第25回代数的組合せ論シンポジウム報告集

2008年6月23–25日

於　北海道大学学術交流会館

平成20年度文部科学省科学研究費基盤研究(B)

(課題番号　18340022　伊藤達郎)

まえがき

この報告集は、２００８年6月２３日(月)から２５日(水)にわたって、北海道大学学術交流会館でおこなわれた研究集会「第25回代数的組合せ論」の講演記録です。７４名の参加者を得る盛会でした。また２４日に開かれた懇親会も６１名の参加者を得る盛会でした。

この集会に関わる講演者の旅費、およびこの報告集の作成にあたっては、科学研究費基盤研究 (B) (研究代表者 金沢大学理学部教授 伊藤達郎) から大きな援助をいただきました。この場を借りて御礼申し上げます。

最後になりましたが、講演者の方々、会場の準備を手伝って下さった大学院生の方々のご協力に感謝します。

２００８年１２月
和嶋　雅幸
竹ヶ原裕元
田辺顕一朗

第25回代数的組合せ論

研 究 集 会

世話人： 和嶋雅幸 (北海道工業大学)
竹ヶ原裕元 (室蘭工業大学)
田辺顕一朗 (北海道大学)

記

日時： 2008年6月23日 (月) – 6月25日 (水)

場所： 北海道大学学術交流会館小講堂

6月23日 (月)

10:00 – 10:50 伊藤 達郎 (金沢大学)
Irreducible representations of Terwilliger algebras for P- and Q-polynomial association schemes

11:00 – 11:50 Paul Terwilliger (University of Wisconsin)
The classification of tridiagonal pairs with q-Racah type

13:30 – 14:20 Jack Koolen (POSTECH)
For fixed $k \geq 3$, there are finitely many distance-regular graphs with valency k

14:30 – 15:00 平木 彰 (大阪教育大学)
Completely regular subgraphs in distance-regular graphs

15:30 – 16:00 田上 真 (金沢大学)
Bipartite graph から得られる Gorenstein polytope

16:10 – 16:40 栗原 大武 (九州大学)
On spherical designs obtained from standard realization of association schemes

16:50 – 17:20 野崎 寛 (九州大学)
2つの球面上の堅い2-内積集合の分類

6月24日 (火)

10:00 – 10:50　吉田 知行 (北海道大学)
有限群上のランダムウォークと統計学への応用

11:00 – 11:50　Serge Bouc (C.N.R.S.)
The functor of units of Burnside rings for p-groups

13:30 – 14:00　丹原 大介 (弘前大学)
区間上の区分線形な同値関係について

14:10 – 14:40　功刀 直子 (東京理科大学), 和田 倶幸 (東京農工大学)
可換 2-シロー部分群をもつ群における主ブロックのカルタン行列の固有値

14:50 – 15:20　淵田 正夫 (東京医科歯科大学), 野村 和正 (東京医科歯科大学名誉教授)
整数行列の固有値と単因子

15:40 – 16:10　野澤 宗平 (千葉大学), 與口 卓志 (千葉大学)
ランク 2 のシャープ指標について

16:20 – 16:50　小田 文仁 (富山商船高等専門学校)
The partial Burnside ring relative to p-centric subgroups

17:00 – 17:30　城本 啓介 (愛知県立大学)
A Wei-type duality theorem for matroids

18:00 – 20:00　懇親会　会場：エンレイソウ, 会費：5500 円 (学生 3000 円)
(参加者 61 名でした.)

6月25日 (水)

10:00 – 10:30　秋山 献之 (福岡大学), 末竹 千博 (大分大学)
On projective planes of order 12 with a collineation group of order 9

10:40 – 11:10　末竹 千博 (大分大学)
The nonexistence of $STD_2[12;6]$'s with an automorphism group of order 9

11:20 – 11:50　中川 暢夫 (近畿大学)
標数 2 の有限体上の方程式と APN 関数の構成について

13:30 – 14:00　C. H. Lam (National Cheng Kung University)
Virasoro frames and frame stabilizers of the lattice VOA $V_{D_{16}^+}$.

14:10 – 14:40　Rowena A. L. Betty (東北大学)
Mass formula for self-orthogonal codes over $\mathbb{Z}_{p^2}$

14:50 – 15:20　中嶋 康博 (東北大学)
Livingstone-Wagner の定理の部分的な一般化

25th Algebraic Combinatorics

Date : June 23–25, 2008
Place : Conference Hall, Hokkaido University, Hokkaido, JAPAN
Organizer : Masayuki Wajima (Hokkaido Institute of Technology)
Yugen Takegahara (Muroran Institute of Technology)
Kenichiro Tanabe (Hokkaido University)

June 23 (Monday)

10:00 – 10:50 Tatsuro Ito (Kanazawa University)
Irreducible representations of Terwilliger algebras for P- and Q-polynomial association schemes

11:00 – 11:50 Paul Terwilliger (University of Wisconsin)
The classification of tridiagonal pairs with q-Racah type

13:30 – 14:20 Jack Koolen (POSTECH)
For fixed $k \geq 3$, there are finitely many distance-regular graphs with valency k

14:30 – 15:00 Akira Hiraki (Osaka Kyoiku University)
Completely regular subgraphs in distance-regular graphs

15:30 – 16:00 Makoto Tagami (Kanazawa University)
Gorenstein polytopes obtained from bipartite graphs

16:10 – 16:40 Hirotake Kurihara (Kyushu University)
On spherical designs obtained from standard realization of association schemes

16:50 – 17:20 Hiroshi Nozaki (Kyushu University)
Classification of tight 2-inner product set on 2 concentric spheres

June 24 (Tuesday)

10:00 – 10:50 Tomoyuki Yoshida (Hokkaido University)
Random walks on finite groups with application to statistics

11:00 – 11:50 Serge Bouc (C.N.R.S.)
The functor of units of Burnside rings for p-groups

13:30 – 14:00 Daisuke Tambara (Hirosaki University)
Piecewise-linear equivalence relations on a interval

14:10 – 14:40 Naoko Kunugi (Tokyo University of Science),
Tomoyuki Wada (Tokyo University of Agriculture and Technology)
Eigenvalues of Cartan matrices of principal 2-blocks with abelian defect groups

14:50 – 15:20 Masao Kiyota (Tokyo Medical and Dental University),
Kazumasa Nomura (Professor emeritus at Tokyo Medical and Dental University)
Eigenvalues and elementary divisors of integral matrices

15:40 – 16:10 Sohei Nozawa (Chiba University), Takashi Yoguchi (Chiba University)
On sharp characters of rank 2

16:20 – 16:50 Fumihito Oda (Toyama National College of Maritime Technology)
The partial Burnside ring relative to p-centric subgroups

17:00 – 17:30 Keisuke Shiromoto (Aichi Prefectural University)
A Wei-type duality theorem for matroids

18:00 – 20:00 Banquet at Enreiso

June 25 (Wednesday)

10:00 – 10:30 Kenzi Akiyama (Fukuoka University), Chihiro Suetake (Oita University)
On projective planes of order 12 with a collineation group of order 9

10:40 – 11:10 Chihiro Suetake (Oita University)
The nonexistence of $STD_2[12;6]$'s with an automorphism group of order 9

11:20 – 11:50 Nobuo Nakagawa (Kinki University)
On equations over finite fields of characteristic 2 and constructions of APN functions

13:30 – 14:00 C. H. Lam (National Cheng Kung University)
Virasoro frames and frame stabilizers of the lattice VOA $V_{D_{16}^+}$.

14:10 – 14:40 Rowena A. L. Betty (Tohoku University)
Mass formula for self-orthogonal codes over $\mathbb{Z}_{p^2}$

14:50 – 15:20 Yasuhiro Nakashima (Tohoku University)
A partial generalization of the Livingstone-Wagner theorem

目次

No.
Date

P- and Q-polynomial association scheme に附随する Terwilliger algebra の既約表現について

伊藤 達郎 (金沢大学)

P- and Q-polynomial association scheme に附随する Terwilliger algebra の既約表現について. 2000年頃から Paul Terwilliger (Wisconsin 大学) と協同で研究を進めてきたが, 1段落つきかけているので, その報告をする. 以下 ground field は複素数体 $\mathbb{C}$ とし, algebra といえば単位元 1 を持つ associative な $\mathbb{C}$-algebra を意味することとする.

1 $\mathcal{X} = (X, \{R_i\}_{0 \le i \le D})$ を P- and Q-polynomial association scheme, T を $\mathcal{X}$ の Terwilliger algebra (T-algebra) とする. T は有限次半単純代数となる. A, A^* を T の標準的生成元, V を T の既約加群とすると, A, A^* は次の意味で TD-pair (tridiagonal pair) となる.

(i) A, A^* の V への作用は対角化可能

(ii) $V = \bigoplus_{i=0}^{d} V_i$ を A の V への作用の固有空間分解とすると

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

ただし $V_{-1} = V_{d+1} = 0$.

(iii) $V = \bigoplus_{i=0}^{d^*} V_i^*$ を A^* の V への作用の固有空間分解とすると

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

ただし $V_{-1}^* = V_{d^*+1}^* = 0$.

No.
Date

tridiagonal pair という名前は (ii), (iii) に由来する. V が T の primary module のとき. (ii) は A の Q-polynomial 性と同値であり. (iii) は A^* の P-polynomial 性と同値である. TD-pair の公理的定義は以下のように行う. V を有限次元線形空間, A, A^* を V の線形変換とし, $\langle A, A^* \rangle$ を A, A^* で生成される $End(V)$ の部分代数とするとき, A, A^* が

(i), (ii), (iii) かつ

(iv) V は $\langle A, A^* \rangle$-加群として既約

をみたすならば. A, A^* を TD-pair と呼ぶ. 今の場合 基礎体が $\mathbb{C}$ なので. (iv) は $End(V) = \langle A, A^* \rangle$ と同値である. 条件 (ii), (iii) においては固有空間の並べ方が意味を持っていることに注意する. もし $V_0, V_1, \cdots, V_d$ なる並べ方に関して (ii) が成立するならば $V_d, \cdots, V_1, V_0$ に関しても (ii) が成立し. その他の並べ方に関しては (ii) は成立しない. 条件 (iii) についても同様である. また A, A^* が TD-pair ならば. A の固有空間の個数と A^* のそれとは一致しなければならないことが知られている. 従って TD-pair の定義において. (ii) の d と (iii) の d^* とはじめから $d = d^*$ としてもさしつかえない. この d を TD-pair A, A^* の直径 と呼ぶ. 自明な場合を除くため. 以下 $d \geq 1$ を仮定する.

以上のようにして. Terwilliger algebra T と T の既約加群 V から TD-pair $A|_V, A^*|_V \in End(V)$ ができ. この意味で T の既約表現の決定問題は TD-pair の分類問題に帰着される. ただしどの TD-pair がこのようにして得られるかということは別の問題として残る. 実際 T の既約加群から得られる TD-pair にはある種の条件がつき (証明されている条件もあれば. 予想されているだけの条件もある). そのことをコントロールしているのが P- and Q-polynomial association scheme の組合せ構造であると考えられる.
なお TD-pair $A, A^* \in End(V)$ と TD-pair $B, B^* \in End(V')$ の同型は. 線形空間としての同型写像 $\varphi : V \longrightarrow V'$ で $\varphi A = B\varphi$, $\varphi A^* = B^*\varphi$ となるものの存在をもって定義とする.

No.
Date

2 TD-pair $A, A^* \in End(V)$ は次の関係式 (TD) をみたす.

$$(TD)\quad \begin{cases} [A, A^2A^* - \beta AA^*A + A^*A^2] = \gamma[A, AA^* + A^*A] + \delta[A, A^*], \\ [A^*, A^{*2}A - \beta A^*AA^* + AA^{*2}] = \gamma^*[A^*, A^*A + AA^*] + \delta^*[A^*, A]. \end{cases}$$

ここで $\beta, \gamma, \gamma^*, \delta, \delta^*$ は定数であり. 直径 d が $d \geq 3$ ならば, TD-pair A, A^* によって一意的に定まる. また $[\ ,\ ]$ は通常のブラケット積で $[X, Y] = XY - YX$ を意味する. 関係式 (TD) は TD-relations (tridiagonal relations) と呼ばれる. 以下

$$\beta = q^2 + q^{-2}$$

なる $q \in \mathbb{C} - \{0\}$ を選び固定する. 今後常に $q^{2(d+1)} \neq 1$ としてみる. このとき関係式 (TD) の意味するところは以下の通りである. TD-pair の定義に現れる条件 (i), (iv) が成立している前提の下で, 条件 (ii), (iii) と 関係式 (TD) は同値である. 従って TD-pair の分類問題は, 生成元 A, A^* と関係式 (TD) によって定義される無限次元代数の有限次元既約表現で A, A^* の作用が対角化可能なものの決定問題と同値である. この無限次元代数は TD-algebra (tridiagonal algebra) と呼ばれるが, TD-pair の標準化を論じた後に改めて定義し直す.

TD-pair $A, A^* \in End(V)$ の固有空間分解を $V = \bigoplus_{i=0}^{d} V_i = \bigoplus_{i=0}^{d} V_i^*$ とし, A の V_i 上の固有値を θ_i, A^* の V_i^* 上の固有値を θ_i^* とおく. このとき $q^2 \neq \pm 1$, $q^2 = 1$, $q^2 = -1$ に応じて θ_i, θ_i^* は次のように書き表わされる.

Case I ($q^2 \neq \pm 1$) 定数 a, a^*, b, b^*, c, c^* が存在して

$$\theta_i = a + bq^{2i} + cq^{-2i} \quad (0 \leq i \leq d),$$
$$\theta_i^* = a^* + b^*q^{2i} + c^*q^{-2i} \quad (0 \leq i \leq d).$$

このとき $\gamma = -(q - q^{-1})^2 a$, $\gamma^* = -(q - q^{-1})^2 a^*$, $\delta = (q - q^{-1})^2 a^2 - (q^2 - q^{-2})^2 bc$, $\delta^* = (q - q^{-1})^2 a^{*2} - (q^2 - q^{-2})^2 b^* c^*$.

No.
Date

Case II ($q^2=1$) 定数 a, a^*, b, b^*, c, c^* が存在して

$$\theta_i = a + bi + ci^2 \qquad (0 \le i \le d),$$
$$\theta_i^* = a^* + b^* i + c^* i^2 \qquad (0 \le i \le d).$$

このとき $r=2c$, $r^*=2c^*$, $\delta = b^2 - c^2 - 4ac$, $\delta^* = b^{*2} - c^{*2} - 4a^*c^*$

Case III ($q^2=-1$) 定数 a, a^*, b, b^*, c, c^* が存在して

$$\theta_i = a + b(-1)^i + c(-1)^i i \qquad (0 \le i \le d),$$
$$\theta_i^* = a^* + b^*(-1)^i + c^*(-1)^i i \qquad (0 \le i \le d).$$

このとき $r=4a$, $r^*=4a^*$, $\delta = -4a^2 + c^2$, $\delta^* = -4a^{*2} + c^{*2}$.

それぞれの場合に応じて TD-pair は, type I, type II, type III と呼ばれる. 本稿は type I の TD-pair の分類を論じる. TD-pair が P- and Q-polynomial association scheme $\mathcal{X} = (X, \{R_i\}_{0 \le i \le D})$ の Terwilliger algebra T の既約表現から来ている場合は, association scheme $\mathcal{X}$ の直径 D がある程度大きければ (例えば $D \ge 5$). TD-pair の固有値 θ_i, θ_i^* $(0 \le i \le d)$ は有理数であり (ただし $\mathcal{X}$ は多角形ではないとする). β は T の primary module ($d=D$) で定まるから. type I ならば q は 1 の中根とはならない. 後で以下 $q \ne$ root of unity と仮定する.

Assumption $q \ne$ root of unity.

q が 1 の中根のときも同様の議論が可能だが, 技術的問題により別のとり扱いが必要なので, type III の TD-pair の分類とあわせて稿を改めて論じたい.

No.
Date

affine 変換 $A \longmapsto \lambda A + \mu I$, $A^* \longmapsto \lambda^* A^* + \mu^* I$ ($\lambda, \lambda^*, \mu, \mu^* \in \mathbb{C}$, $\lambda \neq 0$, $\lambda^* \neq 0$, I は恒等写像) により TD-pair $A, A^* \in End(V)$ から新たな TD-pair $\lambda A + \mu I$, $\lambda^* A^* + \mu^* I \in End(V)$ が得られる. このとき β, 従って ρ は不変である. 従って affine 変換を施すことにより (必要なら固有空間 $\{V_i\}_{i=0}^d$ または $\{V_i^*\}_{i=0}^d$ の順序付けを反転させて), TD-pair A, A^* の固有値を

$$\theta_i = b q^{2i-d} + \varepsilon b^{-1} q^{d-2i} \qquad (0 \leq i \leq d),$$
$$\theta_i^* = \varepsilon^* b^* q^{2i-d} + b^{*-1} q^{d-2i} \qquad (0 \leq i \leq d)$$

としても一般性を失わない ($b, b^* \in \mathbb{C} - \{0\}$ は定数, $\varepsilon, \varepsilon^* \in \{1, 0\}$). また もし $(\varepsilon, \varepsilon^*) = (0, 1)$ ならば, A と A^* を入れ換え 更に $\{V_i^*\}_{i=0}^d$ の順序を反転すると $(\varepsilon, \varepsilon^*) = (1, 0)$ なる TD-pair が得られる. よって

$$(\varepsilon, \varepsilon^*) = (1, 1), (1, 0), (0, 0)$$

としても一般性を失わない. このような TD-pair を 標準化された TD-pair と呼び, $(\varepsilon, \varepsilon^*) = (1, 1), (1, 0), (0, 0)$ に応じて 第1種, 第2種, 第3種の TD-pair という. $(\varepsilon, \varepsilon^*)$ は標準化の仕方によらず 一意的に定まる. 標準化された TD-pair A, A^* のみたす TD-relations は

$$(TD) \quad \begin{cases} [A, A^2 A^* - \beta A A^* A + A^* A^2] = \varepsilon \delta [A, A^*] \\ [A^*, A^{*2} A - \beta A^* A A^* + A A^{*2}] = \varepsilon^* \delta [A^*, A] \end{cases}$$

である ($\beta = q^2 + q^{-2}$, $\delta = -(q^2 - q^{-2})^2$). 以下本稿では, $q \neq$ root of unity の仮定の下に, 標準化された TD-pair の分類を論じる. 分類は affine 量子群 $U_q(\widehat{sl}_2)$ の表現を介して与えられる. Terwilliger algebra の既約表現から来る TD-pair は 実例では すべて第2種 または 第3種であり, 第1種のものは ひとつも現れない. 何らかの組合せ論的構造を反映しているものと思われる.

No.
Date

$q \in \mathbb{C}-\{0\}$ と $(\varepsilon,\varepsilon^*) \in \{(1,1),(1,0),(0,0)\}$ を選び固定する. ただし $q \neq$ root of unity とする. 単位元 1 を持つ associative algebra $\mathcal{A} = \mathcal{A}_q^{(\varepsilon,\varepsilon^*)}$ を生成元 z, z^* と 関係式 (TD) により定義する:

$$(TD)\begin{cases} [z,\ z^2z^*-\beta zz^*z+z^*z^2] = \varepsilon\delta[z,z^*] \\ [z^*,\ z^{*2}z-\beta z^*zz^*+zz^{*2}] = \varepsilon^*\delta[z^*,z] \end{cases}$$

($\beta = q^2+q^{-2}$, $\delta = -(q^2-q^{-2})^2$). $\mathcal{A}$ を <u>TD-algebra</u> と呼ぶ.

$TD_q^{(\varepsilon,\varepsilon^*)}$ = 標準化された TD-pair A, A^* で 固有値が

$$\theta_i = bq^{2i-d}+\varepsilon b^{-1}q^{d-2i},\quad \theta_i^* = \varepsilon^* b^* q^{2i-d}+b^{*-1}q^{d-2i} \qquad (0\le i\le d)$$

for some $b, b^* \in \mathbb{C}-\{0\}$, $d \in \mathbb{N}$

の形 をしている もの の 同型類 の 全体

$Irr(\mathcal{A})$ = $\mathcal{A}$ の 有限次元既約表現 の 同型類 の 全体

$\cup$

$Irr'(\mathcal{A})$ = $\mathcal{A}$ の 有限次元既約表現 $\rho: \mathcal{A} \longrightarrow End(V)$ で

$\rho(z)$, $\rho(z^*)$ が 対角化可能 な もの の 同型類 の 全体

とおく. $TD_q^{(\varepsilon,\varepsilon^*)}$ に 属する TD-pair $A, A^* \in End(V)$ に 対し,

対応 $z \longmapsto A$, $z^* \longmapsto A^*$ により $Irr'(\mathcal{A})$ に 属する 既約表現

$$\rho: \mathcal{A} \longrightarrow End(V) \qquad (\rho(z)=A,\ \rho(z^*)=A^*)$$

が 得られる. この対応は $TD_q^{(\varepsilon,\varepsilon^*)}$ と $Irr'(\mathcal{A})$ の bijection を与える.

以下 $Irr'(\mathcal{A})$ を 決定する こと を 目標 とする. $(\varepsilon,\varepsilon^*)=(1,1)$ の 場合は,

(TD) は Dolan-Grady relations の q-analogue と みなされるので,

$\mathcal{A}$ は q-Onsager algebra と 呼ぶのが ふさわしい. この場合は,

$Irr(\mathcal{A}) = Irr'(\mathcal{A})$ が 成立つので, $Irr'(\mathcal{A})$ の 決定は q-Onsager algebra の 有限次元既約表現 の 決定 を 意味する.

No.
Date

3 $A, A^* \in End(V)$ を TD-pair とし、$V = \bigoplus_{i=0}^{d} V_i = \bigoplus_{i=0}^{d} V_i^*$ を A, A^* の固有空間分解とする.

$$U_i = (V_0^* + \cdots + V_i^*) \cap (V_i + \cdots + V_d)$$

とおくと

$$V = \bigoplus_{i=0}^{d} U_i$$

が成立つ. これを split decomposition と呼ぶ.

$$\dim U_i = \dim V_i, \quad \dim U_i = \dim V_i^* \qquad (0 \le i \le d),$$
$$\dim U_i = \dim U_{d-i} \qquad (0 \le i \le d)$$

が成立つ. A の V_i 上の固有値を θ_i, A^* の V_i^* 上の固有値を θ_i^*. V から U_i への射影を

$$F_i : V = \bigoplus_{i=0}^{d} U_i \longrightarrow U_i$$

とし,

$$R = A - \sum_{i=0}^{d} \theta_i F_i$$
$$L = A^* - \sum_{i=0}^{d} \theta_i^* F_i$$

とおく. R, L を raising map, lowering map と呼ぶ.

$$RU_i \subseteq U_{i+1} \qquad (0 \le i \le d),$$
$$LU_i \subseteq U_{i-1} \qquad (0 \le i \le d)$$

が成立つ (ただし $U_{-1} = U_{d+1} = 0$).

No.
Date

TD-pair $A, A^* \in \mathrm{End}(V)$ が $TD_q^{(\varepsilon,\varepsilon^*)}$ に属するとする. すなわち A, A^* は標準化されていて, 固有値は $\theta_i = bq^{2i-d} + \varepsilon b^{-1} q^{d-2i}$, $\theta_i^* = \varepsilon^* b^* q^{2i-d} + b^{*-1} q^{d-2i}$ である.

$$K = \sum_{i=0}^{d} q^{2i-d} F_i$$

とおく. K は正則であり

$$R = A - (bK + \varepsilon b^{-1} K^{-1})$$
$$L = A^* - (\varepsilon^* b^* K + b^{*-1} K)$$

と書ける. $RU_i \subseteq U_{i+1}$, $LU_i \subseteq U_{i-1}$ $(0 \le i \le d)$ は

$$(TD)_0' \begin{cases} KRK^{-1} = q^2 R \\ KLK^{-1} = q^{-2} R \end{cases}$$

と同値である. よって $(TD)_0'$ の下で, A, A^* のみたすべき TD-relations (TD) は

$$(TD)' \begin{cases} [R, R^2L - \beta RLR + LR^2] = \delta'(\varepsilon^* R^2 K^2 - \varepsilon K^{-2} R^2) \\ [L, L^2R - \beta LRL + RL^2] = \delta'(-\varepsilon^* K^2 L^2 + \varepsilon L^2 K^{-2}) \end{cases}$$

と同値である $(\beta = q^2 + q^{-2}$, $\delta' = -(q - q^{-1})(q^2 - q^{-2})(q^3 - q^{-3}) q^4)$. $(TD)_0'$ は

$$(TD)_0 \begin{cases} \dfrac{qAK - q^{-1}KA}{q - q^{-1}} = bK^2 + \varepsilon b^{-1} I \\ \dfrac{qKA^* - q^{-1}A^*K}{q - q^{-1}} = \varepsilon^* b^* K^2 + b^{*-1} I \end{cases}$$

と同値である. $(TD)_0$ を <u>generalized q-Weyl relations</u> という.

以上をふまえ、単位元1を持つ$\mathbb{C}$上の associative algebra $\mathcal{T} = \mathcal{T}_q^{(\varepsilon,\varepsilon^*)}$ を生成元 x, y, k, k^{-1} と関係式 $(TD)_0'$, $(TD)'$ によって定義する:

$$(TD)_0' \quad \begin{cases} kk^{-1} = k^{-1}k = 1, \\ kxk^{-1} = q^2 x, \quad kyk^{-1} = q^{-2}y, \end{cases}$$

$$(TD)' \quad \begin{cases} [x, x^2y - \beta xyx + yx^2] = \delta'(\varepsilon^* x^2k^2 - \varepsilon k^{-2}x^2), \\ [y, y^2x - \beta yxy + xy^2] = \delta'(-\varepsilon^* k^2y^2 + \varepsilon y^2k^{-2}) \end{cases}$$

($\beta = q^2 + q^{-2}$, $\delta' = -(q-q^{-1})(q^2-q^{-2})(q^3-q^{-3})q^4$). ただし $q \neq$ root of unity, $(\varepsilon, \varepsilon^*) = (1,1), (1,0)$ or $(0,0)$ である。$\mathcal{T}$ を augmented TD-algebra という。任意の $t \in \mathbb{C} - \{0\}$ に対して

$$z_t = x + tk + \varepsilon t^{-1}k^{-1}$$
$$z_t^* = y + \varepsilon^* t^{-1}k + tk^{-1}$$

とおく.

$$(TD)_0 \quad \begin{cases} kk^{-1} = k^{-1}k = 1 \\ \dfrac{qz_tk - q^{-1}kz_t}{q-q^{-1}} = tk^2 + \varepsilon t^{-1} \\ \dfrac{qkz_t^* - q^{-1}z_t^*k}{q-q^{-1}} = \varepsilon^* t^{-1}k^2 + t \end{cases}$$

$$(TD) \quad \begin{cases} [z_t, z_t^2 z_t^* - \beta z_t z_t^* z_t + z_t^* z_t^2] = \varepsilon\delta[z_t, z_t^*] \\ [z_t^*, z_t^{*2} z_t - \beta z_t^* z_t z_t^* + z_t z_t^{*2}] = \varepsilon^*\delta[z_t^*, z_t] \end{cases}$$

($\beta = q^2 + q^{-2}$, $\delta = -(q^2-q^{-2})^2$) が成立つ. 逆に $(TD)_0$, (TD) から $(TD)_0'$, $(TD)'$ が導かれるから. 各々の $t \in \mathbb{C} - \{0\}$ ごとに 生成元 z_t, z_t^*, k, k^{-1} と関係式 $(TD)_0$, (TD) は $\mathcal{T}$ の 2nd presentation を与える.

No.
Date

$b, b^* \in \mathbb{C}-\{0\}$, $d \in \mathbb{N}$ に対し.

$TD_q^{(\varepsilon,\varepsilon^*)}(b, b^*; d)$ = 標準化された TD-pair A, A^* で固有値が
$\theta_i = bq^{2i-d} + \varepsilon b^{-1} q^{d-2i}$, $\theta_i^* = \varepsilon^* b^* q^{2i-d} + b^{*-1} q^{d-2i}$
$(0 \le i \le d)$ であるものの同型類の全体

とおく. θ_i $(0 \le i \le d)$ が相異なり, θ_i^* $(0 \le i \le d)$ と相異なるための条件

$$\pm\varepsilon b, \pm\varepsilon^* b^* \notin \{q^{-d+1}, q^{-d+2}, \cdots, q^{d-2}, q^{d-1}\}$$

が, b, b^*, d に課されることに注意する. $b, b^* \in \mathbb{C}-\{0\}$ に対して

$$b = st, \quad b^* = st^{-1}$$

とおく. $bb^* = s^2$, $bb^{*-1} = t^2$ であるから (s, t) は b, b^* により
$\pm$ 符号を除いて一意的に定まる.

TD-pair $A, A^* \in End(V)$ が $TD_q^{(\varepsilon,\varepsilon^*)}(b, b^*; d)$ に属するとする.
前述したように $V = \bigoplus_{i=0}^{d} U_i$ を split decomposition, $F_i : V \longrightarrow U_i$ を射影,
$K = \sum q^{2i-d} F_i$, $R = A - (bK + \varepsilon b^{-1} K^{-1})$, $L = A^* - (\varepsilon^* b^* K + b^{*-1} K)$
とおく. また $b = st$, $b^* = st^{-1}$ を満たす $s, t \in \mathbb{C}-\{0\}$ を選び固定する.
このとき

$$\rho : \mathcal{T} \longrightarrow End(V) \qquad (x, y, k \longmapsto R, L, sK \text{ respectively})$$

は $\mathcal{T}$ の有限次元既約表現を与える. $\mathcal{T}$ の 2nd generators z_t, z_t^*, $k^{\pm}$
(t は上で選び固定したもの) によって ρ による対応を書くと

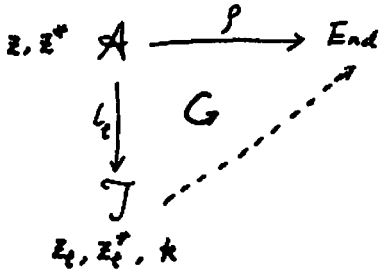
$$\rho : \mathcal{T} \longrightarrow End(V) \qquad (z_t, z_t^*, k \longmapsto A, A^*, sK \text{ respectively})$$

となる. このことは次のように解釈される. $\mathcal{A} = \mathcal{A}_q^{(\varepsilon,\varepsilon^*)}$ とおくと.

No.
Date

$$\iota = \iota_t : \quad \mathcal{A} \longrightarrow \mathcal{T} \qquad (z, z^* \longmapsto z_t, z_t^* \quad \text{respectively})$$

なる algebra homomorphism が自然に定まる（実は injective になる）．
$\mathrm{Irr}'(\mathcal{A})$ と $TD_q^{(\zeta,\zeta^*)}$ の間の 1:1 対応を介して，$\mathrm{Irr}'(\mathcal{A})$ に属する $\mathcal{A}$ の有限次元既約表現 ρ は $\mathcal{T}$ に拡張される：



ただし b, b^* に対し (s,t) の代りに $(-s,-t)$ を選んでもよいから，拡張の仕方は 2 通りある．このようにして $\mathcal{T}$ にまで拡張された表現も同じ記号 ρ で表すことにすると，$\mathcal{T}$ の有限次元既約表現として $\rho : \mathcal{T} \longrightarrow \mathrm{End}(V)$ は次の性質を持つ：

$(C_1)_t$: $\rho(z_t)$, $\rho(z_t^*)$ は対角化可能．

$(C_2)_t$: ρ の $\mathcal{A}_t$ への制限 $\rho|_{\mathcal{A}_t} : \mathcal{A}_t \longrightarrow \mathrm{End}(V)$ は既約

ただし $\mathcal{A}_t$ は z_t, z_t^* によって生成される $\mathcal{T}$ の subalgebra．

逆に $\mathcal{T}$ の有限次元既約表現 $\rho : \mathcal{T} \longrightarrow \mathrm{End}(V)$ が，ある $t \in \mathbb{C}-\{0\}$ について $(C_1)_t$, $(C_2)_t$ をみたすならば，$\rho \circ \iota_t : \mathcal{A} \longrightarrow \mathrm{End}(V)$ は $\mathrm{Irr}'(\mathcal{A})$ に属する．従って

$$\mathrm{Irr}'(\mathcal{T}) = \begin{array}{l}\mathcal{T} \text{ の有限次元既約表現 } \rho : \mathcal{T} \longrightarrow \mathrm{End}(V) \text{ で} \\ \text{ある } t \in \mathbb{C}-\{0\} \text{ について } (C_1)_t,\ (C_2)_t \text{ をみたすものの} \\ \text{同型類の全体}\end{array}$$

~~とおくと 対応 $\rho \longmapsto \rho \circ \iota_t$ は $\mathrm{Irr}'(\mathcal{T})$ から $\mathrm{Irr}'(\mathcal{A})$ への 2:1 の全射とう~~

No.
Date

実は 外の表現よりも $\mathcal{T}$ の表現の方が扱い易い. それ故 $\mathrm{Irr}'(A)$ と決める代りに $\mathrm{Irr}'(\mathcal{T})$ を決めることにする.

$\mathrm{Irr}(\mathcal{T})$ = $\mathcal{T}$ の有限次元既約表現の同型類の全体

とおくと. 我々の問題は次の2点となる.

Problem (1) $\mathrm{Irr}(\mathcal{T})$ を決定せよ.

(2) $\mathrm{Irr}(\mathcal{T})$ に属する $\rho : \mathcal{T} \longrightarrow \mathrm{End}(V)$ が $(C_1)_\xi$, $(C_2)_\xi$ をみたすための判定条件をおめよ.

次の Lemma により この問題をもう少し整理する.

Lemma $\mathrm{Irr}(\mathcal{T})$ に属する $\rho : \mathcal{T} \longrightarrow \mathrm{End}(V)$ が与えられているとする. ρ を通して V を $\mathcal{T}$-加群とみなすと. 次の (i), (ii), (iii) が成立する

(i) k の V への作用は対角化可能である.

(ii) k の V への作用の固有空間分解を $V = \bigoplus_{i=0}^{d} U_i$ とすると. ある $s \in \mathbb{C} - \{0\}$ が存在して k の U_i 上の固有値は sq^{2i-d} $(0 \le i \le d)$ と書ける.

(iii) x, y の V への作用は 0 である. 更に強く

$$xU_i \subseteq U_{i+1}, \quad yU_i \subseteq U_{i-1} \quad (0 \le i \le d)$$

が成立つ. ただし $U_{-1} = U_{d+1} = 0$.

上の Lemma における s, d, A や k の固有空間 U_i の並べる順序は. ρ によって一意的に定まることに注意する. s, d を表現 ρ の(又は $\mathcal{T}$-加群 V の type, 直径 と呼ぶ. $V = \bigoplus_{i=0}^{d} U_i$ を weight space decomposition, U_0 を highest weight space という.

No.
Date

$TD_g^{(\varepsilon,\varepsilon^*)}(b,b^*;d)$ に属する TD-pair $A, A^* \in End(V)$ に対し、対応 $z_t \longmapsto A$, $z_t^* \longmapsto A^*$, $k \longmapsto sK$ により $Irr(\mathcal{T})$ に属する表現 $\rho : \mathcal{T} \longrightarrow End(V)$ が定まる。ただし (s,t) は、$b = st$, $b^* = st^*$ をみたすように前もって選び固定しておく。表現 ρ の type は s, 直径は d となる。ρ の weight space decomposition は TD-pair A, A^* の split decomposition と一致する。更に ρ は $(C_1)_t$, $(C_2)_t$ をみたす。

$Irr_d^s(\mathcal{T})$ = $\mathcal{T}$ の有限次元既約表現 $\rho : \mathcal{T} \longrightarrow End(V)$ で type s, 直径 d をもつものの同型類の全体

$Irr_d^{s,t}(\mathcal{T})$ = $Irr_d^s(\mathcal{T})$ に属する表現の同型類のうちで $(C_1)_t$, $(C_2)_t$ をみたすものの全体

とおくと、$TD_g^{(\varepsilon,\varepsilon^*)}(b,b^*;d)$ から $Irr_d^{s,t}(\mathcal{T})$ への上記の対応は bijective である。従って我々の解くべき問題は次のようになり、以下本稿はその解を述べるためにあてられる。

Problem

(1) $Irr_d^s(\mathcal{T})$ を決定せよ。

(2) $Irr_d^s(\mathcal{T})$ に属する $\rho : \mathcal{T} \longrightarrow End(V)$ が $(C_1)_t$, $(C_2)_t$ をみたすための判定条件を求めよ。

No.
Date

4. $A = A_q^{(\iota,\varepsilon^*)}$ を TD-algebra, $J = J_q^{(\iota,\varepsilon^*)}$ を augmented TD-algebra とする
まず A および J の linear basis を与える.

$$\Lambda_n = \left\{ \lambda = (\lambda_0, \lambda_1, \cdots, \lambda_n) \in \mathbb{Z}^{n+1} \;\middle|\; \lambda_0 \geq 0, \quad \lambda_i \geq 1 \ (1 \leq i \leq n) \right\},$$

$$\Lambda = \bigcup_{n \geq 0} \Lambda_n$$

とおく. $\Lambda_n \ni \lambda = (\lambda_0, \lambda_1, \cdots, \lambda_n)$ が

$$\lambda_0 < \lambda_1 < \cdots < \lambda_i \geq \lambda_{i+1} \geq \cdots \geq \lambda_n$$

for some i $(0 \leq i \leq n)$ を満たすとき, <u>irreducible</u> という.

$$\Lambda^{ir} = \left\{ \lambda \in \Lambda \;\middle|\; \lambda \text{ is irreducible} \right\}$$

とおく. 特に $\Lambda_0, \Lambda_1 \subset \Lambda^{ir}$ である.

$\Lambda \ni \lambda = (\lambda_0, \lambda_1, \cdots, \lambda_n)$ と symbols X, Y に対して word $w_\lambda(X,Y)$ を

$$w_\lambda(X,Y) = \begin{cases} X^{\lambda_0} Y^{\lambda_1} \cdots Y^{\lambda_{n-1}} X^{\lambda_n} & \text{if } n \text{ is even,} \\ X^{\lambda_0} Y^{\lambda_1} \cdots X^{\lambda_{n-1}} Y^{\lambda_n} & \text{if } n \text{ is odd} \end{cases}$$

で定める. word $w_\lambda(X,Y)$ の長さは $|\lambda| = \lambda_0 + \lambda_1 + \cdots + \lambda_n$ である.
$|\lambda| = 0$ のときは $w_\lambda(X,Y) = 1$ と解釈する. すなわち $\lambda_0 = 0$ のときは.
$X^{\lambda_0} = 1$ と解釈する.

No.
Date

Theorem 次の集合は、A の線形空間としての基底をなす.

$$\left\{ W_\lambda(z, z^*) \;\middle|\; \lambda \in \Lambda^{in} \right\}.$$

Theorem 次の集合 (i), (ii) はいずれも $\mathcal{T}$ の線形空間としての基底をなす.

