j\sqrt{q}$, then by Lemma 2.1 and Lemma 2.2 we have $0 \leq C_j < 2$. Therefore

$$(2\sqrt{k_i - 1})^2 - |q^{m-1}\eta_j|^2 = (4 - C_j^2)q^{2m-1} - 4q^{m-1} - 4$$

is positive when m is large, so that satisfies (1). \square

Remark 3.2. We note in particular that if $|\eta_i| \leq 2\sqrt{q-2}$ ($0 \leq i \leq q - 2$), then all the graphs $E_q(2m, Q^+, \rho^i)$ ($1 \leq i \leq q - 1$) as well as all the graphs $E_q(2, Q^+, \rho^i)$ are Ramanujan graphs. It is surprising that for many values of q this condition $\max |\eta_i| \leq 2\sqrt{q-2}$ is satisfied. In the next section, we give computer experiments when this condition is satisfied. If this condition is not satisfied, then for small m the graph $E_q(2m, Q^+, \rho^i)$ is sometimes Ramanujan, and sometimes not Ramanujan. The graph $(V, R_q) = E_q(2m, Q^+, 0)$ is not Ramanujan if and only if $m = 1$ and $q \geq 11$, or $m > 1$ and $q \geq 7$.

4 Computer calculations

In this section, we give the results of computer calculations. We are mainly interested in the following question: Does the inequality $|\eta_i| = |\eta_i(2, q, q-1)| \leq 2\sqrt{q-2}$ hold for all $i = 0, 1, \dots, q-2$? (See Remark 3.2.) In these experiments, we made use of the computer package "M A G M A" (<http://magma.maths.usyd.edu.au/magma>). The results in the first two tables (Table 1 and Table 2) are retested by Professor M. Kaneko.

1. First, for each odd prime $p \leq 500$, we list the maximum value of $|\eta_i| = |\eta_i(2, q, q-1)|$ ($0 \leq i \leq p-2$), $2\sqrt{p-2}$, and the answer to the above question. (Table 1 is omitted here.)
2. For each odd prime $500 \leq p \leq 4000$, we list all the primes p such that $|\eta_i| = |\eta_i(2, q, q-1)| > 2\sqrt{p-2}$ for some i , together with $\max |\eta_i|$ and $2\sqrt{p-2}$. (Table 2 is omitted here.)
3. Finally, we give the answer to the question for each prime power $q = p^r \leq 3000$. (Table 3 is omitted here.)

Remark 4.1. If $q = 2^r$ or $q = 3^r$, then the values of $|K(a, b; q)|$ are integers. Lachaud and Wolfmann [10] proved that if $q = 2^r$ then the $|K(a, b; q)|$ take all the integer values which are congruent to -1 modulo 4 and whose absolute values are less than $2\sqrt{q}$. While, Wolfmann [17] proved that if $q = 3^r$, then the values of $|K(a, b; q)|$ take all the integer values which are congruent to -1 modulo 3 and whose absolute values are less than $2\sqrt{q}$. So, the values in Table 3 for $q = 2^r$ and $q = 3^r$ can be obtained without computer calculation. However, the proof of their claims are nontrivial and must use algebraic geometry.

Remark 4.2. The primes p (up to 5021) for which $\max |\eta_i| > 2\sqrt{p-2}$ make the following series:

$$7, 17, 53, 139, 163, 211, 463, 541, 1093, 1723, 1747, 1931, 2111, 2671, 2713, 2731, \\ 3121, 3593, 3853, 4057, 4733, 5021, \dots,$$

It seems that these primes seem pretty much random. (It would be interesting to know how often they occur, say.) It would be interesting if we could find any regularity in this series.

Remark 4.3. Theorem 3.2 asserts that the graphs $E_q(2m, Q^+, \rho^i)$ ($1 \leq i \leq q-1$) are Ramanujan if m is large. It turns out that for all q considered above (that is, for all primes $2 \leq p \leq 4000$ and for all prime powers $q = p^r \leq 3000$), these graphs are Ramanujan as soon as $m \geq 2$.

References

- [1] E. Bannai, Character tables of commutative association schemes, in "Finite Geometries, Buildings, and Related Topics" (W.M. Kantor *et al.*, Eds.), pp.105-128, Clarendon Press, Oxford, 1990.
- [2] E. Bannai and T. Ito, "Algebraic Combinatorics I," Benjamin/Cummings, Menlo Park, CA, 1984.
- [3] E. Bannai, W.M. Kwok, and S.-Y. Song, Emola type dualities in the character tables of some association schemes, *Mem. Fac. Sci. Kyushu Univ. Ser. A* **44** (1990), 129-143.
- [4] 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.
- [5] 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.
- [6] B. Chang, Decomposition of Gelfand-Graev characters of $GL_3(q)$, *Comm. Algebra* **4** (1976), 375-401.

- [7] K. Chinen and T. Hiramatsu, Hyper-Kloosterman sums and coding theory, Fourth Conference on Algebraic Geometry, Number Theory and Coding Theory, Cryptosystems, Tokyo University, 2000.
- [8] C. Curtis and K. Shinoda, Unitary Kloosterman sums and the Gelfand-Graev representation of GL_2 , *J. Algebra* **216** (1999), 431-447.
- [9] W.M. Kwok, Character tables of association schemes of affine type, *Europ. J. Combin.* **13** (1992), 167-185.
- [10] G. Lachaud and J. Wolfmann, Sommes de Kloosterman, courbes elliptiques et codes cycliques en caractéristique 2. (in French), *C. R. Acad. Sci. Paris Sér. I Math.* **305** (1987), 881-883.
- [11] W.-C.W. Li, Character sums and abelian Ramanujan graphs, *J. Number Theory* **41** (1992), 199-217.
- [12] R. Lidl and H. Niederreiter, "Finite Fields" 2nd ed., Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 1997.
- [13] A. Medrano, P. Myers, H.M. Stark and A. Terras, Finite analogues of Euclidean space, *J. Comput. Appl. Math.* **68** (1996), 221-238.
- [14] W. Schmidt, "Equations Over Finite Fields: An Elementary Approach" Lecture Notes in Math. **536**, Springer-Verlag, Berlin-New York, 1976.
- [15] A. Terras, "Fourier Analysis on Finite Groups and Applications," London Math. Soc. Student Texts **43**, Cambridge University Press, 1999.
- [16] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.* **34** (1948), 204-207.
- [17] J. Wolfmann, The weights of the dual code of the Melas code over $GF(3)$, *Discrete Math.* **74** (1989), 327-329.

Finite analogues of non-Euclidean spaces and Ramanujan graphs

Eiichi Bannai, Osamu Shimabukuro and Hajime Tanaka

Dedicated to the memory of J. J. Seidel

Abstract

This is a companion paper of "Finite Euclidean graphs and Ramanujan graphs" by the same authors.

Finite analogues of the Poincaré upper half plane, i.e., finite upper half plane graphs, were studied by many researchers, including Terras, Evans etc.. Finally, it was proved by combining works of A. Weil, P. Deligne, R. Evans, H. Stark, N. Katz, W. Li and many others, that the finite upper half plane graphs of valency $q + 1$ over the finite field F_q are all Ramanujan graphs. In this paper, we obtain further examples of families of Ramanujan graphs, by using previous works on association schemes and the calculations of their character tables, which are in some sense analogues of the finite upper half planes over finite fields, i.e., finite versions of non-Euclidean spaces. A key observation is that in many (but not all) cases, we can obtain a sharper estimate $|\theta| \leq 2\sqrt{q-2}$ on eigenvalues, instead of the original $|\theta| \leq 2\sqrt{q}$, which was proved by Katz. We combine this observation with the ideas of controlling association schemes and the Ennola type dualities, in our previous papers such as Bannai-Hao-Song (1990), Bannai-Hao-Song-Wei (1991), Bannai-Kwok-Song (1990), Kwok (1991), Tanaka (2001,2002) and many others. At the end, we remark that for each fixed valency $k \geq 3$ there are only finitely many distance-regular Ramanujan graphs of valency k .

Introduction

The finite upper half planes over finite fields \mathbb{F}_q have been studied by many authors. When q is odd, they are defined as follows (see Terras [19, Chapter 19] for details). Namely, let δ be a nonsquare element of \mathbb{F}_q^\times , and we define the *finite upper half plane* H_q by

$$H_q = \{z = x + y\sqrt{\delta} \mid x, y \in \mathbb{F}_q, y \neq 0\} \subset \mathbb{F}_{q^2}.$$

The projective general linear group $PGL(2, q)$ acts transitively on H_q by the fractional linear transformation:

$$g \cdot z = \frac{az + b}{cz + d},$$

for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PGL(2, q)$ and $z \in H_q$. Group theoretically, H_q is the homogeneous space $PGL(2, q)/Z_{q+1}$, where Z_{q+1} is a cyclic subgroup of order $q+1$, and this is identical to $GL(2, q)/GL(1, q^2)$. Also note that the pair $(PGL(2, q), Z_{q+1})$ is a Gelfand-pair, namely, the permutation character of $PGL(2, q)$ acting on $PGL(2, q)/Z_{q+1}$ is multiplicity-free, or equivalently, the associated association scheme is commutative (we refer the reader to [2,1] for the background in the theory of commutative association schemes). In fact, this particular association scheme satisfies the stronger condition that it is symmetric. For odd q , the character table P_1 of the association scheme corresponding to $PGL(2, q)/Z_{q+1}$ is described as follows:

$$P_1 = \begin{bmatrix} 1 & 1 & q+1 & \dots & q+1 \\ 1 & 1 & & & \\ \vdots & \vdots & & & \\ 1 & 1 & (\psi_{ij})_{\substack{1 \leq i \leq q-1 \\ 1 \leq j \leq q-2}} & & \\ 1 & -1 & & & \\ 1 & -1 & & & \\ \vdots & \vdots & & & \\ 1 & -1 & & & \end{bmatrix}. \quad (1)$$

The entries ψ_{ij} are elements of $\mathbb{Q}(\zeta_{q-1}) \cup \mathbb{Q}(\zeta_{q+1})$, where $\zeta_n = \exp(2\pi\sqrt{-1}/n)$, and it is known that they are expressed by using power sums and Soto-Andrade sums (see [19, Chapter 19-21]).

A regular graph of valency k is called *Ramanujan* if all eigenvalues θ such that $|\theta| \neq k$ satisfy

$$|\theta| \leq 2\sqrt{k-1}. \quad (2)$$

By combining works of A. Weil [20], P. Deligne, R. Evans [9,10], H. Stark, N. Katz [11,12], W. Li [14] and many others, it was proved that the finite upper half plane graphs of valency $q+1$ over the finite field \mathbb{F}_q are all Ramanujan graphs, that is, we have

$$|\psi_{ij}| \leq 2\sqrt{q}. \quad (3)$$

for all $1 \leq i \leq q-1$, $1 \leq j \leq q-2$.

Here, we give an example of an interesting family of multiplicity-free permutation groups, or commutative association schemes which are close relatives of the finite upper half planes over finite fields. Namely, we consider the homogeneous space $PGL(2, q)/Z_{q-1}$, where Z_{q-1} is a cyclic subgroup of order $q-1$. Strictly speaking, it is known that the permutation group $PGL(2, q)$ on $PGL(2, q)/Z_{q-1}$ is not multiplicity-free (hence the associated association scheme is not commutative), but if we take $G = Z_2 \times PGL(2, q) \cong GO_3(q)$ and $K = Z_2 \times D_{q-1} (\cong D_{2(q-1)})$ where D_{q-1} is a dihedral subgroup of order $q-1$, then the permutation group G on G/K is multiplicity-free, and moreover, the associated association scheme is also symmetric. The association scheme G/K is of class $q+1$, while the association scheme $PGL(2, q)/Z_{q+1}$ is of class $q-1$. The character table P_2 of the association scheme G/K is of the following form (see [7,13]):

$$P_2 = \begin{bmatrix} 1 & 1 & 2(q-1) & 2(q-1) & q-1 & \dots & q-1 \\ 1 & 1 & q-3 & q-3 & -2 & \dots & -2 \\ 1 & -1 & q-1 & -(q-1) & 0 & \dots & 0 \\ 1 & 1 & -2 & -2 & & & \\ \vdots & \vdots & \vdots & \vdots & & & \\ 1 & 1 & -2 & -2 & (-\psi_{ij})_{\substack{1 \leq i \leq q-1 \\ 1 \leq j \leq q-2}} & & \\ 1 & -1 & -2 & 2 & & & \\ 1 & -1 & -2 & 2 & & & \\ \vdots & \vdots & \vdots & \vdots & & & \\ 1 & -1 & -2 & 2 & & & \end{bmatrix}. \quad (4)$$

Note that the same quantities ψ_{ij} appear in the both character tables. This is not an accident, but is a phenomenon called Ennola type duality, and was observed and explained in Bannai-Kwok-Song [7]. In general, the graphs of valency $q-1$ attached to G/K , i.e., the graphs of valency $q-1$ whose edge sets are orbits of G on $G/K \times G/K$, are not Ramanujan (all the eigenvalues of these graphs appear in the corresponding columns of P_2). However, it is easy to see that if the condition $|\psi_{ij}| \leq 2\sqrt{q-2}$ ($1 \leq i \leq q-1$) is satisfied for a fixed $j \in \{1, 2, \dots, q-2\}$, then the graph of valency $q-1$ corresponding to the column of P_2 is Ramanujan. As we will see in Section 8, our computer experiments show that for odd primes $p < 500$, this condition is satisfied about approximately 90 percent cases of j . Therefore, we obtain many Ramanujan graphs with valency $p-1$. Later, for $q = p^r$ with r odd, we will prove a rigorous (but easy) result $|\psi_{ij}| < 2\sqrt{q}$, which is weaker than $|\psi_{ij}| \leq 2\sqrt{q-2}$, but better than the previous bound (3) (although we have assumed (3), see Lemma 2.1). We will use this result to obtain many other examples of families of Ramanujan graphs. See theorems 2.2, 4.2 and 6.1.

The remaining part of the paper is devoted to showing that essentially the same methods work for far wider classes of association schemes. Namely, we consider all the association schemes considered in papers [5,6,17], and obtain many examples of families of Ramanujan graphs.

Note that, by our constructions, we have only finitely many such graphs for each fixed valency, and so this does not give the answer whether we can construct infinitely many Ramanujan graphs with a fixed valency (cf. [15]). However, we still believe that the constructions of many examples of Ramanujan graphs given in this paper are interesting even if the valency is not fixed. In passing, as an immediate consequence of Bannai-Ito [4] on the spectra of distance-regular graphs, we will show that for each $k \geq 3$, there are only finitely many Ramanujan distance-regular graphs with valency k .

References

- [1] E. Bannai, Character tables of commutative association schemes, in: *Finite Geometries, Buildings, and Related Topics*, W.M. Kantor *et al.* (eds), Clarendon Press, Oxford, 1990, pp. 105-128.
- [2] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin/Cummings, Menlo Park, CA, 1984.
- [3] E. Bannai and T. Ito, The study of distance-regular graphs from the algebraic (i.e., character theoretical) viewpoint, in: *Proceedings of Symposia in Pure Mathematics*, Vol. 47, Amer. Math. Soc., Providence, RI, 1987, pp. 343-349.
- [4] E. Bannai and T. Ito, On distance-regular graphs with fixed valency, IV, *European J. Combinatorics*, **10** (1989), 137-148.
- [5] E. Bannai, S. Hao, 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.

- [6] E. Bannai, S. Hao, 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.
- [7] 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.
- [8] E. Bannai, O. Shimabukuro and H. Tanaka, Finite Euclidean graphs and Ramanujan graphs, submitted.
- [9] R. Evans, Character sums as orthogonal eigenfunctions of adjacency operators for Cayley graphs, in: *Contemporary Mathematics*, Vol. 168, Amer. Math. Soc., Providence, RI, 1994, pp. 33-50.
- [10] R. Evans, Spherical functions for finite upper half planes with characteristic 2, *Finite Fields Appl.*, **1** (1995), 376-394.
- [11] N.M. Katz, Estimates for Soto-Andrade sums, *J. Reine Angew. Math.*, **438** (1993), 143-161.
- [12] N.M. Katz, A note on exponential sums, *Finite Fields Appl.*, **1** (1995), 395-398.
- [13] 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.
- [14] W.-C.W. Li, *Number Theory with Applications*, World Scientific, River Edge, NJ, 1996.
- [15] A. Lubotzky, *Discrete groups, Expanding Graphs and Invariant Measures*, Birkhäuser Verlag, Basel, 1994.
- [16] J. Soto-Andrade, Geometrical Gel'fand models, tensor quotients, and Weil representations, in: *Proceedings of Symposia in Pure Mathematics*, Vol. 47, Amer. Math. Soc., Providence, RI, 1987, pp. 305-316.
- [17] H. Tanaka, On some relationships among the association schemes of the orthogonal groups acting on hyperplanes, master thesis, Kyushu Univ., 2001.
- [18] H. Tanaka, A four-class subscheme of the association scheme coming from the action of $PGL(2, 2^f)$, *European J. Combinatorics*, **23** (2002), 121-129.
- [19] A. Terras, *Fourier Analysis on Finite Groups and Applications*, London Math. Soc. Student Texts **43**, Cambridge University Press, 1999.
- [20] A. Weil, On the Riemann hypothesis in functionfields, *Proc. Nat. Acad. Sci. U. S. A.*, **27** (1941), 345-347.

高次元の双対弧の構成とその埋め込み次元

吉荒 聡 (Satoshi Yoshiara)

大阪教育大学 数理科学講座

1 個人的な動機

Janko の発見した 4 つの散在型単純群のうち、最も位数の大きい J_4 (位数 86, 775, 571, 046, 077, 562, 880 = $2^{21}3^5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$) の位数 2 の元の中心化群 C は

$$2_+^{1+12}(3M_{22})2$$

という構造をしている。すなわち C の最大正規 2-部分群 $O_2(C)$ は位数 2^{13} の extraspecial group (中心、交換子部分群、フラッチニ部分群がすべて位数 2) で位数 2^7 の基本可換部分群を持ち、剰余部分群 $C/O_2(C)$ は 22 次のマシュー群 M_{22} の位数 3 の (非分裂) 中心拡大 $3M_{22}$ を指数 2 の部分群に持つ。拡大 $C/O_2(C)$ は分裂しない。

剰余群 $\bar{C} := C/O_2(C) \cong 3(M_{22})2$ は $O_2(C)/Z(O_2(C)) \cong 2^{12}$ に忠実に作用し、二次形式 $Q(xZ(O_2(C)), yZ(O_2(C))) := [x, y]$ を保つので直交群 $GO_{12}^+(2) = O_{12}^+(2) \cdot 2$ の部分群になるが、指数 2 の部分群 $\bar{C}' \cong 3 \cdot M_{22}$ は更に、あるユニタリ形式を不変にし、 $SU_6(2^2)$ に含まれる (\bar{C}' の外側の位数 2 の元は体 $GF(4)$ の自己同型を引き起こす)。 \bar{C}' の中心 3 はユニタリ群 $SU_6(2^2)$ の中心に対応するので、 $M_{22} \cong \bar{C}'/Z(\bar{C}')$ は $PSU_6(2^2) = U_6(2)$ の部分群と同型である。そこで、22 次の置換群 M_{22} の (ユニタリ計量を持つ) 射影空間 $PG(5, 2^2)$ への射影表現が得られた。

この表現を調べてみると、一つの面白い事実に気づく。すなわち、 $PG(5, 2^2)$ の (ユニタリ計量に関して全等方的な) 2 次元 (射影) 部分空間たちへの M_{22} の作用の軌道中に、長さ 22 のものがただ一つ存在する のである。これを $\mathcal{H}(M_{22})$ と書こう。従って、 M_{22} はこの軌道 $\mathcal{H}(M_{22})$ 上に 3 重可移作用し、特に、 $\mathcal{H}(M_{22})$ に属するどの二つ (及びどの 3 つ) の部分空間の共通部分も一定の次元を持つ。 $\mathcal{H}(M_{22})$ のメンバーである部分空間は 2 次元なので、可能性は限られ、次の事実が確かめられる。

Observation $PG(5, 2^2)$ の 22 個の 2 次元部分空間たちからなる族 $\mathcal{H}(M_{22})$ で、その上にマシュー群 M_{22} が自然に作用し、次の交叉性を持つものが存在する。

- (DA1) どの二つの相異なるメンバーも射影点で交わる
- (DA2) どの 3 つの互いに相異なるメンバーの交わりも空である
- (DA3) $\mathcal{H}(M_{22})$ のメンバーの全体は全空間 $PG(5, 2^2)$ を生成する。

以上の事実は古くから知られていて、例えば Atlas of Finite Groups の M_{22} の構成のうちの項 unitary に具体的な部分空間の実現が記されている。私自身、群

J_4 を調べたことがあり、この様な事実は知っていたのだが、次のようなきっかけで再び、この事実に向き合うことになり、より一般にこの様な交叉性を持つ部分空間の族そのものに興味を抱くようになった。

すなわち、非古典的な極空間の拡大の構成という問題を研究しているうち、このような拡大を与える“種”となるベクトル空間の部分空間の族 (Y -族) の一つの実例が、上の $\mathcal{H}(M_{22})$ 中に「埋め込める」ことに気づいたのであった [Yo0]。更に、上の例は、このような交叉性を持つうちで最大な対象 (後に定義する双対超卵型) であり、それは自然に半倍射影平面 (*semibiplane*) という幾何学的対象 (射影平面の公理を変化させて、2 点を通る線は 0 または 2 本、及びその双対を仮定した幾何) を生み出すので、今まで全く気づかれていなかった多くの高い対称性を持つ半倍射影平面が構成できた [PY]。更に (これは私自身がやったことではないのだが) 有限単純群の分類を仮定すれば、自己同型群が二重可移に作用するような上記の交叉性を持つ対象の分類が出来て [HP]、それによって M_{22} に対する上の部分空間族 $\mathcal{H}(M_{22})$ が特徴付けられる。このような事に味をしめて、上記の交叉性を満たす純有限幾何学的な対象そのものに興味を持つようになったのである。

2 高次元の双対弧

先ほどの Observation の性質を満たす部分空間の族に名前をつけよう。

定義 q を素数のべきとする。 q 元体上の n 次元射影空間 $PG(n, q)$ の d 次元部分空間の族 \mathcal{A} は、次の条件を満たすとき $PG(n, q)$ 中の d 次元双対弧 (d -dimensional dual arc in $PG(n, q)$) と呼ばれる [Yo2]。

- (DA1) どの二つの相異なるメンバーも射影点で交わる
- (DA2) どの3つの互いに相異なるメンバーの交わりも空である
- (DA3) \mathcal{A} のメンバーの全体は全空間を生成する。

次に見るように、 \mathcal{A} が上の条件を満たすとき、 \mathcal{A} は高々 $\theta_q(d) + 1$ 個のメンバーからなる。ただし $\theta_q(d) := q^{d-1} + \dots + q + 1$ とする。

まず \mathcal{A} のメンバー A_0 を一つ取り固定する。すると A_0 以外のメンバー A に対して A と A_0 の共通部分を対応させる写像は、条件 (DA1) により $\mathcal{A} \setminus \{A_0\}$ から A_0 上の射影点全体のなす集合 $PG(A_0)$ への写像である。しかも条件 (DA2) により、この写像は単射である。従って、 $|\mathcal{A} \setminus \{A_0\}| = |\mathcal{A}| - 1 \leq |PG(A_0)| = \theta_q(d)$ であり、求める評価式を得る。

定義 可能な最大数 $\theta_q(d) + 1$ 個のメンバーを持つ双対弧 \mathcal{A} を双対超卵型 (dual hyperoval) という。また次に大きな $\theta_q(d)$ 個のメンバーを持つ双対弧 \mathcal{A} を双対卵型 (dual oval) という。

前節における $PG(5,4)$ の 2 次元部分空間の族 $\mathcal{H}(M_{22})$ は $22 = \theta_4(2) + 1$ 個のメンバーからなるので、 $\mathcal{H}(M_{22})$ は $PG(5,4)$ 中の 2 次元双対超卵型であることに注意しよう。

この概念が初めて現れたのは論文 [HP] であるが、その背後にはマシュー群 M_{22} が自然に作用する $PG(5,4)$ 中の 22 枚の射影平面の集合 $\mathcal{H}(M_{22})$ を幾何学的に捉えようとする Pasini, 吉荒, Del Fra, Huybrechts 等に共通する関心があった。(私の個人的な動機については既に触れた。) 射影空間 $PG(n,q)$ 中の 1 次元双対弧 A が存在すれば $n = 2$ であり、 A はどの相異なる 3 線も一点では交わらないような線の集合であることがすぐ確かめられる。従って、これは射影平面中の従米の意味での双対弧に他ならない。この意味で、 d 次元双対弧という概念は射影平面中の双対弧 (線からなる) の概念を、高次元空間中の d 次元部分空間に一般化したものであるといえる。

以下 $d \geq 2$ を中心に考える。

高次元の双対弧に関する中心問題は以下の 2 つである。

- (a) $PG(n,q)$ 中の d 次元双対超卵型が存在するならば q は偶数か?
- (b) $PG(n,q)$ 中の d 次元双対弧が存在するとき、全空間の次元 n を d, q の関数で上から押さえることができるか?

本来の意味の双対超卵型 (1 次元双対超卵型 自動的に $PG(2,q)$ 中になる) に関しては、良く知られているように、その存在は q が偶数である時に限る。問題 (a) はこの命題の類似が高次元においても成立するか否かを問うものであるが、現時点では完全に解決できていない。詳細はここでは略す。本談話の中心は、問題 (b) に関するものである。

3 全空間の次元の評価

$PG(n,q)$ 中の d 次元双対弧が存在すると仮定すると、公理 (DA1) から明らかに $n \geq 2d$ である。 $PG(2d,q)$ (q は偶数) 中の d 次元双対超卵型の構成法は決定されており [CT]、 $PG(2d+1,2)$ 中の d 次元双対超卵型の族の例は吉荒が与えている [Yo1] (これを剰余-5 章参照-とする双対超卵型は多くの場合自分自身に限る)。また $D = d(d+3)/2$ とするとき、Huybrechts [Hu] は $PG(D,2)$ 中の d 次元双対超卵型を構成している。また、任意の q に対する $PG(5,q)$ 中の 2 次元双対卵型の Veronese 写像を用いた構成が吉荒の論文 [Yo0] 中に (明示されない形で) 現れている。(当時は高次元の双対卵型、双対超卵型、双対弧といった概念は無かった。) この構成を一般化したものが最近 Thas-van Maldeghem により与えられている [TV]。これらについては後で多少詳しく触れる。

さて、問題 (b) に関して今まで得られているうちで最も一般的な結果は、Del Fra [DF] による次の命題である。

命題 $PG(n, q)$ 中の d 次元双対弧が存在するならば次の不等式が成立する。

$$n < 2d + \sum_{j=1}^{d-1} j q^{d-j}$$

Del Fra の評価式の中には q が現れているが、 q を含まない次の形の改良が得られた [Yo3]。この結果を報告し、それがほぼベストであることを示す構成を紹介することが本談話の目的である。ここで \mathcal{A} は簡単のため卵型とするが、十分多くのメンバーからなる双対弧 ($|\mathcal{A}| \geq \theta(d) - \alpha$ 、ここで α は $0 \leq \alpha \leq \alpha(q)$ を満たす整数で $\alpha(q) = \{(q-3)q^{d+1} + (q^d - q^2) + (q-1)d + (3q-1)\}/(q-1)^2$) と仮定しても $q > 2$ のときには同じ結論が成立する。また $q = 2$ の場合、[Yo3] では \mathcal{A} を双対超卵型と仮定しているが、4章で注意するように双対卵型の存在は双対超卵型の存在を導くので、下記の定理は確かに成立する。更に $q = 2$ の場合も $q > 2$ の場合と同じ評価が得られると予想しているが (Del Fra もそれに同意している)、今のところ証明出来ない。

定理 (吉荒, [Yo3], 2002) $PG(n, q)$ 中の d 次元双対卵型 \mathcal{A} が存在するならば次の不等式が成立する。

$$(i) \quad q > 2 \text{ ならば } n \leq 2d + \sum_{j=1}^{d-1} j = d(d+3)/2 = D$$

$$(ii) \quad q = 2 \text{ ならば } n \leq D + 2$$

証明のアイデアは自然であり $q > 2$ の場合の証明は簡単である。講演のときには省略したので概略を述べておく。詳しくは [Yo3, Section2] 参照。

まず \mathcal{A} の二つのメンバー A, B の生成する $2d$ 次元部分空間 $U_0 := \langle A, B \rangle$ から出発し、それとなるべく小さい次元で交わるようなメンバー A_0 を $\mathcal{R}_0 := \mathcal{A} - \{A, B\}$ から選ぶ。 $d - l_0 := \dim(U_0 \cap A_0)$ とする。 $l_0 = 0$ ならば \mathcal{A} のどのメンバー X を取っても $X \subset U_0$ となるので、 $PG(n, q) = \langle A \in \mathcal{A} \rangle = U_0$ であり、このときには当然命題の評価式は成立する。そこで $l_0 \geq 1$ としてよい。また、どのメンバー $X \in \mathcal{R}_0$ についても $U_0 \cap X$ は点 $A \cap X$ と点 $B \cap X$ を通る線を含むので $d - l_0 \geq 1$ 、つまり $l_0 \leq d - 1$ である。

以下 $i = 0, 1, 2, \dots$ 、に対して \mathcal{R}_0 の部分集合 \mathcal{R}_i 、部分空間 U_i 、整数 l_i を次のように帰納的に定義する。 \mathcal{R}_{i-1} 、 U_{i-1} 、 l_{i-1} が与えられているとする。このとき、まずメンバー $X_{i-1} \in \mathcal{R}_{i-1}$ を $\dim(U_{i-1} \cap X_{i-1}) = d - l_{i-1}$ を満たすように取り、固定する。そして

$$\mathcal{R}_i := \{X \in \mathcal{R}_{i-1} \setminus \{X_{i-1}\} \mid X \cap X_{i-1} \notin U_{i-1}\},$$

$$U_i := \langle U_{i-1}, X_{i-1} \rangle,$$

$$d - l_i := \min\{\dim(U_i \cap X) \mid X \in \mathcal{R}_i\}.$$

とおく。この作り方から、集合 \mathcal{R}_i ($i = 0, 1, \dots$) の列は真の減少列、部分空間 U_i ($i = 0, 1, \dots$) の列は真の増大列、整数 l_i ($i = 0, 1, \dots$) の列は真の減少列であることが確認される。すると $d-1 \geq l_0$ なので、最大 $d-1$ 回このような操作を行うと $l_k = 0$ の状態に到達する ($1 \leq k \leq d-1$)。このとき U_k の次元は

$$\begin{aligned} & \dim(U_{k-1}) + \dim(X_{k-1}) - \dim(U_{k-1} \cap X_{k-1}) \\ &= \dim(U_{k-1}) + l_{k-1} = \dots = \dim(U_0) + l_0 + \dots + l_{k-1} \\ &\leq 2d + \sum_{j=1}^{d-1} j = D \end{aligned}$$

と評価できることに注意する。

そこで、示すべきは $U_k = PG(n, q)$ なのであるが、ここが多少微妙である。条件 $l_k = 0$ は部分空間 U_k がすべての \mathcal{R}_k のメンバーを含むことと同値であるから、重要なことは、 \mathcal{R}_k が十分多くのメンバーを含むことを示す点にある。 $|\mathcal{R}_k|$ の評価式をつくり $q > 2$ ならばそれが $\theta_q(d-1) + 1$ より大きいことを示す。すると任意のメンバー $X \in \mathcal{A}$ に対して、 X と \mathcal{R}_k のメンバー達の交点は少なくとも $\theta_q(d-1) + 1$ 点存在する (双対弧の公理 (DA1,2) から)。特に、 \mathcal{R}_k の生成する部分空間 U_k と X の交わり $U_k \cap X$ はこの個数以上の点を含む。しかし、 $\theta_q(d-1)$ は $d-1$ 次元空間の点の総数であるから、 $X \cap U_k$ が X の $(d-1)$ 次元部分空間におさまることは無いので、 $X \subset U_k$ を得る。従って U_k は \mathcal{A} のすべてのメンバー X を含み、 $U_k = PG(n, q)$ であり、これから求める評価式が得られるのである。($q = 2$ のときは $|\mathcal{R}_k|$ の評価式が甘くなるので $U_k = PG(n, q)$ が結論できず、議論に多少の修正が必要となる。)

4 双対弧の二つの構成法

この章では、ヴェロネーズ構成とキャップ構成という、高次元の双対弧 (卵型、超卵形) の二つの構成法を示す。まず一般に次が示せることに注意する。

命題 [Yo3, Section3] q を偶数とする。 \mathcal{A} が $PG(n, q)$ 中の d 次元双対卵型ならば、 \mathcal{A} のメンバーをすべて含む $PG(n, q)$ 中の d 次元双対超卵型がただ一つ存在する。

証明の方針は次の通りである。 $|\mathcal{A}| = \theta_q(d)$ なので、 \mathcal{A} のそれぞれのメンバー X に対して $X \cap Y$ ($Y \in \mathcal{A} \setminus \{X\}$) の形にあらわされないような X の点のただ一つ存在する。これを X 上の“穴”という心で $h(X)$ と記す。 \mathcal{A} が超卵型に拡張されるとすれば、付け加えるべき (ただ一つの) d 次元部分空間は $H := \{h(X) \mid X \in \mathcal{A}\}$ しかありえない。そこで H が実際に部分空間になることを示すのが目標となる。この検証には、 $PG(n, q)$ の任意の $n-d$ 次元部分空間 Y をとるとき $H \cap Y \neq \emptyset$ であることを示して、Bose-Burton の定理 [HT2, Theorem 3.5] を適用する。

ヴェロネーズ構成 (この構成がはっきりと現れた文献は [TV] が初めてだと思われるが、前述のごとく [Yo0] にもその粗形が見出される。以下 [Yo3, Section 3] に従って記述するが、これは Thas-van Maldeghem の構成の“双対形”に相当する。)

V を $GF(q)$ 上の階数 (射影次元と区別するためベクトル空間の次元を階数と呼ぶ) $d+1$ のベクトル空間とし、 e_i ($i = 0, 1, \dots, d$) をその一つの基底とする。また W を $GF(q)$ 上の階数 $D+1$, $D = d(d+3)/2$, のベクトル空間とし、その基底を添え字付けるのに $0 \leq i \leq j \leq d$ を満たす整数 i, j の順序対 (i, j) (全部で $\binom{d+1}{2} + (d+1) = D+1$ 個ある) を取って、 e_{ij} ($0 \leq i \leq j \leq d$) を W の一つの基底とする。このときヴェロネーズ写像 (Veronesean map) とは次の式で与えられる V から W への (または対応する射影空間 $PG(V) \cong PG(d, q)$ から射影空間 $PG(W) \cong PG(D, q)$ への) 写像 ζ のことである [HT1, Section 25.1]。

$$\zeta : V \ni \sum_{i=0}^d x_i e_i \mapsto \sum_{0 \leq i \leq j \leq d} x_i x_j e_{ij} \in W.$$

さて $PG(V) \cong PG(d, q)$ の各点 P に対し、 P の $PG(V)$ における双対 P^\perp (適当な非退化双一次形式に関する) は $PG(V)$ の $d-1$ 次元部分空間であるがそのヴェロネーズ写像 ζ による像 $\zeta(P^\perp)$ を考え、その $PG(W) \cong PG(D, q)$ における双対を取って $X(P)$ とおく:

$$X(P) := (\zeta(P^\perp))^\perp.$$

このとき $X(P)$ は $PG(W)$ における d 次元の部分空間になることが確かめられる。

例えば $P = [e_0]$ とすれば V での自然な内積 $(\sum_{i=0}^d x_i e_i, \sum_{i=0}^d y_i e_i) := \sum_{i=0}^d x_i y_i$ に関する双対 P^\perp は e_1, \dots, e_d により生成される部分空間 $\{\sum_{i=0}^d x_i e_i \mid x_0 = 0\}$ に等しく、そのヴェロネーズ写像 ζ による像 $\zeta(P^\perp)$ は

$$\zeta(P^\perp) = \left\{ \sum_{0 \leq i \leq j \leq d} x_i x_j e_{ij} \mid x_0 = 0 \right\}$$

となる。 $\zeta(P^\perp)$ の元の e_{0j} ($j = 0, \dots, d$) の係数はみな 0 であるから、 $PG(W) \cong PG(D, q)$ での自然な内積 $(\sum_{0 \leq i \leq j \leq d} x_{ij} e_{ij}, \sum_{0 \leq i \leq j \leq d} y_{ij} e_{ij}) := \sum_{0 \leq i \leq j \leq d} x_{ij} y_{ij}$ による $\zeta(P^\perp)$ の双対 $X(P)$ は

$$\langle e_{0j} \mid j = 0, \dots, d \rangle$$

と一致し、これは確かに $PG(W) \cong PG(D, q)$ の d 次元部分空間である。

このようにして $\theta_q(d)$ 個の $PG(V)$ の点 P に対応する $\theta_q(d)$ 個の $PG(W)$ の d 次元部分空間達が得られるが、ここで次が確かめられる。

命題 上の記号の元で $\mathcal{AV}_d(q) := \{X(P) \mid P \in PG(V)\}$ とすれば $\mathcal{AV}_d(q)$ は $PG(W) \cong PG(D, q)$ 中の d 次元双対卵型をなす。 q が偶数のときには

この章のはじめの命題から、この双対卵型 $\mathcal{AV}_d(q)$ は $PG(D, q)$ 中の d 次元双対超卵型 $\mathcal{HV}_d(q)$ に一意的に拡張される。

この構成による双対卵型（超卵型）の持つ基本性質として次が確かめられる。

性質 (V) $PG(V)$ の相異なる 3 点 P, Q, R に対して、 P, Q, R が $PG(V)$ の一つの線上にあることと $X(P)$ が $\langle X(Q), X(R) \rangle$ に含まれることは同値である。

キャップ構成 [Yo3, Section3] κ を $PG(d+1, q)$ を生成するキャップ (*cap*) とする。すなわち κ は $PG(d+1, q)$ の射影点の集合で $PG(d+1, q)$ を生成し、 $PG(d+1, q)$ のどんな線も κ と 2 点以下で交わるようなものである（これは射影平面における弧の概念の高次元への別の形の一般化でもある）。 V を階数 $d+2$ の $GF(q)$ 上のベクトル空間、 e_i ($i = 0, \dots, d+1$) をその一つの基底とする。 V とそれ自身の外積空間 $V \wedge V$ を考えると、これは $e_i \wedge e_j$ ($0 \leq i < j \leq d+1$) を基底とする階数 $\binom{d+2}{2} = D+1$, $D = d(d+3)/2$, のベクトル空間であり、従って $PG(V \wedge V) \cong PG(D, q)$ である。

さて $PG(V) \cong PG(d, q)$ のキャップ κ の各点 $P = [p]$ に対し

$$A(P) := \{p \wedge x \mid x \in V\}$$

とおくと、ウェッジ積の線形性から、 $V \ni x \mapsto p \wedge x \in A(P)$ は全射線形写像で、核は $\langle p \rangle$ であるから、 $A(P)$ は階数 $d+1$ の $V \wedge V$ の部分空間である。 $A(P)$ は P の基底 p の取り方によらない。従って、キャップ κ の点 P に対応して $PG(V \wedge V) \cong PG(D, q)$ の d 次元部分空間 $A(P)$ 達が得られた。このとき次が確かめられる。

命題 上の記号の元で $\mathcal{A}(\kappa) := \{A(P) \mid P \in \kappa\}$ とすれば

$\mathcal{A}(\kappa)$ は $|\kappa|$ 個のメンバーからなる $PG(V \wedge V) \cong PG(D, q)$ 中の d 次元双対弧である。

次がこの構成によって得られた双対弧の持つ特徴的な性質である。この性質を (T) と呼ぶのは論文 [DF] 中の用語に従っている。

性質 (T) κ の相異なる 3 点 P, Q, R に対し、つねに $\dim(A(P) \cap \langle A(Q), A(R) \rangle) = 1$ である。

キャップ κ は通常さほど大きくないので、 $\mathcal{A}(\kappa)$ が双対（超）卵型になることは期待できないが、 $q=2$ の場合は例外である。すなわち $q=2$ のとき、 $PG(d+1, 2)$ の超平面 H を取りその補集合を κ_H とすると、 $|\kappa_H| = \theta_2(d+1) - \theta_2(d) = 2^{d+1}$ であり、 H に含まれない $PG(d+1, 2)$ の線（3点からなる）は H とただ一点で交わることから、 κ_H は $PG(d+1, 2)$ を生成するキャップをなす。 $q=2$ なので $|\kappa_H| = 2^{d+1} = \theta_2(d) + 1$ であることから、次を得る。

応用 $PG(d+1, 2)$ のキャップ κ_H (超平面の補集合) から構成された $A(\kappa_H)$ は $PG(D, 2)$ 中の d 次元双対超卵型をなす。

この双対超卵型はもともと Huybrechts [Hu] が見出したものであるが、それがより一般にキャップからの双対弧の構成の中で位置付けられ、性質 (T) を満たすことの根拠がはっきりしたことになる。

5 二つの構成の比較と関連するいくつかの問題

4章で見たように任意の素数べき q 及び任意の正の整数 d に対して $PG(D, q)$, $D = d(d+3)/2$, 中の d 次元双対卵型 $AV_d(q)$ が存在する。従って $q > 2$ の場合、3章の定理 (i) における評価式 $n \leq D$ で等号が成立し、評価式は best possible である。

また $q = 2$ の場合、4章において構成された $PG(D, 2)$ 中の二つの d 次元双対超卵型 $\mathcal{H}V_d(2)$ と $A(\kappa_H)$ は同型ではない (すなわち $PG(D, 2)$ の自己同型で $\mathcal{H}V_d(2)$ を $A(\kappa_H)$ に移すものは存在しない) ことに注意しよう。というのは、 $A(\kappa_H)$ は性質 (T) を満たすが、一方 $\mathcal{H}V_d(2)$ は性質 (V) を満たすので性質 (T) を満たし得ないからである。この事実は Del Fra による $PG(5, 2)$ 中の 2 次元双対超卵型の分類 ($\mathcal{H}V_2(2)$ か $A(\kappa_H)$ のどちらかに同型) の裏づけにもなっている。

更に $q = 4, d = 2$ の場合 $PG(5, 4)$ 中の二つの 2 次元双対超卵型 $\mathcal{H}(M_{22})$ (第1章で紹介した) と $\mathcal{H}V_2(4)$ も同型ではない。実際、 $\mathcal{H}(M_{22})$ のメンバー上へのマシュー群 M_{22} の作用の 3 重可移性から $\mathcal{H}(M_{22})$ は性質 (T) を満たし、従って性質 (T) を満たさない $\mathcal{H}V_2(4)$ とは同型になりえない。

以上の事実を踏まえて幾つか問題を提起しておきたい。

問題 1 $q = 2$ のときの評価式 $n \leq D + 2$ を $n \leq D$ に改良できないか?

私も Del Fra もそのように出来るはずだと信じているが、完全な証明にはまだアイデアが足りない状態である。

問題 2 $D = d(d+3)/2$ に対して $PG(D, 2)$ 中の d 次元双対超卵型は分類できるか?

一番楽観的なのは $d = 2$ のときと類似の現象が成り立つと期待することであるが、私ははっきりした見通しを持っていない。Thas-van Maldeghem の仕事はいくつかの付加的条件の元でヴェロネーズ構成による双対超卵型 $AV_d(q)$ を (一般の q に対して) 特徴付けたとみなせる。彼らの仕事を良く理解することが、この問題の解決への第一歩となるであろう。その対極として、Huybrechts の仕事 [Hu] は、キャップ構成による双対超卵型 $A(\kappa_H)$ を性質 (T) によって特徴付けようと試みたものとみなせる。こちらの理解も肝要であろう。

問題3 $PG(5, 4)$ 中の2次元双対超卵型 $\mathcal{H}(M_{22})$ のより良い構成法はないか?

$q > 2$ に対する $PG(D, q)$ 中の双対弧の全体の中で、 $\mathcal{H}(M_{22})$ は性質 (T) を満たすという点で、非常に稀な存在のように感じられる。そうだとすれば、 $\mathcal{H}(M_{22})$ を特別な場合を含むような幾何学的に記述できる無限系列の構成は存在しないのかもしれないが、やはり M_{22} の作用がはっきり見えるような明快な構成を期待したい。

問題4 キャップ構成による双対弧 $A(\kappa)$ に、もとのキャップ κ の性質がどの程度反映しているのか?

例えば、幾つか面白い極大キャップが知られているが、それらに対する双対弧はどんな性質を持っているのか? 極大弧 κ に対する双対弧 $A(\kappa)$ は極大か? -つまり $A(\kappa)$ を真に含む双対弧は存在するか? 単に双対弧とせずに、性質 (T) を満たす双対弧に限って見たらどうか?

問題5 ヴェロネース構成による双対(超)卵型 $\mathcal{AV}_d(q)$ ($\mathcal{HV}_d(q)$) の“剰余”双対(超)卵型を完全に決定せよ。

ここで一般に $PG(W) \cong PG(m, q)$ 中の d 次元双対弧 \bar{A} が $PG(V) \cong PG(n, q)$ 中の d 次元双対弧 A の剰余であるとは、ある線形写像 $\rho: V \rightarrow W$ が存在して、 A のどのメンバー X の像 $\rho(X)$ も \bar{A} のメンバーであり、誘導される写像 $\rho: A \rightarrow \bar{A}$ が全単射であることと定義される。すると次の命題が容易に示される。

命題 [Yo3, Section3] A を $PG(V) \cong PG(n, q)$ 中の d 次元双対弧とする。 V の部分空間 K で次の性質 (*) を満たすものがあれば、

$$(*) \quad A \text{ の任意の相異なるメンバー } X, Y \text{ に対して } K \cap (X, Y) = \emptyset$$

標準的な写像 $\rho: V \rightarrow V/K = W$ による A のメンバーの像の集まりを \bar{A} とするとき \bar{A} は $PG(W)$ 中の d 次元双対弧であって A の剰余である。

逆に、 A の任意の剰余 \bar{A} に対し、それを与える線形写像 ρ の核を K とすれば上の性質 (*) が成立する。

この命題により、剰余を求める問題は性質 (*) を満たす部分空間 K の存在に帰着される。その方針で、例えば $2d \leq n \leq D$ を満たす任意の正の整数 n に対して $PG(n, 2)$ 中の d 次元双対超卵型で $A(\kappa_H)$ の剰余であるものが存在する事が確かめられている ([PY, Proposition 6.8] の証明中の議論がそれに相当する)。同様に、 $d \geq 5, q > 2$ のとき $4d - 2 \leq n \leq D$ を満たす任意の正の整数 n に対して $PG(n, q)$ 中の d 次元双対卵型 (q が偶数ならば超卵型) で $\mathcal{AV}_d(q)$ (q が偶数のときには $\mathcal{HV}_d(q)$) の剰余であるものが存在する事が確かめられているが [Yo3, Section 3]、そこでの議論は $2 \leq d \leq 4$ や $2d \leq n \leq 4d - 3$ ではうまく行かない。そこを詰めるのがこの問題の意図であり、これが肯定的に解決されれば、すべて

の素数べき q と正の整数 d 及び $2d \leq n \leq D$ を満たすすべての正の整数 n に対して $PG(n, q)$ 中の d 次元双対 (超) 卵型の存在が確かめられたことになる。

問題 6 q を素数べき、 d を自然数とする。このとき $2d \leq n \leq D$ を満たす任意の自然数 n に対し、 $PG(n, q)$ 中の d 次元双対弧でそれを剰余とするような双対弧は自分自身に限るようなものが存在するか？

3章の定理から $q > 2$ で $n = D$ ならば問題への解答は肯定的である。[PY] で示されているように、[Yo1] で構成された $PG(2d+1, 2)$ 中の d 次元双対超卵型の多くに対して、それを剰余とする双対超卵型は自身に限る。従って $q = 2, n = 2d+1$ のときにも問題への解答は肯定的である。

参考文献

- [DF] A. del Fla, On d -dimensional dual hyperovals, *Geometriae Dedicata* **79** (2000), 157-178.
- [CT] B. Cooperstein and J. A. Thas, On generalized k -arcs in $PG(2n, q)$, preprint.
- [Hu] C. Huybrechts, $c.AG^*$ -geometries and their consequences for some families of d -dimensional subspaces in $PG(m, q)$, to appear in *Discrete Math.*
- [HP] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, *Contrib. Algebra Geom.* **40** (1999), 503-532.
- [HT1] J. W. P. Hirschfeld and J. A. Thas, *General Galois Geometries*, Oxford University Press, 1993.
- [HT2] J. W. P. Hirschfeld and J. A. Thas, *Projective Geometries over Finite Fields*, Second Edition, Oxford University Press, 1998.
- [PY] A. Pasini and S. Yoshiara, On a new family of flag-transitive semibiplanes, *European J. Combin.* **22** (2001), 529-545.
- [TV] J. A. Thas and H. van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, preprint, May, 2002.
- [Yo0] S. Yoshiara, A construction of extended generalized quadrangles using the Veronesean, *European J. Combin.* **18** (1997), 853-848.
- [Yo1] S. Yoshiara, A new family of d -dimensional dual hyperovals in $PG(2d+1, 2)$, *European J. Combin.* **20** (1999), 489-503.
- [Yo2] S. Yoshiara, On a family of planes of a polar space, *European J. Combin.* **22** (2001), 107-118.
- [Yo3] S. Yoshiara, Ambient spaces of dimensional dual arcs, submitted for publication, July, 2002.

Association schemes defined by the action
of finite orthogonal groups on the external lines

Tatsuya Fujisaki
Graduate school of mathematics
Kyushu University

November 26, 2002

1 Introduction

In this paper, we consider the association scheme defined by the action of the orthogonal group over \mathbf{F}_q on the external lines, where q is a power of 2. First we consider relations between the action of orthogonal group and that of its commutator subgroup on the set of external lines. Next we compute the character tables of the association schemes in the case of the four-dimensional orthogonal group and its commutator subgroup. In the case of four-dimensional orthogonal group, the association scheme can be obtained from the action of $SU(2, q^2)$ or $SL(2, q)$ if the orthogonal group is $O^+(4, q)$ or $O^-(4, q)$, respectively.

2 Preliminaries

First we give terminologies on finite projective space and orthogonal group. In this paper, we denote by \mathbf{F}_q the finite field with q elements. Let q be a power of 2, and let ρ be a primitive element of \mathbf{F}_{q^2} . Let V be the vector space over \mathbf{F}_q , with basis e_1, e_2, \dots, e_n where $n = \dim V$ is even and at least 4. Let Q be a non-degenerate quadratic form on V over \mathbf{F}_q and define the orthogonal group $O(Q)$:

$$O(Q) := \{g \in GL(V) \mid Q(gv) = Q(v) \text{ for all } v \in V\}.$$

Denote by $\Omega(Q)$ the commutator subgroup of $O(Q)$. Let B be the symmetric bilinear form obtained from Q . It is well known that there are two types of non-degenerate quadratic forms, which are called hyperbolic type or elliptic type. When $n = \dim V$, if Q is a quadratic form of hyperbolic type, denote $O^+(n, q)$ as $O(Q)$ and if Q is a quadratic form of elliptic type, denote $O^-(n, q)$ as $O(Q)$. Similarly, we denote $\Omega^\pm(n, q)$ as $\Omega(Q)$. It is known that if $\dim V$ is even, then $|O(Q) : \Omega(Q)| = 2$. Moreover, for an element g of $O(Q)$, g is in $\Omega(Q)$ if and only if $\text{rank}(g + \text{id}_V)$ is even (see [3, p.160]).

In the projective space $PG(V)$ defined from V , we call a 1 and 2-dimensional subspace of V a (projective) *point* and a *line*, respectively. We say that a point $\langle v \rangle$ is *singular* if $Q(v) = 0$. A line L is said to be *isotropic*, *secant*, *tangent*, or *external* if the number of singular points contained in L is $q + 1, 2, 1$, or 0 . Remark that any line is isotropic, secant, tangent, or external.

is a quadratic form of elliptic type, hence $\Omega(Q^-) = \Omega^-(4, q)$. It is known that $\Omega^-(4, q) \simeq SL(2, q^2)$. An isomorphism from $SL(2, q^2)$ to $\Omega(Q^-)$ can be defined as follows: to $X \in SL(2, q^2)$, assign $g_X \in \Omega(Q^-) = \Omega^-(4, q)$ by the rule

$$g_X(e_1, e_2, e_3, e_4) := (e_1, e_2, e_3, e_4)(X \otimes \bar{X}). \quad (1)$$

where $\bar{X} := (X_{ij}^q)_{1 \leq i, j \leq 2}$.

Hyperbolic type: Consider another \mathbf{F}_q -subspace of \bar{V} ,

$$V^+ := \{z_1 e_1 + z_2 e_2 + z_2^q e_3 + z_1^q e_4 \mid z_1, z_2 \in \mathbf{F}_{q^2}\}.$$

Then V^+ is a four-dimensional vector space over \mathbf{F}_q with basis $e_1 + e_4, \rho e_1 + \rho^q e_4, e_2 + e_3, \rho e_2 + \rho^q e_3$, and the mapping

$$Q^+(z_1 e_1 + z_2 e_2 + z_2^q e_3 + z_1^q e_4) := z_1^{q+1} + z_2^{q+1}$$

is a quadratic form of hyperbolic type, hence $\Omega(Q^+) = \Omega^+(4, q)$. It is known that $\Omega^+(4, q) \simeq SU(2, q^2)^2$ where

$$\begin{aligned} SU(2, q^2) &:= \{U \in SL(2, q^2) \mid U {}^t \bar{U} = I\} \\ &= \left\{ \begin{pmatrix} \alpha & \beta \\ \beta^q & \alpha^q \end{pmatrix} \mid \alpha, \beta \in \mathbf{F}_{q^2}, \alpha^{q+1} + \beta^{q+1} = 1 \right\}. \end{aligned}$$

An isomorphism from $SU(2, q^2)^2$ to $\Omega(Q^+) = \Omega^+(4, q)$ can be defined as follows: to $X, Y \in SU(2, q^2)$, assign $g_{(X, Y)} \in \Omega(Q^+) = \Omega^+(4, q)$ by the rule

$$g_{(X, Y)}(e_1, e_2, e_3, e_4) := (e_1, e_2, e_3, e_4)(X \otimes Y). \quad (2)$$

Now we give terminologies about association schemes. Let $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be a symmetric association scheme. For each i in $\{0, \dots, d\}$, let A_i be the adjacency matrix of the relation R_i , that is, the rows and columns of A_i are indexed by X and

$$(A_i)_{xy} := \begin{cases} 1 & \text{if } (x, y) \in R_i, \\ 0 & \text{if } (x, y) \notin R_i. \end{cases}$$

Then we have

$$A_i A_j = \sum_{k=0}^d p_{ij}^k A_k$$

for any $i, j \in \{0, \dots, d\}$. So A_0, A_1, \dots, A_d form a basis of the commutative algebra generated by A_0, A_1, \dots, A_d over the complex field (which is called the Bose-Mesner algebra of \mathfrak{X}). Moreover this algebra has a unique basis E_0, E_1, \dots, E_d of primitive idempotents. One of the primitive idempotents is $|X|^{-1} J$ where J is the matrix whose entries are all 1. So we may assume $E_0 = |X|^{-1} J$. Let $P = (p_j(i))_{0 \leq i, j \leq d}$ be the matrix defined by

$$(A_0 \ A_1 \ \dots \ A_d) = (E_0 \ E_1 \ \dots \ E_d) P.$$

We call P the character table of \mathfrak{X} .

Let G be a finite group acting on a finite set X . Then G acts naturally on the set $X \times X$ with orbitals R_0, R_1, \dots, R_d , where we let $R_0 = \{(x, x) \mid x \in X\}$. If, for any orbital R_i , $\{(y, x) \mid (x, y) \in R_i\} = R_i$, then $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq d})$ forms a symmetric association scheme. We denote this association scheme by $\mathfrak{X}(G, X)$. In particular, when $X = G/K$ for some subgroup K of G , we write $\mathfrak{X}(G, K)$ instead of $\mathfrak{X}(G, G/K)$.

3 Relation between $\mathfrak{X}(O(Q), \mathbf{L})$ and $\mathfrak{X}(\Omega(Q), \mathbf{L})$ when $\dim V$ is even

When $\dim V$ is odd, since $\Omega(Q) = O(Q)$, $\Omega(Q)$ acts on \mathbf{L} transitively and each orbital of $O(Q)$ on \mathbf{L} is also an orbital of $\Omega(Q)$. Hence $\mathfrak{X}(O(Q), \mathbf{L})$ coincides with $\mathfrak{X}(\Omega(Q), \mathbf{L})$. In this section, we compare the orbitals of $O(Q)$ with the orbitals of $\Omega(Q)$ when $\dim V$ is even. So, in this section, suppose that $\dim V$ is even and at least 4.

3.1 When $\dim V \geq 6$

Lemma 3.1. (i) *Suppose that $\dim V = 4$ and $O(Q) = O^+(4, q)$. Then for an isotropic line l , $\Omega(Q)_l = O(Q)_l$.*

(ii) *Suppose that $\dim V = 4$. Let w_1, w_2 be a basis of a tangent line. Then $\Omega(Q)_{w_1, w_2}$ is a subgroup of $O(Q)_{w_1, w_2}$ with index 2.*

Proof. (i) is already known (see [3, p.172]). For (ii), we need only to prove that, for a fixed basis w_1, w_2 of a tangent line, $\Omega(Q)_{w_1, w_2}$ is a subgroup of $O(Q)_{w_1, w_2}$ with index 2. Indeed, for any other basis w'_1, w'_2 of a tangent line, from Witt's Theorem, there exists $g \in O(Q)$ such that $\langle gw_1, gw_2 \rangle = \langle w'_1, w'_2 \rangle$. Since $\Omega(Q)$ is a normal subgroup of $O(Q)$, we have $\Omega(Q)_{w'_1, w'_2} = \Omega(Q)_{gw_1, gw_2} = g\Omega(Q)_{w_1, w_2}g^{-1}$. Hence $|\Omega(Q)_{w'_1, w'_2}| = |\Omega(Q)_{w_1, w_2}|$.

When Q is elliptic, we may suppose that $Q = Q^-$. Put $w_1 = e_1, w_2 = e_2 + e_3$. Then w_1, w_2 generates a tangent line and $Q(xw_1 + yw_2) = y^2$ for any $x, y \in \mathbf{F}_q$. Show that

$$\{X \mid X \in SL(2, q^2), g_X \in \Omega(Q)_{w_1, w_2}\} = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbf{F}_q \right\}.$$

For $X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in $SL(2, q^2)$, from the definition of g_X , $g_X w_1 = \alpha^{q+1}e_1 + \alpha\gamma^q e_2 + \alpha^q\gamma e_3 + \gamma^{q+1}e_4$. So if g_X fixes w_1 , then $\alpha^{q+1} = 1$ and $\gamma = 0$, hence $X = \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix}$. Since $g_X w_2 = (\alpha\beta^q + \alpha^q\beta)e_1 + \alpha^{1-q}e_2 + \alpha^{q-1}e_3$, if g_X fixes w_2 , then $\alpha^{q-1} = 1$ and $\alpha\beta^q + \alpha^q\beta = 0$. We have already showed that $\alpha^{q+1} = 1$, so $\alpha = 1$ and $\beta^q + \beta = 0$, that is, $\beta \in \mathbf{F}_q$. Conversely, we can see that if $X = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ for some $x \in \mathbf{F}_q$, then g_X fixes w_1 and w_2 .

Suppose that $\dim V = 6$. If $l_2 \in \mathbf{L}$ satisfies $\dim l_1 + l_2 = 4$ and $Q|_{l_1+l_2}$ is non-degenerate, then a plane l' such that $l_1 + l_2 = l_1 \perp l'$ is isotropic or tangent. Since $\dim l_1 + l_2 = 4$, l_2 is skew to l_1 , but l_2 is also skew to l' . Indeed, it is clear when the line l' is isotropic. When the line l' is tangent, suppose that l_2 meets l' in a

four-dimensional subspace U such that $Q|_U$ is non-degenerate. can be applied to the case that $\dim V \geq 6$ and l_1 and l_2 are contained in a $g|_U$, so $g|_{l_1} = g|_{l_2} = g|_U$. Hence $g|_{l_2} \in \Omega(Q)|_{l_2}$. This method From Theorem 2.1, for any $g \in O(Q)|_{l_1}$, there exists $g' \in \Omega(Q)$ such that $g'|_U =$ six-dimensional subspace U which satisfies $l_1 + l_2 \subset U$ and $Q|_U$ is non-degenerate. When $\dim V \geq 8$, for any $l_2 \in \mathbf{L}$, $O(Q)|_{l_2} = \Omega(Q)|_{l_2}$. Indeed, there exists a orbital of $\Omega(Q)$.

Proof. Now we will prove that for $l_1, l_2 \in \mathbf{L}$ and for $g \in O(Q)|_{l_1}$, there exists $g' \in \Omega(Q)|_{l_1}$ such that $g|_{l_2} = g'|_{l_2}$, which means that each orbital of $O(Q)$ is an

Theorem 3.2. If $\dim V \geq 6$, then each orbital of $O(Q)$ on Π is also an orbital of $\Omega(Q)$. Hence $\mathfrak{X}(O(Q), \Pi)$ coincides with $\mathfrak{X}(\Omega(Q), \Pi)$.

Therefore $|\Omega(Q)_{w_1, w_2}| = |O(Q)_{w_1, w_2}|/2$.

□
$$|O(Q)_{w_1, w_2}| = |O(Q)|/|O(Q)_{w_1, w_2}| = 2q.$$

Since $|O(Q)_{w_1, w_2}| = q(b^2 - 1)^2$, we have

w_2 . α is in \mathbb{F}_q , hence $X = X_\beta$. Conversely, we can see that any $g(X_a, X_a)$ fixes w_1 and $(\alpha + \beta)^2$. So if $g(X, X)$ fixes w_1 , then $\alpha + \beta = 1$. Since $1 = \alpha^{q+1} + \beta^{q+1} = 1 + \alpha + \alpha^q$, we have $\alpha = \gamma, \beta = \delta$, that is, $X = Y$. Next the coefficient of e_1 of $g(X, X)w_1$ is if $g(X, Y)$ fixes w_2 , then $\alpha\delta + \beta\gamma = 0$ and $\alpha\gamma^q + \beta\delta^q = 1$. Since $\gamma^{q+1} + \delta^{q+1} = 1$, $g(X, Y)$, coefficients of e_1, e_2 in $g(X, Y)w_2$ are $\alpha\delta + \beta\gamma, \alpha\gamma^q + \beta\delta^q$ respectively. So For $X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, Y = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SU(2, q^2)$, from the definition of where $X_a := \begin{pmatrix} a & a+1 \\ a+1 & a \end{pmatrix}$.

$$\{(X, Y) \mid X, Y \in SU(2, q^2), g(X, Y) \in \Omega(Q)_{w_1, w_2}\} = \{(X_a, X_a) \mid a \in \mathbb{F}_q\}.$$

for any $x, y \in \mathbb{F}_q$. Show that $e_1, w_2 = e_2 + e_3$. Then w_1, w_2 generates a tangent line and $Q(xw_1 + yw_2) = y^2$

When Q is hyperbolic, we may suppose that $Q = Q^+$. Put $w_1 = e_1 + e_2 + e_3 +$

$|O(Q)_{w_1, w_2}|/2$ are both equal to q .

we have $|O(Q)_{w_1, w_2}| = |O(Q)|/|O(Q)_{w_1, w_2}| = 2q$. Hence $|\Omega(Q)_{w_1, w_2}|$ and

$$\begin{aligned} &= q(q^4 - 1), \\ &= |\{w'_i \mid Q(w'_i) = 0\}| \times |(w_1)^\perp \cap \{w \mid Q(w) = 1\}| \\ &= |\{(w'_i, w'_j) \mid Q(xw'_i + yw'_j) = y^2 \text{ for any } x, y \in \mathbb{F}_q\}| \end{aligned}$$

Since

line $\langle v \rangle$. Let $\langle w \rangle$ be the singular line of l' . Since $\dim l_1 + l_2 = 4$, l_2 has a point $\langle u + w \rangle$ where u is a vector in l_1 , hence $l_2 = \langle v, u + w \rangle$. But since $B(v, w) = 0$ and $v \in l' \subseteq l_1^\perp$, $B(v, u + w) = B(v, u) = 0$, which is a contradiction. Therefore l_2 is skew to l' .

Suppose that l' is isotropic. Then $O(Q)$ must be $O^-(6, q)$ and $O(Q|_{l_1^\perp})$ must be $O^+(4, q)$. Since the line l' is isotropic and $\dim l_1 + l_2 = 4$, l_2 is skew to l_1 and l' . Hence $l_2 = \langle v_1 + w_1, v_2 + w_2 \rangle$ for some basis v_1, v_2 of l_1 and for some basis w_1, w_2 of l' . Let l_3 be an external line in the orbit $O(Q)|_{l_1} l_2$. Then since $O(Q)|_{l_1} = O(Q|_{l_1}) \times O(Q|_{l_1^\perp})$, $l_3 = (g_1 \perp g_2)l_2 = \langle g_1 v_1 + g_2 w_1, g_1 v_2 + g_2 w_2 \rangle$ for some $g_1 \in O(Q|_{l_1}), g_2 \in O(Q|_{l_1^\perp})$. Suppose that $g_1 \perp g_2 \notin \Omega(Q)|_{l_1}$. Then from Lemma 2.3, $g_1 \notin \Omega(Q)|_{l_1}, g_2 \in \Omega(Q)|_{l_1^\perp}$, or $g_1 \in \Omega(Q)|_{l_1}, g_2 \notin \Omega(Q)|_{l_1^\perp}$. If $g_1 \notin \Omega(Q)|_{l_1}, g_2 \in \Omega(Q)|_{l_1^\perp}$, then $id_{l_1} \perp g_2$ is in $\Omega(Q)|_{l_1}$ and maps an external line $\langle g_1 v_1 + w_1, g_1 v_2 + w_2 \rangle$ to l_3 . Since $\langle g_1 v_1 + w_1, g_1 v_2 + w_2 \rangle = \langle v_1 + w'_1, v_2 + w'_2 \rangle$ for some basis w'_1, w'_2 of $\langle w_1, w_2 \rangle$, from Lemma 3.1-(i) and Witt's Theorem, there exists an element g of $\Omega(Q)|_{l_1^\perp} \cap O(Q|_{l_1^\perp})$ such that $w'_1 = gw_1, w'_2 = gw_2$. Hence $id_{l_1} \perp g_2 g = (id_{l_1} \perp g_2)(id_{l_1} \perp g) \in \Omega(Q)|_{l_1}$ maps l_2 to l_3 . If $g_1 \in \Omega(Q)|_{l_1}, g_2 \notin \Omega(Q)|_{l_1^\perp}$, then for $g_3 \in O(Q|_{l_1}) \setminus \Omega(Q)|_{l_1}$ and $g_4 \in O(Q|_{l_1^\perp}) \setminus \Omega(Q)|_{l_1^\perp}$, put $l_4 = (g_3 \perp g_4)l_2$. Then $l_3 = (g_1 g_3^{-1} \perp g_2 g_4^{-1})l_4$, $g_1 g_3^{-1} \notin \Omega(Q)|_{l_1}, g_2 g_4^{-1} \in \Omega(Q)|_{l_1^\perp}$. It follows that there exists an element $id_{l_1} \perp g$ of $\Omega(Q)|_{l_1}$ such that $\pi_3 = (id_{l_1} \perp g)l_4 = (g_3 \perp g_4)l_2$. and $g_3 \perp g_4 \in \Omega(Q)|_{l_1}$.