(i) $\left\{ k^n W_\lambda(x, y) \;\middle|\; n \in \mathbb{Z},\ \lambda \in \Lambda^{in} \right\}$.

(ii) $\left\{ k^n W_\lambda(z_t, z_t^*) \;\middle|\; n \in \mathbb{Z},\ \lambda \in \Lambda^{in} \right\}$.

ただし t は任意に固定された $\mathbb{C}-\{0\}$ の元とする.

2番目の Thm の (i) と Lemma の (iii) を用いると、$\mathrm{Irr}_d^s(\mathcal{T})$ に属する $\rho : \mathcal{T} \longrightarrow \mathrm{End}(V)$ が $(C_1)_t$ をみたすための判定条件が求まる.

Proposition $\mathrm{Irr}_d^s(\mathcal{T})$ に属する $\rho : \mathcal{T} \longrightarrow \mathrm{End}(V)$ に対して、次の (i), (ii) が成立つ.

(i) $\rho(z_t)$ が対角化可能

$\Leftrightarrow$

$\theta_i = st q^{2i-d} + \varepsilon s^{-1} t^{-1} q^{d-2i}$ $(0 \le i \le d)$ が相異なる.

(ii) $\rho(z_t^*)$ が対角化可能

$\Leftrightarrow$

$\theta_i^* = \varepsilon^* s t^{-1} q^{2i-d} + s^{-1} t\, q^{d-2i}$ $(0 \le i \le d)$ が相異なる.

No.
Date

$\theta_i = st q^{2i-d} + \varepsilon s^{-1}t^{-1} q^{d-2i}$ $(0 \le i \le d)$ が相異なる

$\Leftrightarrow$

$\pm \varepsilon st \notin \{ q^{-d+1}, q^{-d+2}, \cdots, q^{d-2}, q^{d-1} \}$

$\theta_i^* = \varepsilon^* s t^{-1} q^{2i-d} + s^{-1} t q^{d-2i}$ $(0 \le i \le d)$ が相異なる

$\Leftrightarrow$

$\pm \varepsilon^* s t^{-1} \notin \{ q^{-d+1}, q^{-d+2}, \cdots, q^{d-2}, q^{d-1} \}$

であるから. Proposition における $(C_1)_t$ は. parameter $(s, t; d)$ に関する条件であり, 表現 $\rho : \mathcal{T} \longrightarrow End(V)$ に関する条件のように見えるのは見掛けだけであることが分る.

$$\Lambda^{(i)} = \left\{ \lambda = (\lambda_0, \lambda_1, \cdots, \lambda_n) \in \Lambda \;\middle|\; \lambda_0 - \lambda_1 + \cdots + (-1)^n \lambda_n = i \right\}$$

$$\Xi^{(i)} = \sum_{\lambda \in \Lambda^{(i)}} \mathbb{C}\, \omega_\lambda(x, y) \quad \subset \mathcal{T}$$

$$\Xi = \sum_{i \in \mathbb{Z}} \Xi^{(i)} \quad \subset \mathcal{T}$$

とおく. Ξ は x, y で生成される $\mathcal{T}$ の subalgebra である.

$$\mathcal{T} = \mathbb{C}[k, k^{-1}]\, \Xi$$

$$= \bigoplus_{i \in \mathbb{Z}} \mathbb{C}[k, k^{-1}]\, \Xi^{(i)}$$

が成立つ. $\mathbb{C}[k, k^{-1}]\, \Xi^{(i)} = \Xi^{(i)} \mathbb{C}[k, k^{-1}]$, $\Xi^{(i)} \Xi^{(j)} \subseteq \Xi^{(i+j)}$ であるから. $\mathcal{T}$ は graded algebra となる. $\Xi^{(0)}$ は $\mathcal{T}$ の subalgebra である.

No.
Date

$\mathcal{T}$ の algebra としての anti-automorphism で $\tau : \mathcal{T} \longrightarrow \mathcal{T}$ で次の性質を持つものが存在する： $w = z_1 z_2 \cdots z_r$ ($z_i \in \{k, k^{-1}, x, y\}$) に対し $z_i = k, k^{-1}, x, y$ に応じて $z_i' = k, k^{-1}, y, x$ とおくと

$$\tau(w) = z_r' \cdots z_2' z_1'.$$

すなわちでは word の語順を反転し，x と y を入れ換える anti-automorphism である．$\tau^2 = id$ が成立つ．$\tau(\mathcal{T}^{(i)}) = \mathcal{T}^{(-i)}$ であるから，$\mathcal{T}^{(0)}$ は τ-不変である．τ の固定点の全体を $\mathcal{T}^{sym}$ とおく：

$$\mathcal{T}^{sym} = \{ v \in \mathcal{T}^{(0)} \mid \tau(v) = v \}.$$

$\mathcal{T}^{sym}$ は $\mathcal{T}^{(0)}$ の部分空間となる．

$\lambda = (\lambda_0, \lambda_1, \cdots, \lambda_n) \in \Lambda$ は，ある i ($0 \le i \le n$) に対して

$$(-1)^i \lambda_i + (-1)^{i+1} \lambda_{i+1} + \cdots + (-1)^n \lambda_n < 0$$

が成立つとき nil とよぶ．

$$\Lambda^{nil} = \{ \lambda \in \Lambda^{(0)} \mid \lambda \text{ is nil} \},$$

$$\mathcal{T}^{nil} = \sum_{\lambda \in \Lambda^{nil}} \mathbb{C}\, w_\lambda(x, y)$$

とおく．$\mathcal{T}^{nil}$ は subalgebra $\mathcal{T}^{(0)}$ の両側 ideal となる．また $\mathcal{T}^{nil}$ は τ-不変である．

subalgebra $\mathbb{C}[k, k^{-1}]\mathcal{T}^{(0)}$ を考える．$\mathbb{C}[k, k^{-1}]$ の各元は $\mathcal{T}^{(0)}$ の各元と可換であることに注意する．$\mathbb{C}[k, k^{-1}]\mathcal{T}^{sym}$ は $\mathbb{C}[k, k^{-1}]\mathcal{T}^{(0)}$ の部分空間であり，$\mathbb{C}[k, k^{-1}]\mathcal{T}^{nil}$ は $\mathbb{C}[k, k^{-1}]\mathcal{T}^{(0)}$ の両側 ideal である．
次の定理が成立つ

No.
Date

Theorem

(i) $\mathbb{C}[k,k^{-1}]\mathfrak{T}^{(0)} = \mathbb{C}[k,k^{-1}]\mathfrak{T}^{sym} + \mathbb{C}[k,k^{-1}]\mathfrak{T}^{nil}$.

(ii) quotient algebra $\mathbb{C}[k,k^{-1}]\mathfrak{T}^{(0)} / \mathbb{C}[k,k^{-1}]\mathfrak{T}^{nil}$ は可換であり, mod $\mathbb{C}[k,k^{-1}]\mathfrak{T}^{nil}$ による生成系として $\mathbb{C}[k,k^{-1}]$, $y^i x^i$ $(i=1,2,\cdots)$ が選べる.

この定理の (ii) を用いて 次のことが示される.

Theorem V を有限次元既約 $\mathcal{T}$-加群. $V = \bigoplus_{i=0}^{d} U_i$ をその weight space decomposition とする. このとき

$$\dim U_i \leq \binom{d}{i} \qquad (0 \leq i \leq d).$$

特に highest weight space U_0 の次元は 1 である.

$$Irr_d^s(\mathcal{T}) = \begin{array}{l} \mathcal{T} \text{ の有限次元既約表現 } \rho : \mathcal{T} \longrightarrow End(V) \text{ で} \\ \text{type } s, \text{ 直径 } d \text{ をもつものの同型類の全体} \end{array}$$

を決定することが我々の第1の目標であった. $Irr_d^s(\mathcal{T})$ に属する表現 $\rho : V \longrightarrow End(V)$ に対して, 次のようにして数列 $\{\sigma_i(V)\}_{i=0}^{d}$ を定める. U_0 を $\mathcal{T}$-加群 V の highest weight space とすると, 前の定理により $\dim U_0 = 1$ である. また前の Lemma の (iii) より $xU_i \subseteq U_{i+1}$, $yU_i \subseteq U_{i-1}$ であるから, U_0 は $y^i x^i$-不変である. 故に

$$y^i x^i u = \sigma_i u \qquad (u \in U_0)$$

なる $\sigma_i \in \mathbb{C}$ が定まる. このとき $\sigma_0 = 1$, $\sigma_d \neq 0$, $\sigma_i = 0$ $(i \geq d+1)$ が成立つ. 従って $\sigma_i = \sigma_i(V)$ と書けば,

No.
Date

$$\sigma : \mathrm{Irr}_d^S(\mathcal{T}) \longrightarrow \left\{ \{\sigma_i\}_{i=0}^d \;\middle|\; \sigma_i \in \mathbb{C},\ \sigma_0 = 1,\ \sigma_d \neq 0 \right\}$$
$$V \longmapsto \{\sigma_i(V)\}_{i=0}^d$$

なる写像が定まる（ここで $\mathcal{T}$ の表現 $\rho : \mathcal{T} \to End(V)$ と $\mathcal{T}$-加群 V とを同一視している.）この写像 σ が bijection となることが我々の主定理である. σ が injection となることは、可積な商代数 $\mathbb{C}[k,k^{-1}]\mathcal{T}^{(a)} \bmod \mathbb{C}[k,k^{-1}]\mathcal{T}^{nil}$ とその生成系 $\mathbb{C}[k,k^{-1}]$, $y^i x^i$ $(i=1,2,\cdots)$ および grading $\mathbb{C}[k,k^{-1}]\mathcal{T} = \bigoplus_{i\in\mathbb{Z}} \mathbb{C}[k,k]\mathcal{T}^{(i)}$ を用いて示すことが出来、σ が surjection となることは、後述するような具体的な表現の構成によって示すことが出来る. 以下 σ が bijection であることを別の言い方で言い表す.

数列 $\{\sigma_i(V)\}_{i=0}^d$ に対して、天下り的ではあるが Drinfel'd polynomial $P_V(\lambda)$ を対応させる:

$$P_V(\lambda) = \frac{1}{Q} \sum_{i=0}^{d} \sigma_i(V) \prod_{j=i+1}^{d} (q^j - q^{-j})^2 (\varepsilon s^{-2} q^{2(d-j)} + \varepsilon^* s^2 q^{-2(d-j)} - \lambda),$$

where

$$Q = (-1)^d (q-q^{-1})^2 \cdots (q^d - q^{-d})^2.$$

$P_V(\lambda)$ は最高次の係数が 1 である d 次多項式である. q, ε, ε^* は augmented TD-algebra $\mathcal{T} = \mathcal{T}_q^{(\varepsilon,\varepsilon^*)}$ を定義するときに前もって与えられており, d は数列 $\{\sigma_i\}_{i=0}^d$ の長さから定まる. s は $\mathcal{T}$-加群 V の type である. $\sigma_0(V) = 1$ であることが, $P_V(\lambda) = \lambda^d + \cdots$ (monic な d 次多項式) に対応している.

$$\sigma_d(V) = Q \cdot P_V(\varepsilon s^{-2} + \varepsilon^* s^2)$$

であるから, $\sigma_d(V) \neq 0$ と $P_V(\varepsilon s^{-2} + \varepsilon^* s^2) \neq 0$ は同値である.

No.
Date

$$\mathcal{P}_d^s = \left\{ P(\lambda) \in \mathbb{C}[\lambda] \;\middle|\; \begin{array}{l} P(\lambda) \text{ は monic な } d \text{ 次多項式で} \\ P(\varepsilon s^{-2} + \varepsilon^* s^2) \neq 0 \end{array} \right\}$$

とおく. 次の定理は 写像の が bijection であることの言い換えである.

Theorem

$$\begin{array}{ccc} \mathrm{Irr}_d^s(\mathcal{T}) & \longrightarrow & \mathcal{P}_d^s \\ V & \longmapsto & P_V(\lambda) \end{array}$$

なる対応は bijection である. ただし $\mathrm{Irr}_d^s(\mathcal{T})$ を有限次元既約 $\mathcal{T}$-加群で type s, 直径 d をもつものの同型類の全体と同一視している.

我々のもうひとつの目標は

$\mathrm{Irr}_d^{s,t}(\mathcal{T}) = \mathrm{Irr}_d^s(\mathcal{T})$ に属する表現の同型類のうちで
$(C_1)_t$, $(C_2)_t$ をみたすものの全体

を決定することであった. 前々の Proposition により

$$(C_1)_t \iff \pm\varepsilon s^{\pm 1},\ \pm\varepsilon^* s t^{\pm 1} \notin \{q^{-d+1}, q^{-d+2}, \cdots, q^{d-2}, q^{d-1}\}$$

が分かっていた. $(C_2)_t$ について次が成立つ.

Theorem $\pm\varepsilon s^{\pm 1}, \pm\varepsilon^* s t^{\pm 1} \notin \{q^{-d+1}, q^{-d+2}, \cdots, q^{d-2}, q^{d-1}\}$ を仮定する.
このとき, $\mathrm{Irr}_d^s(\mathcal{T})$ に属する $\mathcal{T}$-加群 V に対し, 次が成立する:

V が A_t-加群として既約 $\iff$ $P_V(t^2 + \varepsilon\varepsilon^* t^{-2}) \neq 0$.

ただし A_t は Ξ_t, Ξ_t^* によって生成される $\mathcal{T}$ の subalgebra である.

No.
Date

$$\mathcal{P}_d^{s,t} = \left\{ P(\lambda) \in \mathbb{C}[\lambda] \;\middle|\; \begin{array}{l} P(\lambda) \text{ は monic な } d \text{ 次多項式で} \\ P(\varepsilon s^{-2} + \varepsilon^{-1} s^2) \neq 0,\ P(t^2 + \varepsilon\varepsilon^{-1} t^{-2}) \neq 0 \end{array} \right\}$$

とおくと、上の定理は次のように言い直すことが出来る。

Theorem $\pm\varepsilon s t,\ \pm\varepsilon^{-1} s t^{-1} \notin \{ q^{-d+1}, q^{-d+2}, \cdots, q^{d-2}, q^{d-1} \}$ を仮定する。
このとき

$$\begin{array}{ccc} \mathrm{Irr}_d^{s,t}(\mathcal{T}) & \longrightarrow & \mathcal{P}_d^{s,t} \\ V & \longmapsto & P_V(\lambda) \end{array}$$

なる対応は bijection である。

5 $\mathcal{T} = \mathcal{T}_q^{(\varepsilon,\varepsilon^{-1})}$ を augmented TD-algebra とする。$\mathcal{T}$ の有限次元既約表現を affine 量子群 $U_q(\hat{\mathfrak{sl}}_2)$ の表現を介して具体的に構成する。

affine 量子群 $U_q(\hat{\mathfrak{sl}}_2)$ は 生成元 $e_0^{\pm}, e_1^{\pm}, k_0^{\pm 1}, k_1^{\pm 1}$ と関係式

$$\begin{array}{l} k_0 k_1 = k_1 k_0, \quad k_i k_i^{-1} = k_i^{-1} k_i = 1 \\ k_i e_i^{\pm} k_i^{-1} = q^{\pm 2} e_i^{\pm}, \quad k_i e_j^{\pm} k_i^{-1} = q^{\mp 2} e_j^{\pm} \quad (i \neq j) \\ [e_i^+, e_i^-] = \dfrac{k_i - k_i^{-1}}{q - q^{-1}}, \quad [e_i^+, e_j^-] = 0 \quad (i \neq j) \\ [e_i^{\pm}, (e_i^{\pm})^2 e_j^{\pm} - (q^2 + q^{-2}) e_i^{\pm} e_j^{\pm} e_i^{\pm} + e_j^{\pm} (e_i^{\pm})^2] = 0 \quad (i \neq j) \end{array}$$

によって定義される algebra (単位元1を持つ $\mathbb{C}$ 上の associative algebra) である。
関係式 $k_0 k_1 = 1$ を加えたものを $U_q(\hat{\mathfrak{sl}}_2)$-loop algebra と呼ぶ。
本稿では $\mathcal{L}$ という記号で表す:

$$\mathcal{L} \cong U_q(\hat{\mathfrak{sl}}_2) / (k_0 k_1 - 1)$$

No.
Date

$s \in \mathbb{C}-\{0\}$ に対して $\mathcal{Z}$ の元 $x(s)$, $y(s)$ を次のように定める

$$x(s) = \alpha\,(s e_0^+ + \varepsilon s^{-1} e_1^- k_1)$$
$$y(s) = \varepsilon^* s e_0^- k_0 + s^{-1} e_1^+$$

ただし $\alpha = -q^{-1}(q-q^{-1})^2$ である. 次の命題により $\mathcal{T}$ は $\mathcal{Z}$ に埋込まれる.

Proposition　$\mathcal{T}$ から $\mathcal{Z}$ への algebra として homomorphism

$$\varphi_s : \mathcal{T} \longrightarrow \mathcal{Z} \quad (x, y, k \longmapsto x(s), y(s), sk_0 \text{ respectively})$$

が存在する. 更にこの φ_s は injection である.

この命題の埋込み φ_s を通して $\mathcal{Z}$ の表現から $\mathcal{T}$ の表現が得られる.
ここで $\mathcal{Z}$ の有限次元既約表現について先事をものと準約しておく
($\mathcal{Z}$ の有限次元既約表現と $U_q(\hat{\mathfrak{sl}}_2)$ の有限次元既約表現は 1:4 に対応する).

evaluation module と呼ばれる既約 $\mathcal{Z}$-加群 $V(l,a)$ を次のように構成する. $a \in \mathbb{C}-\{0\}$ を選ぶ. a は evaluation parameter と呼ばれる.
$V(l,a)$ を $\mathbb{C}$ 上 $l+1$ 次元の線形空間とし, 基底 $v_0, v_1, \cdots, v_l$ を固定し,
$\mathcal{Z}$ の作用を次のように定める.

$$V(l,a) = \langle v_0, v_1, \cdots, v_l \rangle$$

$$\begin{cases} k_0 v_i = q^{2i-l} v_i, \quad k_1 v_i = q^{l-2i} v_i \\ e_0^+ v_i = a q^{[i+1]} v_{i+1}, \quad e_1^+ v_i = [l-i+1]\, v_{i-1} \\ e_0^- v_i = a^{-1} q^{-1} [l-i+1]\, v_{i-1}, \quad e_1^- v_i = [i+1]\, v_{i+1} \end{cases}$$

ただし $v_{-1} = v_{l+1} = 0$, $[n] = \dfrac{q^n - q^{-n}}{q - q^{-1}}$ である. 実際この作用は well-defined であり. $V(l,a)$ は既約な $\mathcal{Z}$-加群となる. 自明な場合を除くために $l \geq 1$ を仮定する.

No.
Date

evaluation module $V(l,a)$ に数列 $aq^{-l+1}, aq^{-l+3}, \cdots, aq^{l-3}, aq^{l-1}$ を対応させる. この数列を $S(l,a)$ と記し, q-string と呼ぶ:

$$S(l,a) = \{ aq^{2i-l+1} \mid 0 \le i \le l-1 \}.$$

$\mathcal{L}$ は coproduct $\Delta : \mathcal{L} \longrightarrow \mathcal{L} \otimes \mathcal{L}$

$$\Delta(k_i^{\pm 1}) = k_i^{\pm} \otimes k_i^{\pm}$$
$$\Delta(e_i^{+}) = k_i \otimes e_i^{+} + e_i^{+} \otimes 1$$
$$\Delta(e_i^{-}) = 1 \otimes e_i^{-} + e_i^{-} \otimes k_i^{-1}$$

を持つので $\mathcal{L}$-加群どうしの tensor 積は $\mathcal{L}$-加群となる. 特に evaluation modules の tensor 積

$$V = V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n)$$

は $\mathcal{L}$-加群となる. この $\mathcal{L}$-加群 $V = V(l_1,a_1) \otimes \cdots \otimes V(l_n,a_n)$ に q-string の集合 $\{ S(l_i, a_i) \}_{i=1}^{n}$ (正確にいうと multi-set) を対応させる.

2つの q-string $S(l,a)$, $S(l',a')$ は次の条件をみたすとき **一般の位置** にあるという.

(i) $S(l,a) \cup S(l',a')$ は q-string でない
or
(ii) $S(l,a) \subseteq S(l',a')$ または $S(l,a) \supseteq S(l',a')$.

q-string の集合 $\{ S(l_i, a_i) \}_{i=1}^{n}$ は任意の i, j $(i \neq j)$ に対して $S(l_i, a_i)$ と $S(l_j, a_j)$ が一般の位置にあるとき, $\{ S(l_i, a_i) \}_{i=1}^{n}$ を一般の位置にあるという.

No.
Date

evaluation modules の Tensor 積 $V = V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n)$, $V' = V(l_1', a_1') \otimes \cdots \otimes (l_m', a_m')$ について 次が成立する.

(i) V は $\mathcal{Z}$-加群として既約である

$\Leftrightarrow$

$\{S(l_i, a_i)\}_{i=1}^{n}$ は一般の位置にある.

(ii) V, V' がともに $\mathcal{Z}$-加群として既約とすると

$V \simeq V'$ ($\mathcal{Z}$-加群として同型)

$\Leftrightarrow$

$n = m$ かつ $(l_1', a_1'), \cdots, (l_m', a_m')$ を適当に並べかえると

$(l_i, a_i) = (l_i', a_i')$ $(1 \le i \le n)$.

表現 $\rho : \mathcal{Z} \longrightarrow End(V)$ と ρ を通した $\mathcal{Z}$-加群 V に対して, 埋込 $\varphi_s : \mathcal{T} \longrightarrow \mathcal{Z}$ により $\mathcal{T}$ の表現 $\rho \circ \varphi_s : \mathcal{T} \longrightarrow End(V)$ と $\rho \circ \varphi_s$ を通した $\mathcal{T}$-加群 V が定まる. これを $\mathcal{T}$-加群 V via φ_s と呼ぶ. $(\varepsilon, \varepsilon^*) = (1,1), (0,0)$ のときは. 適当な既約 $\mathcal{Z}$-加群 $V = V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n)$ と $s \in \mathbb{C} - \{0\}$ を選ぶと $\mathcal{T}$-加群 V via φ_s としてすべての有限次元既約 $\mathcal{T}$-加群が尽くされる. $(\varepsilon, \varepsilon^*) = (1,0)$ のときも基本的に同様のことが成立するが若干の修正を必要とする. これらのことを以下に詳述する.

Case $(\varepsilon, \varepsilon^*) = (0,0)$

$(\varepsilon, \varepsilon^*) = (0,0)$ のときは. φ_s による $\mathcal{T}$ の像が $\mathcal{Z}$ の Borel subalgebra $\mathcal{B} = \langle e_0^+, e_1^+, k_0^{\pm 1} \rangle$ に一致することに注意する. $\mathcal{T}$ と $\mathcal{B}$ は同型だから, $\mathcal{T}$ の有限次元既約表現はすでに決定されている.

No.
Date

Theorem $(\varepsilon,\varepsilon^*)=(0,0)$ とする. $\mathcal{T}=\mathcal{T}_q^{(\varepsilon,\varepsilon^*)}$ の有限次元既約表現は次の (i), (ii), (iii) により決まる.

(i) evaluation modules の tensor 積 $V=V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$ について次が成立する.

$\mathcal{T}$-加群 V via φ_s は既約である

$\Leftrightarrow$

q-string の集合 $\{S(l_i,a_i)\}_{i=1}^n$ は一般の位置にある.

このとき既約 $\mathcal{T}$-加群 V via φ_s の type は s であり, 直径は $d=l_1+\cdots+l_n$ である.

(ii) evaluation modules の tensor 積 $V=V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$, $V'=V(l_1',a_1')\otimes\cdots\otimes V(l_m',a_m')$ について, V via φ_s, V' via $\varphi_{s'}$ がともに $\mathcal{T}$-加群として既約と仮定する. このとき次が成立する.

V via $\varphi_s \simeq V'$ via $\varphi_{s'}$ ($\mathcal{T}$-加群として同型)

$\Leftrightarrow$

$s=s'$, $n=m$ かつ $(l_1',a_1'),\cdots,(l_m',a_m')$ を適当に並べかえると $(l_i,a_i)=(l_i',a_i')$ $(1\le i\le n)$.

(iii) $\mathrm{Irr}_d^s(\mathcal{T})$ に属する任意の $\mathcal{T}$-加群 V に対し, evaluation modules $V(l_i,a_i)$ $(1\le i\le n)$ が存在して

$V\simeq V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$ via φ_s ($\mathcal{T}$-加群として同型)

ただし $d\ge 1$ とする.

No.
Date

Case $(\varepsilon,\varepsilon^*)=(1,1)$

q-string の集合 $\{S(l_i,a_i)\}_{i=1}^n$, $\{S(l_i',a_i')\}_{i=1}^m$ が 次の条件 を みたすとき 同値 という

$n=m$ かつ $(l_1',a_1'),\cdots,(l_m',a_m')$ を 適当に 並べかえると
$\varepsilon_i\in\{1,-1\}$ $(1\le i\le n)$ が 存在して $(l_i,a_i^{\varepsilon_i})=(l_i',a_i')$ $(1\le i\le n)$.

Theorem $(\varepsilon,\varepsilon^*)=(1,1)$ とする. $\mathcal{T}=\mathcal{T}_q^{(\varepsilon,\varepsilon^*)}$ の有限次既約表現は 次の (i), (ii), (iii) によって 尽くす.

(i) evaluation modules の tensor積 $V=V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$ について 次が 成立する.

$\mathcal{T}$-加群 V via φ_s は 既約 である
$\Leftrightarrow$ $-s^2,-s^{-2}\notin S(l_i,a_i)$ $(1\le i\le n)$ かつ
任意の $\varepsilon_i\in\{1,-1\}$ $(1\le i\le n)$ に対して, q-string の集合 $\{S(l_i,a_i^{\varepsilon_i})\}_{i=1}^n$ は 一般の位置にある.

このとき 既約 $\mathcal{T}$-加群 V via φ_s の type は s であり, 直径は $d=l_1+\cdots+l_n$ である.

(ii) evaluation modules の tensor積 $V=V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$, $V'=V(l_1',a_1')\otimes\cdots\otimes V(l_m',a_m')$ について, V via φ_s, V' via $\varphi_{s'}$ が ともに $\mathcal{T}$-加群として 既約と仮定する. このとき 次が 成立する.

V via φ_s $\simeq$ V' via $\varphi_{s'}$ ($\mathcal{T}$-加群として同型)
$\Leftrightarrow$
$s=s'$ かつ q-string の集合 $\{S(l_i,a_i)\}_{i=1}^n$, $\{S(l_i',a_i')\}_{i=1}^m$ は 同値.

No.
Date

(iii) $\mathrm{Irr}_d^S(\mathcal{T})$ に属する任意の $\mathcal{T}$-加群 V に対して (ただし $d \geq 1$),
evaluation modules $V(l_i, a_i)$ $(1 \leq i \leq n)$ が存在して

$$V \simeq V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n) \text{ via } \varphi_s \quad (\mathcal{T}\text{-加群として同型})$$

Case $(\varepsilon, \varepsilon^*) = (1, 0)$

$(\varepsilon, \varepsilon^*) = (1, 0)$ の場合は

$$x(s) = \alpha(s e_0^+ + s^{-1} e_1^- k_1)$$
$$y(s) = s^{-1} e_1^+$$

であるから. 埋込 φ_s による $\mathcal{T}$ の像は, e_0^+, e_1^+, e_1^-, $k_1^{\pm 1}$ で生成される $\mathcal{Z}$ の subalgebra に含まれる. e_0^+, $e_1^\pm$, $k_1^{\pm 1}$ で生成される $\mathcal{Z}$ の subalgebra を $\mathcal{Z}'$ とおく (e_0^- が生成系から欠けている):

$$\mathcal{Z}' = \langle e_0^+, e_1^\pm, k_1^{\pm 1} \rangle.$$

$\mathcal{Z}'$ の表現 $\rho : \mathcal{Z}' \longrightarrow \mathrm{End}(V)$ と ρ を通した $\mathcal{Z}$-加群 V に対して.
埋込 $\varphi_s : \mathcal{T} \longrightarrow \mathcal{Z}'$ により $\mathcal{T}$ の表現 $\rho \circ \varphi_s : \mathcal{T} \longrightarrow \mathrm{End}(V)$ と
$\rho \circ \varphi_s$ を通した $\mathcal{T}$-加群 V が定まる. これと $\mathcal{T}$-加群 V via φ_s と呼ぶ.
$\mathcal{Z}$ の evaluation module $V(l, a)$ $(l \geq 1,\ a \in \mathbb{C} - \{0\})$ は, $\mathcal{Z}'$-加群
としても既約である. $\mathcal{Z}'$ の生成系から e_0^- が欠けているので,
$a = 0$ のときも evaluation module $V(l, 0)$ $(l \geq 0)$ は $\mathcal{Z}'$-加群
として well-defined であり, 既約な $\mathcal{Z}'$-加群となる:

$$V(l, 0) = \langle v_0, v_1, \cdots, v_l \rangle \quad \begin{cases} e_0^+ v_i = 0 \\ e_1^+ v_i = [l - i + 1]\, v_{i-1} \\ e_1^- v_i = [i + 1]\, v_{i+1} \\ k_1 v_i = q^{l-2i} v_i . \end{cases}$$

No.
Date

$V(l)=V(l,0)$ なる記法を用いる ($l\geq 0$ とする). $l=0$ の場合. $V(0)$ は自明な $\mathcal{L}'$-加群である. $V(l)$ を evaluation module と呼ぶ. $V(l,a)$ と書いたら $l\geq 1$, $a\in\mathbb{C}-\{0\}$ なる evaluation module を意味することとする.

$\mathcal{L}$ の coproduct $\Delta:\mathcal{L}\longrightarrow\mathcal{L}\otimes\mathcal{L}$ は. $\Delta(\mathcal{L}')\subseteq\mathcal{L}'\otimes\mathcal{L}'$ を みたすので. $\mathcal{L}'$-加群どうしの tensor 積は $\mathcal{L}'$-加群となる. 特に evaluation modules の tensor 積

$$V=V(l)\otimes V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$$

は $\mathcal{L}'$-加群となる.

<u>Theorem</u> $(\varepsilon,\varepsilon^*)=(1,0)$ とする. $\mathcal{J}=\mathcal{J}_q^{(\varepsilon,\varepsilon^*)}$ の有限次元既約表現は次の (i), (ii), (iii) によって与る.

(i) evaluation modules の tensor 積 $V=V(l)\otimes V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$ について次が成立する.

$\mathcal{J}$-加群 V via φ_s は既約である
$\Leftrightarrow$ $-s^{-2}\notin S(l_i,a_i)$ $(1\leq i\leq n)$ かつ
q-string の集合 $\{S(l_i,a_i)\}_{i=1}^{n}$ は一般の位置にある.

このとき既約 $\mathcal{J}$-加群 V via φ_s の type は s である. 直径は $d=l+l_1+\cdots+l_n$ である. ($n=0$ も許す. $n=0$ の場合 $V=V(l)$.)

(ii) evaluation modules の tensor 積 $V=V(l)\otimes V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$, $V'=V(l')\otimes V(l_1',a_1')\otimes\cdots\otimes V(l_m',a_m')$ について. V via φ_s, V' via $\varphi_{s'}$ がともに $\mathcal{J}$-加群として既約と仮定する. このとき次が成立する.

No.
Date

V via $\varphi_s \simeq V'$ via $\varphi_{s'}$ (T-加群として同型)

$\Leftrightarrow$

$s = s'$, $\ell = \ell'$, $n = m$ かつ $(l_1, a_1), \cdots, (l_m, a_m)$ と適当に並べかえると

$(l_i, a_i) = (l_i', a_i')$ $(1 \le i \le n)$.

(iii) $\mathrm{Irr}_a^s(T)$ に属する任意の T-加群 V に対して, evaluation modules $V(l)$, $V(l_i, a_i)$ $(1 \le i \le n)$ が存在して

$V \simeq V(l) \otimes V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n)$ via φ_s (T-加群として同型)

ただし $n = 0$ を許す.

これら三つの定理の (iii) の部分は, $\mathrm{Irr}_a^s(T)$ に属する任意の T-加群は埋込 φ_s を通して evaluation modules の tensor 積として表わされることを主張している. この部分の主張の証明は, Drinfeld polynomial $P_V(u)$ に関する以下の考察に基いている.

evaluation modules の tensor 積を

$V = V(a_1, l_1) \otimes \cdots \otimes V(a_n, l_n)$

とおく. ただし $(\varepsilon, \varepsilon^*) = (1,1), (0,0)$ の場合は, $a_i \in \mathbb{C} - \{0\}$ $(1 \le i \le n)$ であり, $(\varepsilon, \varepsilon^*) = (1,0)$ の場合は $a_i = 0$ を許すから $a_i \in \mathbb{C}$ $(1 \le i \le n)$ である. また自明な evaluation module を除くために $l_i \ge 1$ $(1 \le i \le n)$ と仮定する. T-加群 V via φ_s の既約性は仮定しない. $V(l_j, a_j)$ の標準的基底を $v_0, v_1, \cdots, v_{l_j}$ とする (v_i は $v_i^{(j)}$ と書くべきだが $v_i = v_i^{(j)}$ と略記する). 従って

No.
Date

$V(l_i, a_j) = \langle v_0, v_1, \cdots, v_{l_j} \rangle$ $\quad \begin{cases} k\, v_i = q^{2i-l_j} v_i \\ x(s) v_i \in \langle v_{i+1} \rangle \\ y(s) v_i \in \langle v_{i-1} \rangle \end{cases}$

である.

$$U_i = \sum_{i_1+i_2+\cdots+i_n=i} \mathbb{C}\, v_{i_1} \otimes v_{i_2} \otimes \cdots \otimes v_{i_n}$$

とおくと

$$V = \bigoplus_{i=0}^{d} U_i \qquad (d = l_1 + l_2 + \cdots + l_n)$$

であり, $\mathcal{T}$-加群 V via φ_s において

$$k\, u = s q^{2i-d} \qquad (u \in U_i)$$
$$x\, U_i \subseteq U_{i+1}$$
$$y\, U_i \subseteq U_{i-1}$$

が成立つ ($U_{-1} = U_{d+1} = 0$ とする). $\dim U_0 = 1$ であるから.

$$y^i x^i\, u = \sigma_i\, u \qquad (u \in U_0)$$

なる $\sigma_i \in \mathbb{C}$ が定まる. $\sigma_0 = 1$, $\sigma_i = 0$ ($i \geq d+1$) であるが, V の既約性は仮定しなかったから, $\sigma_d \neq 0$ とは限らない. 前と同じように $\mathcal{T}$-加群 V via φ_s の Drinfeld polynomial $P_V(\lambda)$ を

$$P_V(\lambda) = \frac{1}{Q} \sum_{i=0}^{d} \sigma_i \prod_{j=i+1}^{d} (q^j - q^{-j})^2 (\varepsilon^* s^2 q^{2(d-j)} + \varepsilon^* s^{-2} q^{-2(d-j)} - \lambda),$$

where $Q = (-1)^d (q - q^{-1})^2 \cdots (q^d - q^{-d})^2$

で定義する. $\sigma_0 = 1$ なので $P_V(\lambda)$ は monic な d 次多項式である.

No.
Date

($s \in \mathbb{C}-\{0\}$ を任意に固定する.)

Theorem V, V' をそれぞれ evaluation modules の tensor 積とする. $P_V(\lambda)$, $P_{V'}(\lambda)$ を $\mathcal{T}$-module V via φ_s, V' via φ_s の Drinfel'd polynomial とする. $V \otimes V'$ を evaluation modules の tensor 積とするとき, $P_{V\otimes V'}(\lambda)$ を $\mathcal{T}$-module $V\otimes V'$ via φ_s の Drinfel'd polynomial とするとき 次の積公式が成立つ:

$$P_{V\otimes V'}(\lambda) = P_V(\lambda) P_{V'}(\lambda).$$

Corollary evaluation modules の tensor 積 $V = V(l_1,a_1)\otimes \cdots \otimes V(l_n,a_n)$ と $s \in \mathbb{C}-\{0\}$ に対し, $P_V(\lambda)$, $P_{V(l_i,a_i)}(\lambda)$ を $\mathcal{T}$-module V via φ_s, $V(l_i,a_i)$ via φ_s の Drinfel'd polynomial とする. このとき 次が成立つ.

(i) $$P_V(\lambda) = \prod_{i=1}^{n} P_{V(l_i,a_i)}(\lambda),$$

(ii) $$P_{V(l_i,a_i)}(\lambda) = \prod_{a\in S(l_i,a_i)} (\lambda + a + \varepsilon\varepsilon^* a^{-1})$$

ただし $S(l_i,a_i) = \{ a_i q^{2j-l_i+1} \mid 0 \le j \le l_i-1 \}$ であり.

$a_i = 0$ のときは, $S(l_i,0) = \{0,\cdots,0\}$ (0 が l_i 個重複する multi-set) とし, $P_{V(l_i,0)}(\lambda) = \lambda^{l_i}$ とする.

(iii) $S = \bigcup_{i=1}^{n} S(l_i,a_i)$ とおく.

$$P_V(\varepsilon s^{-2} + \varepsilon^* s^2) \neq 0 \iff \begin{cases} -s^2, -s^{-2} \notin S & \text{if } (\varepsilon,\varepsilon^*) = (1,1) \\ -s^{-2} \notin S & \text{if } (\varepsilon,\varepsilon^*) = (1,0) \\ s \in \mathbb{C}-\{0\} & \text{if } (\varepsilon,\varepsilon^*) = (0,0), \text{ i.e., always ok.} \end{cases}$$

$$P_V(t^2 + \varepsilon\varepsilon^* t^{-2}) \neq 0 \iff \begin{cases} -t^2, -t^{-2} \notin S & \text{if } (\varepsilon,\varepsilon^*) = (1,1) \\ -t^2 \notin S & \text{if } (\varepsilon,\varepsilon^*) = (1,0), (0,0) \end{cases}$$

No.
Date

少し前にもどる. evaluation modules の tensor 積 $V=V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$ に対し、理込 $\mathcal{G}_s$ によって V を $\mathcal{T}$-加群とみなすと k の V 上への作用は対角化可能で、k の固有空間への分解 $V=\bigoplus_{i=0}^{d}U_i$ (k の U_i 上の固有値は sq^{2i-d}) は

$$U_i=\sum_{i_1+i_2+\cdots+i_n=i}\mathbb{C}\,v_{i_1}\otimes v_{i_2}\otimes\cdots\otimes v_{i_n}$$

でよこられた. 従って $\dim U_i$ の母函数は次のようになる.

$$\sum_{i=0}^{\infty}(\dim U_i)\lambda^i=\prod_{i=1}^{n}(1+\lambda+\lambda^2+\cdots+\lambda^{l_i}).$$

この V が既約 $\mathcal{T}$-加群であり (そのための条件を述べたのが前出の定理である), $t\in\mathbb{C}-\{0\}$ が

$$\pm\varepsilon^s t,\ \pm\varepsilon^s t^{-1}\notin\{q^{-d+1},q^{-d+2},\cdots,q^{d-2},q^{d-1}\}$$

かつ $P_V(t^2+\varepsilon\varepsilon^* t^{-2})\neq 0$ をみたすとき (すなわち $(C_1)_t,(C_2)_t$ が成立つとき,

$$A=z_t|_V,\quad A^*=z_t^*|_V$$

は TD-pair となるのであった. 更にこの構成法は type I の標準化された TD-pair を尽すのである (前出の三つの定理の (iii) の部分による). $\mathcal{T}$-加群 V から TD-pair $A=z_t|_V$, $A^*=z_t^*|_V$ が生じる場合は, weight space decomposition $V=\bigoplus_{i=0}^{d}U_i$ は, A,A^* の split decomposition と一致する. また TD-pair A,A^* は affine 変換をほどこしても split decomposition は不変である. 従って次の定理を得る.