Suppose that l' is a tangent line. Then since $\dim l_1 + l_2 = 4$, $l_2 = \langle v_1 + w_1, v_2 + w_2 \rangle$ for some basis v_1, v_2 of l_1 and for some basis w_1, w_2 of l' . For $g_1 \perp g_2 \in O(Q)|_{l_1} = O(Q|_{l_1}) \times O(Q|_{l_1^\perp})$, let $l_3 = (g_1 \perp g_2)l_2 = \langle g_1 v_1 + g_2 w_1, g_1 v_2 + g_2 w_2 \rangle$. If $g_1 \perp g_2 \notin \Omega(Q)|_{l_1}$, from Lemma 3.1-(2), there exists an element g of $O(Q|_{l_1^\perp})_{w_1, w_2} \setminus \Omega(Q|_{l_1^\perp})_{w_1, w_2}$. So $g_1 \perp g_2 g = (g_1 \perp g_2)(id_{l_1} \perp g) \in \Omega(Q)|_{l_1}$ and $(g_1 \perp g_2 g)l_2 = l_3$. Therefore we complete the proof of Theorem 3.2. \square

3.2 $\dim V=4$

In order to compare the $O(Q)$ -orbitals and the $\Omega(Q)$ -orbitals, we construct the $\Omega(Q)$ -orbitals by using isomorphisms $\Omega^+(4, q) \simeq SU(2, q^2)^2$ and $\Omega^-(4, q) \simeq SL(2, q^2)$. Put

$$A_0 := \begin{pmatrix} \rho & \\ & \rho^{-1} \end{pmatrix}, B_0 := \begin{pmatrix} & 1 \\ 1 & \end{pmatrix},$$

$v_1 = e_2 + e_3$ and $v_2 = \rho e_2 + \rho^q e_3$. Then, with respect to (V^+, Q^+) and (V^-, Q^-) , the line $\langle e_2 + e_3, \rho e_2 + \rho^q e_3 \rangle$ is external and the element of Λ / \sim corresponding to this line is $\{(e_2), (e_3)\}$ since $(\rho v_1 + v_2)/(\rho + \rho^q) = e_2$ and $(\rho^q v_1 + v_2)/(\rho + \rho^q) = e_3$. In this subsection and in the next section, put $l = \langle e_2 + e_3, \rho e_2 + \rho^q e_3 \rangle$.

Lemma 3.3. (i) If $Q = Q^-$, then $\Omega(Q)_l = \{g_X \mid X \in \langle A_0, B_0 \rangle\}$.

(ii) If $Q = Q^+$, then

$$\Omega(Q)_l = \{g_{(X, Y)} \mid (X, Y) \in \langle (A_0^{-1}, I), (I, A_0^{q-1}), (B_0, B_0) \rangle \}.$$

Proof. (i) It can be easily seen that any $X \in \langle A_0, B_0 \rangle$ satisfies g_X fixes l . Since the line l^\perp is secant, from Proposition 2.3,

$$|\Omega(Q)_l| = 2|\Omega(Q)_l| \times |\Omega(Q|_{l^\perp})| = 2(q^2 - 1) = |\{g_X \mid X \in \langle A_0, B_0 \rangle\}|.$$

Therefore we have $\Omega(Q)_l = \{g_X \mid X \in \langle A_0, B_0 \rangle\}$.

(ii) It can be easily seen that any $(X, Y) \in \langle (A_0^{q-1}, I), (I, A_0^{q-1}), (B_0, B_0) \rangle$ satisfies $g_{(X,Y)}$ fixes l . Since the line l^\perp is external, from Proposition 2.3,

$$|\Omega(Q)_l| = 2(q+1)^2 = |\{g_{(X,Y)} \mid (X, Y) \in \langle (A_0^{q-1}, I), (I, A_0^{q-1}), (B_0, B_0) \rangle\}|.$$

Therefore we have $\Omega(Q)_l = \{g_{(X,Y)} \mid (X, Y) \in \langle (A_0^{q-1}, I), (I, A_0^{q-1}), (B_0, B_0) \rangle\}$. \square

Corollary 3.4. (i) $\mathfrak{X}(\Omega^-(4, q), \mathbf{L})$ is isomorphic to $\mathfrak{X}(SL(2, q^2), O^+(2, q^2))$. (ii) $\mathfrak{X}(\Omega^+(4, q), \mathbf{L})$ is isomorphic to a quotient scheme of $\mathfrak{X}(SU(2, q^2), C_{q+1})^2$ where C_{q+1} is the cyclic group of order $q+1$.

Put $H = \langle A_0, B_0 \rangle$ and $K := \langle (A_0^{q-1}, I), (I, A_0^{q-1}), (B_0, B_0) \rangle$. From Lemma 3.3, the set of relations of $\mathfrak{X}(\Omega^-(4, q), \mathbf{L})$ corresponds to the set of double cosets $H \backslash SL(2, q^2) / H$ and the set of relations of $\mathfrak{X}(\Omega^+(4, q), \mathbf{L})$ corresponds to the set of double cosets $K \backslash SU(2, q^2)^2 / K$.

The set of double cosets $H \backslash SL(2, q^2) / H$ has been determined by Tanaka [5].

Theorem 3.5. *The set of double cosets $H \backslash SL(2, q^2) / H$ consists of*

$$H_0 := \{X \in SL(2, q^2) \mid \text{only one entry of } X \text{ is } 0\}.$$

$$H_t := \left\{ X = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL(2, q^2) \mid \alpha, \beta, \gamma, \delta \in \mathbf{F}_q^\times, \alpha\delta\beta^{-1}\gamma^{-1} = \rho^{\pm t} \right\},$$

($t = 1, \dots, q^2/2 - 1$) and H . \square

Next we determine the set of double cosets $K \backslash SU(2, q^2)^2 / K$. For $a, b \in \mathbf{F}_q$, let $[a, b] := \{(a, b), (a+1, b+1)\}$. and put $[\mathbf{F}_q^2] := \{[a, b] \mid a, b \in \mathbf{F}_q\}$ For an element a of \mathbf{F}_q ,

$$K_a := \left\{ \begin{pmatrix} \alpha & \beta \\ \beta^q & \alpha^q \end{pmatrix} \in SU(2, q^2) \mid \beta^{q+1} = a \right\}.$$

Then we have the following.

Lemma 3.6. *The set of double cosets $K \backslash SU(2, q^2)^2 / K$ consists of*

$$K_{[a,b]} := (K_a \times K_b) \cup (K_{a+1} \times K_{b+1})$$

where $[a, b]$ runs through $[\mathbf{F}_q^2]$.

Proof. First we show that the set of double cosets $\langle A_0^{q-1} \rangle \backslash SU(2, q^2) / \langle A_0^{q-1} \rangle$ consists of $\{K_a\}_{a \in \mathbf{F}_q}$.

For $X = \begin{pmatrix} \alpha & \beta \\ \beta^q & \alpha^q \end{pmatrix}, X' = \begin{pmatrix} \alpha' & \beta' \\ \beta'^q & \alpha'^q \end{pmatrix} \in SU(2, q^2)$, if X' is in the double coset $\langle A_0^{q-1} \rangle X \langle A_0^{q-1} \rangle$, then

$$\begin{pmatrix} \alpha' & \beta' \\ \beta'^q & \alpha'^q \end{pmatrix} = \begin{pmatrix} \rho^{(q-1)(s+t)}\alpha & \rho^{(q-1)(s-t)}\beta \\ \rho^{-(q-1)(s-t)}\beta^q & \rho^{-(q-1)(s+t)}\alpha^q \end{pmatrix} \quad (3)$$

for some integers s, t , hence $\alpha'^{q+1} = \rho^{(q^2-1)(s+t)}\alpha^{q+1} = \alpha^{q+1}$.

Conversely, if $\alpha^{q+1} = \alpha'^{q+1}$, then $\beta^{q+1} = \alpha^{q+1} \div 1 = \alpha'^{q+1} + 1 = \beta'^{q+1}$. Let s', t' be intergers which satisfy $\alpha' = \rho^{(q-1)s'}\alpha$, $\beta' = \rho^{(q-1)t'}\beta$. Then integers s, t such that $2s \equiv s' + t'$, $2t \equiv s' - t' \pmod{q+1}$ satisfy the above equality (3), hence $X' \in \langle A_0^{q-1} \rangle X \langle A_0^{q-1} \rangle$. Therefore each K_a forms a double coset of $\langle A_0^{q-1} \rangle \backslash SU(2, q^2) / \langle A_0^{q-1} \rangle$. Now we can see that if $X' = B_0 X$ or $X B_0$, then $\alpha'^{q+1} = \alpha^{q+1} + 1$, and if $X' = B_0 X B_0$, then $\alpha'^{q+1} = \alpha^{q+1}$. Since $\langle (A_0^{q-1}, I), (I, A_0^{q-1}) \rangle$ is a normal subgroup of K , for $X, Y \in SU(2, q^2)$ such that $X \in K_a, Y \in K_b$,

$$K(X, Y)K = \langle (B_0, B_0) \rangle (K_a \times K_b) \langle (B_0, B_0) \rangle = (K_a \times K_b) \cup (K_{a+1} \times K_{b+1}).$$

Therefore each $K_{[a,b]}$ forms a double coset. \square

Theorem 3.7. *Suppose that $\dim V = 4$. Then for a pair (l, m) of external lines, $O(Q)$ -orbital $O(Q)(l, m)$ is also an $\Omega(Q)$ -orbital if and only if m meets l or l^\perp .*

Proof. When Q is elliptic type, then we may assume that $Q = Q^-$. From Lemma 3.3 (i), the orbitals of the action of $\Omega(Q)$ on \mathbf{L} are

$$\begin{aligned} & \{(g_X l, g_X l) \mid X \in SL(2, q^2)\}, \text{ and} \\ & \{(g_X l, g_Y l) \mid X, Y \in SL(2, q^2), X^{-1}Y \in H_t\} \quad (t = 0, \dots, q^2/2 - 1). \end{aligned}$$

Now put $\gamma_t := 0$ if $t \equiv 0 \pmod{q^2 - 1}$, $(1 + \rho^t)^{-1}$ otherwise and let

$$Y_t := \begin{pmatrix} 1 & \gamma_t + 1 \\ 1 & \gamma_t \end{pmatrix}.$$

Then $Y_{\pm t} \in H_t$. Since for $g_t := g_{Y_t}$, $g_t \pi$ is spanned by $g_t(e_2 + e_3)$ and $g_t(\rho e_2 + \rho^q e_3)$ t is a multiple of $q - 1$ or $q + 1$ if and only if $g_t l$ meets l or l^\perp . Hence $g_X l$ meets l or l^\perp if and only if $X \in H_t$ for some t such that $q - 1|t$ or $q + 1|t$.

Consider the following linear transformation

$$g(e_1, e_2, e_3, e_4) := (e_1, e_3, e_2, e_4). \quad (4)$$

Then $g \in O(Q^-) \backslash \Omega(Q^-)$ and g fixes l . Moreover we have that $g g_t = g_t g$, hence g maps $g_t l$ to $g_t l$. It follows that for each t ,

$$O(Q^-)_t(g_t l) = \{g_X l \mid X \in H_t \cup H_{qt}\}.$$

Hence $O(Q^-)_t(g_t l) = \Omega(Q^-)_t(g_t l)$ if and only if $H_t = H_{qt}$, equivalently, $q - 1|t$ or $q + 1|t$. Therefore we proved that $O(Q^-)_t m = \Omega(Q^-)_t m$ if and only if m meets l or l^\perp .

When Q is hyperbolic type, then we may assume that $Q = Q^+$. From Lemma 3.3 (ii), the orbitals of the action of $\Omega(Q)$ on \mathbf{L} are

$$\{(g_{(X,Y)} l, g_{(Z,W)} l) \mid X, Y, Z, W \in SU(2, q^2), (X^{-1}Y, Z^{-1}W) \in K_{[a,b]}\}$$

($[a, b] \in [\mathbb{F}_{q^2}^2]$). Recall that $X_a = \begin{pmatrix} a+1 & a \\ a & a+1 \end{pmatrix} \in SU(2, q^2)$. The pair $(X_a, X_{a'})$ is in $K_{[a^2, a'^2]}$. For $g_{a, a'} := g_{(X_a, X_{a'})}$, $g_{a, a'} l$ is spanned by

$$\begin{aligned} g_{a, a'}(e_2 + e_3) &= (a + a')e_1 + (a + a' + 1)e_2 + (a + a' + 1)e_3 + (a + a')e_4 \\ g_t(\rho e_2 + \rho^q e_3) &= ((a + 1)a'\rho + a(a' + 1)\rho^q)e_1 + ((a + 1)(a' + 1)\rho + aa'\rho^q)e_2 \\ &\quad + ((a + 1)(a' + 1)\rho^q + aa'\rho)e_3 + ((a + 1)a'\rho^q + a(a' + 1)\rho)e_4 \end{aligned}$$

So $a = a'$ or $a' + 1$ if and only if $g_{a,a'}l$ meets l or l^\perp .

Now the linear transformation g defined in (4) is also in $O(Q^+) \setminus \Omega(Q^+)$ and fixes l . Moreover we have that $gg_{(a,a')} = g_{(a',a)}g$, hence g maps $g_{(a,a')}l$ to $g_{(a',a)}l$. It follows that for a, a' ,

$$O(Q^+)_l(g_{a,a'}l) = \{g_{(X,Y)}l \mid (X, Y) \in K_{[a,a']} \cup K_{[a',a]}\}.$$

Hence $O(Q^+)_l(g_{(a,a')}l) = \Omega(Q^+)_l(g_{(a,a')}l)$ if and only if $K_{[a,a']} = K_{[a',a]}$, equivalently, $a = a'$ or $a = a' + 1$. Therefore we proved that $O(Q^+)_lm = \Omega(Q^+)_lm$ if and only if m meets l or l^\perp . \square

4 Character tables of $\mathfrak{X}(\Omega(Q), \mathbf{L})$ and $\mathfrak{X}(O(Q), \mathbf{L})$ in the case of $\dim V = 4$

In this section, we compute the character tables of $\mathfrak{X}(\Omega(Q), \mathbf{L})$ and $\mathfrak{X}(O(Q), \mathbf{L})$ in the case of $\dim V = 4$ from the result of Section 3.

4.1 $O(Q) = O^-(4, q)$

From Theorem 3.5, the relations of $\mathfrak{X}(\Omega^-(4, q), \mathbf{L})$ are

$$\begin{aligned} R_0 &= \{(g_X l, g_X l) \mid X \in SL(2, q^2)\}, \\ R_t &= \{(g_X l, g_Y l) \mid X, Y \in SL(2, q^2), X^{-1}Y \in H_t\} \quad (1 \leq t \leq q^2/2 - 1), \text{ and} \\ R_{q^2/2} &= \{(g_X l, g_Y l) \mid X, Y \in SL(2, q^2), X^{-1}Y \in H_0\} \end{aligned}$$

The character table of $\mathfrak{X}(\Omega^-(4, q), \mathbf{L}) \simeq \mathfrak{X}(SL(2, q^2), O^+(2, q^2))$ is computed in Tanaka's paper [5]:

$$\begin{pmatrix} 1 & q^2 - 1 & \dots & q^2 - 1 & 2(q^2 - 1) \\ 1 & & & & -2 \\ \vdots & (p_j(i))_{1 \leq i, j \leq q^2/2-1} & & & \vdots \\ 1 & & & & -2 \\ 1 & -2 & \dots & -2 & q^2 - 3 \end{pmatrix}.$$

where

$$p_j(i) := - \sum_{k=1}^{q^2/2-1} (-1)^{T(j,k)} (\varepsilon^{ik} + \varepsilon^{-ik}),$$

$T(j, k) := \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}(\gamma_k^2(\gamma_k^2 + 1)\gamma_j)$, (recall that $\gamma_j = (1 + \rho^j)^{-1}$) and ε is a primitive $(q^2 - 1)$ -th root of unity in the complex field. The ordering of columns corresponds to $R_0, R_1, \dots, R_{q^2/2}$.

The relations of $\mathfrak{X}(O^-(4, q), \mathbf{L})$ are

$$R_0, R_i \quad (q-1 \mid t \text{ or } q+1 \mid t), R_{q^2/2} \text{ and } R_i \cup R_{qi} \quad (t \not\equiv 0 \pmod{q^2-1}).$$

In order to compute the character table of $\mathfrak{X}(O^-(4, q), \mathbf{L})$, we show the following lemma.

Lemma 4.1. *Let σ be a permutation on $\{1, \dots, q^2/2 - 1\}$:*

$$\sigma(i) := \begin{cases} 2i & \text{if } 1 \leq 2i \leq q^2/2 - 1, \\ q^2 - 1 - 2i & \text{otherwise.} \end{cases}$$

Then $p_{\sigma(j)}(\sigma^{-1}(i)) = p_j(i)$.

Proof.

$$\begin{aligned} p_{\sigma(j)}(\sigma^{-1}(i)) &= - \sum_{k=1}^{q^2/2-1} (-1)^{T(\sigma(j),k)} (\varepsilon^{\sigma^{-1}(i)k} + \varepsilon^{-\sigma^{-1}(i)k}) \\ &= - \sum_{k'=1}^{q^2/2-1} (-1)^{T(\sigma(j),\sigma(k'))} (\varepsilon^{\sigma^{-1}(i)\sigma(k')} + \varepsilon^{-\sigma^{-1}(i)\sigma(k')}). \end{aligned}$$

Since

$$\sigma^{-1}(i) := \begin{cases} i/2 & \text{if } i \text{ is even,} \\ (q^2 - 1 - i)/2 & \text{if } i \text{ is odd,} \end{cases}$$

we have $\varepsilon^{\sigma^{-1}(i)\sigma(k')} + \varepsilon^{-\sigma^{-1}(i)\sigma(k')} = \varepsilon^{ik'} + \varepsilon^{-ik'}$. Since $\rho^{\sigma(i)} = \rho^{2i}$ or ρ^{-2i} , we have $\rho^{\sigma(k')} + \rho^{-\sigma(k')} = (\rho^{k'} + \rho^{-k'})^2$ and $\gamma_{\sigma(j)} = \gamma_j^2$ or $1 + \gamma_j^2$. Hence

$$\begin{aligned} T(\sigma(j), \sigma(k')) &= \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}((\rho^{\sigma(k')} + \rho^{-\sigma(k')})^{-2} \gamma_{\sigma(j)}) \\ &= \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}((\rho^{k'} + \rho^{-k'})^{-2} \gamma_j) \quad \text{or} \\ &\quad \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}((\rho^{k'} + \rho^{-k'})^{-2} (1 + \gamma_j)). \end{aligned}$$

Since $\text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}((\rho^{k'} + \rho^{-k'})^{-2}) = 0$, we have

$$T(\sigma(j), \sigma(k')) = \text{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_2}((\rho^{k'} + \rho^{-k'})^{-2} \gamma_j) = T(j, k').$$

Therefore

$$p_{\sigma(j)}(\sigma^{-1}(i)) = - \sum_{k'=1}^{q^2/2-1} (-1)^{T(j,k')} (\varepsilon^{ik'} + \varepsilon^{-ik'}) = p_j(i).$$

□

For the permutation σ in this lemma, $\tau := \sigma^r$ where r satisfies $q = 2^r$ is an involution. Indeed since $\sigma(i) \equiv \pm 2i \pmod{q^2 - 1}$, $\tau^2(i) = \sigma^{2r}(i) \equiv \pm q^2 i \equiv \pm i$. Moreover we have that $p_{\tau(j)}(\tau(i)) = p_j(i)$.

The character table of $\mathfrak{X}(O^-(4, q), \mathbf{L})$ is obtained from that of $\mathfrak{X}(\Omega^-(4, q), \mathbf{L})$ by combining i -th column and $\tau(i)$ -th column where i satisfies $\tau(i) \neq i$. So the character table of $\mathfrak{X}(O^-(4, q), \mathbf{L})$ can be written as follows:

$$\begin{pmatrix} 1 & q^2 - 1 & \cdots & q^2 - 1 & 2(q^2 - 1) & \cdots & 2(q^2 - 1) & 2(q^2 - 1) \\ 1 & & p_j(i) & & & p_j(i) + p_{\tau(j)}(i) & & -2 \\ \vdots & & \vdots & & & \vdots & & \vdots \\ 1 & & p_j(i) & & & p_j(i) + p_{\tau(j)}(i) & & -2 \\ 1 & -2 & \cdots & -2 & -4 & \cdots & -4 & q^2 - 3 \end{pmatrix}.$$

4.2 $O(Q) = O^+(4, q)$

Put $K' = \langle A_0^{q-1} \rangle$. Let $\Gamma_t := \gamma_{(q+1)t} \in \mathbb{F}_q$ and $\{S_t\}_{0 \leq t \leq q-1}$ be the set of relations of $\mathfrak{X}(SU(2, q^2), K')$ and S_t corresponds to the double coset K_{Γ_t} if $0 \leq t \leq q/2-1$, $K_{1+\Gamma_{t-q/2}}$ if $q/2 \leq t \leq q-1$. Remark that $\Gamma_{-t} = 1 + \Gamma_{t-q/2}$ for $q/2 < t < q-1$. From the paper of Evans [2], the character table of $\mathfrak{X}(SU(2, q^2), K')$ is

$$\begin{pmatrix} A & A \\ B & -B \end{pmatrix}$$

where

$$A = \begin{pmatrix} 1 & q+1 & \dots & q+1 \\ 1 & & & \\ \vdots & & (A_{tt'})_{1 \leq t, t' \leq q/2-1} & \\ 1 & & & \end{pmatrix},$$

and

$$B = \begin{pmatrix} 1 & & & \\ 1 & & & \\ \vdots & & (B_{tt'})_{1 \leq t \leq q/2, 1 \leq t' \leq q/2-1} & \\ 1 & & & \end{pmatrix}.$$

where

$$A_{tt'} := - \sum_{k=1}^{q-2} (-1)^{T(\Gamma_{t'}, (q+1)k)} \varepsilon^{(q+1)tk},$$

$$B_{tt'} := - \sum_{k=1}^q (-1)^{T(\Gamma_{t'}, (q-1)k)} \varepsilon^{(q-1)tk}.$$

The ordering of column corresponds to $\{S_t\}_{0 \leq t \leq q-1}$. The relations of the association scheme $\mathfrak{X}(SU(2, q^2), K')^2$ are $\{S_{t,u}\}_{0 \leq t, u \leq q-1}$ where

$$S_{t,u} := \{((XK', YK'), (ZK', WK')) \mid (XK', ZK') \in S_t, (YK', WK') \in S_u\}.$$

The character table of $\mathfrak{X}(SU(2, q^2), K_0)^2$ is

$$\begin{pmatrix} A \otimes A & A \otimes A & A \otimes A & A \otimes A \\ A \otimes B & -A \otimes B & A \otimes B & -A \otimes B \\ B \otimes A & B \otimes A & -B \otimes A & -B \otimes A \\ B \otimes B & -B \otimes B & -B \otimes B & B \otimes B \end{pmatrix}$$

The ordering of each block corresponds to $\{S_{t,u}\}$, $\{S_{t,u+q/2}\}$, $\{S_{t+q/2,u}\}$ and $\{S_{t+q/2,u+q/2}\}$ respectively, where in each relation set index t, u runs through $1 \leq t, u \leq q/2-1$.

From Lemma 3.6, in the set $(SU(2, q^2)/K')^2$,

$$S_{0,0} \cup S_{q/2,q/2} = \{((XK', YK'), (XK', YK')) \mid X, Y \in SU(2, q^2)\} \\ \cup \{((XK', YK'), (XB_0K', YB_0K')) \mid X, Y \in SU(2, q^2)\}$$

forms an equivalence relation and each equivalence class is

$$\{(XK', YK'), (XB_0K', YB_0K')\},$$

which corresponds to the double coset K_{Γ_t, Γ_u} if (XK', YK') or (XB_0K', YB_0K') is in $S_{t,u}$ for some $0 \leq t, u \leq q/2 - 1$, $K_{\Gamma_t, 1 + \Gamma_u}$ otherwise. The relations of $\mathfrak{X}(\Omega^+(4, q), \mathbf{L})$ are $\{R_{[t,u]}\}_{0 \leq t \leq q/2-1, 0 \leq u \leq q-1}$ where

$$R_{[t,u]} = \begin{cases} \{(g_{(X,Y)}^t, g_{(Z,W)}^t) \mid ((XK', YK'), (ZK', WK')) \in S_{t,u} \cup S_{t+q/2, u+q/2}\}, & \text{if } 0 \leq u \leq q/2 - 1 \\ \{(g_{(X,Y)}^t, g_{(Z,W)}^t) \mid ((XK', YK'), (ZK', WK')) \in S_{t,u} \cup S_{t+q/2, u-q/2}\}. & \text{if } q/2 \leq u \leq q - 1 \end{cases}$$

Hence the character table of $\mathfrak{X}(\Omega^+(4, q), \mathbf{L})$ is

$$\begin{pmatrix} A \otimes A & A \otimes A \\ B \otimes B & -B \otimes B \end{pmatrix}.$$

In the above character table, the ordering of columns corresponds to relations $\{R_{[t,u]}\}_{0 \leq t, u \leq q/2-1}$ for the left blocks and $\{R_{[t, u+q/2]}\}_{0 \leq t, u \leq q/2-1}$ for the right blocks. The ordering of rows are indexed by $\{[t, u] \mid 0 \leq t, u \leq q/2 - 1\}$ for the upper block and $\{[t, u + q/2] \mid 0 \leq t, u \leq q/2 - 1\}$ for the lower block.

Now we compute the character table of $\mathfrak{X}(O^+(4, q), \mathbf{L})$. The relations of $\mathfrak{X}(O^+(4, q), \mathbf{L})$ are $R_{[0,0]}$, $R_{[0,q/2]}$, $R_{[t,t]}$, $R_{[t,t+q/2]}$ where $t \neq 0, 1$, $R_{[t,u]} \cup R_{[u,t]}$ and $R_{[t, u+q/2]} \cup R_{[u, t+q/2]}$ where t, u satisfy $0 \leq t < u \leq q/2 - 1$.

For the linear transformation on the $q/2$ -dimensional vector space W defined by the matrix A , let $S_2(A)$ be the matrix representation on the symmetric tensor space of $W \otimes W$.

Theorem 4.2. *The character table of $\mathfrak{X}(O^+(4, q), \mathbf{L})$ can be written as follows:*

$$\begin{pmatrix} S_2(A) & S_2(A) \\ S_2(B) & -S_2(B) \end{pmatrix}. \tag{5}$$

Proof. For $0 \leq t, u \leq q/2 - 1$, the $[t, u]$ -entry of the column corresponding to the relation $S_{[t', u']}$ ($0 \leq t', u' \leq q/2 - 1$) is $A_{t't'} A_{u'u'}$. So the sum of the $[t, u]$ -entry of columns corresponding to $S_{[t', u']}$ and $S_{[u', t']}$ is $A_{t't'} A_{u'u'} + A_{t'u'} A_{u't'}$, which is same to the sum of $[u, t]$ -entry of the two columns. This argument can be applied to the other blocks. Hence the matrix of 5 is the character table of $\mathfrak{X}(O^+(4, q), \mathbf{L})$. \square

References

- [1] E. Bannai, S. Hao, S. Song, "Character tables of the association schemes of finite orthogonal groups acting on the nonisotropic points," J. Combin. Theory Ser. A 54 (1990), no. 2, 164-200.
- [2] R. Evans, "Spherical functions for finite upper half planes with characteristic 2," Finite Fields Appl. 1 (1995), no. 3, 376-394.
- [3] D. E. Taylor, "The Geometry of the Classical Groups," Sigma Series in Pure Mathematics, 9, Heldermann Verlag, Berlin, 1992.
- [4] H. Tanaka, "On some relationships among the association schemes of finite orthogonal groups acting on hyperplanes," Master Thesis, Kyushu University, 2000.

- [5] H. Tanaka, "A four-class subscheme of the association scheme coming from the action of $PGL(2, 4^f)$," *European J. Combin.* 23 (2002), no. 1, 121–129.

ユニタリーヴィラソロ頂点作用素代数の 単純カレント拡大

山内 博

2002年7月2日(火)

1 序文

本稿ではヴィラソロ代数のユニタリー系列に付随した頂点作用素代数 (VOA) の \mathbb{Z}_2 -単純カレント拡大について得られた結果の概略を報告する。ここでの結果は台湾の National Cheng Kung 大学の Ching Hung Lam, Ngau Lam 両氏との共同研究で得られたものであり、詳細は論文 [LLY] を御覧頂きたい。

2 ヴィラソロ代数

定義 2.1. ヴィラソロ代数とは $\bigoplus_{n \in \mathbb{Z}} \mathbb{C}L_n \oplus \mathbb{C}c$ を基底として次の交換関係式で定義される無限次元リー代数 Vir である。

$$[L_m, L_n] = (m - n)L_{m+n} + \delta_{m+n,0} \frac{m^3 - m}{12} c, \quad [c, Vir] = 0. \quad (2.1)$$

ヴィラソロ代数の表現としてここでは最高ウェイト表現を考える。 $c, h \in \mathbb{C}$ をパラメーターとして、 Vir の最高ウェイト表現とは、次の条件を満たす Vir -加群 $M(c, h)$ である。

(i) あるベクトル $0 \neq v_h \in M(c, h)$ が存在して、 $L(n)v_h = 0$ ($n > 0$), $L(0)v_h = hv_h$, $cv_h = cv_h$ を満たしている。

(ii) $M(c, h)$ は Vir -加群として v_h から生成されている。

$M(c, h)$ において h は最高ウェイト、 Vir の中心 c の作用する値 c は中心電荷と呼ばれる。

ヴィラソロ代数の最高ウェイト表現 $M(c, h)$ には極大真部分加群が一意に存在し、それを $J(c, h)$ で表したとき $L(c, h) := M(c, h)/J(c, h)$ は中心電荷 c , 最高ウェイトが h の唯一の既約最高ウェイト加群である。

ヴィラソロ代数の既約最高ウェイト加群には自然に頂点作用素代数の加群の構造が入っており、物理学における共形場理論で重要な役割を果たしている。蘊蓄としてヴィラソロ代数及び頂点作用素代数と理論物理の関係を簡単に説明すると¹、理論物理において究極理論だろうとされる弦理論は空間的に一次元の広がりをもった弦が時間の経過とともに描く膜 = 面の宇宙への埋め込みを考える理論と考える事ができて、これは二次元共形場理論を用いて記述される。この意味で弦理論は共形場理論に含まれると言える。共形場理論は共形変換で不変であれ、という要請を課す理論であり、二次元の共形変換は突き詰めるとヴィラソロ代数でコントロールされることが分かっている。三次元以上のときは異なり、二次元の場合には対称性を担う代数 = ヴィラソロ代数が無限次元であり、無限の自由度を無限次元の代数で統制するため、結果として有限個のパラメーターで理論が記述できる美しい理論ができあがる。その理論を代数を用いて数学的に研究するのがヴィラソロ代数の表現論及び頂点作用素代数の理論であるとされている。物理では負のエネルギーというものはあっては困り、そのため次のユニタリー性を持つ表現が特に重要となる。

定義 2.2. 既約最高ウェイト Vir-加群 $L(c, h)$ は次の条件を満たすエルミート内積 $\langle \cdot, \cdot \rangle$ が存在するとき、ユニタリーと呼ばれる。

(i) $\langle v_h, v_h \rangle = 1, \langle L(n)u, v \rangle = \langle u, L(-n)v \rangle.$

(ii) $\langle \cdot, \cdot \rangle$ は正定値である。

上の定義からすぐ分かる事として、 $L(c, h)$ がユニタリーであるためには $c \geq 0, h \geq 0$ が必要条件となる。実際にはユニタリー性を持つ組 (c, h) は全て決定されており、以下の通りである。

定理 2.3. ((FQS/KR)) ヴィラソロ代数の既約最高ウェイト表現 $L(c, h)$ がユニタリーになる組 (c, h) は以下の通りである。

(i) $c \geq 1, h \geq 1$ である (c, h) .

(ii) m を自然数とし、 $1 \leq s \leq r \leq m + 1$ に対して

$$c_m := 1 - \frac{6}{(m+2)(m+3)}, \quad h_{r,s}^{(m)} := \frac{\{r(m+3) - s(m+2)\}^2 - 1}{4(m+2)(m+3)} \quad (2.2)$$

としたときの $(c_m, h_{r,s}^{(m)})$.

上の定理の (ii) に出て来た $L(c_m, h_{r,s}^{(m)})$ をヴィラソロ代数のユニタリー系列と呼ぶ。単純群の分類に例えると怒られてしまいそうだが、系列 (i) は非可算無限個であり、いくらでも出て来るので無節操である。いわば交代群もしくはシュバレー群と言った感じであ

¹私は物理学を分かって述べている訳ではないため、間違い・不適切な記述があっても御容赦願いたい。

る。それに比べて系列 (ii) は可算個であり、一つ m を止める、即ち中心電荷を固定すると最高ウェイトは有限個の値しか取り得ない。どことなく散在型単純群を思い起こさせる。実際、ユニタリー系列は物理及びモンスターの数学で重要な役割を果たしている。

3 ユニタリーヴィラソロVOA

先程、ヴィラソロ代数の最高ウェイト加群には頂点作用素代数の構造が入ると述べた。より詳しく述べると次のようになる。ヴィラソロ代数の最高ウェイトが0である最高ウェイト加群 $L(c, 0)$ には頂点作用素代数の構造が入る。ここで注意して頂きたいのは、 $L(c, 0)$ はヴィラソロ代数の加群であるとともに、その中に代数構造が入っているという点である。 $L(c, 0)$ -加群について次が成り立つ。

定理 3.1. ($[W]$) $L(c, 0)$ をユニタリーヴィラソロ VOA とする。既約な $L(c, 0)$ -加群は次の通りである。

(i) $c \geq 1$ のとき $L(c, h)$, $h \in \mathbb{C}$. 一般に $L(c, 0)$ -加群は完全可約ではない。

(ii) $c = c_m$ のとき $L(c_m, h_r^{(m)})$, $1 \leq s \leq r \leq m + 1$. 特に任意の $L(c_m, 0)$ -加群は完全可約である。

この定理からヴィラソロ VOA のユニタリー系列はユニタリーであってかつ完全可約性を持つものとして特徴付けられる。このようにユニタリー系列は非常に良い性質を持ったクラスであり、盛んに研究されている。ユニタリー系列のフュージョン規則も既に決定されている。それを述べる前に VOA のフュージョン積を簡単に紹介する。

定義 3.2. V を VOA, W^i , $i = 1, 2, 3$ を既約 V -加群としたとき、 W^1 と W^2 からフュージョン積と呼ばれる新しい V -加群 $W^1 \boxtimes W^2$ を作る操作が定まっており、 $W^1 \boxtimes W^2$ を既約成分に分解したときに出てくる W^3 の重複度を記号 $N_{W^1 W^2}^{W^3}$ で表し、この数をフュージョン規則と呼ぶ。そしてこのフュージョン規則を用いて V の既約加群全体 $\{W^i \mid i \in I\}$ で張られる \mathbb{Z} -自由加群 $\oplus_{i \in I} \mathbb{Z}[W^i]$ に積を

$$[W^i] \times [W^j] = \sum_{k \in I} N_{W^i W^j}^{W^k} [W^k]$$

で入れたものを V のフュージョン代数もしくは Verlinde 代数と呼ぶ。

注釈 3.3. ここでは VOA のフュージョン積・規則について詳しい説明はしないが、要はテンソル積の分岐則のことで有限群の指標環のようなものと思って頂きたい。

定理 3.4. ($\{W\}$) ヴィラソロ VOA $L(c, 0)$ -加群 $L(c_m, h_{r,s}^{(m)})$ らのフュージョン規則は次で与えられる。

$$L(c_m, h_{r_1, s_1}^{(m)}) \times L(c_m, h_{r_2, s_2}^{(m)}) = \sum_{i \in I} \sum_{j \in J} L(c_m, h_{|r_1 - r_2| + 2i - 1, |s_1 - s_2| + 2j - 1}^{(m)}), \quad (3.1)$$

ここで

$$I = \{1, 2, \dots, \min\{r_1, r_2, m + 2 - r_1, m + 2 - r_2\}\},$$

$$J = \{1, 2, \dots, \min\{s_1, s_2, m + 3 - s_1, m + 3 - s_2\}\}.$$

$L(c_m, 0)$ -加群のフュージョン規則を眺めると、一つの特徴を見つけられる。 $h_{r,s}^{(m)}$, $1 \leq s \leq r \leq m + 1$ の最小値、最大値はそれぞれ $h_{1,1}^{(m)} = 0$, $h_{m+1,1}^{(m)} = \frac{1}{4}m(m+1)$ であり、どちらも $\frac{1}{2}\mathbb{Z}$ に含まれている。これらのフュージョン規則は上の定理から次の通りである。

$$L(c_m, 0) \times L(c_m, h_{r,s}^{(m)}) = L(c_m, h_{r,s}^{(m)}),$$

$$L(c_m, \frac{1}{4}m(m+1)) \times L(c_m, h_{r,s}^{(m)}) = L(c_m, h_{m+2-r,s}^{(m)}).$$

一般に、 V を VOA, U を V -加群として任意の既約加群 W とのフュージョン積 $U \boxtimes W$ がまた既約 V -加群になるとき、 U を単純カレントという。上の式から $L(c_m, 0)$, $L(c_m, \frac{1}{4}m(m+1))$ は単純カレント $L(c_m, 0)$ -加群になっている。特に $L(c_m, \frac{1}{4}m(m+1)) \times L(c_m, \frac{1}{4}m(m+1)) = L(c_m, 0)$ である。このことからユニタリ-ヴィラソロ VOA $L(c_m, 0)$ の \mathbb{Z}_2 -単純カレント拡大として $L(c_m, 0) \oplus L(c_m, \frac{1}{4}m(m+1))$ に (S)VOA² の構造が入ることが期待される。ここで VOA の \mathbb{Z}_2 -拡大とは VOA V^0 とその単純カレント加群 V^1 を使って \mathbb{Z}_2 -次数が入った V^0 の拡大 $V^0 \oplus V^1$ の事である。実際、 $m = 1, 2, 3$ の場合には次の拡大があることが知られている。

○ $m = 1$ のとき、 $c_1 = \frac{1}{2}$. $L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2})$: イジング模型と呼ばれる SVOA.

○ $m = 2$ のとき、 $c_2 = \frac{7}{10}$. $L(\frac{7}{10}, 0) \oplus L(\frac{7}{10}, \frac{3}{2})$: $N = 1$ スーパーコンフォーマル代数のユニタリ-系列の最初の SVOA.

○ $m = 3$ のとき、 $c_3 = \frac{4}{5}$. $L(\frac{4}{5}, 0) \oplus L(\frac{4}{5}, 3)$: 3-状態 Potts 模型と呼ばれる VOA (北詰-宮本-山田 [KMY]).

この例から一般の m についても $L(c_m, 0) \oplus L(c_m, \frac{1}{4}m(m+1))$ には $\frac{1}{4}m(m+1)$ が整数の場合には VOA の構造が、半整数の場合には SVOA の構造が入る事が期待される。これが正しい事をこれから示す。

²SVOA = vertex operator superalgebra : 頂点作用素超代数

4 コミュタント構成法

ユニタリーヴィラソロ VOA は Goddard-Kent-Olive によって具体的に構成された。彼らの構成法はコミュタント構成法と呼ばれるものである。それを簡単に復讐する。

V を VOA, U をその部分 VOA とする。このとき V において U と可換なもの全体は部分 VOA をなす。これを $\text{Com}_V(U)$ で表し、 V における U のコミュタントと呼ぶ。定義から U と $\text{Com}_V(U)$ は互いに可換なので V には $U \otimes \text{Com}_V(U)$ と同型な部分 VOA が含まれている。

では Goddard 達の定理を述べよう。 Λ_0, Λ_1 をアフィンリー代数 \hat{sl}_2 の基本ウェイト、 $\mathcal{L}(m, j)$, $m \in \mathbb{N}$, $0 \leq j \leq m$ を最高ウェイトが $(m-j)\Lambda_0 + j\Lambda_1$ のレベル m の \hat{sl}_2 の既約最高ウェイト表現とする。この場合 $\mathcal{L}(m, j)$ らは可積分な表現になっており、ユニタリーな内積が入っている。[FZ] により $\mathcal{L}(m, 0)$ には単純有理型 VOA の構造が入っており、その既約加群は $\mathcal{L}(m, j)$, $0 \leq j \leq m$ で与えられる。さらにこれらのフュージョン規則も決定されており、以下のようになる (cf. [FZ]):

$$\mathcal{L}(m, i) \times \mathcal{L}(m, j) = \sum_{k=\max\{i+j-m\}}^{\min\{i,j\}} \mathcal{L}(m, i+j-2k). \quad (4.1)$$

また対角成分を考えることで次の包含関係があることが分かる。

$$\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0) \supset \mathcal{L}(m+1, 0).$$

定理 4.1. ([GKO])

(i) 上の包含関係において

$$\text{Com}_{\mathcal{L}(1,0) \otimes \mathcal{L}(m,0)}(\mathcal{L}(m+1, 0)) = \mathcal{L}(c_m, 0).$$

(ii) 全ての既約 $\mathcal{L}(c_m, 0)$ -加群は $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0)$ -加群 $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, j)$, $0 \leq j \leq m$ を $\mathcal{L}(m+1, 0) \otimes \mathcal{L}(c_m, 0)$ -加群として分解することで得られる。

この結果から、 $\mathcal{L}(c_m, 0)$ の \mathbb{Z}_2 -単純カレント拡大はもし存在するならば $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0)$ の \mathbb{Z}_2 -単純カレント拡大に含まれていると考えられる。この拡大は Li によって調べられている。

5 アフィン VOA の \mathbb{Z}_2 -単純カレント拡大

先程の公式 (4.1) より、 $\mathcal{L}(m, m)$ のフュージョン規則は次の通りである。

$$\mathcal{L}(m, m) \times \mathcal{L}(m, i) = \mathcal{L}(m, m-i).$$

特に $\mathcal{L}(m, m) \times \mathcal{L}(m, m) = \mathcal{L}(m, 0)$ である。このことから $\mathcal{L}(m, m)$ は単純カレントであり、これを用いて $\mathcal{L}(m, 0)$ を拡大できないかが考えられる。この問題は Li によって解決されている。

定理 5.1. (*[Li]*) 次の $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0)$ の \mathbb{Z}_2 -単純カレント拡大が存在する。

(i) $m \equiv 0 \pmod{4}$ のとき $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0) \oplus \mathcal{L}(1, 0) \otimes \mathcal{L}(m, m) : VOA$.

(ii) $m \equiv 1 \pmod{4}$ のとき $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0) \oplus \mathcal{L}(1, 1) \otimes \mathcal{L}(m, m) : SVOA$.

(iii) $m \equiv 2 \pmod{4}$ のとき $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0) \oplus \mathcal{L}(1, 0) \otimes \mathcal{L}(m, m) : SVOA$.

(iv) $m \equiv 3 \pmod{4}$ のとき $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0) \oplus \mathcal{L}(1, 1) \otimes \mathcal{L}(m, m) : VOA$.

上にできた \mathbb{Z}_2 -拡大を $V(m)$ で表す。

6 ユニタリーヴィラソロ VOA の \mathbb{Z}_2 -単純カレント拡大

先程構成した $V(m)$ には次の包含関係がある。

$$V(m) \supset \mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0) \supset \mathcal{L}(m+1, 0).$$

この関係からコミュタント構成を行うことで望んでいた拡大が得られる:

定理 6.1. (*[LLY]*)

(1) $\text{Com}_{V(m)}(\mathcal{L}(m+1, 0)) = L(c_m, 0) \oplus L(c_m, \frac{1}{4}m(m+1))$.

即ち $U(m) := L(c_m, 0) \oplus L(c_m, \frac{1}{4}m(m+1))$ には (S)VOA 構造が存在する。

(2) (1) で述べた $U(m)$ の (S)VOA 構造は一意的である。

(3) $m \equiv 0, 3 \pmod{4}$ のとき $U(m)$ は有理型 VOA であり、全ての既約加群及びそのフュージョン規則も決定できる。

上の定理の (3) は少し複雑であり、全て書き下すと数項に渡るためここでは省略した。詳細は [LLY] を御覧頂きたい。

注釈 6.2. $m \equiv 1, 2 \pmod{4}$ の場合、 $U(m)$ は有理型 SVOA になる。この場合にも全ての既約加群を決定することはできるが、フュージョン規則までは決定していない。これは SVOA の双対加群の定義が一意的でないためであることと、我々の現在の興味が SVOA より VOA にあることに起因する。

さて、注釈にもあるとおり $m \equiv 1, 2 \pmod{4}$ の場合にも $U(m)$ を考えないのもったいない。そこで超代数になってしまう場合にも二つくっつけることで通常の代数にして考えて見る。

定理 6.3. m を正の奇数とする。このとき $L(c_m, 0) \otimes L(c_{m+1}, 0)$ の \mathbb{Z}_2 -単純カレント拡大

$$W(m) := L(c_m, 0) \otimes L(c_{m+1}, 0) \oplus L(c_m, \frac{1}{4}m(m+1)) \otimes L(c_{m+1}, \frac{1}{4}(m+1)(m+2))$$

が存在し、これは有理型単純 VOA である。 $W(m)$ の既約加群及びそのフュージョン規則も全て決定できる。

$m = 1$ の場合には $W(1)$ をさらに \mathbb{Z}_2 -単純カレント拡大することができる。

定理 6.4. (1) $W(1) = L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, 0) \oplus L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{7}{10}, \frac{3}{2})$ の \mathbb{Z}_2 -単純カレント拡大として

$$L(\frac{1}{2}, 0) \otimes L(\frac{7}{10}, 0) \oplus L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{7}{10}, \frac{3}{2}) \oplus [L(\frac{1}{2}, \frac{1}{16}) \otimes L(\frac{7}{10}, \frac{7}{16})]^\pm$$

には単純 SVOA の構造が入る。

(2) $W(3) = L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, 0) \oplus L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, 5)$ の \mathbb{Z}_2 -拡大ではない拡大

$$L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, 0) \oplus L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, 5) \oplus [L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{4}{3})]^\pm$$

には単純 VOA の構造が入る。

(2) で述べた拡大は \mathbb{Z}_2 -次数の入った拡大ではないが、[M3] [SY] で扱われている VOA と関連してとても重要である。詳しくは今回のシンポジウムでの筑波大学の佐久間伸也氏の報告集を御覧頂きたい。

参考文献

- [FQS] D. Friedan, Z. Qiu and S. Shenker, Conformal invariance, unitarity and two dimensional critical exponents, *MSRI publ.*, **3** (1985), 419-449.
- [FZ] I. Frenkel and Y. Zhu, Vertex operator algebras associated to representations of affine and Virasoro algebras, *Duke Math. J.* **66** (1992), 123-168.

- [GKO] P. Goddard, A. Kent and D. Olive, Unitary representations of the Virasoro and super-Virasoro algebras, *Comm. Math. Phys.* **103** (1986), 105–119.
- [KMY] M. Kitazume, M. Miyamoto and H. Yamada, Ternary codes and vertex operator algebras, *J. Algebra* **223** (2000), 379–395.
- [KR] V. G. Kac and A. K. Raina, “Bombay Lectures on Highest Weight Representations of Infinite Dimensional Lie algebras,” World Scientific, Singapore, 1987.
- [Li] H. Li, The theory of physical superselection sectors in terms of vertex operator algebra language, q-alg/9504026.
- [LLY] C. H. Lam, N. Lan and H. Yamauchi, Extension of Virasoro vertex operator algebra by a simple module, preprint.
- [LY] C. H. Lam and H. Yamada, Tricritical 3-state Potts model and vertex operator algebras constructed from ternary codes, preprint.
- [M1] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra* **179** (1996), 528–548.
- [M2] M. Miyamoto, 3-state Potts model and automorphisms of vertex operator algebras of order 3, *J. Algebra* **239** (2001), 56–76.
- [M3] M. Miyamoto, VOA generated by two conformal vectors whose τ -involutions generate S_3 , math.GR/0112031.
- [SY] S. Sakuma and H. Yamauchi, Vertex operator algebras with automorphism group S_3 , math.QA/0207117.
- [W] Wang, Rationality of Virasoro vertex operator algebras, *IMRN* **71** (1993), 197–211.

Vertex operator algebras with two Miyamoto involutions generating S_3

Shinya Sakuma
and
Hiroshi Yamauchi

Graduate School of Mathematics, University of Tsukuba

1 Introduction

One of the most interesting example of vertex operator algebras (VOAs) is the Moonshine VOA $V^h = \bigoplus_{i=0}^{\infty} V_i^h$ whose full automorphism group is the Monster simple group \mathbb{M} , [FLM]. Its weight two subspace V_2^h coincides with a commutative (non-associative) algebra (called the monstrous Griess algebra) of dimension 196884 constructed by Griess in order to construct the Monster simple group [Gr]. One of the important results is that each $2A$ -involution θ defines a unique idempotent e_θ (called an axis) of the monstrous Griess algebra such that the inner product $\langle e_\theta, e_\phi \rangle$ is uniquely determined by the conjugacy classes of $\theta\phi$, see [Co]. The $2A$ -involutions satisfy several interesting properties. For example, the Bimonster $\mathbb{M} \wr \mathbb{Z}_2$ contains Y_{555} -diagram as generators, where a vertex is a $2A$ -involution and an edge $\theta - \phi$ means $|\theta\phi| = 3$ and no edge between θ and ϕ implies that $\theta\phi$ is of order two.

If e is a rational conformal vector with central charge $\frac{1}{2}$ i.e., e generates a rational VOA $L(\frac{1}{2}, 0)$ called an Ising model, then one can define an involutive automorphism τ_e of V by

$$\tau_e : \begin{cases} 1 & \text{on } W_0 \oplus W_{\frac{1}{2}} \\ -1 & \text{on } W_{\frac{1}{16}}, \end{cases}$$

where W_h denotes the sum of all irreducible $VA(e)$ -modules isomorphic to $L(\frac{1}{2}, h)$ and $VA(e)$ is a subVOA generated by e . In the monstrous Griess

algebra, a conformal vector e with central charge $\frac{1}{2}$ is corresponding to an axis and τ_e is a $2A$ -involution.

A VOA V over \mathbb{R} is referred to be of *moonshine type* if it admits a weight space decomposition $V = \bigoplus_{n=0}^{\infty} V_n$ with $V_0 = \mathbb{R}\mathbf{1}$ and $V_1 = 0$ and it possesses a definite invariant bilinear form $\langle \cdot, \cdot \rangle$ such that $\langle \mathbf{1}, \mathbf{1} \rangle = 1$. Miyamoto studied a VOA of moonshine type which contains two conformal vectors with central charge $\frac{1}{2}$ whose τ -involutions generate S_3 and determined that the possible inner products of such a pair of conformal vectors are $1/2^8$ or $13/2^{10}$ in [M]. Furthermore, he determined the structure of a subalgebra generated by their conformal vectors in Griess algebra V_2 of such a VOA V .

In this lecture, we construct a VOA U generated by two conformal vectors e, f with $|\tau_e \tau_f| = 3$ and $\langle e, f, \rangle = 13/2^{10}$, which has the shape

$$\left(L\left(\frac{4}{5}, 0\right) \oplus L\left(\frac{4}{5}, 3\right) \right) \otimes \left(L\left(\frac{6}{7}, 0\right) \oplus L\left(\frac{6}{7}, 5\right) \right) \\ \oplus L\left(\frac{4}{5}, \frac{2}{3}\right)^+ \otimes L\left(\frac{6}{7}, \frac{4}{3}\right)^+ \oplus L\left(\frac{4}{5}, \frac{2}{3}\right)^- \otimes L\left(\frac{6}{7}, \frac{4}{3}\right)^+. \quad (1)$$

In fact, the structure of VOA of this shape is uniquely determined.

Recently, we proved that a VOA generated by two conformal vectors whose τ -involutions generate S_3 and inner product is equal to $13/2^{10}$ is isomorphic to U . Namely, such a VOA exists uniquely. Therefore, the Moonshine VOA contains U and $W(0) = L(\frac{4}{5}, 0) \oplus L(\frac{4}{5}, 3)$ as a subVOA. Then, the automorphism given by the \mathbb{Z}_3 -symmetry of $W(0)$ is $3A$ element.

2 Preliminaries

For any complex numbers c and h , denote by $L(c, h)$ the irreducible highest weight representation of the Virasoro algebra with central charge c and highest weight h . It is shown in [FZ] that $L(c, 0)$ has a natural structure of a simple VOA. Let

$$c_m := 1 - \frac{6}{(m+2)(m+3)} \quad (m = 1, 2, \dots), \quad (2)$$

$$h_{r,s}^{(m)} := \frac{\{r(m+3) - s(m+2)\}^2 - 1}{4(m+2)(m+3)} \quad (3)$$

for $r, s \in \mathbb{N}$, $1 \leq r \leq m+1$ and $1 \leq s \leq m+2$. It is shown in [W] that $L(c_m, 0)$ is rational and $L(c_m, h_{r,s}^{(m)})$, $1 \leq s \leq r \leq m+1$, provide all

irreducible $L(c_m, 0)$ -modules (see also [DMZ]). This is so-called the unitary series of the Virasoro VOAs. The fusion rules among $L(c_m, 0)$ -modules [W] are given by

$$L(c_m, h_{r_1, s_1}) \times L(c_m, h_{r_2, s_2}) = \sum_{i \in I, j \in J} L(c_m, h_{|r_1 - r_2| + 2i - 1, |s_1 - s_2| + 2j - 1}), \quad (4)$$

where

$$I = \{1, 2, \dots, \min\{r_1, r_2, m + 2 - r_1, m + 2 - r_2\}\},$$

$$J = \{1, 2, \dots, \min\{s_1, s_2, m + 3 - s_1, m + 3 - s_2\}\}.$$

Since $c_3 = \frac{4}{5}$ and $c_4 = \frac{6}{7}$, $L(\frac{4}{5}, 3)$ and $L(\frac{6}{7}, 5)$ are simple currents by (4). It is known that $L(\frac{4}{5}, 0) \oplus L(\frac{4}{5}, 3)$ and $L(\frac{6}{7}, 0) \oplus L(\frac{6}{7}, 5)$ have a simple VOA structure.

Theorem 2.1. (*[KMY]*) *A VOA $L(\frac{4}{5}, 0) \oplus L(\frac{4}{5}, 3)$ is rational and all its irreducible modules are the following:*

$$\begin{aligned} W(0) &:= L(\frac{4}{5}, 0) \oplus L(\frac{4}{5}, 3), & W(\frac{2}{3})^\pm &:= L(\frac{4}{5}, \frac{2}{3})^\pm, \\ W(\frac{2}{5}) &:= L(\frac{4}{5}, \frac{2}{5}) \oplus L(\frac{4}{5}, \frac{7}{5}), & W(\frac{1}{15})^\pm &:= L(\frac{4}{5}, \frac{1}{15})^\pm, \end{aligned}$$

where $W(h)^\pm$ means that $L(\frac{4}{5}, h)$ has two structures by the \mathbb{Z}_2 -grading of the VOA $W(0)$ for $h = \frac{2}{3}, \frac{1}{15}$.

Theorem 2.2. (*[LY]* and *[LLY]*) *A VOA $L(\frac{6}{7}, 0) \oplus L(\frac{6}{7}, 5)$ is rational and all its irreducible modules are the following:*

$$\begin{aligned} N(0) &:= L(\frac{6}{7}, 0) \oplus L(\frac{6}{7}, 5), & N(\frac{4}{3})^\pm &:= L(\frac{6}{7}, \frac{4}{3})^\pm, \\ N(\frac{1}{7}) &:= L(\frac{6}{7}, \frac{1}{7}) \oplus L(\frac{6}{7}, \frac{22}{7}), & N(\frac{1}{21})^\pm &:= L(\frac{6}{7}, \frac{1}{21})^\pm, \\ N(\frac{5}{7}) &:= L(\frac{6}{7}, \frac{5}{7}) \oplus L(\frac{6}{7}, \frac{12}{7}), & N(\frac{10}{21})^\pm &:= L(\frac{6}{7}, \frac{10}{21})^\pm, \end{aligned}$$

where $N(h)^\pm$ means that $L(\frac{6}{7}, h)$ has two structures by the \mathbb{Z}_2 -grading of the VOA $N(0)$ for $h = \frac{4}{3}, \frac{1}{21}, \frac{10}{21}$.

Let \mathfrak{g} be the Lie algebra $sl_2(\mathbb{C})$ with generators h, e, f and relations $[h, e] = 2e, [h, f] = -2f$ and $[e, f] = h$. We use the standard invariant bilinear form on \mathfrak{g} defined by $\langle h, h \rangle = 2$ and $\langle e, f \rangle = 1$. Let $\hat{\mathfrak{g}}$ be the corresponding affine algebra of type $A_1^{(1)}$ and Λ_0, Λ_1 the fundamental weights for $\hat{\mathfrak{g}}$. For any non-negative integers m and j , denote by $\mathcal{L}(m, j)$ the irreducible highest weight $\hat{\mathfrak{g}}$ -module with highest weight $(m - j)\Lambda_0 + j\Lambda_1$.

Then $\mathcal{L}(m, 0)$ has a natural structure of a simple VOA [FZ]. The Virasoro vector Ω^m of $\mathcal{L}(m, 0)$ is given by

$$\Omega^m := \frac{1}{2(m+2)} \left(\frac{1}{2} h_{(-1)} h + e_{(-1)} f + f_{(-1)} e \right) \quad (5)$$

with central charge $3m/(m+2)$.

Let $m \in \mathbb{N}$. Then $\mathcal{L}(m, 0)$ is a rational VOA and $\{\mathcal{L}(m, j) \mid j = 0, 1, \dots, m\}$ is the set of all irreducible $\mathcal{L}(m, 0)$ -modules. The fusion algebra (cf. [FZ]) is given by

$$\mathcal{L}(m, j) \times \mathcal{L}(m, k) = \sum_{i=\max\{0, j+k-m\}}^{\min\{j, k\}} \mathcal{L}(m, j+k-2i). \quad (6)$$

In particular, $\mathcal{L}(m, m) \times \mathcal{L}(m, j) = \mathcal{L}(m, m-j)$ and thus $\mathcal{L}(m, m)$ is a simple current module.

Let $A_1 = \mathbb{Z}\alpha$ be the root lattice of type A_1 with $\langle \alpha, \alpha \rangle = 2$ and V_{A_1} the lattice VOA associated with A_1 . Let

$$A_1^* = \{x \in \mathbb{Q} \otimes_{\mathbb{Z}} A_1 \mid \langle x, \alpha \rangle \in \mathbb{Z}\}$$

be the dual lattice of A_1 . Then $A_1^* = A_1 \cup (\frac{1}{2}\alpha + A_1)$. It is well-known that $V_{A_1} \simeq \mathcal{L}(1, 0)$ and $V_{\frac{1}{2}\alpha + A_1} \simeq \mathcal{L}(1, 1)$ (cf. [FLM] [FZ], etc.). Let $A_1^m = \mathbb{Z}\alpha^1 \oplus \mathbb{Z}\alpha^2 \oplus \dots \oplus \mathbb{Z}\alpha^m$ be the orthogonal sum of m copies of A_1 . Then we have an isomorphism $V_{A_1^m} \simeq (V_{A_1})^{\otimes m} \simeq \mathcal{L}(1, 0)^{\otimes m}$. Let $H^m := \alpha_{(-1)}^1 \mathbb{1} + \dots + \alpha_{(-1)}^m \mathbb{1}$, $E^m := e^{\alpha^1} + \dots + e^{\alpha^m}$ and $F^m := e^{-\alpha^1} + \dots + e^{-\alpha^m}$. Then it is shown in [DL] that H^m , E^m and F^m generate a sub VOA isomorphic to $\mathcal{L}(m, 0)$ in $V_{A_1^m}$. By $V_{A_1} \otimes V_{A_1^m} \simeq V_{A_1^{m+1}}$, $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0)$ contains a sub VOA isomorphic to $\mathcal{L}(m+1, 0)$ generated by H^{m+1} , E^{m+1} and F^{m+1} , whose Virasoro vector Ω^{m+1} is given by (5). It is shown in [DL] and [KR] that $\omega^m := \Omega^1 \otimes \mathbb{1} + \mathbb{1} \otimes \Omega^m - \Omega^{m+1}$ also gives a Virasoro vector with central charge $c_m = 1 - 6/(m+2)(m+3)$. Furthermore, Ω^{m+1} and ω^m are mutually commutative and ω^m generates a simple Virasoro VOA $L(c_m, 0)$. Hence, $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0)$ contains a sub VOA isomorphic to $L(c_m, 0) \otimes \mathcal{L}(m+1, 0)$. Since both $L(c_m, 0)$ and $\mathcal{L}(m+1, 0)$ are rational, every $\mathcal{L}(1, 0) \otimes \mathcal{L}(m, 0)$ -module can be decomposed into irreducible $L(c_m, 0) \otimes \mathcal{L}(m+1, 0)$ -submodules. The following decomposition is obtained in [GKO]:

$$\mathcal{L}(1, \epsilon) \otimes \mathcal{L}(m, n) = \bigoplus_{\substack{0 \leq s \leq m+1 \\ s \equiv n + \epsilon \pmod{2}}} L(c_m, h_{n+1, s+1}^{(m)}) \otimes \mathcal{L}(m+1, s), \quad (7)$$

where $\epsilon = 0, 1$ and $0 \leq n \leq m$. Note that $h_{r,s}^{(m)} = h_{m+2-r, m+3-s}^{(m)}$. This is the famous GKO-construction of the unitary Virasoro VOAs.

3 VOA with two Miyamoto involutions generating S_3

Let $A_1^5 = \mathbb{Z}\alpha^1 \oplus \mathbb{Z}\alpha^2 \oplus \cdots \oplus \mathbb{Z}\alpha^5$ with $\langle \alpha^i, \alpha^j \rangle = 2\delta_{i,j}$ and set $L := A_1^5 \cup (\gamma + A_1^5)$ with $\gamma := \frac{1}{2}\alpha^1 + \frac{1}{2}\alpha^2 + \frac{1}{2}\alpha^3 + \frac{1}{2}\alpha^4$. Then L is an even lattice so that we can construct a VOA V_L associated to L . We have an isomorphism $V_L = V_{A_1^5} \oplus V_{\gamma+A_1^5} \simeq \{\mathcal{L}(1, 0)^{\otimes 4} \oplus \mathcal{L}(1, 1)^{\otimes 4}\} \otimes \mathcal{L}(1, 0)$. By (7) and the fusion rules (4) and (6), we can show the following.

Lemma 3.1. *We have the following inclusions*

$$\begin{aligned} \mathcal{L}(1, 0)^{\otimes 3} &\supset L(\tfrac{1}{2}, 0) \otimes L(\tfrac{7}{10}, 0) \otimes \mathcal{L}(3, 0), \\ \mathcal{L}(1, 1)^{\otimes 3} &\supset L(\tfrac{1}{2}, 0) \otimes L(\tfrac{7}{10}, 0) \otimes \mathcal{L}(3, 3). \end{aligned}$$

Therefore, V_L contains a sub VOA isomorphic to

$$\mathcal{L}(3, 0) \otimes \mathcal{L}(1, 0) \otimes \mathcal{L}(1, 0) \oplus \mathcal{L}(3, 3) \otimes \mathcal{L}(1, 1) \otimes \mathcal{L}(1, 0).$$

Lemma 3.2. *We have the following decompositions:*

$$\begin{aligned} &\mathcal{L}(3, 0) \otimes \mathcal{L}(1, 0) \otimes \mathcal{L}(1, 0) \\ &\simeq \left\{ \begin{array}{c} L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, 0) \\ \oplus \\ L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, 5) \\ \oplus \\ L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{4}{3}) \end{array} \right\} \otimes \mathcal{L}(5, 0) \\ &\oplus \left\{ \begin{array}{c} L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, \frac{5}{7}) \\ \oplus \\ L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, \frac{12}{7}) \\ \oplus \\ L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{1}{21}) \end{array} \right\} \otimes \mathcal{L}(5, 2) \\ &\oplus \left\{ \begin{array}{c} L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, \frac{22}{7}) \\ \oplus \\ L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, \frac{1}{7}) \\ \oplus \\ L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{10}{21}) \end{array} \right\} \otimes \mathcal{L}(5, 4), \end{aligned}$$

and

$$\begin{aligned}
& \mathcal{L}(3, 3) \otimes \mathcal{L}(1, 1) \otimes \mathcal{L}(1, 0) \\
& \simeq \left\{ \begin{array}{c} L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, 5) \\ \oplus \\ L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, 0) \\ \oplus \\ L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{4}{3}) \end{array} \right\} \otimes \mathcal{L}(5, 0) \\
& \oplus \left\{ \begin{array}{c} L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, \frac{12}{7}) \\ \oplus \\ L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, \frac{5}{7}) \\ \oplus \\ L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{1}{21}) \end{array} \right\} \otimes \mathcal{L}(5, 2) \\
& \oplus \left\{ \begin{array}{c} L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, \frac{1}{7}) \\ \oplus \\ L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, \frac{22}{7}) \\ \oplus \\ L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{10}{21}) \end{array} \right\} \otimes \mathcal{L}(5, 4).
\end{aligned}$$

Hence, $\mathcal{L}(3, 0) \otimes \mathcal{L}(1, 0) \otimes \mathcal{L}(1, 0) \oplus \mathcal{L}(3, 3) \otimes \mathcal{L}(1, 1) \otimes \mathcal{L}(1, 0)$ (and V_L) contains a sub VOA U isomorphic to

$$\left[\begin{array}{c} L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, 0) \\ \oplus \\ L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, 5) \\ \oplus \\ L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{4}{3}) \end{array} \right] \oplus \left[\begin{array}{c} L(\frac{4}{5}, 0) \otimes L(\frac{6}{7}, 5) \\ \oplus \\ L(\frac{4}{5}, 3) \otimes L(\frac{6}{7}, 0) \\ \oplus \\ L(\frac{4}{5}, \frac{2}{3}) \otimes L(\frac{6}{7}, \frac{4}{3}) \end{array} \right] \quad (8)$$

as the commutant of $\mathcal{L}(5, 0)$.