<u>Theorem</u> $q\neq$ root of unity とする. type I の TD-pair A,A^* の split decomposition を $V=\bigoplus_{i=0}^{d}U_i$ とすれば

$$\sum_{i=0}^{\infty}(\dim U_i)\lambda^i=\prod_{i=1}^{n}(1+\lambda+\lambda^2+\cdots+\lambda^{l_i})\quad \text{for some } l_i\geq 1,\ (1\leq i\leq n)$$

No.
Date

6 $A = A_q^{(\varepsilon,\varepsilon^*)}$ を TD-algebra とする.

$Irr'(A)$ = A の有限次元既約表現 $\rho : A \longrightarrow End(V)$ で
$\rho(z)$, $\rho(z^*)$ が対角化可能なものの同型類の全体

$TD_b^{(\varepsilon,\varepsilon^*)}$ = 標準化された TD-pair A, A^* で固有値が
$\theta_i = b q^{2i-d} + \varepsilon b^{-1} q^{d-2i}$, $\theta_i^* = \varepsilon^* b^* q^{2i-d} + b^{*-1} q^{d-2i}$ $(0 \le i \le d)$
for some $b, b^* \in \mathbb{C} - \{0\}$, $d \in \mathbb{N}$
の形をしているものの同型類の全体

の間には $A = \rho(z)$, $A^* = \rho(z^*)$ により bijective な対応があった.
これまでの結果をふまえて. $Irr'(A)$ の各同型類の代表を具体的に構成する.

$s, t \in \mathbb{C} - \{0\}$ に対して

$\iota_t : A \longrightarrow \mathcal{T} = \mathcal{T}_q^{(\varepsilon,\varepsilon^*)}$ $(z, z^* \longmapsto z_t, z_t^*$ respectively$)$

$\varphi_s : \mathcal{T} \longrightarrow \mathcal{L}$ $(x, y, k \longmapsto x(s), y(s), sk_0$ respectively$)$

は injective な algebra homomorphism であった.

$\varphi_{s,t} = \varphi_s \circ \iota_t : A \longrightarrow \mathcal{L}$

は injective な algebra homomorphism であり, $z_t(s) = \varphi_{s,t}(z)$, $z_t^*(s) = \varphi_{s,t}(z^*)$
とおくと

$z_t(s) = x(s) + st\,k_0 + \varepsilon s^{-1} t^{-1} k_1$
$z_t^*(s) = y(s) + \varepsilon^* s t^{-1} k_0 + s^{-1} t\, k_1$

である.

No.
Date

$(\varepsilon,\varepsilon^*)=(1,0)$ のときは $\varphi_{s,t}$ の像は $\mathcal{L}'=\langle e_i^+, e_i^+, e_i^-, k_i^{\pm 1}\rangle$ に含まれることに注意する. $(\varepsilon,\varepsilon^*)=(1,1),(0,0)$ のときは, $\mathcal{L}$-加群 V は準同型 $\varphi_{s,t}$ を通して $\mathcal{A}$-加群となる. この $\mathcal{A}$-加群を V via $\varphi_{s,t}$ とよぶ. $(\varepsilon,\varepsilon^*)=(1,0)$ のときに, $\mathcal{L}'$-加群 V が準同型 $\varphi_{s,t}$ を通して $\mathcal{A}$-加群となる. この $\mathcal{A}$-加群を V via $\varphi_{s,t}$ とよぶ. V 上 z, z^* は $z_q(s), z_q^*(s)$ として作用

Theorem $(\varepsilon,\varepsilon^*)=(1,1)$ とする.

(i) $\mathcal{L}$ の evaluation modules の tensor 積 $V=V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$ について次が成立する. $d=l_1+\cdots+l_n$ とおく.

V via $\varphi_{s,t}$ が $\mathrm{Irr}'(\mathcal{A})$ に属する

$\Leftrightarrow \pm st, \pm st^{-1} \notin \{q^{-d+1}, q^{-d+2}, \cdots, q^{d-2}, q^{d-1}\}$

$-s^2, -s^{-2}, -t^2, -t^{-2} \notin S(l_i,a_i)$ $(1\le i\le n)$

かつ 任意の $\varepsilon_i\in\{1,-1\}$ $(1\le i\le n)$ に対して

$\{S(l_i,a_i^{\varepsilon_i})\}_{i=1}^n$ は一般の位置にある.

(ii) $\mathcal{L}$ の evaluation modules の tensor 積 $V=V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$, $V'=V(l_1',a_1')\otimes\cdots\otimes V(l_m',a_m')$ について. V via $\varphi_{s,t}$, V' via $\varphi_{s',t'}$ がともに $\mathrm{Irr}'(\mathcal{A})$ に属するとき, 次が成立する

V via $\varphi_{s,t} \simeq V'$ via $\varphi_{s',t'}$ ($\mathcal{A}$-加群として同型)

$\Leftrightarrow (s,t)=\pm(s',t')$ かつ q-string の集合 $\{S(l_i,a_i)\}_{i=1}^n$, $\{S(l_i',a_i')\}_{i=1}^m$ は同値

(iii) $\mathrm{Irr}'(\mathcal{A})$ に属する任意の $\mathcal{A}$-加群 V に対して (ただし $\dim V\ge 2$ とする), $\mathcal{L}$ の evaluation modules $V(l_i,a_i)$ $(1\le i\le n)$ と $s,t\in\mathbb{C}-\{0\}$ が存在して

$V\simeq V(l_1,a_1)\otimes\cdots\otimes V(l_n,a_n)$ via $\varphi_{s,t}$ ($\mathcal{A}$-加群として同型)

No.
Date

Theorem $(\varepsilon, \varepsilon^*) = (1, 0)$ とする.

(i) $\mathcal{L}'$ の evaluation modules の tensor 積 $V = V(l) \otimes V(l_1, s_1) \otimes \cdots \otimes V(l_n, a_n)$ について次が成立する. ただし $n=0$ を許し, $n=0$ のときは $V = V(l)$ とする. ($l=0$ を許し, $l=0$ のときは $V = V(l_1, s_1) \otimes \cdots \otimes V(l_n, a_n)$ とする.)

V via $\varphi_{s,t}$ が $Irr'(\mathcal{A})$ に属する

$\Leftrightarrow$ $\pm st \notin \{q^{-d+1}, q^{-d+2}, \cdots, q^{d-2}, q^{d-1}\}$ $(d = l + l_1 + \cdots + l_n)$

$-s^{-2}, -t^2 \notin S(l_i, a_i)$ $(1 \le i \le n)$

かつ $\{S(l_i, a_i)\}_{i=1}^n$ は一般の位置にある

(ii) $\mathcal{L}'$ の evaluation modules の tensor 積 $V = V(l) \otimes V(l_1, s_1) \otimes \cdots \otimes V(l_n, a_n)$, $V' = V(l') \otimes V(l_1', s_1') \otimes \cdots \otimes V(l_m', a_m')$ について, V via $\varphi_{s,t}$, V' via $\varphi_{s',t'}$ がともに $Irr'(\mathcal{A})$ に属するとき, 次が成立する.

V via $\varphi_{s,t} \simeq V'$ via $\varphi_{s',t'}$ ($\mathcal{A}$-加群として同型)

$\Leftrightarrow$ $(s,t) = \pm(s',t')$, $n = m$ かつ $(l_1', a_1'), \cdots, (l_m', a_m')$ を適当に並べかえると $(l_i, a_i) = (l_i', a_i')$ $(1 \le i \le n)$.

(iii) $Irr'(\mathcal{A})$ に属する任意の $\mathcal{A}$-加群 V に対して, $\mathcal{L}'$ の evaluation modules $V(l)$, $V(l_i, a_i)$ $(1 \le i \le n)$ と $s, t \in \mathbb{C}^\times$ が存在して

$V \simeq V(l) \otimes V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n)$ via $\varphi_{s,t}$ ($\mathcal{A}$-加群として同型)

ただし $n=0$ を許す.

No.
Date

Theorem $(\varepsilon, \varepsilon^*) = (0,0)$ とする.

(i) 次の evaluation modules の tensor 積 $V = V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n)$ について次が成立する.

V via $\varphi_{s,t}$ が $Irr'(A)$ に属する
$\Leftrightarrow$ $-t^2 \notin S(l_i, a_i)$ $(1 \le i \le n)$
かつ $\{S(l_i, a_i)\}_{i=1}^n$ は一般の位置にある

(ii) 次の evaluation modules の tensor 積 $V = V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n)$, $V' = V(l_1', a_1') \otimes \cdots \otimes V(l_m', a_m')$ について, V via $\varphi_{s,t}$, V' via $\varphi_{s',t'}$ が ともに $Irr'(A)$ に属するなら, 次が成立する.

V via $\varphi_{s,t} \simeq V'$ via $\varphi_{s',t'}$ (A-加群として同型)
$\Leftrightarrow$ $(s,t) = \pm(s',t')$, $n = m$ かつ $(l_1', a_1'), \cdots, (l_m', a_m')$ を適当に並べかえると $(l_i, a_i) = (l_i', a_i')$ $(1 \le i \le n)$.

(iii) $Irr'(A)$ に属する任意の A-加群 V に対して, 次の evaluation modules $V(l_i, a_i)$ $(1 \le i \le n)$ と $s, t \in \mathbb{C} - \{0\}$ が存在して

$V \simeq V(l_1, a_1) \otimes \cdots \otimes V(l_n, a_n)$ via $\varphi_{s,t}$ (A-加群として同型).

ただし $\dim V \ge 2$ (すなわち A-加群 V は自明でない) とする.

$(\varepsilon, \varepsilon^*) = (1,1)$ のときは, A は q-Onsager algebra であり, $Irr'(A)$ は A の有限次元既約表現の同型類の全体となることに注意する.
また $(\varepsilon, \varepsilon^*) = (0,0)$ のときは, A は affine 量子群 $U_q(\hat{\mathfrak{sl}}_2)$ の positive part と同型である.

$Irr'(A)$ に属する A-加群 V で $V \simeq V(l, a)$ via $\varphi_{s,t}$ から生じる TD-pair $A = E_0(\delta)|_V$, $A^* = E_0^*(\delta)|_V$ が Leonard pair であるもの
($(\varepsilon, \varepsilon^*) = (1,0)$ のときは, $a = 0$ となる)

No.
Date

参考文献

P- and Q-polynomial association scheme について

E. Bannai and T. Ito, Algebraic Combinatorics I : Association Schemes, Benjamin/Cummings, London, 1984 の第3章.

Terwilliger algebra について

P. Terwilliger, The subconstituent algebra of an association scheme I, J. Algebraic Combin., 1 (1992) 363-388.

TD-pair について

T. Ito, K. Tanabe and P. Terwilliger, Some algebra related to P- and Q-polynomial association schemes, in 'Codes and Association Schemes (Piscataway NJ, 1999)', Amer. Math. Soc., Providence RI, 2001, 167-192

TD-algebra, augmented TD-algebra について

$(\ell, \ell^*) = (0, 0)$ の場合

T. Ito and P. Terwilliger, The shape of a tridiagonal pair, J. Pure Appl. Algebra 188 (2004) 145-160.

T. Ito and P. Terwilliger, Two non-nilpotent linear transformations that satisfy the cubic q-Serre relations, J. Algebra Appl 6 (2007) 477-503.

一般の (ℓ, ℓ^*) の場合

T. Ito and P. Terwilliger, The augmented tridiagonal algebra, in preparation.

Tridiagonal pairs of q-Racah type

Tatsuro Ito

Kanazawa University

Paul Terwilliger

University of Wisconsin
JSPS fellow 07/08

Overview

This talk concerns the **tridiagonal pairs** of linear transformations.

These pairs come in a number of **types** depending on the form of the eigenvalues.

The most general type is called **q-Racah**.

We classify up to isomorphism the tridiagonal pairs of q-Racah type.

Our proof uses the representation theory of the **quantum affine algebra** $U_q(\widehat{\mathfrak{sl}}_2)$.

Tridiagonal pairs

We now define a tridiagonal pair.

Throughout this talk $\mathbb{F}$ denotes a field with algebraic closure $\overline{\mathbb{F}}$.

Let V denote a vector space over $\mathbb{F}$ with finite positive dimension.

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

Definition of a Tridiagonal pair

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

1. Each of A, A^* is diagonalizable on V.
2. There exists an ordering $\{V_i\}_{i=0}^d$ of the eigenspaces of A such that
   $A^* V_i \subseteq V_{i-1} + V_i + V_{i+1} \qquad (0 \leq i \leq d)$,
   where $V_{-1} = 0$, $V_{d+1} = 0$.
3. There exists an ordering $\{V_i^*\}_{i=0}^\delta$ of the eigenspaces of A^* such that
   $A V_i^* \subseteq V_{i-1}^* + V_i^* + V_{i+1}^* \qquad (0 \leq i \leq \delta)$,
   where $V_{-1}^* = 0$, $V_{\delta+1}^* = 0$.
4. There is no subspace $W \subseteq V$ such that $AW \subseteq W$ and $A^* W \subseteq W$ and $W \neq 0$ and $W \neq V$.

The diameter

Referring to our definition of a TD pair,

it turns out $d = \delta$; we call this common value the **diameter** of the pair.

Standard orderings

Referring to our definition of a TD pair,

An ordering of the eigenspaces of A (resp. A^*) is called **standard** whenever it satisfies condition 2 (resp. 3).

Let $\{V_i\}_{i=0}^d$ denote a standard ordering of the eigenspaces of A.

Then the ordering $\{V_{d-i}\}_{i=0}^d$ is also standard and no further ordering is standard.

A similar result holds for the eigenspaces of A^*.

An open problem for TD pairs

It is an open problem to classify the TD pairs up to isomorphism.

In this talk we consider a special case.

We will define a family of TD pairs said to be **q-Racah**.

In our main result we classify up to isomorphism the q-Racah TD pairs.

The tridiagonal relations

To motivate our results we now review some basic facts about TD pairs.

First of all, any TD pair satisfies two polynomial equations called the **tridiagonal relations**.

These relations are described on the next slide.

The tridiagonal relations

Proposition [Ito+Tanabe+T, 2001] Let A, A^* denote a TD pair over $\mathbb{F}$. Then there exist scalars $\beta, \gamma, \gamma^*, \varrho, \varrho^*$ in $\mathbb{F}$ such that

$$A^3A^* - (\beta+1)A^2A^*A + (\beta+1)AA^*A^2 - A^*A^3 = \gamma(A^2A^* - A^*A^2) + \varrho(AA^* - A^*A),$$

$$A^{*3}A - (\beta+1)A^{*2}AA^* + (\beta+1)A^*AA^{*2} - AA^{*3} = \gamma^*(A^{*2}A - AA^{*2}) + \varrho^*(A^*A - AA^*).$$

These equations are called the **tridiagonal relations**.

The q-Serre relations

In the special case where

$$\beta \neq \pm 2, \quad \gamma = \gamma^* = 0, \quad \varrho = \varrho^* = 0$$

the tridiagonal relations become the cubic **q-Serre relations**

$$A^3A^* - [3]_qA^2A^*A + [3]_qAA^*A^2 - A^*A^3 = 0,$$

$$A^{*3}A - [3]_qA^{*2}AA^* + [3]_qA^*AA^{*2} - AA^{*3} = 0.$$

Here $\beta = q^2 + q^{-2}$ and

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

The Dolan-Grady relations

In the special case where

$$\beta = 2, \quad \gamma = \gamma^* = 0,$$

the tridiagonal relations become the **Dolan-Grady relations**

$$[A, [A, [A, A^*]]] = \varrho[A, A^*],$$

$$[A^*, [A^*, [A^*, A]]] = \varrho^*[A^*, A].$$

Here $[r, s] = rs - sr$.

The shape of a TD pair

For a TD pair A, A^* let $\{V_i\}_{i=0}^d$ (resp. $\{V_i^*\}_{i=0}^d$) denote a standard ordering of the eigenspaces of A (resp. A^*).

It turns out that for $0 \leq i \leq d$ the spaces V_i, V_i^* have the same dimension; we denote this common dimension by ρ_i.

It is known that the sequence $\{\rho_i\}_{i=0}^d$ is symmetric and unimodal; that is $\rho_i = \rho_{d-i}$ for $0 \leq i \leq d$ and $\rho_{i-1} \leq \rho_i$ for $1 \leq i \leq d/2$.

We call the sequence $\{\rho_i\}_{i=0}^d$ the **shape** of A, A^*.

Sharp TD pairs

A TD pair is called **sharp** whenever $\rho_0 = 1$, where $\{\rho_i\}_{i=0}^d$ is the shape of the pair.

Proposition [Ito, Nomura, T 2008] A TD pair over an algebraically closed field is sharp.

Leonard pairs

The TD pairs of shape $(1,1,\ldots,1)$ are called **Leonard pairs**.

The Leonard pairs are classified up to isomorphism [T 2000].

Leonard pairs and orthogonal polynomials

The classification gives a bijection between the Leonard pairs and a family of orthogonal polynomials consisting of the following types:

q-Racah,
q-Hahn,
dual q-Hahn,
q-Krawtchouk,
dual q-Krawtchouk,
quantum q-Krawtchouk,
affine q-Krawtchouk,
Racah,
Hahn,
dual-Hahn,
Krawtchouk,
Bannai/Ito,
orphans (char($\mathbb{F}$) = 2 only).

This family coincides with the terminating branch of the **Askey scheme** of orthogonal polynomials.

The eigenvalues

For a TD pair A, A^* let $\{V_i\}_{i=0}^d$ (resp. $\{V_i^*\}_{i=0}^d$) denote a standard ordering of the eigenspaces of A (resp. A^*).

For $0 \leq i \leq d$ let θ_i (resp. θ_i^*) denote the eigenvalue of A (resp. A^*) associated with V_i (resp. V_i^*).

It is known that

$$\frac{\theta_{i-2} - \theta_{i+1}}{\theta_{i-1} - \theta_i}, \qquad \frac{\theta_{i-2}^* - \theta_{i+1}^*}{\theta_{i-1}^* - \theta_i^*}$$

are equal and independent of i for $2 \leq i \leq d-1$.

Solving the recurrence

For this recurrence the "most general" solution is:

$$\theta_i = a + bq^{2i-d} + cq^{d-2i} \quad (0 \le i \le d), \qquad (1)$$
$$\theta_i^* = a^* + b^*q^{2i-d} + c^*q^{d-2i} \quad (0 \le i \le d), \qquad (2)$$
$$q,\ a,\ b,\ c,\ a^*,\ b^*,\ c^* \in \mathbb{F}, \qquad (3)$$
$$q \neq 0,\ q^2 \neq 1,\ q^2 \neq -1,\ bb^*cc^* \neq 0. \qquad (4)$$

The TD pair A, A^* is said to have **q-Racah type** whenever the above conditions hold.

The Leonard pairs of q-Racah type correspond to the q-Racah polynomials.

TD pairs of q-Racah type

In our main result we classify up to isomorphism the TD pairs over an algebraically closed field that have q-Racah type.

We will state the main result shortly.

In order to do this concisely we first recall TD systems and the parameter array.

TD systems

A TD system is essentially a TD pair, together with fixed standard orderings of their eigenspaces.

For notational purposes we take a more formal approach.

Let A, A^* denote a TD pair.

An ordering of the primitive idempotents of A (resp. A^*) is called **standard** whenever the corresponding ordering of the eigenspaces of A (resp. A^*) is standard.

TD systems

By a **TD system** on V we mean a sequence

$$\Phi = (A; \{E_i\}_{i=0}^d; A^*; \{E_i^*\}_{i=0}^d)$$

that satisfies the following:

1. A, A^* is a TD pair on V.
2. $\{E_i\}_{i=0}^d$ is a standard ordering of the primitive idempotents of A.
3. $\{E_i^*\}_{i=0}^d$ is a standard ordering of the primitive idempotents of A^*.

Some parameters

It is known that a given TD system is determined up to isomorphism by three pieces of data:

the **eigenvalue sequence**,
the **dual eigenvalue sequence**,
the **split sequence**.

We now define these three sequences.

The eigenvalue sequence and dual eigenvalue sequence

For the time being fix a TD system $\Phi = (A; \{E_i\}_{i=0}^d; A^*; \{E_i^*\}_{i=0}^d)$ on V.

For $0 \leq i \leq d$ let θ_i (resp. θ_i^*) denote the eigenvalue of A (resp. A^*) associated with the eigenspace E_iV (resp. E_i^*V).

We call $\{\theta_i\}_{i=0}^d$ (resp. $\{\theta_i^*\}_{i=0}^d$) the **eigenvalue sequence** (resp. **dual eigenvalue sequence**) of Φ.

The split sequence

For $0 \leq i \leq d$ define

$$U_i = (E_0^*V + \cdots + E_i^*V) \cap (E_iV + \cdots + E_dV).$$

It is known that

$$\begin{aligned} V &= \sum_{i=0}^d U_i \quad \text{(direct sum)} \\ (A - \theta_i I)U_i &\subseteq U_{i+1} \quad (0 \leq i \leq d), \\ (A^* - \theta_i^* I)U_i &\subseteq U_{i-1} \quad (0 \leq i \leq d), \end{aligned}$$

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

The split sequence, cont.

Observe that for $0 \leq i \leq d$,

$$\begin{aligned} (A - \theta_{i-1}I)\cdots(A - \theta_1 I)(A - \theta_0 I)U_0 &\subseteq U_i, \\ (A^* - \theta_1^* I)\cdots(A^* - \theta_{i-1}^* I)(A^* - \theta_i^* I)U_i &\subseteq U_0. \end{aligned}$$

Therefore U_0 is invariant under

$$(A^* - \theta_1^* I)\cdots(A^* - \theta_i^* I)(A - \theta_{i-1}I)\cdots(A - \theta_0 I).$$

Let ζ_i denote the corresponding eigenvalue.

We call the sequence $\{\zeta_i\}_{i=0}^d$ the **split sequence** of Φ.

The parameter array

Proposition [Ito, Nomura, T 2008] Up to isomorphism the tridiagonal system Φ is determined by the data

$$(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d; \{\zeta_i\}_{i=0}^d). \qquad (5)$$

We call the sequence (5) the **parameter array** of Φ.

Some notation

Let λ denote an indeterminate.

For later use we define some polynomials in $\mathbb{F}[\lambda]$.

For $0 \leq i \leq d$,

$$\begin{aligned}
\tau_i &= (\lambda-\theta_0)(\lambda-\theta_1)\cdots(\lambda-\theta_{i-1}),\\
\eta_i &= (\lambda-\theta_d)(\lambda-\theta_{d-1})\cdots(\lambda-\theta_{d-i+1}),\\
\tau_i^* &= (\lambda-\theta_0^*)(\lambda-\theta_1^*)\cdots(\lambda-\theta_{i-1}^*),\\
\eta_i^* &= (\lambda-\theta_d^*)(\lambda-\theta_{d-1}^*)\cdots(\lambda-\theta_{d-i+1}^*).
\end{aligned}$$

Note that each of τ_i, η_i, τ_i^*, η_i^* is monic with degree i.

The classification

Definition Let d denote a nonnegative integer and let $(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d)$ denote a sequence of scalars taken from $\mathbb{F}$. We call this sequence **q-Racah** whenever:

(i) $\theta_i \neq \theta_j$, $\theta_i^* \neq \theta_j^*$ if $i \neq j$ $(0 \leq i, j \leq d)$.

(ii) There exist scalars $q, a, b, c, a^*, b^*, c^*$ that satisfy (1)–(4).

The classification

We now state our main result.

Theorem [Ito+T, 08] Assume the field $\mathbb{F}$ is algebraically closed and let d denote a nonnegative integer. Let $(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d)$ denote a q-Racah sequence of scalars in $\mathbb{F}$ and let $\{\zeta_i\}_{i=0}^d$ denote any sequence of scalars in $\mathbb{F}$. Then the following are equivalent:

(i) There exists a TD system Φ over $\mathbb{F}$ that has parameter array $(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d; \{\zeta_i\}_{i=0}^d)$;

(ii) $\zeta_0 = 1$, $\zeta_d \neq 0$, and

$$0 \neq \sum_{i=0}^{d} \eta_{d-i}(\theta_0)\eta_{d-i}^*(\theta_0^*)\zeta_i.$$

Suppose (i), (ii) hold. Then Φ is unique up to isomorphism of TD systems.

The classification in context

Shortly we will outline a proof of our main theorem.

But first we discuss the significance of the main theorem with respect to a certain conjecture called the **classification conjecture**.

The classification conjecture gives the classification of all TD pairs over an algebraically closed field.

This conjecture is stated on the next slide.

The classification conjecture

Conjecture [Ito+T, 07] Assume $\mathbb{F}$ is algebraically closed and let $(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d; \{\zeta_i\}_{i=0}^d)$ (6) denote a sequence of scalars in $\mathbb{F}$. Then there exists a TD system Φ over $\mathbb{F}$ with parameter array (6) if and only if:

(i) $\theta_i \neq \theta_j$, $\theta_i^* \neq \theta_j^*$ if $i \neq j$ $(0 \leq i,j \leq d)$;

(ii) $\zeta_0 = 1$, $\zeta_d \neq 0$, and

$$0 \neq \sum_{i=0}^{d} \eta_{d-i}(\theta_0)\eta_{d-i}^*(\theta_0^*)\zeta_i;$$

(iii) The expressions $\frac{\theta_{i-2}-\theta_{i+1}}{\theta_{i-1}-\theta_i}$, $\frac{\theta_{i-2}^*-\theta_{i+1}^*}{\theta_{i-1}^*-\theta_i^*}$ are equal and independent of i for $2 \leq i \leq d-1$.

Suppose (i)–(iii) hold. Then Φ is unique up to isomorphism of TD systems.

The classification conjecture, cont.

The "only if" direction of the classification conjecture is proved [Ito, Nomura, T 08].

The last assertion of the classification conjecture follows from our earlier remarks.

The "if" direction of the classification conjecture was checked by computer for $d \leq 5$ [Nomura+T, 08].

Our main theorem establishes the "if" direction of the classification conjecture for the case in which $(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d)$ has q-Racah type.

The main theorem: proof outline

In our proof of the main theorem the essential part is to demonstrate that (ii) implies (i).

Assuming $\mathbb{F}$ is algebraically closed, we now fix a q-Racah sequence $(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d)$ of scalars in $\mathbb{F}$, and a sequence $\{\zeta_i\}_{i=0}^d$ of scalars in $\mathbb{F}$ that satisfy condition (ii) of the main theorem.

Our goal is to display a TD system over $\mathbb{F}$ that has parameter array $(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d; \{\zeta_i\}_{i=0}^d)$.

To this end we fix $q, a, b, c, a^*, b^*, c^*$ that satisfy (1)–(4).

Proof outline, cont.

Associated with q is the quantum affine algebra $U_q(\widehat{\mathfrak{sl}}_2)$ over $\mathbb{F}$.

In a nutshell, our proof strategy is:

- Using a, b, c, a^*, b^*, c^* we choose a pair of elements $A, A^* \in U_q(\widehat{\mathfrak{sl}}_2)$.
- Using $\{\zeta_i\}_{i=0}^d$ we pick an appropriate $U_q(\widehat{\mathfrak{sl}}_2)$-module V.
- Using the actions of A, A^* on V we obtain the required TD system.

The algebra $U_q(\widehat{\mathfrak{sl}}_2)$

Definition $U_q(\widehat{\mathfrak{sl}}_2)$ is the associative $\mathbb{F}$-algebra with 1, defined by generators $e_i^{\pm}$, $K_i^{\pm 1}$, $i \in \{0,1\}$ and the following relations:

$$\begin{aligned}
K_i K_i^{-1} &= K_i^{-1} K_i = 1, \\
K_0 K_1 &= K_1 K_0, \\
K_i e_i^{\pm} K_i^{-1} &= q^{\pm 2} e_i^{\pm}, \\
K_i e_j^{\pm} K_i^{-1} &= q^{\mp 2} e_j^{\pm}, \qquad i \neq j, \\
[e_i^+, e_i^-] &= \frac{K_i - K_i^{-1}}{q - q^{-1}}, \\
[e_0^{\pm}, e_1^{\mp}] &= 0,
\end{aligned}$$

$$(e_i^{\pm})^3 e_j^{\pm} - [3]_q (e_i^{\pm})^2 e_j^{\pm} e_i^{\pm} + [3]_q e_i^{\pm} e_j^{\pm} (e_i^{\pm})^2 - e_j^{\pm} (e_i^{\pm})^3 = 0, \qquad i \neq j.$$

The $U_q(\widehat{\mathfrak{sl}}_2)$-module $V(\alpha)$

In the literature on $U_q(\widehat{\mathfrak{sl}}_2)$ there are some finite-dimensional irreducible $U_q(\widehat{\mathfrak{sl}}_2)$-modules $V_n(\alpha)$, where $0 \neq \alpha \in \mathbb{F}$ and n is a positive integer.

These modules are called evaluation modules.

The scalar α is the evaluation parameter and $n+1$ is the dimension.

We will make use of $V_1(\alpha)$; for notational convenience we denote this module by $V(\alpha)$.

$V(\alpha)$ is defined as follows.

The $U_q(\widehat{\mathfrak{sl}}_2)$-module $V(\alpha)$

For all $0 \neq \alpha \in \mathbb{F}$ the $U_q(\widehat{\mathfrak{sl}}_2)$-module $V(\alpha)$ has a basis x, y on which the generators act as follows:

$$\begin{aligned}
K_1 x &= q x, & K_1 y &= q^{-1} y, \\
e_1^- x &= y, & e_1^- y &= 0, \\
e_1^+ x &= 0, & e_1^+ y &= x, \\
K_0 x &= q^{-1} x, & K_0 y &= q y, \\
e_0^- x &= 0, & e_0^- y &= q \alpha^{-1} x, \\
e_0^+ x &= q^{-1} \alpha y, & e_0^+ y &= 0.
\end{aligned}$$

Tensor products of $U_q(\widehat{sl}_2)$-modules

Let V, W denote $U_q(\widehat{sl}_2)$-modules.

Then the tensor product $V \otimes W$ has the following $U_q(\widehat{sl}_2)$-module structure:

For $v \in V$, for $w \in W$ and for $i \in \{0,1\}$,

$$\begin{aligned} e_i^+(v \otimes w) &= e_i^+ v \otimes K_i w + v \otimes e_i^+ w, \\ e_i^-(v \otimes w) &= e_i^- v \otimes w + K_i^{-1} v \otimes e_i^- w, \\ K_i(v \otimes w) &= K_i v \otimes K_i w. \end{aligned}$$

Standard $U_q(\widehat{sl}_2)$-modules

By a standard $U_q(\widehat{sl}_2)$-module of diameter d we mean

$$V(\alpha_1) \otimes V(\alpha_2) \otimes \cdots \otimes V(\alpha_d),$$

where $0 \neq \alpha_i \in \mathbb{F}$ for $1 \leq i \leq d$.

Standard $U_q(\widehat{sl}_2)$-modules: a basis

Let V denote a standard $U_q(\widehat{sl}_2)$-module with diameter d.

Observe that V has a basis

$$v_1 \otimes v_2 \otimes \cdots \otimes v_d \qquad v_i \in \{x, y\} \quad (1 \leq i \leq d).$$

For notational convenience we abbreviate this basis as follows.

For all subsets $s \subseteq \{1, 2, \ldots, d\}$ define

$$u_s = v_1 \otimes v_2 \otimes \cdots \otimes v_d,$$

where $v_i = x$ if $i \notin s$ and $v_i = y$ if $i \in s$ $(1 \leq i \leq d)$.

Standard $U_q(\widehat{sl}_2)$-modules: the weight spaces

For $0 \leq i \leq d$ define

$$U_i = \mathrm{Span}\{u_s \mid s \subseteq \{1, 2, \ldots, d\}, \quad |s| = i\}.$$

Then

$$V = \sum_{i=0}^{d} U_i \qquad \text{(direct sum)},$$

and

$$\dim(U_i) = \binom{d}{i} \qquad (0 \leq i \leq d).$$

Moreover

$$(K_0 - q^{2i-d} I) U_i = 0, \quad (K_1 - q^{d-2i} I) U_i = 0$$

for $0 \leq i \leq d$.

We call $\{U_i\}_{i=0}^d$ the weight spaces of V.

Standard $U_q(\widehat{\mathrm{sl}}_2)$-modules: the weight spaces

It turns out that for $0 \leq i \leq d$,

$$e_0^+ U_i \subseteq U_{i+1}, \qquad e_1^- U_i \subseteq U_{i+1},$$
$$e_0^- U_i \subseteq U_{i-1}, \qquad e_1^+ U_i \subseteq U_{i-1},$$

where $U_{-1} = 0$ and $U_{d+1} = 0$.

Choosing a standard $U_q(\widehat{\mathrm{sl}}_2)$-module

Shortly we will use $\{\zeta_i\}_{i=0}^d$ to choose a standard $U_q(\widehat{\mathrm{sl}}_2)$-module with some good evaluation parameters $\{\alpha_i\}_{i=1}^d$.

To this end we define two elements $R, L \in U_q(\widehat{\mathrm{sl}}_2)$.

The elements $R, L \in U_q(\widehat{\mathrm{sl}}_2)$

We define

$$R = ue_0^+ + ve_1^- K_1,$$
$$L = u^* e_1^+ + v^* e_0^- K_0,$$

where u, v, u^*, v^* are any scalars in $\mathbb{F}$ such that

$$uv^* = -bb^* q^{-1}(q - q^{-1})^2,$$
$$vu^* = -cc^* q^{-1}(q - q^{-1})^2.$$

The elements $R, L \in U_q(\widehat{\mathrm{sl}}_2)$

By construction, for $0 \leq i \leq d$ we have

$$RU_i \subseteq U_{i+1}, \qquad LU_i \subseteq U_{i-1}.$$

Therefore U_0 is invariant under $L^i R^i$.

We are interested in the associated eigenvalue, and we now come to a key step in the argument.

The elements $R, L \in U_q(\widehat{\mathfrak{sl}}_2)$

Proposition There exists a standard $U_q(\widehat{\mathfrak{sl}}_2)$-module $V = \otimes_{i=1}^{d} V(\alpha_i)$ such that for $0 \leq j \leq d$,

ζ_j is the eigenvalue of $L^j R^j$ on U_0.

The proposition is proved using a polynomial called the (nonstandard) **Drinfel'd polynomial**.

From now on we work with the above module V.

The elements $A, A^* \in U_q(\widehat{\mathfrak{sl}}_2)$

We define

$$\begin{aligned} A &= aI + bK_0 + cK_1 + R, \\ A^* &= a^*I + b^*K_0 + c^*K_1 + L. \end{aligned}$$

The A, A^* are diagonalizable on V

By construction

$$(A - \theta_i I)U_i \subseteq U_{i+1},$$
$$(A^* - \theta_i^* I)U_i \subseteq U_{i-1}$$

for $0 \leq i \leq d$.

This implies that A (resp. A^*) is diagonalizable on V with eigenvalues $\{\theta_i\}_{i=0}^{d}$ (resp. $\{\theta_i^*\}_{i=0}^{d}$).

The projections E_i, E_i^*

For $0 \leq i \leq d$ define the elements $E_i, E_i^* \in U_q(\widehat{\mathfrak{sl}}_2)$ as follows:

$$E_i = \prod_{\substack{0 \leq j \leq d \\ j \neq i}} \frac{A - \theta_j I}{\theta_i - \theta_j}, \quad E_i^* = \prod_{\substack{0 \leq j \leq d \\ j \neq i}} \frac{A^* - \theta_j^* I}{\theta_i^* - \theta_j^*}.$$

Observe that E_i (resp. E_i^*) acts on V as the primitive idempotent of A (resp. A^*) associated with the eigenvalue θ_i (resp. θ_i^*).

The A, A^* satisfy the tridiagonal relations

By the defining relations for $U_q(\widehat{\mathfrak{sl}}_2)$ the elements A, A^* satisfy a pair of tridiagonal relations.

This yields

$$E_i A^* E_j = 0, \quad E_i^* A E_j^* = 0$$
$$\text{if} \quad |i-j| > 1, \quad (0 \leq i, j \leq d).$$

Some inequalities

Recall that $\zeta_d \neq 0$ and

$$0 \neq \sum_{i=0}^{d} \eta_{d-i}(\theta_0)\eta^*_{d-i}(\theta^*_0)\zeta_i.$$

These inequalities yield

$$E_0^* E_d E_0^* \neq 0, \qquad E_0^* E_0 E_0^* \neq 0.$$

The issue of irreducibility

Its not quite true that A, A^* act on V as a TD pair, because the irreducibility axiom might fail.

This aspect is handled in the next few slides.

The subalgebra T

Let T denote the subalgebra of $U_q(\widehat{\mathfrak{sl}}_2)$ generated by A, A^*.

Let TE_0^*V denote the T-submodule of V generated by $E_0^*V = U_0$.

We show that TE_0^*V contains a unique maximal proper T-submodule; denote this by M and consider the quotient T-module $L = TE_0^*V/M$.

By construction the T-module L is irreducible.

The subalgebra T, cont.

By the above results the elements $(A; \{E_i\}_{i=0}^d; A^*; \{E_i^*\}_{i=0}^d)$ act on L as a TD system which we denote by Φ.

By construction Φ has eigenvalue sequence $\{\theta_i\}_{i=0}^d$ and dual eigenvalue sequence $\{\theta_i^*\}_{i=0}^d$.

It follows from the choice of V that Φ has split sequence $\{\zeta_i\}_{i=0}^d$.

Therefore Φ has parameter array

$$(\{\theta_i\}_{i=0}^d; \{\theta_i^*\}_{i=0}^d; \{\zeta_i\}_{i=0}^d)$$

and we have accomplished our goal.