Set

$$e := \frac{1}{16} ((\alpha^4 - \alpha^5)_{(-1)})^2 \mathbf{1} - \frac{1}{4} (e^{\alpha^4 - \alpha^5} + e^{-\alpha^4 + \alpha^5}).$$

Then, $e \in U_2$ and e is a conformal vector with central charge $\frac{1}{2}$. We can check that U_2 has conformal vectors e, f with central charge $\frac{1}{2}$ such that $\langle e, f \rangle = \frac{13}{216}$ and $|\tau_e \tau_f| = 3$, and U is generated by such conformal vectors.

By this construction and the \mathbb{Z}_3 -symmetry of $W(0)$ and $N(0)$, we have the following:

Theorem 3.3. A VOA U contains a sub VOA $W(0) \otimes N(0)$. As a $W(0) \otimes N(0)$ -module, U is isomorphic to

$$W(0) \otimes N(0) \oplus W\left(\frac{2}{3}\right)^+ \otimes N\left(\frac{4}{3}\right)^+ \oplus W\left(\frac{2}{3}\right)^- \otimes N\left(\frac{4}{3}\right)^- \quad (9)$$

after fixing suitable choice of \pm -type of $N(\frac{4}{3})^\pm$. Therefore, U is a simple VOA and generated by its weight 2 subspace as a VOA.

Theorem 3.4.

(1) U is rational.

(2) All irreducible U -modules are given by the following:

$$\begin{aligned} &W(0) \otimes N(0) \oplus W\left(\frac{2}{3}\right)^+ \otimes N\left(\frac{4}{3}\right)^+ \oplus W\left(\frac{2}{3}\right)^- \otimes N\left(\frac{4}{3}\right)^-, \\ &W(0) \otimes N\left(\frac{1}{7}\right) \oplus W\left(\frac{2}{3}\right)^+ \otimes N\left(\frac{10}{21}\right)^+ \oplus W\left(\frac{2}{3}\right)^- \otimes N\left(\frac{10}{21}\right)^-, \\ &W(0) \otimes N\left(\frac{5}{7}\right) \oplus W\left(\frac{2}{3}\right)^+ \otimes N\left(\frac{1}{21}\right)^+ \oplus W\left(\frac{2}{3}\right)^- \otimes N\left(\frac{1}{21}\right)^-, \\ &W\left(\frac{2}{5}\right) \otimes N(0) \oplus W\left(\frac{1}{15}\right)^+ \otimes N\left(\frac{4}{3}\right)^+ \oplus W\left(\frac{1}{15}\right)^- \otimes N\left(\frac{4}{3}\right)^-, \\ &W\left(\frac{2}{5}\right) \otimes N\left(\frac{1}{7}\right) \oplus W\left(\frac{1}{15}\right)^+ \otimes N\left(\frac{10}{21}\right)^+ \oplus W\left(\frac{1}{15}\right)^- \otimes N\left(\frac{10}{21}\right)^-, \\ &W\left(\frac{2}{5}\right) \otimes N\left(\frac{5}{7}\right) \oplus W\left(\frac{1}{15}\right)^+ \otimes N\left(\frac{1}{21}\right)^+ \oplus W\left(\frac{1}{15}\right)^- \otimes N\left(\frac{1}{21}\right)^-. \end{aligned}$$

References

- [Co] J. H. Conway, A simple construction for the Fischer-Griess monster group, *Invent. Math.* **79** (1985), 513-540.
- [DL] C. Dong and J. Lepowsky, Generalized vertex algebras and relative vertex operators, *Progress in Math.* **112**, Birkhäuser, Boston, 1993.
- [DMZ] C. Dong, G. Mason and Y. Zhu, Discrete series of the Virasoro algebra and the moonshine module, *Proc. Symp. Pure. Math.*, American Math. Soc. **56** II (1994), 295-316.
- [FLM] I.B. Frenkel, J. Lepowsky and A. Meurman, *Vertex Operator Algebras and the Monster*, Academic Press, New York, 1988.
- [FZ] I.B. Frenkel and Y. Zhu, Vertex operator algebras associated to representation of affine and Virasoro algebras, *Duke Math. J.* **66** (1992), 123-168.
- [GKO] P. Goddard, A. Kent and D. Olive, Unitary representations of the Virasoro and super-Virasoro algebras, *Comm. Math. Phys.* **103** (1986), 105-119.
- [Gr] R. L. Griess, Jr., The friendly giant, *Invent. Math.* **69** (1982), 1-102.

- [KR] V. G. Kac and A. K. Raina, "Bombay Lectures on Highest Weight Representations of Infinite Dimensional Lie algebras," World Scientific, Singapore, 1987.
- [KMY] M. Kitazume, M. Miyamoto and H. Yamada, Ternary codes and vertex operator algebras, *J. Algebra* **223** (2000), 379–395.
- [LLY] C. H. Lam, N. Lam and H. Yamauchi, Extension of Virasoro vertex operator algebra by a simple module, preprint.
- [LY] C. H. Lam and H. Yamada, Tricritical 3-state Potts model and vertex operator algebras constructed from ternary codes, preprint.
- [M] M. Miyamoto, VOAs generated by two conformal vectors whose τ -involutions generate S_3 , math.GR/0112031, to appear in *J. Algebra*.
- [W] W. Wang, Rationality of Virasoro vertex operator algebras, *IMRN* **71** (1993), 197–211.

**"GALOIS THEORY
FOR
COVERING GRAPHS"**

HAROLD STARK

**JOINT WORK
WITH**

AUDREY TERRAS

- REF. 1) **ADVANCES IN MATH.** 154(2000), 132-195.
2) " " " " 121(1996), 124-165.
3) **DIMACS VOLUME, TO APPEAR.**
4) **GROSS AND TUCKER, TOPOLOGICAL
GRAPH THEORY, WILEY INTERSCIENCE,
1987.**

X IS A FINITE CONNECTED GRAPH, POSSIBLY WITH MULTI-EDGES OR LOOPS. GIVE EACH EDGE OF X A DIRECTION (FOR BOOKKEEPING; X IS UNDIRECTED), AND LABEL THE EDGES AND VERTICES.

DEFINITION: A NEIGHBORHOOD OF A VERTEX v OF X CONSISTS OF $\frac{1}{3}$ OF EACH EDGE STARTING AT v AND $\frac{1}{3}$ OF EACH EDGE TERMINATING AT v .

EXAMPLE:



LET Y BE A CONNECTED FINITE GRAPH.
DEFINITION: Y IS A COVERING GRAPH
 OF X IF WE CAN ASSIGN DIRECTIONS
 TO THE EDGES OF Y SO THAT THERE
 EXISTS A MAP $\pi: Y \rightarrow X$ WHICH IS
 A HOMEOMORPHISM OF NEIGHBORHOODS.
 (π IS CALLED A PROJECTION MAP)

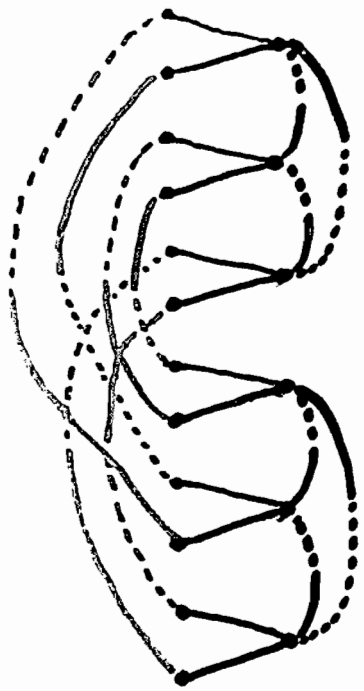
CONVENTION. WHEN WE SPEAK OF A COVER
 Y OF X , AN ASSIGNMENT OF DIRECTIONS
 OF EDGES OF X AND Y AND A PROJECTION
 MAP π ARE PRESUMED TO BE GIVEN AND
 FIXED.

PROPOSITION. π IS ONTO. EVERY $\pi^{-1}(v)$
 AND $\pi^{-1}(e)$ HAS THE SAME CARDINALITY.

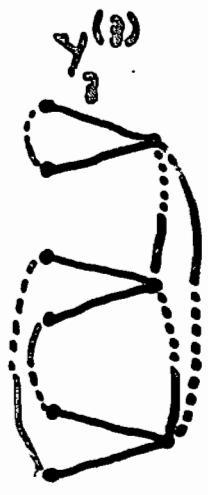
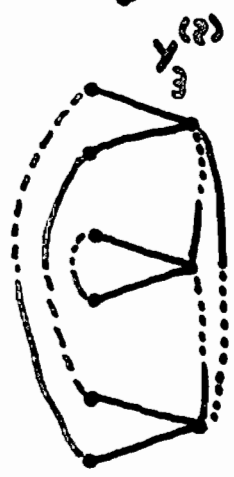
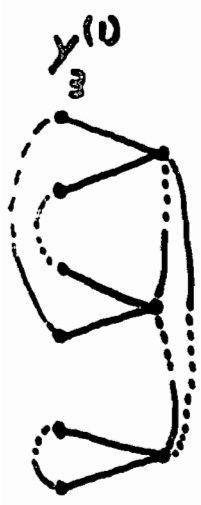
DEFINITION: THIS COMMON CARDINALITY
 IS CALLED THE DEGREE OF THE COVER.

$G = \{1, g, g^2, h, hg, hg^2\}$ $g^3 = h^2 = 1, gh = hg^2$

γ_6



hg^2
 hg
 h
 g^2
 g
 1



THEOREM. SUPPOSE Y IS A COVER OF X WITH PROJECTION MAP π , AND DEGREE d . LET P BE A PATH IN X STARTING AT A VERTEX v OF X . THEN P HAS EXACTLY d LIFTS TO Y . INDEED, GIVEN A VERTEX $\tilde{v} \in \pi^{-1}(v)$ IN Y , THERE IS A UNIQUE PATH \tilde{P} IN Y BEGINNING AT \tilde{v} AND PROJECTING TO P .

DEFINITION. LET T BE A SPANNING TREE OF X . THE d LIFTS OF T TO Y ARE CALLED THE SHEETS OF Y .

SPANNING TREES AND THEIR LIFTS ARE SHOWN IN BLACK.

CONVENTION ON COMPOSITION OF MAPS f AND g : $(fg) \circ (*) = f \circ (g \circ (*))$.

DEFINITION: SUPPOSE Y AND Y' ARE COVERING GRAPHS OF X WITH PROJECTION MAPS π AND π' . SUPPOSE ALSO THAT $i: Y \rightarrow Y'$ IS A GRAPH ISOMORPHISM. IF $\pi = \pi' \circ i$, WE SAY THAT i IS A COVERING ISOMORPHISM AND THAT Y AND Y' ARE COVERING ISOMORPHIC (WITH RESPECT TO X). IF $Y' = Y$, WE SAY i IS A COVERING AUTOMORPHISM OF Y (WITH RESPECT TO X).

PROPOSITION. A GRAPH COVERING Y OF X OF DEGREE d HAS AT MOST d COVERING AUTOMORPHISMS WITH RESPECT TO X .

DEFINITION. IF Y OVER X IS OF DEGREE d AND Y HAS d COVERING AUTOMORPHISMS WITH RESPECT TO X , WE SAY THAT Y IS A NORMAL COVER OF X , OR THAT Y OVER X IS NORMAL, AND THAT THE GROUP $G = G(Y/X)$ OF COVERING AUTOMORPHISMS IS THE GALOIS GROUP OF Y OVER X .

CONVENTION. SUPPOSE Y OVER X IS A NORMAL COVER WITH GROUP $G = G(Y/X)$. PICK A SHEET OF Y AND CALL IT SHEET 1 (WHERE 1 IS THE IDENTITY OF G). IF $g \in G$, WE SAY THAT $g \circ (\text{SHEET } 1)$ IS SHEET g .

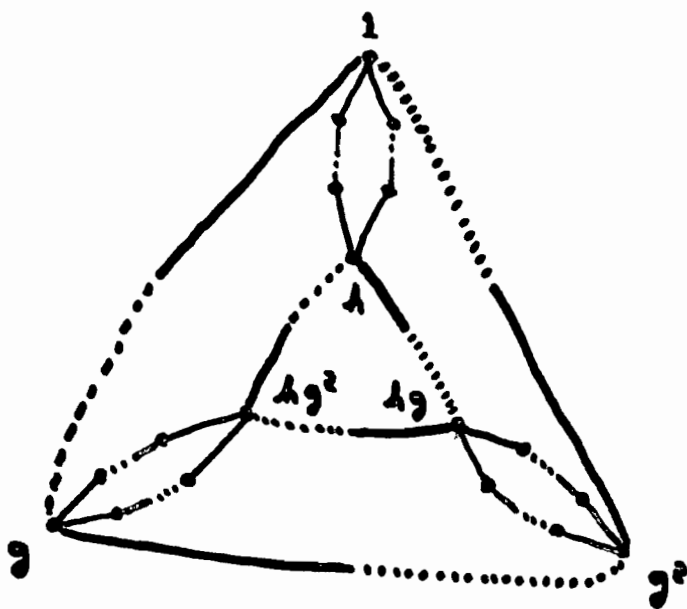
PROPOSITION. $g \circ (\text{SHEET } h) = \text{SHEET } gh$

PROOF : $g \circ (h \circ \text{SHEET } 1) = (gh) \circ \text{SHEET } 1.$

EXAMPLE:

$$G = \{1, g, g^2, h, hg, hg^2\}$$

$$g^3 = h^2 = 1, \quad gh = hg^2$$



COROLLARY. SUPPOSE Y OVER X IS NORMAL WITH GROUP G AND THAT \tilde{P} IS A PATH IN Y STARTING ON SHEET i AND ENDING ON SHEET j WHICH PROJECTS TO A PATH P IN X . IF $g \in G$, THEN $g \cdot \tilde{P}$ IS THE UNIQUE LIFT OF P STARTING ON SHEET gi AND ENDING ON SHEET gj .

THEOREM. SUPPOSE X IS A CONNECTED GRAPH OF RANK λ (WHICH MEANS THAT $X-T$ CONSISTS OF λ EDGES). A FINITE GROUP G IS THE GALOIS GROUP OF A CONNECTED NORMAL COVER Y OF X IF AND ONLY IF G CAN BE GENERATED BY $s\lambda$ ELEMENTS.

SKETCH OF THE CONSTRUCTION OF γ WHEN

$G = \langle \Delta_1, \Delta_2, \dots, \Delta_n \rangle$. LABEL THE Λ

(DIRECTED) EDGES OF $X-T : e_1, e_2, \dots, e_\Lambda$

LABEL $|G|$ COPIES OF T BY GROUP ELEMENTS $g \in G$ (SOON TO BE THE SHEETS OF γ). IN PARTICULAR, IF N IS A VERTEX OF X ,

WE SAY THAT (N, g) IS THE COPY OF N IN SHEET g . LET $1 \leq m \leq \Lambda$ AND

SUPPOSE THAT e_m BEGINS AT VERTEX N AND ENDS AT VERTEX N' . CONNECT

$(N, 1)$ TO (N', Δ_m) AND CALL THE

RESULTING DIRECTED EDGE \tilde{e}_m . THANKS TO THE LAST COROLLARY, WE CONNECT

(N, g) TO $(N', g\Delta_m)$ TO GET $g \circ \tilde{e}_m$ FOR EACH $g \in G$. WHEN WE DO THIS FOR ALL

$m, 1 \leq m \leq \Lambda$, WE HAVE γ .

COROLLARY. AS A SPECIAL CASE, IF

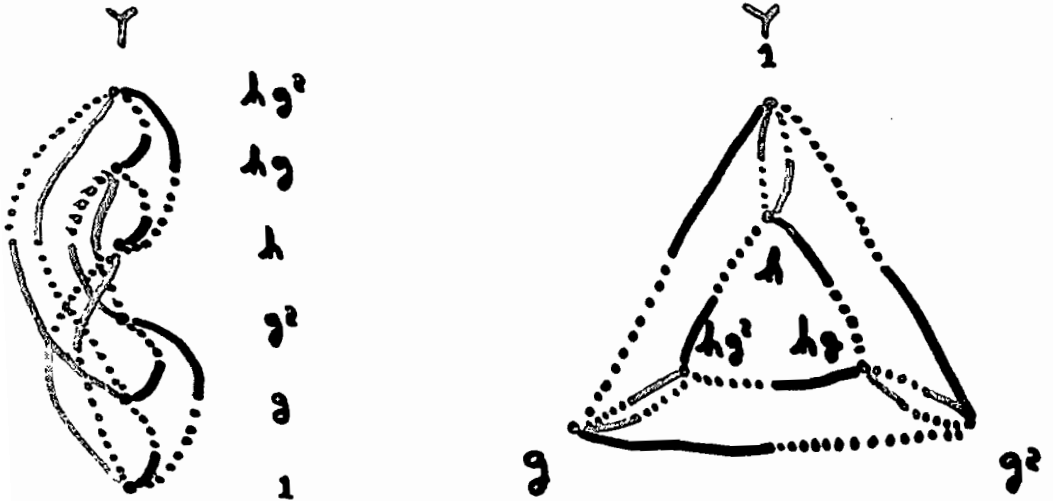
$G = \langle a_1, \dots, a_n \rangle$, WE GET THE

CAYLEY GRAPH OF G AS A NORMAL

COVER OF X :
(ONE VERTEX, n LOOPS)



EXAMPLE:



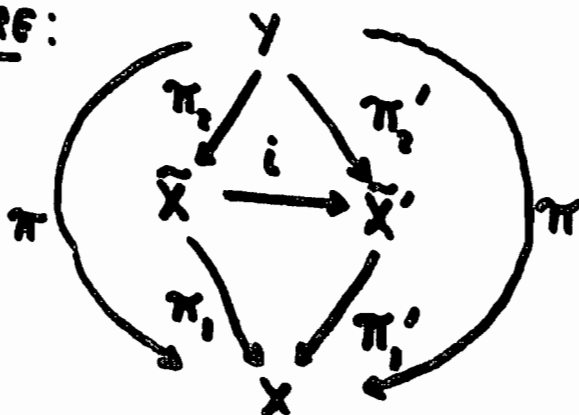
DEFINITION: SUPPOSE THAT Y IS A COVER OF X WITH PROJECTION MAP π . WE SAY THAT \tilde{X} IS INTERMEDIATE TO Y AND X IF THERE ARE PROJECTION MAPS $\pi_1: \tilde{X} \rightarrow X$ AND $\pi_2: Y \rightarrow \tilde{X}$ SUCH THAT $\pi = \pi_1 \pi_2$. WARNING: THERE COULD BE MORE THAN ONE SUCH PAIR π_1, π_2 . IT IS REALLY THE TRIPLE $(\tilde{X}, \pi_1, \pi_2)$ THAT GIVES THE INTERMEDIATE GRAPH.

EXAMPLE: $Y_3^{(1)}, Y_3^{(2)}, Y_3^{(3)}$ ARE ALL INTERMEDIATE TO Y_6 AND X .

EXAMPLE: IN THIS CONTEXT, IF $(\tilde{X}, \pi_1, \pi_2)$ AND $(\tilde{X}', \pi_1', \pi_2')$ ARE INTERMEDIATE, THEN \tilde{X} AND \tilde{X}' ARE COVERING ISOMORPHIC (WITH RESPECT TO X) IF THERE IS A GRAPH ISOMORPHISM $i: \tilde{X} \rightarrow \tilde{X}'$ SUCH THAT $\pi_1 = \pi_1' i$

DEFINITION. SUPPOSE $(\tilde{X}, \pi_1, \pi_2)$ AND $(\tilde{X}', \pi_1', \pi_2')$ ARE INTERMEDIATE TO Y AND X . WE SAY $\tilde{X} = \tilde{X}'$ AND THINK OF \tilde{X} AND \tilde{X}' AS THE SAME INTERMEDIATE GRAPH IF THERE IS A GRAPH ISOMORPHISM $i: \tilde{X} \rightarrow \tilde{X}'$ SUCH THAT $\pi_1 = \pi_1' i$ AND $\pi_2' = i \pi_2$.

PICTURE:



THEOREM (FUNDAMENTAL THM. OF GALOIS

THEORY). SUPPOSE Y OVER X IS NORMAL, $G = G(Y/X)$.

- 1) SUPPOSE \tilde{X} IS INTERMEDIATE TO Y AND X . THEN Y OVER \tilde{X} IS NORMAL AND THERE IS A SUBGROUP $H = H(\tilde{X}) \triangleleft G$ WHICH IS $G(Y/\tilde{X})$.
- 2) TWO INTERMEDIATE GRAPHS \tilde{X}_1 AND \tilde{X}_2 ARE EQUAL (SEE DEF.) $\Leftrightarrow H(\tilde{X}_1) = H(\tilde{X}_2)$
- 3) GIVEN A SUBGROUP H OF G , THERE IS A GRAPH \tilde{X} INTERMEDIATE TO Y AND X SUCH THAT $H = G(Y/\tilde{X})$. WE WRITE $\tilde{X} = \tilde{X}(H)$.
- 4) WE HAVE $H(\tilde{X}(H)) = H$ AND $\tilde{X}(H(\tilde{X})) = \tilde{X}$. SO WE CAN WRITE $\tilde{X} \leftrightarrow H$ FOR THE CORRESPONDENCE BETWEEN GRAPHS \tilde{X} INTERMEDIATE TO Y AND X AND SUBGROUPS H OF THE GALOIS GROUP $G = G(Y/X)$.
- 5). IF $\tilde{X}_1 \leftrightarrow H_1$, AND $\tilde{X}_2 \leftrightarrow H_2$, THEN \tilde{X}_1 IS INTERMEDIATE TO Y OVER \tilde{X}_2 IF AND ONLY IF $H_1 \subset H_2$.

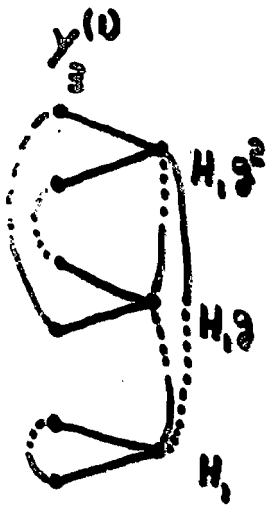
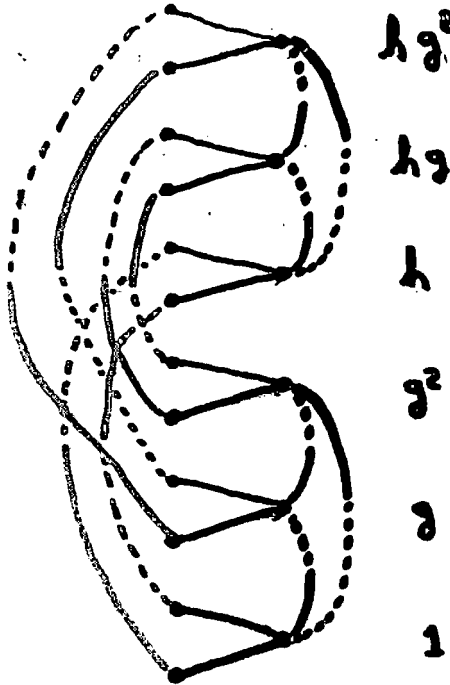
WE DESCRIBE THE CONSTRUCTION GIVING 3).

DEFINITION. SUPPOSE Y OVER X IS NORMAL WITH GROUP G , AND LET H BE A SUBGROUP OF G . AGAIN, WE WRITE THE VERTICES OF Y IN THE FORM (N, g) WHERE N IS A VERTEX OF X , $g \in G$, (N, g) IS ON SHEET g AND PROJECTS TO N BY π . THE VERTICES OF \tilde{X} ARE PAIRS (N, Hg) WHERE Hg RUNS THROUGH THE RIGHT COSETS OF H . WE LET $\pi_2: (N, g) \mapsto (N, Hg)$, $\pi_1: (N, Hg) \mapsto N$. IF e_Y IS A DIRECTED EDGE OF Y STARTING AT (N_0, g_0) , ENDING AT (N_1, g_1) AND PROJECTING TO e IN X GOING FROM N_0 TO N_1 IN X , WE CREATE AN EDGE \tilde{e} OF \tilde{X} STARTING AT (N_0, Hg_0) AND ENDING AT (N_1, Hg_1) . WE DEFINE $\pi_2(e_Y) = \tilde{e}$, $\pi_1(\tilde{e}) = e$. THIS GIVES \tilde{X} .

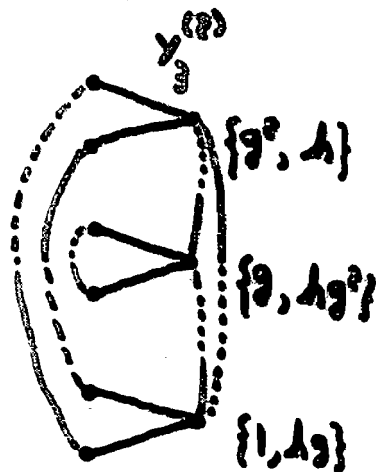
$$G = \{1, g, g^2, \lambda, \lambda g, \lambda g^2\} \quad g^3 = \lambda^2 = 1, \quad g\lambda = \lambda g^2$$

143

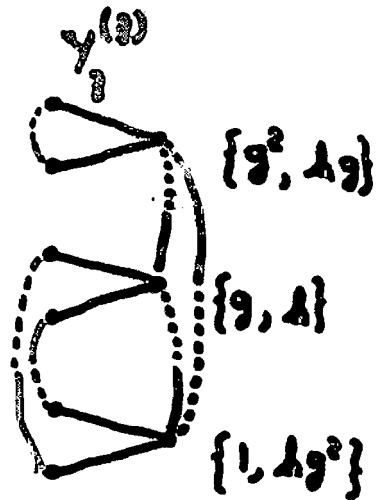
γ_6



$$H_1 = \{1, \lambda\}$$



$$H_2 = \{1, \lambda g\}$$



$$H_3 = \{1, \lambda g^2\}$$

x



DEFINITION. SUPPOSE Y OVER X IS NORMAL WITH GROUP $G = G(Y/X)$. SUPPOSE $\tilde{X}_1 \leftrightarrow H_1$ AND $\tilde{X}_2 \leftrightarrow H_2$. WE SAY \tilde{X}_1 AND \tilde{X}_2 ARE CONJUGATE WITHIN Y OVER X IF H_1 AND H_2 ARE CONJUGATE IN G (I.E. $H_2 = g^{-1}H_1g$ FOR SOME $g \in G$).

EXAMPLE: THE GRAPHS $Y_2^{(1)}$, $Y_3^{(2)}$, $Y_3^{(1)}$ ARE ALL CONJUGATE WITHIN Y_6 OVER X .

THEOREM SUPPOSE Y OVER X IS NORMAL AND THAT \tilde{X}_1 AND \tilde{X}_2 ARE INTERMEDIATE. THEN \tilde{X}_1 AND \tilde{X}_2 ARE CONJUGATE IF AND ONLY IF \tilde{X}_1 AND \tilde{X}_2 ARE COVERING ISOMORPHIC.

SUPPOSE Y OVER X IS NORMAL WITH GROUP $G = G(Y/X)$. LET e BE A (DIRECTED) EDGE IN $X-T$ AND SUPPOSE THE LIFTING OF e TO Y WHICH STARTS ON SHEET 1 TERMINATES ON SHEET $\sigma(e) \in G$.

DEFINITION: WE SAY $\sigma(e)$ IS THE NORMALIZED FROBENIUS AUTOMORPHISM IN G CORRESPONDING TO e .

LET \tilde{X} BE AN INTERMEDIATE GRAPH TO Y OVER X CORRESPONDING TO $H \subseteq G$. THE SHEETS OF \tilde{X} WILL BE LABELED BY THE VARIOUS COSETS Hg OF H IN G . SUPPOSE $[G:H] = m$. IF WE WRITE

$$\begin{pmatrix} Hg_1 \\ Hg_2 \\ \vdots \\ Hg_m \end{pmatrix} \sigma(e) = M(e) \begin{pmatrix} Hg_1 \\ Hg_2 \\ \vdots \\ Hg_m \end{pmatrix}$$

WHERE $M(e)$ IS A PERMUTATION MATRIX

THEN $M(e)$ IN TURN CORRESPONDS TO
A PERMUTATION $\mu(e)$ ON m "LETTERS" $1, 2, \dots, m$.

THEOREM. THE CYCLE STRUCTURE OF
 $\mu(e)$ DESCRIBES THE LIFTS OF e TO \tilde{X} .

EXAMPLE: Y_6 OVER X AGAIN. FOR

$H = H_1, H_2, H_3$ WE MAY TAKE THE
THREE COSET REPRESENTATIVES TO BE
 $1, g, g^2$. WE HAVE FOR $e = (1$

$$\begin{pmatrix} H_1 \\ H_1 g \\ H_1 g^2 \end{pmatrix} \lambda = \begin{pmatrix} H_1 \\ H_1 g^2 \\ H_1 g \end{pmatrix}, \mu(e) = (1)(22) \quad \sigma(e) = \lambda$$

$$\begin{pmatrix} H_2 \\ H_2 g \\ H_2 g^2 \end{pmatrix} \lambda = \begin{pmatrix} H_2 g^2 \\ H_2 g \\ H_2 \end{pmatrix}, \mu(e) = (13)(2)$$

$$\begin{pmatrix} H_3 \\ H_3 g \\ H_3 g^2 \end{pmatrix} \lambda = \begin{pmatrix} H_3 g \\ H_3 \\ H_3 g^2 \end{pmatrix}, \mu(e) = (12)(3)$$

EXAMPLE (BUSER) $G = GL_3(F_2)$ ORDER 168,

$$H_1 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ * & * & * \\ * & * & * \end{pmatrix} \right\}, H_2 = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & * & * \\ 0 & * & * \end{pmatrix} \right\}.$$

BOTH OF ORDER 24 AND INDEX 7.

$$\text{LET } A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

SET $\sigma(A) = A$, $\sigma(B) = B$; IN THE RIGHT ORDER THE SEVEN COSETS OF H_1 AND H_2 GIVE PERMUTATIONS μ_1 AND μ_2 WITH

$$\mu_1(A) = (1436)(2)(57), \mu_1(B) = (132)(4)(576)$$

AND

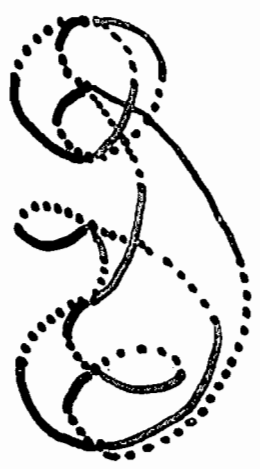
$$\mu_2(A) = (14)(2376)(5), \mu_2(B) = (123)(4)(567).$$

THIS GIVES TWO NON-ISOMORPHIC ISOSPECTRAL GRAPHS AS SCHREIER GRAPHS, BUT HAVING LOOPS AND MULTI-EDGES.

\tilde{X}_1

\tilde{X}_2

7
6
5
4
3
2
1



7
6
5
4
3
2
1



X

WE EXPAND THE TREE (\bullet) OF THE
LAST EXAMPLE AND ADD ONE MORE
EDGE c :

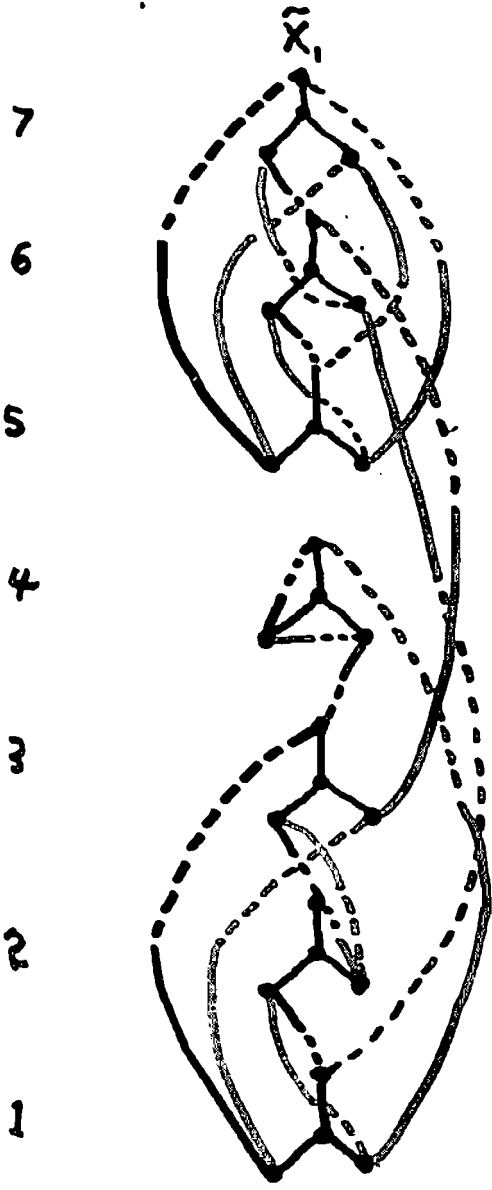


AND TAKE $\sigma(c) = \sigma(b) = B, \sigma(a) = A$

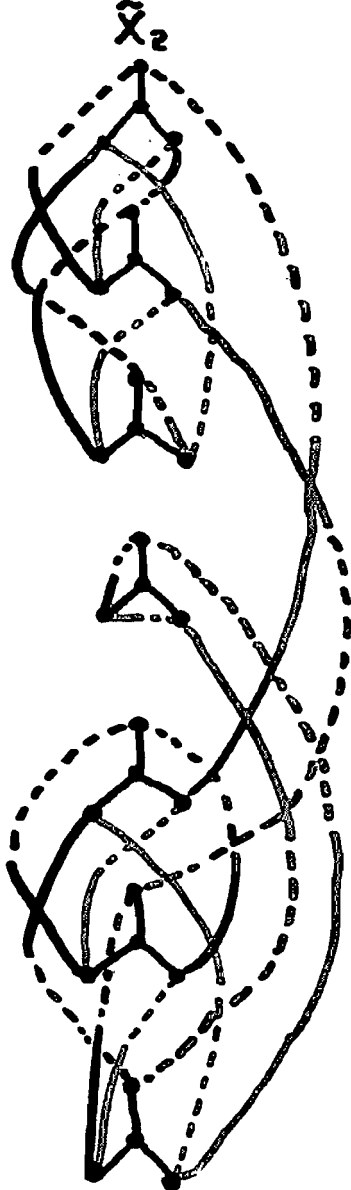
THEOREM (S.-T.) \tilde{X}_1 AND \tilde{X}_2 ARE

ISOSPECTRAL, NON-ISOMORPHIC
REGULAR GRAPHS WITHOUT LOOPS
OR MULTI-EDGES.

THIS IS THE FIRST SUCH EXAMPLE
THAT WE KNOW OF.



$$\begin{aligned} \mu(a) &= (1436)(2)(57) \\ \mu(b) &= \mu(c) \\ &= (132)(4)(576) \end{aligned}$$



$$\begin{aligned} \mu(a) &= (14)(2376)(5) \\ \mu(b) &= \mu(c) \\ &= (123)(4)(567) \end{aligned}$$

2i
7
6
5
4
3
2
1

A formula for the number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$

Vladimir D. Tonchev
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931
USA

Dedicated to Alex Rosa on the occasion of his 60th birthday

Abstract

Assmus [1] gave a description of the binary code spanned by the blocks of a Steiner triple or quadruple system according to the 2-rank of the incidence matrix. Using this description, the author [8] found a formula for the total number of distinct Steiner triple systems on $2^n - 1$ points of 2-rank $2^n - n$. In this paper, a similar formula is found for the number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$. The formula can be used for deriving bounds on the number of pairwise non-isomorphic systems for large n , and for the classification of all non-isomorphic systems of small orders. The formula implies that the number of non-isomorphic Steiner quadruple systems on 2^n points of 2-rank $2^n - n$ grows exponentially. As an application, the Steiner quadruple systems on 16 points of 2-rank 12 are classified up to isomorphism.

1 Introduction

A Steiner triple system $STS(v)$ is a set of v points together with a collection of 3-subsets called blocks or *triples*, such that every pair of points is contained in exactly one block. Alternatively, a Steiner triple system $STS(v)$ is a $2-(v, 3, 1)$ design [2]. A recent monograph with extensive references on triple systems is the book by Colbourn and Rosa [3].

A Steiner quadruple system $SQS(v)$ is a set of v points together with a collection of 4-subsets called blocks or *quadruples*, such that every three points are contained together in exactly one block. Alternatively, an $SQS(v)$ is a $3-(v, 4, 1)$ design (see [2] for more on designs).

The blocks through a point P in an $SQS(v)$, after having P deleted, form an $STS(v-1)$ called *derived*. A *subsystem* of a Steiner system is a subset of the point set together with the blocks contained in it that is itself a Steiner system.

Two Steiner systems on the same point set are *distinct* if their block collections are not identical. Two Steiner systems are *isomorphic* if there is a bijection between their point sets that maps the blocks of the first system into blocks of the second. An *automorphism* of a Steiner system is any permutation of the points that preserves the collection of blocks.

The *incidence matrix* $A = (a_{ij})$ of a Steiner system is a $(0,1)$ -matrix with rows indexed by the blocks, and columns indexed by the points, with $a_{ij} = 1$ if the i th block contains the j th point, and $a_{ij} = 0$ otherwise.

Doyen, Hubaut and Vandensavel [4] found a formula for the rank of the incidence matrix A of a Steiner triple system $STS(v)$ over the binary field (2-rank of A , or $rank_2(A)$). They proved also that the 2-rank of any Steiner triple system $STS(2^n - 1)$ is greater than or equal to $2^n - n - 1$, and the minimum rank $2^n - n - 1$ is achieved if and only if the system is isomorphic to the classical one with blocks being the lines in the binary projective space $PG(n-1, 2)$.

Teirlinck [7] found a formula for the 2-rank of a Steiner quadruple system, and proved that the 2-rank of any $SQS(2^n)$ is greater than or equal to $2^n - n - 1$, with equality if and only if the system is isomorphic to the classical one having as blocks the planes in the binary affine space $AG(n, 2)$.

In this paper, we derive a formula for the total number of $SQS(2^n)$'s whose 2-rank is greater by one than the minimum $2^n - n - 1$. The main tool for deriving this formula is the binary code of a Steiner quadruple system.

A binary linear (n, k) code is a k -dimensional subspace of the n -dimensional vector space $GF(2)^n$ over the binary field $GF(2)$. Two codes are *equivalent* if they differ by a permutation of the coordinates. An automorphism of a code is any permutation of the coordinates which preserves the code as a set of vectors. The Hamming *weight* of a vector is the number of its nonzero components. For more on codes see [6].

An (n, k) code C contains a Steiner system S on n points if the rows of the incidence matrix of S are vectors in C .

The *code* of a Steiner system is the binary linear code spanned by the incidence vectors of the blocks, i.e., by the rows of the incidence matrix.

Assmus [1] proved that two Steiner triple or quadruple systems with the same number of points and the same 2-rank have equivalent codes, and up to isomorphism, all Steiner systems of the same 2-rank can be found in the same code. Assmus also gave an explicit description of the code of a Steiner triple or quadruple system of given 2-rank and its automorphism group.

Using these results, the author of this paper found a formula for the number of distinct Steiner triple systems on $2^n - 1$ points having 2-rank $2^n - n$ [8]. It is the aim of the present paper to derive a similar formula for the number of Steiner quadruple systems on 2^n points of 2-rank $2^n - n$.

The formula can be used as a tool for the classification of all Steiner systems of 2-rank

$2^n - n$ up to isomorphism, and for deriving bounds on the number of pairwise non-isomorphic Steiner systems of 2-rank $2^n - n$. The formula implies that the number of non-isomorphic Steiner quadruple systems $SQS(2^n)$ of 2-rank $2^n - n$ grows exponentially.

2 The code of an $SQS(2^n)$ of 2-rank $2^n - n$

Let A be an incidence matrix of the *classical* Steiner quadruple system on 2^n points having as blocks the planes in the n -dimensional binary affine space $AG(n, 2)$.

By the results of Assmus [1], the code C_n spanned by the rows of the following matrix

$$G = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ & & A & & \end{pmatrix} \quad (1)$$

contains representatives of all isomorphism classes of $SQS(2^n)$'s of 2-rank $2^n - n$. Alternatively, C_n is equivalent to the null space of the matrix

$$H = [R_{n-1}, R_{n-1}], \quad (2)$$

where R_{n-1} is the first order Reed-Muller code of length 2^{n-1} , or equivalently, R_{n-1} is the null space of the incidence matrix of the Steiner quadruple system $SQS(2^{n-1})$ with blocks being the planes in the affine space $AG(n-1, 2)$. This result is implicit in Key and Sullivan [5].

The description of the code C_n as the null space of the matrix (2) implies that the automorphism group of C_n is a product of the automorphism group of R_{n-1} with a group of order $2^{2^{n-1}}$ that corresponds to interchanges of identical coordinates of the two copies of R_{n-1} . Thus, the following holds true.

Lemma 2.1

$$|Aut(C_n)| = 2^{2^{n-1}} \cdot 2^{n-1}(2^{n-1} - 1)(2^{n-1} - 2) \dots (2^{n-1} - 2^{n-2}).$$

The $(2^n, 2^n - n - 1)$ code spanned by the rows of A is equivalent to the extended Hamming code H_n^* of length 2^n . The coordinates of H_n^* can be identified with the points of the n -dimensional binary affine space $AG(n, 2)$. The full automorphism group of H_n^* is the general affine group $GA(n, 2)$ of order

$$2^n(2^n - 1) \dots (2^n - 2^{n-1}).$$

The group $GA(n, 2)$ acts 3-transitively on the 2^n code coordinates of H_n^* . Thus, changing the location of the two ones in the first row of the matrix G given by eq. (1) yields another code equivalent to C_n . For convenience, we will assume that, as in (1), exactly the first two positions are nonzero.

Throughout this paper, we often identify the 2^n coordinates of C_n with the points of the n -dimensional binary affine space $AG(n, 2)$, that is, with the $(0, 1)$ -vectors with n components, ordered lexicographically: coordinate one by $\bar{0} = (0, \dots, 0)$, coordinate two by $\bar{1} = (0, 0, \dots, 0, 1)$, etc., coordinate 2^n by $(1, 1, \dots, 1)$.

Lemma 2.2 *The code C_n contains a total of 2^{n-1} vectors of weight 2 whose supports are 2^{n-1} disjoint pairs that form a class of parallel lines in $AG(n, 2)$.*

Proof. A vector of weight two in C_n is either the first row of (1) , $v = (1, 1, 0, \dots, 0)$, or the sum of v with a row of A that starts with two ones. Since A is the incidence matrix of a $3-(2^n, 4, 1)$ design that is also a $2-(2^n, 4, 2^{n-1} - 1)$ design, there are exactly $2^{n-1} - 1$ rows of A that have ones in the first two positions. Any row of A is the incidence vector of an affine plane in $AG(n, 2)$. According to our labeling of the coordinates of C_n , the four nonzero positions in a row R of A correspond to a quadruple of vectors $x, y, z, t \in GF(2)^n$ such that

$$x + y + z + t = \bar{0}.$$

In particular, if the first two positions of R are nonzero, we have

$$x = \bar{0}, y = \bar{1}, z, t = z + \bar{1}.$$

The two nonzero positions of $v=(1, 1, 0, \dots, 0)$ are labeled by $\bar{0}$ and $\bar{1}$. Consequently, the nonzero positions of any other vector of weight two in C_n are labeled by a pair of points in $AG(n, 2)$ of the form $\{z, z + \bar{1}\}$, $z \neq \bar{0}, \bar{1}$. Note that any such pair is a translation of the affine line $\{\bar{0}, \bar{1}\}$ by the vector z :

$$\{z, z + \bar{1}\} = \{\bar{0}, \bar{1}\} + z.$$

Thus, the 2^{n-1} vectors of weight two in C_n are the incidence vectors of the affine line $\{\bar{0}, \bar{1}\}$ and the $2^{n-1} - 1$ affine lines parallel to the line $\{\bar{0}, \bar{1}\}$. \square

It follows from Lemma 2.2 that the intersection of the general affine group $GA(n, 2)$ with the automorphism group $Aut(C_n)$ of C_n is the stabilizer of a class of parallel lines in $AG(n, 2)$ in $GA(n, 2)$. There are $2^{n-1}(2^n - 1)$ lines in $AG(n, 2)$ that are partitioned into $2^n - 1$ parallel classes. Since all parallel classes are in one orbit under the action of $GA(n, 2)$, we have the following.

Lemma 2.3

$$|GA(n, 2) \cap Aut(C_n)| = |GA(n, 2)| / (2^n - 1) = 2^n(2^n - 2) \dots (2^n - 2^{n-1}).$$

We will need also the following result.

Lemma 2.4 *The 2^{n-1} parallel lines being the supports of the weight two vectors in C_n considered as "points", and the affine planes in $AG(n, 2)$ that contain lines from this parallel class, considered as "blocks", form a trivial $2-(2^{n-1}, 2, 1)$ design.*

Proof. The line $\{\bar{0}, \bar{1}\}$ considered as a pair of affine points is contained in exactly $2^{n-1} - 1$ affine planes, each of the form

$$\{\bar{0}, \bar{1}, z, z + \bar{1}\}.$$

Thus, the line $\{\bar{0}, \bar{1}\}$ appears in exactly one affine plane with every parallel line $\{z, z + \bar{1}\}$, $z \neq \bar{0}, \bar{1}$. The fact that every other line that is parallel to $\{\bar{0}, \bar{1}\}$ also appears in $2^{n-1} - 1$ affine planes follows from the transitivity of the stabilizer of a class of parallel lines in $GA(n, 2)$ on the set of lines in the parallel class. \square

3 Vectors of weight four in C_n

The set of codewords of weight four in C_n consists of vectors of the following three types (i), (ii), (iii):

(i) The rows of A that are the incidence vectors of the affine planes in $AG(n, 2)$. The total number of such vectors is

$$b = \frac{2^n(2^n - 1)(2^n - 2)}{4 \cdot 3 \cdot 2}.$$

The design G with incidence matrix A is the unique (up to isomorphism) 3 -($2^n, 4, 1$) design of minimum 2-rank equal to $2^n - n - 1$. This 3-design is a 2-design with

$$\lambda_2 = 2^{n-1} - 1,$$

and a 1-design with

$$\lambda_1 = \frac{(2^n - 1)(2^{n-1} - 1)}{3}.$$

There are exactly $\lambda_2 = 2^{n-1} - 1$ rows of A that contain ones in the first two positions, and exactly

$$2(\lambda_1 - \lambda_2) = \frac{8(2^{n-1} - 1)(2^{n-2} - 1)}{3}$$

rows of A with exactly one nonzero entry in the first two positions. The number of rows of A that have zeros in the first two positions is

$$b - 2\lambda_1 + \lambda_2 = \frac{2^n(2^n - 1)(2^n - 2)}{4 \cdot 3 \cdot 2} - 2 \frac{(2^n - 1)(2^{n-1} - 1)}{3} + (2^{n-1} - 1). \quad (3)$$

(ii) A set of

$$2(\lambda_1 - \lambda_2) = \frac{8(2^{n-1} - 1)(2^{n-2} - 1)}{3} \quad (4)$$

vectors obtained as the sum of the vector $v=(1, 1, 0, \dots, 0)$ with a row of A that has exactly one nonzero entry in the first two positions.

(iii) Any vector that is the sum of $v=(1, 1, 0, \dots, 0)$ with a vector u of weight six in the extended Hamming code H_n^* starting with two ones: $u = (1, 1, \dots)$. To count this set of vectors, note that any such vector in H_n^* is obtained by extending a codeword of weight five in the Hamming code H_n of length $2^n - 1$, assuming that the added overall parity-check position is the first position. The five nonzero positions of u other than the first position are labeled by five nonzero points in $AG(n, 2)$, one being $\bar{1} = (1, 0, \dots, 0)$, that sum up to the zero vector $\bar{0} \in GF(2)^n$. Equivalently, if $\bar{1}, \alpha, \beta, \gamma, \delta$ are these five points in $AG(n, 2)$, we have

$$\alpha + \beta + \gamma + \delta = \bar{1}.$$

where $\alpha, \beta, \gamma, \delta$ are distinct from $\bar{0}$ and $\bar{1}$. The Hamming code H_n contains a total of

$$\frac{(2^n - 1)(2^n - 2)(2^n - 2^2)(2^n - 2^3)}{5!}$$

vectors of weight five. Among those, there are exactly

$$\frac{(2^n - 2)(2^n - 2^2)(2^n - 2^3)}{4!} \tag{5}$$

vectors with nonzero first position. Consequently, the number of vectors of weight four in C_n that are obtained as the sum of $v=(1, 1, 0, \dots, 0)$ with a vector of weight six in H_n^* is given by formula (5).

It is convenient to arrange the set of codewords of weight four in C_n as in (6).

$$\left(\begin{array}{cc} \hline & A_0 \\ 1 & 0 \\ \dots & \\ 1 & 0 \\ \hline 0 & 1 \\ \dots & \\ 0 & 1 \\ \hline 0 & 0 \\ \dots & \\ 0 & 0 \\ \hline 1 & 0 \\ \dots & \\ 1 & 0 \\ \hline 0 & 1 \\ \dots & \\ 0 & 1 \\ \hline 0 & 0 \\ \dots & \\ 0 & 0 \\ \hline & B_3 \end{array} \right) . \tag{6}$$

The sub-matrices in (6) are defined as follows:

- The rows of (6) that involve A_0, A_1, A_2, A_3 comprise the rows of A .
- A_0 consists of the $2^{n-2}(2^{n-1} - 1)$ rows of A being the incidence vectors of the affine planes that contain supports of vectors of weight two in C_n (Lemma 2.4).
- The rows that involve B_1, B_2 are vectors of weight four of type (ii).
- Each of the matrices A_1, A_2, B_1, B_2 has

$$\lambda_1 - \lambda_2 = \frac{4(2^{n-1} - 1)(2^{n-2} - 1)}{3}$$

rows (see eq. (4)).

- The rows involving B_3 are vectors of type (iii).
- Each of the matrices A_3 and B_3 has

$$\frac{(2^n - 2)(2^n - 2^2)(2^n - 2^3)}{4!}$$

rows (by eqs. (5) and (3)).

Lemma 3.1 *The incidence structure \mathcal{I} with incidence matrix (6), having the 2^n coordinate indices of C_n as points and the supports of codewords of weight four in C_n as blocks, enjoys the following properties:*

(a) *Any triple of points that contains an affine line parallel to $\{\bar{0}, \bar{1}\}$, i.e., a pair of points of the form $\{z, z + \bar{1}\}$, $z \in GF(2)^n$, is contained in exactly one block of \mathcal{I} whose incidence vector is a row of A_0 from eq. (6).*

(b) *Any triple of points that does not contain any pair of points of the form $\{z, z + \bar{1}\}$ is contained in exactly two blocks of \mathcal{I} , one being an affine plane with incidence vector a row of the matrix (7),*

$$\begin{pmatrix} 1 & 0 \\ \dots & A_1 \\ 1 & 0 \\ \hline 0 & 1 \\ \dots & A_2 \\ 0 & 1 \\ \hline 0 & 0 \\ \dots & A_3 \\ 0 & 0 \end{pmatrix}, \quad (7)$$

and the second block has an incidence vector being a row of the matrix (8).

$$\begin{pmatrix} 1 & 0 \\ \dots & B_1 \\ 1 & 0 \\ \hline 0 & 1 \\ \dots & B_2 \\ 0 & 1 \\ \hline 0 & 0 \\ \dots & B_3 \\ 0 & 0 \end{pmatrix}. \quad (8)$$

Proof. (a) Since all affine lines $\{z, z + \bar{1}\}$ are in one orbit under the automorphism group of C_n , it suffices to prove the statement for any triple T that contains the line $\{\bar{0}, \bar{1}\}$. Let $T = \{\bar{0}, \bar{1}, u\}$. There is only one affine plane \mathcal{P} that contains T , namely $\mathcal{P} = \{\bar{0}, \bar{1}, u, u + \bar{1}\}$. The incidence vector of \mathcal{P} is a row of A_0 by Lemma 2.4. Since the rows of (7) are incidence

vectors of affine planes that do not contain any affine line parallel to $\{\bar{0}, \bar{1}\}$, T is not contained in any block of \mathcal{I} with incidence vector being a row of (7). Finally, T is not contained in any block of \mathcal{I} with incidence vector being a row of (8), for any such block does not contain at least one of the points $\bar{0}$ and $\bar{1}$.

To prove (b), it is sufficient to show that every two blocks of \mathcal{I} with incidence vectors from (8) share at most two points (the rest follows by counting the total number of triples covered by blocks with incidence vectors from A_0 , (7), or (8)). Note that the sub-matrix (9) of matrix (8) is obtained by permuting the first two positions in a set of codewords of weight four in the extended Hamming code H_n^* . The minimum Hamming distance of H_n^* is four, thus any two rows of (9) can share at most two nonzero coordinates.

$$\begin{pmatrix} 1 & 0 & & \\ \dots & & B_1 & \\ 1 & 0 & & \\ \hline 0 & 1 & & \\ \dots & & B_2 & \\ 0 & 1 & & \end{pmatrix}. \quad (9)$$

The rows of the sub-matrix (10) of matrix (8) are obtained by adding the vector $(1, 1, 0, \dots, 0)$ to vectors of weight six in H_n^* that start with two ones. The Hamming distance between any two vectors $x = (1, 1, \dots)$, $y = (1, 1, \dots)$, $x \neq y$, $x, y \in H_n^*$, is at least four. Thus, if x and y are both of weight six, they can share at most four nonzero coordinates. Consequently, the rows $x + (1, 1, 0, \dots, 0)$, $y + (1, 1, 0, \dots, 0)$ of (10) that correspond to x and y , can share at most two nonzero coordinates.

$$\begin{pmatrix} 0 & 0 & & \\ \dots & & B_3 & \\ 0 & 0 & & \end{pmatrix}. \quad (10)$$

Finally, if x is a row of (9) and y is a row of (10), then $x' = x + (1, 1, \dots, 0)$ is a vector of weight four in H_n^* and $y' = y + (1, 1, \dots, 0)$ is a vector of weight six in H_n^* , and x' and y' share one nonzero coordinate in the first two positions. Thus, x' , y' can share at most two more nonzero coordinates with indices greater than two. Consequently, x and y share at most two nonzero coordinates. \square

4 $SQS(2^n)$'s in the code C_n

The only codewords of weight four in C_n that contain supports of codewords of weight two are rows of A_0 (see eq. (6)). By Lemma 2.4, the support of every codeword of weight two is covered by exactly $2^{n-1} - 1$ rows of A_0 . It follows that the incidence matrix of any $SQS(2^n)$, or $3-(2^n, 4, 1)$ design D , whose rows are codewords of weight four in C_n , must contain the rows of A_0 : for, the pair of points $\bar{0}, \bar{1}$ that labels the first two code coordinates, as well

as every other pair that is the support of a weight two vector in C_n , must be contained in $\lambda_2 = 2^{n-1} - 1$ blocks of D .

Consequently, the incidence matrix of D is obtained by replacing some set A' of k rows of the matrix (7) with an appropriate set B' of k rows of the matrix (8). Here "appropriate" means that the sets A' , B' , considered as incidence vectors, cover exactly the same sets of triples of points. We call any such pair A' , B' a *matching pair*.

We will describe explicitly a matching pair $\{A', B'\}$, where A' and B' each consists of eight rows.

An affine plane \mathcal{P} in $AG(n, 2)$ is either a 2-dimensional linear subspace of $GF(2)^n$ or a coset of such subspace. Let

$$\mathcal{P} = \{\phi, \alpha + \phi, \beta + \phi, \alpha + \beta + \phi\} = \{\bar{0}, \alpha, \beta, \alpha + \beta\} + \phi$$

for some vectors $\phi, \alpha, \beta \in GF(2)^n$ such that

$$\alpha \neq \bar{0}, \bar{1}, \beta \neq \bar{0}, \bar{1}, \alpha + \beta \neq \bar{0}, \bar{1}. \quad (11)$$

Starting with \mathcal{P} , we construct seven more quadruples that are listed together with \mathcal{P} in Table 4.1.

Table 4.1

ϕ	$\alpha + \phi$	$\beta + \phi$	$\alpha + \beta + \phi$
ϕ	$\alpha + \phi + \bar{1}$	$\beta + \phi + \bar{1}$	$\alpha + \beta + \phi$
ϕ	$\alpha + \phi + \bar{1}$	$\beta + \phi$	$\alpha + \beta + \phi + \bar{1}$
ϕ	$\alpha + \phi$	$\beta + \phi + \bar{1}$	$\alpha + \beta + \phi + \bar{1}$
$\phi + \bar{1}$	$\alpha + \phi + \bar{1}$	$\beta + \phi + \bar{1}$	$\alpha + \beta + \phi + \bar{1}$
$\phi + \bar{1}$	$\alpha + \phi$	$\beta + \phi$	$\alpha + \beta + \phi + \bar{1}$
$\phi + \bar{1}$	$\alpha + \phi$	$\beta + \phi + \bar{1}$	$\alpha + \beta + \phi$
$\phi + \bar{1}$	$\alpha + \phi + \bar{1}$	$\beta + \phi$	$\alpha + \beta + \phi$

Under the assumptions (11), each of the eight quadruples in Table 4.1 consists of four distinct affine points, and since the sum of the four elements in each quadruple is zero, the eight quadruples constitute eight distinct affine planes. In addition, \mathcal{P} , as well as each of the remaining seven affine planes in Table 4.1, do not contain the affine line $\{\bar{0}, \bar{1}\}$ or any affine line $\{z, z + \bar{1}\}$ parallel to $\{\bar{0}, \bar{1}\}$. Thus, the incidence vectors of these eight affine planes are vectors of weight four in C_n being rows of matrix (7).

The eight quadruples in Table 4.1 are obtained by adding $\bar{1}$ to an even number (0, 2 or 4) elements of \mathcal{P} . This collection of eight quadruples is closed under these operations: if we start with any other of the eight rows of Table 4.1 instead of row one and repeat the procedure, we will end up with the same collection of eight quadruples. Consequently, if we repeat this construction by starting with an affine plane \mathcal{P}' that is not any of the eight quadruples in Table 4.1, we obtain a set of eight new quadruples disjoint from the set of those obtained from \mathcal{P} . Thus, the set of all

$$\frac{2^n(2^n - 1)(2^n - 2)}{4 \cdot 3 \cdot 2} - 2^{n-2}(2^{n-1} - 1) = \frac{2^n(2^{n-1} - 1)(2^{n-2} - 1)}{3}$$

affine planes that do not contain affine lines of the form $\{z, z + \bar{1}\}$, i.e., the affine planes whose incidence vectors are rows of matrix (7), is partitioned into $2^{n-3}(2^{n-1} - 1)(2^{n-2} - 1)/3$ disjoint 8-sets, each consisting of eight affine planes as in Table 4.1.

Table 4.2 lists eight quadruples obtained by adding $\bar{1}$ to an odd number (one or three) of points from \mathcal{P} . Alternatively, Table 4.2 is obtained by adding $\bar{1}$ to the entries in the first column of Table 4.1. The conditions (11) imply that each of the eight quadruples in Table 4.2 consists of four distinct affine points. The sum of the four vectors in every row of Table 4.2 is $\bar{1}$.

Table 4.2

$\phi + \bar{1}$	$\alpha + \phi$	$\beta + \phi$	$\alpha + \beta + \phi$
$\phi + \bar{1}$	$\alpha + \phi + \bar{1}$	$\beta + \phi + \bar{1}$	$\alpha + \beta + \phi$
$\phi + \bar{1}$	$\alpha + \phi + \bar{1}$	$\beta + \phi$	$\alpha + \beta + \phi + \bar{1}$
$\phi + \bar{1}$	$\alpha + \phi$	$\beta + \phi + \bar{1}$	$\alpha + \beta + \phi + \bar{1}$
ϕ	$\alpha + \phi + \bar{1}$	$\beta + \phi + \bar{1}$	$\alpha + \beta + \phi + \bar{1}$
ϕ	$\alpha + \phi$	$\beta + \phi$	$\alpha + \beta + \phi + \bar{1}$
ϕ	$\alpha + \phi$	$\beta + \phi + \bar{1}$	$\alpha + \beta + \phi$
ϕ	$\alpha + \phi + \bar{1}$	$\beta + \phi$	$\alpha + \beta + \phi$

We will show that the eight quadruples in Table 4.2 are supports of codewords of C_n that correspond to rows of matrix (8). It is readily seen that if a quadruple from Table 4.2 contains $\bar{0}$, it can be obtained from an affine plane containing $\bar{1}$, by replacing $\bar{1}$ with $\bar{0}$. Similarly, any quadruple from Table 4.2 that contains $\bar{1}$ is obtained from an affine plane containing $\bar{0}$, by replacing $\bar{0}$ with $\bar{1}$. Thus, any quadruple from Table 4.2 that contains either $\bar{0}$ or $\bar{1}$ is the support of a codeword from C_n of type (ii).

If a quadruple from Table 4.2 does not contain either $\bar{0}$ or $\bar{1}$, then adjoining $\bar{0}$ and $\bar{1}$ to it yields a set of six linearly dependent points of $AG(n, 2)$ that support a vector of weight six in the extended Hamming code H_n^* having its first two coordinates equal to 1. Thus, any quadruple from Table 4.2 that does not contain either $\bar{0}$ or $\bar{1}$ is the support of a codeword from C_n of type (iii).

Let A' be the matrix whose rows are the codewords from C_n having as supports the eight quadruples from Table 4.1, and let B' be the matrix whose rows are the codewords from C_n having as supports the eight quadruples from Table 4.2. It is easy to check that the eight quadruples listed in Table 4.2 cover the same set of 32 triples as the eight affine planes from Table 4.1. Thus, $\{A', B'\}$ is a matching pair.

The partition of the set of rows of matrix (7) into disjoint 8-sets of rows whose supports form a configuration as the one in Table 4.1, implies a partition of the set of rows of matrix (8) into disjoint 8-sets of rows whose supports form a configuration as the one in Table 4.2. Thus, the following is true.

Lemma 4.3 *The sets of rows of each of the matrices (7) and (8) can be partitioned into*

$$\frac{2^{n-3}(2^{n-1} - 1)(2^{n-2} - 1)}{3}$$

groups of eight rows each, so that every group of eight rows of matrix (7) forms a matching pair with exactly one group of eight rows of matrix (8).

Theorem 4.4 *The code C_n contains exactly*

$$2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}} \quad (12)$$

distinct Steiner quadruple systems $SQS(2^n)$.

Proof. By the arguments of the preceding paragraphs, all we have to do is find the total number of distinct matching pairs.

If (A', B') and (A'', B'') are two matching pairs such that $A' \cap A'' = \emptyset$, $B' \cap B'' = \emptyset$, then $(A' \cup A'', B' \cup B'')$ is also a matching pair. Thus, a number of (12) distinct matching pairs, and hence distinct $SQS(2^n)$'s, are obtained by using the partition described in Lemma 4.3.

To show that (12) is the actual total number of all distinct matching pairs, we will express this number as the number of solutions of a linear system of equations over the binary field $GF(2)$.

By Lemma 3.1, a triple of points (that is, a triple of the 2^n code coordinates), is covered either by one row of A_0 , or one row of the matrix (7) plus one row of the matrix (8). Note that each of the matrices (7) and (8) contains exactly

$$\frac{2^n(2^n - 1)(2^n - 2)}{4 \cdot 3 \cdot 2} - 2^{n-2}(2^{n-1} - 1) = \frac{2^n(2^{n-1} - 1)(2^{n-2} - 1)}{3}$$

rows.

The $2^{n-2}(2^{n-1})$ rows of A_0 cover $2^n(2^{n-1} - 1)$ triples of points. The number of the remaining triples that are covered by rows of matrix (7) and matrix 8 is

$$\binom{2^n}{3} - 2^n(2^{n-1} - 1) = \frac{2^{n+2}(2^{n-1} - 1)(2^{n-2} - 1)}{3}.$$

Let $M = (m_{ij})$ be the $\frac{2^{n+2}(2^{n-1}-1)(2^{n-2}-1)}{3}$ by $\frac{2^{n+1}(2^{n-1}-1)(2^{n-2}-1)}{3}$ $(0, 1)$ -matrix with rows indexed by the triples of points that are not covered by rows of A_0 , and columns indexed by the rows of matrices (7) and (8), where $m_{ij} = 1$ if the i th triple is covered by the j th row, and $m_{ij} = 0$ otherwise. It follows from Lemma 3.1 that every row of M contains exactly two entries equal to 1: one in a column of M indexed by a row of (7), and the second one in a column of M indexed by a row of (8).