THE END

Papers acknowledging JSPS grant L-07512

1. T. Ito and P. Terwilliger. Tridiagonal pairs of q-Racah type. *Linear Algebra Appl.*, submitted.

2. T. Ito and P. Terwilliger. The Drinfel'd polynomial of a tridiagonal pair. *Des. Codes Cryptogr.*, submitted.

3. T. Ito and P. Terwilliger. The augmented tridiagonal algebra, preprint.

4. K. Nomura and P. Terwilliger. Sharp tridiagonal pairs. *Linear Algebra Appl.*, in press.

5. K. Nomura and P. Terwilliger. Towards a classification of the tridiagonal pairs. *Linear Algebra Appl.*, in press.

6. K. Nomura and P. Terwilliger. The structure of a tridiagonal pair. *Linear Algebra Appl.*, in press.

7. K. Nomura and P. Terwilliger. Tridiagonal pairs and the μ-conjecture. *Linear Algebra Appl.*, submitted.

The Bannai-Ito Conjecture :

For fixed $k > 2$, there are finitely many distance-regular graphs with valency k

Sejeong Bang[1] J.H. Koolen[2] V. Moulton[3]

[1]Department of Mathematics
Pusan National University

[2]Department of Mathematics
POSTECH

[3]Department of Computer Science
University of East Anglia

Outline

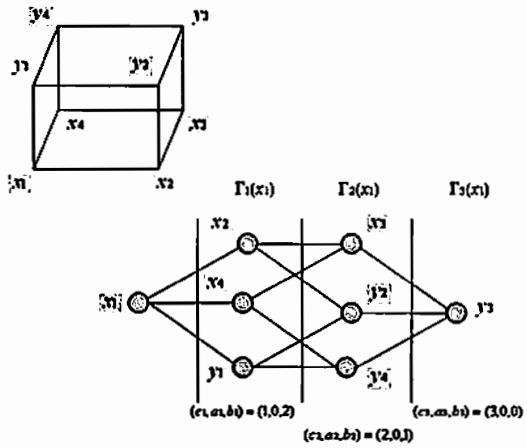
Let $\Gamma = (V(\Gamma), E(\Gamma))$ be a connected undirected regular graph (with valency k).

- Distance $d(x, y)$
- Diameter $D = D(\Gamma) := \max\{d(x, y) \mid x, y \in V(\Gamma)\}$
- For a vertex $x \in V(\Gamma)$,

$$\Gamma_i(x) := \{y \in V(\Gamma) \mid d(x, y) = i\}$$

- Note that $V(\Gamma) = \{x\} \dot{\cup} \Gamma_1(x) \dot{\cup} \cdots \dot{\cup} \Gamma_D(x)$

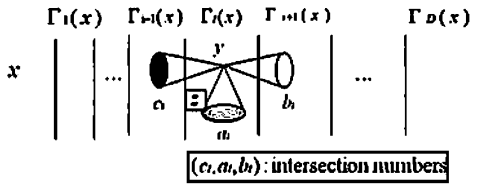
Equitable Partition $V = \{x_1\} \dot{\cup} \Gamma_1(x_1) \dot{\cup} \Gamma_2(x_1) \dot{\cup} \Gamma_3(x_1)$



Distance-Regular Graphs (DRG)

A connected graph Γ with diameter D is *distance-regular* if for each $i = 0, 1, \ldots, D$, $\exists\ c_i, a_i, b_i \geq 0$ such that if $d(x, y) = i$ then

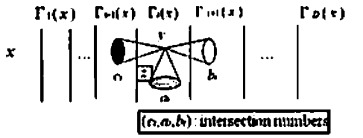
$$c_i = |\Gamma_{i-1}(x) \cap \Gamma_1(y)|,\ a_i = |\Gamma_i(x) \cap \Gamma_1(y)| \text{ and } b_i = |\Gamma_{i+1}(x) \cap \Gamma_1(y)|\ .$$



Parameters

Let Γ be a DRG.

1. $k := b_0$ (valency of Γ)
2. $c_i + a_i + b_i = k \quad (0 \leq i \leq D)$
3. $c_i \leq c_{i+1} \quad (1 \leq i \leq D-1)$
4. $b_i \geq b_{i+1} \quad (0 \leq i \leq D-2)$
5. $a_i \geq \max\{a_1 + 1 - b_i,\ a_1 + 1 - c_i\} \quad (1 \leq i \leq D-1)$



Examples

- Five Platonic Solids
- Hamming Graphs
- Johnson Graphs
- Grassmann Graphs
- ....

✓ Any DRG is a regular graph with valency k.

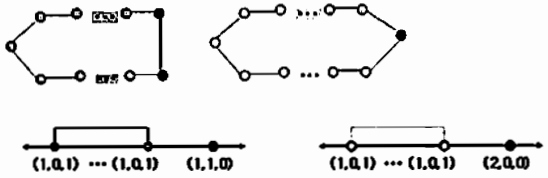
Question

For an integer $k \geq 2$, are there only finitely many DRG with valency k ?

- **Existence**
  Hamming Graph $H(D, q)$ $(D, q \geq 2)$
  (diameter= D, valency= $D(q-1)$)
- **Finiteness**
  Show that $|V| \leq f(k)$ for a function f.
  $\Rightarrow$ Show that $\ell((c_1, a_1, b_1)) \leq g(k)$ for a function g.

$k = 2$

$(c_i, a_i, b_i) \in \{(1,0,1), (1,1,0), (2,0,0)\}$



There are **infinitely** many DRGs with valency $k = 2$.

The Bannai-Ito Conjecture (1984)

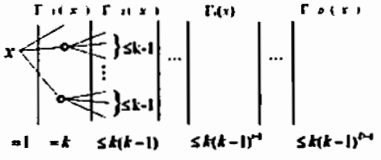
For given integer $k \geq 3$,
there are only finitely many DRGs with given valency k.

Diameter Bounds (Regular Graphs)

It is clear that for fixed $v < \infty$, there are only finitely many graphs with at most v-vertices.

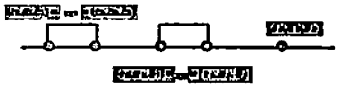
Let Γ be a connected regular graph with valency k and diameter D

$\Rightarrow \quad |V(\Gamma)| \leq 1 + k + k(k-1) + k(k-1)^2 + \cdots + k(k-1)^{D-1}$



We want to find a function F satisfying $D \leq F(k)$.

Diameter Bounds (DRG)



- $D = \sum \ell(c_i, a_i, b_i) + 1$
- head $\mathbf{h} := \ell(c_1, a_1, b_1)$ and tail $\mathbf{t} := \ell(b_1, a_1, c_1)$
- $\mathbf{t} \leq \mathbf{h}$

A.A.Ivanov (1983)

$$D(\Gamma) = \sum \ell(c_i, a_i, b_i) + 1 \leq 4^{k(\Gamma)}\mathbf{h}(\Gamma)$$

We want to find a function F satisfying $\mathbf{h} \leq F(k)$.

Known Results

- $k = 3$: 13 DRGs and $D \leq 8$ (Biggs, Boshier and Shawe-Taylor 1983)
- $k = 4$: 17 intersection arrays and $D \leq 7$ (Brouwer and Koolen 1999)
- $k = 5, 6, 7$: Koolen and Moulton (2002)
- $k = 8, 9, 10$ and $a_1 = 0$: Koolen and Moulton (2004)

Bannai-Ito (1986-1988)

The conjecture is true if

- $k = 3, 4$
- *bipartite*
- $a_1 = 0$ *and* $D\text{-}\mathbf{h}\text{-}\mathbf{t} \leq C$ *for any* $C \geq 1$.

Bang, Koolen and Moulton (2007, 2008?) : The conjecture is true if

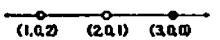
- $D - \mathbf{h} - \mathbf{t} \leq C$ for any $C \geq 1$
- $D - \mathbf{h} - \mathbf{t} \leq \epsilon \mathbf{h}$ for some $\epsilon = \epsilon(k) > 0$
- Regular Near Polygons

$k = 3$ (Biggs et al. 1986)

$(c_i, a_i, b_i) \in \{(1,1,1), (1,0,2), (2,0,1), (1,2,0), (2,1,0), (3,0,0)\}$
Note : $D = \sum \ell(i) + 1 \leq 4^k \mathbf{h}$.

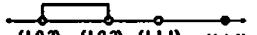
$D \leq 2$: K_4, $K_{3,3}$, O_3

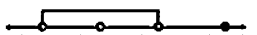
$D \geq 3$: Only 10 DRGs

1. 3-cube 

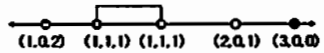
2. The Heawood Graph 

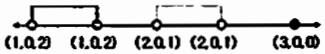
3. The Pappus graph 

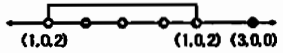
4. The Coxeter Graph 

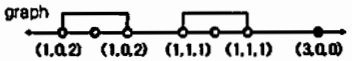
5. Tutte's 8-cage 

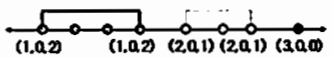
$k = 3$

6. The Dodecahedron 

7. The Desargues graph 

8. Tutte's 12-cage 

9. The Biggs-Smith graph 

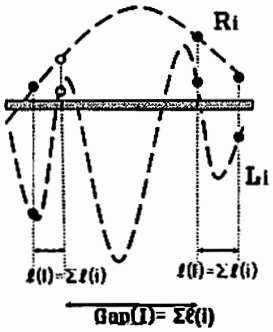
10. The Foster graph 

Well-Placed Intervals

Let $\mathcal{G} = \{(\gamma_i, \alpha_i, \beta_i)\}$ be a (κ, λ)-graphical sequence.

$\mathfrak{R}_i := \alpha_i + 2\sqrt{\beta_i \gamma_i}$ $\quad$ $\mathfrak{L}_i := \alpha_i - 2\sqrt{\beta_i \gamma_i}$

Remark : the sequence $\{\mathfrak{R}_i\}_{i=1}^{g}$ is unimodal and $\mathfrak{R}_i \geq \mathfrak{R}_1 \ \ \forall i$.



$\mathcal{I} = [\mathcal{I}_{\min}, \mathcal{I}_{\max}]$
: *well-placed interval* if

1. $\mathcal{I} \subseteq (\mathfrak{R}_1, \max_i \mathfrak{R}_i)$;
2. $\mathfrak{L}_i, \mathfrak{R}_i \notin \mathcal{I}$ for all $1 \leq i \leq g$;
3. $\mathcal{I} \subseteq (\mathfrak{L}_i, \mathfrak{R}_i)$ for some i.

Sequences

Let $\kappa \geq 3$ and $0 \leq \lambda \leq \kappa - 2$ be integers.

A sequence $\mathcal{G} = \{(\gamma_i, \alpha_i, \beta_i)\}_{i=1}^{g}$ is called a (κ, λ)-graphical sequence if

1. $\gamma_i + \alpha_i + \beta_i = \kappa \ \ (\gamma_i, \alpha_i, \beta_i \in \mathbb{N}_0, \ \beta_i, \gamma_i \geq 1)$
2. $(\gamma_1, \alpha_1, \beta_1) = (1, \lambda, \kappa - \lambda - 1)$
3. $\alpha_i \geq \max\{\lambda + 1 - \beta_i, \ \lambda + 1 - \gamma_i\}$
4. $\gamma_i \leq \gamma_{i+1}, \ \ \beta_i \geq \beta_{i+1} \ \ \forall i$

Note : For DRG Γ, $\mathcal{G} = \{(c_i, a_i, b_i)\}_{i=1}^{D(\Gamma)-1}$: (k, a_1)-graphical sequence.

Let $\ell : \{1, \ldots, g\} \to \mathbb{N}_0$ be a function.
$\mathcal{T}(\mathcal{G}, \ell)$:(κ, λ)-tridiagonal sequence if each element $(\gamma_i, \alpha_i, \beta_i) \in \mathcal{G}$ consecutively appear exactly $\ell(i)$ times.

Let $\mathrm{h} = \mathrm{h}(\mathcal{T}) := \ell(1)$ and $D = D(\mathcal{T}) := 1 + \sum_{i=1}^{g} \ell(i)$.

Christoffel Numbers

Let $\mathcal{T}(\mathcal{G}, \ell)$ be a (κ, λ)-tridiagonal sequence with $(\gamma_D, \alpha_D, \beta_D) = (c, \kappa - c, 0)$ where $D = D(\mathcal{T})$.

Define orthogonal polynomials $\{v_i(x)\}_{i=0}^{D}$ by

$$\begin{aligned} v_0(x) &= 1, v_1(x) = x, \\ x v_i(x) &= \beta_{i-1} v_{i-1}(x) + \alpha_i v_i(x) + \gamma_{i+1} v_{i+1}(x) \ (1 \leq i \leq D-1) \\ v_{D+1}(x) &= (x - \alpha_D) v_D(x) - \beta_{D-1} v_{D-1}(x) \end{aligned}$$

- $\kappa_i := v_i(\kappa) \quad (0 \leq i \leq D)$
- $u_i(x) := \frac{v_i(x)}{\kappa_i} \quad (0 \leq i \leq D)$
- $M(\theta) := \sum_{i=0}^{D} \frac{v_i(\theta)^2}{\kappa_i} = \frac{1}{\kappa_D}\{v'_{D+1}(\theta) v_D(\theta) - v'_D(\theta) v_{D+1}(\theta)\} = \sum_{i=0}^{D} \kappa_i u_i(\theta)^2$

" The Christoffel Numbers of the Orthogonal Polynomials "

Outline of the Proof (I)

1. For each i satisfying $\mathfrak{R}_i > \mathfrak{R}_1$, $\exists$ well-placed interval $\mathcal{I} \subseteq (\mathfrak{L}_i, \mathfrak{R}_i)$ in which we can approximate the Christoffel number for any eigenvalue θ of $\mathcal{T}$ in $\mathcal{I}$:

$$C_1 \left(\frac{1}{9\kappa^4}\right)^{\mathrm{Gap}(\mathcal{I})} \ell(\mathcal{I}) \prod_{j=1}^{a-1} \left(\left(\frac{\beta_j}{\gamma_j}\right) \rho_j(\theta)^2\right)^{\ell(j)}$$

$$\leq \sum_{i=0}^{D(\mathcal{T})} \kappa_i u_i(\theta)^2 \leq C_2 (9\kappa^4)^{\mathrm{Gap}(\mathcal{I})} \ell(\mathcal{I}) \prod_{j=1}^{a-1} \left(\left(\frac{\beta_j}{\gamma_j}\right) \rho_j(\theta)^2\right)^{\ell(j)}$$

2. This implies that two eigenvalues of $\mathcal{T}(\mathcal{G}, \ell)$ in $\mathcal{I}$ that are algebraic conjugate are very close if $\mathbf{h}$ is large and $\frac{\mathrm{Gap}(\mathcal{I})}{\mathbf{h}}$ is small enough.
3. If $\ell(\mathcal{I}) \geq \epsilon \mathbf{h}$ holds for a constant $\epsilon > 0$ then there exist constants $C_i = C_i(\kappa, \epsilon, \mathcal{G}, \mathcal{I}) > 0$ such that

$$\text{either } \mathbf{h} \leq C_1 \text{ or } \mathrm{Gap}(\mathcal{I}) > C_2 \mathbf{h}\,.$$

Outline of the Proof (II)

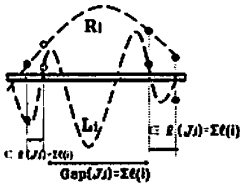
Bang, Koolen and Moulton (2007)

Let $k \geq 3$ be given. Then there exists $\epsilon = \epsilon(k) > 0$ such that the Bannai-Ito conjecture is true for any DRG with valency k and D-h-t$\leq \epsilon \mathbf{h}$.

Hence, suppose that $\mathcal{T}(\mathcal{G}, \ell)$ is a (κ, λ)-tridiagonal sequence satisfying $D - \mathbf{h} - \mathbf{t} > \epsilon \mathbf{h}$.

Gaol: Find a function $H = H(\kappa, \mathcal{G}) > 0$ such that $\mathbf{h} \leq H$ holds.

Outline of the Proof (III)



- there exists i such that $\ell(i) > \left(\frac{\epsilon}{|\mathcal{G}|}\right) \mathbf{h}$ $\quad (\because\ D - \mathbf{h} - \mathbf{t} > \epsilon \mathbf{h})$
- there exists a well-placed interval $\mathcal{J}_i \subseteq (\mathfrak{L}_i, \mathfrak{R}_i)$
  $\Rightarrow \ell(\mathcal{J}_i) \geq \ell(i) > \left(\frac{\epsilon}{|\mathcal{G}|}\right) \mathbf{h}$
- Either $\mathbf{h} \leq C_1$ or $\mathrm{Gap}(\mathcal{J}_i) > C_2 \mathbf{h}$ hold for some $C_i = C_i(\kappa, \mathcal{G})$
- If $\mathrm{Gap}(\mathcal{J}_i) > C_2 \mathbf{h}$ then there exists i' such that $\ell(i') > \left(\frac{C_2}{|\mathcal{G}|}\right) \mathbf{h}$

Note : $\mathfrak{R}_{i'} > \mathfrak{R}_i$ and $\mathfrak{R}_i < \mathfrak{R}_{i'} < \cdots < \max \mathfrak{R}_j$

By using induction, $\exists\ H(\kappa, \mathcal{G}) > 0$ satisfying $\underline{\mathbf{h} \leq H(\kappa, \mathcal{G})}$ ∎

Conclusion

Bang, Koolen and Moulton (2007)

Let $k \geq 3$ be given. Then there exists $\epsilon = \epsilon(k) > 0$ such that the Bannai-Ito conjecture is true for any DRG with valency k and D-h-t$\leq \epsilon \mathbf{h}$.

Hence, suppose that $\mathcal{T}(\mathcal{G}, \ell)$ is a (κ, λ)-tridiagonal sequence satisfying $D - \mathbf{h} - \mathbf{t} > \epsilon \mathbf{h}$.

Gaol: Find a function $H = H(\kappa, \mathcal{G}) > 0$ such that $\mathbf{h} \leq H$ holds.

$\therefore$ **For fixed integer $k > 2$, there are only finitely many distance-regular graphs with valency k.**

Completely regular subgraphs in distance-regular graphs

平木 彰 (大阪教育大学)　Akira HIRAKI (Osaka Kyoiku University)

1. Definition.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a connected graph with usual shortest path distance ∂_Γ. Let d be the diameter of Γ (i.e., the maximal distance of two vertices in Γ). Set

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

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

$$A(x,y) = \Gamma_i(x) \cap \Gamma_1(y),\ B(x,y) = \Gamma_{i+1}(x) \cap \Gamma_1(y),\ C(x,y) = \Gamma_{i-1}(x) \cap \Gamma_1(y).$$

Definition 1. Let i be an integer with $0 \le i \le d$.

(i) We say $c_i(\Gamma)$-*exists* if $c_i(\Gamma) = |C(x,y)|$ is a constant whenever $\partial_\Gamma(x,y) = i$.

(ii) We say $a_i(\Gamma)$-*exists* if $a_i(\Gamma) = |A(x,y)|$ is a constant whenever $\partial_\Gamma(x,y) = i$.

(iii) We say $b_i(\Gamma)$-*exists* if $b_i(\Gamma) = |B(x,y)|$ is a constant whenever $\partial_\Gamma(x,y) = i$.

A connected graph Γ of diameter d is said to be *distance-regular* if $c_i(\Gamma)$-exists and $b_i(\Gamma)$-exists for $i = 0, \ldots, d$. Then Γ is a regular graph of valency $k = k(\Gamma) = b_0(\Gamma)$ and that $a_i(\Gamma)$-exists with $a_i(\Gamma) = k(\Gamma) - c_i(\Gamma) - b_i(\Gamma)$ for $i = 0, \ldots, d$. The constants $c_i(\Gamma), a_i(\Gamma)$ and $b_i(\Gamma)$ ($i = 0, \ldots, d$) are called the *intersection numbers* of Γ.

For more background information about distance-regular graphs we refer the reader to [1, 2, 3].

Definition 2. Let Y be a non-empty subset of vertices in Γ. We identify Y with the induced subgraph on it. Let $z \in V\Gamma$. Define

$$\partial_\Gamma(z, Y) = \partial_\Gamma(Y, z) = \min\{\partial_\Gamma(z,v) \mid v \in Y\}. \tag{1}$$

Let

$$t(Y) = t_\Gamma(Y) = \max\{\partial_\Gamma(Y,x) \mid x \in V\Gamma\} \tag{2}$$

which is called the *covering radius of* Y *in* Γ. Set

$$\Gamma_i(Y) = \{x \in V\Gamma \mid \partial_\Gamma(Y,x) = i\} \tag{3}$$

for $i = 0, 1, \ldots, t(Y)$.

(i) A subgraph Y is called *completely regular* if for any integer i with $0 \le i \le t(Y)$

$$\gamma_i = |\Gamma_{i-1}(Y) \cap \Gamma_1(x)|,\ \alpha_i = |\Gamma_i(Y) \cap \Gamma_1(x)|,\ \beta_i = |\Gamma_{i+1}(Y) \cap \Gamma_1(x)| \tag{4}$$

are constants whenever $x \in \Gamma_i(Y)$.

(ii) A subgraph Y is called *strongly closed* if $C(u,v) \cup A(u,v) \subseteq Y$ for any $u, v \in Y$.

(iii) Let m be an integer with $1 \leq m \leq d-1$. We say *the condition* $(SC)_m$ *holds* if for any pair of vertices at distance m there exists a strongly closed subgraph of diameter m containing them.

Let Δ be a strongly closed subgraph of Γ with diameter $m = d(\Delta)$. For any vertices x and y in Δ, a shortest path between x and y in Γ is contained in the subgraph Δ. So the distance in Δ coincides with the distance in Γ. In particular, $c_i(\Delta)$-exists and $a_i(\Delta)$-exists with $c_i(\Delta) = c_i$ and $a_i(\Delta) = a_i$ for $i = 1, \ldots, m$. Moreover, if Δ is a regular graph of valency $k(\Delta)$, then $b_i(\Delta)$-exists with $b_i(\Delta) = k(\Delta) - c_i - a_i$ for $i = 1, \ldots, m$, and thus Δ is distance-regular. However there exist several examples of non-regular strongly closed subgraphs in a distance-regular graph (see [5], [10], [6]).

- Suppose Γ is either the doubled Grassmann graph, the doubled Odd graph, or the Odd graph. The it satisfies the condition $(SC)_j$ for $j = 1, \ldots, d-1$, where $d = d(\Gamma)$. Any strongly closed subgraph of odd diameter $2m+1 \leq d-1$ is a doubled Grassmann graph, or a doubled Odd graph But any strongly closed subgraph of even diameter $2m \leq d-1$ is non-regular distance-biregular graph.
- For any pair of vertices at distance 6 in the Foster graph there exists a 2-subdivision graph of the Peterson graph (the graph obtained from the Peterson graph by replacing each edge by a path of length 2) containing them as a strongly closed subgraph.
- For any pair of vertices at distance 5 in the Biggs-Smith graph there exists a 3-subdivision graph of the complete graph K_4 (the graph obtained from the complete graph K_4 by replacing each edge by a path of length 3) containing them as a strongly closed subgraph

The next results are direct consequences of [4, Theorem 1], [10, Theorem 1.1], [5, Proposition 4.5] (see also [6, Corollary 7]).

Proposition 3. *Let Γ be a distance-regular graph of diameter $d \geq 3$ and valency $k \geq 3$. Let m be an integer with $1 \leq m \leq d-1$. Suppose the condition $(SC)_m$ holds. Then the following hold.*

(i) *The condition $(SC)_j$ holds for all j with $1 \leq j \leq m$.*

(ii) *Any strongly closed subgraph of diameter m satisfies the condition $(SC)_j$ for all j with $1 \leq j \leq m-1$.*

(iii) *Let $r = r(\Gamma) := \max\{i \mid (c_i, a_i, b_i) = (c_1, a_1, b_1)\}$. Then one of the following holds.*

  (a) $m \leq r$.

  (b) $m = r+2 \in \{5, 8\}$, $a_1 = 0$ *and* $(c_{r+1}, a_{r+1}, b_{r+1}) = (c_{r+2}, a_{r+2}, b_{r+2}) = (1, 1, k-2)$.

  (c) $r = 4$, $m = 6$, $a_1 = \cdots = a_6 = 0$, $c_5 = c_6 = 2$ *and* $k \in \{3, 57\}$.

  (d) Γ *is either the doubled Grassmann graph, the doubled Odd graph, or the Odd graph.*

  (e) $b_{m-1} > b_m$ *and any strongly closed subgraph of diameter m is distance-regular.*

2. Examples and Results.

We are interested in a distance-regular graph Γ which satisfies the following two conditions.

- The condition $(SC)_i$ holds for any integer i with $1 \leq i \leq d-1$.
- There exists a strongly closed subgraph Δ which is completely regular in Γ.

The following are examples of such distance-regular graphs.

- Suppose Γ is a Hamming graph (resp. a dual polar graph). Then Γ satisfies the condition $(SC)_i$ for $i = 1, \ldots, d-1$, where $d = d(\Gamma)$. Any strongly closed subgraph of diameter i is also a Hamming graph (resp. a dual polar graph). Also any strongly closed subgraph of diameter i is completely regular of covering radius $d-i$ in Γ.
- Suppose Γ is a regular near $2d$-gon with $a_1 > 0$ and $c_2 > 1$. Then Γ satisfies the condition $(SC)_i$ for $i = 1, \ldots, d-1$, where $d = d(\Gamma)$. Any strongly closed subgraph of diameter i is also a regular near $2i$-gon with $a_1 > 0$ and $c_2 > 1$. Also any strongly closed subgraph of diameter 1 is completely regular of covering radius $d-1$ in Γ.
- Suppose Γ is a Hermitian forms graph of diameter $d = d(\Gamma)$. Then Γ satisfies the condition $(SC)_i$ for $i = 1, \ldots, d-1$. Any strongly closed subgraph of diameter i is also a Hermitian forms graph. Also any strongly closed subgraph of diameter $d-1$ is completely regular of covering radius 2 in Γ.

A proof of these facts are given in [6], [8] and [9]. Another examples are given in [9].

The following are main results in this talk (see [8]).

Theorem 4. *Let Γ be a distance-regular graph of diameter $d \geq 4$ and $c_2 > 1$. Suppose that for any integer i with $1 \leq i \leq d-1$ and for any pair of vertices at distance i in Γ there exists a strongly closed subgraph of diameter i containing them. If there exists a strongly closed subgraph Δ of diameter j with $2 \leq j \leq d-2$ which is completely regular in Γ, then*

$$c_i = \begin{bmatrix} i \\ 1 \end{bmatrix}, \quad a_i = \begin{bmatrix} i \\ 1 \end{bmatrix} a_1, \tag{5}$$

hold for $i = 1, \ldots, d-1$, where

$$\begin{bmatrix} i \\ 1 \end{bmatrix} = \begin{bmatrix} i \\ 1 \end{bmatrix}_q := q^{i-1} + \cdots + q + 1$$

denotes the Gaussian binomial coefficient with basis $q := c_2 - 1$. Moreover any strongly closed subgraph Λ of diameter h with $4 \leq h \leq d-1$ is either a Hamming graph or a dual polar graph.

Theorem 5. *Let Γ be a distance-regular graph of diameter $d \geq 4$. Then the following conditions are equivalent.*

(i) *Γ is either a Hamming graph or a dual polar graph.*

(ii) *For any integer i with $1 \leq i \leq d-1$ and for any pair of vertices at distance i in Γ there exists a regular strongly closed subgraph of diameter i containing them which is completely regular of covering radius $d-i$.*

(iii) *For any integer i with $1 \leq i \leq d-1$ and for any pair of vertices at distance i in Γ there exists a strongly closed subgraph of diameter i containing them. Moreover there exists a strongly closed subgraph of diameter j with $2 \leq j \leq d-1$ which is completely regular of covering radius $d-j$ in Γ.*

The case that Δ has diameter 2 had already studied and the similar result had been obtained by H. Suzuki [11].

References

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

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

[3] C. D. Godsil, Algebraic combinatorics, Chapman and Hall, Inc., 1993

[4] A. Hiraki, A distance-regular graph with strongly closed subgraphs, *J. Alg. Combin.* **14** (2001), 127–131.

[5] A. Hiraki, A characterization of the doubled Grassmann graphs, the doubled Odd graphs, and the Odd graphs by strongly closed subgraphs, *Europ. J. Combin.* **24** (2003), 161–171.

[6] A. Hiraki, A characterization of the Hamming graph by strongly closed subgraphs, *Europ. J. Combin.* **29** (2008), 1603–1616.

[7] A. Hiraki, A characterization of some distance-regular graphs by strongly closed subgraphs, to appear in Europ. J. Combin.

[8] A. Hiraki, A characterization of the Hamming graphs and dual polar graphs by completely regular subgraphs, preprint.

[9] A. Hiraki, Completely regular subgraphs in distance-regular graphs, in preparation.

[10] H. Suzuki, On strongly closed subgraphs of highly regular graphs, *Europ. J. Combin.* **16** (1995), 197–220.

[11] H. Suzuki, Parallelogram-free distance-regular graphs having completely regular strongly regular subgraphs, preprint.

Bipartite graphから得られるGorenstein polytopes

田上　真
金沢大学理学部計算科学科

1　序文

頂点が全て格子点にある多面体をlattice polytopeと言う．$S \subset \mathbb{R}^n$, $t \in \mathbb{N}$に対して，$tS = \{tx \mid x \in S\}$, $L_S(t) = \sharp(tS \cap \mathbb{Z}^n)$とおく．Ehrhart[6]は$d$次元lattice polytopeに対して$L_P(t)$は常に$t$についての$d$次多項式になることを示した．$L_P(t)$を$P$のEhrhart多項式という．$\mathrm{Ehr}_P(z) = 1 + \sum_{t \in \mathbb{N}} L_P(t) z^t$を$P$のEhrhart級数という．$P \subset \mathbb{R}^n$を$d$次元lattice polytopeとすると，$L_P(t)$は$d$次多項式であるので$P$のEhrhart級数はある$s \leq d$に対して

$$\mathrm{Ehr}_P(z) = \frac{\sum_{i=0}^{s} h_i z^i}{(1-z)^{d+1}}.$$

と有理関数の形に書ける．sをPのdegree, $r = d + 1 - s$をcodegreeと言う．また分子の多項式をh^*-多項式と言う．次のことがよく知られている: $h_0 = 1$, codegree rはtP°が格子点を持つ最小のtと一致し，$h_s = \sharp(rP^\circ \cap Z^n)$が成り立つ，ここで$S \subset \mathbb{R}^n$に対して$S^\circ$で$S$のrelative interiorを表している．Ehrhart多項式及びEhrhart級数に関する優良な参考文献としてBeck-Robins[3]がある．

Ehrhart多項式は代数的意味を持っており，多面体から構成されるEhrhart環のHilbert関数として考えることができる．Ehrhart環がGorensteinである時，PがGorensteinであると言う．Ehrhart環及びGorenstein性については[8], [11]を参照のこと．PがGorensteinである必要十分条件はh^*-多項式の係数が対称であること，即ち$h_i = h_{s-i}$が任意のiについて成り立つことである，これはEhrhart多項式の言葉で言うと，$L_{P^\circ}(r) = 1$かつ任意の$t > r$に対して$L_P(t-r) = L_{P^\circ}(t)$が成り立つことと同値である．

$G = (V, E)$を多重辺とループを持たない無向グラフとする，ここでVは頂点集合，Eは辺集合を表している（多重辺があっても下記と同様のことは成り立つ）．$M \subset E$がmatchingであるとはMの任意の異なる2つの辺は交わらない時を言う．もし任意の頂点があるMの辺上にあるならば，Mをperfect matchingと言う．MをGのperfect mathcingとする．それぞれのperfect matching Mに対して、その特性ベクトル$\chi_M \in \mathbb{R}^E$を次のように定義する: $e \in E$に対して

$$(\chi_M)_e := \begin{cases} 1: & \text{if } e \in M, \\ 0: & \text{otherwise.} \end{cases}$$

定義 1.1 (perfect matching polytope).

$$P_G := \mathrm{conv}\{\chi_M \mid M \text{ は } G \text{ の perfect matching}\} \subset \mathbb{R}^E.$$

一般にP_Gはfull-dimensionではなく，P_Gの内格子点というとrelative interior上の格子点を考えていることに注意する．Edmondの定理よりPerfect matching polytopeのhyperplane表示が解っている:

定理 1 (Edmond[5]). $G = (V, E)$を偶数個の頂点を持ったグラフとする．この時$x = (x_e)_{e \in E} \in \mathbb{R}^E$が$P_G$上にある必要十分条件は次の3条件が成り立つことである:

(1) $x_e \geq 0$ $(\forall e \in E)$,

(2) $\sum_{v \in e} x_e = 1$ $(\forall v \in V)$,

(3) $\sum_{e \in C(S,S')} x_e \geq 1$ $(\forall S \subset V,\ |S|$ は奇数*)*.

ここで $v \in e$ は v が e の端点であることを表しており, S' は S の補集合, $S, T \subset V$ に対して $C(S,T) = \{(u,v) \in E \mid u \in S,\ v \in T\}$ を表している.

もしグラフが bipartite グラフであれば条件 (3) を取り除くことができることが知られている. 即ち $x \in P_G$ である必要十分条件は定理の条件 (1), (2) が成り立つことである. S に対して $C(S,S')$ の元を bridge ということにする. Perfect matching polytope については Grötschel-Lovász-Schrijver[7] を参照のこと.

Grid graph $G(m,n) = (V,E)$ は次のように定義される:

$$V := \{(i,j) \mid 0 \leq i \leq m-1,\ 0 \leq j \leq n-1\},$$

$$((i,j),(k,l)) \in E \Longleftrightarrow |i-k| + |j-l| = 1.$$

Torus graph $G_T(m,n)$ は $G(m,n)$ と同じ頂点集合をもったもので, $G(m,n)$ に辺 $((0,j),(m-1,j))$ $(0 \leq j \leq n-1)$ と $((i,0),(i,n-1))$ $(0 \leq i \leq m-1)$ を付け加えたグラフである.

Beck-Haase-Sam[2] は Edmond の定理を用いて Grid graph の perfect matching polytope がいつ Gorenstein に成るかを決定した. また一部の parameter に対する Torus graph の perfect matching polytope が Gorenstein になることを証明した. $P(m,n)$, $P_T(m,n)$ でそれぞれ $G(m,n)$, $G_T(m,n)$ の perfect matching polytope を表す. 即ち Beck-Haase-Sam[2] は次を示した.

定理 2 (B-H-S[2]). *m は 1 か偶数, かつ n は偶数であるとする. この時 $P_T(m,n)$ は Gorenstein である.*

また Beck-Haase-Sam はその次元も計算している.

命題 1.1 (B-H-S[2]). *mn は偶数であるとする. この時*

(1) $\dim P(m,n) = (m-1)(n-1)$,

(2) $n > 2$ *が偶数の時,* $\dim P_T(2,n) = n+1$,

(3) $m > 2$, $n > 2$ *がどちらも偶数である時,* $\dim P_T(m,n) = mn+1$,

(4) $n > 1$ *が奇数の時,* $\dim P_T(2,n) = n$,

(5) $m > 2$ *が偶数,* $n = 1$ *の時,* $\dim P_T(m,n) = 1$,

(6) $m > 2$ *が偶数,* $n > 1$ *が奇数の時,* $\dim P_T(m,n) = mn$.

我々は第 2 節で定理 2 を補完する. 即ち次を示す.

定理 3. *mn は偶数であるとする. この時 $P_T(m,n)$ が Gorenstein である必要十分条件は $m = 1$ 又は偶数, かつ n は偶数, 又は $(m,n) = (2,3), (2,5)$ であることである.*

定理 2 はもっと一般的な次の命題の系として得られていた.

定理 4 (B-H-S[2]). *G は偶数頂点を持った k-regular bipartite graph とする. この時 G の Perfect matching polytope は Gorenstein である.*

定理 4 により Gorenstein polytope の無限族を構成できる. 第 3 節で我々は graph から構成される新しい polytope を導入する. この polytope は perfect matching polytope の自然な拡張になっており, Edmond の定理と類似の結果が成り立つことを示す. またこの polytope を用いて定理 4 を拡張し, さらに多くの Gorenstein polytope を構成する. graph から Gorenstein polytope を構成する別の方法として Ohsugi-Hibi[10] がある.

2 Torus graphs と Perfect matching polytopes

この節で Beck-Haase-Sam の Torus graph の Gorenstein 性の特徴づけの補完を行う.

補題 2.1. $G_T(m,n)=(V,E)$ を *Torus graph* とし $m,n\geq 3$ とする. この時, 任意の $S\subset V$ $(2\leq |S|\leq |V|-2)$ に対して, *6* 本以上の *bridge* が存在する.

[証明] S の点を黒点, S' の点を白点とする. 各列において全ての点が黒か白である場合, 各行に少なくとも 2 本の bridge があり $m\geq 3$ であるから補題は従う. よってある列が存在しその列には黒も白もあるとしてよい. 一般性を失うことなくその列は 1 列目であり $(1,1)$ は白であるとしてよい. すでにこの列には少なくとも 2 本の bridge が存在する. 2 通りに場合わけする. (I) 1 行目に黒が存在する場合, (II) 1 行目に黒が存在しない場合.

(I) この場合 1 行目には少なくとも 2 本の bridge が存在する. よってすでに 4 本の bridge を持っている. $2\leq |S|\leq |V|-2$ であるから, $(1,1)$ 以外に白点が存在する. その点を (i,j) とする. 一般性を失うことなく $i\neq 1$ としてよい. もし i 行目に黒が存在したら bridge は少なくとも 2 本増える. よって i 行目は全て白であるとする. 1 行目の黒を $(1,k)$ とすると k 列目には少なくとも 2 本の bridge が存在する. よってこの場合少なくとも 6 本の bridge が存在する.

(II) もし各列に黒点が存在するならば, 各列に少なくとも 2 本以上の bridge がかかるので, $n\geq 3$ より補題は従う. よってある列が存在してその列の全ての点は白であるとしてよい. この場合 1 列目のある黒 $(i,1)$ は同じ行にも列にも白を持っている. よって白と黒の立場を逆転させて (I) の状態を得る. **[証明終]**

[定理 3 の証明] $P=P_T(m,n)$ とする. まず十分性を示す. $m=1$ 又は偶数, かつ n は偶数の場合は定理 2 ですでに示されている. Edmond の定理により $x\in tP^\circ$ である必要十分条件は

(1') $x_e>0$ $(\forall e\in E)$,

(2') $\sum_{v\in e}x_e=t$ $(\forall v\in V)$,

(3') $\sum_{e\in C(S,S')}x_e>t$ $(\forall S\subset V, 3\leq |S|\leq |V|-3$ は奇数$)$,

となる (下記にみるように (1'), (2'), (3') を全て満たしている点が存在することがわかるのでこの必要十分条件性が言える).