Using the partition from Lemma 4.3, we can rearrange the rows and columns of M so that M becomes a block matrix with blocks of size 32 by 16, where the blocks along the main diagonal correspond to matching pairs (A', B') as those defined by Table 4.1 and Table 4.2, and all blocks off the main diagonal consist of zeros only. It follows that the rank of M is equal to the sum of the ranks of the blocks along the main diagonal. Every such block is the incidence matrix of 32 3-subsets of a set of eight affine points versus 16 quadruples as

those listed in Table 4.1 and Table 4.2, and its 2-rank is easily calculated to be 15. Thus, the 2-rank of M is equal to

$$\text{rank}_2(M) = 15 \cdot \frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3} = 5 \cdot 2^{n-3}(2^{n-1}-1)(2^{n-2}-1).$$

Let us consider the following homogeneous system of linear equations over $GF(2)$.

$$Mx' = 0, \quad (13)$$

where $x = (x_1, x_2, \dots)$ and the unknowns x_i take values in $\{0, 1\}$. Every nonzero solution of (13) is a $(0, 1)$ -vector of an even weight, say $2k$, and the support of x is the union of two disjoint subsets of size k that correspond to a matching pair (A', B') , $|A'| = |B'| = k$. The zero solution corresponds to the trivial matching pair $A' = B' = \emptyset$. Conversely, every matching pair corresponds to a solution of (13). Consequently, the total number of matching pairs is equal to the number of solutions of the system (13):

$$2^{\frac{2^{n+1}(2^{n-1}-1)(2^{n-2}-1)}{3} - \text{rank}_2(M)} = 2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}}.$$

This completes the proof. \square

The number (12) includes $SQS(2^n)$'s of 2-rank $2^n - n$, as well as $SQS(2^n)$'s of 2-rank $2^n - n - 1$ that are isomorphic to the classical system of the planes in $AG(n, 2)$. The total number of the latter is easily found by using Lemma 2.1 and Lemma 2.3:

$$\frac{|Aut(C_n)|}{|GA(n, 2) \cap Aut(C_n)|} = 2^{2^{n-1}-n}.$$

Thus we have the following.

Corollary 4.5 *The code C_n contains a total of*

$$2^{2^{n-1}-n} \quad (14)$$

$SQS(2^n)$'s of 2-rank $2^n - n - 1$ being isomorphic to the classical Steiner system of the planes in $AG(n, 2)$.

Corollary 4.6 *The code C_n contains a total of*

$$2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^{n-1}-n} \quad (15)$$

$SQS(2^n)$'s of 2-rank $2^n - n$.

Now it is easy to find the total number of *all* distinct $SQS(2^n)$'s on a given set of 2^n points of 2-rank $2^n - n$, as the product of the number (15) of such systems that are contained in the code C_n with the number $(2^n)!/|Aut(C_n)|$ of distinct codes that are equivalent to C_n .

Theorem 4.7 *The total number of distinct $SQS(2^n)$'s of 2-rank $2^n - n$ is*

$$\frac{(2^n)! \left(2^{\frac{2^{n-3}(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^{n-1}-n} \right)}{2^{2^{n-1}+n-1}(2^{n-1}-1)(2^{n-1}-2) \dots (2^{n-1}-2^{n-2})}. \quad (16)$$

5 A mass formula and bounds for $SQS(2^n)$'s of 2-rank $2^n - n$

If D is an $SQS(2^n)$ of 2-rank $2^n - n$ in the code C_n with generator matrix (1), then C_n is the linear span of the rows of the incidence matrix of D . Thus, every automorphism of D preserves C_n , and the total number of distinct $SQS(2^n)$'s of 2-rank $2^n - n$ in C_n that are isomorphic to D is equal to $|Aut(C_n)|/|Aut(D)|$. Assume that the total number of isomorphism classes of $SQS(2^n)$'s of 2-rank $2^n - n$ is s , and let D_1, \dots, D_s be representatives of these isomorphism classes. Then the formula (15) implies that

$$2^{\frac{2^n-3(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^n-1-n} = \sum_{i=1}^s \frac{|Aut(C_n)|}{|Aut(D_i)|}. \quad (17)$$

The "mass" formula (17) can be used for classifying all $SQS(2^n)$'s of 2-rank $2^n - n$ up to isomorphism: one has to find sufficiently many pairwise non-isomorphic designs D_1, D_2, \dots of the given rank so that equality holds in (17). We will apply this formula to classify all $SQS(16)$'s of 2-rank 12 in the next section.

Formula (17) can be used also for deriving lower and upper bounds on the number of isomorphism classes of $SQS(2^n)$'s of 2-rank $2^n - n$. If U (resp. u) is an upper (resp. lower) bound for the group orders $|Aut(D_i)|$, that is,

$$u \leq |Aut(D_i)| \leq U \text{ for all } 1 \leq i \leq s,$$

then (17) implies that

$$\frac{2^{\frac{2^n-3(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^n-1-n}}{|Aut(C_n)|} u \leq s \leq \frac{2^{\frac{2^n-3(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^n-1-n}}{|Aut(C_n)|} U.$$

In particular, the trivial lower bound $|Aut(D_i)| \geq 1$ implies the following.

Theorem 5.1 *The number of pairwise non-isomorphic Steiner quadruple systems $SQS(2^n)$ of 2-rank $2^n - n$ is greater or equal to*

$$\frac{2^{\frac{2^n-3(2^{n-1}-1)(2^{n-2}-1)}{3}} - 2^{2^n-1-n}}{2^{2^n-1+n-1}(2^{n-1}-1)(2^{n-1}-2)\dots(2^{n-1}-2^{n-2})}. \quad (18)$$

Corollary 5.2 *The number of non-isomorphic Steiner quadruple systems $SQS(2^n)$ of 2-rank $2^n - n$ grows exponentially with n .*

6 Classification of $SQS(16)$'s of 2-rank 12

There is only one (up to isomorphism) Steiner quadruple system on eight points: the classical system with blocks being the planes in $AG(3, 2)$ whose 2-rank is $2^3 - 3 - 1 = 4$. Thus, there are no $SQS(8)$'s of 2-rank 5, which is also confirmed by formulas (15) and (16).

According to formula (15), the code C_4 of an $SQS(2^4)$ of 2-rank 12 contains a total of

$$2^{14} - 2^4 = 16,368$$

$SQS(2^4)$'s of 2-rank 12, and by formula (14), C_4 contains $2^4 = 16$ "classical" $SQS(2^4)$'s of 2-rank 11. Note that the total number of all distinct $SQS(16)$'s of 2-rank 12 is 995,350,356,000 by formula (16).

It is relatively easy to generate the $SQS(2^4)$'s in C_4 by using the partition described in Lemma 4.3. For each $SQS(2^4)$ found in C_4 , we computed the binary code C' of length 140 and dimension 12 spanned by the point by block incidence matrix (C' is called a *point code* in [9]). According to the weight distribution of their point codes, the 16,368 $SQS(16)$'s in C_4 were partitioned into 15 classes.

Table 6.1 lists data for representatives of the 15 classes such as the order of the automorphism group $|Aut|$, orbit lengths of the automorphism group on the 16 points, the total number of codewords of the first three nonzero weights in C' , and the total number distinct designs in C_4 with the given weight distribution.

Table 6.1 $SQS(16)$'s of 2-rank 12

No.	$ Aut $	# Distinct in C_4	Orbits	Weights
1	21504	16	16	35(16), 48(7), 56(128)
2	3072	112	16	16(1), 35(16), 43(16)
3	3072	112	16	32(3), 35(16), 51(48)
4	1536	224	8,8	8(1), 35(24), 43(8)
5	1536	224	8,8	35(16), 40(3), 48(4)
6	768	448	4,12	24(1), 32(2), 35(20)
7	768	448	4,12	24(1), 35(16), 43(12)
8	768	448	16	32(2), 35(16), 40(4)
9	768	448	16	35(16), 40(4), 48(6)
10	256	1344	4,4,8	16(1), 35(20), 40(2)
11	256	1344	8,8	24(1), 35(16), 40(2)
12	256	1344	4,4,8	32(1), 35(16), 40(2)
13	128	2688	8,8	32(2), 35(16) 40(2)
14	96	3584	2,2,6,6	24(1), 32(1), 35(18)
15	96	3584	2,2,6,6	32(1), 35(16), 40(3)

The order of the automorphism group of C_4 is 344064 by Lemma 2.1. Since

$$2^{14} - 2^4 = 16368 = 344064 \left(\frac{1}{21504} + \frac{2}{3072} + \frac{2}{1536} + \frac{4}{768} + \frac{3}{256} + \frac{1}{128} + \frac{2}{96} \right),$$

it follows from the "mass" formula (17) that these 15 non-isomorphic $SQS(2^4)$'s represent all isomorphism classes. Thus, we have the following.

Theorem 6.2 *There are exactly 15 isomorphism classes of $SQS(16)$'s of 2-rank 12.*

Base blocks and generators of the automorphism group for these 15 $SQS(16)$'s are available from the author at

<http://www.math.mtu.edu/~tonchev/sqs16r12.html>.

References

- [1] E.F. Assmus, Jr., On 2-ranks of Steiner triple systems, *Electronic J. Combinatorics* **2** (1995) paper R9.
- [2] C. J. Colbourn and J.F. Dinitz, eds., "The CRC Handbook of Combinatorial Designs", CRC Press, Boca Raton, 1996.
- [3] Charles J. Colbourn and Alexander Rosa, "Triple systems", Oxford Science Publications, Oxford 1999.
- [4] J. Doyen, X. Hubaut, and M. Vandensavel, Ranks of incidence matrices of Steiner triple systems, *Math. Z.* **163** (1978), 251-259.
- [5] J.D. Key and F.E. Sullivan, Steiner systems from binary codes, *Ars Combinatoria* **52** (1999), 153-159.
- [6] V.S. Pless and W.C. Huffman, eds., "Handbook of Coding Theory", North Holland, Amsterdam 1998.
- [7] L. Teirlinck, On projective and affine hyperplanes, *J. Combin. Theory Ser. A* **28** (1980), 290-306.
- [8] V. D. Tonchev, A mass formula for Steiner triple systems $STS(2^n - 1)$ of 2-rank $2^n - n$, *J. Combin. Theory, Ser. A* **95** (2001), 197-208.
- [9] V. D. Tonchev and R. Weishaar, Steiner triple systems of order 15 and their codes, *J. Statistical Planning and Inference*, **58** (1997), 207-216.

On Hadamard Matrices of Order $2(p+1)$ with an Automorphism of Odd Prime Order p

Daniel B. Dalan*, Masaaki Harada† and Akihiro Muncinasa*

December 25, 2002

Abstract

In this paper, we investigate Hadamard matrices of order $2(p+1)$ with an automorphism of odd prime order p . In particular, the classification of such Hadamard matrices for the cases $p = 19$ and 23 is given. Self-dual codes related to such Hadamard matrices are also investigated.

1 Introduction

A Hadamard matrix H of order n is an $n \times n$ matrix whose entries are from $\{1, -1\}$ such that $HH^t = nI$ where H^t is the transpose of H and I is the identity matrix. It is known that the order n is necessarily 1, 2, or a multiple of 4. Two Hadamard matrices H and K are said to be equivalent if there exist $(1, -1, 0)$ -monomial matrices A, B with $K = AHB$. An automorphism of a Hadamard matrix H is an equivalence of H to itself. The set of all automorphisms of H forms a group under composition called the automorphism group of H denoted in this paper by $\text{Aut}(H)$.

All Hadamard matrices of orders up to 28 have been classified (cf. [3] and [13]). In this paper, we investigate Hadamard matrices of order $2(p+1)$ with an automorphism of odd prime order p ($p = 19, 23$).

We also investigate self-dual codes of length 40 over \mathbb{F}_5 generated by our Hadamard matrices of order 40, and self-dual codes of length 48 over \mathbb{F}_3 generated by our Hadamard matrices of order 48. We relate the binary extremal doubly-even self-dual $[40, 20, 8]$ codes obtained from our Hadamard designs to Yorgov's classification [16].

2 Hadamard $2-(2p+1, p, (p-1)/2)$ Designs with an Automorphism of Order p

Let $p > 3$ be an odd prime. If a Hadamard matrix H of order $2p+2$ has an automorphism of order p , then H is constructed from a symmetric $2-(2p+1, p, (p-1)/2)$ design with an automorphism of order p with one fixed point. This follows from a well-known connection between Hadamard matrices and symmetric designs, together with a bound on the number of fixed points [4, p. 82].

Let D be a symmetric $2-(2p+1, p, (p-1)/2)$ design with an automorphism of order p . Then, as in Tonchev [14, 15], D has an incidence matrix of the form

$$A = A(M, N, P, Q) = \begin{bmatrix} & & & & 1 \\ & M & & N & \vdots \\ & & & & 1 \\ & & & & 0 \\ & & P & & J-Q & \vdots \\ & & & & & 0 \\ 1 \cdots 1 & 0 \cdots 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

*Department of Mathematics, Kyushu University, Fukuoka 812-8581, Japan

†Department of Mathematical Sciences, Yamagata University, Yamagata 990-8560, Japan

where J is the all-one matrix of order p , M, N, P, Q are circulant matrices satisfying

$$MJ = NJ = PJ = QJ = \frac{p-1}{2}J. \quad (1)$$

For circulant matrices M, N, P, Q satisfying (1), the matrix A is an incidence matrix of a symmetric $2-(2p+1, p, (p-1)/2)$ design if and only if the following equalities hold:

$$MM^t + NN^t = \frac{p+1}{2}I + \frac{p-3}{2}J \quad (2)$$

$$PP^t + QQ^t = \frac{p+1}{2}I + \frac{p-3}{2}J \quad (3)$$

$$MM^t + PP^t = \frac{p+1}{2}I + \frac{p-3}{2}J \quad (4)$$

$$NN^t + QQ^t = \frac{p+1}{2}I + \frac{p-3}{2}J \quad (5)$$

$$MP^t = NQ^t. \quad (6)$$

The equalities (1) and (2) mean that the matrix $[M \ N]$ is an incidence matrix of a $2-(p, (p-1)/2, (p-3)/2)$ design. Touchev [14, 15] used this fact to classify all $2-(2p+1, p, (p-1)/2)$ designs with an automorphism of order p for $p = 13, 17$. In this paper, we carry out a similar classification for $p = 19, 23$. However, there is an important difference between his case and our case. If $p \equiv -1 \pmod{4}$, then $(p-3)/2$ is even, and there exists a $2-(p, (p-1)/2, (p-3)/4)$ design. Such a design can be constructed as the Paley difference set consisting of the quadratic residues modulo p . So, if $p \equiv -1 \pmod{4}$, then we have a special case which does not occur when $p \equiv 1 \pmod{4}$, namely, the case where one of M, N, P, Q is an incidence matrix of a $2-(p, (p-1)/2, (p-3)/4)$ design. It follows from the equalities (2)–(5) that, if one of the four matrices M, N, P, Q is an incidence matrix of a $2-(p, (p-1)/2, (p-3)/4)$ design, then so are the other three.

Let Z be the $p \times p$ circulant matrix with first row $(0, 1, 0, 0, \dots, 0)$. Then

$$A(M, N, P, Q) \cong A(MZ, NZ, P, Q) \quad (7)$$

$$\cong A(M, N, PZ, QZ) \quad (8)$$

$$\cong A(MZ, N, PZ, Q) \quad (9)$$

$$\cong A(M, NZ, P, QZ). \quad (10)$$

where $A \cong B$ means that the designs defined by A and B are isomorphic, or equivalently, there exist permutation matrices T_1, T_2 such that $T_1AT_2 = B$.

For convenience, we take $\mathbb{Z}/p\mathbb{Z}$ as the row and the column indices of a matrix of order p . Let α be a primitive root modulo p , and let Y be the matrix whose (i, j) entry is $\delta_{i\alpha, j}$. Then

$$Y^tZY = Z^\alpha \quad (11)$$

holds, so that Y^tMY is a circulant $(0, 1)$ -matrix whenever M is a circulant $(0, 1)$ -matrix. Clearly, we have

$$A(M, N, P, Q) \cong A(Y^tMY, Y^tNY, Y^tPY, Y^tQY). \quad (12)$$

Since α is a primitive root modulo p , we have, by putting $T = Y^{(p-1)/2}$,

$$T^tZT = Z^t. \quad (13)$$

In particular, from (12) we find

$$A(M, N, P, Q) \cong A(M^t, N^t, P^t, Q^t). \quad (14)$$

It is known that every Hadamard $2-(4t+3, 2t+1, t)$ design is extendable in exactly one way (up to isomorphism) to a Hadamard $3-(4t+4, 2t+2, t)$ design. Suppose that $A(M, N, P, Q)$ satisfies (1)–(6).

Define $A^* = A^*(M, N, P, Q)$ by

$$A^* = \begin{bmatrix} & & 1 & & & 0 \\ M & N & \vdots & J-M & J-N & \vdots \\ & & 1 & & & 0 \\ & & 0 & & & 1 \\ P & J-Q & \vdots & J-P & Q & \vdots \\ & & 0 & & & 1 \\ 1 \cdots 1 & 0 \cdots 0 & 0 & 0 \cdots 0 & 1 \cdots 1 & 1 \\ 1 \cdots 1 & 1 \cdots 1 & 1 & 0 \cdots 0 & 0 \cdots 0 & 0 \end{bmatrix}.$$

Then A^* is an incidence matrix of the Hadamard $3-(2(p+1), p+1, (p-1)/2)$ design extended from the 2-design with incidence matrix $A(M, N, P, Q)$. One checks easily that

$$A^*(M, N, P, Q) \cong A^*(P, Q, M, N). \quad (15)$$

Define $B = B(M, N, P, Q)$ and $H = H(M, N, P, Q)$ by

$$B = (B_{ij}) = \begin{bmatrix} 1 & 1 \cdots 1 & 1 \cdots 1 & 1 \\ 1 & & & 1 \\ \vdots & M & N & \vdots \\ 1 & & & 1 \\ 1 & & & 0 \\ \vdots & P & J-Q & \vdots \\ 1 & & & 0 \\ 1 & 1 \cdots 1 & 0 \cdots 0 & 0 \end{bmatrix},$$

$$H = (H_{ij}) = ((-1)^{B_{ij}}).$$

Then H is a Hadamard matrix of order $2(p+1)$. One checks easily that

$$H(M, N, P, Q) \cong H(P, Q, M, N). \quad (16)$$

Here “ \cong ” means the equivalence of Hadamard matrices.

For the remainder of this section, we assume $p = 19$ or 23 , and we shall deal with the special case where each of M, N, P, Q is an incidence matrix of a cyclic $2-(p, (p-1)/2, (p-3)/4)$ design. For $p = 19$ or 23 , it is known that the only cyclic $(p, (p-1)/2, (p-3)/4)$ difference set (up to equivalence) is the one constructed from the quadratic residues modulo p [5], so that we have

$$M, N, P, Q \in \{M_0 Z^i \mid 0 \leq i < p\} \cup \{M_0^t Z^i \mid 0 \leq i < p\}, \quad (17)$$

where M_0 is the circulant matrix in which the support of the first row consists of the nonzero quadratic residues modulo p . We will show in this special circumstance that, there are exactly three Hadamard $2-(2p+1, p, (p-1)/2)$ designs up to equivalence. By (7) and (14), we may assume without loss of generality that $M = M_0$. By (10), we can also retake N up to multiplication by Z , so we may assume either $N = M_0$, or $N = M_0^t$. By (8), we can also retake P up to multiplication by Z . Observe that Q is uniquely determined by M, N, P by (6). Therefore,

$$A(M, N, P, Q) \cong A(M_0, M_0, M_0, M_0) \quad \text{or,} \quad (18)$$

$$\cong A(M_0, M_0, M_0^t, M_0^t) \quad \text{or,} \quad (19)$$

$$\cong A(M_0, M_0^t, M_0, M_0^t) \quad \text{or,} \quad (20)$$

$$\cong A(M_0, M_0^t, M_0^t, Q), \quad (21)$$

where, in the last case,

$$Q = (M_0^t)^2 M_0^{-1}.$$

Note

$$\begin{aligned} M_0 J &= \frac{p-1}{2} J, \\ M_0 M_0^t &= \frac{p-3}{4} J + \frac{p+1}{4} I, \\ M_0 + M_0^t + I &= J. \end{aligned}$$

Eliminating M_0^t , we find

$$M_0^2 + M_0 = \frac{p+1}{4} (J - I).$$

Multiplying both sides by M_0^{-1} , we find

$$(J - I) M_0^{-1} = \frac{4}{p+1} (M_0 + I).$$

Now

$$\begin{aligned} Q &= (M_0^t)^2 M_0^{-1} \\ &= M_0^t (J - I - M_0) M_0^{-1} \\ &= M_0^t \left(\frac{4}{p+1} (M_0 + I) - I \right) \\ &= \frac{p-3}{p+1} J + I - \frac{p-3}{p+1} M_0^t \end{aligned}$$

is apparently not a $(0, 1)$ -matrix. Alternatively, one can argue as follows. The matrix $(M_0^t)^2 M_0^{-1}$ has an eigenvalue $\theta = \bar{\alpha}^2/\alpha$, where α is a root of the quadratic equation $\alpha^2 + \alpha + (p+1)/4 = 0$. One can check easily that θ is not an algebraic integer, hence not an eigenvalue of a $(0, 1)$ -matrix. Thus Q is not a $(0, 1)$ -matrix. Therefore, (21) is impossible.

The three 2-designs we obtain from (18)–(20) are denoted by $S_{2p+1,1}$, $S_{2p+1,2}$ and $S_{2p+1,3}$, respectively. We denote by $E(D)$, $H(D)$ the Hadamard 3-design, the Hadamard matrix, respectively, obtained from the Hadamard 2-design D . For $p = 19$ and $p = 23$, we have verified by computer that the three 2-designs $S_{2p+1,i}$ ($i = 1, 2, 3$) are pairwise non-isomorphic, that the three 3-designs $E(S_{2p+1,i})$ ($i = 1, 2, 3$) are pairwise non-isomorphic, and that the three Hadamard matrices $H(S_{2p+1,i})$ ($i = 1, 2, 3$) are pairwise inequivalent. The orders of the automorphism groups of the Hadamard designs and matrices are listed in Table 1. In the next sections, we consider the generic case where none of M, N, P, Q is an incidence matrix of a $2-(p, (p-1)/2, (p-3)/4)$ design for $p = 19$ and $p = 23$.

Table 1: The orders of the automorphism groups for the special cases

	$ \text{Aut}(S_{2p+1,i}) $	$ \text{Aut}(E(S_{2p+1,i})) $	$ \text{Aut}(H(S_{2p+1,i})) $
$p = 19$	171	342	27360
$p = 23$	253	506	48576

We remark that the above argument can be generalized to an arbitrary prime p as long as a cyclic $(p, (p-1)/2, (p-3)/4)$ difference set is unique up to equivalence. Under this condition, we see that there are at most three Hadamard $2-(2p+1, p, (p-1)/2)$ designs up to equivalence, with the property that each of the matrices M, N, P, Q is an incidence matrix of a cyclic $2-(p, (p-1)/2, (p-3)/4)$ design.

3 The Case $p = 19$

In this section, we give the classification of Hadamard matrices of order 40 with an automorphism of order 19. If p is an odd prime dividing the order of the automorphism group of a Hadamard matrix of

order n , then either p divides n or $n - 1$, or $p \leq n/2 - 1$ [14]. Hence the largest prime which can divide the order of the automorphism group of a Hadamard matrix of order 40 is 19.

As the first step, we classify symmetric 2-(39, 19, 9) designs with an automorphism of order 19. Using this classification, Hadamard 3-(40, 20, 9) designs with an automorphism of order 19 and Hadamard matrices of order 40 with an automorphism of order 19 are classified.

In order to classify such 2-designs, we need all circulant matrices M, N, P and Q satisfying the conditions (1)–(6). First we tabulate all solutions to the system of equations:

$$MM^t + NN^t = \frac{p+1}{2}I + \frac{p-3}{2}J \quad (22)$$

$$MJ = NJ = \frac{p-1}{2}J \quad (23)$$

under the additional condition

$$MM^t \neq \frac{p+1}{4}I + \frac{p-3}{4}J. \quad (24)$$

In order to give the list of solutions in a compact manner, we identify a circulant matrix $\sum_{i=0}^{p-1} a_i Z^i$ ($a_i = 0$ or 1) with the set $\{i \in \mathbb{Z}/p\mathbb{Z} \mid a_i = 1\}$. If $M, N \subset \mathbb{Z}/p\mathbb{Z}$ are subsets whose corresponding circulant matrices give a solution to (22)–(23), then so is the pair $aM + b.aN + b$, where $a, b \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$. In other words, the set of solutions to (22)–(23) is invariant under the affine transformation $x \mapsto ax + b$ of $\mathbb{Z}/p\mathbb{Z}$. We thus list the solutions up to affine transformation only. Under the condition (24), there are exactly 15 solutions $\{M, N\}$ to (22)–(23) up to affine transformation, given below.

$$\begin{aligned} & \{M_1, M_2\}, \{M_1, M_3\}, \{M_1, M_3^t\}, \{M_4, M_5\}, \{M_4, M_5^t\}, \\ & \{M_4, M_6\}, \{M_4, M_6^t\}, \{M_7, M_8\}, \{M_7, M_8^t\}, \{M_9, M_{10}\}, \\ & \{M_9, M_{10}^t\}, \{M_{11}, M_{12}\}, \{M_{11}, M_{12}^t\}, \{M_{13}, M_{14}\}, \{M_{13}, M_{14}^t\} \end{aligned}$$

where M_i ($i = 1, \dots, 14$) are listed in Table 2. We note the omission of $\{M_1, M_2^t\}$ due to the property $M_2 = M_2^t$.

Table 2: M_1, M_2, \dots, M_{14} ($p = 19$)

i	M_i	i	M_i
1	{0, 1, 2, 5, 6, 8, 11, 13, 15}	8	{0, 1, 2, 4, 7, 11, 13, 15, 16}
2	{0, 3, 7, 8, 9, 10, 11, 12, 16}	9	{0, 1, 2, 3, 4, 6, 8, 12, 15}
3	{1, 8, 9, 11, 12, 15, 16, 17, 18}	10	{0, 1, 2, 5, 6, 9, 11, 12, 14}
4	{0, 1, 2, 3, 4, 7, 12, 14, 15}	11	{0, 1, 2, 3, 4, 6, 10, 14, 15}
5	{0, 1, 2, 4, 6, 7, 10, 12, 16}	12	{0, 1, 2, 4, 8, 11, 13, 14, 16}
6	{0, 1, 2, 4, 6, 10, 13, 15, 16}	13	{0, 1, 2, 3, 4, 6, 8, 11, 15}
7	{0, 1, 2, 3, 4, 6, 9, 13, 14}	14	{0, 1, 2, 5, 7, 10, 11, 13, 14}

If $\{M, N\}$ is a solution to (22)–(23), then

$$\begin{aligned} (M, N, P, Q) &= (M, N, N^t, M^t), (M, N^t, N, M^t), \\ & (N, M, M^t, N^t), (N, M^t, M, N^t) \end{aligned}$$

are also solutions to (1)–(6). If D is the design with incidence matrix $A(M, N, N^t, M^t)$, then we denote by D^t, D^t the designs with incidence matrices $A(M, N^t, N, M^t)$, $A(N, M, M^t, N^t)$, respectively. The notation conforms with the equivalence

$$A(M, N^t, N, M^t) \cong A(M^t, N, N^t, M) = A(M, N, N^t, M^t)$$

which implies that D^t is isomorphic to the dual design of D . We note that D^t has incidence matrix $A(N, M^t, M, N^t)$.

For each $i = 1, 2, \dots, 8$, we define $D_{39,i}$ to be the design with incidence matrix $A(M, N, N^t, M^t)$, where (M, N) is given in Table 3. Then we also have designs $D_{39,i}^t, D_{39,i}'$ and $D_{39,i}^{t'}$. Altogether we have

32 designs. However, since $M_2 = M'_2$, we see $D_{39,1} \cong D_{39,1}^t$ and $D'_{39,1} \cong D_{39,1}^t$. Our computer search revealed that the 30 designs $D_{39,1}, D'_{39,1}, D_{39,i}, D'_{39,i}, D_{39,i}^t, D'_{39,i}^t$ ($i = 2, \dots, 8$) form a complete set of representatives for isomorphism classes of designs obtained by solutions to (1)–(6), under the additional condition (24). Moreover, none of these 30 designs is isomorphic to $S_{39,i}$ ($i = 1, 2, 3$), since their automorphism groups are different (see Table 4).

Table 3: $D_{39,1}, D_{39,2}, \dots, D_{39,8}$

Designs	(M, N)
$D_{39,1}$	(M_1, M_2)
$D_{39,2}$	(M_1, M_3)
$D_{39,3}$	(M_4, M_5)
$D_{39,4}$	(M_4, M_6)
$D_{39,5}$	(M_7, M_8)
$D_{39,6}$	(M_9, M_{10})
$D_{39,7}$	(M_{11}, M_{12})
$D_{39,8}$	(M_{13}, M_{14})

Table 4: $|\text{Aut}(D_{39,i})|$ and $|\text{Aut}(D'_{39,i})|$

i	$ \text{Aut}(D_{39,i}) $	$ \text{Aut}(D'_{39,i}) $
1, 2, 5, 6, 7, 8	19	19
3, 4	57	57

Now let $H(D)$ be the Hadamard matrix defined by a design D described above. Then (16) implies $H(D) \cong H(D')$. We have verified that $H(D_{39,1}), H(D_{39,i})$ ($2 \leq i \leq 8$), $H(D_{39,i}^t)$ ($2 \leq i \leq 8$) and $H(S_{39,i})$ ($i = 1, 2, 3$) are inequivalent.

Similarly, let $E(D)$ be the Hadamard 3-(40, 20, 9) design defined by a design D described above. Then (15) implies $E(D) \cong E(D')$. We have verified that $E(D_{39,1}), E(D_{39,i})$ ($2 \leq i \leq 8$), $E(D_{39,i}^t)$ ($2 \leq i \leq 8$) and $E(S_{39,i})$ ($i = 1, 2, 3$) are non-isomorphic. In other words, there is a one-to-one correspondence between isomorphism classes of 3-designs and equivalence classes of Hadamard matrices.

Theorem 1. *There are exactly 33 inequivalent 2-(39, 19, 9) designs with an automorphism of order 19. There are exactly 18 inequivalent Hadamard matrices of order 40 with an automorphism of order 19.*

The relationship among the orders of the automorphism groups of the Hadamard 2-designs D , the Hadamard 3-designs $E(D)$ and Hadamard matrices $H(D)$ is listed in Table 5.

Table 5: The orders of the automorphism groups ($p = 19$)

$ \text{Aut}(D) $	$ \text{Aut}(E(D)) $	$ \text{Aut}(H(D)) $
19	19	76
57	57	228
171	342	27360

It is known [9] that the code $C_5(H)$ over \mathbb{F}_5 generated by the rows of a Hadamard matrix H of order 40 is self-dual. We have computed the minimum weights of the 18 codes from the above 18 inequivalent Hadamard matrices of order 40 with an automorphism of order 19, and only $C_5(H(S_{39,2}))$ has minimum weight 13 and the others have minimum weights less than 13. Note that the largest minimum weight among known [40, 20] codes is 13 and Q'_{40} constructed in [9, p. 186] is the only known [40, 20, 13] code (cf. [2]). The code Q'_{40} has generator matrix $[I, B_{20}]$ where B_{20} is the 20×20 conference matrix of

the Paley type. An argument similar to [12, Theorem 4.2] shows that Q'_{40} is generated by the following Hadamard matrix:

$$\begin{bmatrix} I + B_{20} & I + B_{20} \\ I - B_{20} & -I + B_{20} \end{bmatrix}$$

which is easily seen to be equivalent to the Hadamard matrix $H(S_{39,2})$ (cf. Section 2). Hence $C_5(H(S_{39,2}))$ is equivalent to Q'_{40} .

Let A be an incidence matrix of a Hadamard 2-(39, 19, 9) design D and let $C(D)$ be the binary code with generator matrix

$$\begin{bmatrix} & 1 \\ A & \vdots \\ & 1 \end{bmatrix}.$$

By [6, Theorem 17.3.1], $C(D)$ is self-dual. In addition, $C(D)$ is a doubly-even code. Since $C(D)$ contains the all-one's vector, $C(D)$ is equivalent to the binary code generated by the columns of the incidence matrix of the Hadamard 3-design $E(D')$. Let D_1 and D_2 be Hadamard 2-(39, 19, 9) designs. If Hadamard 3-designs $E(D'_1)$ and $E(D'_2)$ are isomorphic then $C(D_1)$ and $C(D_2)$ are equivalent.

Here we investigate the 18 codes corresponding to the 18 equivalence classes of Hadamard 3-designs. We have verified that the two codes $C(S_{39,1})$ and $C(S_{39,2})$ have minimum weight 4 and the other 16 codes are extremal, that is, their minimum weights are 8. Yorgov [16] showed that there are exactly three inequivalent extremal doubly-even self-dual [40, 20, 8] codes with an automorphism of order 19. The three codes B_1 , B_2 and B_3 are distinguished by the orders of the automorphism groups, namely, 38, 114 and 6840, respectively. The relation between the three codes B_1 , B_2 , B_3 and our 16 extremal codes is listed in Table 6.

Table 6: Extremal doubly-even self-dual codes of length 40

Yorgov's codes	Our extremal codes
B_1	$C(D_{39,1}), C(D_{39,2}), C(D_{39,6}), C(D_{39,7})$ $C(D_{39,8}), C(D_{39,2}^t), C(D_{39,5}^t), C(D_{39,6}^t)$ $C(D_{39,7}^t), C(D_{39,8}^t)$
B_2	$C(D_{39,3}), C(D_{39,4}), C(D_{39,5}), C(D_{39,4}^t)$
B_3	$C(D_{39,3}^t), C(S_{39,3})$

4 The Case $p = 23$

As done in the previous section, in this section, we give the following classification:

Theorem 2. *There are exactly 109 non-isomorphic Hadamard 2-(47, 23, 11) designs with an automorphism of order 23. There are exactly 56 inequivalent Hadamard matrices of order 48 with an automorphism of order 23.*

The approach used in the classification is similar to that given in the previous section, so in this section, only results are given. When $p = 23$, under the condition (24), there are exactly 53 solutions $\{M, N\}$ to (22)–(23) up to affine transformation, given below,

$$\begin{aligned} & \{M_1, M_2\}, \{M_1, M_2^t\}, \{M_1, M_3\}, \{M_1, M_3^t\}, \{M_4, M_5\}, \{M_4, M_5^t\}, \\ & \{M_4, M_6\}, \{M_4, M_6^t\}, \{M_7, M_8\}, \{M_7, M_8^t\}, \{M_7, M_9\}, \{M_7, M_9^t\}, \\ & \{M_{10}, M_{11}\}, \{M_{2i}, M_{2i+1}\}, \{M_{2i}, M_{2i+1}^t\} \quad (i = 6, \dots, 25) \end{aligned}$$

where M_i ($i = 1, \dots, 51$) are listed in Table 7. We note the omission of $\{M_{10}, M_{11}^t\}$ due to the property $M_{11} = M_{11}^t$.

For each $i = 1, 2, \dots, 27$, we define $D_{47,i}$ to be the design with incidence matrix $A(M, N, N^t, M')$, where (M, N) is given in Table 8. The designs $D_{47,i}^t$, $D'_{47,i}$ and $D'^t_{47,i}$ are also defined. Among the

Table 7: M_1, M_2, \dots, M_{51} ($p = 23$)

i	M_i	i	M_i
1	{0, 1, 2, 4, 5, 10, 11, 13, 18, 19, 21}	27	{0, 1, 2, 4, 5, 7, 9, 11, 12, 15, 18}
2	{0, 1, 2, 3, 4, 7, 8, 11, 13, 15, 20}	28	{0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 17}
3	{0, 2, 3, 4, 5, 7, 10, 11, 14, 15, 21}	29	{0, 1, 2, 4, 7, 9, 13, 14, 16, 17, 19}
4	{0, 1, 2, 4, 6, 7, 11, 13, 15, 16, 19}	30	{0, 1, 2, 3, 4, 6, 8, 11, 14, 18, 20}
5	{0, 1, 2, 3, 4, 7, 8, 15, 17, 18, 20}	31	{0, 1, 2, 4, 10, 11, 12, 15, 16, 17, 20}
6	{1, 6, 8, 9, 11, 12, 15, 16, 17, 18, 19}	32	{0, 1, 2, 3, 4, 5, 7, 11, 12, 17, 19}
7	{0, 1, 2, 3, 5, 10, 11, 13, 16, 19, 20}	33	{0, 1, 2, 4, 5, 9, 11, 14, 15, 17, 20}
8	{0, 1, 2, 3, 4, 7, 8, 10, 12, 14, 19}	34	{0, 1, 2, 3, 4, 6, 7, 10, 11, 15, 17}
9	{0, 2, 3, 9, 10, 14, 16, 18, 20, 21, 22}	35	{0, 1, 2, 4, 8, 11, 13, 14, 16, 18, 19}
10	{0, 1, 2, 3, 5, 7, 12, 13, 16, 19, 20}	36	{0, 1, 2, 3, 4, 6, 7, 11, 16, 17, 19}
11	{0, 3, 5, 9, 10, 11, 12, 13, 14, 18, 20}	37	{0, 1, 2, 4, 6, 9, 10, 12, 13, 18, 20}
12	{0, 1, 2, 3, 4, 5, 7, 9, 14, 15, 19}	38	{0, 1, 2, 3, 4, 6, 8, 11, 12, 18, 20}
13	{0, 1, 2, 4, 7, 8, 11, 14, 16, 17, 19}	39	{0, 1, 2, 4, 7, 10, 11, 12, 14, 19, 20}
14	{0, 1, 2, 3, 4, 6, 8, 9, 12, 13, 16}	40	{0, 1, 2, 3, 5, 6, 7, 10, 14, 16, 17}
15	{0, 1, 2, 4, 6, 10, 11, 13, 16, 18, 19}	41	{0, 1, 2, 4, 6, 8, 9, 14, 17, 19, 20}
16	{0, 1, 2, 3, 4, 5, 8, 10, 13, 17, 20}	42	{0, 1, 2, 3, 4, 5, 8, 9, 13, 15, 19}
17	{0, 1, 2, 4, 6, 10, 11, 12, 15, 16, 18}	43	{0, 1, 2, 4, 9, 11, 12, 14, 17, 18, 20}
18	{0, 1, 2, 3, 4, 6, 8, 11, 12, 15, 18}	44	{0, 1, 2, 3, 4, 6, 9, 10, 11, 14, 16}
19	{0, 1, 2, 3, 5, 8, 9, 10, 13, 15, 19}	45	{0, 1, 3, 4, 6, 7, 10, 12, 14, 18, 19}
20	{0, 1, 2, 3, 5, 6, 8, 12, 14, 16, 19}	46	{0, 1, 2, 3, 4, 5, 8, 10, 15, 18, 19}
21	{0, 1, 2, 3, 5, 11, 12, 15, 18, 19, 20}	47	{0, 1, 3, 4, 6, 7, 11, 13, 15, 17, 18}
22	{0, 1, 2, 3, 4, 7, 8, 11, 13, 16, 17}	48	{0, 1, 2, 3, 4, 6, 7, 12, 14, 17, 21}
23	{0, 1, 2, 3, 5, 8, 13, 15, 17, 19, 20}	49	{0, 1, 2, 5, 6, 8, 9, 13, 15, 17, 18}
24	{0, 1, 2, 3, 4, 5, 7, 11, 13, 16, 20}	50	{0, 1, 2, 3, 4, 5, 8, 11, 14, 18, 19}
25	{0, 1, 2, 3, 6, 8, 11, 12, 16, 17, 19}	51	{0, 1, 2, 4, 6, 8, 13, 15, 16, 18, 19}
26	{0, 1, 2, 3, 4, 6, 8, 11, 12, 16, 17}		

Table 8: $D_{47,1}, D_{47,2}, \dots, D_{47,27}$

Designs	(M, N)
$D_{47,1}$	(M_1, M_2)
$D_{47,2}$	(M_1, M_3)
$D_{47,3}$	(M_4, M_5)
$D_{47,4}$	(M_4, M_6)
$D_{47,5}$	(M_7, M_8)
$D_{47,6}$	(M_7, M_9)
$D_{47,i}$ ($i = 7, \dots, 27$)	(M_{2i-4}, M_{2i-3})

108 designs, we see $D_{47,7} \cong D'_{47,7}$ and $D'_{47,7} \cong D''_{47,7}$ since $M_{11} = M''_{11}$. Our computer search revealed that the 106 designs $D_{47,7}, D'_{47,7}, D_{47,i}, D'_{47,i}, D''_{47,i}$ and $D'''_{47,i}$ ($i = 1, \dots, 6, 8, \dots, 27$) form a complete set of representatives for isomorphism classes of designs obtained by solutions to (1)-(6), under the additional condition (24). Moreover, none of these 106 designs is isomorphic to $S_{47,i}$ ($i = 1, 2, 3$), since their automorphism groups are different (see Table 9).

Table 9: $|\text{Aut}(D_{47,i})|$ and $|\text{Aut}(D'_{47,i})|$

i	$ \text{Aut}(D_{47,i}) $	$ \text{Aut}(D'_{47,i}) $
7	1081	1081
$1, \dots, 6, 8, \dots, 27$	23	23

We have verified that the Hadamard matrices $H(D_{47,7}), H(D_{47,i})$ ($i = 1, \dots, 6, 8, \dots, 27$), $H(D'_{47,i})$ ($i = 1, \dots, 6, 8, \dots, 27$) and $H(S_{47,i})$ ($i = 1, 2, 3$) are inequivalent. We remark that $H(D_{47,7})$ is equivalent to the Hadamard matrix of the Paley type, since $H(D_{47,7})$ is the only Hadamard matrix with an automorphism of order 47 among those we classified. As for Hadamard 3-designs, we have verified that $E(D_{47,7}), E(D_{47,i})$ ($i = 1, \dots, 6, 8, \dots, 27$), $E(D'_{47,i})$ ($i = 1, \dots, 6, 8, \dots, 27$) and $E(S_{47,i})$ ($i = 1, 2, 3$) are inequivalent. In other words, there is a one-to-one correspondence between isomorphism classes of 3-designs and equivalence classes of Hadamard matrices. Therefore the number of designs and Hadamard matrices are as claimed in Theorem 2. The relationship among the orders of the automorphism groups of the Hadamard 2-designs D , the Hadamard 3-designs $E(D)$ and Hadamard matrices $H(D)$ is listed in Table 10.

Table 10: The orders of the automorphism groups ($p = 23$)

$ \text{Aut}(D) $	$ \text{Aut}(E(D)) $	$ \text{Aut}(H(D)) $
23	23	92
1081	1081	103776
253	506	48576

The ternary code $C_3(H)$ generated by the rows of a Hadamard matrix H of order 48 is self-dual (cf. [11]). We have verified that, among the 56 codes obtained from the Hadamard matrices we classified, only $C_3(H(D_{47,7}))$ and $C_3(H(S_{47,2}))$ are extremal, that is, their minimum weights are 15. On the other hand, only two inequivalent extremal self-dual codes of length 48 are currently known, namely, the extended quadratic residue code Q_{48} and the Pless symmetry code P_{48} . Note that the two codes are generated by Hadamard matrices of order 48 [11]. As mentioned above, $H(D_{47,7})$ is equivalent to the Hadamard matrix of the Paley type, so $C_3(H(D_{47,7}))$ is equivalent to Q_{48} . In [12, Theorem 4.2], a Hadamard matrix H_{48} of order 48 generating the code P_{48} is given. As in the case of the code Q'_{40} discussed at the end of Section 3, it can be readily seen that the Hadamard matrix H_{48} is equivalent to the Hadamard matrix $H(S_{47,2})$. Hence $C_3(H(S_{47,2}))$ is equivalent to P_{48} .

Table 11: Doubly-even codes of length 48

$\dim(C)$	$d(C)$	Codes C
24	12	$C(D_{47,7}), C(D_{47,9}), C(D_{47,21}), C(D_{47,23})$ $C(D_{47,24}), C(D_{47,27}), C(D'_{47,2}), C(D'_{47,4})$ $C(D'_{47,9}), C(D'_{47,10}), C(D'_{47,14}), C(D'_{47,16})$ $C(D'_{47,18}), C(D'_{47,19}), C(D'_{47,23}), C(D'_{47,27})$
13	16	$C(S_{47,1})$
24	4	$C(S_{47,2})$
24	8	the other 38 codes

By an argument similar to the end part of the previous section, we now consider binary codes $C(D)$ obtained from incidence matrices of the above symmetric 2-(47, 23, 11) designs D with an automorphism of order 23. Note that the binary codes $C(D)$ are doubly-even self-orthogonal codes, but these are not necessarily self-dual. Recall that the codes $C(D_1)$ and $C(D_2)$ from 2-designs D_1 and D_2 are equivalent if the 3-designs $E(D_1^t)$ and $E(D_2^t)$ are isomorphic. Hence we only consider the 56 codes corresponding to the 56 equivalence classes of Hadamard 3-designs. The dimensions $\dim(C)$ and the minimum weights $d(C)$ of the codes are listed in Table 11.

It is known [7] that any extremal doubly-even self-dual [48, 24, 12] code with an automorphism of order 23 is equivalent to the extended quadratic residue code QR_{48} of length 48. Hence the extremal doubly-even self-dual codes in the table must be equivalent to QR_{48} . $H(S_{47,1})$ is a [48, 13, 16] code with weight enumerator $1 + 759y^{16} + 6672y^{24} + 759y^{32} + y^{48}$. Note that the largest minimum weight among known [48, 13] codes is 16 [2]. The binary code generated by the binary Paley type normalized Hadamard matrix of order 24, that is, $(H + J)/2$ where H is the Paley type normalized Hadamard matrix, is equivalent to the binary Golay [24, 12, 8] code G_{24} [1, Table 7.1]. From the form of $H(S_{47,1})$ or $S_{47,1}$, the code $C(S_{47,1})$ is equivalent to the code with generator matrix

$$\begin{bmatrix} M & M \\ 1 \cdots 1 & 0 \cdots 0 \end{bmatrix}$$

where M is a generator matrix of G_{24} .

Acknowledgment. The authors would like to thank Vladimir Tonchev for his useful comments.

References

- [1] E.F. Assmus, Jr. and J.D. Key, "Designs and Their Codes," Cambridge Univ. Press, Cambridge, 1992.
- [2] A.E. Brouwer, "Bounds on the size of linear codes," in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman (Eds.), Elsevier, Amsterdam, 1998, 295-461. Also published electronically at <http://www.win.tue.nl/~aeb/voorlincod.html>.
- [3] R. Craigen, "Hadamard matrices and designs," in *The CRC Handbook of Combinatorial Designs*, C.J. Colbourn and J.H. Dinitz (Eds.), CRC Press, Boca Raton 1996, 370-377.
- [4] P. Dembowski, "Finite Geometries," Springer-Verlag, Berlin-Heidelberg-New York, 1968.
- [5] M. Hall, Jr., A survey of difference sets, *Proc. Amer. Math. Soc.* **7** (1956) 975-986.
- [6] M. Hall, Jr., "Combinatorial Theory (2nd ed.)," Wiley, New York, 1986.
- [7] W.C. Huffman, Automorphisms of codes with applications to extremal doubly-even codes of length 48, *IEEE Trans. Inform. Theory* **28** (1982) 511-521.
- [8] C. Lam, S. Lam, and V.D. Tonchev, Bounds on the number of affine, symmetric, and Hadamard designs and matrices. *J. Combin. Theory Ser. A* **92** (2000) 186-196.
- [9] J.S. Leon, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(5)$, *J. Combin. Theory Ser. A* **32** (1982) 178-194.
- [10] C. Lin, W.D. Wallis and Z. Lie, Equivalence classes of Hadamard matrices of order 32, *Congr. Numer.* **95** (1993) 179-182.
- [11] C.L. Mallows, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$, *SIAM. J. Appl. Math.* **31** (1976), 649-666.
- [12] V. Pless, Symmetry codes over $GF(3)$ and new five-designs, *J. Combin. Theory Ser. A* **12** (1972) 119-142.

- [13] N.J.A. Sloane, A library of Hadamard matrices, published electronically at <http://www.research.att.com/~njas/hadamard>.
- [14] V.D. Tonchev, Hadamard matrices of order 28 with automorphisms of order 13, *J. Combin. Theory Ser. A* **35** (1983) 43-57.
- [15] V.D. Tonchev, Hadamard matrices of order 36 with automorphisms of order 17, *Nagoya Math. J.* **104** (1986) 163-174.
- [16] V.Y. Yorgov, Binary self-dual codes with automorphisms of odd order, (in Russian), *Probl. Pereda. Inform.* **19** (1983), 11-24. English translation in *Probl. Inform. Transm.* **19** (1983), 260-270.

GEOMETRIC ASPECTS OF LARGE DEVIATIONS FOR RANDOM WALKS ON A CRYSTAL LATTICE

MOTOKO KOTANI

1. THE GROMOV-HAUSDORFF LIMITS OF CRYSTAL LATTICES

The purpose of this talk is to discuss relations among certain convex polyhedra appearing in various situations; Gromov-Hausdorff limits of crystal lattices, homological directions of infinite paths in finite graphs and the large deviation property (LDP) of random walks on crystal lattices.

Consider the square lattice \mathbb{Z}^2 as a metric space with the graph-distance d , with $d(x, y)$ being the length a shortest path joining the vertices x, y . Now we change the scaling. Namely, given a positive constant ϵ , we consider the metric space $(\mathbb{Z}^2, \epsilon d)$ homothetic to (\mathbb{Z}^2, d) . By letting ϵ tend to zero, we find $\lim_{\epsilon \downarrow 0} (\mathbb{Z}^2, \epsilon d)$ to be the euclidean 2-space \mathbb{R}^2 with the Manhattan distance d_1 ,

$$d_1((x_1, y_1), (x_2, y_2)) = |x_1 - x_2| + |y_1 - y_2|.$$

What will happen with a more general infinite graph with periodicity? The graph we consider is a *crystal lattices*, which is defined to be an abelian covering graph of a finite graph. The square lattice, the triangular lattice and the hexagonal lattice are the typical examples.

Theorem 1. *Let (X, d) be a crystal lattice with the graph-distance.*

- (1) *(a special case of Gromov's result [2]) There exists a normed linear space $(L, \|\cdot\|)$ of finite dimension such that*

$$\lim_{\epsilon \downarrow 0} (X, \epsilon d) = (L, d_1),$$

where $d_1(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|$.

- (2) *The unit ball $\overline{\mathcal{D}} = \{\mathbf{x} \in L \mid \|\mathbf{x}\| \leq 1\}$ is a polyhedron. Thus the norm $\|\cdot\|$ is not Euclidean.*

As a corollary, we establish a precise asymptotic for the number of vertices in a crystal lattice.

¹collaboration with T. Sunada

Corollary 2.

$$\#\{x \in X \mid d(x_0, x) \leq n\} \sim (\#X_0) \text{vol}(\mathcal{D})n^k \quad (n \rightarrow \infty),$$

where $\text{vol}(\mathcal{D})$ is the volume of \mathcal{D} with respect to the Lebesgue measure on $\Gamma \otimes \mathbb{R}$ such that $\text{vol}(\Gamma \otimes \mathbb{R}/\Gamma \otimes \mathbb{Z}) = 1$.

Example 1. For the hexagonal lattice, $L = \mathbb{R}^2$ and $\overline{\mathcal{D}}$ is the hexagon (including the interior) in \mathbb{R}^2 .

We shall see that the convex polyhedron we captured in Theorem 1 is somehow related with a long time asymptotic of a random walk on a crystal lattice.

2. HOMOLOGICAL DRIFTING OF RANDOM WALKS ON FINITE GRAPHS

Before going further, let us give a simple observation on a random walk on finite graphs. Let X_0 be a finite connected graph, possibly with multiple edges and loop edges. We denote the set of all oriented edges in X_0 by E_0 . An oriented edge is an edge with the origin and terminus assigned, which are denoted by $o(e)$ and $t(e)$, respectively, and the reverse edge by \bar{e} . A decomposition $E_0 = E_0^+ \sqcup E_0^-$ with $E_0^- = \{\bar{e} \mid e \in E_0^+\}$ is called an orientation of X_0 .

We shall consider a random walk on X_0 given by a *transition probability* p , i.e. a positive valued function $p : E_0 \rightarrow \mathbb{R}$ satisfying

$$\sum_{e \in E_{0,x}} p(e) = 1 \quad (x \in X_0),$$

where $E_{0,x} = \{e \in E_0 \mid o(e) = x\}$. Note that we don't assume symmetry for p .

An infinite path c in X_0 is a collection of edges $c = (e_1, e_2, \dots)$ with $t(e_i) = o(e_{i+1})$ for $i = 1, 2, \dots$.

Theorem 3. (1) *There exists a 1-chain $\gamma_p \in C_1(X_0, \mathbb{R})$ such that*

$$\lim_{n \rightarrow \infty} \frac{1}{n} (e_1(c) + \dots + e_n(c)) = \gamma_p \quad \text{a.e. } c = (e_1, e_2, \dots).$$

(2) $\partial \gamma_p = 0$, where $\partial : C_1(X_0, \mathbb{R}) \rightarrow C_0(X_0, \mathbb{R})$ is the boundary map. Thus it defines an element γ_p in the first homology group $H_1(X_0, \mathbb{R})$.

The proof relies on the Birkhoff's ergodicity.

What are the possible values of γ_p when p runs over all transition probabilities. To give an answer, by choosing an orientation $E_0^+ \subset E_0$, define the ℓ^1 -norm on $H_1(X_0, \mathbb{R})$ by

$$\left\| \sum_{e \in E_0^+} a_e e \right\|_1 = \sum_{e \in E_0^+} |a_e|.$$

It is obvious that $\|\cdot\|_1$ does not depend on the choice of E_0^+ .

Theorem 4. *Let*

$$\mathcal{D}_0 = \{\gamma_p \in H_1(X_0, \mathbb{R}) \mid p \text{ is a transition probability on } X_0\}.$$

Then it is the unit ball with respect to the $\|\cdot\|$ -norm. That is

$$\mathcal{D}_0 = \{\alpha \in H_1(X_0, \mathbb{R}) \mid \|\alpha\|_1 < 1\}.$$

In particular, $\overline{\mathcal{D}}_0$ is a convex polyhedron in $H_1(X_0, \mathbb{R})$, symmetric around the origin.

What we find about combinatorial properties of $\overline{\mathcal{D}}_0$ are the following.

Theorem 5. 1. $\overline{\mathcal{D}}_0$ is “rational” in the sense that all extreme points of $\overline{\mathcal{D}}_0$ are in $H_1(X_0, \mathbb{Q})$.

2. $\alpha \in H_1(X_0, \mathbb{Q})$ is a vertex of \mathcal{D}_0 if and only if $\alpha = c/\|c\|_1$ for a circuit (simple closed path) c in X_0 .

3. A face of the highest dimension corresponds to an orientation E_0^+ of X_0 which is strongly connected. A face of lower dimensions corresponds to an oriented subgraph contained in a strongly connected orientation (with a compatible orientation).

4. Let F_1 and F_2 be faces of \mathcal{D}_0 and X_{F_1} and X_{F_2} are the corresponding oriented subgraphs. $F_1 \subset F_2$ iff $X_1 \subset X_2$ as orientated graphs (namely they have compatible orientations).

The homology class γ_p is a sort of a quantity to measure homological drift of the random walk. In fact, we obtain

Proposition 6. $\gamma_p = 0$ if and only if p gives a symmetric random walk, i.e. there is a measure m of X_0 such that $p(e)m(o(e)) = p(\bar{e})m(t(e))$, or equivalently the transition operator L is symmetric with respect to the measure m .

We may also establish another geometric feature of \mathcal{D}_0 . For $\alpha \in H_1(X_0, \mathbb{Z})$, denote by $l(\alpha)$ the minimum of length of closed paths c in X_0 with $[c] = \alpha$.

Corollary 7 (A graph analogue of a result due to Gromov).

$$\#\{\alpha \in H_1(X_0, \mathbb{Z}) \mid l(\alpha) \leq x\} \sim \text{vol}(\mathcal{D}_0)x^k \quad (x \rightarrow \infty),$$

where $k = \text{rank}(H_1(X_0, \mathbb{Z}))$ and $\text{vol}(\mathcal{D}_0)$ is the volume of \mathcal{D}_0 with respect to the Lebesgue measure on $H_1(X_0, \mathbb{R})$ such that

$$\text{vol}\left(H_1(X_0, \mathbb{R})/H_1(X_0, \mathbb{Z})\right) = 1.$$

3. CRYSTAL LATTICES

Now we shall proceed to the case of crystal lattices. A crystal lattice X is a connected locally finite infinite graph X on which a free abelian group Γ acts as an automorphism group and its quotient $X_0 = \Gamma \backslash X$ has a finite graph structure.

A piecewise linear map Φ of X into $\Gamma \otimes \mathbb{R} \cong \mathbb{R}^k$ ($k = \text{rank } \Gamma$) is said to be a *periodic realization* if it satisfies

$$\Phi(\sigma x) = \Phi(x) + \sigma,$$

here in the right hand side σ stands for the translation by the vector $\sigma \otimes 1 \in \Gamma \otimes \mathbb{R} \cong \mathbb{R}^k$.

There always exists a periodic realization of a given crystal lattice X with a lattice group Γ . Using a periodic realization, it is straightforward to see

$$c_1 n^k \leq \#\{x \in X \mid d(x_0, x) \leq n\} \leq c_2 n^k$$

with some positive constants c_1 and c_2 . Thus the positive integer $k = \text{rank}(\Gamma)$ does not depend on the choice of a lattice group Γ . We call k the *dimension* of X .

Now we consider a random walk on X given by a Γ -invariant transition probability p , or equivalently the lift of a transition probability p_0 on X_0 . Given a periodic realization Φ , we put $\xi_n(c) = \Phi(x_n(c))$ for $c \in \Omega_x(X)$. (the site of a particle starting at x_0 in n -steps). We thus obtain a $\Gamma \otimes \mathbb{R}$ -valued process $\{\xi_n\}_{n=0}^\infty$.

To describe the asymptotic behavior of $\{\xi_n\}$ as n goes to ∞ , we need to introduce a surjective homomorphism $\rho : H_1(X_0, \mathbb{Z}) \rightarrow \Gamma$. Let $\alpha \in H_1(X_0, \mathbb{Z})$ and represent α by a closed path c in X_0 . Take a lift \tilde{c} of c in X . Since $o(\tilde{c})$ and $t(\tilde{c})$ project down to the same element in X_0 , there exists $\sigma \in \Gamma$ such that $t(\tilde{c}) = \sigma o(\tilde{c})$. We then put $\rho(\alpha) = \sigma$. We extend ρ to a surjective homomorphism $\rho_{\mathbb{R}} : H_1(X_0, \mathbb{R}) \rightarrow \Gamma \otimes \mathbb{R}$.

As a corollary of Theorem 3, we obtain

Corollary 8.

$$\lim_{n \rightarrow \infty} \frac{1}{n} \xi_n(c) = \rho_{\mathbb{R}}(\gamma_{p_0}) \quad \text{a.e. } c \in \Omega_x(X).$$

Now comes a discussion about large deviations principle for the process $\{\xi_n\}$. As $\frac{1}{n} \xi_n(c) \rightarrow \rho_{\mathbb{R}}(\gamma_{p_0})$ as $n \rightarrow \infty$ for a.e. paths c , the probability for $\frac{1}{n} \xi_n(c) \rightarrow \xi \neq \rho_{\mathbb{R}}(\gamma_{p_0})$ tends to zero as $n \rightarrow \infty$. Large Deviation is to study its decay rate. More precisely

Definition 1 (Large Deviation Principle). *A large deviation principle holds for a process $\{\xi_n\}$ if there exists a lower semi-continuous function $I : \Gamma \otimes \mathbb{R} \rightarrow [0, \infty]$ which satisfies*

1. $\{\xi \mid I(\xi) \leq c\}$ is compact for every $c < \infty$.
2. For every $A \subset \Gamma \otimes \mathbb{R}$,

$$\begin{aligned} -I(\text{int}A) &\leq \liminf_{n \rightarrow \infty} \frac{1}{n} \log P_x\left(\frac{1}{n}\xi_n \in \text{int}A\right) \\ &\leq \limsup_{n \rightarrow \infty} \frac{1}{n} \log P_x\left(\frac{1}{n}\xi_n \in \overline{A}\right) \leq -I(\overline{A}), \end{aligned}$$

where $I(K) = \inf\{I(\mathbf{z}) \mid \mathbf{z} \in K\}$ for $K \subset \Gamma \otimes \mathbb{R}$.

Very roughly, in a good situation, it indicates that

$$P_x\left(\frac{1}{n}\xi_n = \xi\right) \sim \beta_n(\xi)e^{-nI(\xi)},$$

with $\lim_{n \rightarrow \infty} \frac{1}{n} \log \beta_n(\xi) = 0$. As I represents the decay rate, it is called the *rate function*.

Theorem 9. *A large deviation property holds for $\{\xi_n\}$.*

To give more details, we let

$$\langle \cdot, \cdot \rangle : (\Gamma \otimes \mathbb{R}) \times \text{Hom}(\Gamma, \mathbb{R}) \rightarrow \mathbb{R}$$

be the pairing map between $\Gamma \otimes \mathbb{R}$ and its dual $(\Gamma \otimes \mathbb{R})^* = \text{Hom}(\Gamma, \mathbb{R})$.

Lemma 10. *Let $\chi \in \text{Hom}(\Gamma, \mathbb{R})$.*

- 1.

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log E(e^{\langle \xi_n, \chi \rangle}) = c(\chi)$$

exists.

2. $e^{c(\chi)}$ is the maximal positive eigenvalue of the “twisted” transition operator $L_\chi : C(E_\chi) \rightarrow C(E_\chi)$, where

$$C(E_\chi) = \{s : X \rightarrow \mathbb{R} \mid s(\sigma x) = e^{\chi(\sigma)}s(x)\},$$

and $L_\chi = L|_{C(E_\chi)}$ (it is easy to check that $L(C(E_\chi)) \subset C(E_\chi)$).

3. c is real analytic, and the hessian of c is strictly positive definite everywhere. Thus the correspondence $\chi \mapsto (\nabla c)(\chi)$ is a diffeomorphism of $\text{Hom}(\Gamma, \mathbb{R})$ onto an open subset \mathcal{D} in $\Gamma \otimes \mathbb{R}$.

By using a general recipe in the theory of large deviation (see [1]), with the rate function $I : \Gamma \otimes \mathbb{R} \rightarrow [0, \infty]$ defined by

$$I(\mathbf{z}) = \sup_{\chi} (\langle \mathbf{z}, \chi \rangle - c(\chi))$$

we have the LDP for our random walk.

We also see

Proposition 11. $\mathcal{D} = \rho_{\mathbb{R}}(\mathcal{D}_0)$, and hence is independent of p . That is

$$\mathcal{D} = \{\mathbf{x} \in \Gamma \otimes \mathbb{R} \mid \|\mathbf{x}\|_1 < 1\},$$

where

$$(1) \quad \|\mathbf{x}\|_1 = \inf\{\|\alpha\|_1 \mid \alpha \in H_1(X_0, \mathbb{R}), \rho_{\mathbb{R}}(\alpha) = \mathbf{x}\}.$$

Therefore $\overline{\mathcal{D}}$ is a convex polyhedron, symmetric around the origin, and rational in the sense that the vertices of $\overline{\mathcal{D}}$ are in $\Gamma \otimes \mathbb{Q}$.

We easily find that I takes finite value in $\overline{\mathcal{D}}$ and infinite in $(\overline{\mathcal{D}})^c$. Indeed,

$$I(\mathbf{z}) = \langle \mathbf{z}, \chi_0 \rangle - c(\chi_0), \quad (\nabla c)(\chi_0) = \mathbf{z},$$

and hence, I is real analytic in \mathcal{D} .

The assertion (2) affords us a bridge between the large deviation and positive harmonic functions. In fact, if we denote by K the set of positive harmonic functions f on X with $f(x_0) = 1$, then, by the Harnack inequality, we find that K is a compact convex set in the space of functions with the topology of pointwise convergence, which is, by the Krein-Milman theorem, the closed convex hull of the *extreme points* of K . We may also check that the extreme points of K are exactly the minimal harmonic functions, where a harmonic function f is said to be *minimal* if, whenever $0 \leq g(x) \leq f(x)$ for any other harmonic function g , then $g(x) = Cf(x)$ for some constant $C \geq 0$. From this characterization of extreme points, it follows that a positive valued function f is an extreme point if and only if there exists $\chi \in \text{Hom}(\Gamma, \mathbb{R})$ such that $f \in C(E_\chi)$ and $L_\chi f = f$. We thus obtain the correspondence $f \mapsto \chi$ between the set of extreme points and the level set $c^{-1}(0)$, which turns out to be one-to-one. This says that the *minimal Martin boundary* is identified with $c^{-1}(0)$ (if the random walk is *transient*); see [5].

4. GROMOV-HAUSDORFF CONVERGENCE

Finally, as an application of the LDP, we show

Theorem (1'). *Let X be a crystal lattice and $\|\cdot\|_1$ is the norm defined in (1). Then, in the pointed Gromov-Hausdorff topology,*

$$\lim_{\epsilon \downarrow 0} (X, \epsilon d, x_0) = (\Gamma \otimes \mathbb{R}, d_1, 0) \quad (x_0 \in X, 0 \in \Gamma \otimes \mathbb{R}),$$

where $d_1(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|_1$.

The unit ball in $\Gamma \otimes \mathbb{R} \cong \mathbb{R}^k$ with respect to the distance d_1 coincides with the convex polyhedron we capture in the LDP. Actually the key of the proof is a characterization of the boundary $\partial \mathcal{D}$ due to the LDP.

To be more precise, put $\ell_x(\sigma) = d(x, \sigma x)$ and $\ell(\sigma) = \inf_{x \in X} \ell_x(\sigma)$ for $x \in X$ and $\sigma \in \Gamma$. By using the LDP, we prove

Lemma 12.

(1) For $x \in X$, $\sigma \in \Gamma$, the limit $\lim_{n \rightarrow \infty} \frac{1}{n} \ell_x(\sigma^n)$ exists.

(2)

$$\lim_{n \rightarrow \infty} \frac{1}{n} \ell_x(\sigma^n) = \lim_{n \rightarrow \infty} \frac{1}{n} \ell(\sigma^n).$$

We denote the limit by $\|\sigma\|_\infty$.

(3)

$$\|\sigma\|_1 = \|\sigma\|_\infty.$$

From this, it is standard to show Theorem 4.

Remark. In this talk, the ℓ^1 -norm of $H_1(X_0, \mathbb{R})$ plays an important role but the ℓ^2 -norm also relevant to a long time asymptotic of R.W. on a crystal lattice. Earlier, we established the central limit theorem (CLT) for a symmetric random walk on a crystal lattice.

Define

$$\|\alpha\|_2^2 = \sum_{e \in E_0^+} |a_e|^2 \quad (\alpha = \sum_{e \in E_0^+} a_e e \in H_1(X_0, \mathbb{R})),$$

$$\|\mathbf{x}\|_2 = \inf \{ \|\alpha\|_2 \mid \alpha \in H_1(X_0, \mathbb{R}), \rho_{\mathbb{R}}(\alpha) = \mathbf{x} \},$$

for $\mathbf{x} \in \Gamma \otimes \mathbb{R}$. Then one has

$$P\left(\frac{1}{\sqrt{n}} \xi_n \in A\right) \rightarrow \frac{1}{(4\pi a)^{k/2}} \int_A \exp\left(-\frac{\|\mathbf{x}\|_2^2}{4a}\right) d\mathbf{x},$$

where $a = (m(X_0))^{-1}$ (see [3]).

REFERENCES

- [1] R. S. Ellis, *Large deviations for a general class of random vectors*, Ann. Prob. **12**(1984), 1-12.
- [2] M. Gromov, *Metric Structures for Riemannian and Non-Riemannian Spaces*, Birkhäuser, 1999.
- [3] M. Kotani and T. Sunada, *Albanese maps and off diagonal long time asymptotics for the heat kernels*, Comm. Math. Phys. **209**(2000), 633-670.
- [4] M. Kotani and T. Sunada, *Standard realizations of crystal lattices via harmonic maps*, Trans. Amer. Math. Soc. **353**(2000), 1-20
- [5] S. A. Sawyer, *Martin boundaries and random walks*, Contemporary Math. **206**(1997), 17-44.

E-mail address: kotani@math.tohoku.ac.jp

MATHEMATICAL INSTITUTE, GRADUATE SCHOOL OF SCIENCES, TOHOKU UNIVERSITY, Aoba, Sendai 980-8578, JAPAN

共役類の長さ と 既約指標の次数

千葉大学理学部
野澤 宗平

§1 有限群の共役類の長さ と 既約指標の次数の間に生じる幾つかの類似性 と 関連する結果 (菅家邦彦 との共同研究) について述べる. 以下, G は有限群 とし, $\text{Con}(G)$, $\text{Irr}(G)$ でそれぞれ G の共役類全体, および (\mathbb{C} 上の) 既約指標全体の集合を表す. また, 自然数 m の素因数全体の集合を $\pi(m)$ で表し, $\text{ccl}(G)$, $\rho^*(G)$, $\text{cd}(G)$, $\rho(G)$ をそれぞれ次の様に定める.

$$\begin{aligned}\text{ccl}(G) &:= \{ |C| \mid C \in \text{Con}(G) \}, & \rho^*(G) &:= \bigcup_{C \in \text{Con}(G)} \pi(|C|) \\ \text{cd}(G) &:= \{ \chi(1) \mid \chi \in \text{Irr}(G) \}, & \rho(G) &:= \bigcup_{\chi \in \text{Irr}(G)} \pi(\chi(1)).\end{aligned}$$

共役類 と 既約指標の間には $|\text{Con}(G)| = |\text{Irr}(G)|$ が成り立つ. このことは $\text{ccl}(G)$ と $\text{cd}(G)$ の間に多くの類似性を引き起こす要因の一つと考えられる. また, 群の位数に関する等式

$$\begin{aligned}|G| &= |Z(G)| + \sum_{C \in \text{Con}(G), |C| > 1} |C| && \text{(類等式)} \\ &= |G : G'| + \sum_{\chi \in \text{Irr}(G), \chi(1) > 1} \chi(1)^2\end{aligned}$$

は, $\text{ccl}(G) = \{1\}$ および $\text{cd}(G) = \{1\}$ がともに G がアーベル群であるための必要十分条件であることを示している.

一般に, 与えられた共役類の長さの集合 $\text{ccl}(G)$ あるいは既約指標の次数の集合 $\text{cd}(G)$ をもつ群の構造を調べる問題は, 1953年に発表された $|\text{ccl}(G)| = 2$ に関する N. Ito [12] の結果に始まる.

定理 (N. Ito [12]) $\text{ccl}(G) = \{1, m\}$ ならば, m は素数べき ($= p^e$) で, G は sylow p 部分群 と アーベル群の直積である.

I. M. Isaacs と D. S. Passman は Ito の結果の $\text{cd}(G)$ 版として, 次の定理を与えた.

定理 (I. M. Isaacs and D. S. Passman [8]) $\text{cd}(G) = \{1, m\}$ ならば, $G''' = 1$ で, 次のいずれか一方が起こる.

- (1) G は指数 m の可換な正規部分群をもつ。
- (2) m は素数べき ($= p^e$) で、 G は Sylow p 部分群とアーベル群の直積である。

その後、 $|\text{cd}(G)| \geq 3$ の場合について、I. M. Isaacs, T. Noritzsch, D. S. Passman, B. Huppert 等 ([1], [6], [7], [8], [17] 参照) によって活発に研究されたが、 $|\text{cd}(G)| = 2$ の結果ほど詳細な群構造が得られたとは言い難い。

一方、 $\text{ccl}(G)$ に関しては上記の Ito の結果後、D. Chillag and M. Herzog による次の結果が与えられるまで、ほとんど研究されることがなかった。

定理 (D. Chillag and M. Herzog [4])

- (1) $|\text{ccl}(G)| \geq 3$ で、 $\text{ccl}(G)$ の元はすべて素数べきとし、 G は可換な直積因子をもたないと仮定する。このとき、
 - (a) G は可解で、ある素数 p に対して p べき零であり、かつ G の Sylow p 部分群 P は可換である。
 - (b) $O_{p'}(G)$ は可換である。
 - (c) $Z(G) = O_p(G)$ 。
 - (d) $P/O_p(G)$ は $O_{p'}(G)$ 上に fixed point free に作用する。特に、 $P/Z(G)$ は巡回群で、 G は quasi-Frobenius 群である。
 - (e) ある素数 $q (\neq p)$ に対して、 $O_{p'}(G) \in \text{Syl}_q(G)$ である。特に、 $|G| = p^a q^b$ 。

- (2) 逆に、有限群 G が (1) の (a) から (e) までをすべて満たすならば、

$$\text{ccl}(G) = \{1, |P : O_p(G)|, |O_{p'}(G)|\}.$$

ここでの目的は、D. Chillag and M. Herzog の結果の一般化を与えることと、 $|\text{ccl}(G)| = 3$ をもった群の既約指標の次数に関する特徴付けを与えることである。なお、C-H の一般化 (後述の定理 1 (1) の一部と定理 3 を併せた結果) は既に S. Dolfi によっても得られている。すなわち、

定理 (S. Dolfi [5]) 群 G は可換な直積因子をもたないと仮定する。ある素数の集合 π に対して、 G が class- π -separable (すなわち、任意の $C \in \text{Con}(G)$ に対して、 $|C|$ は π 数、 π' 数、または 1 のいずれか) であるための必要十分条件は、 $G = MN$ で、 $G/O_\pi(G)$ が Frobenius 群となることである。ここで、 M は G の可換な Hall π 部分群、 N は G の可換な正規 Hall π' 部分群である。

この S. Dolfi の結果は、 $\text{cd}(G)$ に関する O. Manz の結果の $\text{ccl}(G)$ 版である。

定理 (O. Manz [14]) π をある素数の集合とする。もし群 G が π -separable で、かつ character- π -separable ならば、 $\ell_\pi(G) \leq 3$ である。特に、 $\pi = \{p\}$ ならば、 $\ell_p(G) \leq 2$ である。

§2 次の条件 (*) を満たす群について考察しよう。

(*) $\text{ccl}(G) = \{1, m, n\}$ で、 $(m, n) = 1$ かつ $m < n$ 。

このような群の例としては、3 次の対称群 S_3 、4 次の交代群 A_4 、位数 pq (p, q は相異なる素数で、 $p < q = 1 + kp$ とする) の Frobenius 群 G_{pq} 等がある。

G	$\text{ccl}(G)$	$\text{cd}(G)$	degree pattern
S_3	$\{1, 2, 3\}$	$\{1, 2\}$	$(1, 1, 2)$
A_4	$\{1, 3, 4\}$	$\{1, 3\}$	$(1, 1, 1, 3)$
G_{pq}	$\{1, p, q\}$	$\{1, p\}$	$(\underbrace{1, \dots, 1}_p, \underbrace{p, \dots, p}_k)$

上の表から、これらの群においては

- $\text{cd}(G)$ は $\text{ccl}(G)$ から最大数を除いたもの、
- degree pattern は、1 次指標が m 個、 m 次の既約指標が k 個 (ただし、 $n = 1 + km$)

となっていることが読みとれる。条件 (*) を満たす群を GAP で調べたところすべてこのようになっていた。

注意 1 条件 (*) において、 $(m, n) = 1$ は必要である。例えば、 $\text{SL}(2, 3)$ では、

$$\text{ccl}(\text{SL}(2, 3)) = \{1, 4, 6\}, \quad \text{cd}(\text{SL}(2, 3)) = \{1, 2, 3\}$$

となっており、 $\text{cd}(\text{SL}(2, 3)) = \{1, 4\}$ とはならない。

注意 2 条件 (*) を満たす群は必ずしも存在しない。例えば、次のことが知られている。

- $\text{ccl}(G) = \{1, m, m+1\}$ ならば、 $m+1$ は素数べきである (M. Bianchi 等 [3])。
- m が奇数ならば、 $\text{ccl}(G) = \{1, m, m+2\}$ を満たす群 G は存在しない (A. Mann [2, Chap. 3, §11])。

そこで次の問題が考えられる。

問題 1 G が条件 (*) を満たすならば, $\text{cd}(G) = \{1, m\}$ となるか. さらに, $n = 1 + km$ とすると, degree pattern は $(\underbrace{1, \dots, 1}_m, \underbrace{m, \dots, m}_k)$ となるか.

問題 2 条件 (*) を満たす群が存在するための m, n に関する数論的条件を与えよ.

問題 1 に関しては, 次の結果が得られた.

定理 1 $\text{ccl}(G) = \{1, m_1, \dots, m_s, n_1, \dots, n_t\}$ とし, $m = m_1 \cdots m_s$, $n = n_1 \cdots n_t$ とおく. もし $(m, n) = 1$ ならば, 次が成り立つ.

- (1) (a) G は可解群で, $G = MN \times A$ と表せる. ここで, M は G の非正規な可換 Hall $\pi(m)$ 部分群, N は正規な可換 Hall $\pi(n)$ 部分群, A は可換群である.
 - (b) $s = t = 1$, $m < n$ かつ $n \equiv 1 \pmod{m}$ である. 特に, $\text{ccl}(G) = \{1, m, n\}$ となる.
 - (c) G は quasi-Frobenius 群である.
 - (d) もし G が可換な直積因子をもたないならば, M は巡回群で, $O_{\pi(m)}(G) = Z(G)$ かつ $N = O_{\pi(n)}(G) = G'$ となる.

(2) $\text{cd}(G) = \{1, m\}$ である. 特に, G の degree pattern は $(\underbrace{1, \dots, 1}_{m|Z(G)|}, \underbrace{m, \dots, m}_{k|Z(G)|})$ である. ここで, $n = 1 + km$ である.

定理 1 から直ちに次の系が得られる.

系 1.1 $\text{ccl}(G) = \{1, m_1^{(1)}, \dots, m_{s_1}^{(1)}, \dots, m_1^{(r)}, \dots, m_{s_r}^{(r)}\}$ とし, 各 $k = 1, 2, \dots, r$ に対して, $m^{(k)} = m_1^{(k)} \cdots m_{s_k}^{(k)}$ とおく. このとき, 異なる i, j に対して $(m^{(i)}, m^{(j)}) = 1$ ならば, $r \leq 2$ となる.

特に, 素数に関するチェビシエフの定理より, $\text{ccl}(G)$ が連続する r 個の整数値をもつ場合について, 次が成り立つ.

系 1.2 $\text{ccl}(G) = \{1, 2, \dots, r\}$ ならば, $r \leq 3$ である. 特に, $r = 3$ のとき, $G/Z(G) \cong S_3$ となる.

$r = 2$ の場合については, Ishikawa [9] の結果がある. 系 1.2 は $\text{cd}(G)$ に関する次の B. Huppert [6, §32] の結果の $\text{ccl}(G)$ 版であるが, 同様の結果が M. Bianchi 等 [3] によっても得られている.

定理 (B. Huppert [6]) $\text{cd}(G) = \{1, 2, \dots, t\}$ とするとき、次が成り立つ。

- (1) G が可解である $\iff t \leq 4$.
- (2) もし $t > 4$ ならば、 $t = 6$ で、 $G = \text{SL}(2, 5)Z(G)$.

問題 2, すなわち、条件 (*) を満たす群が存在するための m, n に関する数論的条件に関しては、次の定理 2 と N. Ito and G. Michler の結果を必要とする。

定理 2 G は条件 (*) を満たし、かつ可換な直積因子をもたないと仮定する。 M^* を G の中心 $Z(G)$ に含まれない G の $\pi(m)$ 部分群、 N^* を G の正規な $\pi(n)$ 部分群とし、 $G^* = M^*N^*$ とおく。このとき、 $\text{ccl}(G^*) = \{1, |M^* : M^* \cap Z(G)|, |N^*|\}$ が成り立つ。

定理 (N. Ito and G. Michler [10]) p を素数とする。このとき、次は同値。

- (1) G は可換な正規 Sylow p 部分群をもつ。
- (2) G は p 可解で、任意の $\chi \in \text{Irr}(G)$ に対して $p \nmid \chi(1)$ である。

群 G が条件 (*) を満たすならば、定理 1 (1) (a) より、 G の Sylow 部分群はすべて可換である。従って、上の Ito-Michler の定理は任意の $p \in \pi(G)$ に対して

$$\text{Syl}_p(G) \ni P \text{ が } G \text{ の正規部分群} \iff p \notin \rho(G)$$

を意味する。従って、定理 1 (2) より、

任意の $p \in \pi(m)$ に対して、 G の Sylow p 部分群 P は正規部分群でなく、
任意の $q \in \pi(n)$ に対して、 G の Sylow q 部分群 Q は正規部分群である。

そこで、定理 2 の M^* として G の Hall $\pi(m)$ 部分群 M を、 N^* として G の Sylow q 部分群 Q をとれば、任意の $q \in \pi(n)$ と任意の $Q \in \text{Syl}_q(G)$ に対して、 $\text{ccl}(MQ) = \{1, m, |Q|\}$ が成り立つ。このとき、定理 1 (1) (b) より、 $|Q| \equiv 1 \pmod{m}$ となる。

以上のことから、条件 (*) を満たす群が存在するための m, n に関する条件として次の結果が得られる。

系 2.1 G は条件 (*) を満たし、かつ可換な直積因子をもたないと仮定する。 n の素因数分解を $n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$ とするとき、任意の $i (= 1, 2, \dots, t)$ に対して

$$p_i^{e_i} \equiv 1 \pmod{m}$$

が成り立つ。

注意 この結果は、先に紹介した A. Mann の結果 ($n = m + 2$ で、 n は奇数) および M. Bianchi 等の結果 ($n = m + 1$ の場合) を含んでいる。

定理 1 と次の定理 3 を併せると、先に述べた S. Dolfi [5] の定理と同様の結果が得られる。

定理 3 G は可換な直積因子をもたないと仮定する。ある $\pi \subset \pi(|G|)$ に対して、 G が次の 4 条件

- (1) G が可換な Hall π 部分群 M をもつ;
- (2) G が可換な正規 Hall π' 部分群 N をもつ;
- (3) $Z(G) = O_\pi(G)$;
- (4) $G/Z(G)$ は Frobenius 核 $NZ(G)/Z(G)$ をもった Frobenius 群である;

を満たすならば、 $\text{ccl}(G) = \{1, |M : Z(G)|, |N|\}$ となる。

§3 定理 1 と定理 2 の証明の概略について述べよう。定理 1 の証明におけるキーポイントは、次の N. Ito および B. Huppert の結果である。

定理 (N. Ito [11]) $\rho^*(G) \ni p, q (\neq)$ とする。任意の $C \in \text{Con}(G)$ に対して、 $pq \nmid |C|$ ならば、(必要ならば、 p と q を入れ替えることによって) G は p べき零で、 G の Sylow p 部分群は可換群となる。

補題 (B. Huppert [6]) G は可換な有限群 A に作用すると仮定し、 $\hat{A} = \text{Irr}(A) = \text{Hom}(A, \mathbb{C}^\times)$ とおく。このとき、

- (1) $(|G|, |A|) = 1$ ならば、 $A \cong \hat{A}$ (as G -sets) である。
- (2) G が可換群ならば、 $\text{cd}(G\hat{A}) = \{|a^G| \mid a \in A\}$ である。

定理 1 の証明の概略。

N. Ito の結果より、任意の $p \in \pi(m)$ に対して、 G は p べき零、かつ $P \in \text{Syl}_p(G)$ は可換としてよい。このとき、 $G/O_{p'}(G) \cong P$ であるから、 $O_{p'}(G) \geq G'$ であることに注意する。

$\pi := \pi(m) = \{p_1, p_2, \dots, p_r\}$ とし、 $G_0 := G$ 、 $G_i := G_{i-1} \cap O_{p_i'}(G)$ ($1 \leq i \leq r$) とおく。従って、 $H := \bigcap_{i=1}^r O_{p_i'}(G) \geq G'$ で、 H は π' 群である。

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_r = H \supset \{1\}$$

は G の正規列で、

$$G_{i-1}/G_i = G_{i-1}/(G_{i-1} \cap O_{p_i'}(G))$$

$$\begin{aligned} &\cong G_{i-1}O_{p_i'}(G)/O_{p_i'}(G) \\ &\leq G/O_{p_i'}(G) \cong P_i \in \text{Syl}_{p_i}(G) \end{aligned}$$

であるから、 G は π 可解で、 $H = O_{\pi'}(G)$ は G の唯一の Hall π' 部分群となる。
また、 M を G の Hall π 部分群とすると、

$$D(M) \leq M \cap G' \leq M \cap H = \{1\}.$$

よって、 M は可換群である。

$\bar{G} := G/C_G(H)$ とし、 $g \in G \setminus C_G(H)$ とする。 $H = O_{\pi'}(G)$ であるから、 $|g^G|$ は π' 数。従って、 $|\bar{g}^{\bar{G}}|$ は π' 数かまたは 1 である。よって、任意の $p \in \pi$ に対して、 $(|\bar{G} : Z(\bar{G})|, p) = 1$ となり、 $Z(\bar{G})$ は \bar{G} の Hall π 部分群を含む。これより、 $\bar{M} \triangleleft \bar{G}$ を得る。

次に、 H が可換であることを示す。もしある $x \in H \setminus Z(H)$ が存在するならば、 $|x^G|$ は π' 数となり、 $C_G(x)$ は G のある Hall π 部分群を含む。従って、 $MC_G(H) \triangleleft G$ と $C_G(H) \leq C_G(x)$ より $x \in C_G(M)$ となり、 $H = Z(H) \cup C_H(M)$ を得る。しかし、 H は非可換であると仮定したから、 $H = C_H(M)$ でなければならない。このとき、 $G = M \times H$ であるが、これは G の共役類の長さに関する仮定に反する。よって、 H は可換である。特に、 $G'' = \{1\}$ となり、 G は可解群である。また、明らかに M は G の正規部分群とならない。

さらに、 N を G の可換な Hall $\pi(n)$ 部分群、 A を G の可換な Hall $\pi(mn)'$ 部分群とすると、 $H = N \times A$ で、

$$G = MH = M(N \times A) = MN \times A$$

と表せる。これで (1)(a) が示せた。

以下、 G は可換な直積因子をもたないと仮定しても一般性を失わない。従って、 $G = MN$ で、 M は G の非正規な可換 Hall $\pi(m)$ 部分群、 $N = H$ は G の正規な可換 Hall $\pi(n)$ 部分群としてよい。

N は可換群であるから、 $N = [M, N] \times C_N(M)$ であり、しかも G は可換な直積因子をもたないと仮定しているので $C_N(M) = \{1\}$ が得られる。これより、 $N = G'$ と $Z(G) = O_{\pi}(G)$ が容易に導かれる。

$x \in M \setminus Z(G)$ とする。このとき、

$$|x^G| = |x^{MN}| = |x^N| = |N : C_N(x)| = |N|$$

である。ここで、 $C_N(x) = \{1\}$ となることは次による。

もし $g \in C_N(x)$ とすると、 $C_G(xg) = C_G(x) \cap C_G(g)$ かつ $|x^G|$ は π' 数より、 $|g^G| = 1$ 。従って、 $g \in N \cap Z(G) = \{1\}$ となり、 $C_N(x) = \{1\}$ を得る。

同様に, $y \in N \setminus \{1\}$ ならば, $|y^G| = |M : Z(G)|$ がいえる.

以下, $m_1 = |M : Z(G)|$, $n_1 = |N|$ とおく.

任意の $g \in G \setminus (M \cup N)$ に対して, $g = xy$ ($x \in M \setminus \{1\}$, $y \in N \setminus \{1\}$) とおく. もし $x \in Z(G)$ ならば, $|g^G| = |y^G| = m_1$ であることに注意する.

(i) $|g^G|$ が π 数のとき, $|g^G| \leq |M : Z(G)| = m_1$ であり, また, M は可換であるから

$$|g^G| \geq |g^M| = |y^M| = |M : Z(G)| = m_1.$$

従って, $|g^G| = m_1$ となり, $s = 1$ を得る.

(ii) $|g^G|$ が π' 数のとき, $x \in M \setminus Z(G)$ より, $|g^G| = |x^N| = |N| = n_1$. 従って, $t = 1$ である.

以上のことから, $m = m_1 = |M : Z(G)|$, $n = n_1 = |N|$ を得る. さらに, 任意の $y \in N \setminus \{1\}$ に対して $|y^G| = m$ であることと $N \triangleleft G$ より, $n = |N| = 1 + km$ ($\exists k \in \mathbb{Z}$) となる. よって, (1)(b) が示せた.

(1)(c) と (d) の証明 ([13] 参照) は省略し, (2) を示そう.

$\hat{N} = \text{Irr}(N)$ とおく. このとき,

$$|y^G| = |y^M| = |M : C_M(y)| = |M : Z(G)| = m$$

であるから, 先に述べた補題より

$$\text{cd}(G) = \text{cd}(MN) = \text{cd}(M\hat{N}) = \{|y^M| \mid y \in N\} = \{1, m\}.$$

また, G の 1 次指標の個数は $|G : G'| = |G : N| = |M| = m|Z(G)|$ であるから,

$$\sum_{\chi \in \text{Irr}(G)} \chi(1)^2 = |G| = m|Z(G)| + k|Z(G)|m^2.$$

従って, $|\{\chi \in \text{Irr}(G) \mid \chi(1) = m\}| = k|Z(G)|$ を得る. ■

定理 2 の証明の概略

M^* を含む G の Hall $\pi(m)$ 部分群を M , G の唯一の Hall $\pi(n)$ 部分群を N とする. このとき, 任意の $g \in G^*$ に対して, $|g^G| = m, n$ となる場合についてそれぞれ $|g^{G^*}|$ を計算すればよい.

• $|g^G| = m$ の場合: $C_{G^*}(g) = M^*N^* \cap (Z(G) \times N) = (M^* \cap Z(G)) \times N^*$ であるから, $|g^{G^*}| = |M^*N^* : (M^* \cap Z(G)) \times N^*| = |M^* : M^* \cap Z(G)|$.

• $|g^G| = n$ の場合: g を含む G^* の Hall $\pi(m)$ 部分群 M_g^* が存在して, $M_g^* \leq C_{G^*}(g)$ である. 一方, $|C_{G^*}(g)| = |G^* \cap M^h| \leq |G^*|_{\pi(m)} = |M^*| = |M_g^*|$ ($\exists h \in G$)

であるから、 $C_{G^*}(g) = M_g^*$ を得る。従って、 $|g^{G^*}| = |M^*N^* : M_g^*| = |N^*|$ となる。

以上により、定理 2 が示せた。 ■

§4 最後に、定理 1 の応用として、 $\text{cd}(G)$ および $\text{ccl}(G)$ から構成されるグラフ間の 1 つの対応を与えてみたい。

一般に、 $\text{cd}(G)$ の元の素因数の集合 $\rho(G)$ の元を頂点とし、 $p, q \in \rho(G)$ に対して、 $pq \mid n$ を満たす $n \in \text{cd}(G)$ が存在するとき、2 つの頂点 p, q を辺で結ぶことにより、degree グラフ $\Gamma(G)$ が構成できる。同様に、 $\text{ccl}(G)$ の元の素因数の集合 $\rho^*(G)$ の元を頂点とし、 $p, q \in \rho^*(G)$ に対して、 $pq \mid n$ を満たす $n \in \text{ccl}(G)$ が存在するとき、2 つの頂点 p, q を辺で結ぶことにより、class-length グラフ $\Gamma^*(G)$ を構成する。

degree グラフ $\Gamma(G)$ に対しては、O. Manz, R. Staszewski, W. Willems 等による次の定理が知られている。

定理 (O. Manz [15], O. Manz-R. Staszewski-W. Willems [16]) 任意の有限群 G に対して、

- (1) $\Gamma(G)$ の連結成分は高々 3 個である。
- (2) G が可解ならば、 $\Gamma(G)$ の連結成分は高々 2 個である。

系 1.1 を $\Gamma^*(G)$ の言葉で言い換えることで、これと類似の結果が得られる。

定理 4 任意の有限群 G に対して、

- (1) $\Gamma^*(G)$ の連結成分は高々 2 個である。
- (2) $\Gamma^*(G)$ の連結成分が 2 個ならば、 G は可解である。
- (3) G が非可換単純群ならば、 $\Gamma^*(G)$ の連結成分は 1 個である。

さらに、定理 1 と定理 4 から、直ちに $\Gamma^*(G)$ と $\Gamma(G)$ の間の対応を得る。

系 4.1 任意の有限群 G に対して、

- (1) $\Gamma^*(G)$ の連結成分が 2 個ならば、 $\Gamma(G)$ の連結成分は 1 個である。
- (2) $\Gamma(G)$ の連結成分が 2 個以上ならば、 $\Gamma^*(G)$ の連結成分は 1 個である。

参考文献

- [1] Y. Berkovich, D. Chillag and M. Herzog, *Finite groups in which the degrees of the nonlinear irreducible characters are distinct*, Proc. Amer. Math. Soc. 115 (1992), 955–959.

- [2] Y. Berkovich and E. M. Zhmud', *Characters of Finite groups Part I, II*, Amer. Math. Soc. Trans. Math. monographs **172** (1998), **181** (1999).
- [3] M. Bianchi, D. Chillag, M. Herzog, B. Mauri and C. Scoppola, *Applications of a graph related to conjugacy classes in finite groups*, Arch. Math. **58** (1992), 126–132.
- [4] D. Chillag and M. Herzog, *On the length of the conjugacy classes of finite groups*, J. Algebra **131** (1990), 110–125.
- [5] S. Dolfi, *Arithmetical Conditions on the Length of the Conjugacy Classes of a Finite Group*, J. Algebra **175** (1995), 753–771.
- [6] B. Huppert, *Character Theory of Finite Groups*, Walter de Gruyter, Berlin, 1998.
- [7] I. M. Isaacs, *Character Theory of Finite Groups*, Acad. Press, New York, 1976.
- [8] I. M. Isaacs and D. Passman, *A characterization of groups in terms of the degrees of their characters*, Pac. J. Math. **15** (1965), 877–903, **24** (1968), 467–510.
- [9] K. Ishikawa, *Finite p -Group with Two Conjugacy Length*, thesis (Chiba Univ), (2001).
- [10] N. Ito, *Some studies on group characters*, Nagoya Math. J. **2** (1951), 17–28.
- [11] ———, *On the degrees of irreducible representations of a finite group*, Nagoya Math. J. **3** (1951), 5–6.
- [12] ———, *On finite group with given conjugate types I*, Nagoya Math. J. **6** (1953), 17–28.
- [13] K. Kanke and S. Nozawa, *Finite groups with three class lengths*, preprint.
- [14] O. Manz, *Degree problems II: π -separable character degrees*, Comm. Algebra **11** (1985), 2421–2431.
- [15] ———, *Endliche auflösbare Gruppen, deren sämtliche Charaktergrade Primzahlpotenzen sind*, J. Algebra **94** (1985), 211–255.
- [16] O. Manz, R. Staszewski and W. Willems, *On the number of components of a graph related to character degrees*, Proc. Amer. Math. Soc. **103** (1988), 31–37.
- [17] T. Noritzsch, *Groups having three complex irreducible character degrees*, J. Algebra **175** (1995), 767–789.

位数16の自己同型群をもつ位数12の射影平面について

福島工業高等専門学校 機械工学科

末竹 千博

知られている有限射影平面の位数はすべて素数べきである。逆に、任意の素数べきに対して、それを位数としてもつ有限射影平面が存在する。有限射影平面の位数に関する最良の結果は Bruck-Ryser の定理 [1] である。有限射影平面の位数は素数べきであるという予想があるが、もしこの定理を根拠に言っているとしたら、十分根拠のある予想だとは思われない。Bruck-Ryser の定理でカバー出来ない最小の位数は 10 であるが、この位数については多くの数学者が研究し、最終的には 1989 年に H.Lam と L.Thiel と S.Swiercz[4] により計算機を用いてその非存在が証明された。Bruck-Ryser の定理でカバー出来ない次の位数は 12 である。この位数の射影平面については、Z.Janko と T.van Trung が一連の論文 (例えば [3]) でその自己同型群の可能性を調べた。1987 年に K.Horvatic-Baldaser と E.Kramer と I.Maturic-Bedenic[2] は、位数 12 の射影平面の自己同型群の位数は 16 の約数であるか、9 の約数であるかを証明した。この結果が位数 12 の射影平面についての最良の結果だと思われる。このノートでは位数 16 の自己同型群をもつ位数 12 の射影平面について調べる。もし、このような位数 12 の射影平面が存在したとすると、位数 8 の自己同型群を持つ symmetric $(12, 6, 12, 0, 2)$ -divisible design が存在する。(一般論については、末竹 [5] を参照のこと) そこで、我々の研究方向はこの design の非存在を如何に示すかということである。でも残念ながら、現時点で得られた結果は、 H を位数 12 の射影平面の位数 16 の自己同型群とすると、 H は generalized quaternion group であることである。なお、自己同型群の仮定を考えない場合でも、symmetric $(12, 6, 12, 0, 2)$ -divisible design の存在・非存在は知られていないことを注意しておく。

§1 一般論

ここで書く大半の事柄は、末竹 [5] に書かれている。

仮定 1.1 $\Pi = (\mathcal{P}, \mathcal{L})$ を位数 n の射影平面とする。 G を共通な center P_0 と共通な axis l_0 をもつ Π の位数 $m (\neq 1, n)$ の elation group とする。

明らかに、 m は n の約数で、 $P_0 \in l_0$ である。

$(P_0) = \{l_0, l_1, \dots, l_n\}$, $(l_0) = \{P_0, P_1, \dots, P_n\}$ とする。

$\mathcal{P}_0, \mathcal{P}_1, \dots, \mathcal{P}_{\frac{n^2}{m}+n}$ を \mathcal{P} 上の G -orbits とする。

$\mathcal{L}_0, \mathcal{L}_1, \dots, \mathcal{L}_{\frac{n^2}{m}+n}$ を \mathcal{L} 上の G -orbits とする。

このとき、次のように仮定してよい。

$$\mathcal{P}_i = \{P_i\}, \mathcal{L}_i = \{l_i\} \quad (0 \leq i \leq n),$$

$$|\mathcal{P}_i| = |\mathcal{L}_i| = m \quad (n+1 \leq i \leq \frac{n^2}{m} + n),$$

$$(l_i) = \mathcal{P}_{(i-1)\frac{n}{m}+(n+1)} \cup \mathcal{P}_{(i-1)\frac{n}{m}+(n+2)} \cup \dots \cup \mathcal{P}_{(i-1)\frac{n}{m}+(n+\frac{n}{m})} \quad (1 \leq i \leq n),$$

$$(P_i) = \mathcal{L}_{(i-1)\frac{n}{m}+(n+1)} \cup \mathcal{L}_{(i-1)\frac{n}{m}+(n+2)} \cup \dots \cup \mathcal{L}_{(i-1)\frac{n}{m}+(n+\frac{n}{m})} \quad (1 \leq i \leq n)$$

Ω を G の point orbit、 Δ を G の line orbit とするとき、 $(\Omega \Delta) = |\Omega \cap (l)|$ とおく。ここで、 $l \in \Delta$ 。 $(\Omega \Delta)$ は l のとり方によらず Ω と Δ にのみ依存して決まる。

G の部分集合 K に対して、 $\widehat{K} = \sum_{\mu \in K} \mu$ ($\in Z[G]$)、 $K^{-1} = \{\mu^{-1} | \mu \in K\}$ とおく。

$$m_{ij} = (\mathcal{P}_j, \mathcal{L}_i) \quad (0 \leq i, j \leq \frac{n^2}{m} + n)$$

$$M = (m_{ij})_{0 \leq i, j \leq \frac{n^2}{m} + n}, \quad L = (m_{ij})_{n+1 \leq i, j \leq \frac{n^2}{m} + n} = (l_{ij})_{0 \leq i, j \leq \frac{n^2}{m} - 1} \quad \text{とおく。}$$

$n+1 \leq i, j \leq \frac{n^2}{m} + n$ に対して、 $P_j \in \mathcal{P}_j$ 、 $l_i \in \mathcal{L}_i$ を選ぶ。

$$D_{ij} = \{\mu \in G | P_j^\mu \in (l_i)\} \quad (n+1 \leq i, j \leq \frac{n^2}{m} + n) \quad \text{とおく。}$$

$$\text{明らかに、 } |D_{ij}| = m_{ij} = 0, 1 \quad (n+1 \leq i \leq \frac{n^2}{m} + n)$$

補題 1.2 (i) $n+1 \leq i, i' \leq \frac{n^2}{m} + n$ とする。このとき、

$$\sum_{n+1 \leq j \leq \frac{n^2}{m} + n} \widehat{D_{ij}}^{-1} \widehat{D_{i'j}}$$

$$= \begin{cases} n & \text{if } i = i', \\ 0 & \text{if } i \neq i' \text{ and } \{i, i'\} \subseteq \{\frac{kn}{m} + (n+1), \frac{kn}{m} + (n+2), \dots, \frac{kn}{m} + (n + \frac{n}{m})\} \\ & \text{for some } 0 \leq k \leq n-1, \\ \widehat{G} & \text{otherwise} \end{cases}$$

(ii) $n+1 \leq j, j' \leq \frac{n^2}{m} + n$ とする。このとき、

$$\sum_{n+1 \leq i \leq \frac{n^2}{m} + n} \widehat{D_{ij}}^{-1} \widehat{D_{ij'}}$$

$$= \begin{cases} n & \text{if } j = j', \\ 0 & \text{if } j \neq j' \text{ and } \{j, j'\} \subseteq \{\frac{kn}{m} + (n+1), \frac{kn}{m} + (n+2), \dots, \frac{kn}{m} + (n + \frac{n}{m})\} \\ & \text{for some } 0 \leq k \leq n-1, \\ \hat{G} & \text{otherwise} \end{cases}$$

補題 1.3 (i) $0 \leq i, i' \leq \frac{n^2}{m} - 1$ とする。このとき、

$$\sum_{0 \leq j \leq \frac{n^2}{m} - 1} l_{ij} l_{i'j} = \begin{cases} n & \text{if } i = i', \\ 0 & \text{if } i \neq i' \text{ and } \{i, i'\} \subseteq \{\frac{kn}{m}, \frac{kn}{m} + 1, \dots, (\frac{kn}{m} + (\frac{n}{m} - 1))\} \text{ for some } 0 \leq k \leq n-1, \\ m & \text{otherwise} \end{cases}$$

(ii) $0 \leq j, j' \leq \frac{n^2}{m} - 1$ とする。このとき、

$$\sum_{0 \leq i \leq \frac{n^2}{m} - 1} l_{ij} l_{ij'} = \begin{cases} n & \text{if } j = j', \\ 0 & \text{if } j \neq j' \text{ and } \{j, j'\} \subseteq \{\frac{kn}{m}, \frac{kn}{m} + 1, \dots, (\frac{kn}{m} + (\frac{n}{m} - 1))\} \text{ for some } 0 \leq k \leq n-1, \\ m & \text{otherwise} \end{cases}$$

補題 1.4 (i) $l_{ij} = 0, 1$ ($0 \leq i, j \leq \frac{n^2}{m} - 1$)

(ii)

$$L = \begin{pmatrix} L_{00} & L_{01} & \cdots & L_{0n-1} \\ L_{10} & L_{11} & \cdots & L_{1n-1} \\ \vdots & \vdots & & \vdots \\ L_{n-10} & L_{n-11} & \cdots & L_{n-1n-1} \end{pmatrix}$$

とおく。ここで、各 L_{ij} ($0 \leq i, j \leq n-1$) は $\frac{n}{m}$ 次の正方行列。このとき、各 L_{ij} ($0 \leq i, j \leq n-1$) は置換行列である。

(iii) I を $\frac{n}{m}$ 次の単位行列、 J を $\frac{n}{m}$ 次の全 1 正方行列とすると

$$L^t L = \begin{pmatrix} nI & mJ & \cdots & mJ & mJ \\ mJ & nI & \cdots & mJ & mJ \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ mJ & mJ & \cdots & mJ & nI \end{pmatrix} = {}^t L L$$

定義 1.5 結合構造 $S = (Q, B, I)$ を次のように定義する。

$$Q = \{Q_0, Q_1, \dots, Q_{\frac{n^2}{m}-1}\}, B = \{B_0, B_1, \dots, B_{\frac{n^2}{m}-1}\} \quad (0 \leq i, j \leq \frac{n^2}{m} - 1)$$

$$Q_i I B_j \iff l_{ij} = 1$$

$$Q_i = \{Q_{\frac{im}{m}}, Q_{\frac{im}{m}+1}, \dots, Q_{\frac{im}{m}+\frac{n}{m}-1}\}$$

$$B_i = \{B_{\frac{im}{m}}, B_{\frac{im}{m}+1}, \dots, B_{\frac{im}{m}+\frac{n}{m}-1}\} \quad (0 \leq i \leq n-1) \text{ とおく。}$$

定理 1.6 $S = (Q, B, I)$ は n point classes Q_1, Q_2, \dots, Q_n と n block classes B_1, B_2, \dots, B_n をもつ symmetric $(n, \frac{n}{m}, 0, m)$ -divisible design である。

仮定 1.7 H を Π の collineation group で、 G は H の正規部分群とする。

$\forall \varphi \in H$

$\varphi^{-1}G\varphi = G$ 故 $P_0^\varphi = P_0, l_0^\varphi = l_0$

φ は $\{P_0, P_1, \dots, P_n\}$ 上の置換を引き起こす。

φ は $\{P_{n+1}, P_{n+2}, \dots, P_{\frac{n^2}{m}+n}\}$ 上の置換を引き起こす。

φ は $\{B_0, B_1, \dots, B_n\}$ 上の置換を引き起こす。

φ は $\{B_{n+1}, B_{n+2}, \dots, B_{\frac{n^2}{m}+n}\}$ 上の置換を引き起こす。

φ は $\{Q_0, Q_1, \dots, Q_{n-1}\}$ 上の置換を引き起こす。

φ は $\{B_0, B_1, \dots, B_{n-1}\}$ 上の置換を引き起こす。

$P_j^\varphi = P_{j_1}, I_i^\varphi = L_{i_1}$ とすると、

$m_{ij} = |P_j \cap l_i| = |(P_j \cap l_i)^\varphi| = |P_j^\varphi \cap l_i^\varphi| = |P_{j_1} \cap L_{i_1}| = (P_{j_1} L_{i_1}) = m_{i_1 j_1}$

こうして、 φ は $L = (l_{ij})_{0 \leq i, j \leq \frac{n^2}{m}-1}$ の行と列に関して置換を引き起こす。従って、 φ は S の自己同型を引き起こす。この自己同型を $\bar{\varphi}$ とかくことにする。

§2 位数 16 の collineation group をもつ位数 12 の射影平面

仮定 2.1 H を位数 12 の射影平面 $\Pi = (P, \mathcal{L})$ の位数 16 の collineation group とする。

補題 2.2 H は cyclic または generalized quaternion group である。

証明 $Z_2 \times Z_2 \not\leq H$ ゆえ言える。 □

$G \leq Z(H), |G| = 2, G = \langle \varphi \rangle$ とする。

G は H の正規部分群。

G は elation group である。

G の center を P_0 、axis を l_0 とする。

$(P_0) = \{l_0, l_1, \dots, l_{12}\}, (l_0) = \{P_0, P_1, \dots, P_{12}\}$ とする。

P_0, P_1, \dots, P_{84} を \mathcal{P} の G -orbits、

L_0, L_1, \dots, L_{84} を \mathcal{L} の G -orbits とする。

ここで

$$\mathcal{P}_i = \{P_i\}, \mathcal{L}_i = \{l_i\} \quad (0 \leq i \leq 12)$$

$$|\mathcal{P}_i| = |\mathcal{L}_i| = 2 \quad (13 \leq i \leq 84)$$

$$(l_i) = \mathcal{P}_{6(i-1)+13} \cup \mathcal{P}_{6(i-1)+14} \cup \cdots \cup \mathcal{P}_{6(i-1)+18} \\ = \mathcal{P}_{6i+7} \cup \mathcal{P}_{6i+8} \cup \cdots \cup \mathcal{P}_{6i+12} \quad (1 \leq i \leq 12)$$

$$(P_i) = \mathcal{L}_{6i+7} \cup \mathcal{L}_{6i+8} \cup \cdots \cup \mathcal{L}_{6i+12} \quad (1 \leq i \leq 12)$$

$$M = (m_{ij})_{0 \leq i, j \leq 84}, \quad m_{ij} = (P_j \mathcal{L}_i)$$

$$L = (m_{ij})_{13 \leq i, j \leq 84} = (l_{ij})_{0 \leq i, j \leq 71}$$

$13 \leq i, j \leq 84$ に対して、 $P_j \in \mathcal{P}_j$, $l_i \in \mathcal{L}_i$ を選ぶ。

$$D_{ij} = \{\mu \in G \mid P_{ij}^\mu \in (l_i)\} \quad (13 \leq i, j \leq 84)$$

$$|D_{ij}| = m_{ij} = 0 \text{ or } 1$$

• $0 \leq i, i' \leq 71$ とする。このとき

$$\sum_{0 \leq j \leq 71} l_{ij} l_{i'j} = \begin{cases} 12 & \text{if } i = i', \\ 0 & \text{if } i \neq i', \{i, i'\} \subseteq \{6k, 6k+1, \dots, 6k+5\} \text{ for some } 0 \leq k \leq 11, \\ 2 & \text{otherwise} \end{cases}$$

• $0 \leq j, j' \leq 71$ とする。このとき

$$\sum_{0 \leq i \leq 71} l_{ij} l_{ij'} = \begin{cases} 12 & \text{if } j = j', \\ 0 & \text{if } j \neq j', \{j, j'\} \subseteq \{6k, 6k+1, \dots, 6k+5\} \text{ for some } 0 \leq k \leq 11, \\ 2 & \text{otherwise} \end{cases}$$

• $l_{ij} = 0 \text{ or } 1$

$$\bullet L = \begin{pmatrix} L_{00} & L_{01} & \cdots & L_{011} \\ L_{10} & L_{11} & \cdots & L_{111} \\ \vdots & \vdots & \cdots & \vdots \\ L_{110} & L_{111} & \cdots & L_{1111} \end{pmatrix} \text{とおく。}$$

ここで、各 L_{ij} は 6 次の正方行列とすると、各 L_{ij} は 6 次の置換行列になる。

• I を 6 次の単位行列、 J を 6 次の全 1 正方行列とすると、

$$L'L = {}^tLL = \begin{pmatrix} 12I & 2J & \cdots & 2J & 2J \\ 2J & 12I & \cdots & 2J & 2J \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 2J & 2J & \cdots & 2J & 12I \end{pmatrix}$$

• 結合構造 $S = (Q, B, I)$ を次のように定義する。

$$Q = \{Q_0, Q_1, \dots, Q_{71}\}, B = \{B_0, B_1, \dots, B_{71}\}$$

$0 \leq i, j \leq 71$ に対して、

$$B_i I Q_j \iff l_{ij} = 1$$

$0 \leq i \leq 11$ に対して、

$$\mathcal{Q}_i = \{Q_{6i}, Q_{6i+1}, \dots, Q_{6i+5}\}$$

$$\mathcal{B}_i = \{B_{6i}, B_{6i+1}, \dots, B_{6i+5}\} \text{ とおく。}$$

• $S = (\mathcal{Q}, \mathcal{B}, I)$ は 12 points classes $\mathcal{Q}_0, \mathcal{Q}_1, \dots, \mathcal{Q}_{11}$ と 12 block classes $\mathcal{B}_0, \mathcal{B}_1, \dots, \mathcal{B}_{11}$ をもつ symmetric $(12, 6, 12, 0, 2)$ -divisible design になる。

• $\forall \tau \in H, \tilde{\tau} = \tau G \in H/G = \tilde{H}$ は S に自然に作用する。

補題 2.2 より、次を得る。

補題 2.3 \tilde{H} は位数 8 の cyclic group または dihedral group になる。後者の場合、

$$\tilde{H} = \langle \tilde{\tau}, \tilde{\mu} \mid \tilde{\mu}^{-1} \tilde{\tau} \tilde{\mu} = \tilde{\tau}^{-1}, \tilde{\mu}^2 = 1, \tilde{\tau}^4 = 1 \rangle$$

補題 2.4 \tilde{H} は S の point set \mathcal{Q} 上、block set \mathcal{B} 上、半正則に作用する。

証明 この補題が成り立たないとする。もし、必要ならば Π の dual を考えることにより、

$\exists \tau \in H$ s.t. $\tilde{\tau} \neq 1$, $\tilde{\tau}$ は \mathcal{Q} のある点を固定する。

$\tilde{\tau}$ が Q_0 を固定するとしてよい。

τ は P_{13} を集合として固定する。

$$4 \mid |\langle \tau, G \rangle|$$

$$2 \cdot |\langle \tau, G \rangle_{P_{13}}| = |P_{13}^{\langle \tau, G \rangle}| \cdot |\langle \tau, G \rangle_{P_{13}}| = |\langle \tau, G \rangle|$$

$$\text{故に、} |\langle \tau, G \rangle_{P_{13}}| = \frac{1}{2} |\langle \tau, G \rangle| = 2 \text{ or } 4 \text{ or } 8$$

$$\text{故に、} \exists \mu \in \langle \tau, G \rangle; o(\mu) = 2, P_{13}^\mu = P_{13}$$

$$\mu \neq \varphi$$

$$\text{ここで、} G = \langle \varphi \rangle$$

G は位数 2 の元を 1 つしかもたないので、これは矛盾。 □

§3 H が cyclic のとき

H が位数 16 の cyclic group とする。 $H = \langle \tau \rangle$ とする。 H の作用は次の 4 つの場合のいずれかである。

H の $(P_0) - \{I_0\}$ 上の orbits のサイズと $(I_0) - \{P_0\}$ 上の orbits のサイズは次のようになる。

Case 1 4,4,4 と 4,4,4 である。

Case 2 8,4 と 8,4 である。

Case 3 4,4,4 と 8,4 である。

Case 4 8,4 と 4,4,4 である。

Case 3 は Π の dual を考えれば、Case 4 に帰着される。故に、Case 3 は考えなくてよい。

Case 4 が起こったとする。 τ^4 は l_0 を axis としてもつ位数 4 の elation になる。 τ^4 は F_0 を通る 5 つの lines を固定し、他の 8 個の lines を動かす。これは、矛盾。故に、Case 4 は起こらぬ。

こうして、Case 1 と Case 2 のみを考えればよい。

Case 1 を考える。 τ を単に τ と書くことにする。

$$\begin{aligned} \tau = & (Q_0, Q_6, Q_{12}, Q_{18}, Q_1, Q_7, Q_{13}, Q_{19})(Q_2, Q_8, Q_{14}, Q_{20}, Q_3, Q_9, Q_{15}, Q_{21}) \\ & (Q_4, Q_{10}, Q_{16}, Q_{22}, Q_5, Q_{11}, Q_{17}, Q_{23})(Q_{24}, Q_{30}, Q_{36}, Q_{42}, Q_{25}, Q_{31}, Q_{37}, Q_{43}) \\ & (Q_{26}, Q_{32}, Q_{38}, Q_{44}, Q_{27}, Q_{33}, Q_{39}, Q_{45})(Q_{28}, Q_{34}, Q_{40}, Q_{46}, Q_{29}, Q_{35}, Q_{41}, Q_{47}) \\ & (Q_{48}, Q_{54}, Q_{60}, Q_{66}, Q_{49}, Q_{55}, Q_{61}, Q_{67})(Q_{50}, Q_{56}, Q_{62}, Q_{68}, Q_{51}, Q_{57}, Q_{63}, Q_{69}) \\ & (Q_{52}, Q_{58}, Q_{64}, Q_{70}, Q_{53}, Q_{59}, Q_{65}, Q_{71}) \end{aligned}$$

τ の B における作用も同様である。すなわち、上の τ の Q における作用において、 Q の代わりに B を書けばよい。

Q_0, Q_1, \dots, Q_5 を適当に並びかえて、 $L_{00} = I$ としてよい。 τ の作用があるので、 Q_6, Q_7, \dots, Q_{23} と対応するように並びかえる。

$Q_{24}, Q_{25}, \dots, Q_{29}$ を適当に並びかえて、 $L_{04} = I$ としてよい。 τ の作用があるので、 $Q_{30}, Q_{31}, \dots, Q_{47}$ を対応するように並びかえる。

$Q_{48}, Q_{49}, \dots, Q_{53}$ を適当に並びかえて、 $L_{08} = I$ としてよい。 τ の作用があるので、 $Q_{54}, Q_{55}, \dots, Q_{71}$ を対応するように並びかえる。

$$\begin{pmatrix} a & b & c & d & e & f \\ b & a & d & c & f & e \\ g & h & i & j & k & l \\ h & g & j & i & l & k \\ m & n & o & p & q & r \\ n & m & p & o & r & q \end{pmatrix}$$

なる形の 6 次の置換行列の全体からなる集合を Ω とする。 $|\Omega| = 48$ 。

$$M = \begin{pmatrix} a & b & c & d & e & f \\ b & a & d & c & f & e \\ g & h & i & j & k & l \\ h & g & j & i & l & k \\ m & n & o & p & q & r \\ n & m & p & o & r & q \end{pmatrix} \in \Omega \text{ に対して、 } M^* = \begin{pmatrix} b & a & d & c & f & e \\ a & b & c & d & e & f \\ h & g & j & i & l & k \\ g & h & i & j & k & l \\ n & m & p & o & r & q \\ m & n & o & p & q & r \end{pmatrix}$$

と定義する。

$$(l_{ij})_{0 \leq i \leq 23, 0 \leq j \leq 71} =$$

$$\begin{pmatrix} I & L_{01} & L_{02} & L_{03} & I & L_{05} & L_{06} & L_{07} & I & L_{09} & L_{010} & L_{011} \\ L_{03}^* & I & L_{01} & L_{02} & L_{07}^* & I & L_{05} & L_{06} & L_{011}^* & I & L_{09} & L_{010} \\ L_{02}^* & L_{03}^* & I & L_{01} & L_{06}^* & L_{07}^* & I & L_{05} & L_{010}^* & L_{011}^* & I & L_{09} \\ L_{01}^* & L_{02}^* & L_{03}^* & I & L_{05}^* & L_{06}^* & L_{07}^* & I & L_{09}^* & L_{010}^* & L_{011}^* & I \end{pmatrix}$$

とかける。ここで、 $L_{0j} \in \Omega$ for $j \in \{1, 2, 3, 5, 6, 7, 9, 10, 11\}$ 。

条件を満たす $(l_{ij})_{0 \leq i \leq 23, 0 \leq j \leq 71}$ を、数値計算ソフト Turbo Pascal で探すが無存在であった。

Case 2 を考える。 τ を単に τ と書くことにする。

$$\tau = (Q_0, Q_6, Q_{12}, Q_{18}, Q_{24}, Q_{30}, Q_{36}, Q_{42})$$

$$(Q_1, Q_7, Q_{13}, Q_{19}, Q_{25}, Q_{31}, Q_{37}, Q_{43})$$

$$(Q_2, Q_8, Q_{14}, Q_{20}, Q_{26}, Q_{32}, Q_{38}, Q_{44})$$

$$(Q_3, Q_9, Q_{15}, Q_{21}, Q_{27}, Q_{33}, Q_{39}, Q_{45})$$

$$(Q_4, Q_{10}, Q_{16}, Q_{22}, Q_{28}, Q_{34}, Q_{40}, Q_{46})$$

$$(Q_5, Q_{11}, Q_{17}, Q_{23}, Q_{29}, Q_{35}, Q_{41}, Q_{47})$$

$$(Q_{25}, Q_{54}, Q_{60}, Q_{66}, Q_{49}, Q_{55}, Q_{61}, Q_{67})$$

$$(Q_{50}, Q_{56}, Q_{62}, Q_{68}, Q_{51}, Q_{57}, Q_{63}, Q_{69})$$

$$(Q_{52}, Q_{58}, Q_{64}, Q_{70}, Q_{53}, Q_{59}, Q_{65}, Q_{71})$$

τ の B における作用も同様である。すなわち上の τ の Q における作用において、 Q の代わりに B を書けばよい。 $L_{80} = L_{88} = I$ としてよい。

$$(l_{ij})_{0 \leq i, j \leq 71} = (L_{ij})_{0 \leq i, j \leq 11} =$$

$$\begin{pmatrix} L_{00} & L_{01} & L_{02} & L_{03} & L_{04} & L_{05} & L_{06} & L_{07} & L_{08} & L_{09} & L_{010} & L_{011} \\ L_{07} & L_{00} & L_{01} & L_{02} & L_{03} & L_{04} & L_{05} & L_{06} & L_{011}^* & L_{08} & L_{09} & L_{010} \\ L_{06} & L_{07} & L_{00} & L_{01} & L_{02} & L_{03} & L_{04} & L_{05} & L_{010}^* & L_{011}^* & L_{08} & L_{09} \\ L_{05} & L_{06} & L_{07} & L_{00} & L_{01} & L_{02} & L_{03} & L_{04} & L_{09}^* & L_{010}^* & L_{011}^* & L_{08} \\ L_{04} & L_{05} & L_{06} & L_{07} & L_{00} & L_{01} & L_{02} & L_{03} & L_{08}^* & L_{09}^* & L_{010}^* & L_{011}^* \\ L_{03} & L_{04} & L_{05} & L_{06} & L_{07} & L_{00} & L_{01} & L_{02} & L_{011} & L_{08}^* & L_{09}^* & L_{010}^* \\ L_{02} & L_{03} & L_{04} & L_{05} & L_{06} & L_{07} & L_{00} & L_{01} & L_{010} & L_{011} & 0L_8^* & L_{09}^* \\ L_{01} & L_{02} & L_{03} & L_{04} & L_{05} & L_{06} & L_{07} & L_{00} & L_{09} & L_{010} & L_{011} & L_{08}^* \\ I & L_{81} & L_{82} & L_{83} & L_{80}^* & L_{81}^* & L_{82}^* & L_{83}^* & I & L_{89} & L_{810} & L_{811} \\ L_{83}^* & I & L_{81} & L_{82}^* & L_{83} & L_{80}^* & L_{81}^* & L_{82}^* & L_{811}^* & I & L_{89} & L_{810} \\ L_{82}^* & L_{83}^* & I & L_{81} & L_{82} & L_{83} & L_{80}^* & L_{81}^* & L_{810}^* & L_{811}^* & I & L_{89} \\ L_{81}^* & L_{82}^* & L_{83}^* & I & L_{81} & L_{82} & L_{83} & L_{80}^* & L_{89}^* & L_{810}^* & L_{811}^* & I \end{pmatrix}$$

$$\text{ここで, } L_{ij} = \begin{pmatrix} a & b & c & d & e & f \\ g & h & i & j & k & l \\ m & n & o & p & q & r \\ s & t & u & v & w & x \\ a_1 & b_1 & c_1 & d_1 & e_1 & f_1 \\ g_1 & h_1 & i_1 & j_1 & k_1 & l_1 \end{pmatrix} \text{ に対して } L_{ij}^* = \begin{pmatrix} g & h & i & j & k & l \\ a & b & c & d & e & f \\ s & t & u & v & w & x \\ m & n & o & p & q & r \\ g_1 & h_1 & i_1 & j_1 & k_1 & l_1 \\ a_1 & b_1 & c_1 & d_1 & e_1 & f_1 \end{pmatrix}$$

である。また、 $L_{89}, L_{810}, L_{811} \in \Omega$ である。 $(\Omega$ は Case 1 で定義したものである。) 条件を満たす $(L_{ij})_{8 \leq i \leq 11, 0 \leq j \leq 11}$ があるかどうか Turbo Pascal で調べるが非存在であった。以上より、次の定理を得る。

定理 π を位数 12 の射影平面で、 H を位数 16 の π の自己同型群とすると H は位数 16 の generalized quaternion group である。

注意 H が位数 16 の generalized quaternion group のときは、対応する symmetric $(12, 6, 12, 0, 2)$ -design のタイプが多くて計算が大変であるが、対応する symmetric $(12, 6, 12, 0, 2)$ -design が存在しないことを示すことにより、起こらないことが、今年中には言えそうである。

参考文献

- [1] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, *Canad. J. Math* **1**(1949), 88-93.
- [2] K. Horvatic-Baldasar, E. Kramer and I. Matulic-Bedenic, On full collineation group of projective planes of order 12, *Punime Mat.* **2**(1987), 9-11.
- [3] Z. Janko and T. van Trung, Projective plane of order 12 do not have a four group as a collineation group, *J. of Combin. Ser. A* **32**(1982), 401-404.

- [4] C. W. H. Lam, L. Thiel and S. Swiercz, The nonexistence of finite projective plane of order 10, *Canad. J. Math* **41**(1989), 1117-1123.
- [5] C. Suetake, Projective planes and divisible designs, *Int. J. Math. Game Theory Algebra* **11**(2001), no.6, 15-33.

g -th MDS Codes and Matroids

Keisuke SHIROMOTO

Department of Electronics and Informatics

Ryukoku University

Seta, Otsu 520-2194, JAPAN;

`keisuke@rins.ryukoku.ac.jp`

Abstract

In this note, we give a relationship between the generalized Hamming weights for linear codes over finite fields and the rank functions of matroids. We also consider a construction of g -th MDS codes from m -paving matroids.

Keywords: generalized Hamming weights, g -th MDS codes, paving matroids.

1 Introduction

The closed connection between matroid theory and coding theory has been discussed by many researchers. For instance, Greene ([2]) gave a proof of the MacWilliams identity ([4]) for the Hamming weight enumerator of a linear code by using the Tutte polynomial of the corresponding matroid. Barg ([1]) studied the relation between the support weight enumerator of a linear code and the Tutte polynomial of the matroid. In addition, he showed the MacWilliams equation of the support weight enumerator in a simple form. In [7], Rajpal studied paving matroids and the corresponding linear codes.

The generalized Hamming weights of a linear code were introduced by Wei ([10]). The weights are natural extensions of the concept of

minimum Hamming weights of linear codes. Many applications of the generalized Hamming weights are well-known. They are useful in cryptography (cf. [10]), in trellis coding (cf. [3]), etc. The generalized Hamming weights have been determined for binary Hamming codes, MDS codes, Golay codes, Reed-Muller codes and their duals ([10]).

The g -th maximum distance separable (MDS) code was defined by Wei ([10]) as a linear code which meets the generalized Singleton bound on the g -th generalized Hamming weight. In [9], Tsfasman and Vlăduț gave a construction of the codes from algebraic-geometric codes.

In this note, we consider the generalized Hamming weights for the m -paving codes. We also look for a construction of the codes from matroid theory. Then we give some examples of the codes.

2 Notation and Terminology

We begin by introducing matroids, as in [6]. A *matroid* is an ordered pair $M = (E, \mathcal{I})$ consisting of a finite set E and a collection \mathcal{I} of subsets of E satisfying the following three conditions:

- (I1) $\emptyset \in \mathcal{I}$.
- (I2) If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$.
- (I3) If I_1 and I_2 are in \mathcal{I} and $|I_1| < |I_2|$, then there is an element e of $I_2 - I_1$ such that $I_1 \cup e \in \mathcal{I}$.

The members of \mathcal{I} are the *independent sets* of M , and a subset of E that is not in \mathcal{I} is called *dependent*. A minimal dependent set in M is called a *circuit* of M , and a maximal independent set in M is called a *base* of M . For a subset X of E , we define the *rank* of X as follows:

$$r(X) := \max\{|Y| : Y \subseteq X, Y \in \mathcal{I}\}.$$

The *dual matroid* M^* of M is defined as the matroid, the set of bases of which is

$$\{E - B : B \text{ is a base of } M\}.$$

When we denote the rank of M^* by r^* , the following is well-known:

$$r^*(X) = |X| - r(M) + r(E - X).$$

Throughout this note, let \mathbb{F}_q be a finite field of q elements. For an $m \times n$ matrix A over \mathbb{F}_q , if E is the set of column labels of A and \mathcal{I} is the set of subsets X of E for which the multiset of columns labelled by X is linearly independent in the vector space \mathbb{F}_q^m , then $M[A] := (E, \mathcal{I})$ is a matroid and is called *vector matroid* of A (cf. [6]).

For a vector $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ and a subset $D \subseteq \mathbb{F}_q^n$, we define the *supports* of \mathbf{x} and D respectively as follows:

$$\begin{aligned} \text{supp}(\mathbf{x}) &:= \{i \mid x_i \neq 0\}, \\ \text{Supp}(D) &:= \bigcup_{\mathbf{x} \in D} \text{supp}(\mathbf{x}). \end{aligned}$$

Let C be an $[n, k]$ code over \mathbb{F}_q . For each g , $1 \leq g \leq k$, the g -th *generalized Hamming weight* (GHW) $d_g(C)$ is defined by Wei ([10]) as follows:

$$d_g(C) := \min\{|\text{Supp}(D)| \mid D \text{ is an } [n, g] \text{ subcode of } C\}.$$

The *weight hierarchy* of C is the set of integers $\{d_g(C) \mid 1 \leq g \leq k\}$. The followings were also proved by Wei ([10]):

$$\textit{Monotonicity} \quad : \quad 1 \leq d_1(C) < d_2(C) < \dots < d_k(C) \leq n.$$

$$\textit{Duality} \quad : \quad \text{Let } C^\perp \text{ be the dual code of } C. \text{ Then}$$

$$\{d_g(C) \mid 1 \leq g \leq k\} = \{1, 2, \dots, n\} - \{n+1 - d_{g'}(C^\perp) \mid 1 \leq g' \leq n-k\}.$$

$$\textit{Generalized Singleton bound} \quad : \quad d_g(C) \leq n - k + g.$$

3 GHW and m -Paving Matroids

3.1 a connection

First, we introduce the connection between the generalized Hamming weights of a linear code and matroid theory. It is usual, for studying the relationship between linear codes and matroids, to deal with the matroid of a generator matrix of a linear code ([1], [7], etc.). In this paper, however, we shall study the rank $n - k$ matroid $M[H]$ of a parity-check matrix H of an $[n, k]$ code C to focus on the generalized Hamming weights of C . Since it finds that $M[H]$ is determined by C (not the chosen parity-check matrix H), we shall represent

$M[H] = M_C$. However, a linear code C has more information than the matroid M_C . Indeed, a matroid is the vector matroid of several linear codes. It is also clear that the dual matroid $(M_C)^*$ corresponds to the matroid M_{C^\perp} of the dual code C^\perp .

The following is well-known ([11]).

Proposition 3.1 *Let H be a parity-check matrix for a linear code C over \mathbb{F}_q . Then $d_g(C) = \delta$ if and only if the following two conditions hold:*

- (1) *every set of $\delta - 1$ columns of H has rank $\delta - g$ or more;*
- (2) *there exist δ columns of H with rank $\delta - g$.*

The above result immediately shows the following theorem.

Theorem 3.2 *Let $M_C = M[H]$ be the vector matroid of a parity-check matrix H for an $[n, k]$ code C over \mathbb{F}_q . Then $d_g(C) = \delta$ for a g , $1 \leq g \leq k$, if and only if the following two conditions hold:*

- (1) *for any $(\delta - 1)$ -subset X of $E(M_C)$, $r(X) \geq \delta - g$;*
- (2) *there exists a δ -subset Y of $E(M_C)$ with $r(Y) = \delta - g$.*

Example 3.3 Let M_C be a uniform matroid $U_{n-k, n}$, that is, a matroid on an n -element set E , any $(n - k)$ -element subset of E of which is a base. For any $(n - k + g - 1)$ -element subset X , it follows that $r(X) = n - k$ for every g , $1 \leq g \leq k$. There exists an $(n - k + g)$ -element subset Y such that $r(Y) = n - k$ for every g . Therefore we have that $d_g(C) = n - k + g$ for every g . Consequently it follows that C is an MDS code.

3.2 m -paving matroids

An m -paving matroid was introduced by Rajpal ([8]) and the matroid is a generalization of a paving matroid, that is, a rank r matroid whose circuits have cardinality r or $r + 1$.

Definition 3.4 A rank r matroid M is m -paving for $m \leq r$ if all circuits of M have cardinality exceeding $r - m$.

It is not difficult to show that any uniform matroid $U_{r, n}$ is 0-paving, and any paving matroid is 1-paving. These are the only 0-paving and

1-paving matroids. In [8], Rajpal showed that if G is a generator matrix of a first-order Reed-Muller code $R(1, m)$, then the matroid $M[G]$ is a maximal binary $(m - 2)$ -paving matroid.

For $m \leq n - k$, we define an m -paving code as an $[n, k]$ code C over \mathbb{F}_q such that the matroid M_C is an m -paving. From the above argument, it is clear that the dual code $R(m - 2, m)$ of a Reed-Muller code $R(1, m)$ is an $(m - 2)$ -paving code.

The following result indicates the minimum Hamming weight of a paving code.

Proposition 3.5 ([7]) *For a parity-check matrix H of an $[n, k]$ code C , if $M[H]$ is a 1-paving matroid, then the minimum Hamming weight of C is $n - k$ or $n - k + 1$.*

On the generalized Hamming weights of an m -paving code, we shall prove a bound which is a generalization of the above result.

Theorem 3.6 *If an $[n, k]$ code C over \mathbb{F}_q is an m -paving code, then*

$$d_g(C) \geq n - k + g - m \quad (1)$$

for any g , $1 \leq g \leq k$.

We remark that the bound (1) contains Proposition 3.5 because the bound corresponds to $d_1(C) \geq n - k$ for a 1-paving code C . Combining the above bound and the generalized Singleton bound, we note that if C is a m -paving code, then $d_g(C) = n - k + g - m$ or $n - k + g - m + 1$ or, \dots , or $n - k + g$.