$(m,n)=(2,3)$ とする. $L_{P^\circ}(3)=0$, $L_{P^\circ}(4)\neq 0$ であることを示す. グラフは 3−regular であるので, $t=3$ に対して (1'), (2') を満たす格子点は全ての辺で 1 を取らなければいけない. $S=\{(0,0),(0,1),(0,2)\}$ を取ると (3') は成り立たない. よって $3P^\circ$ に格子点は存在しない. $x\in\mathbb{R}^E$ を図 1 のように定めると $x\in 4P^\circ$ であることは簡単に判定できる.

よって $L_{P^\circ}(4)\neq 0$ であり, polytope P の codegree は 4 であることが解る. 一方命題 1.1 により $\dim P_T(2,3)=3$. よって polytope $P_T(2,3)$ の degree は 0 であり, $P_T(2,3)$ は unimodular simplex, 特に Gorenstein になる.

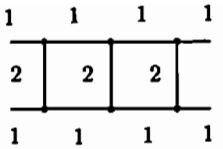


図 1: $(m,n)=(2,3)$ 上の x

$(m,n)=(2,5)$ とする. グラフは 3−regular であるので Edmond の定理の条件 (1'), (2') より $P^\circ, 2P^\circ$ には格子点は存在しない. all 1-vector $\mathbf{1}=(1,1,\ldots,1)$ が $3P^\circ$ に入る. 実際 $\mathbf{1}$ は $t=3$ に対して条件 (1'), (2') を満たし, またどのように 3 点又は 5 点を S として取っても (3') が成立することは容易に確認できる. よって $L_{P^\circ}(3)\neq 0$ であり, P の codegree は 3 である. 以下 $L_{P^\circ}(t)=L_P(t-3)$ を示す.

$\iota: R^E \longrightarrow R^E$ を $\iota(x)=x+\mathbf{1}$ と定義する. $x\in lP$ とすると, x が $t=l$ で (1), (2), (3) を満たし, $\mathbf{1}$ が $t=3$ に対して (1'), (2'), (3') を満たすことから $\iota(x)$ は $t=l+3$ で (1'), (2'), (3') を満たしている. よって ι は $lP\cap\mathbb{Z}^E$ から $(l+3)P^\circ\cap\mathbb{Z}^E$ への単射を与える. 逆写像 ι^{-1} もまた $(l+3)P^\circ\cap\mathbb{Z}^E$ から $lP\cap\mathbb{Z}^E$ への単射を与えることを示す. これが示されれば $L_{P^\circ}(l+3)=|(l+k)P^\circ\cap\mathbb{Z}^E|=|lP\cap\mathbb{Z}^E|=L_P(l)$ が解る.

$x\in(l+3)P$ とすると, $y=\iota^{-1}(x)=x-\mathbf{1}$ は $t=l$ に対して (1), (2) を満たしている. もしある S に対して, (3) が成り立たないとすると, S の中に孤立点があってはならない. また対称性より考える S は全頂点数の半分以下としてよい. よって (3) を満たさない奇数濃度の S に対してその配置の可能性は図 2, 3 の 4 つである (対称性を考えている), ここで大きい点は S の点を表しており, 太い辺は S の induced subgraph を表している.

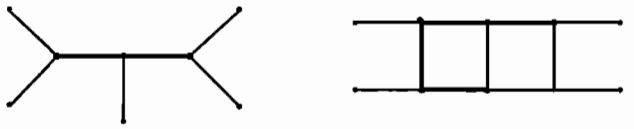


図 2: $(m,n)=(2,5)$

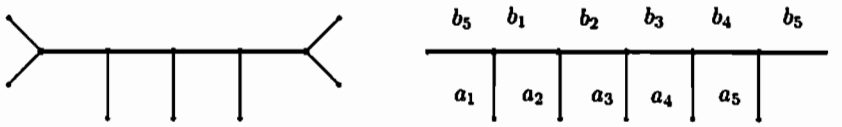


図 3: $(m,n)=(2,5)$ 上の y

図 2 の 3 つの場合には系 3.2 より条件 (1), (2) から (3) は従う. 図 3 を考える. x は $t=l+3$ に対して (3') を満たしているので, $\sum_{e\in C(S,S')}x_e\geq l+4$, よって

$$\sum_{e\in C(S,S')}y_e=\sum_{e\in C(S,S')}(x_e-1)\geq l-1.$$

もし $\sum_{e\in C(S,S')} y_e < l$ ならば $\sum_{e\in C(S,S')} y_e = \sum_{1\le i\le 5} a_i = l-1$ となる．一方 y に対する (2) より

$$5l = \sum_{v\in S, v\in e} y_e = \sum_{1\le i\le 5} a_i + 2\sum_{1\le i\le 5} b_i \equiv l-1 \pmod 2.$$

これは矛盾である．よって y は (3) を常に満たしている．これは ι^{-1} が $(l+3)P^\circ \cap \mathbb{Z}^E$ から $lP\cap\mathbb{Z}^E$ への単射を与えていることを示している．

必要性を示すためにその対偶を示す．まず $m=2, n\ge 7$ は奇数とする．1 が $3P^\circ$ に入ることは $(m,n)=(2,5)$ の時と同様に簡単に解る，よって codegree は 3. また ι が $lP\cap\mathbb{Z}^E$ から $(l+3)P^\circ\cap\mathbb{Z}^E$ への単射を与えることも同様である．ある $y\notin 2P$ で $\iota(y)\in 5P^\circ$ なるものが存在することを示せば $L_P(2) < L_{P^\circ}(5)$ が解り，Gorenstein でないことが示される．

図 4 のようにベクトル y を定める．

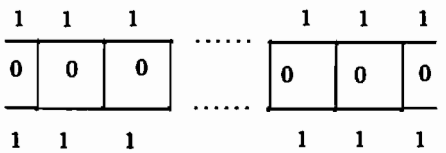


図 4: $(m,n)=(2,n)$, $n\ge 7$ の y

この y は上の行の全ての点を S として考えると (3) を満たさない．よって $y\notin 2P$．しかし一方 $x=\iota(y)=y+1\in 5P^\circ$ であることを示す．もし S に対して $\sum_{e\in C(S,S')} y_e \ge t$ とすると，1 は (3') を満たすので，$\sum_{e\in C(S,S')} x_e > t+3$ となる．よって $|S|\le 7$(奇数) で $\sum_{e\in C(S,S')} y_e < 2$ である時だけを考えればよい．$\sum_{e\in C(S,S')} y_e < 2$ となるのは S として上の行の点を全て取った場合である．この場合上の行から下の行に 7 本以上の辺が出ているので，$7=\sum_{e\in C(S,S')} x_e \ge t+4=6$ となる．よって $x\in 5P^\circ$．

次に $m\ge 4$ は偶数，$n=3$ の場合を考える．対称性により $m=3$, $n\ge 4$ は偶数とする．グラフは 4−regular であるから 1 は $t=4$ に対して (1'), (2') を満たす．また補題 2.1 より (3') を満たすことも解る．よって $1\in 4P^\circ$ であり，P の codegree は 4 である．ι が $lP\cap\mathbb{Z}^E$ から $(l+4)P^\circ\cap\mathbb{Z}^E$ への単射を与えることは上と同様である．よって Gorenstein でないことを示すにはある $y\notin 3P$ で $\iota(y)\in 7P^\circ$ なるものの存在を示せば十分である．図 5 のようにベクトル y を定める (太線以外の部分は 0 と定める)．

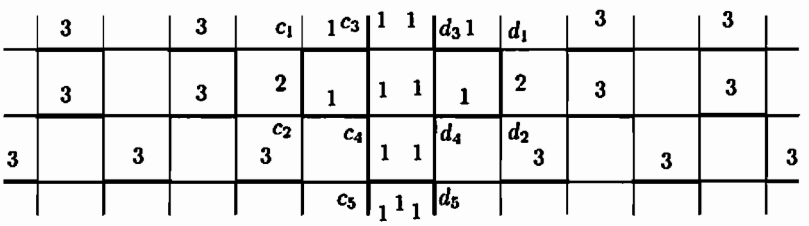


図 5: $(m,n)=(3,n)$, $n\ge 4$ の y

S として $c_i (1\le i\le 5)$ の 5 点を取ると，$\sum_{e\in C(S,S')} y_e = 1 < 3$．よって $y\notin 3P$．$x=\iota(y)\in 7P^\circ$ であることを示す．(1'), (2') が成り立つことは明らか．(3') が全ての奇数濃度の S に対して成り立つことを示さなければいけないが，補題 2.1 と $m=2, n\ge 7$ の時と同様の議論により，$\sum_{e\in C(S,S')} y_e \le 1$

なる S だけを考えればよい．S を選出する時に $\sum_{e\in C(S,S')} y_e \leq 1$ を満たすには c_i 達は全て選ぶか全て選らばないかのどちらかである．このことは d_i 達にとっても同様である．よって考えるべき S の候補は c_i 達は全て選び d_i は全て入っておらず，c_i, d_i 達と disjoint な matching で全ての辺が weight 3 を持っているものから構成される．この時 $|C(S,S')| \geq 8$ であることを示す．もしこれが示せたとすると，$\sum_{e\in C(S,S')} x_e = \sum_{e\in C(S,S')}(y_e+1) \geq 1+\sum_{e\in C(S,S')} 1 \geq 8$ となり，$x \in 7P^\circ$ が解る．しかしこの時，各行には右と左に少なくとも 1 本の bridge があり，3 行目の matching が一つずれていることより，3 行目から 1, 2 行目に bridge が出ている．よって $|C(S,S')| \geq 8$ である．

$m \geq 4$ が偶数，$n \geq 5$ が奇数である場合を考える．補題 2.1 より $1 \in 4P^\circ$ であり，P の codegree は 4 である．この場合も $y \notin 2P$, $x = \iota(y) \in 6P^\circ$ である y を構成する．ベクトル y を各行の辺には 1 を各列の辺には 0 を対応させて定義する．1 行目の点を S とすると，$\sum_{e\in C(S,S')} y_e = 0 < 2$. よって $y \notin 2P$.

$x = \iota(y)$ が全ての奇数濃度の S に対して $\sum_{e\in C(S,S')} x_e > 6$ を示す．補題 2.1 と上と同様の議論により，S の候補としては $\sum_{e\in C(S,S')} y_e = 0$ のものだけを考えればよい．この条件を満たす S を選出する時は各行において点は全て取るか全て取らないかのどちらかである．よってこの場合少なくとも $2n$ 本の bridge ができる．よって $|C(S,S')| \geq 2n \geq 10$ であり，$\sum_{e\in C(S,S')} x_e = \sum_{e\in C(S,S')}(y_e+1) \geq |C(S,S')| \geq 10$. よって $x \in 6P^\circ$. **[証明終]**

注意 1. 定理 3 により，$P = P_T(2,5)$ は codegree 3 の Gorenstein である．また命題 1.1 により $\dim P_T(2,5) = 5$ であるので P の次数は 3 であることが解る．$P_T(2,5)$ の頂点は $P_T(2,5)$ の格子点全体で，それらは $G_T(2,5)$ の perfect matching で与えられる．perfect matching の数は簡単に数えられ 11 と解る．$h_1 = L_P(1)-(d+1) = 11-6 = 5$ であるから，その Ehrhart 級数は

$$\mathrm{Ehr}_P(z) = \frac{1+5z+5z^2+z^3}{(1-z)^6},$$

で与えられる．

3 S-matching polytope

この節でグラフを用いた新しい polytope を構成する．

$G = (V,E)$ をグラフとし，$S \subset V$ に対して $\langle S\rangle$ で S の G における induced subgraph を表す．また G の subgraph $N_G(S) = (V_S, E_S)$ を次のように定義する:

$$\Gamma(S) := \{x \in S' \mid \text{ある } y \in S \text{ に対して}, (x,y) \in E\},$$

$$V_S := S \cup \Gamma(S).$$

$$E_S := C(S,S') \cup \{(x,y) \in E \mid x, y \in S\}.$$

$N_G(S)$ を S の G における Neighbor graph と言う．$M \subset E_S$ で M の任意の異なる 2 辺は S の点で交わらず，S のすべて点は M のある辺の端点になっているものを $S-$matching と言う．

定義 3.1 (S-matching polytope). 部分集合 S に対して，$N_G(S) = (V_S, E_S)$ を Neighbor graph とする．この時，S の S-matching polytope P_S を次のように定義する:

$$P_S := \mathrm{conv}\{\chi_M \in \mathbb{R}^{E_S} \mid M \text{ は } S-matching,\},$$

ここで $\chi_M \in \mathbb{R}^{E_S}$ は M の characteristic vector を表す．

注意 2. S として頂点全体をとると, P_S は perfect matching polytope と一致する.

定理 5. $G=(V,E)$ をグラフとし, $S\subset V$ に対して, $N_G(S)=(V_S,E_S)$ をその *Neighbor graph* とする. $\langle S\rangle$ が *bipartite* であると仮定する. この時 $x\in\mathbb{R}^{E_S}$ が P_S 上にある必要十分条件は次の二条件が成り立つことである:

(1) $x_e\geq 0\ (\forall e\in E_S)$,

(2) $\sum_{v\in e}x_e=1\ (\forall v\in S)$.

[証明] 証明は Vempala[13] の lecture note にある bipartite graph に対する Edmond の定理の証明と同じようにできる.

定理の条件の不等式で定義される polytope を C で表すとする. M を $S-$matching とすると, χ_M は明らかに定理の不等式と等式を満たす. よって $P_S\subset C$ である. 逆に C の中にある格子点が与えられると明らかに一つの $S-$matching が対応している. よって C の頂点は全て格子点であることを示せば十分である.

ある C の頂点 $x=(\ldots,x_e,\ldots)$ が分数成分をもっているとする. x に対して $N_G(S)$ の新しい subgraph $N_G(S)_x$ を作る. $N_G(S)_x$ の頂点集合は V_S, 辺集合は x において分数成分の $e\in E_S$ からなる. 次のように場合分けする. (I) $N_G(S)_x$ が cycle を含まない場合, (II) $N_G(S)_x$ が cycle を含む場合.

(I) この時 $N_G(S)_x$ の連結成分は次数 1 の頂点を少なくとも 2 つ持つ. 次数 1 の頂点は C の 2 番目の条件より S の点ではありえない. 二つの次数 1 の点を端点とする path を $e_1,e_2,\ldots,e_m$ とする. この時 $\epsilon:=\min\{x_{e_i},1-x_{e_i}\mid 1\leq i\leq m\}$ と定める. この時 $\underline{x}$ を path 以外の値は変えず, $\underline{x}_{e_1}:=x_{e_1}-\epsilon$, $\underline{x}_{e_2}:=x_{e_2}+\epsilon,\ldots$ と ϵ を加えることと引くことを交互に施して定義する. $\overline{x}$ も $+\epsilon$ からはじめること以外同様に定義する. この時明らかに $\underline{x}$ も $\overline{x}$ も C の 2 条件を満たしている. よって $\underline{x},\overline{x}\in C$ である. 一方 $x=(\underline{x}+\overline{x})/2$ であるので, x は C の頂点ではありえない. よって矛盾.

(II) 次に $N_G(S)_x$ に cycle が存在する場合, もしその cycle が偶数の長さを持ったとすれば, この場合も (I) と同様に $\overline{x},\underline{x}$ が C の中に定義され, x が C の頂点でないことが示される.

もし cycle が奇数の長さを持ったとすると, $\langle S\rangle$ は bipartite であるので, その cycle は必ず $\Gamma(S)$ の点を含まないといけない. cycle を $e_1,\ldots,e_m$ とし $v\in\Gamma(S)$ が e_1, e_m と incident であるとする. この時 x に対して $\overline{x}$ を次のように定義する cycle 以外では値を変えず, $\overline{x}_{e_1}=x_{e_1}+\epsilon$, $\overline{x}_{e_2}=x_{e_2}-\epsilon$ と交互に ϵ を足すことと引くことを繰り返す. cycle の長さは奇数なので $\overline{x}_{e_m}=x_{e_m}+\epsilon$ となる. また同様に $\underline{x}_{e_1}=x_{e_1}-\epsilon$, $\underline{x}_{e_2}=x_{e_2}+\epsilon$ と交互に繰り返す, 最後は $\underline{x}_{e_m}=x_{e_m}-\epsilon$ となる. $v\in\Gamma(S)$ であるので $\underline{x},\overline{x}$ は条件 (1), (2) をそのまま満たし, $\underline{x},\overline{x}\in C$ かつ $x=(\underline{x}+\overline{x})/2$ となる. よってこの場合もまた x は頂点と成り得ず矛盾である. **[証明終]**

次に $\langle S\rangle$ が bipartite である場合の P_S の次元を求める公式を与える.

命題 3.1. $G=(V,E)$ をグラフ, $S\subset V$, $N_G(S)=(V_S,E_S)$ をその *Neighbor graph* とする. $\langle S\rangle$ は連結な *bipartite* で, 任意の $e\in E_S$ はある S*-matching* に属していると仮定する. この時

$$\dim P_S=\begin{cases}|E_S|-|S|: & \text{if } \Gamma(S)\neq\emptyset,\\ |E_S|-|S|+1: & \text{otherwise.}\end{cases}$$

[証明] $S\times E_S$ 行列 I を

$$I_{v,e}=\begin{cases}1: & v\in e,\\ 0: & \text{otherwise.}\end{cases}$$

と定義する. 定理 5 より, P_S は $Ix = {}^t\mathbf{1}, x \in \mathbb{R}^{E_S}_{\geq 0}$ の解空間と一致する, ここで ${}^t x$ は x の転置を表している. 適当な $\sum \lambda_M = 1, \lambda_M > 0$ に対して, $x = \sum \lambda_M \chi_M$ とおく, ここで和は全ての S-matching を動く. 仮定より任意の $e \in E_S$ はある S-matching に属しているので, $Ix = {}^t\mathbf{1}$ で $x_e > 0$ $(\forall e \in E_S)$ なるものが構成できた. よって P_S の次元は $Ix = 0$ の解空間の次元と等しい. 以下 I の rank を調べる. I の v 行ベクトルを I_v, I の e 列ベクトルを $I^{(e)}$ で表すとする. I の列は $C(S,S)$ と $C(S,S')$ の部分に分かれる.

まず $\Gamma(S) = \emptyset$ の場合を考える. この時 $C(S,S')$ の列は存在しない. $\sum_v a_v I_v = 0$ とする. もし $e = (v,v') \in E_S$ ならば $I^{(e)}$ は v, v' 成分のみ 1 で他は 0 であるので, $\sum_v a_v I_v = 0$ より $a_v = -a_{v'}$ でなければならない. よって $(v,v') \in E_S$ ならば $a_v = -a_{v'}$ となる. $\langle S \rangle$ は bipartite であるので, $S = S_1 \cup S_2$, $C(S_i, S_i) = \emptyset$ と分かれる. $\langle S \rangle$ は連結であるので, ある $v \in S_1$ に対して $a_v = \lambda$ ならば, 任意の $u \in S_1$ に対して $a_u = \lambda$, 任意の $w \in S_2$ に対して, $a_w = -\lambda$ となる. これは行空間の次元が $|S| - 1$ であることを示している. よって $Ix = 0$ の解空間の次元は $|E_S| - |S| + 1$ となる.

次に $\Gamma(S) \neq \emptyset$ の場合を考える. $\sum_v a_v I_v = 0$ とする. $\Gamma(S)$ の定義より, $v' \in \Gamma(S)$ に対して, ある $v \in S$ が存在して $e = (v,v') \in E_S$ となる. この時 $I^{(e)}$ は v 成分のみ 1 で他は 0 である. よって $a_v = 0$. 一方 $v, v' \in S$ が隣接しているとすると, $a_v = -a'_v$ でなくてはならないことは上と同様である. $\langle S \rangle$ は連結であるから, 結果的に $\sum_v a_v I_v = 0$ ならば $a_v = 0$ $(\forall v \in S)$ となり, I の行空間の次元は $|S|$ になる. よって $Ix = 0$ の解空間の次元は $|E_S| - |S|$ となる. **[証明終]**

注意 3. $\langle S \rangle$ が連結でない時はその連結成分を $C_1, \ldots, C_k$ とし, それぞれの S-matching polytope を P_{C_i} とすると $P_S = P_{C_1} \times P_{C_2} \times \cdots \times P_{C_k}$ となる. よってその次元は

$$\dim P_S = \sum_{i=1}^{k} \dim P_{C_i}$$

となる.

系 3.1. *induced subgraph* $\langle S \rangle$ が *bipartite* であり, 任意の $v \in S$ の次数が定数 k であるとする. この時 P_S は *codegree* k の *Gorenstein polytope* になる.

[証明] Beck-Haase-Sam[2] と同様である. 即ち定理 5 より $x \in \mathbb{R}^{E_S}$ に対して, $x \in tP_S^\circ$ である必要十分条件は $(1'')$ $x_e > 0$ $(\forall e \in E_S)$, $(2'')$ $\sum_{v \in e} x_e = t$ $(\forall v \in S)$ となる. $(1'')$, $(2'')$ により, $t < k$ に対して tP_S° 内に格子点は存在せず, $\mathbf{1} \in \mathbb{R}^{E_S}$ は kP_S° の唯一の格子点である. よって $L_{P_S}(k) = 1$.

$\iota : \mathbb{R}^{E_S} \longrightarrow \mathbb{R}^{E_S}$: $\iota(y) = y + \mathbf{1}$ を考える. 任意の $v \in S$ の次数が定数 k であるので条件 (2), $(2'')$ に出てくる変数の数は常に k である. よって $y \in tP_S \cap \mathbb{Z}^{E_S}$ に対して,

$$\sum_{v \in e} \iota(y)_e = \sum_{v \in e} (y_e + 1) = t + k$$

となり $\iota(x) \in (t+k)P_S \cap \mathbb{Z}^{E_S}$ が解る. 逆に $x \in (t+k)P_S^\circ \cap \mathbb{Z}^{E_S}$ とすると $x_e \geq 1$ であるから $\iota^{-1}(x)_e = x_e - 1 \geq 0$. また

$$\sum_{v \in e} \iota^{-1}(x)_e = \sum_{v \in e} (x_e - 1) = t + k - k = t$$

であるので $\iota^{-1}(x) \in tP_S \cap \mathbb{Z}^{E_S}$.

以上より ι は $tP_S \cap \mathbb{Z}^{E_S}$ から $(t+k)P_S \cap \mathbb{Z}^{E_S}$ への一対一対応を与えることが解る. よって $L_{P_S}(t) = L_{P_S^\circ}(t+k)$ であり, P_S は Gorenstein である. **[証明終]**

注意 4. Ohsugi-Hibi[9], Sullivant[12] の結果と Athanasiadis-Bruns-Römer[1], [4] の結果を結びつけることにより, 系 3.1 の S-matching polytope は compressed Gorenstein polytope であり, h^*-多項式の係数は unimodal であることが解る, 即ちある j が存在して $h_0 \leq \cdots \leq h_{j-1} \leq h_j \geq h_{j+1} \geq \cdots \geq h_s$ が成り立つ.

例 1. Beck-Haase-Sam[2] により, 大きい m,n に対して $P(m,n)$ は Gorenstein ではない. 一方 Grid graph $G=G(m,n)=(V,E)$ に対して

$$S:=\{(i,j)\mid 1\le i\le m-2,\ 1\le j\le n-2\}\subset V$$

とおくと, 明らかに $\langle S\rangle$ は bipartite であり, S の任意の点は次数 4 を持っている. よって系 3.1 より S-matching polytope P_S は codegree 4 の Gorenstein polytope になる. またその次元は命題 3.1 より, $|E_S|-|S|=mn-m-n$ となる.

系 3.2. $G=(V,E)$ をグラフ, $S\subset V$, $|S|$ は奇数とする. もし $\langle S\rangle$ が *bipartite* であるならば, 次が成り立つ: $t\in\mathbb{R}_{\ge 0}$, $x\in\mathbb{R}^E_{\ge 0}$ に対して,

$$\sum_{v\in e}x_e=t\ (\forall v\in S)\implies\sum_{e\in C(S,S')}x_e\ge t.$$

[証明] 射影を考えることにより $x\in\mathbb{R}^{E_S}_{\ge 0}$ としてよい. $\sum_{v\in e}x_e=t\ (\forall v\in S)$ であるので定理 5 より $x\in tP_S$. P_S の頂点は matching M で $S\subset M$ であるものに対する特性ベクトルになっている. S は奇数濃度をもつので M は必ず S の外に出る. よって特性ベクトル χ_M は $\sum_{e\in C(S,S')}(\chi_M)_e\ge 1$ を満たす. よって任意の点 $x\in P_S$ が $\sum_{e\in C(S,S')}x_e\ge 1$ を満たす. 特に $x\in tP_S$ に対して $\sum_{e\in C(S,S')}x_e\ge t$. **[証明終]**

参考文献

[1] C. A. Athanasiadis, Ehrhart polynomials, simplicial polytopes, magic squares and a conjecure of Stanley, *J. Reine Angew. Math.* **583** (2005), 163-174.

[2] M. Beck, C. Haase and Steven V. Sam, Grid graphs, Gorenstein polytopes, and Domino Stackings, preprint at http://arxiv.org/abs/0711.4151.

[3] M. Beck and S. Robins, *Computing the Continuous Discretely*, Springer, 2006.

[4] W. Bruns and T. Römer, h-vectors of Gorenstein polytopes, *J. Combin. Theorey Ser. A* **114** (2007), 165-176.

[5] J. Edmond, Maximum matching and a polyhedron with $(0,1)$-vertices, *J.Res.Nat.Bur. Standards* **69B**(1965), 125-130.

[6] E. Ehrhart, Sur les polyédres rationnels homothétiques á n dimensions, *C.R. Acad. Sci. Paris*, 254: 616-618, 1962.

[7] M. Grötschel, L. Lovász and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, 1988.

[8] T. Hibi, *Algebraic Combinatorics on Convex Polytopes*, Carslaw, 1992.

[9] H. Ohsugi and T. Hibi, Convex polytopes all of whose reverse lexicographic initial ideals are square free, *Proc. Amer. Math. Soc.* **129** (2001), 2541-2546.

[10] H. Ohsugi and T. Hibi, Special simplices and Gorenstein toric rings, *J. Combin. Theory Ser. A* **113** (2006), no.4, 718-725.

[11] R.P. Stanley, *Combinatorics and Commutative Algebra*, second ed., Progr. Math., vol. 41, Birkhäuser, Basel, 1996.

[12] S. Sullivant, Compressed polytopes and statistical disclosure limitation, *Tohôku Math. J.* (2) **58** (2006) 433-445.

[13] S. Vempala, lecture note on perfect matching polytopes, available at http://www-math.mit.edu/ vempala/18.433/L5.pdf

On spherical designs obtained from standard realization of association schemes

HIROTAKE KURIHARA

Graduate School of Mathematics Kyushu University
Hakozaki 6-10-1 Higashi-ku Fukuoka, 812-8581 Japan
ma207004@math.kyushu-u.ac.jp

1 Introduction

Let $S^{d-1} = \{(x_1, x_2, \ldots, x_d) \in \mathbb{R}^d \mid x_1^2 + x_2^2 + \cdots + x_d^2 = 1\}$ be the d-dimensional unit sphere in $\mathbb{R}^d$, endowed with the inner product $\langle\ ,\ \rangle$. The concept of spherical designs was introduced by Delsarte-Goethals-Seidel[2] in 1977.

Definition 1.1. $X \subset S^{d-1}$ is a non-empty finite set. Let t be a positive integer. X is called a *spherical t-design* if

$$\frac{1}{|S^{d-1}|}\int_{S^{d-1}} f(\xi)d\xi = \frac{1}{|X|}\sum_{\xi \in X} f(\xi)$$

holds for all polynomial $f(x) = f(x_1,\ x_2,\ \ldots,\ x_n)$ of degree at most t.

t is called a *strength* of X if the maximal value of t for which of X is a t-design.

In other words, if finite set X is a spherical t-design then X can give approximation to the sphere with respect to the integral of polynomial of degree at most t.

We shall take up crystal lattices in nature. Crystal lattices excel in symmetry and periodicity. Through the internal forces binding two atoms in a crystal, the atoms are placed in equilibrium. We can regard a crystal lattice as an infinite graph embedded in a Euclidean space, whose vertices and edges are the atoms and the internal forces binding two atoms respectively. Since a crystal lattice is periodical, there exists fundamental patterns in the crystal lattice and its quotient graph is finite. Now we consider the edges in the quotient graph embedded in a Euclidean space, we obtain a set of finite vectors. The *building block* $B(\Gamma)$ is such a set of finite vectors obtained from the quotient graph Γ .

Example 1.2. Let $\mathrm{M}(k)$ be a graph consisting of 2 vertices and k multiple edges joining them. Figure 1 represent $\mathrm{M}(3)$ and its the standard realization.

We have $B(\mathrm{M}(3)) = \{(0, \pm\frac{2}{\sqrt{6}}), (\pm\frac{1}{\sqrt{2}}, \pm\frac{1}{\sqrt{6}}), (\pm\frac{1}{\sqrt{2}}, \mp\frac{1}{\sqrt{6}})\}$, namely $B(\mathrm{M}(3))$ is a set of vertices of a hexagon.

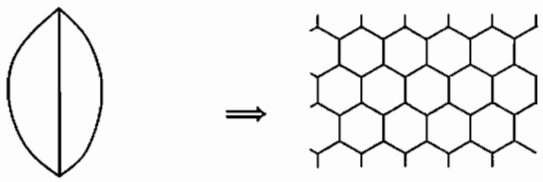


Figure 1: M(3) and its the standard realization

We consider similarities between the balanced configuration of the atoms of a crystal and a spherical design. Generally speaking, a building block, does not always have the same norm. Hence we get the following result by the assumption that building block have the same norm and the realization is non-degenerate. The realization is called *non-degenerate* if the realization is injective and direction of the realization is injective.

Theorem 1.3. *Let $\Gamma = (V, E)$ be a connected graph. $B(\Gamma)$ is the building block of Γ. If the realization is non-degenerate and the vectors in $B(\Gamma)$ have the same norm, then the set of normalized vectors of $B(\Gamma)$ is the spherical 3-design. Moreover, the strength of $B(\Gamma)$ is three except $\Gamma = \mathrm{M}(3)$.*

For Theorem 1.3, it is the problem what graph give the building block having the same norm. In fact, there exist the graphs satisfied with the assumption of Theorem 1.3. As the part of answer, we give the following theorem:

Theorem 1.4. *Let $\Gamma = (V, E)$ be a finite graph. If Γ is edge-transitive, then the elements in the building block of Γ have the same norm.*

An edge-transitive graph is a graph such that any two edges are equivalent under some element of its automorphism group. For definition of an edge-transitive graph, Theorem 1.4 is a straight result. Next, we consider the following question: Is there the graph whose building block has the same norm except edge transitive graphs? Theorem 1.5 is a part of answer of the above question and the main theorem in this paper.

Theorem 1.5. *Let $\mathfrak{X} = (X, \{R_i\}_{0 \le i \le s})$ be a symmetric association scheme of class s. If $\Gamma = (X, R_i)$ is a connected graph, then the elements in the building block of Γ have the same norm.*

We give the definition and properties of a association scheme. For detail of properties, we refer to Bannai-Ito[1].

Definition 1.6. Let X be a finite set and let R_i $(i = 0, 1, \ldots, s)$ be subsets of $X \times X$ with the property that

1. $R_0 = \{(x, x) | x \in X\}$.
2. $X \times X = R_0 \cup R_1 \cup \cdots \cup R_s$, $R_i \cap R_j = \emptyset$ if $i \neq j$.

3. ${}^tR_i = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$, where ${}^tR_i = \{(x, y) \,|\, (y, x) \in R_i\}$.

4. For any $i, j, k \in \{0, 1, \ldots, s\}$ and $(x, y) \in R_k$, $|\{z \in X \,|\, (x, z) \in R_i, (z, y) \in R_j\}|$ is constant and do not depend on $(x, y) \in R_k$. $p^k_{i,j}$ denotes $|\{z \in X \,|\, (x, z) \in R_i, (z, y) \in R_j\}|$, the number $p^k_{i,j}$ is called an *intersection number.*

Such a configuration $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq s})$ is called a *commutative association scheme* of class s on X. Moreover if an association scheme with the additional property $i = i'$ for every $i \in \{0, 1, \ldots, s\}$, then this association scheme is called *symmetric* association scheme.

2 Standard realizations

In this section, we observe on the theory of crystal lattices. For the details, we refer [4, 5].

We introduce some symbols of a graph for a explain of a standard realization. Let $\Gamma = (V, E)$ be a finite graph with a set V of vertices and a set E of all oriented edges. For an edge $e \in E$, let $o(e)$ and $t(e)$ denote the *origin* and *terminus* of e respectively. The *inverse* edge of e be denoted by $\bar{e}$. For a vertex $x \in V$, we put $E_x = \{e \in E \mid o(e) = x\}$. When we give Γ a direction, E^o denotes the set of given directed edges. We put $|V| = n$ and $|E^o| = m$. Then, we remark $|E| = 2m$.

We first define a crystal lattice. Let $\widetilde{\Gamma}$ be a graph and $\mathrm{Aut}(\widetilde{\Gamma})$ means the automorphism group of $\widetilde{\Gamma}$. $\widetilde{\Gamma}$ is called a *d-dimensional crystal lattice* if $\widetilde{\Gamma}$ holds the following properties:

1. $\mathrm{Aut}(\widetilde{\Gamma})$ have a sub group L that is isomorphism to $\mathbb{Z}^d$,

2. L operate freely on $\widetilde{V}$ and the set of undirect edges of $\widetilde{\Gamma}$,

3. A graph $\Gamma = (V, E)$ is a finite graph, where $V = \widetilde{V}/L$ and $E = \widetilde{E}/L$. The graph $\Gamma = (V, E)$ is called a *fundamental finite graph.*

Next, we give a method of a realization of a crystal lattice into Euclidean space $\mathbb{R}^d$. A map $\Phi : \widetilde{V} \to \mathbb{R}^d$ is called a *periodic realization* about L of a crystal lattice $\widetilde{\Gamma}$ if Φ holds the following properties:

1. There exists an injective homomorphism $\rho : L \to \mathbb{R}^d$ such that $\Phi(gx) = \Phi(x) + \rho(g)$ for any $x \in \widetilde{V}$ and $g \in L$,

2. $\rho(L)$ is a discrete subgroup in $\mathbb{R}^d$, and the maximal rank of $\rho(L)$ is equal to d.

For a periodic realization Φ of a crystal lattice, we define a map v from $\widetilde{E}$ to $\mathbb{R}^d$ as $v(e) = \Phi(t(e)) - \Phi(o(e))$. Since v is invariant about the operator of L as a function on $\widetilde{E}$, we regard v as a function on E. $\{v(e)\}_{e \in E}$ determines completely the periodic realization Φ. The system vectors $\{v(e)\}_{e \in E}$ is called a

building block of the periodic realization Φ. We remark that a building block is antipodal about $0 \in \mathbb{R}^d$.

We construct a crystal lattice whose fundamental finite graph is a given finite graphs. Let $C_0(\Gamma, \mathbb{R})$ and $C_1(\Gamma, \mathbb{R})$ be the set of $\mathbb{R}$-linear combination of V and E respectively. About $C_1(\Gamma, \mathbb{R})$, we request $\bar{e} = -e$ for $e \in E$.

We define the boundary operator $\partial : C_1(\Gamma, \mathbb{R}) \to C_0(\Gamma, \mathbb{R})$ as $\partial(e) = t(e) - o(e)$. Let $H_1(\Gamma, \mathbb{R})$ be the kernel of ∂. In this sense, $H_1(\Gamma, \mathbb{R})$ is called a *first homological group*. Then $\dim H_1(\Gamma, \mathbb{R})$ is equal to $1 - n + m$, we put $d = \dim H_1(\Gamma, \mathbb{R})$.

For a closed path $c = (e_1, \ldots, e_i)$ of Γ, $e_1 + \cdots + e_i \in C_1(\Gamma, \mathbb{Z})$ is represented by the identical symbol c. Since $\partial c = 0$, we have $c \in H_1(\Gamma, \mathbb{Z})$. Conversely, every elements of $H_1(\Gamma, \mathbb{Z})$ are given as $e_1 + \cdots + e_i$ obtained from a closed path.

For $e, e' \in E$, We set a inner product as

$$e \cdot e' = \begin{cases} 1 & \text{if } e = e', \\ -1 & \text{if } \bar{e} = e', \\ 0 & \text{otherwise.} \end{cases}$$

Then $C_1(\Gamma, \mathbb{R})$ is induced the inner product, a direction E^o of Γ is an orthonormal basis of $C_1(\Gamma, \mathbb{R})$.

We restrict this inner product within $H_1(\Gamma, \mathbb{R})$. For a surjective homomorphism $\mu : H_1(\Gamma, \mathbb{Z}) \to L$, let W denotes the subspace spanned by $\ker \mu$ in $H_1(\Gamma, \mathbb{R})$. And we set H the intersection space $W^{\perp} \cap H_1(\Gamma, \mathbb{R})$. The dimension of H is d, we can regard H as a Euclidean space $\mathbb{R}^d$ when we choose an orthonormal basis of H. We remark $H = H_1(\Gamma, \mathbb{R})$ in the case where $L = H_1(\Gamma, \mathbb{Z})$.

Let $P : C_1(\Gamma, \mathbb{R}) \to H$ be an orthogonal projection. For $e \in E$, We set $P(e) = v(e)$. Thus, we obtain a periodic realization with the building block $\{v(e)\}_{e \in E}$. The periodic realization obtained from the above construction holds the following conditions: For every $x \in V$, and every $\xi \in \mathbb{R}^d$,

$$\sum_{e \in E_x} v(e) = 0, \tag{2.1}$$

$$\sum_{e \in E} \langle v(e), \xi \rangle^2 = 2\langle \xi, \xi \rangle, \tag{2.2}$$

It is known that a periodic realization holding the above conditions is the unique up to similar transform. This realization is called a *standard realization*. As the following, a standard realization means a standard realization with $L = H_1(\Gamma, \mathbb{Z})$. In addition, such a building block $\{v(e)\}_{e \in E}$ is denoted by $B(\Gamma)$.

3 Proof sketch of Theorem 1.5

We first give some symbols before the proof. Let $\Gamma = (V, E^o)$ be an oriented graph. We index the vertices and the edges as $V = \{x_1, x_2, \ldots x_n\}$ and $E^0 =$

$\{e_1, e_2, \dots e_m\}$. For $1 \leq \alpha \leq m$, we set $e_\alpha = {}^t(0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{R}^m$ with 1 in the α-th place. We regard $C_1(\Gamma, \mathbb{R})$ as m-dimensional Hermitian space with an orthonormal basis $\{e_\alpha \mid e_\alpha \in E^o\}$. For $1 \leq \beta \leq n$, we put $d_\alpha = \mathrm{cut}(\{x_\beta\}, X \setminus \{x_\beta\}) \in H_1(\Gamma, \mathbb{Z})^\perp$. We define a *incidence matrix* of Γ about the orientation as $D = {}^t(d_1, d_2, \dots, d_n)$, which size is $n \times m$.