3.3 g -th MDS codes

We consider a special class of linear codes defined as follows:

Definition 3.7 ([10]) *Let C be an $[n, k]$ code over \mathbb{F}_q . For g , C is called a g -th MDS code if $d_g(C) = n - k + g$.*

It is well-known that an MDS code is also a g -MDS code for any g and a g -MDS code is always a g' -th MDS code for any g' , $g' \geq g$.

The following proposition is due to Tsfasman and Vlăduț (Corollary 4.1 in [9]).

Proposition 3.8 *If C is an $[n, k, d]$ code and $r = n + 2 - k - d$, then the dual code C^\perp is an r -th MDS code.*

Now we give a construction of g -th MDS codes from m -paving matroids. That also indicates a duality for g -th MDS codes. From Theorem 3.2, it is not difficult to prove the following lemma.

Lemma 3.9 *Let C be an $[n, k]$ code. Then C is a g -th MDS code if and only if $r(X) = n - k$ for any $(n - k + g - 1)$ -element subset $X \subseteq E(M_C)$.*

Theorem 3.10 *Let C be an $[n, k]$ code over \mathbb{F}_q . If C is a g -paving code for $0 \leq g \leq \min\{n - k, k - 1\}$, then C^\perp is a $(g + 1)$ -th MDS code.*

Proof. Since M_C is a g -paving matroid, it follows that $|A| \geq (n - k) - g + 1$ for any circuit A of M_C . If we take any $(k + g)$ -element subset X of $E := E(M_C) = E(M_{C^\perp})$, then we have that

$$\begin{aligned} r^*(X) &= |X| - r(M_C) + r(E - X) \\ &= (k + g) - (n - k) + (n - k - g) \\ &= k. \end{aligned}$$

From Lemma 3.9, it follows that C^\perp is a $(g + 1)$ -th MDS code. The theorem follows. \square

Let P , Q and R be the following binary matrices:

$$P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$

$$R = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

In [8], it is showed that the matroids $M[P]$, $M[Q]$ and $M[R]$ are the only binary maximal 2-paving matroids of rank 5. From Theorem 3.10, we have the following result.

Corollary 3.11 *The binary codes whose generator matrices are P , Q and R are the binary third MDS codes.*

The following proposition is mentioned in [9] (Corollary 4.1) as a construction of g -th MDS codes. We can also give a proof for the result by using Theorem 3.10. That means Theorem 3.10 is a generalization of the following proposition.

Corollary 3.12 ([9]) *For an $[n, k, d]$ code C and $g = n + 2 - k - d$, the dual code C^\perp is a g -th MDS code.*

Proof. We set $g' = n + 1 - k - d$. Since the minimum Hamming weight d corresponds to the minimum order of curcuits in M_C , we have that $|A| \geq (n - k) - g' + 1 = d$ for any curcuit A . So C is a g' -paving code. Therefore it follows, from Theorem 3.10, that C^\perp is a $(g' + 1)$ -th MDS code. \square

Now we give a characterization of a generator matrix of a g -th MDS code.

Corollary 3.13 *Let G be a generator matrix of an $[n, k]$ code C over \mathbb{F}_q . For a g , $1 \leq g \leq \min\{n - k, k - 1\}$, C is a g -th MDS code if and only if the matroid $M[G]$ is a $(g - 1)$ -paving matroid.*

References

- [1] A. Barg, The matroid of supports of a linear code, *Applicable Algebra in Engineering, Communication and Computing*, 8 (1997) pp. 165–172.

- [2] C. Greene, Weight enumeration and the geometry of linear codes, *Studies in Applied Mathematics* **55** (1976) pp. 119–128.
- [3] T. Kasami, T. Tanaka, T. Fujiwara and S. Lin, On the optimum bit orders with respect to the state complexity of trellis diagrams for binary linear codes, *IEEE Trans. Inform. Theory* **39** (1993) pp. 242–245.
- [4] F. J. MacWilliams, A theorem on the distribution of weights in systematic code, *Bell Syst. Tech. J.* **42** (1962) 654.
- [5] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam 1977.
- [6] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.
- [7] S. Rajpal, On paving matroids and a generalization of MDS codes, *Discrete Applied Mathematics* **60** (1995) pp. 343–347.
- [8] S. Rajpal, On binary k -paving matroids and Reed-Muller codes, *Discrete Mathematics* **190** (1998) pp. 191–200.
- [9] M. A. Tsfasman and S. G. Vlăduț, Geometric approach to higher weights, *IEEE Trans. Inform. Theory* **41** (1995) pp. 1564–1588.
- [10] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37** (1991) pp. 1412–1418.
- [11] V. Wei, Generalized Hamming weights; Fundamental open problems in coding theory, *Arithmetic, geometry and coding theory* (Luminy, 1993) pp. 269–281.
- [12] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

Extendability of linear codes over finite fields

Tatsuya Maruta

Department of Information Systems, Aichi Prefectural University

(愛知県立大学 情報科学部 丸田辰哉)

Nagakute, Aichi 480-1198, Japan

E-mail: maruta@ist.aichi-pu.ac.jp

Abstract

We survey classical known results and recent new results about extendability of linear codes over finite fields. The geometric method used to prove most of recent results is also shown.

1. Extension theorems and their applications

Let C be an $[n, k, d]_q$ code, that is a linear code over $\text{GF}(q)$ of length n with dimension k whose minimum Hamming distance is d , where $\text{GF}(q)$ stands for the finite field of order q . The weight distribution of C is the list of numbers A_i which is the number of codewords of C with weight i . The weight distribution with $(A_0, A_d, \dots) = (1, \alpha, \dots)$ is also expressed as $0^1 d^\alpha \dots$. We only consider *non-degenerate* codes having no coordinate which is identically zero. Two $[n, k, d]_q$ codes C_1 and C_2 are *equivalent* if there exists a monomial matrix M with entries in $\text{GF}(q)$ such that C_2 coincides with $C_1 M = \{cM \mid c \in C_1\}$.

The code obtained by deleting the same coordinate from each codeword of C is called a *punctured code* of C . If there exists an $[n+1, k, d+1]_q$ code C' which gives C as a punctured code, C is called *extendable* (to C') and C' is an *extension* of C . C is *doubly extendable* if there exists an extension of C which is also extendable. In this section we survey known results about extendability of linear codes over $\text{GF}(q)$.

Obviously every $[n, 1, d]_q$ code is extendable. And an $[n, 2, d]_q$ code C is not extendable iff $n = s(q+1)$ and $d = sq$ for some integer s ([8]). It is well known that every $[n, k, d]_2$ code with d odd is extendable by adding an overall parity check. So, we mainly consider non-binary linear codes with dimension $k \geq 3$.

The following theorems are generalizations of the fact that every binary linear code with odd minimum distance is extendable.

Theorem 1.1 ([4],[5]). *Let C be an $[n, k, d]_q$ code with $\gcd(d, q) = 1$ such that $i \equiv 0$ or $d \pmod{q}$ for all i with $A_i > 0$. Then C is extendable.*

Theorem 1.2 ([12]). *Let C be an $[n, k, d]_q$ code with $\gcd(d, q) = 1$, $q = p^h$, p prime. Then C is extendable if*

$$\sum_{i \not\equiv d \pmod{p}} A_i = q^{k-1}.$$

Theorem 1.1 was first proved for ternary linear codes by van Eupen and Lisonek [2] using quadratic forms. Extension theorems can be used to construct new codes from old ones or to prove the nonexistence of some linear codes.

- Example 1.1.** (1) $[q^2, 4, q^2 - q - 1]_q$ codes are extendable by Theorem 1.1 (see [4]).
 (2) The Golay $[11, 6, 5]_3$ code has the unique weight distribution $0^1 5^{132} 6^{132} 8^{330} 9^{110} 11^{24}$ and is extendable by Theorem 1.1.
 (3) A $[52, 7, 33]_4$ code found by Gulliver with weight distribution

$$0^1 33^{936} 34^{468} 35^{1443} 36^{936} 37^{1991} 38^{468} 39^{2850} 40^{741} 41^{3237} 42^{1248} 43^{1443} 44^{234} 45^{429} 49^{39}$$

is extendable by Theorem 1.2.

- (4) It is not so difficult to prove the nonexistence of $[406, 5, 304]_4$ codes but for $[405, 5, 303]_4$ codes. If a $[405, 5, 303]_4$ code exists, then it can be shown that $A_j = 0$ for all $j \notin \{303, 304, 319, 320\}$. So such a code doesn't exist by Theorem 1.1.

We pose the following conjecture improving Theorem 1.2:

Conjecture. Let C be an $[n, k, d]_q$ code with $\gcd(d, q) = 1$, $q = p^h$, p prime. Then C is extendable if

$$\sum_{i \not\equiv d \pmod{p}} A_i < q^{k-2}(2q-1).$$

Simonis, who originally proved Theorem 1.2, also showed that the above conjecture is true for $q = 3, 4$ ([12]). The next theorem partially corroborates our conjecture.

Theorem 1.3 ([9]). *The conjecture is true when:*

- (1) $h = 1$ (i.e. q is prime),
- (2) $q = 4$,
- (3) $h = 2$ with $n \equiv 0, d \equiv -1 \pmod{p}$, or
- (4) $h = 2$ with $n \equiv d \equiv 1 \pmod{p}$ and $A_i = 0$ for all $i \equiv 1 \pmod{p}$, $i \not\equiv n \pmod{q}$.

A $[4, 3, 2]_3$ code has the unique weight distribution $0^1 2^{12} 3^8 4^6$ satisfying $\sum_{i \not\equiv 2 \pmod{3}} A_i = 3(2 \cdot 3 - 1)$ and is not extendable. Hence the condition in our conjecture is best possible for $q = 3$.

When $h \geq 3$, we can get the following result.

Theorem 1.4 ([9]). *Let C be an $[n, k, d]_q$ code with $\gcd(d, q) = 1$, $q = p^h$, p prime, $h \geq 3$. Then C is extendable if*

$$\sum_{i \not\equiv d \pmod{p^{h-1}}} A_i < q^{k-2}(2q-1).$$

Let C be an $[n, k, d]_q$ code with $k \geq 3$, $\gcd(d, q) = 1$. Define

$$\Phi_0 = \frac{1}{q-1} \sum_{q \mid i, i \neq 0} A_i, \quad \Phi_1 = \frac{1}{q-1} \sum_{i \not\equiv 0, d \pmod{q}} A_i.$$

We call the pair (Φ_0, Φ_1) the *diversity* of \mathcal{C} . Theorem 1.1 implies that every $[n, k, d]_q$ code with $\gcd(d, q) = 1$ is extendable if $\Phi_1 = 0$. When $d \equiv -1 \pmod{q}$, there are many linear codes satisfying $A_i = 0$ for all $i \not\equiv 0, -1 \pmod{q}$, which are extendable by Theorem 1.1 (e.g. Example 1.1 (1), (2)). The following theorem is a stronger result than Theorem 1.1 when $d \equiv -2 \pmod{q}$.

Theorem 1.5 ([10]). *Let \mathcal{C} be an $[n, k, d]_q$ code with diversity (Φ_0, Φ_1) , $k \geq 3$, $d \equiv -2 \pmod{q}$ such that $A_i = 0$ for all $i \not\equiv 0, -1, -2 \pmod{q}$ for odd $q \geq 5$. Then*

- (1) \mathcal{C} is extendable.
- (2) $(\Phi_0, \Phi_1) \in \{(\theta_{k-2}, 0), (\theta_{k-3}, 2q^{k-2}), (\theta_{k-2} + (\rho - 2)q^{k-2}, 2q^{k-2})\} \cup \{(\theta_{k-2} + iq^{k-2}, (q - 2i)q^{k-2}) \mid 1 \leq i \leq \rho - 1\}$, where $\theta_j = (q^{j+1} - 1)/(q - 1)$, $\rho = \theta_1/2$.
- (3) \mathcal{C} is doubly extendable if $(\Phi_0, \Phi_1) \neq (\theta_{k-2} + (\rho - 2)q^{k-2}, 2q^{k-2})$.

Example 1.2. (1) Let \mathcal{C} be a $[q^2 - 1, 4, q^2 - q - 2]_q$ code with odd $q \geq 5$. Then it can be easily verified that $A_i = 0$ for all $i \notin \{q^2 - q - 2, q^2 - q - 1, q^2 - q, q^2 - 2, q^2 - 1\}$. Hence, applying Theorem 1.5, \mathcal{C} is extendable. Actually \mathcal{C} is doubly extendable since every $[q^2, 4, q^2 - q - 1]_q$ code is also extendable.

(2) Let \mathcal{C} be a $[q, 3, q - 2]_q$ code with odd $q \geq 5$. Since \mathcal{C} is MDS, the weight distribution is uniquely determined with diversity $(\theta_1 + (\rho - 2)q, 2q)$. Applying Theorem 1.5, \mathcal{C} is extendable. But it is well known that \mathcal{C} is not doubly extendable (there is no $[q + 2, 3, q]_q$ code).

(3) $[q^{k-2} - 2, k, q^{k-1} - q^{k-2} - 2]_q$ codes are doubly extendable (diversity $(\theta_{k-3}, 2q^{k-2})$).

(4) Applying Theorem 1.5, the nonexistence of codes with parameters $[105, 4, 83]_5$ and $[205, 4, 163]_5$ was recently proved ([7]).

For an $[n, k, d]_q$ code \mathcal{C} with a generator matrix G , the *residual code of \mathcal{C} with respect to a codeword c* , denoted by $\text{Res}(\mathcal{C}, c)$, is the code generated by the restriction of G to the columns where c has a zero entry. The next theorem is the only one with the condition $q|d$ for general k .

Theorem 1.6 ([8]). *An $[n, k, d]_q$ code \mathcal{C} is not extendable if q divides d and if $\text{Res}(\mathcal{C}, c)$ is an $[n - d, k - 1, d/q]_q$ code for some $c \in \mathcal{C}$ of weight d .*

In Section 2 we give a survey of recent results about the extendability of ternary linear codes. In Section 3 we give a geometric method used to prove most of the results obtained by the author. A geometrical proof of Theorems 1.1 and 1.2 is also given to demonstrate our approach.

2. Extendability of ternary linear codes

In this section we give a survey of known results about the extendability of ternary linear codes from [11].

Theorem 2.1. *Let \mathcal{C} be an $[n, 3, d]_3$ code with diversity (Φ_0, Φ_1) , $\gcd(3, d) = 1$. Then*

- (1) $(\Phi_0, \Phi_1) \in \{(4, 0), (1, 6), (4, 3), (4, 6), (7, 3)\}$.
- (2) \mathcal{C} is extendable if $(\Phi_0, \Phi_1) \in \{(4, 0), (1, 6), (4, 6), (7, 3)\}$.

(3) \mathcal{C} is extendable iff $\sum_{d < i \equiv d \pmod{3}} A_i > 0$ when $(\Phi_0, \Phi_1) = (4, 3)$.

Example 2.1. (1) $[3, 3, 1]_3$ codes are unique up to equivalence. A $[3, 3, 1]_3$ code is extendable, for the weight distribution is $0^1 1^{62} 1^2 3^8$ (diversity $(4, 6)$).

(2) There are two $[24, 3, 16]_3$ codes up to equivalence ([2]). One with weight distribution $0^1 16^{12} 17^{12} 18^2$ has diversity $(1, 6)$ and the other with weight distribution $0^1 16^{18} 18^8$ has diversity $(4, 0)$.

(3) There are three $[16, 3, 10]_3$ codes with diversity $(4, 3)$ up to equivalence ([2]). The codes with weight distribution $0^1 10^{12} 11^4 12^8 14^2$ or $0^1 10^{12} 11^6 12^6 15^2$ are not extendable but the one with weight distribution $0^1 10^{10} 11^6 12^8 13^2$ is extendable.

Theorem 2.2. Let \mathcal{C} be an $[n, 4, d]_3$ code with diversity (Φ_0, Φ_1) , $\gcd(3, d) = 1$. Then

(1) $(\Phi_0, \Phi_1) \in \{(13, 0), (4, 18), (13, 9), (10, 15), (16, 12), (13, 18), (22, 9)\}$.

(2) \mathcal{C} is extendable if $(\Phi_0, \Phi_1) \in \{(13, 0), (4, 18), (13, 18), (22, 9)\}$.

(3) \mathcal{C} is not extendable if $\sum_{d < i \equiv d \pmod{3}} A_i < 6$ when $(\Phi_0, \Phi_1) \in \{(13, 9), (10, 15), (16, 12)\}$.

Example 2.2. (1) $[9, 4, 5]_3$ codes are unique up to equivalence. A $[9, 4, 5]_3$ code is extendable, for the weight distribution is $0^1 5^{36} 6^{24} 8^{18} 9^2$ (diversity $(13, 0)$).

(2) There are three $[8, 4, 4]_3$ codes up to equivalence ([2]). A $[8, 4, 4]_3$ code with weight distribution $0^1 4^{20} 5^{32} 6^8 7^{16} 8^4$ is extendable (diversity $(4, 18)$) but the one with weight distribution $0^1 4^{24} 5^{16} 6^{32} 8^8$ is not extendable (diversity $(16, 12)$, $\sum_{d < i \equiv d \pmod{3}} A_i = 0$).

It can be proved that the other $[8, 4, 4]_3$ code with weight distribution $0^1 4^{22} 5^{24} 6^{20} 7^8 8^6$ (diversity $(10, 15)$, $\sum_{d < i \equiv d \pmod{3}} A_i = 8$) is not extendable.

Theorem 2.3. Let \mathcal{C} be an $[n, 5, d]_3$ code with diversity (Φ_0, Φ_1) , $\gcd(3, d) = 1$. Then

(1) $(\Phi_0, \Phi_1) \in \{(40, 0), (13, 54), (40, 27), (31, 45), (40, 36), (40, 45), (49, 36), (40, 54), (67, 27)\}$.

(2) \mathcal{C} is extendable if $(\Phi_0, \Phi_1) \in \{(40, 0), (13, 54), (40, 54), (67, 27)\}$.

(3) \mathcal{C} is not extendable if $\sum_{d < i \equiv d \pmod{3}} A_i < 18$ when $(\Phi_0, \Phi_1) \in \{(40, 27), (31, 45),$

$(40, 45), (49, 36)\}$.

(4) \mathcal{C} is not extendable if $\sum_{d < i \equiv d \pmod{3}} A_i < 24$ when $(\Phi_0, \Phi_1) = (40, 36)$.

Example 2.3. (1) $[10, 5, 5]_3$ codes are unique up to equivalence. A $[10, 5, 5]_3$ code is extendable, for the weight distribution is $0^1 5^{72} 6^{60} 8^{90} 9^{20}$ (diversity $(40, 0)$).

(2) It can be proved that the $[49, 5, 31]_3$ code found by Bogdanova & Bouklicv ([1]) with weight distribution $0^1 31^{88} 32^{52} 33^{72} 36^8 40^{20} 41^2$ (diversity $(40, 27)$, $\sum_{d < i \equiv d \pmod{3}} A_i = 20$) is not extendable.

Theorem 2.4. Let \mathcal{C} be an $[n, 6, d]_3$ code with diversity (Φ_0, Φ_1) , $\gcd(3, d) = 1$. Then

(1) $(\Phi_0, \Phi_1) \in \{(121, 0), (40, 162), (121, 81), (94, 135), (121, 108), (112, 126), (130, 117), (121, 135), (148, 108), (121, 162), (202, 81)\}$.

(2) \mathcal{C} is extendable if $(\Phi_0, \Phi_1) \in \{(121, 0), (40, 162), (121, 162), (202, 81)\}$.

(3) \mathcal{C} is not extendable if $\sum_{d < i \equiv d \pmod{3}} A_i < 54$ when $(\Phi_0, \Phi_1) \in \{(121, 81), (94, 135),$

$(121, 135), (148, 108)\}$.

(4) \mathcal{C} is not extendable if $\sum_{d < i \equiv d \pmod{3}} A_i < 72$ when $(\Phi_0, \Phi_1) \in \{(121, 108), (112, 126), (130, 117)\}$.

Example 2.4. A $[200, 6, 130]_3$ code found by Gulliver ([3]) is extendable, for the weight distribution is $0^1 130^{144} 131^{224} 132^{64} 133^{112} 134^{32} 139^{32} 140^{64} 142^{32} 144^8 148^4 150^8 152^4$ (diversity (40, 162)). See also Example 2.5.

For general $k \geq 3$, the following theorem can be proved.

Theorem 2.5. Let \mathcal{C} be an $[n, k, d]_3$ code with diversity (Φ_0, Φ_1) , $k \geq 3$, $\gcd(3, d) = 1$.

(1) \mathcal{C} is extendable if $(\Phi_0, \Phi_1) \in \{(\theta_{k-2}, 0), (\theta_{k-3}, 2 \cdot 3^{k-2}), (\theta_{k-2}, 2 \cdot 3^{k-2}), (\theta_{k-2} + 3^{k-2}, 3^{k-2})\}$.

(2) \mathcal{C} is doubly extendable if $(\Phi_0, \Phi_1) \in \{(\theta_{k-2}, 0), (\theta_{k-3}, 2 \cdot 3^{k-2}), (\theta_{k-2} + 3^{k-2}, 3^{k-2})\}$ when $d \equiv 1 \pmod{3}$.

(3) \mathcal{C} is extendable if $\Phi_0 + \Phi_1 < \theta_{k-2} + 3^{k-2}$ or $\Phi_0 + \Phi_1 \geq \theta_{k-2} + 2 \cdot 3^{k-2}$.

Example 2.5. A $[200, 6, 130]_3$ code in Example 2.4 is doubly extendable.

3. A geometric method

We denote by $\text{PG}(r, q)$ the projective geometry of dimension r over $\text{GF}(q)$. A j -flat is a projective subspace of dimension j in $\text{PG}(r, q)$. 0-flats, 1-flats, 2-flats, $(r-2)$ -flats and $(r-1)$ -flats are called *points*, *lines*, *planes*, *secundums* and *hyperplanes* respectively as usual. We denote by \mathcal{F}_j the set of j -flats of $\text{PG}(r, q)$. Note that the number of points in a j -flat is $\theta_j = (q^{j+1} - 1)/(q - 1)$.

Let \mathcal{C} be a non-degenerate $[n, k, d]_q$ code. The columns of a generator matrix of \mathcal{C} can be considered as an n -multiset of $\Sigma = \text{PG}(k-1, q)$ denoted also by \mathcal{C} . We see linear codes from this geometrical point of view. An i -point is a point of Σ which has multiplicity i in \mathcal{C} . Denote by γ_0 the maximum multiplicity of a point from Σ in \mathcal{C} and let C_i be the set of i -points in Σ , $0 \leq i \leq \gamma_0$. For any subset S of Σ we define the *multiplicity of S with respect to \mathcal{C}* , denoted by $m_{\mathcal{C}}(S)$, as

$$m_{\mathcal{C}}(S) = \sum_{i=1}^{\gamma_0} i \cdot |S \cap C_i|,$$

where $|T|$ denotes the number of points in T for a subset T of Σ . Then we obtain the partition $\Sigma = \bigcup_{i=0}^{\gamma_0} C_i$ such that

$$\begin{aligned} n &= m_{\mathcal{C}}(\Sigma), \\ n - d &= \max\{m_{\mathcal{C}}(\pi) \mid \pi \in \mathcal{F}_{k-2}\}. \end{aligned}$$

Conversely such a partition of Σ as above gives an $[n, k, d]_q$ code in the natural manner if there exists no hyperplane including the complement of C_0 in Σ . An f -set F in $\text{PG}(r, q)$ is called an $\{f, m; r, q\}$ -*minihyper* if $m = \min\{|F \cap \Delta| \mid \Delta \in \mathcal{F}_{r-1}\}$. So C_0 forms a $\{\theta_{k-1} - n, \theta_{k-2} - (n - d); k - 1, q\}$ -minihyper when $\gamma_0 = 1$.

Since $(n + 1) - (d + 1) = n - d$, we get the following.

Lemma 3.1. *C is extendable iff there exists a point $P \in \Sigma$ such that $m_C(\pi) < n - d$ for all hyperplanes π through P .*

Let Σ^* be the dual space of Σ (considering \mathcal{F}_{k-2} as the set of points of Σ^*). Then Lemma 3.1 is equivalent to the following:

Lemma 3.2. *C is extendable iff there exists a hyperplane Π of Σ^* such that*

$$\Pi \subset \{\pi \in \mathcal{F}_{k-2} \mid m_C(\pi) < n - d\}.$$

From now on, let C be an $[n, k, d]_q$ code with $\gcd(q, d) = 1$. We denote by \mathcal{F}_j^* the set of j -flats of Σ^* , so $\mathcal{F}_j^* = \mathcal{F}_{k-2-j}$, $0 \leq j \leq k - 2$. We define

$$\begin{aligned} F &= \{\pi \in \mathcal{F}_{k-2} \mid m_C(\pi) \not\equiv n - d \pmod{q}\}, \\ F_0 &= \{\pi \in \mathcal{F}_{k-2} \mid m_C(\pi) \equiv n \pmod{q}\}, \\ F_1 &= F \setminus F_0. \end{aligned}$$

Note that $\Phi_0 = |F_0|$, $\Phi_1 = |F_1|$. Then F forms a *blocking set* in Σ^* with respect to lines which meets every line in Σ^* .

Lemma 3.3. *$F \cap L \neq \emptyset$ for all $L \in \mathcal{F}_1^*$.*

Proof. Suppose $F \cap L = \emptyset$, $L = \{\pi_0, \dots, \pi_q\} \in \mathcal{F}_1^*$. Then π_0, \dots, π_q are the hyperplanes through $L \in \mathcal{F}_{k-3}$ in Σ with $m_C(\pi_i) \equiv n - d \pmod{q}$. Since $\sum_{i=0}^q (m_C(\pi_i) - m_C(L)) + m_C(L) = n$, we get $n - d \equiv n \pmod{q}$. This contradicts that $\gcd(d, q) = 1$.

Most of the theorems presented in Section 1 can be proved investigating the geometrical structure of F . We give elementary proofs of Theorems 1.1 and 1.2 from our geometrical point of view. Note that $|\{\pi \in \mathcal{F}_{k-2} \mid m_C(\pi) = i\}| = A_{n-i}/(q-1)$ ($0 \leq i \leq n - d$). So, the condition " $i \equiv 0$ or $d \pmod{q}$ for all i with $A_i > 0$ " in Theorem 1.1 is equivalent to " $m_C(\pi) \equiv n$ or $n - d \pmod{q}$ for all $\pi \in \mathcal{F}_{k-2}$ ".

The following lemmas give characterizations of hyperplanes. Let S be a proper subset of $\Sigma = \text{PG}(r, q)$.

Lemma 3.4. *S is a hyperplane of Σ iff every line in Σ meets S in one point or in $q + 1$ points.*

Proof. Assume that every line in Σ meets S in one point or in $q + 1$ points. Let l_0 be a line in Σ . Then we can find a point $Q_0 \in F$ on l_0 . Let δ_{j-1} be a $(j - 1)$ -flat included in S , $1 \leq j \leq r - 1$. Taking a line l_j which is skew to δ_{j-1} , we can get a point $Q_j \in S$ (on l_j) not on δ_{j-1} . Since every line through Q_j and a point of δ_{j-1} meets S in $q + 1$ points, we get $\delta_j = \langle Q_j, \delta_{j-1} \rangle \in \mathcal{F}_j$ included in S . Inductively, we get a hyperplane δ_{r-1} included in S . If a point $Q \in S$ not in δ_{r-1} exists, then we have $S = \langle Q, \delta_{r-1} \rangle = \Sigma$, a contradiction. Hence we obtain $S = \delta_{r-1}$. The converse is trivial. \square

Lemma 3.5 ([6]). *S is a hyperplane of Σ iff $|S| = \theta_{r-1}$ and S is a blocking set with respect to lines in Σ .*

Proof of Theorem 1.1. By the condition we have $F_1 = \emptyset$, so $F = \{\pi \in \mathcal{F}_{k-2} \mid m_{\mathcal{C}}(\pi) \equiv n \pmod{q}\}$. Take a secandum δ in $\Sigma = \text{PG}(k-1, q)$ with $m_{\mathcal{C}}(\delta) = t$. Let a be the number of hyperplanes in F through δ and let b be the number of the other hyperplanes of Σ through δ . Then we have $a + b = q + 1 \equiv 1 \pmod{q}$ and $(n-t)a + (n-d-t)b + t \equiv n \pmod{q}$, so that $d(a-1) \equiv 0 \pmod{q}$. Since $\gcd(d, q) = 1$, we obtain $a \equiv 1 \pmod{q}$, whence $a = 1$ or $q + 1$. This implies that every line in the dual space Σ^* meets F in one point or $q + 1$ points. Applying Lemma 3.4, F forms a hyperplane of Σ^* , whence \mathcal{C} is extendable by Lemma 3.2. \square

Proof of Theorem 1.2. We put

$$F' := \{\pi \in \mathcal{F}_{k-2} \mid m_{\mathcal{C}}(\pi) \not\equiv n - d \pmod{p}\}.$$

Since $F \subset F'$, F' forms a blocking set with respect to lines by Lemma 3.3. The assumption $\sum_{i \neq d \pmod{p}} A_i = q^{k-1}$ implies that $|F'| = \theta_{k-2}$. It follows from Lemma 3.5 that F' is a hyperplane of Σ^* , whence \mathcal{C} is extendable by Lemma 3.2. \square

References

- [1] G. T. Bogdanova and I. G. Bouklev, New linear codes of dimension 5 over $\text{GF}(3)$, in: Proc. 4th Intern. Workshop on Algebraic and Combinatorial Coding Theory, Novgorod, Russia (1994), 41-43.
- [2] M. van Eupen and P. Lisonek, Classification of some optimal ternary linear codes of small length, *Des. Codes Cryptogr.* **10** (1997), 63-84.
- [3] T.A. Gulliver, personal communications (2001).
- [4] R. Hill, An extension theorem for linear codes, *Des. Codes Cryptogr.* **17** (1999), 151-157.
- [5] R. Hill and P. Lizak, Extensions of linear codes, Proc. IEEE Int. Symposium on Inform. Theory (Whistler, Canada, 1995), pp. 345.
- [6] J.W.P. Hirschfeld, Projective geometries over finite fields 2nd ed., Clarendon Press, Oxford, 1998.
- [7] I. Landjev, A. Rouseva, T. Maruta, R. Hill, On optimal codes over the field with five elements, submitted.
- [8] T. Maruta, On the extendability of linear codes, *Finite Fields and Their Appl.* **7** (2001), 350-354.
- [9] T. Maruta, Extendability of linear codes over $\text{GF}(q)$ with minimum distance d , $\gcd(d, q) = 1$, submitted.
- [10] T. Maruta, A new extension theorem for linear codes, submitted.
- [11] T. Maruta, Extendability of ternary linear codes, preprint.
- [12] J. Simonis, Adding a parity check bit, *IEEE Trans. Inform. Theory* **46** (2000) 1544-1545.

On Association Schemes with A. V. Ivanov's Condition

神戸学院女子短期大学
生田 卓也

1 定義と準備

X を位数 n の有限集合とする. $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ をクラス d の symmetric association schemes とする.

A_i を R_i に対する隣接行列とする. $\mathcal{A} = \langle A_0, A_1, \dots, A_d \rangle$ を実数体 \mathbf{R} 上の algebra とする. \mathcal{A} を association scheme $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ の Bose-Mesner algebra と呼ぶ. $\{E_i\}_{0 \leq i \leq d}$ を \mathcal{A} の primitive idempotents の集合とする ($E_0 = \frac{1}{n}J$).

$$(A_0, A_1, \dots, A_d) = (E_0, E_1, \dots, E_d) \cdot P$$

で表されるサイズ $d+1$ の正方行列 P を $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ の 1st eigenmatrix と呼ぶ. 一方,

$$(E_0, E_1, \dots, E_d) = \frac{1}{n}(A_0, A_1, \dots, A_d) \cdot Q$$

で表されるサイズ $d+1$ の正方行列 Q を $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ の 2nd eigenmatrix Q と呼ぶ.

P, Q の形は次の通りである:

$$P = (p_{ij})_{\substack{0 \leq i \leq d \\ 0 \leq j \leq d}} = \begin{pmatrix} 1 & k_1 & \dots & k_d \\ 1 & & & \\ \vdots & & p_{ij} & \\ 1 & & & \end{pmatrix}, \quad k_i \text{ は } R_i \text{ の valency.}$$

$$Q = (q_{ij})_{\substack{0 \leq i \leq d \\ 0 \leq j \leq d}} = \begin{pmatrix} 1 & m_1 & \dots & m_d \\ 1 & & & \\ \vdots & & q_{ij} & \\ 1 & & & \end{pmatrix}, \quad m_i = \text{rank } E_i.$$

P の行と列は各々 $\{E_i\}_{0 \leq i \leq d}, \{A_i\}_{0 \leq i \leq d}$ でインデックスされている. Q の行と列は各々 $\{A_i\}_{0 \leq i \leq d}, \{E_i\}_{0 \leq i \leq d}$ でインデックスされている.

P と Q の間には直交関係:

$$PQ = QP = nI$$

が成り立つ. また, Q の (i, j) 成分 $q_{i,j}$ は P の (j, i) 成分 $p_{j,i}$ と multiplicity m_i と valency k_i を用いて次のように表される [1]:

$$q_{i,j} = \frac{m_j}{k_i} p_{j,i}$$

が成り立つ.

$\{\Lambda_j\}_{0 \leq j \leq d'}$ を $\Lambda_0 = \{0\}$ である $\{0, 1, \dots, d\}$ の分割とする. $R_{\Lambda_j} = \cup_{\ell \in \Lambda_j} R_\ell$ で定義する. $\mathcal{X} = (X, \{R_{\Lambda_j}\}_{0 \leq j \leq d'})$ が association scheme の条件を満たすとき, $\mathcal{X} = (X, \{R_{\Lambda_j}\}_{0 \leq j \leq d'})$ を $\mathcal{Y} = (X, \{R_i\}_{0 \leq i \leq d})$ の fusion scheme と呼ぶ.

一方, $\Lambda_0 = \{0\}$ である $\{0, 1, \dots, d\}$ の任意の分割 $\{\Lambda_j\}_{0 \leq j \leq d'}$ ($2 \leq d' \leq d$) に対して, $\mathcal{X} = (X, \{R_{\Lambda_j}\}_{0 \leq j \leq d'})$ が fusion scheme になるとき, $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を amorphous であると言う.

次の定理は, 与えられた association scheme $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ に対して, 何時 fusion scheme が構成できるのかを示してくれる.

Theorem 1.1 (*E. Bannai and M. Muzychuk*) $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を symmetric association scheme とする. $\{\Lambda_j\}_{0 \leq j \leq d'}$ ($\Lambda_0 = \{0\}$) を $\{0, \dots, d\}$ の分割とする. このとき, 任意の ℓ_1, ℓ_2 ($1 \leq \ell_1, \ell_2 \leq d'$) に対して, 行列 P の $(\Delta_{\ell_1}, \Lambda_{\ell_2})$ -block が constant row sum になるような $\{0, \dots, d\}$ の分割 $\{\Delta_j\}_{0 \leq j \leq d'}$ ($\Delta_0 = \{0\}$) が存在するならば, $\mathcal{X} = (X, \{R_{\Lambda_j}\}_{0 \leq j \leq d'})$ は $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ の fusion scheme になる.

このことを行列 Q の言葉で述べると次になる:

Corollary 1.2 与えられた $\{0, 1, \dots, d\}$ の分割 $\{\Lambda_j\}_{0 \leq j \leq d'}$ ($\Lambda_0 = \{0\}$) に対して, 任意の ℓ_1, ℓ_2 ($1 \leq \ell_1, \ell_2 \leq d'$) に対して, 行列 Q の $(\Lambda_{\ell_2}, \Delta_{\ell_1})$ -block が constant row sum になるような $\{0, 1, \dots, d\}$ の分割 $\{\Delta_j\}_{0 \leq j \leq d'}$ ($\Delta_0 = \{0\}$) が存在する.

Remark 1.3 Theorem 1.1 と Corollary 1.2 で述べられる $\{0, 1, \dots, d\}$ の分割 $\{\Lambda_j\}_{0 \leq j \leq d'}$, $\{\Delta_j\}_{0 \leq j \leq d'}$ は, $\{\Lambda_j\}_{0 \leq j \leq d'}$ が与えられれば $\{\Delta_j\}_{0 \leq j \leq d'}$ の存在は unique に決まる.

2 Edwin van Dam's Results and A. V. Ivanov's Conjecture

最近, Edwin R. van Dam 氏は論文 [3] で, 完全グラフを 4 つの strongly regular graphs に分割する分類結果を提出している. van Dam 氏の論文によれば, 次の場合が現れる:

Theorem 2.1 (*Edwin R. van Dam*) 完全グラフを 4 つの strongly regular graph に分割すると, 次の 3 つのタイプが現れる:

(i) amorphous association scheme,

(ii) 次の 1st eigenmatrix P を持つ symmetric association schemes:

$$P = \begin{pmatrix} 1 & k_1 & k_2 & k_3 & k_4 \\ 1 & s_1 & r_2 & r_3 & r_4 \\ 1 & r_1 & s_2 & s_3 & r_4 \\ 1 & r_1 & s_2 & r_3 & s_4 \\ 1 & r_1 & r_2 & s_3 & s_4 \end{pmatrix},$$

(iii) 固有行列として次の形を持つグラフ:

$$P = \begin{pmatrix} 1 & k_1 & k_2 & k_3 & k_4 \\ 1 & s_1 & s_2 & r_3 & r_4 \\ 1 & s_1 & r_2 & s_3 & r_4 \\ 1 & s_1 & r_2 & r_3 & s_4 \\ 1 & r_1 & s_2 & s_3 & r_4 \\ 1 & r_1 & s_2 & r_3 & s_4 \\ 1 & r_1 & r_2 & s_3 & s_4 \end{pmatrix}.$$

Theorem 2.1 (iii) に現れる行列 P は正方行列でないので, association scheme はくっついていない. 従って, van Dam 氏の結果を association scheme に制限すると, (i), (ii) の場合のみ現れる.

また, van Dam 氏は (ii) の行列について, 次の 2 つの例を出している:

$$P = \begin{pmatrix} 1 & v-4 & 1 & 1 & 1 \\ 1 & -4 & 1 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 \\ 1 & 0 & -1 & 1 & -1 \\ 1 & 0 & 1 & -1 & -1 \end{pmatrix}, \quad (1)$$

$$P = \begin{pmatrix} 1 & 2^{3t} - 4 - 3(2^{2t}) - 3(2^t) & 2^{2t} + 2^t + 1 & 2^{2t} + 2^t + 1 & 2^{2t} + 2^t + 1 \\ 1 & -4 - 3(2^t) & 1 + 2^t & 1 + 2^t & 1 + 2^t \\ 1 & -4 + 2^t & 1 + 2^t & 1 - 2^t & 1 - 2^t \\ 1 & -4 + 2^t & 1 - 2^t & 1 + 2^t & 1 - 2^t \\ 1 & -4 + 2^t & 1 - 2^t & 1 - 2^t & 1 + 2^t \end{pmatrix} \quad (2)$$

(2) は $t = 3$ に対して次の行列を得る:

$$P = \begin{pmatrix} 1 & 3276 & 273 & 273 & 273 \\ 1 & -52 & 17 & 17 & 17 \\ 1 & 12 & 17 & -15 & -15 \\ 1 & 12 & -15 & 17 & -15 \\ 1 & 12 & -15 & -15 & 17 \end{pmatrix}. \quad (3)$$

(1) は完全グラフと $L_{1,1,1}(2)$ の wreath product である. (3) は $GF(2^{12})$ 上のクラス $d = 45$ の cyclotomic scheme の fusion として構成される. (1) は imprimitive association scheme で, (3) は primitive association scheme の例である.

1991 年夏, Moscow 近郊の Vladimir で代数的組合せ論の国際会議が開催された. その時, A.V.Ivanov は次の予想問題を出した:

A.V.Ivanov's conjecture: $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を symmetric association scheme とする. 任意の $i (\neq 0)$ に対して $\Gamma_i = (X, R_i)$ が strongly regular graph とする. このとき, $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ は amorphous であるか?

van Dam 氏の結果は, (1), (3) の例が存在するので, この予想問題の反例になっている.

我々は, A.V.Ivanov's conjecture を更に考察するために, 次の条件を A.V.Ivanov's condition と呼ぶ:

A.V.Ivanov's condition: $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を symmetric association scheme とする. 任意の $i \in \{1, \dots, d\}$ に対して, $\Gamma_i = (X, R_i)$ は strongly regular graph である.

我々の立場として勿論重要な goal は *classification* である. 次の問題は自然に出てくる:

目的: A.V.Ivanov's condition を満たす対称 association schemes を分類せよ.

A.V.Ivanov's condition を満たす対称 association scheme \mathcal{X} で, van Dam 氏の結果の (ii) の状況にある non-amorphous association schemes はたくさん存在するのか. それとも, さほど多くの例は存在しないのか. また, non-amorphous association schemes の 1st eigennmatrix P はどのような形をしているのか? に興味がある.

3 考察

我々の興味の対象は, A.V.Ivanov's condition を持つ symmetric association scheme の 1st eigennmatrix P の shape である. この節以降, $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ は A.V.Ivanov's condition を満たすと仮定する.

$\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ の 1st eigennmatrix P :

$$P = \left(\begin{array}{c|ccc} 1 & k_1 & \dots & k_d \\ \hline 1 & & & \\ \vdots & & & \\ 1 & & & \end{array} \right) \begin{array}{c} \\ P_0 \\ \\ \end{array}$$

において, P_0 を P の主要部と呼ぶ. P_0 の列ベクトルを

$$p_0 = [p_1, \dots, p_d]$$

とおく.

Fact 1. 各 i ($i = 1, \dots, d$) に対して, $\tilde{\mathcal{X}} = (X, \{R_0, R_i, (X \times X) - R_0 - R_i\})$ は strongly regular graph であるから, 主要部 P_0 の各列 p_i ($1 \leq i \leq d$) には丁度 2 種類の値 a_i, b_i が並ぶ. この値は $\Gamma_i = (X, R_i)$ の固有値 a_i, b_i に一致する.

Fact 2. Strongly regular graph の complement も strongly regular graph である.

Fact 3. P_1, P_2 を 1st eigennmatrix P とする.

$$P_1 = U_1 P_2 U_2$$

を満たす置換行列 U_1, U_2 が存在するなら, $P_1 \sim P_2$ とする.

Fact 4. P_0 の各列に現れる a_i, b_i は単なる記号と見なすことができるので, 必要なら a_i と b_i の役割を入れ替えてよい.

Fact 3 と Fact 4 より P の第 2 行目は

$$P = \begin{pmatrix} 1 & k_1 & k_2 & \dots & k_d \\ 1 & a_1 & a_2 & \dots & a_d \\ 1 & & & & \\ \vdots & & & & \\ 1 & & & & \end{pmatrix}$$

としてよい. Fact 1, Fact 3 と Fact 4 より P の第 2 列は次の形としてよい.

$$P = \begin{pmatrix} 1 & k_1 & \dots & k_d \\ 1 & a_1 & & \\ \vdots & \vdots & & \\ 1 & a_1 & & \\ 1 & b_1 & & \\ \vdots & \vdots & & \\ 1 & b_1 & & \end{pmatrix}.$$

これより, P は次の一般形から出発してよい.

$$P = \begin{pmatrix} 1 & k_1 & k_2 & \dots & k_d \\ 1 & a_1 & a_2 & \dots & a_d \\ \vdots & \vdots & & & \\ 1 & a_1 & & & \\ 1 & b_1 & & & \\ \vdots & \vdots & & & \\ 1 & b_1 & & & \end{pmatrix}. \quad (4)$$

4 結果

この節では, van Dam 氏の結果の拡張と A.V.Ivanov's condition を持つ高々クラス $d \leq 6$ の symmetric association schemes の分類結果を述べる.

Proposition 4.1 $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を A.V.Ivanov's condition を持つ symmetric association scheme とする. Non-amorphous association schemes である次の 2 つの無限系列が存在する:

(1)

$$P = \begin{pmatrix} 1 & k_1 & k_2 & k_2 & \dots & \dots & \dots & k_2 \\ 1 & a_1 & a_2 & a_2 & \dots & \dots & \dots & a_2 \\ 1 & b_1 & a_2 & b_2 & \dots & \dots & \dots & b_2 \\ \hline 1 & b_1 & b_2 & a_2 & & & & b_2 \\ \vdots & \vdots & \vdots & & \ddots & & & \\ \vdots & \vdots & \vdots & & & \ddots & & \\ \vdots & \vdots & \vdots & & & & \ddots & \\ 1 & b_1 & b_2 & b_2 & & & & a_2 \end{pmatrix},$$

但し,

$$\begin{aligned}
 b_1 &= -\frac{k_1(a_1 + (d-2)^2)}{(n-1)d^2 - 4d(n-1) + 4(n-1) - k_1}, \\
 a_2 &= -\frac{a_1 + 1}{d-1}, \\
 b_2 &= \frac{f_1}{(d-1)((n-1)d^2 - 4d(n-1) + 4(n-1) - k_1)}, \\
 f_1 &= ((n-1)d + k_1 - 2n + 2)a_1 + (-n + k_1 + 1)d^2 \\
 &\quad + (4n - 3k_1 - 4)d + 3k_1 - 4n + 4, \\
 m_1 &= \frac{k_1}{(d-2)^2}, \\
 m_i &= \frac{(n-1)d^2 - 4d(n-1) + 4(n-1) - k_1}{(d-1)(d-2)^2} \quad (2 \leq i \leq d), \\
 k_2 &= \frac{n - k_1 - 1}{d-1}.
 \end{aligned}$$

a_1 は次の 2 方程式の解である.

$$(-n+1)a_1^2 - 2k_1a_1 - n(-n+k_1+1)d^2 + 4n(-n+k_1+1)d - 5k_1n + 4n^2 + k_1^2 - 4n = 0.$$

(2)

$$P = \left(\begin{array}{ccc|cccc}
 1 & k_1 & k_2 & k_3 & \dots & \dots & \dots & k_3 \\
 1 & a_1 & a_2 & a_3 & \dots & \dots & \dots & a_3 \\
 1 & b_1 & a_2 & b_3 & \dots & \dots & \dots & b_3 \\
 \hline
 1 & b_1 & b_2 & b_3 & & & & a_3 \\
 \vdots & \vdots & \vdots & & \ddots & & & \\
 \vdots & \vdots & \vdots & & & \ddots & & \\
 \vdots & \vdots & \vdots & & & & \ddots & \\
 1 & b_1 & b_2 & a_3 & & & & b_3
 \end{array} \right),$$

但し,

$$\begin{aligned}
 b_1 &= -\frac{k_1((d-3)a_1 + (d-2)^2)}{g_1}, \\
 a_2 &= -\frac{(d-3)^2(a_1 + 1)}{d^2 - 5d + 7}, \\
 b_2 &= -\frac{(d-3)f_1}{(d^2 - 5d + 7)g_1}, \\
 a_3 &= -\frac{a_1 + 1}{d^2 - 5d + 7}, \\
 b_3 &= \frac{f_2}{(d^2 - 5d + 7)g_1}, \\
 m_3 &= (d-3)m_2, \quad m_3 = \dots = m_d,
 \end{aligned}$$

$$\begin{aligned}
m_2 &= -\frac{-(n-1)d^2 + (4n+k_1-4)d - 4n - 3k_1 + 4}{(d^2 - 5d + 7)(d-2)^2}, \\
m_1 &= \frac{(d-3)k_1}{(d-2)^2}, \\
k_2 &= \frac{(n-k_1-1)(d-3)^2}{d^2 - 5d + 7}, \\
k_3 &= \dots = k_d = \frac{n-k_1-1}{d^2 - 5d + 7}, \\
f_1 &= (-k_1d^2 + (-n+6k_1+1)d + 2n - 9k_1 - 2)a_1 \\
&\quad + (n-k_1-1)d^3 - (7n-6k_1-7)d^2 \\
&\quad - (11k_1-16n+16)d - 12n + 5k_1 + 12, \\
f_2 &= (d-3)((n-1)d^2 + (-5n+5)d + 6n+k_1-6)a_1 \\
&\quad + k_1d^3 - (n+7k_1-1)d^2 + (4n+18k_1-4)d \\
&\quad - 4n - 17k_1 + 4, \\
g_1 &= (n-1)d^2 - (4n+k_1-4)d + 4n + 3k_1 - 4.
\end{aligned}$$

a_1 は次の 2 方程式の解である.

$$\begin{aligned}
&-(n-1)(d-3)a_1^2 - 2k_1(d-3)a_1 + n(n-k_1-1)d^2 \\
&+ (-4n^2 + 4n + k_1^2 + 3k_1n)d - k_1n - 3k_1^2 - 4n + 4n^2 = 0.
\end{aligned}$$

Remark 4.2 Proposition 4.1 の 1st eigenmatrix P の形は, 各々次の形から出発している.

(i)

$$P = \left(\begin{array}{ccc|ccc}
1 & k_1 & k_2 & k_3 & \dots & k_d \\
1 & a_1 & a_2 & a_3 & \dots & a_d \\
1 & b_1 & a_2 & b_3 & \dots & b_d \\
\hline
1 & b_1 & b_2 & a_3 & & b_d \\
\vdots & \vdots & \vdots & & \ddots & \\
1 & b_1 & b_2 & b_3 & & a_d
\end{array} \right),$$

(ii)

$$P = \left(\begin{array}{ccc|ccc}
1 & k_1 & k_2 & k_3 & \dots & k_d \\
1 & a_1 & a_2 & a_3 & \dots & a_d \\
1 & b_1 & a_2 & b_3 & \dots & b_d \\
\hline
1 & b_1 & b_2 & b_3 & & a_d \\
\vdots & \vdots & \vdots & & \ddots & \\
1 & b_1 & b_2 & a_3 & & b_d
\end{array} \right).$$

Remark 4.3 Proposition 4.1 で $d=4$ とすると, (i), (ii) の形は一致する. 従って, Proposition 4.1 は van Dam 氏の結果 (Theorem 2.1 (ii)) の一般化になっている.

Remark 4.4 (2) について $3 \leq t \leq 10$ の範囲で計算すると, $k_1 (= 2^{3t} - 4 - 3(2^{2t}) - 3(2^t))$, $k_2 (= 2^{2t} + 2^t + 1)$ の値は次のようになる.

t	k_1	k_2
3	292	73
4	3276	273
5	29596	1057
6	249660	4161
7	2047612	16513
8	16579836	65793
9	133429756	262657
10	1070593020	1049601

Proposition 4.1 (i) で $d = 4$ においてコンピュータを使って計算すると、次の表のようなパラメータを持つ strongly regular graph が現れる。但し、行列 (1) で記述できる場合は除いて計算している。表の意味は次の通りである。Proposition 4.1 (i) では $\Gamma_1 = (X, R_1)$ とその他 $\Gamma_i = (X, R_i)$ ($i \neq 1$) の 2 種類の strongly regular graph のパラメータ (n, k, λ, μ) が現れる。そこで、 $\Gamma_1 = (X, R_1)$ に対するパラメータを k_1, λ_1, μ_1 とおき、これ以外のパラメータを k_2, λ_2, μ_2 とおいている。

n	k_1	λ_1	μ_1	k_2	λ_2	μ_2
6348	4616	3340	3400	577	56	52
1701	500	103	165	400	100	92
1750	636	194	252	371	84	77
2160	1016	448	504	381	72	66
2738	1564	870	924	391	60	55
5070	3836	2890	2940	411	36	33
3675	2672	1930	1976	334	33	30
1800	1028	568	612	257	40	36
4096	♣ 3276	2612	2652	273	20	18
875	304	78	120	190	45	40
1701	1088	682	720	204	27	24
5887	5232	4646	4680	218	9	8
1058	604	330	364	151	24	21
1728	1256	904	936	157	16	14
3750	3260	2830	2860	163	8	7
2205	1856	1558	1584	116	7	6
300	92	10	36	69	18	15
512	♣ 292	156	180	73	12	10
1156	924	734	756	77	6	5
507	368	262	280	46	5	4
162	92	46	60	23	4	3
50	28	18	12	7	0	1
243	176	130	120	22	1	2
288	164	100	84	41	4	6
676	540	434	420	45	2	3
375	176	94	72	66	9	12
1445	1216	1026	1008	76	3	4
722	412	246	220	103	12	15
1200	872	640	616	109	8	10
2646	2300	2002	1980	115	4	5
4375	3888	3458	3432	162	5	6
768	236	100	60	177	36	42
1000	444	218	180	185	30	35
1352	772	456	420	193	24	28
1944	1340	934	900	201	18	21
3136	2508	2012	1980	209	12	14
6728	6076	5490	5460	217	6	7
2883	2096	1534	1496	262	21	24
2178	1244	730	684	311	40	45
6480	5456	4600	4560	341	16	18

♣ は (2) で現れる場合である。

ところが、この表において $\Gamma_1 = (X, R_1)$, $\Gamma_i = (X, R_i)$ ($i = 2, 3, 4$) が実際に存在する strongly regular graph は ♣ の場合のみである。

Proposition 4.5 $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ を *A. V. Ivanov's condition* を満たす対称 *association schemes* で高々クラス $d = 6$ とする. このとき, 次の場合のみが現れる:

- (i) *amorphous association schemes*,
- (ii) (i) and (ii) in Proposition 4.1.

References

- [1] E.Bannai and T.Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin/Cummings Publ., Menlo Park, 1984.
- [2] A.E.Brouwer, M.A.Cohen and N.Neumaier, *Distance-Regular Graphs*, Springer-Verlag, Heidelberg, 1989.
- [3] Edwin R. van Dam, *Strongly regular decompositions of the complete graph*, Journal of Algebraic Combinatorics, to appear.
- [4] T. Ito, A.Munemasa, and M.Yamada, *Amorphous association schemes over the Galois rings of characteristic 4*, Europ. J. Combinatorics 12, 1991, 513 – 526.
- [5] A.A.Ivanov and C.E.Praeger, *Problem session at ALCOM-91*, Europ. J. Combinatorics 15, 1994, 105 – 112.
- [6] M.E.Muzychuk, Ph.D.thesis, unpublished.

Kobe Gakuin Women's College
27-1 Hayashiyama-cho, Nagata-ku
Kobe, Japan, 653-0861

On The Association Schemes of Type II Matrices Constructed on Paley Graphs

Rie HOSOYA

Graduate School of Natural Science and Technology

Kanazawa University

Kakuma-machi, Kanazawa-shi, Ishikawa 920-1192, JAPAN

According to Jaeger, Matsumoto and Nomura, there is a mapping \mathcal{N} from the category of type II matrices W to that of association schemes. The association scheme $\mathcal{N}(W)$ obtained from W somehow controls the structure of W ; W is decomposed into a generalized tensor product if and only if $\mathcal{N}(W)$ is imprimitive. However, we have only few examples of type II matrix calculated for known type II matrices and it is yet to be settled what sort of association schemes arise as $\mathcal{N}(W)$. In this paper, we study $\mathcal{N}(W)$ for the type II matrix W constructed on a Paley graph. We show that if the size of the type II matrix W is greater than 9, $\mathcal{N}(W)$ is a trivial association scheme.

1 Introduction

Throughout this paper, $M[i, j]$ denotes the (i, j) -entry of a matrix M and $\mathbf{u}[h]$ denotes the h -th entry of a vector \mathbf{u} . Let M be an $m \times n$ matrix whose entries are all nonzero. We associate an $n \times m$ matrix M^- defined by the following.

$$M^- [i, j] = \frac{1}{M[j, i]}.$$

Let I denote the identity matrix and let J denote the all ones matrix. Let $\text{Mat}_n(\mathcal{C})$ denote the set of $n \times n$ complex matrices. $W \in \text{Mat}_n(\mathcal{C})$ is said to be a *type II matrix* if $WW^- = nI$. It is clear that if W is a type II matrix, then the transpose W^T of the matrix and W^- are type II matrices as well.

The definition of type II matrices was first introduced explicitly in the study of *spin models*. See [1, 7] for details.

Example 1.1 (1) Let ζ be a primitive n -th root of 1. Then the matrix $W \in \text{Mat}_n(\mathbf{C})$ defined by $W[i, j] = \zeta^{(i-1)(j-1)}$ is a type II matrix. W is called a *cyclic type II matrix* of size n .

(2) Let α be a root of the quadratic equation $t^2 + nt + n = 0$. Then the matrix $W \in \text{Mat}_n(\mathbf{C})$ defined by $W[i, j] = 1 + \delta_{i,j}\alpha$ is a type II matrix. W is called a *Potts type II matrix* of size n .

Let $W \in \text{Mat}_n(\mathbf{C})$ be a type II matrix. If $S, S' \in \text{Mat}_n(\mathbf{C})$ are permutation matrices and $D, D' \in \text{Mat}_n(\mathbf{C})$ are nonsingular diagonal matrices, then it is easy to see that $SDWD'S'$ is also a type II matrix. We say that two type II matrices W and W' are *type II equivalent* if $W' = SDWD'S'$ for suitable choices of permutation matrices S, S' and diagonal matrices D, D' . It is clear that this defines an equivalence relation on the set of type II matrices.

For a type II matrix $W \in \text{Mat}_n(\mathbf{C})$ and for $1 \leq i, j \leq n$, we define an n -dimensional column vector $\mathbf{u}_{i,j}^W$ by the following.

$$\mathbf{u}_{i,j}^W[h] = \frac{W[h, i]}{W[h, j]}.$$

Let

$$\mathcal{N}(W) = \{M \in \text{Mat}_n(\mathbf{C}) \mid \mathbf{u}_{i,j}^W \text{ is an eigenvector for } M \text{ for all } 1 \leq i, j \leq n\}.$$

It is known that $\mathcal{N}(W)$ is the Bose-Mesner algebra of a commutative association scheme. $\mathcal{N}(W)$ is called a *Nomura algebra*. Moreover, there exists a duality map from $\mathcal{N}(W)$ to $\mathcal{N}(W)$. $\mathcal{N}(W)$ is called the *dual* of $\mathcal{N}(W)$. We often say $\mathcal{N}(W)$ has a dual (See Section 2 [5]).

We are interested in the association schemes $\mathcal{N}(W)$ obtained from type II matrices W . Suzuki and the author showed that W is decomposed into a generalized tensor product if and only if $\mathcal{N}(W)$ is imprimitive [5].

We are now interested in type II matrices associated with primitive association schemes. Well known examples are the following.

Example 1.2 (1) Let W be a cyclic type II matrix of size n . Then $\mathcal{N}(W)$ is the Bose-Mesner algebra of the group scheme of cyclic group of order n .

(2) Let W be a Potts type II matrix of size $n \geq 5$. Then $\mathcal{N}(W)$ is trivial, i.e., Bose-Mesner algebra of the class 1 association scheme.

We study the Nomura algebra of a type II matrix constructed on a Paley graph. Let q be a prime power with $q \equiv 1 \pmod{4}$. The *Paley graph* $P(q)$ has as vertex set the finite field \mathbf{F}_q , with two vertices adjacent if and only if

their difference is a non-zero square. It is strongly regular, with parameters $(q, \frac{1}{2}(q-1), \frac{1}{4}(q-5), \frac{1}{4}(q-1))$ and their eigenvalues are given as

$$k = \frac{1}{2}(q-1), \quad r = \frac{-1 \pm \sqrt{q}}{2}, \quad s = \frac{-1 \mp \sqrt{q}}{2}.$$

Let Γ be a strongly regular graph, and let A_i be the i -th adjacency matrices of Γ for $i = 0, 1, 2$. For a matrix $W = t_0A_0 + t_1A_1 + t_2A_2$ ($t_i \in \mathbf{C}$), Jaeger gives a construction of t_i for W to be a type II matrix (See Equation (33) in [6]).

We restate Jaeger's result for the case Γ is a Paley graph $\mathbf{P}(q)$. Let $\mathbf{P}(q)$ be a Paley graph over a finite field \mathbf{F}_q with $q \equiv 1 \pmod{4}$. The adjacency matrix A of $\mathbf{P}(q)$ is defined as follows:

$$A[x, y] = \begin{cases} 1 & \text{if } x - y \text{ is a square in } \mathbf{F}_q \\ 0 & \text{otherwise} \end{cases},$$

where $x, y \in \mathbf{F}_q$. We construct a matrix $W \in \text{Mat}_q(\mathbf{C})$ by the following.

$$W = t_0I + t_1A + t_2(J - I - A)$$

where t_i 's satisfy the following equations.

$$t_2 = t_1^{-1}, \tag{1}$$

$$s^2 + (r+1)^2 - s(r+1)(t_1^2 + t_1^{-2}) = 1, \tag{2}$$

$$t_0 = -st_1 + (r+1)t_1^{-1} \tag{2}$$

for $(r, s) \in \{(\frac{-1 \pm \sqrt{q}}{2}, \frac{-1 \mp \sqrt{q}}{2})\}$. Note that r and s are eigenvalues of the Paley graph $\mathbf{P}(q)$. We write $t_1 = t, t_2 = t^{-1}$. Jaeger showed that the matrix W defined above is a type II matrix (See 3.4 in [6]). We say W is a *type II matrix constructed on a Paley graph $\mathbf{P}(q)$* . Since -1 is a square in \mathbf{F}_q , A is symmetric. Hence W is also symmetric.

Our main result is:

Theorem 1.1 *Let W be a type II matrix constructed on a Paley graph $\mathbf{P}(q)$ with $q \equiv 1 \pmod{4}$. If $q > 9$, then $\mathcal{N}(W)$ is trivial, i.e., the Bose-Mesner algebra of the class 1 association scheme.*

Here we will first prove the above theorem for the case $q = p$ where p is a prime by using the structure of Paley graphs. Then we show the theorem in general by using only the parameters of Paley graphs.

According to A. Chan, the theorem holds for type II matrices constructed on conference graphs, which are in a wide class of strongly regular graphs with parameters $(4m+1, 2m, m-1, m)$, if $m > 2$. Note that a conference graph becomes a Paley graph when $4m+1$ is a prime power. In fact we do not use the condition $4m+1$ is prime power when we prove the theorem.

2 The entries of type II matrices constructed on Paley graphs

Let $(r, s) = (\frac{-1 \pm \sqrt{q}}{2}, \frac{-1 \mp \sqrt{q}}{2})$. Then Equation (1) is equivalent to

$$t + t^{-1} = \pm \frac{1}{\sqrt{-s(r+1)}}. \quad (3)$$

Then we may regard t as a root of the quadratic equation $x^2 \mp \frac{1}{\sqrt{-s(r+1)}}x + 1 = 0$.

Let \bar{t} be the complex conjugate of t . We have $t\bar{t} = 1$, in other words, $\bar{t} = t^{-1}$.

Consider the galois group $G = \text{Gal}(K/\mathbb{Q})$ of the minimal polynomial of t over \mathbb{Q} . There exists $\sigma \in G$ such that $\sigma(t) = t^{-1} = \bar{t}$.

By Equation (2), we have

$$t_0 = \pm 1.$$

Here the choice of plus or minus sign depends on sign of r, s .

Equation (4) has in general four solutions in t , which can be obtained from one of them by inversion or change of sign. We can obtain at most 4 kinds of type II matrices depending on the value of t for fixed r and s . We can, however, verify that if one of them is obtained from the other by inversion or change of sign of t , they are type II equivalent to each other, which means we have only one type II matrix up to type II equivalence for given r and s .

3 The graph description of Nomura algebras

We restate the results of [7] for a type II matrix constructed on a Paley graph $P(q)$.

Let W be a type II matrix in $\text{Mat}_X(\mathbb{C})$. Let Γ be a graph whose vertex set is $X \times X$. For two vertices (a, b) and $(c, d) \in X \times X$, we say that (a, b) is *adjacent* to (c, d) if and only if the Hermitian inner product $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle := \sum_{x \in X} \mathbf{u}_{a,b}(x) \overline{\mathbf{u}_{c,d}(x)}$ is nonzero. The graph Γ is said to be a *Jones graph*. Since $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$ is nonzero if and only if $\langle \mathbf{u}_{c,d}, \mathbf{u}_{a,b} \rangle$ is nonzero we obtain an undirected graph Γ .

Let C_0, C_1, \dots, C_d denote the connected components of a Jones graph Γ . Let A_i be a matrix in $\text{Mat}_X(\mathbb{C})$ with (a, b) -entry equal to 1 if $(a, b) \in C_i$ and to 0 otherwise.

Proposition 3.1 ([7] Theorem 5) *The set $\{A_i \mid 0 \leq i \leq d\}$ is the basis of Hadamard idempotents of $\mathcal{N}(W)$.*

From now on, we consider the case W is a type II matrix constructed on a Paley graph $P(q)$. Since W is symmetric the above proposition implies that the set $\{A_i \mid 0 \leq i \leq d\}$ is the basis of Hadamard idempotents of $\mathcal{N}(W)$ and we can get the dimension of $\mathcal{N}(W)$. In order to prove that $\mathcal{N}(W)$ is trivial, we only have to show that the number of the connected components of the Jones graph for W is exactly equal to 2.

3.1 Basic properties of $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$

Lemma 3.2 *For any $a, b, c, d \in \mathbb{F}_q$, the following hold.*

$$\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle = \langle \mathbf{u}_{a+k,b+k}, \mathbf{u}_{c+k,d+k} \rangle$$

for all $k \in \mathbb{F}_q$.

Let $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$.

Lemma 3.3 *For any $a, b, c, d \in \mathbb{F}_q$, the following hold.*

$$\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle = \langle \mathbf{u}_{\alpha a, \alpha b}, \mathbf{u}_{\alpha c, \alpha d} \rangle$$

for any square $\alpha \in \mathbb{F}_q^*$.

Lemma 3.4 *For any $a, b, c, d \in \mathbb{F}_q$ and for a primitive element g of \mathbb{F}_q^* , $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle = 0$ if and only if $\langle \mathbf{u}_{ga,gb}, \mathbf{u}_{gc,gd} \rangle = 0$.*

3.2 Connected components of $\Gamma(W)$

Let $\Gamma(W)$ denote the Jones graph for W .

It is trivial that $\{(a, a) \in \mathbb{F}_q \times \mathbb{F}_q \mid a \in \mathbb{F}_q\}$ generates a connected component of $\Gamma(W)$. We write $C_0 := \{(a, a) \in \mathbb{F}_q \times \mathbb{F}_q \mid a \in \mathbb{F}_q\}$.

Let $q = p^e$ for a prime p and a natural number e , and let $\mathbb{F}_p = \{0, 1, \dots, p-1\}$. Let $\{\alpha_0 = 1, \alpha_1, \dots, \alpha_{e-1}\}$ be a basis of \mathbb{F}_q over \mathbb{F}_p , and let g be a primitive element of \mathbb{F}_q^* .

Lemma 3.5 *Assume that $\langle \mathbf{u}_{0,1}, \mathbf{u}_{\alpha_i, 1+\alpha_i} \rangle$ is nonzero for $i = 0, 1, \dots, e-1$. Then the set of vertices $C_1^1 := \{(k, 1+k) \in \mathbb{F}_q \times \mathbb{F}_q \mid k \in \mathbb{F}_q\}$ is included in the same connected component of the Jones graph $\Gamma(W)$.*

Lemma 3.6 *Assume that $\langle \mathbf{u}_{0,1}, \mathbf{u}_{\alpha_i, 1+\alpha_i} \rangle$ and $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle$ are nonzero for all $i, i = 0, 1, \dots, e-1$. Let $C_1^h := \{(k, k+g^{h-1}) \mid k \in \mathbb{F}_q\}$ for $1 \leq h \leq p-1$. Then the sets of vertices $C_1^1, C_1^2, \dots, C_1^{p-1}$ are included in the same connected component of the Jones graph $\Gamma(W)$.*

Proof. We proceed by induction on h . For the case $h = 1$ the claim is true because of Lemma 3.5. Suppose that the claim is true for the case $h \leq m$. Because of the assumption $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle$ is nonzero and by Lemma 3.3 or Lemma 3.4, we can see that $\langle \mathbf{u}_{0,g^{m-1}}, \mathbf{u}_{g^{m-1},g^{m-1}+g^m} \rangle$ is nonzero. By Lemma 3.2, $\langle \mathbf{u}_{k,k+g^{m-1}}, \mathbf{u}_{k+g^{m-1},k+g^{m-1}+g^m} \rangle$ is nonzero for $k \in \mathbf{F}_q$. This leads to that $(k, k + g^{m-1})$ and $(k + g^{m-1}, k + g^{m-1} + g^m)$ are adjacent for each $k \in \mathbf{F}_q$. Since the union of the sets $C'_1, C'_2, \dots, C'_{m-1}$ is connected, C'_m is also included in the same connected component. This completes the proof. \blacksquare

Proposition 3.7 *Let W be a type II matrix constructed on the Paley graph $\mathcal{P}(q)$ under the notation above. If $\langle \mathbf{u}_{0,1}, \mathbf{u}_{\alpha_i,1+\alpha_i} \rangle$ and $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle$ are nonzero for all $i, i = 0, 1, \dots, e - 1$, then $\mathcal{N}(W)$ is trivial.*

Proof. By Lemma 3.6, the sets of vertices $C'_1, C'_2, \dots, C'_{p-1}$ generate a connected component of the Jones graph $\Gamma(W)$. We may write $C_1 = C'_1 \cup C'_2 \cup \dots \cup C'_{p-1}$. Hence the Jones graph $\Gamma(W)$ consists of two connected components C_0 and C_1 . This implies the dimension of $\mathcal{N}(W)$ is equal to 2. Therefore $\mathcal{N}(W)$ is trivial. \blacksquare

4 Computations of $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle$ and $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle$

Let t satisfy Equation (4). It is easy to see that $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle$ is a linear combination of $1, t^{-1}, t^2, t^{-2}, t^{-3}, t^4, t^{-4}$. Their coefficients are described in terms of the quadratic residue character η .

4.1 Expressions of $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle$ in terms of t, t^{-1}

Let $S_2 = \sum_{x \in \mathbf{F}_q} \eta(x)\eta(x-1)\eta(x-2)$. If $\eta(2) = 1$, we have

$$\begin{aligned} \langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle &= \frac{1}{8}(q-3-S_2)t^4 + \frac{1}{8}(q+1+S_2)t^{-4} \\ &\quad + \frac{1}{4}(q+5+S_2)t^2 + \frac{1}{4}(q-3-S_2)t^{-2} + 2t^{-1} + \frac{1}{4}(q-9). \end{aligned}$$

If $\eta(2) = -1$, we have

$$\begin{aligned} \langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle &= \frac{1}{8}(q-3-S_2)t^4 + \frac{1}{8}(q-7+S_2)t^{-4} + 2t^{-3} \\ &\quad + \frac{1}{4}(q+5+S_2)t^2 + \frac{1}{4}(q-3-S_2)t^{-2} + \frac{1}{4}(q-5). \end{aligned}$$

4.2 Expressions of $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle$ in terms of t, t^{-1}

Let $S_{1+g} = \sum_{x \in \mathbb{F}_q} \eta(x)\eta(x-1)\eta(x-1-g)$. If $\eta(1+g) = 1$, we have

$$\begin{aligned} \langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle &= \frac{1}{8}(q-3-S_{1+g})t^4 + \frac{1}{8}(q+1+S_{1+g})t^{-4} \pm t^3 \\ &\quad + \frac{1}{4}(q-3+S_{1+g})t^2 + \frac{1}{4}(q-3-S_{1+g})t^{-2} \pm t^{-1} + \frac{1}{4}(q-1). \end{aligned}$$

If $\eta(1+g) = -1$, we have

$$\begin{aligned} \langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle &= \frac{1}{8}(q+1-S_{1+g})t^4 + \frac{1}{8}(q-3+S_{1+g})t^{-4} \pm t^{-3} \\ &\quad + \frac{1}{4}(q-3+S_{1+g})t^2 + \frac{1}{4}(q-3-S_{1+g})t^{-2} \pm t + \frac{1}{4}(q-1). \end{aligned}$$

5 Proof of Theorem 1.1 for the case $q = p$

In this section, we prove our main theorem for the case $q = p$.

Lemma 5.1 *Let W be a type II matrix constructed on the Paley graph $P(p)$ with a prime $p \equiv 1 \pmod{4}$. Then $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle$ is nonzero.*

Proof. Assume $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle = 0$. We may regard $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle$ as a polynomial in t and t^{-1} over \mathbb{Q} , i.e., $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle = f(t, t^{-1})$ where t and t^{-1} satisfy Equation (4). By the assumption, we have

$$\sigma(f(t, t^{-1})) = 0$$

for $\sigma \in G = \text{Gal}(K/\mathbb{Q})$ which is defined in Section 2. Hence

$$f(t, t^{-1}) - \sigma(f(t, t^{-1})) = 0. \dots (*)$$

Note that $\sigma(f(t, t^{-1}))$ is obtained by replacing t with t^{-1} in $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle$.

If $\eta(2) = 1$, Equation (*) is equivalent to

$$-\frac{1}{4}(2+S_2)(t^2+t^{-2}) + \frac{1}{2}(4+S_2) \mp 2(t+t^{-1})^{-1} = 0,$$

and this is equivalent to

$$S_2 = -2 \mp \frac{2+(3-p)\sqrt{p}}{4-p}.$$

S_2 is not a rational integer for any prime $p \equiv 1 \pmod{4}$. This contradicts the fact that $S_2 = \sum_{x \in \mathbb{F}_p} \eta(x)\eta(x-1)\eta(x-2)$ is a rational integer. Hence $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,2} \rangle$ is nonzero. The case $\eta(2) = -1$ is similarly proved. \blacksquare

Lemma 5.2 *Let W be a type II matrix constructed on the Paley graph $P(p)$ for a prime p with $p > 9$. Then $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle$ is nonzero for a primitive element g of \mathbf{F}_p .*

Proof. If $\eta(1+g) = 1$, we have

$$S_{1+g} = \frac{2 \pm (p-5)\sqrt{p}}{p-4}.$$

S_{1+g} is not a rational integer for any prime $p \equiv 1 \pmod{4}$ with $p > 5$. This contradicts the fact that $S_{1+g} = \sum_{x \in \mathbf{F}_p} \eta(x)\eta(x-1)\eta(x-1-g)$ is a rational integer. Hence $\langle \mathbf{u}_{0,1}, \mathbf{u}_{1,1+g} \rangle$ is nonzero if $\eta(1+g) = -1$ is similarly proved. ■

Proof of Theorem 1.1

By applying Lemma 5.1 and Lemma 5.2 to Proposition 3.7, we obtain the result. ■

6 Proof of Theorem 1.1 in General

In this section, we show that $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$ is nonzero for distinct $a, b, c, d \in \mathbf{F}_q$ where $q = p^e > 9$ for a prime p and a natural number e . This implies that Theorem 1.1 holds for $q > 9$.

Proposition 6.1 *Let W be a type II matrix of size $|X|$. If $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$ is nonzero where $a, b, c, d \in X$ are distinct and $|X| \geq 5$, then $\mathcal{N}(W)$ is trivial.*

Let t satisfy Equation (4). It is easy to see that $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$ is a linear combination of $1, t, t^{-1}, t^2, t^{-2}, t^3, t^{-3}, t^4, t^{-4}$. We can see that $\pm t, \pm t^{-1}, \pm t^3, \pm t^{-3}$ appear when $x = a, b, c$, or d . Set $U_w(t, t^{-1}) := \sum_{x=a,b,c,d} \frac{W[x,a] \overline{W[x,c]}}{W[x,b] \overline{W[x,d]}}$. Hence we have the following.

$$\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle = U_w(t, t^{-1}) + l_1 t^2 + l_2 t^{-2} + m_1 t^4 + m_2 t^{-4} + n,$$

where $4 + l_1 + l_2 + m_1 + m_2 + n = q$. Then $\pm U_w(t, t^{-1}) \in \{4t, 4t^{-1}, 4t^3, 4t^{-3}, t + 3t^{-1}, 3t + t^{-1}, 2(t + t^{-1}), t + 3t^3, 3t + t^3, 2(t + t^3), t + 3t^{-3}, 3t + t^{-3}, 2(t + t^{-3}), t^{-1} + 3t^3, 3t^{-1} + t^3, 2(t^{-1} + t^3), t^3 + 3t^{-3}, 3t^3 + t^{-3}, 2(t^3 + t^{-3})\}$. The sign \pm depends on that of t_0 .

Proposition 6.2 *Let W be a type II matrix constructed on a Paley graph $P(q)$ for $q = p^{2e} > 9$. Then $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$ is nonzero for any distinct $a, b, c, d \in \mathbf{F}_q$.*

Proof. Let $r = \frac{-1+\sqrt{q}}{2} = \frac{-1+p^e}{2}$. Since $t + t^{-1} = \pm(r + 1)^{-1}$ and $t_0 = (r + 1)(t + t^{-1})$, we can choose plus sign without loss of generality. Suppose $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle = 0$. $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$ can be regarded as a polynomial in t, t^{-1} over \mathbf{Q} , so we can write $f(t, t^{-1}) = \langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$. As we have seen in Section 2, there exists $\sigma \in G = \text{Gal}(K/\mathbf{Q})$ such that $\sigma(t) = \bar{t} = t^{-1}$. By the assumption, $f(t^{-1}, t) = 0$. Therefore we have $f(t, t^{-1}) + f(t^{-1}, t) = 0$, which is equivalent to

$$(l_1 + l_2)(t^2 + t^{-2}) + (m_1 + m_2)(t^4 + t^{-4}) + 2n = -U_w(t, t^{-1}) - U_w(t^{-1}, t).$$

Set $l = l_1 + l_2$, and $m = m_1 + m_2$. Then we have

$$l(t^2 + t^{-2}) + m(t^4 + t^{-4}) + 2n = -U_w(t, t^{-1}) - U_w(t^{-1}, t), \dots (*)$$

where $4 + l + m + n = q$. $U_w(t, t^{-1}) + U_w(t^{-1}, t)$ is one of the following:

$$4(t+t^{-1}), 4(t^3+t^{-3}), 2(t+t^{-1})+2(t^3+t^{-3}), (t+t^{-1})+3(t^3+t^{-3}), 3(t+t^{-1})+(t^3+t^{-3}).$$

Note that

$$t^2 + t^{-2} = (t + t^{-1})^2 - 2 = \frac{4}{(1 + p^e)^2} - 2,$$

$$t^3 + t^{-3} = (t + t^{-1})^3 - 3(t + t^{-1}) = \frac{8}{(1 + p^e)^3} - \frac{6}{(1 + p^e)},$$

$$t^4 + t^{-4} = (t^2 + t^{-2})^2 - 2 = \frac{16}{(1 + p^e)^4} - \frac{16}{(1 + p^e)^2} + 2.$$

By plugging in these values to the equation (*), the left hand side of (*) becomes the following.

$$k\left\{\frac{4}{(1 + p^e)^2} - 2\right\} + l\left\{\frac{16}{(1 + p^e)^4} - \frac{16}{(1 + p^e)^2} + 2\right\} + 2n.$$

Multiplying $\frac{1}{2}(1 + p^e)^4$ and putting $m = q - 4 - l - n$, the left hand side of (*) is equivalent to

$$(2 + p^e)\{- (2 - p^e)(1 + p^e)^4 - 2lp^e(1 + p^e)^2 + 8p^e(l + n + 1) - 16\}.$$

Multiplying $\frac{1}{2}(1 + p^e)^4$, the right hand side of (*) is written as follows:

$U_w(t, t^{-1}) + U_w(t^{-1}, t)$	RHS $\times \frac{1}{2}(1 + p^e)^4$
$4(t + t^{-1})$	$-4(2 + p^e)(1 + p^e + p^{2e}) + 4$
$4(t^3 + t^{-3})$	$4(2 + p^e)(3p^{2e} + 3p^e - 1) + 4$
$2(t + t^{-1}) + 2(t^3 + t^{-3})$	$4(2 + p^e)(p^{2e} + p^e - 1) + 4$
$(t + t^{-1}) + 3(t^3 + t^{-3})$	$4(2 + p^e)(2p^{2e} + 2p^e - 1) + 4$
$3(t + t^{-1}) + (t^3 + t^{-3})$	$-4(2 + p^e) + 4$

Both sides of (*) become integers by multiplying $\frac{1}{2}(1 + p^e)^4$, and the left hand side is divisible by $(2 + p^e)$ although the right hand side is not divisible by $(2 + p^e)$. We have contradiction. For the case $r = \frac{-1-p^e}{2}$, we only have to exchange p^e by $-p^e$, and we can see that the left hand side of (*) is divisible by $(2 - p^e)$ although the right hand side is not divisible by $(2 - p^e)$ whenever $p^e > 3$ after multiplying $\frac{1}{2}(1 - p^e)$. Hence $\langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$ is nonzero whenever $q = p^{2e}$ and $q > 9$. ■

Corollary 6.3 *Theorem 1.1 holds for $q = p^{2e}$.*

For the case $q = p^{2e+1}$, we can verify that the symmetric polynomial $f(t, t^{-1}) + f(t^{-1}, t)$ is not divisible by the minimal polynomial of $t + t^{-1}$ if $q > 5$. Hence $f(t, t^{-1}) = \langle \mathbf{u}_{a,b}, \mathbf{u}_{c,d} \rangle$ is nonzero for $q > 5$. Combining these facts, we can complete the proof of the main theorem.

Remarks.

- (1) Type II matrices constructed on $P(5)$ are type II equivalent to cyclic type II matrix of size 5, and their Nomura algebra is Bose-Mesner algebra of group scheme of cyclic group C_5 .
- (2) If r is negative, a type II matrix W constructed on $P(9)$ is type II equivalent to the tensor product of Potts type II matrix of size 3, and $\mathcal{N}(W)$ is Bose-Mesner algebra of group scheme of $C_3 \otimes C_3$. If r is positive, $\mathcal{N}(W)$ is trivial where W is a type II matrix constructed on $P(9)$.

References

- [1] E. Bannai and E. Bannai, "Generalized generalized spin models (four-weight spin models)," *Pacific J. Math.* **170** (1995), 1-16.
- [2] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin-Cummings, California, 1984.
- [3] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, 1989.
- [4] A. Chan, Private communication.
- [5] R. Hosoya and H. Suzuki, "Type II Matrices and Their Bose-Mesner algebras," to appear.

- [6] F. Jaeger, "Strongly regular graphs and spin models for the Kauffman polynomials," *Geometriae Dedicata* **44** (1992), 23–52.
- [7] F. Jaeger, M. Matsumoto and K. Nomura, "Bose-Mesner algebras related to type II matrices and spin models", *J. Alg. Comb.* **8** (1998), 39–72.

A Note on Plethysm Composition

Tomoyuki YOSHIDA (Hokkaido Univ.)

July 03, 2002

0 Plethysm(0): Formal Power Series

Let $f(t) = \sum_{n=1}^{\infty} a_n t^n / n!$ and $g(t) = \sum_{n=0}^{\infty} b_n t^n / n!$ be two ordinary formal power series. Then the composition $(g \circ f)(t) = g(f(t))$ is again a formal power series and is explicitly given by the following formula:

$$(g \circ f)(t) = \sum_{n=0}^{\infty} \sum_{\sum i \mu_i = n} \frac{a_1^{\mu_1} a_2^{\mu_2} \cdots}{1!^{\mu_1} \mu_1! 2!^{\mu_2} \mu_2! \cdots} b_{\sum \mu_i} t^n.$$

How about functions in multivariables x_1, x_2, \dots ? Of course, the composition $g(f(x_1, x_2, \dots))$ is non-sense because $f(x_1, x_2, \dots)$ and $g(x_1, x_2, \dots)$ are single-valued functions with multi-variables. However, it is known that such compositions can be defined in some cases (Plethysm (1) - (3)).

1 Plethysm(1): Symmetric Functions

The notion of plethysm is first introduced by Littlewood and Pólya (Littlewood 1950). Let Λ be the ring of symmetric functions in the variables x_1, x_2, \dots with coefficients in \mathbf{Q} . Let $p_n = \sum_i x_i^n$ be the power symmetric functions. Then $\{p_n\}_{n=1,2,\dots}$ makes a polynomial basis of Λ , that is, $\Lambda = \mathbf{Q}[p_1, p_2, \dots]$. Furthermore, Λ has the \mathbf{Q} -basis $p_\lambda = p_{\lambda_1} \cdots p_{\lambda_n}$, where $\lambda = (\lambda_1, \dots, \lambda_n)$ is a partition, that is, $\lambda_1 \geq \dots \geq \lambda_n > 0$. Now, let $f, g \in \Lambda$ and express f as a sum of monomials:

$$f = \sum_{\alpha} u_{\alpha} x^{\alpha}, \text{ where } x^{\alpha} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots$$

2 PLETHEYSM(2): CHARACTER RING

When $u_0 = 0$, we can define a sequence of polynomials y_1, y_2, \dots by

$$\prod_{\alpha} (1 + x^{\alpha} t)^{u_{\alpha}} = \prod_i (1 + y_i t).$$

Then the *plethysm composition* is defined as follows:

$$(g \circ f)(x_1, x_2, \dots) := g(y_1, y_2, \dots)$$

For a fixed f , the map $g \mapsto g \circ f$ is a ring homomorphism. Furthermore

$$p_n(y_1, y_2, \dots) = \sum_{\alpha} u_{\alpha} (x^{\alpha})^n, \quad \text{where } (x^{\alpha})^n := x_1^{n\alpha_1} x_2^{n\alpha_2} \dots$$

Thus

$$\begin{aligned} p_n \circ f &= f(x_1^n, x_2^n, \dots), & p_m \circ p_n &= p_n \circ p_m = p_{mn} \\ (h \circ g) \circ f &= h \circ (g \circ f), & f \circ p_1 &= p_1 \circ f = f. \end{aligned}$$

2 Pletheysm(2): Character Ring

As is well-known, there is a ring homomorphism from the ring of characters of symmetric groups $R = \bigoplus_{n \geq 0} R(S_n)$ to Λ :

$$\begin{aligned} \text{ch} &: R \longrightarrow \mathbb{C}\Lambda, \\ &; \chi (\in R(S_n)) \longmapsto \frac{1}{n!} \sum_{\sigma \in S_n} \chi(\sigma) p_{\text{type}(\sigma)}. \end{aligned}$$

Then the plethysm on the character ring R by using those on Λ :

$$u \circ v = \text{ch}^{-1}(\text{ch}(u) \circ \text{ch}(v)).$$

Let U and V be an S_m -module and an S_n -module, respectively. Then the wreath product $S_m \wr S_n$ acts on U and $V^{\otimes m}$. Thus we can construct an induced representation

$$U \circ V := \text{Ind}_{S_m \wr S_n}^{S_{mn}} (U \otimes V^{\otimes m}).$$

If u, v be the characters of U, V , then the character of $U \circ V$ is given by $u \circ v$.

3 Plethysm(3): Formal Power Series, again

We can define the *plethysmic composition* for formal power series with infinite variables. Let

$$f(x_1, x_2, \dots) = \sum_{\lambda} \frac{a_{\lambda_1 \lambda_2 \dots}}{1!^{\lambda_1} \lambda_1! 2!^{\lambda_2} \lambda_2! \dots} x_1^{\lambda_1} x_2^{\lambda_2} \dots, \quad (a_0 = 0)$$

$$g(x_1, x_2, \dots) = \sum_{\lambda} \frac{b_{\lambda_1 \lambda_2 \dots}}{1!^{\lambda_1} \lambda_1! 2!^{\lambda_2} \lambda_2! \dots} x_1^{\lambda_1} x_2^{\lambda_2} \dots,$$

be two formal power series. Here $\lambda = (\lambda_1, \lambda_2, \dots)$ runs partitions, that is, a series of nonnegative integers with $\sum \lambda_i < \infty$. We simply write f and g as

$$f(t) = \sum_{\lambda} \frac{a_{\lambda}}{\lambda!} x^{\lambda}, \quad g(t) = \sum_{\lambda} \frac{b_{\lambda}}{\lambda!} x^{\lambda}$$

Now, let f_n ($n = 1, 2, \dots$) be the following polynomials:

$$f_n(x_1, x_2, \dots) := f(x_n, x_{2n}, x_{3n}, \dots).$$

Then the *plethysm composition* is defined by

$$(g * f)(x_1, x_2, \dots) := g(f_1, f_2, f_3, \dots).$$

We can easily prove the following:

$$x_n * f = f_n, \quad x_m * x_n = x_n * x_m = x_{mn}, \quad f * x_1 = x_1 * f = f.$$

By the isomorphism $Q[x_1, x_2, \dots] \cong \Lambda$; $x_i \longleftrightarrow p_i$, the both plethysm compositions are corresponding: $x_i \longleftrightarrow p_i$, $g * f \longleftrightarrow g \circ f$.

4 Plethysm(4): Species

The concept of species was introduced by Joyal(1981). A *species* S is a functor from \mathbf{Bij} , the category of finite sets and bijections, to \mathbf{Set}_f , the category of finite sets and maps. A species S accompanies a formal power series in one variables:

$$S(t) = \sum_{n=0}^{\infty} \frac{|S([n])|}{n!} t^n,$$

4 PLETHYSM(4): SPECIES

where $[n] = \{1, 2, \dots, n\}$. For example, the species Tree of trees is the functor for which the value Tree(X) is the set of tree on X . Joyal defined the composition $T \circ S$ of species S, T such that $(T \circ S)(t) = T(S(t))$.

Furthermore, Bergeron (1987) generalized Joyal's composition of species to so-called S -species. Let \mathcal{P} be the category whose object is a pair (X, σ) of a finite set X and a permutation σ on X , and whose morphism $\theta : (x, \sigma) \rightarrow (Y, \tau)$ is a bijection $\theta : X \xrightarrow{\cong} Y$ such that $\theta\sigma = \tau\theta$.

For two S -species F, G , the value of the *plethysm composition* $G \circ F$ at (X, σ) consists of the triplets $(\pi, t_\pi, (m_i))$ satisfying the conditions :

- (a) $\pi = \{X_1, X_2, \dots\}$ is a partition of X with $\sigma(X_i) \in \pi$.
- (b) $t_\pi \in G[\pi, \sigma_\pi]$, where σ_π is a permutation on π defined by $\sigma_\pi : X_i \mapsto \sigma(X_i)$.
- (c) $m_i \in F[X_i, \sigma_i]$, $\sigma_i = \text{some } \sigma^k \text{ s.t. } \sigma^k(X_i) = X_i$.

Example. Let C_n ($n = 1, 2, \dots$) be S -species such that

$$C_n[X, \sigma] := \begin{cases} \{\sigma\} & \sigma \text{ a cycle on } X \text{ of length } n = |X|. \\ \emptyset & \text{else.} \end{cases}$$

Then

$$C_m \circ C_n = C_n \circ C_m = C_{mn}.$$

To an S -species $F : \mathcal{P} \rightarrow \text{Set}_f$, there associates a formal power series

$$F(t) := \sum_{\lambda} \frac{a_{\lambda}}{\text{aut}(\lambda)} t^{\lambda},$$

where $\lambda = (\lambda_1, \lambda_2, \dots)$ runs over partitions.

$$a_{\lambda} := |F[X, \sigma_{\lambda}]|, \quad \sigma_{\lambda} \in \text{Sym}(X) \text{ is of type } \lambda$$

$$\text{aut}(\lambda) := 1^{\lambda_1} \lambda_1! 2^{\lambda_2} \lambda_2! \dots$$

Then

$$(G \circ F)(t) = (G * F)(t),$$

that is, the generating function of $G \circ F$ equals to the plethysm composition of generating functions $F(t)$ and $G(t)$.

I do not think that the concept of S -species is rather bad because for a permutation σ of type λ ,

$$\text{aut}(\lambda) = 1^{\lambda_1} \lambda_1! 2^{\lambda_2} \lambda_2! \dots \neq 1^{\lambda_1} \lambda_1! 2^{\lambda_2} \lambda_2! \dots = |\text{Aut}(X, \sigma)|.$$

in general. The concept of plethysm for species and S -species is essentially the same as those of formal power series and can not be applied widely more than Plethysm (3).

5 Plethysm (5): FFFF

The concept of species and its generalization nowadays become one of the most useful tools in enumerative combinatorics. However, categorically viewing, the concept of species does not look to be a good mathematical concept. Why do we use \mathbf{Set}_f instead of \mathbf{Bij} ? Why do we consider, for example, the category of trees? The category of bijections \mathbf{Bij} is too poor. It is a groupoid and categorically equivalent to the disjoint union of symmetric groups S_n ($n = 0, 1, 2, \dots$). Comparing with \mathbf{Bij} , the category of finite sets and maps \mathbf{Set}_f is one of the best categories in all categories. Here we introduce a generalization of the concept of species by using the language of faithful functors with finite fibres (FFFF).

Assume that \mathcal{S} is a skeletally small category in which any object is decomposed into a coproduct of a finite number of connected objects. Here skeletal smallness means that the category is equivalent to a small category. A functor $F : \mathcal{E} \rightarrow \mathcal{S}$ is called *FFF-functor* if it is faithful and has finite fibers:

$$|F^{-1}(N)/\cong| := \#\{X \in \mathcal{E} \mid F(X) \cong N\}/\cong < \infty.$$

An \mathcal{E} -structure on N along an FFF-functor $F : \mathcal{E} \rightarrow \mathcal{S}$ is (X, σ) , where $X \in \mathcal{E}$ and $\sigma : F(X) \cong N$. We denote by $\mathbf{Str}(\mathcal{E}/N)$ the category of such \mathcal{E} -structures. Then the correspondence $N \mapsto \mathbf{Str}(\mathcal{E}/N)/\cong$, the set of isomorphism classes, is a species (on \mathcal{S}).

Let $S : \mathcal{S} \rightarrow \mathbf{Set}_f$ be a species (on \mathcal{S}). Then we have a category $\mathbf{Elt}_S(\mathcal{S})$ of *elements*, whose object is an element, that is, a pair (X, a) , where $X \in \mathcal{S}, a \in F(X)$.

Lemma. *There is a bijective correspondence up to isomorphism between FFF-functors and species by the above way.*

I think that the concept of FFF-functors is more convenient than those of species. We can now rewrite the plethysm composition for species or S -species by using FFF-functors. Let $F : \mathcal{E} \rightarrow \mathcal{S}, G : \mathcal{F} \rightarrow \mathcal{S}$ be two FFF-functors. We denote by $\mathbf{Con}(N)$ the set of coproduct components of N . Then we can define the *plethysm composition* of F and G by the following:

$$\begin{aligned} \mathcal{F} \circ_G \mathcal{E} &:= \{(Y, \mu) \mid Y \in \mathcal{F}, \mu : \mathbf{Con}(G(Y)) \rightarrow \mathcal{E}\} \\ G \circ F : \mathcal{F} \circ_G \mathcal{E} &\rightarrow \mathcal{S}; (Y, \mu) \mapsto \coprod_J F(\mu(J)) \times J \end{aligned}$$

6 Plethysm (6): Condition (P)

Let \mathcal{S} be the skeletally small category with finite coproducts, so that it has coproduct $X+Y$ and an initial object \emptyset . Then the dual category \mathcal{S}^{op} has finite products, and so the set of isomorphism classes of \mathcal{S}^{op} makes a semigroup with identity element. Let t^N denote the class of object of \mathcal{S}^{op} corresponding to an object N of \mathcal{S} . Then

$$\begin{aligned} t^M = t^N &\iff M \cong N \\ t^M \cdot t^N &= t^{M+N}, \quad t^\emptyset = 1. \end{aligned}$$

We can now construct the semigroup algebra $\mathbf{Q}[\mathcal{S}^{\text{op}}/\cong]$, which consists of finite summation

$$f(t) = \sum'_N a_N t^N,$$

where N runs over a complete set of representatives of isomorphism classes of objects of \mathcal{S} . When $\mathcal{S} = \mathbf{Set}_f$, an object of \mathbf{Set}_f is isomorphic to $[n] := \{1, 2, \dots, n\}$, and so $\mathbf{Q}[\mathcal{S}^{\text{op}}/\cong]$ is just the polynomial ring $\mathbf{Q}[t]$ in one variable. Thus we can view $\mathbf{Q}[\mathcal{S}^{\text{op}}/\cong]$ as a ring of polynomials with exponents in objects of \mathcal{S} . Assume furthermore that \mathcal{S} is a unique factorization category with $\emptyset, 1, X+Y, X \times Y$, and so on, if necessary. Let $\mathcal{I} = \text{Con}(\mathcal{S})$, the full subcategory of connected(= indec.) objects of \mathcal{S} . In the category \mathcal{S} , the unique factorization property means that any object X of \mathcal{S} can be uniquely factorized as a coproduct as follows:

$$X \cong \coprod_{I \in \mathcal{I}/\cong} m_I(X) I, \quad ; m_I(X) \geq 0$$

In this case, the "ring of polynomial ring" $\mathbf{Q}[[\mathcal{S}^{\text{op}}/\cong]]$ is really isomorphic to the usual polynomial ring $\mathbf{Q}[t^I \mid I \in \mathcal{I}/\cong]$.

Similarly, we can define the *ring of formal power series* as the complete semigroup ring $\mathbf{Q}[[\mathcal{S}^{\text{op}}/\cong]]$. Thus such a formal power series is an infinite sum of the form $\sum_N a_N t^N$, where N runs over a complete set of isomorphism classes of objects of \mathcal{S} .

It is natural to ask whether or not there exists a composition operator for polynomials and power series:

Question: How to define the composition $(g \circ f)(t)$ of two polynomials or power series $f(t), g(t)$?

6 PLETHYSM (6): CONDITION (P)

Of course, $g \mapsto g \circ f$ should be a ring homomorphism, and $t^N \circ t^M = t^{M \times N}$ should hold, too. But what does $(1+t^M)^N$, the composition of t^N and $1+t^M$, mean? How to define it?

In addition to the unique factorization property, assume that the product of connected objects is also connected:

Assumption (P) : $I, J \in \mathcal{I} \implies I \times J \in \mathcal{I}$.

For two power series

$$f(t) = \sum'_{M \in \mathcal{S}} \frac{a_M}{|\text{Aut}(M)|} t^M, \quad g(t) = \sum'_{N \in \mathcal{S}} \frac{b_N}{|\text{Aut}(N)|} t^N, \quad a_\emptyset = 0,$$

the *plethysm composition* of $f(t)$ and $g(t)$ is defined by

$$(g \circ f)(t) := \sum'_{N \in \mathcal{S}} \frac{b_N}{|\text{Aut}(N)|} f(t)^N,$$

where $N \cong \coprod_{J \in \mathcal{I}} m_J(N)J$ is a Krull-Schmidt decomposition in a strict sense of $N\mathcal{S}$ and

$$f(t)^N := \prod_J \left(\sum'_{M \in \mathcal{S}} \frac{a_M}{|\text{Aut}(M)|} t^{M \times J} \right)^{m_J(N)},$$

Clearly we have

$$t^I \circ t^J = t^{I \times J}, \quad (h \circ g) \circ f = h \circ (g \circ f)$$

and furthermore for $g(t) = t^J$ ($J \in \mathcal{I}$), we have

$$(g \circ f)(t) = (f \circ g)(t) = \sum'_M \frac{a_M}{|\text{Aut}(M)|} t^{M \times J}.$$

Example. When $\mathcal{S} = \text{Set}_f$, the category of finite sets, the above composition $(g \circ f)(t)$ is nothing but the usual composition of power series.

Example. Let Surj be the category of surjections $X \xrightarrow{\pi_X} \overline{X}$ of finite sets. The type of a surjection $X \xrightarrow{\pi_X} \overline{X}$ is

$$(\lambda_1, \lambda_2, \dots), \quad \text{where } \lambda_i := \#\{y \in \overline{X} \mid \#\pi^{-1}(y) = i\}.$$

7 PLETHYSM (7): FINITE GROUP ACTION

Then $\sum_i i\lambda_i = |X|$ and $\sum_i \lambda_i = |\bar{X}|$. An isomorphism class of surjections is bijectively corresponding to the partition. In fact, a surjection $X \xrightarrow{\pi_X} \bar{X}$ is decomposed as

$$\coprod_{y \in \bar{X}} ((\pi_X)^{-1}(y) \longrightarrow \{y\}).$$

Thus a connected object is isomorphic to $[n] := (\{1, 2, \dots, n\} \longrightarrow \{*\})$. Hence $\lambda = (\lambda_1, \lambda_2, \dots)$ and $X(\lambda) := \coprod \lambda_i [i]$ are bijectively corresponding. We have

$$|\text{Aut}(X(\lambda))| = \prod_i i!^{\lambda_i} \lambda_i! = \text{aut}(\lambda)$$

Clearly, $[i] \times [j] \cong [ij]$. Hence the composition defined in this section is the same as those of Plethysm (3).

Example. The category of rooted forests (disjoint unions of rooted trees) satisfies the property (P).

7 Plethysm (7): Finite Group Action

Let Γ be a finite group and let $\mathcal{S} := \text{Set}_\Gamma^\Gamma$ be the category of finite Γ -sets and Γ -maps. Unfortunately, the category \mathcal{S} does not satisfy the condition (P). In fact, the product $\Gamma/H \times \Gamma/K$ of transitive Γ -sets is not transitive in general. Thus the definition of the plethysm composition in $\mathbf{Q}[(\text{Set}_\Gamma^\Gamma)^{\text{op}} / \cong]$ given in the previous section can not applied in this case. To define plethysm composition for polynomials (or power series) with exponents in finite Γ -sets, we have to extend the definition of polynomials and power series.

We first consider usual polynomials in one variable with coefficients in non-negative integers. Such a polynomial $F(t)$ is constructed from a map $F \xrightarrow{\delta} 2^M$, where F, M are finite sets and 2^M is a power set of M , as follows:

$$F(t) = \sum_{f \in F} t^{|\delta(f)|} \in \mathbf{Q}[t]$$

Using this idea to the category of finite Γ -sets, we have a new definition of polynomials (with coefficients in non-negative integers).

Let Γ be a finite group. Then a *polynomial* with coefficients in non-negative integers of *degree* at most N is defined to be an isomorphism class of a Γ -map $[\delta : F \longrightarrow 2^M]$, where F, M are finite Γ -sets, 2^M is a power set with canonical

7 PLETHYSM (7): FINITE GROUP ACTION

Γ -action. Let $\mathbf{B}^+(2^M)$ be the set of the classes of polynomials of degree at most M , so that $\mathbf{B}^+(2^M)$ is an additive monoid with bilinear map

$$\mathbf{B}^+(2^M) \times \mathbf{B}^+(2^N) \longrightarrow \mathbf{B}^+(2^{M+N}); (F, G) \longmapsto F \times G$$

A polynomial with coefficients in a commutative ring k of degree at most M is defined to be an element of $k \otimes \mathbf{B}^+(2^M)$, the Grothendieck group of the additive monoid $\mathbf{B}^+(2^M)$ of Γ -sets over the Γ -set 2^M .

Let H be a subgroup of Γ and (x_J) variables associated to conjugacy classes of subgroups of Γ . $[F \xrightarrow{\delta_F} 2^M]$ a polynomial of degree at most M . For any $f \in F^H$, where F^H is the H -fixed point set of F , the subset $\delta_F(f) \subset M$ is an H -subset, and so we can consider the induced Γ -set $\delta_F(a) \uparrow^\Gamma = \text{Ind}_H^\Gamma(\delta_F(f))$. Let

$$\delta_F(f) \uparrow^\Gamma \cong \coprod'_{J \leq \Gamma} m_J(f)(\Gamma/J)$$

be an orbit decomposition. Then we have a ring homomorphism

$$\varphi_H : \mathbf{Q} \otimes \mathbf{B}^+(2^M) \longrightarrow \mathbf{Q}; [F \xrightarrow{\delta_F} 2^M] \longmapsto \sum_{f \in F^H} \prod'_{(J) \in C(\Gamma)} x_J^{m_J(f)}$$

Then $\varphi = (\varphi_H)_{(H) \in C(G)}$, where $C(G)$ denotes the set of all conjugacy classes of subgroups, is an injective ring homomorphism to $\mathbf{Q}[x_J \mid J \in C(\Gamma)]$

Take any polynomial $f(t) = \sum'_M a_M t^M$, where M runs over finitely many Γ -sets and a_M 's are non-negative integers. Then for each M , there is a finite set A_M with $|A_M| = a_M$. Let $A = \coprod'_M A_M$ and $M' = \coprod \{M \mid a_M \neq 0\}$. We assume that A has a trivial Γ -action. Then the assignment $a(\in A_M) \longmapsto M \subseteq M'$ is a Γ -map, and so we have a "polynomial" $A \longrightarrow 2^{M'}$, that is, our new definition of "polynomials" involves those of old definition of polynomials with exponents in finite Γ -sets.

Now the *plethysm composition* of $\delta_F : F \longrightarrow 2^M$ and $\delta_G : G \longrightarrow 2^N$ is defined as follows:

$$\begin{aligned} (G \xrightarrow{\delta_G} 2^N) \circ (F \xrightarrow{\delta_F} 2^M) &:= (G \circ F \xrightarrow{\delta_{G \circ F}} 2^{M \times N}) \\ G \circ F &:= \{(g, \mu) \mid g \in G, \mu : \delta_G(g)(\subseteq N) \longrightarrow F\}, \\ (g, \mu) &\longmapsto \{(i, j) \mid j \in \delta_G(g), i \in \delta_F(\mu(j))\} \subseteq M \times N. \end{aligned}$$

This definition can be uniquely extended to those of $F, G \in k \otimes \mathbf{B}^+(2^M)$.

8 PLETHYSM (8): TOPOS

In the trivial group case $\Gamma = 1$,

$$(G \circ F)(t) = G(F(t)),$$

where $F(t) := \sum_{f \in F} t^{|\delta(f)|}$, etc.

Example. Let $F := \mathbb{F}_q$, and let $N := \{1, \dots, n\}$ be the set of coordinates on which a finite group Γ acts. Then $F^N := \{v = (v_i)_{i \in N} \mid v_i \in F\}$ is an n -dimensional vector space over F with Γ -action. A Γ -code is a $F\Gamma$ -submodule $C \subseteq F^N$. Then there is a Γ -map called a support map:

$$\text{supp} : C \longrightarrow 2^N; u \longmapsto \{i \in N \mid u_i \neq 0\} \subseteq N.$$

In our viewpoint, $\text{supp} : C \longrightarrow 2^N$ is just a "polynomial". This "polynomial" is nothing but the weight enumerator polynomial

$$W_C(t) = \sum_{u \in C} t^{|\text{supp}(u)|} = \sum_{u \in C} t^{\text{wt}(u)}.$$

if we ignore the Γ -action. In general case, we can substitute a Γ -sets X, Y :

$$\begin{array}{ccc} W_C(X, Y) & \longrightarrow & C \\ \downarrow & & \downarrow \text{supp} \\ (X + Y)^N & \xrightarrow{\iota} & 2^N \end{array} \quad (\iota : \lambda \longmapsto \lambda^{-1}(Y)),$$

and so W_C becomes now a functor on finite Γ -sets in one or two variables. We can prove a MacWilliams type identity for W_C .

8 Plethysm (8): Topos

A topos is a set-like category and has any finite coproducts $X + Y$, finite products $X \times Y$, an initial object \emptyset , a terminal object $\mathbf{1}$, pull-backs $X \times_Z Y$, push-outs $X +_W Y$, exponential objects Y^X , a subobject classifier $\mathbf{1} \xrightarrow{t} \Omega$, power objects Ω^X , a partial map classifier (an injective hull) $\eta_X : X \longmapsto \tilde{X}$, and so on. Furthermore, a topos is a unique factorization category, and so any object is expressed as a finite coproducts of connected objects.

The most typical topos is the category of sets, in which the above objects are given by disjoint union, direct products, an empty set, a one-point set,

8 PLETHYSM (8): TOPOS

fiber products, fiber sums, mapping space, a two point set with base point, power sets, sets added base point.

We are especially interested in a so-called skeletally small and locally finite topos. Here a category is skeletally small if it is equivalent to a small category. Furthermore, a topos is locally finite if every hom-set is a finite set: $|\text{Hom}(X, Y)| < \infty$.

Example. Here we list some typical examples of skeletally small and locally finite toposes. We can treat such a topos as if it is \mathbf{Set}_f . The only properties which hold in \mathbf{Set}_f and do not hold in a general toposes are (XM) the exclusive middle ($(A^c)^c = A$), (B) Boolean algebra $\text{Sub}(X)$, (AC) Axiom of Choice, (CT) the connectivity of a terminal object $\mathbf{1}$.

(1) \mathbf{Set}_f : the category of finite sets and maps. In this topos, we have $Y^X = \text{Map}(X, Y)$, $\Omega = \mathbf{2} = \{0, 1\}$, $\tilde{X} = X + \mathbf{1}$. All of (XM), (B), (AC), (CT) hold.

(2) \mathbf{Set}_f^Γ : the category of finite Γ -sets and Γ -maps (Γ is a finite or infinite group), where $X + Y, X \times Y, Y^X, \Omega, \tilde{X}$, etc. are same as \mathbf{Set}_f . (AC) does not hold.

(3) \mathbf{Set}_f^S : the category of finite S -sets and S -maps (S is a finite monoid). In this topos, Y^X is given by the set $\text{Map}_S(S \times X, Y)$ of S -maps from $S \times X$ to Y , together with S -action defined by

$$(u, \lambda) \mapsto {}^u\lambda; (s, x) \mapsto \lambda(su, x).$$

Furthermore, the subobject classifier $t : \mathbf{1} \rightarrow \Omega$ is defined by

$$\Omega := \text{Sub}(S) = \{A \subseteq S \mid SA = A\}, \quad t : * \mapsto S.$$

(XM), (B), (AC) do not hold.

(4) \mathbf{Surj} : the category of surjection of finite sets. In this topos,

$$\Omega = (\mathbf{3} \rightarrow \mathbf{2}) = [2] + [1], \quad (Y \rightarrow \bar{Y})^{(X \rightarrow \bar{X})} = (Y^X \mapsto \bar{Y}^{\bar{X}}),$$

and so on. (XM), (B), (AC) do not hold.

(5) The categories of rooted forests of bounded height $\leq h$. The category of di-graphs. The category of functors from a finite category to \mathbf{Set}_f and natural transformations. (XM), (B), (AC), (CT) do not hold.

8 PLETHYSM (8): TOPOS

Now, Let \mathcal{E} be a skeletally small and locally finite topos, and put $\mathcal{I} := \text{Con}(\mathcal{E})$, the full subcategory of connected objects of \mathcal{E} . Sometimes, we write $|\text{Hom}(I, X)$ as $\varphi_I(X)$ for $I \in \mathcal{I}$. Then the following hold:

$$\begin{aligned} \varphi_I(X + Y) &= \varphi_I(X) + \varphi_I(Y), \quad \varphi_I(X \times Y) = \varphi_I(X) \cdot \varphi_I(Y), \\ X \cong Y &\iff \varphi_I(X) = \varphi_I(Y) \text{ for any } I \in \mathcal{I}. \end{aligned}$$

As is in the case of the category of finite Γ -sets, we consider a morphism of the form $\delta_F : F \longrightarrow \Omega^M$. From such a morphism, we can construct a functor $X \longmapsto F(X)$ by the pullback diagram:

$$\begin{array}{ccc} F(X) & \longrightarrow & F \\ \downarrow & & \downarrow \delta_F \\ \tilde{X}^N & \longrightarrow & \Omega^N \end{array}$$

Then $\varphi_I(F(X))$, $I \in \mathcal{I}$ can be presented by a polynomial in the variables $x_J := \varphi_J(X)$, $J \in \mathcal{I}$. Thus it is natural to define a *polynomial* of degree at most M with non-negative coefficients by a morphism of the form $\delta_F : F \longrightarrow \Omega^M$.

Take two "polynomials" $\delta_F : F \longrightarrow \Omega^M$ and $\delta_G : G \longrightarrow \Omega^N$. We can write the plethysm composition defined for "polynomials" in the case where $\mathcal{E} = \text{Set}_f^\Gamma$ by using only some standard operations inside the topos \mathcal{E} . The *plethysm composition* $\delta_{G \circ F} : G \circ F \longrightarrow \Omega^{M \times N}$ is constructed by the the following pullback square:

$$\begin{array}{ccccc} G \circ F & \longrightarrow & \tilde{F}^N & \longrightarrow & \Omega^{M \times N} \\ \downarrow & & \downarrow & & \\ G & \xrightarrow{\delta_G} & \Omega^N & & \end{array}$$

Here the vertical arrow $\tilde{F}^N \longrightarrow \Omega^N$ is constructed as follows:

$$(F \longrightarrow 1) \longmapsto (\tilde{F} \longrightarrow \tilde{1} = \Omega) \longmapsto (\tilde{F}^N \longrightarrow \Omega^N).$$

Next $\tilde{F}^N \longrightarrow \Omega^{M \times N}$ is constructed as follows:

$$(\tilde{F} \xrightarrow{\delta_F} \widetilde{\Omega^M} \xrightarrow{\rho} \Omega^M) \longmapsto (\tilde{F}^N \longrightarrow (\Omega^M)^N = \Omega^{M \times N}),$$

where ρ is the retraction of the subobject $\Omega^M \hookrightarrow \widetilde{\Omega^M}$.

9 Plethysm (9): Tambara Functor

In the final section, we study the "polynomial" and "power series" with coefficients. The most suitable coefficients ring of polynomials is a Tambara functor.

Let \mathcal{E} be a skeletally small and locally finite topos. A *Tambara functor* \mathbf{T} from \mathcal{E} to the category of commutative semirings is a functor equipped with three kinds of maps additive transfer, restriction and multiplicative transfer. Thus each $\mathbf{T}(X)$ has a semi-ring structure, and to each $f : X \rightarrow Y$, \mathbf{T} assigns three maps

$$\begin{aligned} f_! &: \mathbf{T}(X) \rightarrow \mathbf{T}(Y) \quad (\text{additive transfer}), \\ f^* &: \mathbf{T}(Y) \rightarrow \mathbf{T}(X) \quad (\text{restriction}), \\ f_* &: \mathbf{T}(X) \rightarrow \mathbf{T}(Y) \quad (\text{multiplicative transfer}). \end{aligned}$$

Here $f_!$ is an additive map called a transfer map, f^* is a semi-ring homomorphism called a restriction map, and f_* is a multiplicative map.

For example, for a finite group Γ and a commutative ring k , the functors $X \mapsto G_0(\text{Mod}^{k\Gamma}/X)$ (the character ring functor of a finite group), $X \mapsto G_0(\text{Set}_f^\Gamma/X)$ (the Burnside ring functor), and $\text{Ext}_{k\Gamma}^{**}(kX, A)$ (the cohomology ring functor with coefficients in a commutative ring A) are all Tambara functors together with additive transfer (or additive induction), restriction, and multiplicative transfer (or multiplicative induction). The notation \mathcal{E}/X denotes the so-called comma category, that is, its object has the form $A \rightarrow X$. Furthermore, $X \mapsto 2^X$ (power set) is a Tambara functor from Set_f . In fact, for a map $f : X \rightarrow Y$, the structure maps are given by $f_!(A) = A$, $f^*(B) = f^{-1}(B)$ and $f_*(A) = \{y \in Y \mid f^{-1}(y) \subseteq A\}$.

The easiest example of Tambara functors on Set_f^Γ is $X \mapsto \text{Map}_\Gamma(X, A) = \text{Ext}_{k\Gamma}^0(X, A)$, where A is a commutative Γ -algebra over a commutative ring k . The three maps are given by

$$\begin{aligned} f_!(\lambda) &: y \mapsto \sum_{x \in f^{-1}(y)} \lambda(x), & f^*(\mu) &: x \mapsto \mu(f(x)), \\ f_*(\lambda) &: y \mapsto \prod_{x \in f^{-1}(y)} \lambda(x), \end{aligned}$$

where $\lambda : X \rightarrow A$ is a Γ -map and $f : X \rightarrow Y$ is a Γ -map between finite Γ -sets X, Y .

9 PLETHYSM (9): TAMBARA FUNCTOR

Now let \mathbf{T} be a Tambara functor on \mathcal{E} . Then any monomorphism $j : N \rightarrow N'$ induces additive maps as follows:

$$j_! : \mathbf{T}(\Omega^N) \rightarrow \mathbf{T}(\Omega^{N'}), \quad j^* : \mathbf{T}(\Omega^{N'}) \rightarrow \mathbf{T}(\Omega^N).$$

Thus we have a pair of covariant and contravariant functors $(-)_!, (-)^* : N \rightarrow \mathbf{T}(\Omega^N)$ from \mathcal{E}_{mon} to Mod_k which are same on objects. Thus we can consider the colimits and limits, and then we have the ring of polynomials and the ring of formal power series with exponents in \mathcal{E} and with coefficients in \mathbf{T} defined by

$$\text{Pol}(\mathcal{E}) := \varinjlim \mathbf{T}(\Omega^N), \quad \text{Pow}(\mathcal{E}) := \varprojlim \mathbf{T}(\Omega^N).$$

Similarly, we can define the ring of Hurwitz series by $\varprojlim \mathbf{T}(\Omega^N)/\text{Aut}(N)$.

We can now construct the *plethysm composition* for our polynomials. To do it, we only need to construct the map

$$\circ : \mathbf{T}(\Omega^N) \times \mathbf{T}(\Omega^M) \mapsto \mathbf{T}(\Omega^{M \times N}).$$

We first consider the following sequence of morphisms in \mathcal{E} :

$$\begin{array}{c} \Omega^M \xrightarrow{\eta} \widetilde{\Omega^M} \xrightarrow{(\rho, \chi_\eta)} \Omega^M \times \Omega \xleftarrow{ev} \\ (\Omega^M \times \Omega)^N \times N \xrightarrow{\pi} (\Omega^M \times \Omega)^N = \Omega^{M \times N} \times \Omega^N, \end{array}$$

where (i) $\rho : \widetilde{\Omega^M} \rightarrow \Omega^M$ is the canonical retraction to the inclusion $\eta : \Omega^M \rightarrow \widetilde{\Omega^M}$, (ii) $\chi_\eta : \widetilde{\Omega^M} \rightarrow \Omega$ is the characteristic morphism of the subobject $\eta : \Omega^M \rightarrow \widetilde{\Omega^M}$, (iii) $ev : X^N \times N \rightarrow X$ is the evaluation morphism, which is the adjoint to $\text{id} : X^N \rightarrow X^N$ ($X := \Omega^M \times \Omega$), (iv) π is the projection to the first constitute.

Thus applying the operators in the Tambara functor \mathbf{T} , we have the following map:

$$\begin{array}{c} \mathbf{T}(\Omega^M) \xrightarrow{\eta_*} \mathbf{T}(\widetilde{\Omega^M}) \xrightarrow{(\rho, \chi_\eta)_!} \mathbf{T}(\Omega^M \times \Omega) \xrightarrow{ev^*} \\ \mathbf{T}((\Omega^M \times \Omega)^N \times N) \xrightarrow{\pi_*} \mathbf{T}((\Omega^M \times \Omega)^N) = \mathbf{T}(\Omega^{M \times N} \times \Omega^N), \end{array}$$

Next, let

$$\pi^* : \mathbf{T}(\Omega^N) \rightarrow \mathbf{T}(\Omega^{M \times N} \times \Omega^N)$$

be the map induced from the projection $\Omega^{M \times N} \times \Omega^N \rightarrow \Omega^N$.

9 PLETHYSM (9): TAMBARA FUNCTOR

At last, we have the required map

$$\circ : \mathbf{T}(\Omega^N) \times \mathbf{T}(\Omega^M) \xrightarrow{\langle , \rangle} \mathbf{T}(\Omega^{MN} \times \Omega^N) \xrightarrow{\pi_1} \mathbf{T}(\Omega^{M \times N}),$$

where \langle , \rangle is the pairing operator in the Tambara functor \mathbf{T} and π is the projection.

This definition of polynomials and plethysm composition look complicated a little, but we can treat such polynomials as if they are in one variable. Here is an example. The *derivation* $\partial F \rightarrow \Omega^M$ of $\delta : F \rightarrow \Omega^M$ is defined by the subobject classified by $\widehat{\delta} : F \times M \rightarrow \Omega$ which is the transpose of δ . Furthermore, let \in_M be the subobject classified by $\text{ev} : \Omega^M \times M \rightarrow \Omega$, and so we have a morphism $\partial : \in_M \rightarrow \Omega^M$. Then the operation $\partial_! \partial^*$ on $\mathbf{T}(\Omega^M)$ induced by ∂ is just the derivation corresponding to $t d/dt$. Of course, usual derivation laws hold, especially $\partial(G \circ F) = \partial(G)(F) \cdot \partial(F)$. Furthermore, there is a Tambara functor version of derivation, too.

References

- [BLL] F.Bergeron, G.Labbell, P.Leroux, "Combinatorial Species and Tree-like Structures", Encyclopedia of Math., Cambridge, 1998.
- [J] P.T.Johnstone, "Topos Theory", Academic Press, 1977.
- [J] A.Joyal, Une théorie combinatoire des series formelles, Advances in Math. 42 (1981), 1–82.
- [M] I.G.Macdonald, "Symmetric Functions and Hall Polynomials" (2nd Edition), Oxford, 1995.
- [Y1] T.Yoshida, Categorical aspects to generating functions (I), J.Algebra,
- [Y2] T.Yoshida, Categorical aspects to generating functions (II), preprint.

$(r, 2r)$ 型超幾何関数の選点直交多項式

Discrete orthogonal polynomials obtained from $(r, 2r)$ -hypergeometric functions

水川裕司 (Hiroshi Mizukawa)

*Division of Mathematics, Hokkaido University, Sapporo 060-0810, Japan **

e-mail: mzh@math.sci.hokudai.ac.jp

1 序

群とその部分群のペア, (G, H) が Gelfand pair とは誘導表現 1_H^G が G -module として無重複であることである. このとき of 1_H^G の各既約成分に (定数倍を除いて) 一意的に H -不変な現が存在し, それを zonal spherical function と言う. 坂内-伊藤の本 [5] に有限群の Gelfand pair から得られる選点直交多項式についての記述があるが, ここでは B 型 Weyl 群と対称群のなす, $(W(B_n), S_n)$ というペアから得られる Krautchook 多項式と言う選点直交多項式の一般化を試みたいと思う. そしてその結果が多変数の超幾何である $(n+1, m+1)$ 型超幾何関数と呼ばれる物で記述できることを見る.

2 有限群の Gelfand Pair

G を有限群, そして H をその部分群とする.

Definition 2.1. 誘導表現 1_H^G が無重複のとき, (G, H) を *Gelfand pair* とよぶ.

さて, 以下では (G, H) を Gelfand pair とする, そして誘導表現 1_H^G が以下のように分解しているとする;

$$V = 1_H^G = \bigoplus_{i=1}^s V_i, \quad V_i \not\cong V_j \quad (i \neq j).$$

このとき事実として $s = |H \backslash G / H|$ である.

$$\{g_i; 1 \leq i \leq s\}$$

*Current Address : Department of Mathematics, Faculty of Science, Okayama University, Okayama 700-8530, Japan

を両側剰余類 $H \backslash G / H$ の代表系とする. さらに $D_i = H g_i H$ とおく. V_i^H を V_i の H -不変部分空間とする. Frobenius の相互律から;

$$\dim V_i^H = \langle V_i, 1_H \rangle_H = \langle V_i, 1_H^G \rangle_G = 1$$

である. ここで $\langle V, W \rangle_G$ は交叉数である. $[*]*$ を V_i 上定義された G -不変な複素内積, そして $\dim V_i = n$ とする. いま

$$\{v_1^i, \dots, v_n^i\}$$

を V_i の正規直交基底, ただし $v_1^i \in V_i^H$ とする. $(\rho_{k\ell}^i)_{1 \leq k, \ell \leq n}$ を G の V_i 上の行列表現とする. $C(G/H)$ を各右側剰余類上定置な G 上の関数とする, とまり,

$$C(G/H) := \{f : G \rightarrow \mathbb{C}; f(xh) = f(x) \forall x \in G, \forall h \in H\}$$

である. このとき $\dim C(G/H) = [G : H]$ は明らかである. 線形写像

$$\varphi_i : V_i \rightarrow C(G/H)$$

を $g, h \in G$ and $v \in V_i$. に対して

$$\varphi_i(v)(g) = [v|gv_1^i]$$

で定義する.

$$\varphi_i(gv)(k) = [gv|kv_1^i] = [v|g^{-1}kv_1^i] = \varphi_i(v)(g^{-1}k) = (g\varphi_i(v))(k)$$

かつ $\varphi \neq 0$ なので, φ は単射な G -線形写像である. そして次を得る,

$$C(G/H) = \bigoplus_{i=1}^s \varphi_i(V_i).$$

いま, $\omega_i \in \varphi_i(V_i)$ を $g \in G$ に対して, $\omega_i(g) = [v_1^i|gv_1^i] = \overline{\rho_{11}^i(g)}$ で定義する. 上での議論から,

$$\varphi_i(V_i)^H = \mathbb{C}\omega_i$$

である.

Definition 2.2. 関数 ω_i を (G, H) の zonal spherical functions とよぶ.

いかにこの zonal spherical function の幾つか挙げておく.

Proposition 2.3. (1) $g \in G$ と $h_1, h_2 \in H$ に対して,

$$\omega_i(h_1 g h_2) = \omega_i(g).$$

(2) 任意の $g \in G$ に対して $\omega_i(1) = 1$ かつ $\omega_i(g^{-1}) = \overline{\omega_i(g)}$.

次が zonal spherical function の直交性である.

Proposition 2.4. $g \in D_k$ に対して $\omega_i(D_k) = \omega_i(g_i)$ と書いたとき,

$$\frac{1}{|G|} \sum_{k=1}^s |D_k| \omega_i(D_k) \overline{\omega_j(D_k)} = \delta_{ij} \dim V_i^{-1}$$

である.

3 Gelfand Pair $(G(r, 1, n), S_n)$ とその Zonal Spherical Function について

$\mathbb{N}_0 = \{0, 1, 2, \dots\}$ を自然数の集合とする. ここでは正の整数 r を固定する. 一の原始 r 乗根を $\xi = \exp 2\pi\sqrt{-1}/r$ と置く. $C^n = \langle \xi \rangle \times \dots \times \langle \xi \rangle$ を cyclic group $C = \langle \xi \rangle$ の n 個の直積とする. 対称群 S_n は C^n 上に次のように作用する.

$$\sigma(\xi_1, \xi_2, \dots, \xi_n) = (\xi_{\sigma^{-1}(1)}, \xi_{\sigma^{-1}(2)}, \dots, \xi_{\sigma^{-1}(n)}), \quad (\xi_1, \xi_2, \dots, \xi_n) \in C^n, \\ \sigma \in S_n.$$

wreath product $C \wr S_n$ とはこの作用から得られる半直積群のことである [11, 14]. この群を $G(r, 1, n) = C \wr S_n$ と書き複素鏡映群という. この節では, $G = G(r, 1, n)$ とその部分群 $H = G(1, 1, n) = S_n$ を考える.

まずは両側剰余類の記述から述べよう.

Proposition 3.1. (1) 両側剰余類の代表系 $\mathcal{D}_{r,n}$ は次で与えられる.

$$\mathcal{D}_{r,n} = \left\{ \underbrace{(1, \dots, 1)}_{\ell_0}, \underbrace{(\xi_1, \dots, \xi_1)}_{\ell_1}, \dots, \underbrace{(\xi^{r-1}, \dots, \xi^{r-1})}_{\ell_{r-1}}, 1 \in G; \sum_{i=0}^{r-1} \ell_i = n \right\}.$$

(2) 代表系の個数は

$$|H \backslash G / H| = \binom{n+r-1}{n}$$

である.

群 G は n -変数の多項式の空間に

$$(\xi_1, \xi_2, \dots, \xi_n; \sigma) f(x_1, \dots, x_n) = f(\xi_{\sigma(1)}^{-1} x_{\sigma(1)}, \xi_{\sigma(2)}^{-1} x_{\sigma(2)}, \dots, \xi_{\sigma(n)}^{-1} x_{\sigma(n)})$$

のように作用する. 以下この作用を用いて誘導表現の既約分解の実現を考えよう. \mathbb{N}_0^n から分割数全体 Par への写像を,

$$\psi: \mathbb{N}_0^n \ni (k_0, k_1, \dots, k_{r-1}) \mapsto (0^{k_0} 1^{k_1} \dots (r-1)^{k_{r-1}}) \in Par$$

で定義する. この写像を用いて次の定理を得る.

Proposition 3.2. 誘導表現 $1_{S_n}^{G(r,1,n)}$ は,

$$1_{S_n}^{G(r,1,n)} \cong \bigoplus_{\sum_{i=0}^{r-1} k_i = n} V^{(k_0, k_1, \dots, k_{r-1})}$$

と分解する. ここで各 $V^{(k_0, k_1, \dots, k_{r-1})}$ は既約な $G(r, 1, n)$ -加群であり次のように定義される;

$$V^{(k_0, k_1, \dots, k_{r-1})} = \bigoplus_{f \in M_n(\psi(k_0, k_1, \dots, k_{r-1}))} \mathbb{C}f.$$

ここで, $\lambda = (\lambda_1, \dots, \lambda_n)$ に対して,

$$M_n(\lambda) = \{x_{\sigma(1)}^{\lambda_1} x_{\sigma(2)}^{\lambda_2} \cdots x_{\sigma(n)}^{\lambda_n}; \sigma \in S_n\}$$

である.

この分解に現れる既約成分は複素鏡映群の Specht 加群の内一成分からなる分割でパラメトライズされるもの全てである. さらに, これは特に無重複である, 因って次が言えたことになる.

Proposition 3.3. (G, H) は Gelfand pair.

Example 3.4. $G = G(3, 1, 3)$ and $H = S_3$ として例を見てみよう. 誘導表現 1_H^G は次のように分解する:

$$\begin{aligned} 1_H^G = & V^{(3,0,0)} \oplus V^{(0,3,0)} \oplus V^{(0,0,3)} \oplus V^{(2,1,0)} \oplus V^{(2,0,1)} \\ & \oplus V^{(1,2,0)} \oplus V^{(1,0,2)} \oplus V^{(0,2,1)} \oplus V^{(0,1,2)} \oplus V^{(1,1,1)}. \end{aligned}$$

幾つかの既約成分を書き下してみよう:

$$V^{(0,1,2)} = \mathbb{C}x_1^2x_2x_3 \oplus \mathbb{C}x_1^2x_3x_2 \oplus \mathbb{C}x_2^2x_3x_1, \quad V^{(0,3,0)} = \mathbb{C}x_1x_2x_3.$$

これをみていると 例えば S_3 不変な $V^{(0,2,1)}$ の部分空間は

$$\mathbb{C}(x_1^2x_2x_3 + x_1^2x_3x_2 + x_2^2x_3x_1)$$

で有ることがわかる. これは monomial symmetric polynomial と呼ばれる対象多項式である. 勿論これは S_n -不変な元でも有る.

これより下は内積を定義し zonal spherical function を考える.

各既約成分 $V^{(k_0, k_1, \dots, k_{r-1})}$ 上の内積を

$$[\alpha x^\lambda | \beta x^\mu] = \alpha \bar{\beta} \delta_{\lambda, \mu} \frac{1}{\binom{n}{k_0, k_1, \dots, k_{r-1}}}$$

で定義する. ここで α と β は複素数である, k_i は λ のなかで i に等しい成分の数, そして $x^\lambda = x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ とする. この内積は $G(r, 1, n)$ -不変であることがすぐわかる, つまり, $g \in G(r, 1, n)$, $f_1(x), f_2(x) \in V^{(k_0, k_1, \dots, k_{r-1})}$ に対して

$$[(gf_1)(x) | (gf_2)(x)] = [f_1(x) | f_2(x)]$$

である. monomial symmetric polynomial を定義しておこう.

$$\lambda = (\lambda_1, \lambda_2, \dots) = (0^{k_0} 1^{k_1} 2^{k_2} \cdots (r-1)^{k_{r-1}})$$

, に対して monomial symmetric polynomial とは,

$$\begin{aligned} m_\lambda(x) &= \frac{1}{k_0!k_1!\cdots k_n!} \sum_{\sigma \in S_n} x_{\sigma(1)}^{\lambda_1} x_{\sigma(2)}^{\lambda_2} \cdots x_{\sigma(n)}^{\lambda_n} \\ &= \sum_{I_n^{k_0 k_1 \cdots k_{r-1}}} x_{i_1^{(0)}}^0 \cdots x_{i_{k_0}^{(0)}}^0 x_{i_1^{(1)}}^1 \cdots x_{i_{k_1}^{(1)}}^1 \cdots x_{i_1^{(r-1)}}^{r-1} \cdots x_{i_{k_{r-1}}^{(r-1)}}^{r-1}. \end{aligned}$$

で定義される対称多項式である. ここで, $I_n^{k_j} = \{i_1^{(j)} \cdots i_{k_j}^{(j)}; 1 \leq i_1^{(j)} < \cdots < i_{k_j}^{(j)} \leq n\}$ に対して $I_n^{k_0 k_1 \cdots k_{r-1}} = \{i^{(0)}, \dots, i^{(r-1)}; i^{(j)} \in I_n^{k_j}, \cup_{i=0}^{r-1} i^{(j)} = \{1, 2, \dots, n\}\}$ である. 明らかに monomial symmetric polynomial は

$$[m_\lambda(x)|m_\mu(x)] = \delta_{\lambda\mu}$$

を満たす. $g = (\xi_1, \xi_2, \dots, \xi_n; \sigma) \in G$ と置いて次のように計算する:

$$\begin{aligned} [m_\lambda(x)|(gm_\lambda)(x)] &= [m_\lambda(x)|m_\lambda(\xi_{\sigma(1)}^{-1}x_{\sigma(1)}, \xi_{\sigma(2)}^{-1}x_{\sigma(2)}, \dots, \xi_{\sigma(n)}^{-1}x_{\sigma(n)})] \\ &= \frac{[x^\lambda|x^\lambda]}{k_0!k_1!\cdots k_n!} \sum_{\sigma \in S_n} \xi_{\sigma(1)}^{\lambda_1} \xi_{\sigma(2)}^{\lambda_2} \cdots \xi_{\sigma(n)}^{\lambda_n} \\ &= m_\lambda(\xi_1, \xi_2, \dots, \xi_n)/m_\lambda(1, \dots, 1). \end{aligned}$$

これで (G, H) の zonal spherical function の対称多項式による表示が得られた.