Lemma 3.1. *If Γ is a simple and k-regular graph, then $D{}^tD = kI_n - A$.*

Take a graph $\Gamma = (X, R_i)$ of $\mathfrak{X}$. We set that $A = A_i$ and $k = k_i$ for brevity. We fix $x \in X$, and put $x = x_1$. Let $e_1, e_2, \dots, e_k$ be the edges with the origin x_1. Let $x_2, x_3, \dots, x_{k+1}$ be the vertices as the terminal $e_1, e_2, \dots, e_k$ respectively. We prove that $v(e_\alpha)$ have the same norm for $1 \leq \alpha \leq k$.

The set $\{d_2, d_3, \dots, d_n\}$ is a basis of $H_1(\Gamma, \mathbb{R})^\perp$. Let $P' : C_1(\Gamma, \mathbb{R}) \to H_1(\Gamma, \mathbb{R})^\perp$ be an orthogonal projection. For $e \in E$, We set $P'(e) = \boldsymbol{u}(e)$. Since $1 = \|\boldsymbol{u}(e)\| + \|\boldsymbol{v}(e)\|$ for any $e \in E$, it suffices to show that $\boldsymbol{u}(e_\alpha)$ have the same norm for $1 \leq \alpha \leq k$.

Let B denote the matrix which remove the first low and the first column from A. Namely, B is the adjacency matrix of the graph $\Gamma \setminus \{x_1\}$.

Lemma 3.2. *For $\alpha, \beta \in \{1, 2, \dots k\}$, we have $\boldsymbol{u}(e_\alpha) \cdot \boldsymbol{u}(e_\beta) = (kI_{n-1} - B)^{-1}_{\alpha,\beta}$.*

Lemma 3.3. $(kI_{n-1} - B)^{-1} = \sum_{l=0}^{2s-1} a_l B^l \quad (a_l \in \mathbb{R})$

We have finished the preparations for a proof of Theorem 1.5. For Lemma 3.2 and 3.3, we have $\|\boldsymbol{u}(e_\alpha)\|^2 = \sum_{l=0}^{2s-1} a_l (B^l)_{\alpha,\alpha}$ for $1 \leq \alpha \leq k$.

We consider $(\alpha+1, \alpha+1)$-entry of A^l:

$$A^l_{\alpha+1,\alpha+1} = \sum_{\nu_1=1}^{n} \sum_{\nu_2=1}^{n} \cdots \sum_{\nu_{l-1}=1}^{n} A_{\alpha+1,\nu_1} A_{\nu_1,\nu_2} \cdots A_{\nu_{l-1},\alpha+1}.$$

We separate the summation on the right hand side into two terms T_1 and T_2. One of term T_1 is the summation where each indexes $\nu_1, \nu_2, \dots, \nu_{l-1}$ run from 2 to n:

$$T_1 = \sum_{\nu_1=2}^{n} \sum_{\nu_2=2}^{n} \cdots \sum_{\nu_{l-1}=2}^{n} A_{\alpha+1,\nu_1} A_{\nu_1,\nu_2} \cdots A_{\nu_{l-1},\alpha+1},$$

the other of term T_2 is the summation where not less than one indexes are equal to 1:

$$T_2 = \sum_{\nu_1 \text{ or } \nu_2 \text{ or } \dots \text{ or } \nu_{l-1} = 1} A_{\alpha+1,\nu_1} A_{\nu_1,\nu_2} \cdots A_{\nu_{l-1},\alpha+1}.$$

Then T_1 coincide with $B^l_{\alpha\,\alpha}$. Furthermore, let Y_p denote the set $\{(s_1, s_2, \dots, s_p) \in \mathbb{N}^p \mid s_1 + s_2 + \cdots + s_p = l\}$, T_2 coincide with

$$\sum_{p=2}^{l} \sum_{(s_1,s_2,\dots,s_p) \in Y_p} (A^{s_1})_{\alpha+1,1} (A^{s_2})_{1,1} \cdots (A^{s_{p-1}})_{1,1} (A^{s_p})_{1,\alpha+1}.$$

Since $(x_1, x_{\alpha+1}) \in R_i$ $(1 \leq \alpha \leq k)$ and $\mathfrak{X} = (X, \{R_i\}_{0 \leq i \leq s})$ is a symmetric association scheme, $(A^{s_1})_{\alpha+1,1} = (A^{s_p})_{1,\alpha+1}$ does not depend on α. Hence,

$B^l_{\alpha,\alpha} = A^l_{\alpha+1,\alpha+1} - T_2$ have the same value for $1 \leq \alpha \leq k$. This fact means that $\boldsymbol{u}(e_\alpha)$ have the same norm for $1 \leq \alpha \leq k$. For the connectedness of Γ, the vector $\boldsymbol{v}(e)$ for every $e \in E$ have the same norm.

4 Examples

We introduce some spherical designs obtained from the standard realization.

Example 4.1. We give designs from strongly regular graphs. It is known that a strongly regular graph determine a association scheme of class 2 with a relation of the distance. Let $\Gamma = (V, E)$ be a strongly regular graph with a parameter (n, k, λ, μ). We set $X = V$ and $R_i = \{(x, y) \in X \times X \mid d(x, y) = i\}$ for $i \in \{0, 1, 2\}$, Then $(X, \{R_0, R_1, R_2\})$ is a symmetric association scheme of class 2.

As the following, $\boldsymbol{v}(e)$ means the normalized vectors of $\boldsymbol{v}(e)$, for short. We have the inner product set $A(B(\Gamma)) =$

$$\{0, \pm\frac{k}{\mu((k-2)n+2)}, \pm\frac{2k}{\mu((k-2)n+2)}, \pm\frac{\mu n - \mu - k}{\mu((k-2)n+2)}, \pm\frac{n-1}{(k-2)n+2}, -1\}.$$

Therefore $B(\Gamma)$ is at most 10-distance set. Especially, for Γ is a strongly regular graph with a parameter $(n, k, 0, 1)$, namely a Moore graph, $B(\Gamma)$ is 6-distance set.

Example 4.2. There exist some graphs whose building block having the same norm as in Figure 2. This graph is a neither edge-transitive nor strongly regular graph. All either edge-transitive nor strongly regular graphs with at most 9 vertices are classified [3].

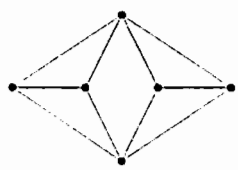


Figure 2: neither edge-transitive nor strongly regular graph

We have not finished the classification the graphs whose building block having the same norm yet. It is important problem for characterization of the standard realization to classify the graphs whose building block having the same norm.

Acknowledgment

The author thanks Professor Eiichi Bannai for suggesting these problems as a master course project for me.

References

[1] E. Bannai and T. Ito, *Algebraic combinatorics I. association schemes*, The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.

[2] P. Delsarte, JM Goethals, and JJ Seidel, *Spherical codes and designs*, Geom. Dedicata **6** (1977), no. 3, 363–388.

[3] J. Shigezumi, *A construction of spherical designs from finite graphs with the theory of crystal lattice*, [arXiv:0804.2956[math.CO]] (2008).

[4] T. Sunada, *Why do diamonds look so beautiful? — introduction to discrete harmonic analysis — (in japanese)*, Springer Japan, 2006.

[5] ———, *Crystals that nature might miss creating*, Notices of Amer. Math. Soc. **55** (2008), 208–215.

[6] B. Venkov, *Réseaux et designs sphériques (in french)*, Réseaux euclidiens, designs sphériques et formes modulaires **37** (2001), 10–86.

2つの球面上の堅い2-内積集合の分類

九州大学大学院数理学研究院
日本学術振興会特別研究員 DC1
野崎　寛（Hiroshi Nozaki）

1 Introduction

X をユークリッド空間 $\mathbb{R}^d$ 上の有限集合とする．$A(X) := \{(x,y) \mid x,y \in X, x \neq y\}$ を異なる X の2元の内積の集合とする．また，X の元 x について，$A(x) := \{(x,y) \mid x \neq y \in X\}$, $B(x) := \{(x,y) \mid x \neq y \in X, (x,x) \geq (y,y)\}$ と定義する．

Definition 1.1.
- $|A(X)| = s$ であるとき，X を s-内積集合（s-inner product set）と呼ぶ．
- 全ての $x \in X$ について，$|A(x)| \leq s$ であるとき，X を局所 s-内積集合（locally s-inner product set）と呼ぶ．
- 全ての $x \in X$ について，$|B(x)| \leq s$ であるとき，X を内部 s-内積集合（inside s-inner product set）であると呼ぶ．

すぐに分かるように，内部内積集合は局所内積集合の一般化，局所内積集合は内積集合の一般化である．いくつか記号を用意する．

$RS := S_1 \cup S_2 \cup \cdots \cup S_p \subset \mathbb{R}^d$ を原点中心の p 個の球とする．r_i を S_i の半径とし，$0 \leq r_1 < r_2 < \cdots < r_p$ と仮定する．$r_1 = 0$ のときは S_1 は原点になるが，それも特別な球としてみなす．$X_i := X \cap S_i$ と定義する．RS が原点を含むとき $\varepsilon_{RS} := 1$，原点を含まないとき，$\varepsilon_{RS} := 0$ と定義する．$\mathrm{P}_s(\mathbb{R}^d)$ を s 次以下の d 変数斉次多項式全体の張る線形空間とする．$\mathrm{Hom}_s(\mathbb{R}^d)$ を s 次の d 変数斉次多項式全体の張る線形空間とする．$\mathrm{Harm}_s(\mathbb{R}^d) := \{f \in \mathrm{Hom}_s(\mathbb{R}^d) \mid \Delta f = 0\}$．ここで $\Delta = \sum_{i=1}^{d} \frac{\partial^2}{\partial^2 x_i}$．$\Delta f = 0$ を満たす多項式を調和多項式と呼ぶ．$\mathrm{P}_s^*(\mathbb{R}^d) := \oplus_{i=0}^{\lfloor s/2 \rfloor} \mathrm{Hom}_{s-2i}(\mathbb{R}^d)$．ここで $\lfloor s/2 \rfloor$ は，$s/2$ を超えない最大の整数を表す．$\mathrm{P}_s(RS)$, $\mathrm{Hom}_s(RS)$, $\mathrm{Harm}_s(RS)$ と書いて，それぞれ対応する線形空間を RS 上に制限したものとする．例えば，$\mathrm{P}_s(RS) = \{f|_{RS} \mid f \in \mathrm{P}_s(RS)\}$．これら線形空間の次元はよく知られている．

Theorem 1.1 ([1, 3, 5]).

1. $\dim(\mathrm{P}_l(RS)) = \begin{cases} \varepsilon_{RS} + \sum_{i=0}^{2(p-\varepsilon_{RS})-1} \binom{d+l-i-1}{d-1}, & \text{if } l \geq 2(p-\varepsilon_{RS}) \\ \dim(\mathrm{P}_l(\mathbb{R}^d)) = \binom{d+l}{l}, & \text{if } l \leq 2(p-\varepsilon_{RS})-1, \end{cases}$

2. $\dim(\mathrm{P}_l^*(RS)) = \begin{cases} \varepsilon_{RS} + \sum_{i=0}^{(p-\varepsilon_{RS})-1} \binom{d+l-2i-1}{d-1}, & \text{if } l \text{ is even and } l \geq 2(p-\varepsilon_{RS}) \\ \sum_{i=0}^{(p-\varepsilon_{RS})-1} \binom{d+l-2i-1}{d-1}, & \text{if } l \text{ is odd and } l \geq 2(p-\varepsilon_{RS}) \\ \dim(\mathrm{P}_l^*(\mathbb{R}^d)) = \sum_{i=0}^{\lfloor \frac{l}{2} \rfloor} \binom{d+l-2i-1}{d-1}, & \text{if } l \leq 2(p-\varepsilon_{RS})-1 \end{cases}$.

内部 s-内積集合の元の個数には以下の様なFisher型の上界が示される．ここで，$-X \subset X$ を満たすとき，X を極対的であるという．

Theorem 1.2 ([9]). *1. $X \subset RS$ を p 個の同心球面上の内部 s-内積集合とする．このとき，*

$$|X| \leq \dim(\mathrm{P}_s(RS)). \tag{1.1}$$

2. $X \subset RS$ を p 個の同心球面上の極対的な内部 s-内積集合とする．このとき，

$$|X| \leq \begin{cases} 2\dim(\mathrm{P}_{s-1}^*(RS)) + \varepsilon_{RS}, & \text{if } s-1 \text{ is odd} \\ 2\dim(\mathrm{P}_{s-1}^*(RS)), & \text{if } s-1 \text{ is even and } 0 \notin X \end{cases}. \tag{1.2}$$

この上界を満たす集合を堅いと呼ぶ．堅い内部内積集合の具体例の中には，堅いEuclidean designになっている例が多数存在している [9].

Definition 1.2 (Euclidean designs [11, 2]). X を $RS \subset \mathbb{R}^d$ 上の有限集合とする．$w : X \to \mathbb{R}_{>0}$ を重み関数とする．任意の $f \in \mathrm{P}_t(RS)$ に対して，

$$\sum_{i=1}^{p} \frac{\sum_{y \in X_i} w(y)}{|S_i|} \int_{S_i} f(x) d\sigma_i(x) = \sum_{x \in X} w(x) f(x)$$

を満たすとき，(X, w) をEuclidean t-designと呼ぶ．左辺は球面 S_i 上の積分を意味しており，$\int_{S_i} d\sigma_i(x) = |S_i|$.

ここで $w(x)$ が定数関数で，$p = 1$ のとき，X は球面 t-デザインと呼ばれる．Euclidean designの元の個数について，Fisher型の上界が以下のように知られている．

Theorem 1.3 ([3, 6, 7]). *1. $X \subset RS$ を Euclidean $2e$-design とする．そのとき，*

$$|X| \geq \dim(\mathrm{P}_e(RS)).$$

2. $X \subset RS$ を Euclidean $(2e-1)$-design とする．そのとき，

$$|X| \geq \begin{cases} 2\dim(\mathrm{P}_{e-1}^*(RS)) - 1, & \text{if } e-1 \text{ is even and } 0 \in X \\ 2\dim(\mathrm{P}_{e-1}^*(RS)), & \text{otherwise} \end{cases}.$$

この上界を達成するデザインを堅いデザインと呼ぶ．極対的でないとき，とくにTheorem 1.2とTheorem 1.3は一致している．また，原点を含まないとき，極対的である場合も，一致している．堅いデザインとの関係にも注意しながら，堅い内部内積集合について考察を与える．

2 球面 S^{d-1} の場合

球面の場合，内部 s-内積集合は局所 s-内積集合であることに注意する．また，球面上の内積と距離は一対一の対応があり，局所 s-内積集合は局所 s-距離集合であることにも注意する．s を固定したときに，元の個数が最大である X を optimal な (局所)s-内積集合と定義する．$s=2, d=3$ を考えたとき，optimal な 2-内積集合（$\subset S^2$）は正四面体の辺の中点からなる 6 点である．optimal な局所 2-内積集合 ($\subset S^2$) は，正 20 面体から巧く 7 点を選ぶことで構成できる [10]．つまり，一般には optimal な s-内積集合と局所 s-内積集合は一致していない．

それでは，Fisher 型の上界を満たす局所 s-内積集合はどの様なものがあるのだろうか？堅い s-内積集合については，それが堅い球面 t-デザインであることが知られており [4]，分類も $t=4,5,7$ を除いて完了している．堅い局所内積集合も球面デザインと深く関係していることが期待され，興味深い対象であるのだが，次の結果が得られた．

Theorem 2.1 ([10]). *1.* X が堅い局所 s-内積集合であることと，X が堅い s-内積集合であることが同値．

2. X が堅い極対的な局所 s-内積集合であることと，X が堅い極対的な s-内積集合であることが同値．

この定理は，堅い局所 s-内積集合が，ウエイト付の球面 $2s$-デザインであることを示すことにより得られる．なぜなら，ウエイト付の球面デザインが Fisher 型の上界を達成するとき，ウエイトが X の元に依らない一定の値になることが知られているからだ [12]．この証明で用いられた，堅い局所内積集合と堅いウエイト付きの球面デザインとの対応の理論は非常に興味深い．

3 2つの球面の内積集合の場合

内部内積集合の分類が大きな目標であるが，それより強い条件である，内積集合の分類から試みた．s, p が小さいときには次のように分類が与えられる．

Theorem 3.1 ([9]). $d \geq 2$ において 2 つの球面上の堅い 2-または 3-内積集合は存在しない．

上の定理は非存在を示したものだが，これは Fisher 型の上界については内部内積集合が本質的な性質を持つことを意味している．この定理の証明には主に次の二つの上界を証明し用いた．

Theorem 3.2 ($\mathbb{R}^d$ 上の Rankin bound [9]). X を $\mathbb{R}^d$ 上の有限集合とする．

1. 任意の $\alpha \in A(X)$ に対して，$\alpha < 0$ が成り立つとき，$|X| \leq d+1$.

2. 任意の $\alpha \in A(X)$ に対して，$\alpha \leq 0$ が成り立つとき，$|X| \leq 2d+1$.

この上界を達成する例も簡単に見つけることが出来る．例えば，1 については regular simplex がそうであるし，2 については cross polytope に原点を加えたものがそうである．つぎの定理は球面上の absolute bound である Fisher 型の上界を本質的に改善する上界である．

Theorem 3.3 ([10]). X を球面 S^{d-1} 上の s-内積集合（s-距離集合）とする．次数 s の多項式 $F_X(t)$ を

$$F_X(t) := \prod_{\alpha \in A(X)} (t-\alpha) = \sum_{i=0}^{s} f_i G_i^{(d)}(t),$$

と定義する．ここで $f_i \in \mathbb{R}$, $G_i^{(d)}$ は $G_i^{(d)}(1) = \dim(\mathrm{Harm}_i(\mathbb{R}^d))$ と正規化された i 次 *Gegenbauer* 多項式．そのとき，

$$|X| \leq \sum_{i \text{ with } f_i > 0} h_i, \tag{3.1}$$

ここで右辺は $f_i > 0$ を満たす $0 \leq i \leq s$ についての和を意味する．

もし，すべての $1 \leq i \leq s$ について $f_i \geq 0$ かつ $f_0 > 0$ を満たすならば，Linear programming bound [4] が適用でき，良い上界が得られる:

Theorem 3.4 (Linear programming bound [4]). X を球面 S^{d-1} 上の s-内積集合（s-距離集合）とする．次数 s の多項式 $F_X(t)$ を

$$F_X(t) := \prod_{\alpha \in A(X)} (t-\alpha) = \sum_{i=0}^{s} f_i G_i^{(d)}(t),$$

と定義する．もし，$f_0 > 0$ かつ，すべての $1 \leq i \leq k$ について $f_i \geq 0$ であるならば，

$$|X| \leq \frac{F_X(1)}{f_0}.$$

しかし，ひとつでも $f_i < 0$ となる様な i が存在するならば，有効な上界は知られていなかった．Theorem 3.3 の上界を達成する例も存在しており，linear programming bound が適用できない距離集合に対して，Theorem 3.3 は有効である．$s = 2$ かつ $f_0 > 0, f_1 \leq 0, f_2 > 0$ のとき，この上界は $|X| \leq \binom{d+1}{2}$ となるが，$d \geq 7$ のとき d 次元 regular simplex の辺の中点の集合が，この上界を達成する例になっている [10, 8].

References

[1] Ei. Bannai and Et. Bannai, Algebraic Combinatorics on Spheres, Springer, Tokyo, 1999 (in Japanese).

[2] Ei. Bannai, Et. Bannai, M. Hirao, and M. Sawa: Cubature formulas in numerical analysis and Euclidean tight designs, accepted for publication, in a special issue in honor of Michel Deza (*Europ. J. Combinatorics*)

[3] P. Delsarte and J.J. Seidel, Fisher type inequalities for Euclidean t-designs, *Lin. Algebra and its Appl.* 114–115 (1989), 213–230.

[4] P. Delsarte, J.M. Goethals, and J.J. Seidel, Spherical codes and designs, *Geom. Dedicata* 6 (1977), No. 3, 363–388.

[5] A. Erdélyi et al, *Higher Transcendental Functions II*, (Bateman Manuscript Project), MacGraw-Hill, 1953.

[6] H.M. Möller, Kubaturformeln mit minimaler Knotenzahl, *Numer. Math.* 25 (1975/76), no. 2, 185–200.

[7] H.M. Möller, Lower bounds for the number of nodes in cubature formulae, Numerische Integration (Tagung, Math. Forschungsinst., Oberwolfach, 1978), 221–230, *Internat. Ser. Numer. Math.* 45, Birkhäuser, Basel-Boston, Mass., 1979.

[8] O.R. Musin, On spherical two-distance sets, preprint.

[9] H. Nozaki: Inside s-inner product sets and Euclidean design. preprint.

[10] H. Nozaki and M. Shinohara, On a generalization of distance sets.

[11] A. Neumaier and J.J. Seidel, Discrete measures for spherical designs, eutactic stars and lattices. *Nederl. Akad. Wetensch. Indag. Math.* 50 (1988), no. 3, 321–334.

[12] M.A. Taylor, Cubature for the sphere and the discrete spherical harmonic transform, *SIAM J. Numer. Math.* 32 (1995), 667–670

Random Walks on Finite Groups with Applications to Statistics

有限群上のランダムウォークと統計学への応用

吉田知行

YOSHIDA, Tomoyuki

yoshidat@math.sci.hokudai.ac.jp

2007/06/24 於北大

New Trend—(Computational) Algebraic Statistics

Application of Linear Algebra, Finite Group, Symmetric Group, Linear Group, Representation, Gröbner basis, Galois Theory, Invariant Theory, Symmetric Polynomial, Algebraic Geometry, Graph, Enumeration, etc.

Application to Biology(Phylogenetics, Evolution, DNA), Social Science, Archeology, Historical Linguistics, etc..

"Algebraic Statistics for Computational Biology", Pachter, Sturmfels(ed), Cambridge (2005)

Scatter plot of isotope of lead: Pb204, Pb206, Pb207, Pb208
Thirty two bronze mirrors of Tsubai-Otsukayama tomb.

By Plücker coordinate, Regression analysis,
(Fact 1) They are almost exactly on a (regression) plane P.
(Fact 2) There are some lines containing three points.
(Fact 3) Some simple rational dividing points (e.g.3:7, 4:7).

What does such patterns mean?—Mix of lead.
(Reason 1) These bronze has three origins X, Y, Z.
X came from northern east china. Y from Sichuan.
Probably, Z came from Gangnam region, not from Japan.
(Reason 2) Mixture of defectives.
(Reason 3) The size of a fusion reactor.

Linear Algebra, Computational geometry, Pattern recognition, Projective geometry, Error analysis.

Part I
Random Walks (RW) on a finite group(FG).
Application of group characters.
Part II
Random samplings of contingency tables.
Exact test of coincidence numbers.
Part III
Bootstrap, Binary test, symmetric semigroup.
Phylogenetic tree, perfect matching, Gelfand pair.
RW on distance regular graphs(DRG).

"Harmonic Analysis on Finite Groups", Cambridge. 2008.

Diaconis, saloff-Coste, Fulman, Kerov, Woess, Gluck.

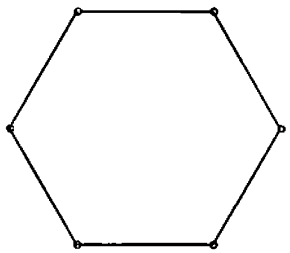
First Example

Example 1. RW on a circle $Z_m = \mathbb{Z}/m\mathbb{Z} = \{0, 1, \cdots, m-1\}$.
Start at 0. Move x to $x \pm 1$ with the same probability $1/2$.

Transition probability $p(x,y) = \begin{cases} 1/2 & x - y = \pm 1 \\ 0 & \text{else} \end{cases}$

Transition matrix $P = (p(x,y))_{x,y \in Z_m}$

$$\begin{bmatrix} 0 & 1/2 & 0 & 0 & \cdots & 1/2 \\ 1/2 & 0 & 1/2 & 0 & \cdots & 0 \\ 0 & 1/2 & 0 & 1/2 & \cdots & \\ & \ddots & \ddots & \ddots & \ddots & \\ 0 & \ddots & \ddots & \ddots & 0 & 1/2 \\ 1/2 & 0 & & 0 & 1/2 & 0 \end{bmatrix}$$



$P^n = (p^{(n)}(x,y))_{x,y}$: transition matrix at n-th step.

$$p^{(n)}(x,y) = \frac{1}{n} \sum_{z \in C_m} \cos^n \left[\frac{2\pi z}{m}\right] \cos\left[\frac{2\pi z(x-y)}{m}\right]$$

By discrete Fourier transformation,
THEOREM (Diaconis):
If m odd, $n \geq m^2$, then $\|P^n - U\|_1 \leq 2\exp\left(-\frac{\pi^2 n}{2m^2}\right)$,
If $m \geq 6$, then $\|P^n - U\|_1 \geq \exp\left(-\frac{\pi^2 n}{2m^2} - \frac{\pi^4 n}{2m^4}\right)$.

Note : $p(x) := p(0,x)$. Then $p(x,y) = p(y-x)$.
$\widehat{P} := \frac{1}{2}(g + g^{-1})$ (g generator of C_n).
$p^{(n)}(x,y) = p^{(n)}(0, y-x)$ is the coefficient of $y-x$ in $\widehat{P}^n$ in $\mathbb{C}C_n$.

Calculation of $\widehat{\mu}^n$ in $\mathbb{C}G$.

(G, μ) : Probability space on a finite group G.
Distribution $\mu : G \to \mathbb{R}$. $0 \leq \mu(x) \leq 1$, $\sum_{x \in G} \mu(x) = 1$.
$p(x,y) = \mu(x^{-1}y)$: one-step transition prob of move $x \to y$.
Start at x_0. Choose y with prob $= p(y)$, then move to $x_1 = x_0 y$. Next choose y with prob $\mu(y)$, move to $x_2 = x_1 y$, ...
We have RW $x_0 \to x_1 \to x_2 \to \cdots$. Then n-step trans.Prob.

$$\begin{aligned} p^{(n)}(x,y) &= \sum_{x_1, \cdots, x_{n-1}} p(x,x_1)p(x_1,x_2)\cdots p(x_{n-1},y) \\ &= \sum_{y_1 \cdots y_n = x^{-1}y} \mu(y_1)\cdots\mu(y_n) \\ \therefore \sum_y \mu^{(n)}(y)y &= \left(\sum_x \mu(x)x\right)^n, \quad p^{(n)}(x,y) = \mu^{(n)}(x^{-1}y). \end{aligned}$$

$\mathbb{C}G$: group algebra. For $P : G \to \mathbb{C}$, $\widehat{P} := \sum_{x \in G} P(x)x$. Then $\widehat{P}\widehat{Q} = \widehat{P * Q}$ in $\mathbb{C}G$.

$(P * Q)(x) := \sum_{y \in G} P(xy^{-1})Q(y)$: convolution product.

Conj$(G) = \{C_1, C_2, \cdots, C_r\}$: conjugacy classes. $x_i \in C_i$.
$Z(\mathbb{C}G) = \{x \in \mathbb{C}G \mid yx = xy \quad \forall y \in \mathbb{C}G\}$: center.
$Z(\mathbb{C}G)$ is the linear spans of class sums $\widehat{C_1}, \cdots, \widehat{C_r}$.
$\widehat{A} = \sum_{a \in A} a$ ($A \subset G$ identified with $A : G \to \{0,1\}$).
$\widehat{P}$ is in $Z(\mathbb{C}G) \Leftrightarrow P$ is class function (=CF), i.e.
$P(xy) = P(yx)$.

$\mathrm{Irr}(G) = \{\chi_1, \cdots, \chi_r\}$: irred. characters. $\chi_i * \chi_j = \dfrac{|G|}{\chi_i(1)}\delta_{ij}\chi_i$.

$e_{\chi_i} := \dfrac{\chi_i(1)}{|G|}\widehat{\chi_i} = \dfrac{\chi_i(1)}{|G|}\sum_{x\in G}\chi_i(x^{-1})x$:Primitive idempotents.

$e_{\chi_i}e_{\chi_j} = \delta_{ij}e_{\chi_i}, \sum_i e_{\chi_i} = 1.\ \omega_{\chi_i}(g) := \dfrac{\chi_i(g)}{\chi_i(1)}$.

$\widehat{P} = \dfrac{1}{|G|}\sum_i \chi_i(1)\,(\overline{\chi_i} * P)(g)\,g$ for $P : G \to \mathbb{C}$.

$$\boxed{\widehat{P} = \sum_i \omega_i(\widehat{P})e_{\chi_i}, \quad \therefore \widehat{P}^m = \sum_i \omega_i(\widehat{P})^m e_{\chi_i}}$$ if P is CF.

$\because \omega_{\chi_i} : Z(\mathbb{C}G) \to \mathbb{C}$ is algebra hom.

(G, μ) : prob.space on finite group G, μ : CF, $E := \mathrm{supp}(\mu)$.

$$\left(\sum_{x\in G}\mu(x)x\right)^n = \sum_{x\in G}\mu^n(x)x \text{ in } Z(\mathbb{C}G).$$

$$\mu^{(n)} = \sum_{\chi\in \mathrm{Irr}(G)}\omega_\chi(\widehat{\mu})^n e_\chi$$

$|\omega_\chi(\widehat{\mu})| \le 1$. Under $n \to \infty$,

$\mu^{(n)}$ = (Uniform term)+(Oscillation term)+(Convergence term)

$U = e_1 = \frac{1}{|G|}\sum_{g\in G} g$: uniform distribution.
O : the sum on $\chi \ne 1$ such that $|\omega_\chi(\widehat{\mu})| = 1$.
C : the sum on χ such that $|\omega_\chi(\widehat{\mu})| < 1$.

Convergence to uniform distribution U

THEOREM (Diaconis-Shahshahani 1981).
$\mu^{(n)} \to U \Leftrightarrow \langle E^{-1}E\rangle = G$.
When $t \in E$ is a conj.class, then $\Leftrightarrow [t, G] = G$.

$\rho := \mathrm{Max}\left\{\left|\dfrac{\chi(x)}{\chi(1)}\right| : x \in E, E^{-1}E \not\subseteq \mathrm{Ker}\chi\right\}$: Convergence ratio.

Convergence term $C \sim c\rho^n$.

Problem Given G, find a conj.class $E \ni x$ such that $\rho_x = \mathrm{Max}_\chi|\chi(x)/\chi(1)|$ is minimum.

S_n:symmetric group. $1 \ne x \in E$:conjugacy class.
$U = e_1$, $O = \pm e_{\mathrm{sgn}}$.
$\rho_x = \mathrm{Max}\left\{\left|\frac{\chi_\lambda(x)}{\chi_\lambda(1)}\right| : \chi_\lambda \ne 1, \mathrm{sgn}\right\}$

THEOREM. $\mathrm{Min}_{x\ne 1}\rho_x = 2/n(n-3)$.
This value is realized by $(n-1)$-cycle t_{n-1}.

$$\chi_\lambda(t_{n-1}) = \begin{cases}(-1)^b & \lambda = [a, 2, 1^{b-2}](a+b=n, 2 \le a \le n-2)\\ 0 & \text{else}\end{cases}$$

For $x = t_n$ (n-cycle), $\rho_x = 1/(n-1)$
For $x = t_2$ (transposition), $\rho_x = 1 - 2/(n-1)$. Very slow.
By Frobenius, $\lambda = 1^{\mu_1}2^{\mu_2}\cdots n^{\mu_n}$,

$$\frac{\chi_\lambda(t_2)}{\chi(1)} = \frac{1}{n(n-1)}\sum_i i^2(\mu_i - \mu_i')$$

Data set

Two dimensional Data Set $[f,g]$, where $f : N \to I, g : N \to J$.
$N = \{1,2,\cdots,n\}$: the set of observations, the set of persons.
I, J: the sets of categories.
$X[f,g] := \left(|f^{-1}(i) \cap g^{-1}(j)|\right)_{i\in I, j\in J}$ (Contingency Table, C-tab).
$X[f] := \left(|f^{-1}(i)|\right)_{i\in I}$: marginal distribution.

$X[f] = X[f'] \Leftrightarrow [f] \sim [f']$, i.e. $\exists \pi \in S_n; f' = f\pi$
$X[f,g] = X[f',g'] \Leftrightarrow [f,g] \sim [f',g']$, i.e., $\exists \pi \in S_n; f' = f\pi, g' = g\pi$.

$S_f := \{\pi \in S_n \mid f\pi = f\}$ Young subgroup.
$|S_f| = \prod_i |f^{-1}(i)| = \prod_i x_{i+}$, $x_{i+} := \sum_j x_{ij}$
marginal distribution
$X[f] = (|f^{-1}(i)|)_i = (x_{i+}), X[g] = (|g^{-1}(i)|)_j = (x_{+j})$
$\sharp\{(f,g) \mid X[f,g] = (x_{ij})\} = n! \Big/ \prod_{ij} x_{ij}!$
$\sharp\{(f,g) \mid X[f] = (a_i), X[g] = (b_j)\} = n!^2 \Big/ \prod_i x_{a_i}! \prod_j b_j!$
$\mathbf{H(x)} = \mathbf{Prob}(X[f,g] = (x_{ij}) \mid x_{i+} = a_i, x_{+j} = b_j)$

$$= \prod_i x_{i+}! \prod_j x_{+j}! \Big/ n! \prod_{ij} x_{ij}!$$

Multiply Hypergeometric distribution(MHGD)

Given marginal distribution $a = (a_i), b = (b_j)$.
$\mathbf{DS}_n(a,b)$: the set of data set,
$\Omega_n(a,b)$: the set of C-tab's.
Canonical surjective map $X : \mathbf{DS}_n(a,b) \longrightarrow \Omega_n(a,b)$.
Take any $[f,g] \in \mathbf{DS}_n(a,b)$.

THEOREM: S_n transitively acts on $\mathbf{DS}_n(a,b)$

THEOREM: RW on (S_n, U) induces a RW on $(\Omega_n(a,b), MHGD)$

$$S_n \longrightarrow \Omega_n(a,b); \pi \longmapsto X[f, g\pi]$$

Coincidence number of C-tab

$N = \{1,2,\cdots,n\}$.
Data set $[f, g : N \to \Lambda]$, C-Tab $X = X[f,g]$,
$a = (a_\lambda) = X[f]$, $b = (b_\lambda) = X[g]$.
$x_0[f,g] := \mathrm{Tr}(X) = \sharp\{i \in N \mid f(i) = g(i)\}$
$x_0(\pi) := x_0[f, g\pi]$. $G \leq S_n$ **transfer**

THEOREM $m = E_{\pi\in G}[x_0(\pi)] = \dfrac{1}{n}\displaystyle\sum_\lambda a_\lambda b_\lambda$

COR. $E_\pi\left[\binom{x_0(\pi)}{t}\right] = \dfrac{(n-t)!}{n!} \displaystyle\sum_{\sum t_\lambda} \prod_\lambda \binom{a_\lambda}{t_\lambda}\binom{b_\lambda}{t_\lambda} t_\lambda!$

Exact P-value of coincidence numbers

$$F_{a,b}(z) = {}_2F_0(-a,-b;z) = \sum_{k\geq 0}\binom{a}{k}\binom{b}{k}k!\,z^k$$

$$F(z) := \prod_{\lambda} F_{a_\lambda,b_\lambda}(z) = \sum_{k\geq 0}\binom{n}{k}k!q(k)\,z^k$$

$q(0) = 1, q(1) = m$ ↘hen P-value

$$P(r) := \mathbf{Prob}(x_0(\pi) \geq r) = \frac{1}{n!}\sharp\{\pi \in S_n \mid x(\pi) \geq r\}$$

THEOREM: $\displaystyle\sum_{k\geq 1} P(k)\,z^{k-1} = \sum_{k\geq 1} q(k)\,(z-1)^{k-1}$

Higher dimensional C-Tab is difficult

Markov chain Monte-Carlo(MCMC) method — RW by transposition. Convergence is slow.

$\Omega_n(a,b) \cong S_f\backslash S_n/S_g \cong S_n^{\Delta}\backslash(S_n \times S_n)/(S_f \times S_g)$

$[f : N \to I, g : N \to J, h : N \to K]$ **: 3-dim C-tab.**

$\Omega_n(a,b,c) \cong S_n^{\Delta}\backslash(S_n \times S_n \times S_n)/(S_f \times S_g \times S_h)$

Given $\alpha,\beta,\gamma \in S_n$, **Enumerate** $\sigma,\tau,\rho \in S_n$ **s.t.**

$$\begin{cases} f\sigma = f\alpha, & f\sigma = f\gamma \\ g\tau = g\beta, & g\tau = g\alpha, \\ h\rho = h\beta, & h\rho = h\gamma \end{cases} \therefore \begin{cases} \alpha \in S_f\sigma \cap S_g\tau \\ \beta \in S_g\tau \cap S_h\rho \\ \gamma \in S_h\rho \cap S_f\sigma \end{cases} \therefore \begin{cases} S_f\sigma = S_f\alpha = S_f\gamma \\ G_g\tau = S_g\beta = S_g\alpha \\ S_h\rho = S_h\beta = S_h\gamma \end{cases}$$

Application: Japanese-Korean languages.

Λ **: set of head sounds,**

$f(i)$ $(g(i))$ **head of** i**-th word in Japanese (Korean).**

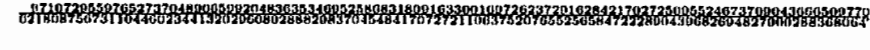
$f, g : N \longrightarrow \Lambda$, $a_\lambda := |f^{-1}(\lambda)|, b_\lambda := |g^{-1}(\lambda)|$.

$$F(u) := \prod_{\lambda}\left\{\sum_{k\geq 0}\begin{pmatrix} a_\lambda \\ k \end{pmatrix}\begin{pmatrix} b_\lambda \\ k \end{pmatrix}k!\,u^k\right\} = \sum_{k\geq 0}\begin{pmatrix} n \\ k \end{pmatrix}k!\,q(k)\,u^k$$

$$p(x) = \sum_{k\geq x}(-1)^{k-x}\begin{pmatrix} k \\ x \end{pmatrix}q(k)$$

$P(x \geq x_0) = p(x_0) + p(x_0+1) + \cdots + p(n)$.

Japanese and Korean: $x_0 = 53$. $P(x \geq 53) =$



$P(x \geq 53) = 0.00156169$**(exact),** 0.000554 **(normal),** 0.00238 **(binomial)**

Appendix—Exact χ^2-test of independence

$X = (x_{ij})$: $I \times J$-C.Tab **s.t.** $x_{i+} = a_i, x_{+j} = b_j, x_{++} = n$: **given.**

$f : N \to I, g : N \to J$, $|N| = n$.

Occupancy probability $H(X) = \dfrac{\prod_i a_i!\prod_j b_j!}{n!\prod_{i,j} x_{ij}!}$

Exact probability Prob $\left(\chi^2(X) := \sum_{i,j}\frac{(x_{ij}-a_ib_j/n)^2}{a_ib_j/n} \geq x\right)$**?**

Prob $\left(\sum_{i,j}\left(\prod_{i'\neq i}a_{i'}\right)\left(\prod_{j'\neq j}b_{j'}\right)x_{ij}^2 = x\right)$ **?**

$$\Sigma[f,g] := \sum_{ij} = \sharp\left\{\begin{pmatrix} s & i \\ t & j \end{pmatrix}\middle|\begin{array}{l} s : I \to N, fs = 1, gsi = j \\ t : J \to N, gt = 1, ftj = i \end{array}\right\}$$

♯ of 2-cycles in bipartite graph with $V = I \cup J, E = N$.

$$\mathbf{Prob} = \frac{1}{n!}\sum_{\pi in S_n}\Sigma[f,g\pi] = ?, \quad \sharp\{\pi \in S_n \mid g\pi t = 1, g\pi si = j\} = ?$$

Appendix—Categorical view point

$[h : N \to K], [h' : N \to K]$: Data sets. $\mathsf{tab}[h] := (|h^{-1}(k)|)_{k \in K}$

$\boxed{\mathsf{tab}[h] = \mathsf{tab}[h'] \Longleftrightarrow \exists \pi \in \mathsf{Sym}(N); h' = h\pi}$

(Proof of $\Rightarrow$)
set: Category of finite set.
set/K: Comma cat (object $A \to K$).
Connected object $k_* : \{*\} \to K$ $(* \mapsto k \in K)$.
$\mathsf{Hom}(k_*, h) \cong h^{-1}(k)$. $\therefore |\mathsf{Hom}(k_*, h)| = |\mathsf{Hom}(k_*, h')|$. $\therefore h \cong h'$.

- **Yoneda-like lemma : $X \cong Y \Leftrightarrow |\mathsf{Hom}(I, X)| = |\mathsf{Hom}(I, Y)|$.**
- **Burnside homomorphism $\varphi : \Omega(G) \to \tilde{\Omega}(G)$ is injective.**

Categorical version of average formula

$\mathcal{E}$:Locally finite topos (e.g. set^G for f.group G).
C:Normal connected object, i.e. $\mathsf{Aut}(C)$ acts transitively on $\mathsf{Hom}(I, C)$ for any connected I, e.g., a progenerator, and G/N in set^G for $N \leq G$ normal.
$N \cong mC$ $(m \geq 1)$, $f, g : N \to L$. $\mathbf{Eq}(\pi) \subseteq N$ equalizer of $f, g\pi$,
$x_I(\pi) := |\mathsf{Hom}(I, \mathbf{Eq}(\pi))|$ (coincidence number). $P(f, g)$ pullback of f, g. I connected and $\mathsf{Hom}(I, C) \neq \emptyset$.

$$\boxed{\textbf{THEOREM}\ \frac{1}{|\mathsf{Aut}(N)|}\sum_{\pi \in \mathsf{Aut}(N)} x(\pi) = \frac{1}{|\mathsf{Hom}(I, N)|}|\mathsf{Hom}(I, P)|}$$

Semigroup

Build representation theory of symmetric semigroups T_n and cyclic semigroups CS_n.

$\mathbb{C}T_n/\mathrm{Rad} \cong \bigoplus_{r=1}^{n} \mathbb{C}S_n$. **Parametrize irreducible representations.**

$G_0(\mathbb{C}T_n) = \bigoplus_{r=1}^{n} G_0(\mathbb{C}S_n)$.

Bootstrap sampling of C-Tab's. (Uniform dist) + (Sgn part) + (Vanishing part) + (Nilpotent part).
The nilpotency of $J(\mathbb{C}T_n)$? (Polynomial growth?)

Partial Burnside ring $\Omega(T_n, \mathcal{Y}) \cong G_0(T_n)$? $\mathcal{Y}$?
Relation : $[X \cup Y] + [X \cap Y] = [X] + [Y], [\emptyset] = 0$.
$\Omega(CS_n)$? $G_0(\mathbb{C}CS_n)$?

References, Sites

- **Persi Diaconis.**
http://stat.stanford.edu/ cgates/PERSI/index.html
- **Saloff-Coste**
http://www.math.cornell.edu/ lsc/lau.html
- **Takemura (竹村彰道)**
http://www.e.u-tokyo.ac.jp/ takemura/
- **Aoki (青木敏)**
http://www.sci.kagoshima-u.ac.jp/ aoki/
- **Bernd Sturmfels.**
http://math.berkeley.edu/ bernd/
- **Omori (大森裕浩)**
http://www.e.u-tokyo.ac.jp/ omori/

The functor of units of Burnside rings

Serge Bouc

CNRS-Université de Picardie

Hokkaido University-24/06/08

— 06 —

Overview

1. Burnside rings
2. Units
3. p-groups : combinatorial answer
4. p-groups : algebraic answer
5. Method : biset-functors

The Burnside ring of a finite group

Definition

The Burnside group $B(G)$ of a finite group G is the Grothendieck group of the category of finite G-sets. It is a ring for the product induced by cartesian product of G-sets.

- In other words $B(G) = \mathbb{Z}^{(\{\text{finite } G\text{-sets}\})}/<[X \sqcup Y] - [X] - [Y]>$, and $[X][Y] = [X \times Y]$.
- As an abelian group, it has a basis $\{[G/H] \mid H \in [s_G]\}$, where $[s_G] = \{H \leq G, \text{ mod. } G\}$.

Ring structure

- If $H \leq G$, the map $\phi_H : [X] \mapsto |X^H|$ yields a ring homomorphism $B(G) \to \mathbb{Z}$, and the product map $\Phi : \prod_{H \in [s_G]} \phi_H : B(G) \to \prod_{H \in [s_G]} \mathbb{Z}$ is injective (Burnside (1911)).
- Dress (1969) has determined the prime spectrum of $B(G)$, and characterized the (finite) cokernel of Φ.
- It follows that $\mathbb{Q}B(G)$ is a split semisimple commutative $\mathbb{Q}$-algebra. The formulae for primitive idempotents of $\mathbb{Q}B(G)$ have been stated independently by Gluck and 吉田 (1983) :

$$\forall H \in [s_G],\ e_H^G = \frac{1}{|N_G(H)|} \sum_{K \leq H} |K| \mu(K,H) [G/K] \ .$$

Units

- Let $B^\times(G)$ denote the group of multiplicative units (i.e. invertible elements) of $B(G)$. Since $B^\times(G) \hookrightarrow \prod_{H\in[s_G]} \mathbb{Z}^\times = \prod_{H\in[s_G]} \{\pm 1\}$, it follows that $B^\times(G)$ is an elementary abelian 2-group.
- In particular, finding the rank of $B^\times(G)$ should be an easy problem. It is a very hard problem, as shown by the following observation (Tom Dieck (1979)) : the statement

$$\text{If } G \text{ has odd order, then } B^\times(G) = \{\pm 1\}$$

is equivalent to the odd order theorem (Feit-Thompson (1963)).
- For an arbitrary finite group, not so much is known on this problem. The work of many people (T. Tom Dieck, T. Matsuda, T. Matsuda - T. Miyata, T. Yoshida, E. Yalçın, ...) recently led to the solution for finite p-groups (more generally for finite nilpotent groups).

The case of p-groups : combinatorial answer

Notation

Let p be a prime number, and P be a finite p-group. If $S \leq P$, denote by $Z_P(S)$ the subgroup of $N_P(S)$ defined by $Z_P(S)/S = Z(N_P(S)/S)$.

Definition

A finite group G has normal rank 1 if all the abelian normal subgroups of G are cyclic.

The finite p-groups of normal rank 1 are the cyclic groups C_{p^n} $(n \geq 0)$, the generalized quaternion 2-groups Q_{2^n} $(n \geq 3)$, the dihedral 2-groups D_{2^n} $(n \geq 4)$, and the semi-dihedral groups SD_{2^n} $(n \geq 4)$.

Genetic subgroups

From now on P denotes a finite p-group, though definitions and results extend to all nilpotent finite groups.

Definition

A subgroup $S \leq P$ is called genetic if the following two conditions are fulfilled :

1. The group $N_P(S)/S$ has normal rank 1.
2. If $x \in G$ is such that $S^x \cap Z_P(S) \leq S$, then $S^x = S$.

Example : If $S \trianglelefteq P$, then S is a genetic subgroup of P if and only if P/S has normal rank 1.

Definition

Define a relation $\widehat{=}_P$ on the set of subgroups of P by
$S \widehat{=}_P T \Leftrightarrow \exists x \in P,\ S^x \cap Z_P(T) \leq T$ and $T \cap Z_P(S^x) \leq S^x$.

Genetic bases

Theorem (B. (2005))

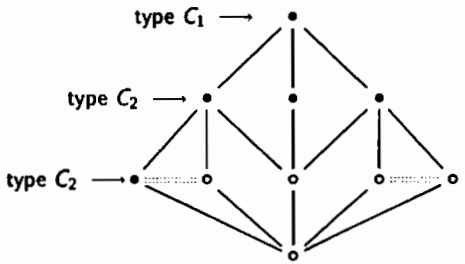
1. *The relation $\widehat{=}_P$ is an equivalence relation on the set of genetic subgroups of P.*
2. *If S and T are genetic subgroups of P and if $S \widehat{=}_P T$, then $N_P(S)/S \cong N_P(T)/T$.*

Definition

A genetic basis of P is a set of representatives of genetic subgroups of P for the relation $\widehat{=}_P$.
The type of a genetic subgroup S of P is the isomorphism class of $N_P(S)/S$.

The type of a genetic subgroup of P is one of C_{p^n} $(n \geq 0)$, Q_{2^n} $(n \geq 3)$, D_{2^n} $(n \geq 4)$, or SD_{2^n} $(n \geq 4)$.

An example of [illegible]



D_8

Combinatorial answer

Theorem

Let P be a finite p-group, and $\mathcal{G}$ be a genetic basis of P. Then $B^\times(P) \cong (\mathbb{Z}/2\mathbb{Z})^{u_P}$, where u_P is the number of elements of $\mathcal{G}$ whose type is trivial, C_2, or D_{2^n}.

Examples :

- If P is abelian, then $u_P = 1 + |\{S < P \mid |P : S| = 2\}|$ (Matsuda (1982)).
- $B^\times(D_8) \cong (\mathbb{Z}/2\mathbb{Z})^5$.

Operations on $B^\times(G)$

- Let $H \leq G$. Then restriction $B(G) \to B(H)$ induces a group homomorphism $Res^G_H : B^\times(G) \to B^\times(H)$.
- Let $H \leq G$. Then tensor induction $B(H) \to B(G)$ induces a group homomorphism $Ten^G_H : B^\times(H) \to B^\times(G)$.
- Let $N \trianglelefteq G$. Then inflation from $B(G/N)$ to $B(G)$ induces a group homomorphism $Inf^G_{G/N} : B^\times(G/N) \to B^\times(G)$.
- Let $N \trianglelefteq G$. Then taking fixed points by N induces a group homomorphism called deflation $Def^G_{G/N} : B^\times(G) \to B^\times(G/N)$.
- Let $f : G \to G'$ be a group isomorphism. Then f induces a group isomorphism $Iso(f) : B^\times(G) \to B^\times(G')$.

Faithful elements

Definition

Let G be a finite group. The set of faithful elements of $B^\times(G)$ is the subgroup of $B^\times(G)$ defined by $\partial B^\times(G) = \bigcap_{1 \neq N \trianglelefteq G} Ker\ Def^G_{G/N}$.

Theorem (Yalçın (2005), B. (2007))

Let P be a p-group of normal rank 1. Then $\partial B^\times(P)$ is trivial, except if $P \cong C_1, C_2, D_{2^n}$. In these cases $\partial B^\times(P) = \{1, v_P\}$.

$$v_P = \begin{cases} -[P/P] & \text{if } P \cong C_1 \\ [P/P] - [P/1] & \text{if } P \cong C_2 \\ [P/P] + [P/1] - [P/I] - [P/J] & \text{if } P \cong D_{2^n}, \\ \text{where } |I| = |J| = 2, & Z(P) \neq I \neq_P J \neq Z(P) \end{cases}$$

Algebraic answer

Theorem (B. (2007))

Let P be a finite p-group, and $\mathcal{G}$ be a genetic basis of P. Let $\mathcal{U} = \{S \in \mathcal{G} \mid type(S) \in \{C_1, C_2, D_{2^n}\}_{n \geq 4}\}$. Then the set

$$\{Ten^P_{N_P(S)} Inf^{N_P(S)}_{N_P(S)/S} \upsilon_{N_P(S)/S} \mid S \in \mathcal{U}\}$$

is an $\mathbb{F}_2$-basis of $B^\times(P)$.

In other words the map $\oplus\, Ten^P_{N_P(S)/S} Inf^{N_P(S)}_{N_P(S)/S} : \bigoplus_{S \in \mathcal{G}} \partial B^\times(N_P(S)/S) \to B^\times(P)$ is an isomorphism.

Example : For $P = D_8$, the group $B^\times(P)$ has an $\mathbb{F}_2$-basis

$$\begin{cases} -[P/P] \\ [P/P] - [P/Q] & \forall Q.\ |P:Q| = 2 \\ [P/P] + [P/1] - [P/I] - [P/J] & (\text{choose } I, J.\ |I| = |J| = 2,\ <I,J> = P) \end{cases}$$

Bisets

The five types of operations Res^G_H, Ten^G_H, $Inf^G_{G/N}$, $Def^G_{G/N}$, $Iso(f)$ on $B^\times$ can be unified using bisets :

Definition

Let G and H be (finite) groups. An (H, G)-biset U is a (finite) set with a left H-action and a right G-action, which commute i.e.

$$(h \cdot u) \cdot g = h \cdot (u \cdot g).$$

- If G, H, and K are groups, if U is an (H, G)-biset and V a (K, H)-biset, the composition $V \circ U$ is the (K, G)-biset $V \times_H U = (V \times U)/<(vh, u) \sim (v, hu)>$.
- If G is a group, the identity biset Id_G is the (G, G)-biset G with left and right action by multiplication.

Biset functors

If U is an (H, G)-biset and X is a G-set, then $Hom_G(U^{op}, X)$ is an H-set. This extends to a group homomorphism $B^\times(U) : B^\times(G) \to B^\times(H)$. This endows $B^\times$ with a structure of biset functor.

Definition

A biset functor F consists of the following data :

1. If G is a group, then $F(G)$ is an abelian group.
2. If U is an (H, G)-biset, then $F(U) : F(G) \to F(H)$ is a group homomorphism.
3. If U and U' are isomorphic (H, G)-bisets, then $F(U) = F(U')$.
4. If U and U' are (H, G)-bisets, then $F(U \sqcup U') = F(U) + F(U')$.
5. If U is an (H, G)-biset and V is a (K, H)-biset, then $F(V) \circ F(U) = F(V \circ U)$.
6. If G is a group, then $F(Id_G) = Id_{F(G)}$.

The biset category

Equivalently, a biset functor is an additive functor from the biset category to abelian groups :

Definition

The biset category $\mathcal{C}$ for finite groups is defined as follows :

- The objects are finite groups.
- If G, H are finite groups, then $Hom_{\mathcal{C}}(G, H) = B(H, G)$, the Burnside group of finite (H, G)-bisets.
- The composition of morphisms $G \to H \to K$ is obtained by linearly extending the product $(V, U) \mapsto V \times_H U$ of bisets.
- The identity morphism of G is the (class of) the (G, G)-biset Id_G.

A p-biset functor is a biset functor which is "defined only on p-groups", i.e. an additive functor from the full subcategory $\mathcal{C}_p$ of $\mathcal{C}$ consisting of p-groups, to the category of abelian groups.

Operations

Let F be a biset functor, and G be a finite group.

- If $H \leq G$, let res_H^G denote the (H, G)-biset G, and set $Res_H^G = F(res_H^G) : F(G) \to F(H)$.
- If $H \leq G$, let ind_H^G denote the (G, H)-biset G, and set $Ind_H^G = F(ind_H^G) : F(H) \to F(G)$.
- If $N \trianglelefteq G$, let $inf_{G/N}^G$ denote the $(G, G/N)$-biset G/N, and set $Inf_{G/N}^G = F(inf_{G/N}^G) : F(G/N) \to F(G)$.
- If $N \trianglelefteq G$, let $def_{G/N}^G$ denote the $(G/N, G)$-biset G/N, and set $Def_{G/N}^G = F(def_{G/N}^G) : F(G) \to F(G/N)$.
- If $f : G \to G'$ is a group isomorphism, let $iso(f)$ denote the (G', G)-biset G', and set $Iso(f) = F(iso(f)) : F(G) \to F(G')$.

Rational p-biset functors

Let F be a biset functor, and G be a finite group. The set of faithful elements of $F(G)$ is defined by $\partial F(G) = \bigcap_{1 \neq N \trianglelefteq G} Def_{G/N}^G$.

Definition

A p-biset functor is called rational if for any p-group P and any genetic basis $\mathcal{G}$ of P, the map $\oplus\, Ind_{N_P(S)/S}^P Inf_{N_P(S)/S}^{N_P(S)} : \bigoplus_{S \in \mathcal{G}} \partial F(N_P(S)/S) \to F(P)$ is an isomorphism.

Example : The functor of rational representations $R_{\mathbb{Q}}$ is defined by $G \mapsto R_{\mathbb{Q}}(G)$, and the map $R_{\mathbb{Q}}(U)$ is induced by $\mathbb{Q}U \otimes_{\mathbb{Q}G} -$.
The set $\partial R_{\mathbb{Q}}(G)$ consists of linear combinations of faithful irreducible rational representations of G.
The p-biset functor $R_{\mathbb{Q}}$ is rational (based on Roquette (1958)).

Using biset functors

Biset functors form an abelian category $\mathcal{F}$, and p-biset functors form an abelian category $\mathcal{F}_p$.

Theorem (B. (2005))

Rational p-biset functors form a Serre subcategory of $\mathcal{F}_p$, stable by duality.

Theorem (B. (2007))

1. *The map Φ induces an injective morphism of biset functors $\epsilon : B^\times \to \mathbb{F}_2 B^*$.*
2. *The image by ϵ of the p-biset functor $B^\times$ is contained in the p-biset functor $\mathbb{F}_2 R_{\mathbb{Q}}^*$.*
3. *Hence $B^\times$ is a rational p-biset functor.*

Functorial structure

Recall that simple p-biset functors are indexed by pairs (H, V), wher H is a finite p-group and V is a simple $\mathbb{Z}Out(H)$-module (notation $(H, V) \mapsto S_{H,V}$).

Theorem (B. (2007))

The functor $B^\times$ is a uniserial object of the category $\mathcal{F}_p$ of p-biset functors. More presisely :

- *If $p > 2$, then $B^\times$ is a simple object of $\mathcal{F}_p$, isomorphic to $S_{1,\mathbb{F}_2}$.*
- *If $p = 2$, then the full lattice of proper subobjects $\{0\} = F_0 \subset F_1 \subset \ldots \subset F_n \subset \ldots$ of $B^\times$ is such that $F_1/F_0 \cong S_{1,\mathbb{F}_2}$, and $F_i/F_{i-1} \cong S_{D_{2^{i+2}},\mathbb{F}_2}$, for $i \geq 2$.*

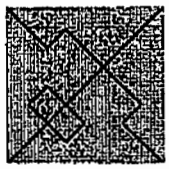
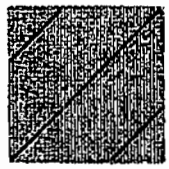
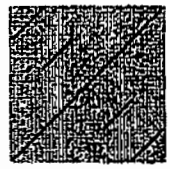
Piecewise-linear equivalence relations on an interval

D. Tambara

Hirosaki University

1. Introduction

An equivalence relation on a set X is a subset of $X \times X$ satisfying the conditions of reflexivity, symmetry, and transitivity. We consider an equivalence relation R on an interval $[a_0, a_1] = \{x \mid a_0 \leq x \leq a_1\}$ such that R is a union of finite number of segments. We are interested in the shape of R. Here are three examples of R.

We further impose on R the condition that the quotient $[a_0, a_1]/R$ is isomorphic to an interval. (This excludes the second and the third of the above three.) This amounts to saying that R is give as

$$R = \{(x, x') \mid f(x) = f(x')\}$$

for some map $f: [a_0, a_1] \to [0, 1]$.

We use the following terms. The *kernel-pair* of a map $f: X \to Z$ is the set

$$\{(x, x') \in X \times X \mid f(x) = f(x')\}.$$

This is an equivalence relation on X. The *fiber product* of maps $f: X \to Z$ and $g: Y \to Z$ is the set

$$\{(x, y) \in X \times Y \mid f(x) = g(y)\}.$$

We specify our class of maps. A map $f: [a_0, a_1] \to [b_0, b_1]$ is called a *P-map* if there exist $\alpha_0, \ldots, \alpha_n$ such that

$$a_0 = \alpha_0 < \cdots < \alpha_n = a_1$$

and $f|[\alpha_i, \alpha_{i+1}]$ is linear with nonzero slope for each i. (This name is provisional.)

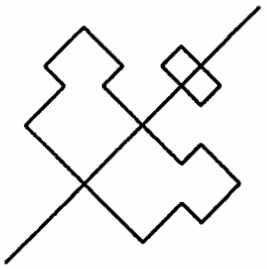
With these terms we state our problem: What shape is the kernel-pair of a P-map $f: [a_0, a_1] \to [0, 1]$? What shape is the fiber product of P-maps $f: [a_0, a_1] \to [0, 1]$ and $g: [b_0, b_1] \to [0, 1]$?

In §2 and §3 we observe some basic facts. In §4 we give a theorem about parameterization of connected components of fiber products.

Example. Here are pictures of a P-map f and its kernel-pair R, and P-maps f, g and their fiber product W.

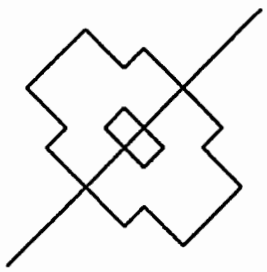
(1) If f has the graph

then R is



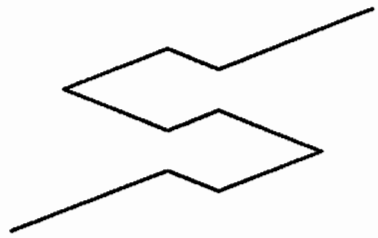
(2) If f has the graph

then R is



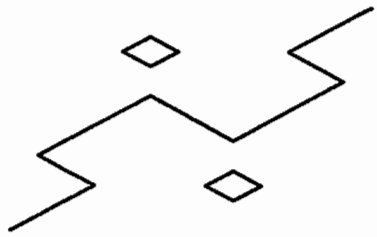
(3) If f and g have respectively the graphs

then W is



(4) If f and g have respectively the graphs

then W is

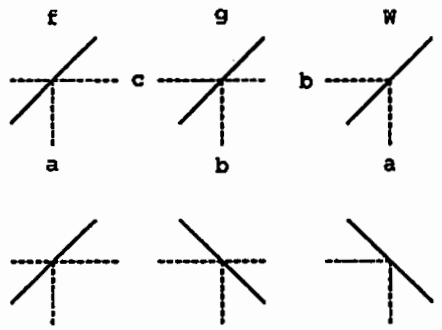


2. Local pictures

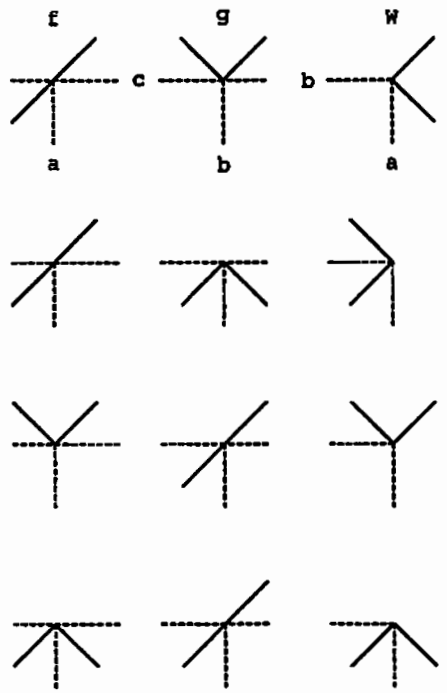
Let $f\colon [a_0, a_1] \to [0,1]$ and $g\colon [b_0, b_1] \to [0,1]$ be P-maps. Put $W = \{(x,y) \mid f(x) = g(y)\}$. Let $(a,b) \in W$. We look at W around (a,b).

The following pictures show the graph of $f(x)$ around $x = a$, the graph of $g(y)$ around $y = b$, and W around $(x,y) = (a,b)$ in various cases. We put $c = f(a) = g(b)$.

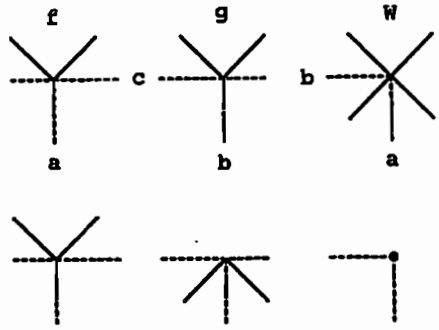
(1)



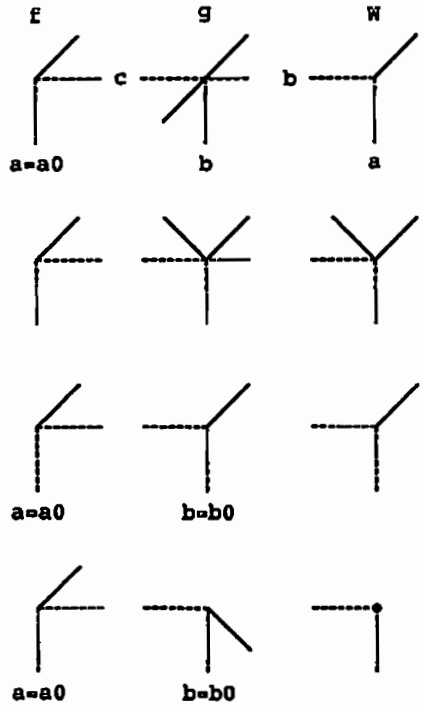
(2)



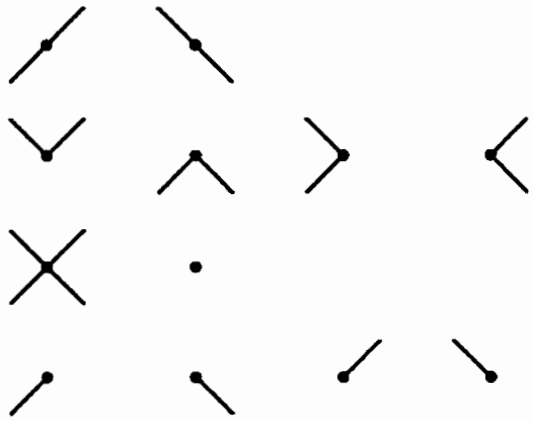
(3)



(4)



Hence we conclude that W around the point (a, b) has one of the following twelve shapes.



3. Connectivity

Let $f\colon [a_0, a_1] \to [0,1]$ and $g\colon [b_0, b_1] \to [0,1]$ be P-maps. Put $W = \{(x,y) \mid f(x) = g(y)\}$.

If $a_0 < a < a_1$ and f is increasing on $(a-\epsilon, a)$ and decreasing on $(a, a+\epsilon)$ for a small ϵ, we say f has a local maximum at a. Local minimum is defined similarly. Local maximum and local minimum are called extremum.

If f has an extremum at a, g has an extremum at b, and $f(a) = g(b)$, we say f and g have a common extremum. (3) of §2 shows this case.

Proposition 1. *Assume that $f(a_0) = 0, f(a_1) = 1, g(b_0) = 0, g(b_1) = 1$ and that f and g have no common extremum.*

Then every connected component of W is homeomorphic to either an interval or a circle.

Proof. Among the above twelve figures the seventh and the eighth are excluded by the assumption. Therefore W is locally homeomorphic to an interval. Then the conclusion follows.

When V be a union of segments in $\mathbb{R}^2$, we say $p \in V$ is an *end point* of V if there exists a neighborhood N of p such that $N \cap V$ is a segment with end point p.

Proposition 2. *Every connected component of W has even number of end points.*

Proof. We regard W as a graph. A vertex of W is an end point, a crossing point, or an isolated point. An edge of W is a connected sequence of segments joining two vertices.

Let C be a connected component of W. Count pairs (v, e) such that v is a vertex of C, e is an edge of C, and $v \in e$.

Every edge has two vertices. Hence the number of pairs (v, e) is even.

A vertex v belongs to no edge if v is an isolated point, one edge if v is an end point, and four edges if v is a crossing point.

Hence there must be even number of end points.

Corollary 3. *Assume* $f(a_0) = 0, f(a_1) = 1, g(b_0) = 0, g(b_1) = 1$. *Then the points* (a_0, b_0), (a_1, b_1) *belong to the same connected component of* W.

Proof. End points of W are only (a_0, b_0), (a_1, b_1). Let C be the component of W containing (a_0, b_0). By Proposition 2 C has another end point. It must be (a_1, b_1).

The following is proved similarly.

Corollary 4. *Assume that* f *and* g *are surjective. Then*

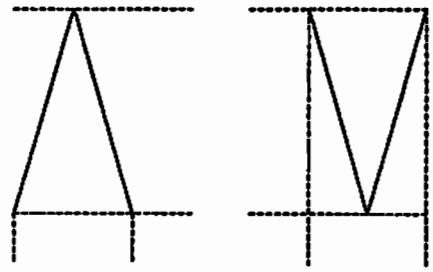
$$f^{-1}(0) \times g^{-1}(0) \cup f^{-1}(1) \times g^{-1}(1)$$

is contained in a connected component of W.

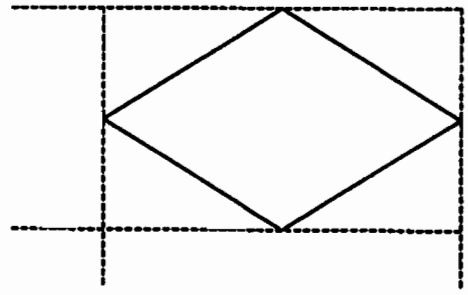
4. Circular components

If a subset V of $\mathbb{R}^2$ is a union of segments and homeomorphic to a circle, we say V is circular. We consider here the question how circular connected components arise in fiber products.

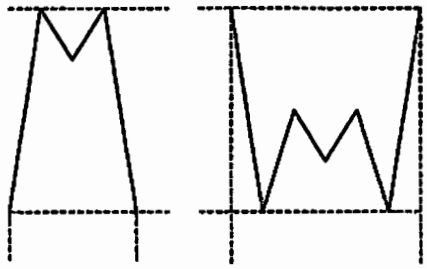
Example.
(1) If f and g have the graphs



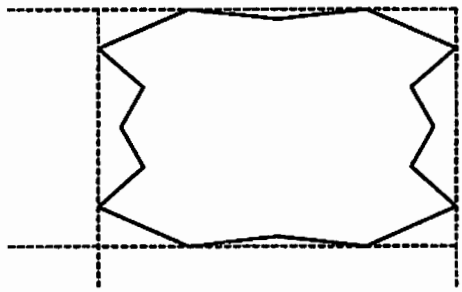
then $\{(x, y) \mid f(x) = g(y)\}$ is



(2) If f and g have the graphs



then $\{(x, y) \mid f(x) = g(y)\}$ is



These examples are generalized as follows. Let $f: [a_0, a_1] \to [0, 1]$, $g: [b_0, b_1] \to [0, 1]$ be P-maps. Put $W = \{(x, y) \mid f(x) = g(y)\}$.

Let $\mathcal{D}$ be the set of $(\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1)$ satisfying the following conditions.

- $a_0 \leq \alpha_0 < \alpha_1 \leq a_1$.
- $b_0 \leq \beta_0 < \beta_1 \leq b_1$.
- $0 \leq \gamma_0 < \gamma_1 \leq 1$.
- $f([\alpha_0, \alpha_1]) = [\gamma_0, \gamma_1]$, $f(\alpha_0) = f(\alpha_1) = \gamma_0$ (resp. $= \gamma_1$).
- $g([\beta_0, \beta_1]) = [\gamma_0, \gamma_1]$, $g(\beta_0) = g(\beta_1) = \gamma_1$ (resp. $= \gamma_0$).
- $f(x)$ does not have an extremum at $x = \alpha_0, \alpha_1$.
- $g(y)$ does not have an extremum at $y = \beta_0, \beta_1$.

Let $D = (\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1) \in \mathcal{D}$. By Corollary 4 we know that

$$(f^{-1}(\gamma_0) \times g^{-1}(\gamma_0) \cup f^{-1}(\gamma_1) \times g^{-1}(\gamma_1)) \cap [\alpha_0, \alpha_1] \times [\beta_0, \beta_1]$$

is contained in a connected component of W. Call this component $\omega(D)$. We know that $\omega(D)$ has no end point.

Let $\mathcal{C}$ be the set of connected components of W which are not a single point and have no end point. Thus we have a map $\omega: \mathcal{D} \to \mathcal{C}$.

Theorem 5. *ω is a bijection.*

If f and g have no common extremum, then $\mathcal{C}$ consists of the circular components of W, so we have a bijection between $\mathcal{D}$ and the set of circular components of W.

Taking $g = f$, we obtain the following.

Corollary 6. *Let* $f\colon [a_0, a_1] \to [0,1]$ *be a P-map. Let* $R = \{(x,x') \mid f(x) = f(x')\}$. *Assume that*

$$f^{-1}(0) = \{a_0\}, \quad f^{-1}(1) = \{a_1\}.$$

Then R *is connected if and only if* $\mathcal{D}$ *(for* f *and* f*) is empty.*

5. Summary

Let $f\colon [a_0, a_1] \to [0,1]$, $g\colon [b_0, b_1] \to [0,1]$ be P-maps and let $W = \{(x,y) \mid f(x) = g(y)\}$. Assume that f and g have no common extremum.

We have obtained a bijection

$$\text{circular component } C \text{ of } W \leftrightarrow (\alpha_0, \alpha_1, \beta_0, \beta_1, \gamma_0, \gamma_1).$$

Finally we mention a problem. A part of Hilbert's sixteenth problem concerns the topology of real plane algebraic curves ([1]). Every connected component of an algebraic curve X in $\mathbb{RP}^2$ is homeomorphic to a circle. One component may lie inside another component. This inclusion defines a partial order on the set of components of X. The problem is to classify partially ordered sets arising from a curve of a fixed degree. We can ask the analogous question for W.

References

1. G. Wilson, Hilbert's sixteenth problem, Topology 17, 63–73, 1978.

可換2-シロー部分群をもつ群における主ブロックのカルタン行列の固有値

功刀直子（東京理科大学　理学部）
和田倶幸（東京農工大学 共生科学技術研究院）

1　はじめに

G を有限群, F を標数 $p>0$ の代数的閉体とし, B を FG のブロックでその defect group を D とする. $l=l(B)$ を B に含まれる既約 Brauer (modular) 指標の個数とする. B のカルタン行列 $C_B=(c_{ij})$ とは, $l\times l$ 行列で, 各成分 c_{ij} は B に属する既約 FG-加群 S_j が i 番目の射影的直既約 FG-加群 P_i の中に組成因子として現れる重複度を表す. C_B は非負, 直既約行列であるから Frobenius-Perron 固有値 (i.e. 唯一の最大固有値) $\rho(B)$ をもつ. R_B を C_B の固有値全体, 同様に E_B を C_B の ($\mathbb{Z}$-) 単因子全体の集合とする.

カルタン行列 C_B の固有値がどのようなときに整数になるか, どのようなときに固有値と単因子が一致するのかについて考えてきた. ほとんどの場合に $\rho(B)$ が整数ならばすべての固有値が整数になり, さらに $R_B=E_B$ をみたす. そこで次の予想を得た.

Conjecture([5]). G を有限群, B を FG のブロックで defect group を D とする. B のカルタン行列 C_B の固有値について次は同値である.

(a) $\rho(B)\in\mathbb{Z}$.
(b) $\rho(B)=|D|$.
(c) $R_B=E_B$.

注 1. (c)$\Longrightarrow$(b)$\Longrightarrow$(a) である.

この予想は次の場合には証明されている.

1 ([1, Proposition 2]). $D \lhd G$ ならば (c) が成り立つ.

2 ([1, Theorem 1]). G が p-可解群ならば, (b) と (c) は同値である. ((a) ならば (b) はまだ証明されていない.)

3 ([1, Proposiiton 3]). B が巡回ブロック (i.e. Dが巡回群) ならば (a),(b),(c) はさらに次の (d) に同値である.

(d) B と b は森田同値である. ここで b は B のBrauer対応子 (i.e. b は $FN_G(D)$ のブロックで $b^G = B$ をみたすもの) .

注 2. **1** より b は常に (c) をみたす. 森田同値であれば $C_B = C_b$ となり, B も (c) をみたす. よって (d) が (c) より強い.

4 ([1, Proposition 4]). B が tame block (i.e. $p = 2$ で $D \simeq$ dihedral, generalized quaternion または semidihedral 2-群) ならば (a),(b),(c) はさらに **3** の (d) に同値である.

注 3. (c) と (d) は一般には同値にならない. (d) ならば (c) であるが, (c) ならば (d) とは限らない. その例として $l(B) = 1$ の次の例がある ([1, Example]). $G = \mathrm{SL}(2,3) \cdot E_{3^3}$ (半直積) で $p = 3$ とする. G の非主ブロック B_1 は $l(B_1) = 1, k(B_1) = 12$ である. 一方 Brauer 対応子 b_1 は $l(b_1) = 1$ だが $k(b_1) = 17$ となり, B_1 と b_1 は森田同値ではない. $l(B_1) = 1$ なので $C_{B_1} = (|D|)$ より $R_{B_1} = E_{B_1} = \{|D|\}$ である.

Question. 上の例は $D \simeq \mathbb{Z}_3 \mathrm{wr} \mathbb{Z}_3$ で D が non abelian な場合である. D が abelian のときには, (c) と (d) は同値にならないだろうか?

この問題に関しては **3** により巡回ブロックの場合には正しい. また次の場合に正しい. これらの結果は Koshitani-Kunugi の結果 [3] に触発された.

5 ([5, Theorem C]). G は有限群で 3-シロー部分群 P が基本可換群 E_{3^2} に同型とする. B を G の 3-主ブロックとするとき, Conjecture の (a),(b),(c) は **3** の (d) と同値 (もう少し強く Puig 同値) である. このとき $O^{3'}(G)/O_{3'}(G)$ の構造が決まる.