Theorem 3.5. *Gelfand pair (G, H) の zonal spherical function は*

$$\omega^{(k_0, k_1, \dots, k_{r-1})}(\xi_1, \xi_2, \dots, \xi_n; \sigma) = m_\lambda(\xi_1, \xi_2, \dots, \xi_n)/m_\lambda(1, \dots, 1)$$

で得られる. ここで $\lambda = (0^{k_0} 1^{k_1} 2^{k_2} \cdots (r-1)^{k_{r-1}})$ そして $\sum_{i=0}^{r-1} k_i = n$ である.

4 $(G(r, 1, n), S_n)$ の Zonal Spherical Functions を Hypergeometric Functions で表示する

この節での目的は前節の zonal spherical function を各両側剰余類上で評価し超幾何関数で表示することである.

そのために必要な記号を用意しよう.

$$\frac{1}{(n-m)!} = (-1)^m \frac{(-n)_m}{n!},$$

ここで $(x)_m$ は shifted factorial である, つまり, x を不定元として $m > 0$ ならば,

$$(x)_m = x(x+1)(x+2) \cdots (x+m-1)$$

そして $m = 0$ ならば,

$$(x)_0 = 1$$

である. 以下ではもし $n - m$ が負の整数ならば $\frac{1}{(n-m)!} = 0$ であることに注意しよう. $m, m_i (1 \leq i \leq k-1) \in \mathbb{N}_0$ にたいして

$$\binom{x}{m} = (-1)^m \frac{(-x)_m}{m!}$$

かつ

$$\binom{x}{m_1, \dots, m_{k-1}, x - \sum_{i=1}^{k-1} m_i} = (-1)^{\sum_{i=1}^{k-1} m_i} \frac{(-x)_{\sum_{i=1}^{k-1} m_i}}{\prod_{i=1}^{k-1} m_i!}.$$

と定義する. 定義からすぐわかることは $n \in \mathbb{Z}$ にたいして,

$$(n)_{s-t} = \frac{(n)_s}{(-n-s+1)_t} (-1)^t$$

である. ここで超幾何関数達を定義しておこう.

Gauss' hypergeometric functions [2, 8, 18]

$${}_2F_1(a, b; c; x) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k}{(c)_k} \frac{x^k}{k!}.$$

Appell-Lauricella's hypergeometric functions

$b = (b_1, \dots, b_d) \in \mathbb{C}^d$ とする.

$$F_D(a, b; c; x) = \sum_{(m_1, \dots, m_d) \in \mathbb{N}_0^d} \frac{(a)_{m_1 + \dots + m_d} \prod (b_i)_{m_i} x_1^{m_1} \dots x_d^{m_d}}{(c)_{m_1 + \dots + m_d} m_1! \dots m_d!}$$

そしてこれらを含むより一般的な超幾何関数として次が知られている.

$(n+1, m+1)$ -hypergeometric functions [3, 9, 10, 12, 13, 18]

$\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{C}^n, \beta = (\beta_1, \dots, \beta_{m-n-1}) \in \mathbb{C}^{m-n-1}$ そして $X = (x_{ij})_{\substack{1 \leq i \leq n, \\ 1 \leq j \leq m-n-1}}$.

$$F(\alpha, \beta; \gamma, X) = \sum_{(a_{i,j}) \in M_{n, m-n-1}(\mathbb{N}_0)} \frac{\prod_{i=1}^n (\alpha_i)_{\sum_{j=1}^n a_{i,j}}, \prod_{i=1}^{m-n-1} (\beta_i)_{\sum_{j=1}^{m-n-1} a_{j,i}}}{(\gamma)_{\sum_{i,j} a_{i,j}}} \frac{\prod x_{ij}^{a_{i,j}}}{\prod a_{i,j}!}.$$

これは一般には無限級数だが, $\gamma = -N$ ならば, 定義を次のように修正し多項式になる.

$$F(\alpha, \beta; -N, X) = \sum_{\substack{\sum_{i,j} a_{i,j} \leq N \\ (a_{i,j}) \in M_{n, m-n-1}(\mathbb{N}_0)}} \frac{\prod_{i=1}^n (\alpha_i)_{\sum_{j=1}^n a_{i,j}}, \prod_{i=1}^{m-n-1} (\beta_i)_{\sum_{j=1}^{m-n-1} a_{j,i}}}{(-N)_{\sum_{i,j} a_{i,j}}} \frac{\prod x_{ij}^{a_{i,j}}}{\prod a_{i,j}!}.$$

以下扱うのはこの多項式のケースである. 前節同様 $\lambda = (0^{k_0} 1^{k_1} \dots (r-1)^{k_{r-1}})$ と仮定する.

$$m_{(\ell_0, \ell_1, \dots, \ell_{r-1})}^{(k_0, k_1, \dots, k_{r-1})} = m_{\lambda}(\underbrace{1, \dots, 1}_{\ell_0}, \underbrace{\xi, \dots, \xi}_{\ell_1}, \dots, \underbrace{\xi^{r-1}, \dots, \xi^{r-1}}_{\ell_{r-1}})$$

と定義する. 同様に,

$$\omega_{(\ell_0, \ell_1, \dots, \ell_{r-1})}^{(k_0, k_1, \dots, k_{r-1})} = \frac{1}{\binom{n}{k_0, k_1, \dots, k_{r-1}}} m_{(\ell_0, \ell_1, \dots, \ell_{r-1})}^{(k_0, k_1, \dots, k_{r-1})}$$

と置く.

Proposition 4.1. $\ell_0 + \ell_1 + \dots + \ell_{r-1} = k_0 + k_1 + \dots + k_{r-1} = n$ としたとき.

(1)

$$m_{(\ell_0, \ell_1, \dots, \ell_{r-1})}^{(k_0, k_1, \dots, k_{r-1})} = \sum_{a \in \mathcal{A}} \prod_{i=0}^{r-1} \binom{\ell_i}{a_{i0}, a_{i1}, \dots, a_{i,r-1}} \xi^{\sum_{0 \leq i, j \leq r-1} i j a_{i,j}},$$

ここで,

$$\mathcal{A} = \mathcal{A}_{(\ell_0, \ell_1, \dots, \ell_n)}^{(k_0, k_1, \dots, k_n)} = \{a = (a_{ij}) \in M(r, \mathbb{N}_0); \sum_{i=0}^{r-1} a_{ij} = k_j, \sum_{j=0}^{r-1} a_{ij} = \ell_i\}.$$

(2) 母関数は

$$\sum_{k_0 + \dots + k_{r-1} = n} m_{(\ell_0, \ell_1, \dots, \ell_n)}^{(k_0, k_1, \dots, k_n)} t_0^{k_0} t_1^{k_1} \dots t_{r-1}^{k_{r-1}} = \prod_{i=0}^{r-1} (\sum_{j=0}^{r-1} \xi^{ij} t_j)^{\ell_i}$$

で与えられる.

Example 4.2. $r = 3$ and $n = 4$ で例を見てみよう. $(k_0, k_1, k_2) = (1, 1, 2)$ そして $(\ell_0, \ell_1, \ell_2) = (1, 2, 1)$ の場合. 直接計算では,

$$\begin{aligned} \omega_{(1,2,1)}^{(1,1,2)} &= \frac{1}{12} m_{2211} (1, \xi, \xi, \xi^2) \\ &= \frac{1}{12} (2\xi^3 + 3\xi^4 + 2\xi^5 + 3\xi^6 + 2\xi^7) = -\frac{1}{4} \xi^2. \end{aligned}$$

それで, 命題から

$$\mathcal{A}_{(1,2,1)}^{(1,1,2)} = \left\{ \begin{pmatrix} 1 & & \\ & 2 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & 1 \\ & 1 & \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & 1 \\ & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & 1 \end{pmatrix}, \begin{pmatrix} & 1 & \\ & & 1 \\ 1 & & 1 \end{pmatrix}, \begin{pmatrix} & 1 & \\ & & 2 \\ 1 & & \end{pmatrix} \right\}$$

であり、これより

$$\begin{aligned}\omega_{(1,2,1)}^{(1,1,2)} &= \frac{1}{12} m_{(1,2,1)}^{(1,1,2)} = \frac{1}{12} (\xi^6 + 2\xi^5 + 2\xi^7 + 2\xi^4 + 2\xi^6 + 2\xi^3 + \xi^4) \\ &= \frac{1}{12} (2\xi^3 + 3\xi^4 + 2\xi^5 + 3\xi^6 + 2\xi^7) = -\frac{1}{4} \xi^2\end{aligned}$$

と言う風に計算できる。

これの何処が超幾何なんだ!と思われるであろうが、ここまで来ればかなり良い線行っているのである。後は有限離散版(?)のPfaffの公式(特異点の交換)の様なことをすれば目的を達成できる。そのための準備をしよう。

Lemma 4.3.

$$m_{(\ell_0, \ell_1, \dots, \ell_{r-1})}^{(k_0, k_1, \dots, k_{r-1})} = \sum_{a \in \mathcal{A}} \binom{n - \sum a_{ij}}{k_0, a_{01}, \dots, a_{0r-1}} \prod_{i=1}^{r-1} \left[\binom{\ell_i}{a_{i0}, a_{i1}, \dots, a_{ir-1}} \prod_{j=1}^{r-1} (\xi^{ij} - 1)^{a_{ij}} \right]$$

そして、もう一つ

Lemma 4.4. $a_{0j} = k_j - \sum_{i=1}^{r-1} a_{ij}$ として $k_0 = n - \sum_{i=1}^{r-1} k_i$ と置くと、

$$\binom{n - \sum_{ij} a_{ij}}{k_0, a_{01}, \dots, a_{0r-1}} = \binom{n}{k_0, \dots, k_{r-1}} \frac{\prod_{j=1}^{r-1} (-k_j)^{\sum_{i=1}^{r-1} a_{ij}}}{(-n)^{\sum_{1 \leq i, j \leq r-1} a_{ij}}}$$

を得る。

そして、これを組み合わせると次のような定理が得られる。

Theorem 4.5. *Gelfand pair* $(G(r, 1, n), S_n)$ の *zonal spherical function* は $(n+1, m+1)$ -*hypergeometric function* で次のように表示される。

$$\omega_{(\ell_0, \ell_1, \dots, \ell_n)}^{(k_0, k_1, \dots, k_n)} = F((-\ell_1, \dots, -\ell_{r-1}), (-k_1, \dots, -k_{r-1}); -n; \tilde{\Xi}_r).$$

ここで $\tilde{\Xi}_r = (1 - \xi^{ij})_{1 \leq i, j \leq r-1}$ である。

さらに Proposition 2.4 の直交性をこのケースの場合に書き下してみる。

Theorem 4.6. もし $k = (k_0, k_1, \dots, k_{r-1})$ が $\sum_{i=0}^{r-1} k_i = n$ を満たすとき、

$$\begin{aligned}\frac{1}{r^n} \sum_{\ell \in \mathcal{D}_{r,n}} \binom{n}{\ell_0, \dots, \ell_{r-1}} F(-\bar{\ell}, -\bar{k}; -n; \tilde{\Xi}) \overline{F(-\bar{\ell}, -\bar{k}'; -n; \tilde{\Xi})} \\ = \binom{n}{k_0, \dots, k_{r-1}}^{-1} \prod_{i=0}^{r-1} \delta_{k_i, k_i'}\end{aligned}$$

である。ここで $\ell = (\ell_0, \ell_1, \dots, \ell_{r-1})$ に対して $\bar{\ell} = (\ell_1, \dots, \ell_{r-1})$ と置いた。

なお、ここで得られた超幾何関数型の直交多項式であるが、これが一体どのくらいのバリエーションを持つのかは非常に興味の有ることである。他の例として文献の[赤澤-水川 [1]]では2面体群のwreath productとその部分群にB型Weyl群をとり、この例とは異なる直交関係を持つ同じタイプの直交多項式を発見している。

参考文献

- [1] H. Akazawa and H. Mizukawa, *Orthogonal polynomials arising from the wreath products of dihedral group*, Preprint, 2002.
- [2] E. Andrews, R. Askey and R. Roy *Special Functions*, Encyclopedia of Mathematics and its Applications, Cambridge, 1999
- [3] K. Aomoto and M. Kita *Theory of Hypergeometric Functions(in Japanese)*, Springer Tokyo, 1994
- [4] S. Ariki, T. Terasoma and H. -F. Yamada, Higher Specht polynomials, Hiroshima Math. J. 27 (1997), no. 1, 177-188.
- [5] E. Bannai and T. Ito, *Algebraic Combinatorics I. Association Schemes*, The Benjamin/Cummings Publishing Co. CA, 1984
- [6] C. Dunkl, A Krawtchouk polynomial addition theorem and wreath products of symmetric groups, Indiana Univ. Math. J. 25 (1976), no. 4, 335-358.
- [7] C. Dunkl, Cube group invariant spherical harmonics and Krawtchouk polynomials, Math. Z. 177 (1981), no. 4, 561-57
- [8] C. Dunkl and Y. Xu, *Orthogonal Polynomials of Several Variables*, Encyclopedia of Mathematics and its Applications, 81. Cambridge University Press, Cambridge, 2001.
- [9] I. M. Gelfand, General theory of hypergeometric functions (in Russian), Dokl. Akad. Nauk SSSR 288 (1986), no. 1, 14-18.
- [10] I. M. Gelfand and S. I. Gelfand, Generalized hypergeometric equations (in Russian), Dokl. Akad. Nauk SSSR 288 (1986), no. 2, 279-283
- [11] G. James and A. Kerber, *The Representation Theory of the Symmetric Group*, Encyclopedia of Mathematics and its Applications, 16, 1981.
- [12] M. Kita, On hypergeometric functions in several variables. II. The Wronskian of the hypergeometric functions of type $(n + 1, m + 1)$, J. Math. Soc. Japan 45 (1993), no. 4, 645-669.
- [13] M. Kita and M. Ito, On the rank of the hypergeometric system $E(n + 1, m + 1; \alpha)$, Kyushu J. Math. 50 (1996), no. 2, 285-295.
- [14] I. G. Macdonald, *Symmetric Functions and Hall Polynomials, 2nd. ed.* , Oxford, 1995.

- [15] H. Mizukawa, *Zonal spherical functions on the complex reflection groups and $(n + 1, m + 1)$ -hypergeometric functions*, Preprint, 2002.
- [16] D. Stanton, Some q -Krawtchouk polynomials on Chevalley groups, *Amer. J. Math.* 102, 625-662 (1980), no. 4
- [17] D. Stanton, Three addition theorems for some q -Krawtchouk polynomials, *Geom. Dedicata* 10 (1981), no. 1-4, 403-425
- [18] M. Yoshida, *Hypergeometric Functions, My Love. Modular Interpretations of Configuration Spaces*. Aspects of Mathematics, E32. Friedr. Vieweg and Sohn, Braunschweig, 1997.

有限環上の上半平面から得られる symmetric association scheme

九大数理 田上 真 (Makoto Tagami)
Graduate School of Mathematics, Kyushu University

1 Introduction

有限上半平面（以下簡単の為、これら有限体、有限環上の上半平面を FUHP と略記する）は Poincare 上半平面

$$H = \{x + iy \mid x, y \in \mathbb{R}, y > 0\}.$$

の有限版の類似として定義される。FUHP には一般線形群が可移に作用しており、この作用により association scheme ができる。有限体上の上半平面の場合には、この association scheme の relation は Poincare 距離の類似である対称な距離で与えられており、symmetric association scheme であることが分かる。symmetric なので特に commutative になり、character table すなわち spherical functions が考えられるが、それは [5], [4] ですべて求められている。

一般に群 G とその部分群 K が与えられた時に G は G/K に左からの積により可移に作用する、この作用により得られる association scheme を $X(G, K)$ で表すことにする。

association scheme はたくさんのグラフの集まりと思えるが、特に上半平面をグラフと思ったものを上半平面グラフということにすると、体の場合は2つの relation を除いて、性質のいいグラフである Ramanujan graph になる ([7] 参照)。しかし残念ながら、[2] の中で、有限環に対する上半平面グラフは一般には Ramanujan graph にはならないことが示されている。

一方、有限環に対しては一般線形群の作用によって得られる association scheme が有限体上の上半平面と同じように symmetric になるかどうかは未だ言及されていない。この報告で、有限環上に対しても association scheme が symmetric になることの証明の概略を述べ、その後、relation がどのように与えられるか議論する。

2 Definitions and lemmas

まず、この報告で使われる記号を定義しておく。 p は奇素数、環 R に対して $U(R)$ は単数群を表すとす。簡単のため、 $(\text{mod } p)$ を (p) と略記する。

$n \in \mathbb{N}$ に対して $R_n := \mathbb{Z}/p^n\mathbb{Z}$, 便宜上 $R_0 = \{0\}$ としておく。 R_n の単数群を $U_n := U(R_n) = \{x \in R_n \mid x \not\equiv 0 (p)\}$ とす。 $|U_n| = p^{n-1}(p-1)$ 。よく知られてるように、 U_n は巡回群であるから、 $U_n = \langle \delta \rangle = \{\delta^i \mid i \in \mathbb{Z}\}$ となる δ が存在する。この δ をひとつ固定しておく。

次にある R_n の拡大環を定義する。形式的な R_n 上の基底として、 $\{1, \sqrt{\delta}\}$ を持つ rank 2 の自由加群を M_n とす。すなわち、

$$M_n := \{x + y\sqrt{\delta} \mid x, y \in R_n\}.$$

M_n に積を定義する。 $x_1 + y_1\sqrt{\delta}, x_2 + y_2\sqrt{\delta} \in M_n$ に対して、

$$(x_1 + y_1\sqrt{\delta}) \cdot (x_2 + y_2\sqrt{\delta}) := x_1x_2 + y_1y_2\delta + (x_1y_2 + x_2y_1)\sqrt{\delta}.$$

この時、 M_n は可換環になる。

複素平面の時と同様に、 $z = x + y\sqrt{\delta} \in M_n$ に対して

$$\text{Re}(z) := x, \text{Im}(z) := y, \bar{z} := x - y\sqrt{\delta}, N_n(z) := x^2 - y^2\delta$$

とする。ノルム N_n は M_n の積を保存する。すなわち、次が成り立つ。

$$N_n(zw) = N_n(z)N_n(w) \quad (\forall z, w \in M_n).$$

以上の記号の元、次の補題が成り立つ。補題の証明はこの報告では割愛する。

補題 2.1. $U(M_n) = \{z \in M_n \mid N_n(z) \in U\}$.

補題 2.2. $N_n : U(M_n) \longrightarrow U_n$ は全射。

有限体上の上半平面は有限体 \mathbb{F}_q の拡大体 \mathbb{F}_{q^2} の部分集合として定義したが、有限環上の上半平面は R_n の拡大環 M_n の部分集合として定義される ([2])。

定義 2.1 (有限環上の上半平面).

$$\mathbb{H} := \{x + y\sqrt{\delta} \mid x \in R_n, y \in U\}.$$

$|\mathbb{H}| = p^{2n-1}(p-1)$ である。

R_n 上の一般線形群を

$$G_n := \text{GL}(2, R_n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R_n, ad - bc \neq 0 (p) \right\}$$

とする。簡単に分かるように $|G_n| = p^{4n-3}(p-1)^2(p+1)$ である。また、 G_n の中心は対角行列全体からなる。すなわち、 $Z(G_n) = \{aI \mid a \in U_n\}$ 。次の補題は [2] による。

補題 2.3. $z \in \mathbb{H}$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_n$ に対して次が成り立つ。

(a) $cz + d \in U(M)$.

(b) $(az + b)/(cz + d) \in \mathbb{H}$.

補題 2.3 より、 $z \in \mathbb{H}$, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_n$ に対して、

$$g \cdot z := \frac{az + b}{cz + d}$$

として、 G_n が \mathbb{H} に作用していることがわかる。可移に作用していることを見るために、アフィン群と呼ばれる G_n の部分群 A_n を考える。

$$A_n := \left\{ \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \mid y \in U_n, x \in R_n \right\}.$$

簡単に分かるように $|A_n| = |\mathbb{H}| = p^{2n-1}(p-1)$ である。 $\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in A_n$ に対して、

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \cdot \sqrt{\delta} = x + y\sqrt{\delta}.$$

よって、 A_n の元により $\sqrt{\delta}$ を \mathbb{H} の任意の元に移すことができるので、 A_n は \mathbb{H} に可移に作用している。よって特に G_n も可移に作用している事が分かる。

次に G_n の $\sqrt{\delta}$ における固定部分群を考える。この部分群は Poincare 上半平面の場合と比較して直交群と呼ばれている。

$$K_n := \{g \in G_n \mid g \cdot \sqrt{\delta} = \sqrt{\delta}\} = \left\{ \begin{pmatrix} a & b\delta \\ b & a \end{pmatrix} \mid a, b \in R_n, a^2 - b^2\delta \neq 0 (p) \right\}.$$

簡単に分かるように $|K_n| = p^{2(n-1)}(p+1)(p-1)$ である。 K_n は $\begin{pmatrix} a & b\delta \\ b & a \end{pmatrix}$ に $a + b\sqrt{\delta}$ を対応させるという写像で $U(M)$ と同型になる。有限体の場合は直交群は巡回群であったが、有限環の場合は巡回群にはならない。すなわち、次の命題が成り立つ。

命題 . $U(M_n) \simeq \mathbb{Z}/p^n\mathbb{Z} \oplus \mathbb{Z}/p^{n-1}(p^2 - 1)\mathbb{Z}$.

以下、混乱がなければ R_n, U_n, G_n, A_n, K_n をそれぞれ R, U, G, A, K と略記する。添え字を強調したいときは添え字も書くことにする。

この K に対して G の両側剰余分解 $K \backslash G / K$ を求める。

$$G = \sum_{x \in R, y \in U} \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} K = \sum_{z \in A} zK$$

と分解される。この分解により $K \backslash G / K$ の完全代表系を A から取れる事が分かる。 \mathbb{H} と G/K または A を次の対応により G - 集合として同一視する。

$$x + y\sqrt{\delta} \longleftrightarrow \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} K \longleftrightarrow \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}.$$

以下、 H 上の関数は上の同一視により、 G/K または A 上の関数と同一視する。例えば、

$$\text{Im}(x + y\sqrt{\delta}) = \text{Im}\left(\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} K\right) = \text{Im}\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$$

などと書く。

A の2つの元が同じ類に入っているかどうかの判定式を求めるために、ポアンカレ距離の類似として上半平面上に距離を定める。この距離は [2] で導入されたものである。

定義 2.2 (distance). $z, w \in \mathbb{H}$ に対して、距離関数 d を次で定義する。

$$d(z, w) := \frac{N(z - w)}{\text{Im}(z)\text{Im}(w)}.$$

d が G の作用で不変であることは容易に確かめられる。すなわち、

$$\forall g, h \in G, \forall z, w \in \mathbb{H}, d(g \cdot z, h \cdot w) = d(z, w)$$

が成り立つ。

$a \in R_n$ に対して、

$$S(a) := \{g \in A \mid d(\sqrt{\delta}, g \cdot \sqrt{\delta}) = a\}$$

とおく。 d は G の作用で不変なので、 $S(a)$ はいくつかの両側剰余類の和になっている。よって、後はそれぞれの $S(a)$ に対して両側剰余分解を調べていけばよい。

3 類の判定式と association scheme の対称性

この節で、各右剰余類が同じ類に入るかどうかの判定式を求める。

補題 3.1. $c \in U_n$ とする。この時、

$$\#\{(x, y) \mid x, y \in R_n, x^2 - y^2\delta = c\} = p^{n-1}(p+1)$$

が成り立つ。

有限体の場合、 $S(a)$ 達が両側剰余類になったが（前述の同一視をしている事に注意）、有限環の場合では一般に $S(a)$ はひとつの両側剰余類にならず、いくつかの類に分解する。しかし、有限環の場合にもいくつかの距離に対しては次の定理が成り立つ。この定理は [2] で示されている。

定理 3.1. $a \neq 0, 4\delta(p) \in R_n$ とする。この時、 $S(a)$ はひとつの両側剰余類になる。

この定理は補題 3.1 を用いると、簡単に得られる。

$a \equiv 0, 4\delta(p) \in R_n$ の場合、 $S(a)$ は 2 つ以上の両側剰余類に分解する。この分解を見るために、次の定義をする。

定義 3.1 (p 進付値). $a (\neq 0) \in R_n$ に対して、 $p^l \parallel a$ 、すなわち $p^l \mid a$ かつ $p^{l+1} \nmid a$ とする。 $a = 0$ の時は $l = n$ とする。このとき、 l を a の p 進付値といい、 $h(a)$ と書く。

p 進付値を用いて、次の補題を得る。

補題 3.2. $a, b, c, d \in R_n$ とする。また、 $h := \min\{h(a), h(b), h(c), h(d)\}$, $a = p^h a', b = p^h b', c = p^h c', d = p^h d'$ where $a', b', c', d' \in R_{n-h}$ とおく。この時、

$$\begin{aligned} \exists (x, y) \neq (0, 0) (p) \text{ s.t. } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} &\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} (p^n) \\ \iff \det \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &\equiv 0 (p^{n-h}). \end{aligned}$$

$\forall a \equiv 0, 4\delta (p)$ に対して新しい関数 $H_a : S(a) \rightarrow \{0, 1, \dots, n\}$ と $L_H : A \rightarrow \bigcup_{i=0,1,\dots,n} U_i$ を次のように定義する。

(1) $a \equiv 0 (p)$ の場合

$g = \begin{pmatrix} 1+l & k \\ 0 & 1 \end{pmatrix} \in S(a)$ と書いておく。この時、 $H_a(g) := \min\{h(l), h(k)\}$ 、 $k = k'p^{H_a(g)}$ 、 $l = l'p^{H_a(g)}$ として

$$L_H(g) := \frac{N_{n-h}(k' + l'\sqrt{\delta})}{1+l}$$

と定義する。 $L_H(g) \in U_{n-H_a(g)}$ となっている。

(2) $a \equiv 4\delta (p)$ の場合

$g = \begin{pmatrix} -1+l & k \\ 0 & 1 \end{pmatrix} \in S(a)$ と書いておく。この時、 $H_a(g) := \min\{h(l), h(k)\}$ 、 $k = k'p^{H_a(g)}$ 、 $l = l'p^{H_a(g)}$ として

$$L_H(g) := \frac{N_{n-h}(k' + l'\sqrt{\delta})}{-1+l}$$

と定義する。 $L_H(g) \in U_{n-H_a(g)}$ となっている。

補題 3.2 を使うと H, L_H により次の定理が得られる。

定理 3.2. $a \equiv 0$ or $4\delta (p)$, $g_1K, g_2K \in S(a)$ とする。この時、 $Kg_1K = Kg_2K$ であるための必要十分条件は

$$H_a(g_1) = H_a(g_2) \quad \text{かつ} \quad L_H(g_1) \equiv L_H(g_2)$$

である。

この定理を用いるとすぐに次の系が得られる

系 . $X(G, K)$ は *symmetric association scheme* である。

定理 3.2 によって G の K による両側分解が得られる。

$$G = \sum_{a \neq 0, 4\delta (p)} Kg_aK + \sum_{\substack{1 \leq h \leq n-1 \\ u \in U_{n-h} \\ i=0 \text{ or } 4\delta}} Kg_{h,u}^iK + K \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} K + K$$

ここで、それぞれの $a \neq 0, 4\delta (p)$ に対して、 $g_a \in S(a)$ を固定し、また $1 \leq \forall h \leq n-1, \forall u \in U_{n-h}, i = 0, 4\delta$ に対して、

$$d(\sqrt{\delta}, g_{h,u}^i \cdot \sqrt{\delta}) \equiv i (p), H(g_{h,u}^0) = H(g_{h,u}^{4\delta}) = h, L_H(g_{h,u}^0) = L_H(g_{h,u}^{4\delta}) = u$$

となる $g_{h,u}^0, g_{h,u}^{4\delta} \in A$ を固定している。このような $g_{h,u}^i$ が存在することは補題 3.1 が保障している。

よって両側剰余類の個数は

$$p^n - 2p^{n-1} + 2p^{n-1} = p^n$$

であることがわかる。この値は R_n の位数と同じ値である事に注意する。

4 上半平面上の距離の修正

以下、Poincare 距離の類似であった距離 d を $X(G, K)$ の relation を与えるように修正する。新しい距離を d_R で表すとすると、 $z, w \in \mathbb{H}$ に対して、

(1) $d(z, w) \not\equiv 0, 4\delta \pmod{p}$ の時

$d_R(z, w) := d(z, w)$ とする。

(2) $d(z, w) \equiv 0 \pmod{p}$ の時

$r := \operatorname{Re}(z - w), k := \operatorname{Im}(z - w), h := \min\{h(r), h(k)\}$ として、さらに $r = p^h r', k = p^h k'$ ($r', k' \in R_{n-h}$) と書いておく。その時、

$$d_R(z, w) := \frac{N_{n-h}(r' + k'\sqrt{\delta})p^h}{\operatorname{Im}(z)\operatorname{Im}(w)}.$$

ここで、 $N_{n-h}(r' + k'\sqrt{\delta}) \in R_{n-h}$ であるが、 p^h を掛けているので、 $d_R(z, w) \in R_n$ としてよい事が分かる。

(3) $d(z, w) \equiv 4\delta \pmod{p}$ の時

$r := \operatorname{Re}(z - w), k := \operatorname{Im}(z + w), h := \min\{h(r), h(k)\}$ として、さらに $r = p^h r', k = p^h k'$ ($r', k' \in R_{n-h}$) と書いておく。その時、

$$d_R(z, w) := \frac{N_{n-h}(r' + k'\sqrt{\delta})p^h}{\operatorname{Im}(z)\operatorname{Im}(w)} + 4\delta.$$

ここでも (2) と同様に、 $d_R(z, w) \in R_n$ としてよい。

この時、任意の $a \in R_n$ に対して、 $L_a := \{(z, w) \mid z, w \in \mathbb{H}, d_R(z, w) = a\}$ とすると、 $\{L_a\}_{a \in R_n}$ が $X(G, K)$ の relation を与える。

また、補題 3.1 を用いると valency も計算できる。

$z \in \mathbb{H}$ を固定して、 $v_i := \#\{w \in \mathbb{H} \mid (z, w) \in L_a\}$ とすると

$$i \neq 0, 4\delta(p) \implies v_i = p^{n-1}(p+1)$$

$$i = p^h u \text{ or } p^h u + 4\delta \quad (1 \leq h \leq n-1, u \in U_{n-h}) \implies v_i = p^{n-h-1}(p+1)$$

$$i = 0 \text{ or } 4\delta \implies v_i = 1$$

Acknowledgement 筆者はこの問題を提起して頂き、多くの有益な御助言を頂いた坂内英一先生に感謝いたします。また、助言をいただいた安田貴徳君にも感謝します。

参考文献

- [1] J. Angel, N. Celniker, S. Poulos, A. Terras, C. Trimble, and E. Velasquez, Special functions on finite upper half planes, *Contemp. Math.* **138** (1992), 1-26.
- [2] J. Angel, B. Shook, A. Terras, C. Trimble, Graph spectra for finite upper half planes over rings, *Linear Algebra and Its Applications*, **226-228** (1995), 423-457.
- [3] E. Bannai and T. Ito, *Algebraic Combinatorics I, Association Schemes*, Benjamin/Cummings, Menlo Park, CA, 1984.
- [4] R. Evans, Characters sums as orthogonal eigenfunctions of adjacency operators for Caley graphs, *Cont. Math.*, **168** (1994), 33-50.
- [5] J. Soto-Andrade, Geometrical Gelfand models, tensor quotients, and Weil representations, *Proc. Symp. Pure Math.*, **47**, Amer. Math. Soc., Providence, 1987, 305-316.
- [6] M. Suzuki, finite simple groups, Kinokuniya, 1987.
- [7] A. Terras, *Fourier Analysis on Finite Groups and Applications*, London Math.Soc., 1999.

群上の単項式について

山口大学教育学部 飯寄 信保

平成 14 年 11 月 26 日

1 群上の単項式

G を群とする。またその群 G を含むようなより大きい群を G_0 と置くことにする。 G 係数の単項式 $f(X)$ とは、ここでは次のようなものをさすことにする。

$$f(X) = a_1 X_1^{e_{11}} X_2^{e_{12}} \cdots X_n^{e_{1n}} a_2 \cdots a_r X_1^{e_{r1}} X_2^{e_{r2}} \cdots X_n^{e_{rn}} a_r$$

ここで $a_i \in G$ であり $e_{ij} \in \mathbb{Z}$ は有理整数である。用語を一通り紹介すると、 a_i らは、この単項式の係数といい、単項式の全ての係数で生成される G の部分群をこの単項式の係数群と呼ぶ。単項式の集合 A について論じるとき A に属する単項式の係数群全体で生成される G の部分群を A の係数群と言う。 X_i らは、単項式の変数または単に語と呼ばれる。 $a_j X_i^{e_{ij}} a_j^{-1}$ を我々は、セルと呼ぶことにする。このとき整数 e_{ij} をこのセルの次数と呼ぶ。次数の総和を単項式の次数と呼んだり、 $i = j$ を満たすようなセルの次数だけを足したものを対角次数と呼んだり研究の方針に従って、セルの次数は気ままに加減乗除され適当な名前と呼ばれている。例えば、次数の全ての絶対値の和を、単項式の長さという。また、単項式の集合 A について論じるとき、 A に属する単項式の次数の最大公約数を A の次数と呼んだりする。古くからこの単項式についての研究があり、近代的な研究の頂点としてホールの一連の結果がある。その重要な一部分として単項式 $f(X)$ に群 G_0 の要素を X に代入したときに単位元 1 となるようなものを見つけること、すなわち、群上の方程式 $f(X) = 1$ の解を勘定するというものがある。もちろんあの単項式の解の総数は 3 つであるとか、この単項式は解が 100 個もあるというようなこと、または、解がただ 3 つであるような単項式を特徴付けよなどというものではない（ただ、解がない場合は、特徴付け可能であり、ただひとつの場合は特徴付けするのは容易いであろうと思う）。ホールのやったことは、フロベニウスによる彼自身が群論の基本定理と名付けた定理の形式を一般の場合に恐ろしいほど拡張したことである。フロベニウスの基本定理とは、単項式が次数 n のセルの場合、 G でのその単項式の解の個数は G の位数と n の最大公約数で割り切れるというものである（このフロベニウスの定理は、現代において

多くの影響を及ぼしており、例えば吉田氏の拡張、飯寄-八牧のフロベニウス予想の解決、さらには浅井-吉田予想の提唱また浅井-竹ヶ原-庭崎によるその一連の研究等がある)。ホールの仕事は、一変数の単項式の集合 A の G_0 における共通解の個数は、 A の係数群の G_0 における中心化群の位数と A の次数の最大公約数で割り切れるというものである。この結果を別の言葉で言い換えると、 A の係数群が G のとき、 A の関係を保つような群の拡大(通常の拡大と少々意味合いが違う)が G_0 の中においては、その総数は G の G_0 における中心化群の位数と A の次数 n の最大公約数で割り切れるということである。さらに言い換えると、 A_0 を G と X で生成される無限巡回群の自由積(この自由積を $M_1(G)$ と書くことにする)の中で A を含む最小の正規部分群とすると、

$$\text{Hom}_G(M_1(G)/A_0, G_0) \cong 0 \quad (|C_{G_0}(G)|, n) \cdots \cdots (\dagger)$$

となる。今から言うことは、当たり前のことであるが、この言い換え達は、群上の単項式の解を観察するときも、単項式全体を観察することが有益であることを示している。さて、そうすると単項式全体 $M_n(G)$ (n 変数の)はどのように捉えることができようか? 当初に述べた単項式の定義からいって、群 G とランク n の自由群(これは $X_i (i = 1, \dots, n)$ から生成されているとする)の自由積を考えるのが適当である。このように単項式全体を捉えると (\ddagger) との接続もうまくいくことになる。一般に単項式の話していくには、この単項式全体を用いて議論していくのが良いのだろうが、一般過ぎて難しいところがある。そこでまず、 G の中で A は共通解を持つものとして議論することにした。この仮定は、ある程度一般の場合に戻すこともできるもので決して強すぎるものでないと思える(A の共通解一つを G に付け加えてやれば、この仮定を満たすようにできる)。この仮定の上で、 G^n の中に存在する A の共通解を $g = (g_1, \dots, g_n)$ と置くと、 $M_n(G)$ の自己同型

$$t_g : X_i \mapsto g_i X_i \cdots \cdots (*)$$

を用いて、 A の t_g による像を考えてやると、その像は共通解として単位元 $1 = (1, \dots, 1)$ を持つ。このようにして、我々の仮定は「 A は共通解 $1 = (1, \dots, 1)$ を持つもの」としてよいことがわかる。このようなことから、我々は単項式全体の中から 1 を解に持つような単項式について考えれば良いことになった。このような単項式全体を $SM_n(G)$ と書くことにする。これは先に考えた単項式全体の為す群の中で正規部分群になっていて、とても育ちのよい集合であることがわかる。ところが、ここでいきなり問題が発生してしまう。というのは、 $M_n(G)$ を考えていたときに、 G 係数の単項式であることを $M_n(G)$ から容易に見ることができた。しかし、 $SM_n(G)$ については、このままではごっそり G の情報が落ちてしまう。なぜならば、 $SM_n(G)$ は自由群であるからだ。これでは、張り切って $SM_n(G)$ だけを弄繰り回してもなんの結果も得

られない。(これとは別に、私にとって、この手の話では弄くる対象が一つの演算しか持っていない大変術がゆい状態に陥ることが多い。)これを、解決するために、研究中の諸手続き・計算過程を見直すと、妙に(*)のような謂わば代入とすることができるような準同型を考えることが多いことに気づく。 $SM_n(G)$ に $SM_n(G)$ の元を代入するなどという荒っぽいことはやめたい。そこで $SM_n(G)^n$ を考えると代入という演算が自然と意味を持つようになる。これを公理的整備すると、半分配環という構造のものであることがわかる(詳しくは、平成9年度の代数学シンポジウムの報告集参照)。大雑把に説明すると、 $SM_n(G)^n$ は加法が非可換で、右分配則が成立しない環のようなものである。加法が非可換であることや、分配法則が面倒なことなどいろいろと大変なことはあるが、この我々の扱う半分配環は通常環論の議論が平行して行える。例えば、準同型定理、イデアル、モジュール、冪等元等々などである。特に、代入(正式には、合成積)についての可逆元の為す群 U の構造は、明らかにされており、($n=1$ のとき)

$$U \simeq G \text{ wr } S_2$$

である(阿部)。このことにより、直ちに

$$G \simeq H \iff SM_1(G) \simeq SM_1(H)$$

であることがえられる($n=1$ のとき以外でも同様なことが言える。また矢印の左側の同型は群としてのものであり、右側のものは半分配環としての同型である)。もう一つ、ここで注意しておきたいのは、我々の半分配環と通常環(群環)との関係である。我々の半分配環においてイデアルという概念が自然に定義でき、その剰余群も自然に半分配環になっていることが観察できる。このような観察下で自然に湧き出てくる疑問は、「どのようなイデアルで剰余すると我々の半分配環は通常環になるのだろうか?」である。これについての答えは、非常に簡単で「加法が可換になれば良い」つまり、イデアルとして $SM_n(G)^n$ の交換子群をとればよいのである。このときが成立する:

$$(SM_n(G)^n)^{ab} \simeq \text{Mat}_n(\mathbb{Z}[G]).$$

以上に述べたことは、単項式の集合を半分配環として捉える必要性の傍証でしかないが全く無視できるものでないのは確かであろう。

2 G_0 上の単項式?

半分配環構造による群の特徴づけはいろいろと考えられて、結果を出すことができる。アーベル群、非可換単純群の特徴付けは、そのもつとも簡単なものであるが、そのような議論を企むとき、必要な考え方がある。元々単項式は群の要素を代入して群の要素を得るといった写像的な考えの基に展開されてい

る。正確に言うと、 n 変数の単項式 $f(X) \in M_n(G)$ と $g = (g_1, \dots, g_n) \in G_0^n$ に対して、

$$\varphi_g : X_i \mapsto g_i$$

で定義される $M_n(G)$ から G_0 への群準同型による $f(X)$ の像 $\varphi_g(f(X))$ を $f(g)$ と置くと単項式 $f(X)$ は G_0^n から G_0 への写像となる。このように考えると今までの単項式全体は、この写像的な考えには直接的には対応していないことがわかる（有限群上の写像は有限個になるが、我々の単項式の個数は無限個である）。この弱点を補うために次の式で定義される $M_n(G)$ の正規部分群を考える：

$$I(G_0) = \bigcap_{g \in G_0^n} \text{Ker} \varphi_g.$$

この正規部分群による剰余群 $M_n(G)/I(G_0)$ を $M_n(G, G_0)$ とおくと、これは G_0^n から G_0 への写像の集合と同一視できる ($SM_n(G)/I(G_0)$ を $SM_n(G, G_0)$ とおく。また、この $M_n(G, G_0)$ の属する要素を G_0 上の単項式と呼ぶことにする)。 $M_n(G, G_0)^n$ は半分配環であり、 $SM_n(G)^n$ をそのイデアル $I(G_0)^n$ で剰余してできた半分配環になっている。例えば、 $G = G_0$ をクラス 2 以下の冪零群とする。このとき、

$$SM_1(G, G_0) \simeq G/Z(G) \times Z/\exp(G)Z$$

が成立する。ここで右辺は和を群の積、乗法を $(a, n)(b, m) = (a^m b^n, mn)$ として得られる可換環である。

このセクションの最後の注意として群 G_0^n の部分集合 S 上の単項式という概念を定義しておこう。これは $M_n(G, G_0)$ とほとんど同様にして定義されるのであるが、残念なことに一般には素直な意味での半分配環を構成することができない（しかし、「モジュール」になる。モジュールの定義は通常のモジュールの定義から右分配法則に関係するところを削除して得られるものであり、半分配環論でも通常の環論のモジュールと同様な働きをする。面白いことに G -群かつ加群は群 G の群環のモジュールであるが、 G -群の n 個の直積は全て自然に $SM_n(G)^n$ -モジュールになる。）正確な定義を与えておこう。 $I(S)$ を $I(S) = \bigcap_{g \in S} \text{Ker} \varphi_g$ で定義する。 S 上の単項式群とは $M_n(G)/I(S)$ で定義される群であり、これを $M_n(G, S)$ とかく。単項式の解集合と単項式群との関係を表現すると、「単項式の集合 A に対して、 A_0 を $M_n(G)$ の中で A を含む最小の正規部分群とする。このとき、 $(M_n(G)/A_0)^n$ は $SM_n(G)^n$ -モジュールとなる。 G_0^n もやはり $SM_n(G)^n$ -モジュールであり、

$$\text{Hom}_{SM_n(G)^n}((M_n(G)/A_0)^n, G_0^n)$$

は、 A の共通解 S と自然に同一視できる。また、 S 上の単項式群は $M_n(G)/A_0$ である。」のようになる。浅井-吉田の予想は大雑把に言うと、上の式の中に現れてくる $M_n(G)/A_0$ のアーベル化した群（これは、我々の言葉では、次数によって表現できる）によって、 S の状態が記述できるだろうというものである。

3 G から見た G_0 の複雑さ

前の節で群の部分集合上の単項式という概念を与えたが、この応用例として群とその部分集合の関係を表す一つの指標のようなものを与えたい（指標といっても表現論のそれではない）。

この節においては、全て一変数の単項式のみを扱うため、単項式といったら一変数のものと考えてほしい。

単項式 f のセルの数をセルの長さといい、 $\text{clen}(f)$ であらわすことにする。群上の、あるいは部分集合上の単項式が実際どのくらいのセルの長さの単項式で表記できるかという疑問は、素朴かつ自然なものだと思う。それ故に、 G_0 の部分集合 A 上の単項式 $fI(A)$ に対して、

$$\text{clen}(fI(A)) = \min\{\text{clen}(u) | u \in fI(A)\}$$

とにおいて、この $\text{clen}(fI(A))$ を A 上の単項式 $fI(A)$ のセルの長さと呼ぶことにする（これを計算するときは、コクセター-トッドのコセット数え上げ法の論法を用いるのが一番早いように思える）。セルの長さについて更なる疑問として、「いったいどの位のセルの長さの単項式で G -係数の A 上の単項式を表記できるのであろうか」がある。そこで、

$$\text{crank}_G(A) = \text{Max} \quad \{\text{clen}(fI(A)) | fI(A) \in M_1(G, AS)\}$$

と定義して、 $\text{crank}_G(A)$ を A の G -セル階数と呼ぶことにする。このセル階数について次のようなことがわかっている。

1. G_0 が可換群であれば G_0 のセル階数は 1 である。
2. G_0 がクラス 2 の冪零群であれば、 G_0 のセル階数は 2 以下である。
3. G の G -セル階数が 30 に満たないならば G は可解群である。

3 に挙げた 30 という数はすごく大雑把に計算したもので、実際はもっと大きい数に置き換えることができるであろうと思われる。このような観察は、いくらでも時間があればできるが、一般的傾向として（もし「可換」が「非可換」より簡単な構造と考えれば）セル階数が小さいほど G から見た A の構造(?) は簡単なものといえよう。例えば、 A が G と可換であったら、 A のセル階数は 1 である。

このセル階数の計算は、職人芸の世界であるが一般的なアルゴリズムはやはりコクセター-トッドのコセット数え上げ法によるものだと思う。

最後に、任意の単純群は位数 2 の元と奇素数 p の位数の元の二つにより生成することができる。例えば、モンスターであっても、 $M_1(2)/I(p)$ というように表示ができる。であるから位数 2 の元を係数としてセル階数を調べれば、その複雑さを数値的に表現できるのではないかという予測ができる。実際根拠はないが、位数とセル階数が一致する有限単純群は存在しないのではない

かと思う（群のセル階数の上下からの評価は可能であるが、正確な値を計算するのは手計算ではほとんど不可能な状態である。）

4 特殊な単項式

表題に特殊という形容詞を用いたが、むしろ簡単という形容詞を当てたほうが適切であったかもしれない。この節では一般の単項式を扱うのではなく X^m のような単項式またはその変形について話していきたい。

この形の単項式の考察は、古くからなされておりフロベニウスがもうすでにおこなっている。 m を G の位数の約数とすれば $X^m = 1$ の解の個数 $\sigma_G(m)$ は先に述べたとおり m の倍数である。 $\phi_G(m) = \sigma_G(m)/m$ と定義した数は、多分群 G の構造と密接に関係しているだろうと考えられる（ファイト）。フロベニウスは $\phi_G(m) = 1$ であったら $X^m = 1$ の解集合は部分群になるだろうと予想したのである。この予想は幸運にも正しかった。しかし、どうして部分群になるのかというきちんとした、そして明快な満足のいく理由を筆者は知らない。筆者の感想は兎も角、 X^m という形の単項式は興味深いものだという事は確かであろう。次のような問題を考えてみよう。「単項式 X^m が群 G のある性質を持つ部分集合を全て 1 にしてしまうとき、 G の性質を特徴づけられるか？」もちろんここでは、「ある性質」や「 G の性質」が重要である（この問題において、 X^m を適当に替えると興味深い問題が出てくることもある）。一番簡単なものは、「単項式 X^m が群 G の要素を全て 1 にしてしまうとき、 $\exp(G)$ は m の約数である。」である。これでは、さすがに面白くない。全く自明じゃない例として、次ぎの興味深いものがある。

定理（ケーゲル） p を素数、 $f(X) = X^p$ とする。 G を有限群、 N を G の指数 p の正規部分群とする。もし、 $f(G - N) = \{1\}$ を満たせば、 N は冪零群である。

この定理をもちて有名なトンプソンによるフロベニウス核の冪零性の定理を示すことが出来る。残る部分はこの定理の変形を単項式の見地からの考えて見たい。シャープ指標ある理論のブラウアー指標の類似、またそれによる素数グラフのモジュラーバージョン（千吉良—飯寄「Prime graphs and Brauer characters」J. Group Theory 1(1998) 363-368）と同じ視点から、 p 正則元に付いて注目して類似の変形を試みる。そのためにまずケーゲルの定理は次のように変形してみる。

定理（ケーゲル） p を素数、 $f(X) = X^p$ とする。 G を有限群、 N を G の指数 p の正規部分群とする。もし、ある $z \in G - N$ に対し $f(zN) = \{1\}$ を満たせば、 N は冪零群である。

千吉良-飯寄の見方からいうと素数 p の部分は無視をしてどうなるかということである。より具体的にいうと「 N の p 正則元に対してケーゲルの定理と同様な事柄が成立しているとき、 N の構造はどのようなものであるか」である。この答えとして次が成立する。

命題 p を素数, $f(X) = X^p$ とする。 G を有限群, N を G の指数 p の正規部分群とする。もし、ある $z \in G - N$ に対し $f(z(N_{p'})) = \{1\}$ を満たせば、 N は p -冪零で $O_{p'}(N)$ は冪零群である。

この命題は有限単純群の分類定理を用いると証明できる。ただし、 $p = 2$ のときは容易に証明でき、良い演習問題といった感じである。さて、証明方針は、最小の反例を考え、それが単純群であることを示し、その後単純群のシロー p -部分群の構造を調べて矛盾を導くといった具合である。その鍵となる補題は次のものである。しかし、この命題は分類定理を用いたにしては野暮ったい条件が多くついている。大体「 N が正規部分群である」やら「指数 p の」という条件は強すぎる。実は、上の命題を用いて更にコピー&ペーストするようにこの命題の証明を同様に行うことにより次の進化した定理が得られる。

定理 G を有限群とする。 p を素数, $f(X) = X^p$ とする。もし、ある $z \in G$ に対し $f(z(G_{p'})) = \{1\}$ を満たせば、 N は p -冪零で $O_{p'}(N)$ は冪零群である。

大分すっきりした形に納まったと思う。

最後に、単項式の研究はいろいろな側面から研究されるべきであり、単項式群の諸性質を調べるだけでなく、個々の単項式の性質の解明も重要な課題であると、筆者は考えている。

以上

On $(2n, 2, 2n, n)$ RDS's

Yutaka Hiramine

Department of Mathematics, Faculty of Education, Kumamoto University

Kurokami, Kumamoto, Japan

E-mail: hiramine@gpo.kumamoto-u.ac.jp

1 Introduction

An (m, u, k, λ) *relative difference set* (RDS) in a group G relative to a subgroup U of order u and index m is a k -element subset R of G such that every element $g \in G \setminus U$ has exactly λ representations $g = r_1 r_2^{-1}$ with $r_1, r_2 \in R$ and no non-identity element of U has such a representation. The subgroup U is often called the *forbidden* subgroup. If $u = 1$, then R is an (m, k, λ) *difference set* (DS) in the usual sense. A $(u\lambda, u, u\lambda, \lambda)$ RDS is called *semiregular*. An RDS R in a group G relative to a subgroup U is semiregular if and only if R is a complete set of right coset representatives of G/U .

Let R be a $(2n, 2, 2n, n)$ RDS in a group G of order $4n$ relative to a *normal* subgroup $U \simeq \mathbb{Z}_2$ of G . Such a group is called an *Hadamard group* of order $4n$ by N. Ito ([4]). In this article, we remove the condition that the forbidden subgroup is normal and show that a Sylow 2-subgroup of G is noncyclic and n is even unless $n = 1$. We also give examples of RDS's relative to non-normal forbidden subgroups.

For a subset X of G , we set $X^{(-1)} = \{x^{-1} \mid x \in X\}$ and we identify a subset X of G with a group ring element $\hat{X} = \sum_{x \in X} x \in \mathbb{C}[G]$. Moreover, for $f = \sum_{x \in G} a_x x \in \mathbb{C}[G]$ ($a_x \in \mathbb{C}$, $\forall x \in G$), we set $f^{(-1)} = \sum_{x \in G} a_x x^{-1} \in \mathbb{C}[G]$. The terminologies are taken from [2] and [6].

2 The case that a Sylow 2-subgroup is cyclic

In this section we show the following.

Theorem 2.1 *If a group G of order $4n$ contains a $(2n, 2, 2n, n)$ RDS, then a Sylow 2-subgroup of G is non-cyclic and n is even unless $n = 1$.*

Proof. Assume n is even and a Sylow 2-subgroup of G is cyclic. In his paper [4], N. Ito showed the non-existence of $(2n, 2, 2n, n)$ RDS in G relative to a normal subgroup U of G of order 2 (see Proposition 7 of [4]). However, his proof does not depend on the normality of U . Thus the theorem holds in this case.

Assume n is odd. If there is an element x of order 2 outside U , then x is represented even times as a difference $d_1 d_2^{-1}$ with $d_1, d_2 \in R$ because $x = x^{-1}$. This is contrary to $2 \nmid n$. Hence U contains all involutions of G and so $G \triangleright U$. By [4], $n = 1$. Thus we have the theorem.

By Theorem 2.1, $PSL(2, q)$ with $q \equiv 3, 5 \pmod{8}$ contains no $(2n, 2, 2n, n)$ RDS. We ask the following :

Question : Is there any finite simple group of order $8m$ that contains a $(4m, 2, 4m, 2m)$ RDS ?

3 A conjugacy class t^G

Let R be a $(2n, 2, 2n, n)$ RDS in a group G of order $4n$ relative to a normal subgroup $U \simeq \mathbb{Z}_2$ of G . Such a group is called an *Hadamard group* of order $4n$ by N. Ito ([4]) and he showed that a $2n$ by $2n$ matrix $H = (h_{ij})$ defined by $h_{ij} = 1$ if $Rr_i r_j^{-1} \cap U = \{1\}$ and $h_{ij} = -1$ otherwise is an Hadamard matrix of order $2n$. In this section, we remove the condition that the forbidden subgroup is normal and study the relation between a $(2n, 2, 2n, n)$ RDS and an Hadamard matrix.

Hypothesis 3.1 *Let G be a group of order $4n (> 4)$ that contains a $(2n, 2, 2n, n)$ RDS R relative to a subgroup $U = \langle t \rangle \simeq \mathbb{Z}_2 : RR^{(-1)} = 2n + n(G - U)$. Assume that $t^G \not\subseteq R^{(-1)}R$, where t^G is the set of conjugates of t in G .*

Lemma 3.2 *We may assume that $t \notin R^{(-1)}R$.*

Proof. By assumption, $ctc^{-1} \notin R^{(-1)}R$ for some $c \in G$. Then $t \notin (Rc)^{(-1)}(Rc)$. Hence, exchanging R for Rc if necessary, we may assume that $t \notin R^{(-1)}R$.

In the rest of this section we assume that $t \notin R^{(-1)}R$. We note that $t \notin R^{(-1)}R (= RR^{(-1)})$ whenever $G \triangleright U$ (see Proposition 2.8 of [5]).

Lemma 3.3 *The following hold.*

- (i) $tR = Rt = G \setminus R$.
- (ii) $|xR \cap yU| = 1$ for all $x, y \in G$.

Proof. By assumption, $R \cap Rt = \phi$. Hence, as $|G| = 2|R|$, we have $G = R \cup Rt$ and so $Rt = G \setminus R$. Similarly, $tR = G \setminus R$ as $t \notin RR^{(-1)}$. Thus (i) holds.

Since $t \notin R^{(-1)}R$, R is a complete set of left coset representatives of G/U . Hence xR is also a complete set of left coset representatives for $x \in G$ and so $|xR \cap yU| = 1$ for all $x, y \in G$. Thus (ii) holds.

Lemma 3.4 *Assume $t \notin R^{(-1)}R$ and let $r, s \in G$. Then $r \notin sR$ if and only if $rt \in sR$.*

Proof. By Lemma 3.3, $|r^{-1}sR \cap U| = 1$. Hence the lemma holds.

Notation 3.5 Assume $t \notin R^{(-1)}R$. We define $h_{r,s} \in \{\pm 1\}$ ($r, s \in R$) by

$$h_{r,s} = \begin{cases} 1 & \text{if } r \in sR \\ -1 & \text{otherwise.} \end{cases} \quad (1)$$

Lemma 3.6 Assume $t \notin R^{(-1)}R$. Fix u and v with $u, v \in R, u \neq v$. Then $|\{r \in R \mid h_{r,u}h_{r,v} = 1\}| = n$.

Proof. We have $h_{r,u}h_{r,v} = 1$ if and only if either (i) $r \in uR$ and $r \in vR$ or (ii) $r \notin uR$ and $r \notin vR$. By Lemma 3.4, $r \notin uR$ if and only if $r \in uRt$. It follows that $h_{r,u}h_{r,v} = 1$ if and only if either (i) $r = ur_1 = vr_2$ or (ii) $r = ur_1t = vr_2t$ for some $r_1, r_2 \in R$. This is equivalent to either (i) $r = ur_1$ and $r_1r_2^{-1} = u^{-1}v$ or (ii) $r = ur_1t$ and $r_1r_2^{-1} = u^{-1}v$. Note that $|R \cap ur_1U| = 1$ for any $r_1 \in R$ by Lemma 3.3. Hence, given distinct $u, v \in R$, $h_{r,u}h_{r,v} = 1$ for some $r \in R$ if and only if $r_1r_2^{-1} = u^{-1}v$ and $R \cap ur_1U = \{r\}$ for some $r_1, r_2 \in R$. Therefore the lemma holds by the definition of RDS.

Proposition 3.7 Let R be a $(2n, 2, 2n, n)$ RDS in a group G relative to a subgroup $\langle t \rangle (\simeq \mathbb{Z}_2)$. Assume $t^G \not\subset R^{(-1)}R$. Then, we may assume $t \notin R^{(-1)}R$ and have that a $2n \times 2n$ $\{\pm 1\}$ -matrix $(h_{r,s})$ defined by the following is an Hadamard matrix of order $2n$:

$$h_{r,s} = 1 \iff s^{-1}r \in R$$

Proof. By Lemma 3.2, we may assume that $t \notin R^{(-1)}R$. Let $u, v \in R$. If $u = v$, then clearly $\sum_{r \in R} h_{r,u}h_{r,u} = 2n$. Assume $u \neq v$. Then, by Lemma 3.6, $\sum_{r \in R} h_{r,u}h_{r,v} = 1 \cdot n + (-1) \cdot (2n - n) = 0$. Thus $2n \times 2n$ matrix $(h_{r,s})$ is an Hadamard matrix.

4 Construction of $(2n, 2, 2n, n)$ RDS's

In this section we give examples of groups that contain $(2n, 2, 2n, n)$ RDS's relative to *non-normal* forbidden subgroups.

Throughout this section we assume the following :

Hypothesis 4.1 Let R be a $(2n, 2, 2n, n)$ RDS in a group G of order $4n (> 4)$ relative to a subgroup $\langle t \rangle$ of order 2. There exists a normal subgroup N of G of index 2 such that $G = \langle t \rangle N$. Set $R = A + Bt$, where A and B are subsets of N . We may assume $|A| \leq |B|$ by exchanging R for Rt if necessary.

Proposition 4.2 Let notations be as in Hypothesis 4.1. The following hold :

- (i) there exists a positive integer m such that $n = 2m^2$ and $|N| = 4m^2, |A| = 2m^2 - m$,
- (ii) $AA^{(-1)} + A^t(A^t)^{(-1)} = 2(m^2 + (m^2 - m)N)$, where $A^t = t^{-1}At$, and
- (iii) $B = N \setminus A^t$.

Conversely, if a subset A of N satisfies (i) and (ii), then a subset R of G defined by $R = A + (N - A^t)t$ is a $(4m^2, 2, 4m^2, 2m^2)$ RDS.

Proof. By assumption, $RR^{(-1)} = 2n + n(N + Nt - 1 - t)$. On the other hand, $RR^{(-1)} = (A + Bt)(A^{(-1)} + tB^{(-1)}) = (AA^{(-1)} + BB^{(-1)}) + (B(A^t)^{(-1)} + A(B^t)^{(-1)})t$. Hence we have

$$AA^{(-1)} + BB^{(-1)} = 2n + n(N - 1) \quad (2)$$

and

$$B(A^t)^{(-1)} + A(B^t)^{(-1)} = n(N - 1). \quad (3)$$

By (3), $A^t \cap B = \phi$. On the other hand, $|A| + |B| = |R| = |N| = 2n$ and $A^t, B \subset N$. Hence (iii) holds.

Set $a = |A|$ and $b = |B|$. Then, by (2) and (3), $a + b = 2n$ and $2ab = n(2n - 1)$. From this, we have $a = n - \sqrt{\frac{n}{2}}$ and $b = n + \sqrt{\frac{n}{2}}$. Set $m = \sqrt{\frac{n}{2}}$. Then $n = 2m^2$ and $|A| = 2m^2 - m$, $|B| = 2m^2 + m$. Thus (i) holds.

By (iii) and equation (2), we have $AA^{(-1)} + (N - A^t)(N - (A^t)^{(-1)}) = 4m^2 + 2m^2(N - 1)$. It follows that $AA^{(-1)} + A^t(A^t)^{(-1)} + (4m^2 - 2(2m^2 - m))N = 2m^2 + 2mN$. Thus (ii) holds.

Assume that a subset A of N satisfies (i) and (ii) and set $B = N \setminus (A^t)$. Then, one can easily verify that $(A + Bt)(A^{(-1)} + tB^{(-1)}) = 4m^2 + 2m^2(N\langle t \rangle - \langle t \rangle)$. Thus $R (= A + Bt)$ is a $(4m^2, 2, 4m^2, 2m^2)$ RDS relative to $\langle t \rangle$.

A $(4s^2, 2s^2 + \varepsilon s, s^2 + \varepsilon s)$ DS ($\varepsilon = \pm 1$) is called an *Hadamard difference set* of order s^2 .

Example 4.3 Let $N = \langle x \rangle \simeq \mathbb{Z}_{16}$ and let t_ε ($\varepsilon = \pm 1$) be an automorphism of N of order 2 defined by $x^{t_\varepsilon} = x^{8+\varepsilon}$. Set $A = \{1, x, x^3, x^4, x^5, x^{11}\}$ and $B = N \setminus A^t$, where $t = t_\varepsilon$. Then one can verify that A with $m = 2$ satisfies (i) and (ii) of Proposition 4.2. This implies that the semi-dihedral group SD_{32} of order 32 and the modular 2-group $M_5(2)$ of order 32 have $(16, 2, 16, 8)$ RDS's relative to a non-normal subgroup of order 2 (see [3]).

If t leaves $AA^{(-1)}$ invariant in Proposition 4.2, then we have the following :

Proposition 4.4 Let A be an Hadamard difference set of order m^2 in a group N of order $4m^2$ and $\langle t \rangle$ a group of order 2 operating on N as an automorphism group of N . Let $G = N\langle t \rangle$ be a semidirect product of N by $\langle t \rangle$. Then $R = A \cup (N \setminus A^t)t$ is a $(4m^2, 2, 4m^2, 2m^2)$ RDS in G relative to $\langle t \rangle$.

Proof. As $AA^{(-1)} = m^2 + (m^2 - m)N$, $A^t(A^t)^{(-1)} = m^2 + (m^2 - m)N$. Hence A satisfies (i) and (ii) of Proposition 4.2. Therefore, $R = A + (N - A^t)t$ is a $(4m^2, 2, 4m^2, 2m^2)$ RDS in G relative to $\langle t \rangle$.

In [1], K.T. Arasu, et al. constructed a $(2n, 2, 2n, n)$ RDS in a group $Z_2 \times N$, where N is a group of order $2n$ containing an Hadamard difference set. The above proposition can be regarded as a slight generalization of their result.

Example 4.5 Let X be a group of order 4 and set $D = \{1\} \subset X$. Then D is an Hadamard difference set of order 1. Assume that a group $\langle y \rangle$ of order 2 operates on X . By Proposition 4.4, the following hold.

- (i) If $X = \langle x_1, x_2 \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ and y centralizes X , then $\{1\} \cup \{x_1, x_2, x_1x_2\}y$ is a $(4, 2, 4, 2)$ RDS in $\langle x_1, x_2, y \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ relative to $\langle y \rangle$.
- (ii) If $X = \langle x \rangle \simeq \mathbb{Z}_4$ and y centralizes X , then $\{1\} \cup \{x, x^2, x^3\}y$ is a $(4, 2, 4, 2)$ RDS in $\langle x, y \rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$ relative to $\langle y \rangle$.
- (iii) If $X = \langle x \rangle \simeq \mathbb{Z}_4$ and y inverts X , then $\{1\} \cup \{x, x^2, x^3\}y$ is a $(4, 2, 4, 2)$ RDS in $\langle x, y \rangle \simeq D_8$.

References

- [1] K.T. Arasu, D. Jungnickel, S.L. Ma, A. Pott, Relative difference sets with $n = 2$, *Discrete Mathematics* **147** (1995), 1-17.
- [2] D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.
- [3] Y. Hiramane, Semiregular relative difference sets in 2-groups containing a cyclic subgroup of index 2, to appear in *Journal of Combinatorial Theory*, Ser. A.
- [4] N. Ito, On Hadamard groups, *J. of Algebra* **168** (1994), 981-987.
- [5] D. Jungnickel, On Automorphism Groups of Divisible Designs, *Can. J. Math.* **24** (1982), 257-297.
- [6] A. Pott, "Finite Geometry and Character Theory," *Lecture Notes in Mathematics* 1601, Springer-Verlag, Berlin (1995)