2 主定理

ここでは 5 の結果と同じことが $p=2$ の場合に証明できることを示す. 有限群 X に対し $O'(X)$ は X の奇数指数の最小の正規部分群, $O(X)$ は X の奇数位数の最大正規部分群のこととする. 以下の定理において (d) と (e) の同値性は少々きつい感じを与えると思うが, (d) から (e) をいうとき, カルタン行列の固有値がうまく応用できる. 結果としてこの場合 (c) から (d) がいえる.

定理 ([4, Theorem]). $\tilde{G}$ を有限群とし, 2-シロー部分群 P はアーベル群であるとする. $\tilde{B}$ を $\tilde{G}$ の 2-主ブロックとするとき次は同値である.

(a) $\rho(\tilde{B}) \in \mathbb{Z}$

(b) $\rho(\tilde{B}) = |D|$

(c) $R_{\tilde{B}} = E_{\tilde{B}}$

(d) $\tilde{B} \sim \bar{b}$ は森田同値（もう少し強く Puig 同値）である. ただし $\bar{b}$ は $\tilde{B}$ の Brauer 対応子.

(e) $O(\tilde{G}) = \{1\}$ とし, $G = O'(\tilde{G})$ とおく. このとき $G = G_1 \times \cdots \times G_r \times S$ となる. ここで $G_i \simeq \mathrm{PSL}(2, q_i)$, $3 < q_i \equiv 3 \pmod 8$, $1 \leq i \leq r$ で, S はアーベル 2-群である.

注 4. $\tilde{G}$ が p-可解群のときは, defect group D がアーベル群ならば, $\tilde{B}$ と $\bar{b}$ が森田同値になっていることは, Morita, Dade 等により知られているので, 上の (e) の主張は非可解群の場合について書いてある.

証明のスケッチ (d)→(c)→(b)→(a) は明らかである. (e)→(d) については, 各 $G_i \simeq \mathrm{PSL}(2, q_i)$ の主ブロックとその Brauer 対応子の間には Erdmann により森田同値（Puig 同値）が存在する. それを直積 $G = G_1 \times \cdots \times G_r \times S$ の主ブロックと Brauer 対応子の間の森田同値 (Puig 同値) につなげる. 次に [3] で得られた方法により $B_0(G)$ と $B_0(N_G(P))$ の間の森田同値 (Puig 同値) は自然に $B_0(\tilde{G})$ と $B_0(N_{\tilde{G}}(P))$ の間の森田同値 (Puig 同値) に拡張できることが分かる.

(a)→(e). 次の構造定理を使う. 有限群をやっている人には奇異に見えるかもしれないが, 現在構造定理を使わずに一般の有限群でブロック間のカテゴリーの同値性を証明するのは, きわめて難しい.

命題 (Walter, Bender). G を可換 2-シロー部分群をもつ非可解有限群とする.

すると

$$O'(G)/O(G) \simeq G_1 \times \cdots \times G_r \times S$$

となる. ここで G_i $(1 \leq i \leq r)$ は次の単純群のうちのどれかである.

(1) $\mathrm{PSL}(2,q)$, $q \equiv 3$ *or* $5 \pmod 8$, $q > 3$

(2) $\mathrm{SL}(2,2^n)$, $n > 1$

(3) J_1

(4) $R(q)$, $q = 3^{2m+1}$

key lemma として使ったものは $|G:H| = q$ で q が p と異なる素数のときに証明したが, それを次のように一般に拡張できることを奥山哲郎氏に教えて頂いた. 謝してここではそれを証明する.

補題. G を有限群とし, $G \rhd H$ で $|G:H|$ が p で割れないとする. b を H の p-ブロックとし, B を b をカバーする G の任意の p-ブロックとする. すると $\rho(B) = \rho(b)$ である.

証明 b に属する既約 Brauer 指標を $\mathrm{IBr}(b) = \{\psi_1, \ldots, \psi_l\}$ とし, ψ_i に対応する射影的直既約指標を Ψ_i, $1 \leq i \leq l$ とする. b をカバーする G の p-ブロック全体を $\Delta := B_1 + \cdots + B_m$ とする. このとき $\mathrm{IBr}(\Delta) = \{\varphi_1, \ldots, \varphi_r\}$ とし, φ_i に対応する射影的直既約指標を Φ_i, $1 \leq i \leq r$ とする.

C_b の固有値 $\rho(b)$ に属する固有ベクトルで各成分が正のものを $(a_1, \ldots, a_l)$ とする. すると $(a_1, \ldots, a_l)C_b = \rho(b)(a_1, \ldots, a_l)$ である. $C_b(\psi_1, \ldots, \psi_l)^T = (\Psi_1, \ldots, \Psi_l)^T$ であるから

$$\begin{aligned}(a_1, \ldots, a_l)(\Psi_1, \ldots, \Psi_l)^T &= (a_1, \ldots, a_l)C_b(\psi_1, \ldots, \psi_l)^T \\ &= \rho(b)(a_1, \ldots, a_l)(\psi_1, \ldots, \psi_l)^T\end{aligned}$$

を得る. ここで $(x_1, \ldots, x_l)^T$ は $(x_1, \ldots, x_l)$ の転置である. すると誘導指標について

$$(a_1, \ldots, a_l)({\Psi_1}^G, \ldots, {\Psi_l}^G)^T = \rho(b)(a_1, \ldots, a_l)({\psi_1}^G, \ldots, {\psi_l}^G)^T \quad (*)$$

を得る. FG, FH の Jacobson radical を $J(FG), J(FH)$ とする. $G \rhd H$ で $|G:H|$ が p と素のときは, $J(FG) = FG \cdot J(FH)$ が成り立つ. このことから $G \rhd H$ で $|G:H|$ が p と素のときは, 既約 FG-加群を H に制限したときの各既約因子の重複度である ramification index と, 対応する射影的直既約 FG-加群を H に制限したときの対応する各射影的直既約因子の重複度である

ramification index は一致するという定理（Willems の定理と呼ばれているようだ）および Nakayama relation により

$$\Psi_i{}^G = \sum_{j=1}^{r} b_{ij}\Phi_j \Longleftrightarrow \varphi_{j\,H} = \sum_{i=1}^{l} b_{ij}\psi_i \quad \text{(Nakayama relation)} \tag{1}$$

$$\Longleftrightarrow \Phi_{j\,H} = \sum_{i=1}^{l} b_{ij}\Psi_i \quad \text{(Willems)} \tag{2}$$

$$\Longleftrightarrow \psi_i{}^G = \sum_{j=1}^{r} b_{ij}\varphi_j \quad \text{(Nakayama relation)} \tag{3}$$

である．故に

$$\begin{aligned}(a_1,\ldots,a_l)(b_{ij})C_\Delta(\varphi_1,\ldots,\varphi_r)^T &= (a_1,\ldots,a_l)(b_{ij})(\Phi_1,\ldots,\Phi_r)^T\\ (1)\text{ より} \qquad &= (a_1,\ldots,a_l)({\Psi_1}^G,\ldots,{\Psi_l}^G)^T\\ (*)\text{ より} \qquad &= \rho(b)(a_1,\ldots,a_l)({\psi_1}^G,\ldots,{\psi_l}^G)^T\\ (3)\text{ より} \qquad &= \rho(b)(a_1,\ldots,a_l)(b_{ij})(\varphi_1,\ldots,\varphi_r)^T\end{aligned}$$

を得る．ここで $\{\varphi_1,\ldots,\varphi_r\}$ は $\mathbb{C}$ 上 1 次独立な類関数であるから

$$(\sum_{i=1}^{l} a_ib_{i1},\ldots,\sum_{i=1}^{l} a_ib_{ir})C_\Delta = \rho(b)(\sum_{i=1}^{l} a_ib_{i1},\ldots,\sum_{i=1}^{l} a_ib_{ir}) \quad (**)$$

をみたす．ここで $a_i > 0, 1 \le i \le l$ また $b_{ij} \ge 0$ であるから，$\sum_{i=1}^{l} a_ib_{it} = 0 \Longleftrightarrow$ $b_{it} = 0$ for $\forall i$ となることに注意する．Δ は b をカバーしているから行列 (b_{ij}) の各列は零ではない．よって $(**)$ より $\rho(b)$ は C_Δ の固有値でその固有ベクトルは正である．

$\mathrm{IBr}(\Delta) = \{\varphi_1,\ldots,\varphi_r\}$ をブロックごとに並べ替える．$\mathrm{IBr}(B_i) = \{\varphi_{i1},\ldots,\varphi_{il_i}\}$, $1 \le i \le m$ とする．σ を $\{\varphi_1,\ldots,\varphi_r\}$ から $\{\varphi_{11},\ldots,\varphi_{1l_1},\ldots,\varphi_{m1},\ldots,\varphi_{ml_m}\}$ へ並べ替える置換とする．Q をその置換行列とする．Q は $r \times r$ 行列で $r = l_1 + \cdots + l_m$ である．

$x := (\sum_{i=1}^{l} a_ib_{i1},\ldots,\sum_{i=1}^{l} a_ib_{ir})$ とすると $x > 0$ で，$x^\sigma = xQ$ となる．

$xC_\Delta = \rho(b)x$ より,

$$xQQ^{-1}C_\Delta Q = \rho(b)xQ$$

であるから

$$x^\sigma \begin{pmatrix} C_{B_1} & & O \\ & \ddots & \\ O & & C_{B_m} \end{pmatrix} = \rho(b)x^\sigma$$

となる. x^σ の B_i-part を x_i^σ とすると

$$x_i^\sigma C_{B_i} = \rho(b)x_i^\sigma, \quad 1 \le i \le m$$

を得る. C_{B_i} は直既約行列であるから $x_i^\sigma > 0$ に注意するとこれは $\rho(B_i) = \rho(b)$, $1 \le i \le m$ を意味する. □

(a)→(e) の証明. (e) が成り立たないとする. すると命題から $O'(\tilde{G})$ は $\mathrm{PSL}(2,q)$, $q \equiv 5 \pmod 8$, $\mathrm{SL}(2,2^n)$, J_1, $R(q)$ のうちどれかを因子 G_i として含む. ところがこれらの単純群の主ブロックのカルタン行列における最大固有値は $\rho(B_0(G_i)) > |P_i|$ をみたす. ここで P_i は G_i のシロー 2-部分群である. 補題より $\rho(B_0(\tilde{G})) = \rho(B_0(G)) > |P|$ となる. これは (a) に反する. なぜならもし $\rho(B_0(\tilde{G}))$ が整数ならば [2, Corollary 4.6] よりそれは $|P|$ を割らなくてはいけない. □

注 5. (1) 定理の (e) の主張の中に $O(\tilde{G}) = \{1\}$ という仮定があるが, 主ブロックは $O(\tilde{G})$ を kernel に含むので, 群の構造としては mod $O(\tilde{G})$ で決まるという意味である.

(2) 補題が $|G : H|$ が p と素であればよい, というように拡張されたため, 奇素数 p のときに $\tilde{G}/O^{p'}(\tilde{G})$ は一般には可解群にならないが, 位数は p と素なので p が奇素数のときもこの議論は使える. 少し問題はあるが, この補題は D がアーベル群のとき, B とその Brauer 対応子 b の間に森田同値があるかどうかを単純群の場合に帰着する役割を果たしている補題であるといえる.

References

[1] M. Kiyota, M. Murai and T. Wada, Rationalty of eigenvalues of Cartan matrices in finite groups, J. Algebra, 249 (2002), 110-119.

[2] M. Kiyota and T. Wada, Some remarks on eigenvalues of the Cartan matrix in finite groups, Comm. Algebra, 21 (1993), 3839-3860.

[3] S. Koshitani and N. Kunugi, Broué's conjecture holds for principal 3-blocks with elementary abelian defect group of order 9, J. Algebra, 248 (2002), 575-604.

[4] N. Kunugi and T. Wada, Eigenvalues of Cartan matrices of principal 2-blocks with abelian defect groups, J. Algebra, 319 (2008), 4404-4411.

[5] T. Wada, Eigenvector matrices of Cartan matrices for finite groups, J. Algebra, 308 (2007), 629-640.

整数行列の固有値と単因子について
On eigenvalues and elementary divisors of integral matrices

東京医科歯科大学教養部　清田正夫
東京医科歯科大学名誉教授　野村和正
College of Liberal Arts and Sciences
Tokyo Medical and Dental University
Masao KIYOTA and
Kazumasa NOMURA (Prof. Emeritus)

1　結果

整数を成分にもつ n 次行列 A を考える。A の特性根を $\lambda_1, \lambda_2, \ldots, \lambda_n$ とする。定義より A の特性多項式 $f_A(x) = |xI - A|$ は

$$f_A(x) = (x - \lambda_1)(x - \lambda_2)\cdots(x - \lambda_n)$$

と因数分解される。一方、A の単因子を $e_1, e_2, \ldots, e_n$ とする。定義より $e_1, e_2, \ldots, e_n$ は

$$e_i \mid e_{i+1} \qquad (1 \leq i \leq n-1) \tag{1}$$

をみたす 整数であり、A は対角行列 $\mathrm{diag}(e_1, e_2, \ldots, e_n)$ と対等になる。すなわち、行列式の値が ± 1 であるような整数行列 P, Q が存在して、

$$PAQ = \mathrm{diag}(e_1, e_2, \ldots, e_n) \tag{2}$$

となる。これらの特性根と単因子との間に次の関係があることは、よく知られている。

$$\lambda_1\lambda_2\cdots\lambda_n = \pm e_1e_2\cdots e_n. \tag{3}$$

これは (2) の両辺の行列式を比較することですぐにわかる。これに加えて、次の関係があることがわかった。

定理1　k を n 以下の自然数とする。A の n 個の特性根から任意に k 個を選んで作った積は、最初の k 個の単因子の積 $e_1e_2\cdots e_k$ で割り切れる。

すなわち、任意の k $(1 \leq k \leq n)$ と任意の $i_1, \ldots, i_k$ $(1 \leq i_1 < i_2 < \cdots < i_k \leq n)$ に対して

$$\lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_k} = ce_1e_2\cdots e_k \tag{4}$$

をみたす代数的整数 c が存在する。

特性根と単因子の関係は、(3) と (4) で尽くされることもわかった。実際、次の結果が得られた。

定理2 $f(x)$ を最高次係数が 1 の整数係数の多項式とし、$e_1, e_2, \ldots, e_n$ を (1) を満たす整数とする。$f(x)$ を複素数の範囲で $f(x) = (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n)$ と因数分解する。これらが (3) と (4) をみたすならば、$f(x)$ を特性多項式にもち、単因子が $e_1, e_2, \ldots, e_n$ であるような整数行列が存在する。

注意 定理 1 と定理 2 は、有理整数環を一般の単項イデアル整域でおきかえても成立する。ここでは、話を簡単にするために有理整数環上の話に絞った。

2 定理 1 の証明の概略

n 次整数行列 A の特性多項式を

$$\begin{aligned} f_A(x) &= (x-\lambda_1)(x-\lambda_2)\cdots(x-\lambda_n) \\ &= x^n - s_1 x^{n-1} + \cdots + (-1)^n s_n \end{aligned}$$

とし、A の単因子を $e_1, e_2, \ldots, e_n$ とする。目標は、任意の k $(1 \le k \le n)$ と任意の $i_1, \ldots, i_k$ $(1 \le i_1 < i_2 < \cdots < i_k \le n)$ に対して

$$\lambda_{i_1}\lambda_{i_2}\cdots\lambda_{i_k} = c e_1 e_2 \cdots e_k \tag{5}$$

をみたす代数的整数 c の存在を示すことにある。

$\mathrm{rank}(A) = r < k$ のときは定理は自明に成立するので、$k \le r$ と仮定する。さらに $r = n$ つまり A は正則としてよい。まず、次のことに注意する。

補題1 各 s_i $(1 \le i \le n)$ は単因子の最初の i 個の積 $e_1 e_2 \cdots e_i$ で割り切れる。

証明 $s_1 = \mathrm{tr}(A)$, $s_n = \det(A)$ はよく知られているが、一般に s_i は A の principal i-minors すべての和となる。一方、$e_1 \cdots e_i$ は A の i-minors の最大公約数なので、補題 1 が成り立つ。Q.E.D.

以下、簡単のため $k = 2$ の場合について説明する。目標は、任意の i, j $(1 \le i < j \le n)$ に対して、代数的整数として $\lambda_i\lambda_j$ が $e_1 e_2$ で割り切れることを示すことである。これを示すために、$\{\lambda_i\lambda_j \mid 1 \le i < j \le n\}$ を根に持つ多項式 $F(x)$ を考える：

$$F(x) = \prod_{i<j}(x - \lambda_i\lambda_j) = x^N + c_1 x^{N-1} + \cdots + c_N$$

ここで、$N = n(n-1)/2$ である。さて、$\lambda_i\lambda_j$ $(1 \le i < j \le n)$ が e_1e_2 で割り切れることは、次の Claim から容易に導かれる。

Claim　各 c_i $(1 \le i \le N)$ は $(e_1e_2)^i$ で割り切れる。

以下、Claim の証明の方針を述べる。c_i は $\lambda_1, \ldots, \lambda_n$ の対称式であることに注意する。したがって、c_i は基本対称式 $s_1, \ldots, s_n$ の多項式となる。たとえば、$c_1 = -s_2$, $c_2 = s_1s_3 - s_4$ となる。この証明を思い返してみよう。まず $\lambda_1, \ldots, \lambda_n$ から作られる単項式達の間に次のような辞書式順序を入れる：

$$\lambda_1^{p_1} \cdots \lambda_n^{p_n} > \lambda_1^{q_1} \cdots \lambda_n^{q_n}$$

となるのは、

$$p_1 = q_1, \cdots, p_{l-1} = q_{l-1}, p_l > q_l$$

なる番号 l が存在するとき。

さて f を $\lambda_1, \ldots, \lambda_n$ の対称式とする。f に現れる単項式のなかで、上の順序について最大のもの (leading term) を $\lambda_1^{p_1}\lambda_2^{p_2}\cdots\lambda_n^{p_n}$ とし、その係数を m とする。指数ベクトル $(p_1, \ldots, p_n)$ の階差列を $(q_1, \ldots, q_n)$ とおく：

$$q_1 = p_1 - p_2, \ \ldots, \ q_{n-1} = p_{n-1} - p_n, \ q_n = p_n. \tag{6}$$

ここで q_i は非負であることに注意する。$\lambda_1, \ldots, \lambda_n$ の対称式 $s_1^{q_1}s_2^{q_2}\cdots s_n^{q_n}$ は f と同じ最大項 (leading term) を持つので、

$$f_1 = f - ms_1^{q_1}s_2^{q_2}\cdots s_n^{q_n}$$

とおけば f_1 の leading term は f の leading term より真に小さい。以下、上の操作を繰り返すことにより、f が $s_1, \ldots, s_n$ の多項式で書き表わされることが分かる。

上のアルゴリズムを $F(x)$ の係数 c_i に適用すると、c_i は基本対称式 $\{s_j\}$ の整数係数の多項式となる。定理の状況に戻すと、補題 1 より次が得られる。

補題 2　非負整数 $p_1, \ldots, p_n$, $q_1, \ldots, q_n$ が (6) を満たすとき、$s_1^{q_1}\cdots s_n^{q_n}$ は $e_1^{p_1}\cdots e_n^{p_n}$ で割り切れる。

さて、c_i の leading term は作り方から $\lambda_1^i\lambda_2^i$ と一致するかまたはそれより小さい。よって補題 2 と仮定 $e_j \mid e_{j+1}$ から $(e_1e_2)^i \mid c_i$ が出る。以上により Claim が証明された。

3　定理２の証明の概略

ここでは、$n=4$ の場合について、A を具体的に構成することで証明のかわりとする。$f(x)$ を最高次係数が 1 の整数係数の 4 次多項式とし、$e_1, e_2, \ldots, e_4$ を (1) を満たす整数とする。さて、多項式

$$f(x) = (x-\lambda_1)(x-\lambda_2)(x-\lambda_3)(x-\lambda_4)$$

を展開したものを

$$f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4.$$

とし、行列 A を次のように定義する。

$$A = \begin{pmatrix} 0 & 0 & 0 & -\frac{a_4}{e_1e_2e_3} \\ e_3 & 0 & 0 & -\frac{a_3}{e_1e_2} \\ 0 & e_2 & 0 & -\frac{a_2}{e_1} \\ 0 & 0 & e_1 & -a_1 \end{pmatrix}.$$

ここで、A の最後の列に現れる分数について、分母が 0 の場合は分数自身を 0 と定義する。A の特性多項式が $f(x)$ となること、および、A の単因子が e_1, e_2, e_3, e_4 となることは容易に確かめることができる。A の成分がすべて整数であることは、条件 (4) から出る。

4　付記

北海道大学における本稿の講演（2008 年 6 月 24 日）の後に、弘前大学の丹原大介氏より定理 1 の別証明の概略が寄せられました。丹原氏の了解を得て、ここに、彼から寄せられた内容を、そのままの形で掲載します。

n 次の行列 A と n 以下の自然数 k があるとき、A の k 次小行列式すべてを自然な順番に並べてつくられる行列があります。その行列を B と書くと、B の size は 2 項係数の ${}_nC_k$。B の固有値は、A の n 個の固有値から k 個選んでとった積全体です。A の単因子のはじめの k 個の積は B の成分すべてを割るので、B の固有値すべてを割ることになり、つまり、A の固有値の任意の k 個の積を割るといえます。

ランク 2 のシャープ指標について

野澤宗平 (千葉大学)
與口卓志 (千葉大学大学院自然科学研究科)

1. 目的

G を有限群, χ を G の指標とするとき,

$$L := \{\chi(g) \mid 1 \neq g \in G\},$$
$$f_L(x) := \prod_{\ell \in L}(x - \ell)$$

とおく. このとき $f_L(\chi(1))$ は有理整数で, しかも $|G|$ で割り切れる (cf. [2], [3]). 特に, $f_L(\chi(1)) = |G|$ が成り立つとき, χ を type L の sharp 指標と呼ぶ. 定義から

$$\chi \text{ が sharp 指標} \iff \chi + 1_G \text{ が sharp 指標}$$

が直ちに従うので, 以下では $(\chi, 1_G)_G = 0$ の場合だけ考える (normalized な sharp 指標と呼ばれる).

sharp の概念は元々ある種の置換群において発生したものであるが, 近年はより一般に指標の問題として研究がなされており, その成果として χ が整数値でない場合は既に完全な分類が存在する (cf. [1]). 従って, 現在は整数値の sharp 指標が主な研究対象である.

整数値の sharp 指標を調べる上で基礎となるのは次の補題である.

補題 1. $L \subset \mathbb{Z}$, $|L| > 1$ とするとき, 以下が成り立つ:

(1) $L = \{\ell_1, \ell_2\}$ ならば, $(\chi, \chi)_G = 1 - \ell_1\ell_2$.
(2) $|L| > 2$ ならば, $(\chi, \chi)_G < -\min(L) \cdot \max(L)$.

さらに, (1), (2) のどちらのケースであっても $\min(L) < 0$ である.

この補題により $(\chi, \chi)_G$ には L に応じた制限が付く. そこで, 特定の L を 1 つ固定し, その type を持つ sharp 指標を全て分類する試みがなされている.

例 1. $L=\{\ell,\ell+1\}$ のとき, G は 2-transitive Frobenius である.

例 2. $L=\{\ell,\ell+2\}$ のとき, G は完全に分類されている.

例 3. $L=\{\ell,\ell+3\}$ のときは, $Z(G)>1$ または $\ell=-3$ の場合だけが分類されている.

我々の目標は例 3 を一般化し $L=\{\ell,\ell+p\}$ (p : 奇素数) の場合について研究することである. しかし, 現時点ではまだ一般化のための手がかりが不足しているため, 今回は

$$L=\{-1,p-1\} \text{ or } \{1-p,1\}$$

の場合だけを取り扱う. このとき, 補題 1 から $(\chi,\chi)_G=p$ となり χ の既約成分の個数に強い制限が得られる. 逆に, ノルムがあまり影響しない箇所については, 上記の 2 つ以外の type においても類似の議論が成り立つ.

今回我々が得た第 1 の結果は次の定理である:

定理 2. p を奇素数, $L=\{-1,p-1\}$ or $\{1-p,1\}$ とする. G が type L の sharp 指標を持つならば, $|G|$ は p で割り切れる.

これは一見すると極めて自然な結果であるが, G が自明な中心を持つ場合は証明に若干の手間を要する. 一方, $Z(G)>1$ の場合は G に関してより多くの情報を引き出すことができる. それらの成果について 3 節で紹介する.

2. $|G|$ が p で割り切れること

本節では定理 2 がいかにして証明されるか概略を説明する. 実は, $Z(G)>1$ の場合はより強く以下の事実が成り立つ:

補題 3. G が type $\{\ell,\ell+p\}$ の sharp 指標を持つならば, $Z(G)$ は p-群である. さらに $\exp Z(G)=1$ or p が成り立つ.

これは次のように示される. $Z(G)$ から素数位数の元 z を 1 つとり, $Z=\langle z\rangle$, $o(z)=q$ とおく. χ の既約成分のうち, Z を kernel に含むもの全部の和を ψ, Z を kernel に含まな

いもの全部の和を θ とおく. このとき, ψ, θ の定め方から $g \in G - Z$ に対して

$$\sum_{i=1}^{q} \chi(gz^i) = \sum_{i=1}^{q} \psi(gz^i) + \sum_{i=1}^{q} \theta(gz^i) = \sum_{i=1}^{q} \psi(g) = q\psi(g)$$

が成り立つ. ここで各 i に対して $\chi(gz^i) \in \{\ell, \ell + p\}$ より, $p = q$ であるか, さもなければ

$$\chi(g) = \chi(gz) = \cdots = \chi(gz^{q-1}) = \psi(g), \quad \theta(g) = 0$$

である. もし後者だとすると, θ が $G - Z$ で 0 をとることから, θ が type $\{0, m\}$ $(m \in \mathbb{Z})$ の sharp 指標になることが示せる. このとき補題 1 より θ が既約になるが, これは起こり得ない. よって $p = q$ でなければならず, $Z(G)$ が p-群であると分かる.

後半を示すためには, $\exp Z(G) > p$ と仮定したとき $(\chi, \chi)_G$ が補題 1 によって決まる値を上回ってしまうことを確認する. しかし, 煩雑な計算になるのでここでは割愛する.

このように $Z(G) > 1$ の場合はうまく解決するので, 問題となるのは $Z(G) = 1$ の場合である. そこで,

$$Z(G) = 1, \quad L = \{\ell, \ell + p\}, \quad \ell \in \{-1, 1 - p\}$$

かつ, $|G|$ が p で割り切れないと仮定しよう. $\chi(1) = n$ とおくと, sharp 指標の定義より $|G| = (n - \ell)(n - \ell - p)$ と表される. $|L| = 2$ の場合の一般論から次が成り立つ.

補題 4. $p_1 \in \pi(n - \ell)$, $p_2 \in \pi(n - \ell - p)$ とする (ここで, $\pi(m)$ は m のすべての素因数からなる集合を表す). このとき, G は位数 $p_1 p_2$ の元を持たない.

上の補題より, G の素数グラフは少なくとも 2 つの連結成分を持つ. このような群は Williams [5] によって分類されており, その結果を用いると次のいずれかが成り立つことが分かる:

(a) G は Frobenius または 2-Frobenius,

(b) G の non-abelian composition factor S であって, $|G|_{\Gamma'} = |S|_{\Gamma'}$ を満たすものが存在する.

ここで, $\Gamma = \bigcup_{2|n-\chi(g)} \pi(g)$ である. 上の各ケースについて細かい計算と議論を経て矛盾が導かれる. 以下にそれぞれのアウトラインを紹介する.

(a) が成り立つとき

このとき, 2-Frobenius の定義から

$$N \leq K \leq G, \quad N \triangleleft G, \quad H : K \text{ の } G \text{ における補群},$$
$$HN : \text{Frobenius 群}$$

とおくことができる. $|G|$ が $n-\ell$ と $n-\ell-p$ という互いに素な 2 数の積で表されていることと補題 4 を用いると, $|H| = n-\ell$, $|K| = n-\ell-p$ が示される.

$M = HN$ とおき, χ の M への制限 χ_M を考える. M は Frobenius 群であるから, 補題 3 の証明と同様に, χ_M の既約成分のうち N を kernel に含むものの和を ψ, N を kernel に含まないものの和を θ とおき, $\chi_M = \psi + \theta$ と表す. このとき, M が Frobenius 群であることを用いて計算していくと, このようなケースが起こり得ないと分かる.

(b) が成り立つとき

$a := |G|_{\Gamma'}$, $b := |G|_{\Gamma}$ とおく. このとき明らかに $(a,b) = 1$ かつ

$$ab = |G| = (n-\ell)(n-\ell-p).$$

Γ の定め方と補題 4 より, $\{a,b\} = \{n-\ell, n-\ell-p\}$ でなければならない. $\ell \in \{-1, 1-p\}$ であるから, いずれのケースであっても $b < 2a+1$ が成り立つ.

すると, 仮定より $|S|_{\Gamma'} = a$ であるから, $|S|_{\Gamma} < 2|S|_{\Gamma'} + 1$ という条件を得る. しかし, この条件を満たす非可換単純群は決して多くない. その全てのケースをしらみ潰しに検証していった結果, 結局 (b) のケースは起こり得ないことが示せた.

以上より, G が自明な中心を持つ場合も $|G|$ は p の倍数となり, 定理 2 が証明される.

3. $Z(G) > 1$ のケースについて

一般に sharp 指標の議論では, 自明でない中心を持つ群のほうが扱いやすいことが多い. 実際, $L = \{\ell, \ell+p\}$, $\ell \in \{-1, 1-p\}$ のケースに関しても $Z(G) > 1$ の場合にはより多くの結果を得ることができる. 本節では我々が現在得ている結果を紹介する.

以下, $Z(G) > 1$ とする. このとき, 補題 3 と同様にして $Z = Z(G) \cong Z_p$ が得られる. さらに $(\chi, \chi)_G = p$ であるから, $\mathrm{Irr}(Z) = \{1_Z, \lambda, \ldots, \lambda^{p-1}\}$ とおけば,

$$\chi = \psi + (\theta_1 + \cdots + \theta_{p-1}), \quad \psi \in \mathrm{Irr}(G/Z), \quad \theta_i \in \mathrm{Irr}(G, \lambda^i)$$

と表すことができる (ここで, $\mathrm{Irr}(G, \lambda^i)$ は $(\lambda^i)^G$ の既約成分全体を表す). 簡単のため $n = \chi(1)$, $k = n - \ell$ とおく. このとき $|G| = p^2k(k-1)$ である.

$g \in G - Z$ に対して

$$\beta_g := \sharp\{x \in Z \mid \chi(gx) = \ell + p\}$$

と定めよう. このとき, $\psi(g) = \ell + \beta_g$ が成り立つ. 明らかに $\beta_g \in \{0, \ldots, p\}$ であるから, ψ が $G - Z$ で取る値は $\ell, \ell+1, \ldots, \ell+p$ のいずれかに限定される. この事実は非常に有用な手がかりである.

いま, $G - Z$ から p-元 g_1, g_2 をとると, $p \mid \psi(1) - \psi(g_i)$ である. よって

$$p \mid \psi(g_1) - \psi(g_2) = \beta_{g_1} - \beta_{g_2}.$$

となるので, $\beta_{g_1} = \beta_{g_2}$ であるか, さもなければ $\{\beta_{g_1}, \beta_{g_2}\} = \{0, p\}$ でなければならない. このことから, p-元における β_g の値について次のいずれかが成り立つ:

(A) $G - Z$ の任意の p-元 g に対し, $\beta_g = 0$ or p.

(B) $\exists C \notin \{0, p\}$ s.t. $G - Z$ の任意の p-元 g に対し $\beta_g = C$.

実は (B) $\iff p^3 \nmid |G|$ であることが証明できる. すなわち, 上の Case (A), Case (B) はそれぞれ $|G|$ が p^3 で割り切れる場合と割り切れない場合に対応している.

一方, θ_i が $\mathbb{Q}[\omega]$ $(\omega = \lambda(z))$ に値をとることに注目すると G の p'-元 g に対して $\theta_i(g)$ の値を計算することが可能で,

$$\theta_1(g) = \begin{cases} -\gamma & \text{if } o(g) \mid k, \\ 1 - \gamma & \text{if } o(g) \mid k-1 \end{cases}$$

となることが分かる. ただし, ここで γ は 0 か 1 のいずれかで,

$$\chi(z) = \ell + p\gamma \text{ for } 1 \neq z \in Z.$$

を満たすようにとる. このように ψ や θ_i の取る値が決まることにより, 様々な計算を行うことができるようになる.

たとえば, Case (A), Case (B) のいずれの場合にも $G/Z(G)$ の素数グラフが非連結になることが証明でき, また θ_i の p'-元での値が分かることから Case (B) の場合には θ_i が G の principal p-block に属することなどが示せる.

こうした議論を積み重ねて得られた次の定理が我々の第 2 の結果である:

定理 5. p を素数, $L = \{-1, p-1\}$ or $\{1-p, 1\}$, $Z(G) > 1$ とする. もし G が type L の sharp 指標 χ を持つならば, $G/Z(G)$ の素数グラフは非連結である. さらに ψ を χ の既約成分のうち $Z(G)$ を kernel に含む (唯一の) 既約指標とすれば, 次のいずれかが成り立つ:

(i) $|G| = p^2k(k-1)$ for $k \in \{p, p(p-1)/2\}$,
(ii) $|G|_p \geqq p^3$, かつ $\mathrm{Im}\,\psi = L \cup \{0\} \cup \{\psi(1)\}$,
(iii) $|G|_p = p^2$, $G = Z(G) \times R$, かつ $G/Z(G)$ の Sylow p-部分群は self-centralizing.

本稿で上の定理の完全な証明を説明することはできないが, 現在これらの結果を用いて $L = \{-1, p-1\}$ or $\{1-p, 1\}$, $Z(G) > 1$ の場合の完全な分類を進めており, 現在よりも完成された形で発表される見通しである.

参考文献

[1] D. Alvis, S. Nozawa, *Sharp characters with irrational values*, J. Math. Soc. Japan 48 (1996) 567–591.

[2] H. F. Blichfeldt, *A theorem concerning the invariants of linear homogeneous groups with some applications to substitution groups*, Trans. Amer. Math. Soc. 5 (1904) 461–466.

[3] P. J. Cameron and M.Kiyota, *Sharp characters of finite groups*, J. Algebra 115 (1988) 125–143.

[4] N. Iiyori and H.Yamaki, *Prime Graph Components of the Simple Groups of Lie Type over the Field of Even Characteristic*, J. Algebra 155 (1993) 335–343.

[5] J. S. Williams, *Prime Graph Components of Finite Groups*, J. Algebra 69 (1981) 487–513.

THE PARTIAL BURNSIDE RING RELATIVE TO p-CENTRIC SUBGROUPS

FUMIHITO ODA

1. Introduction

Let G be a finite group and let p be a prime. Let $\mathfrak{X}$ be a family of subgroups of G such that it is closed under taking G-conjugation. In [Yo90], some conditions such that the R-submodule $R \otimes_{\mathbf{Z}} \Omega(G, \mathfrak{X})$ of ordinary Burnside algebra $R \otimes_{\mathbf{Z}} \Omega(G)$ over a commutative ring R has ring structure are considered. If $\mathfrak{X}$ satisfies the condition $(\mathbf{C})_p$ (see 3.6 of [Yo90]), then $\Omega(G, \mathfrak{X})_{(p)}$ has a canonical ring structure (see 3.11 of [Yo90]). The ring $\Omega(G, \mathfrak{X})_{(p)}$ was called a generalized Burnside ring with respect to $\mathfrak{X}$ in [Yo90], [Od96] and [OY01]. Recently, there are some generalized version of Burnside ring for some mathematical objects. For instance the ring $\Omega(G, \mathfrak{X})$ is called a partial Burnside ring relative to $\mathfrak{X}$ in [Ta06], if $\Omega(G, \mathfrak{X})$ is a subring of the ordinary Burnside ring $\Omega(G)$.

The present report is a survey of [Od]. The purpose of this report is to show that if $\mathfrak{X}$ is the set of all p-centric subgroups of G then $\Omega(G, \mathfrak{X})_{(p)}$ is a generalized Burnside ring with respect to $\mathfrak{X}$. A key lemma (Lemma 3.2) of the main results (Theorem 3.10 and Corollary 3.11) of this paper is used to show that the family $\mathfrak{X}$ satisfies the condition $(\mathbf{C})_p$ that is discussed in [Yo90]. The lemma is used by Sawabe's work on the reduced Lefschetz module (see Proposition 6 of [Sa06]). The family $\mathfrak{X}$ of all p-centric subgroups of G is the first example such that it satisfies the condition $(\mathbf{C})_p$ but not closed under taking subgroups.

Díaz and Libman showed that the ring $\Omega(G, \mathfrak{X})_{(p)}$ is isomorphic to the Burnside ring $\mathcal{A}(\mathcal{F})_{(p)}$ of the fusion system associated to G and a Sylow p-subgroup in [DL07]. They showed some properties of $\mathcal{A}(\mathcal{F})_{(p)}$ for any saturated fusion system $\mathcal{F}$ (Theorem 1.4 and Theorem 1.5 of [DL07]). Assuming Theorem 1.6 of [DL07], our Theorem 3.13 and 3.14 give alternative proofs in a particular case of Theorem 1.4 and 1.5 there. However, those are special case of their original results.

The paper is organized as follows: Section 2 recalls some definitions and results from the theory of generalized Burnside ring of [Yo90]. Section 3 is an application to the all p-centric subgroups of G, showing main results, relationship between our results and those of [DL07].

2. The generalized Burnside ring

2.1. Notation. If G is a finite group and p a prime, denote by G_p a Sylow p-subgroup of G, by $|G|_p$ the order of G_p and by $|G|_{p'}$ is the quotient $|G|/|G|_p$. Let $\mathfrak{X}$ be a family of subgroups of a finite group G such that it is closed under G-conjugation. If X is a finite G-set, denote by $[X]$ the isomorphism class of finite G-sets containing X. Denote by WH the quotient group $N_G(H)/H$. If H is a subgroup of G, denote by (H) the G-conjugacy

class $\{{}^gH|g \in G\}$, where ${}^gH = gHg^{-1}$. If $g \in G$ is an element of G, denote by $\langle g \rangle$ the cyclic group generated by g.

2.2. The mark homomorphism. Let $\Omega(G, \mathfrak{X})$ be the submodule of the ordinary Burnside ring $\Omega(G)$ of a finite group G generated by elements $[G/H]$ for $H \in \mathfrak{X}$. Then $\Omega(G, \mathfrak{X})$ is a free $\mathbb{Z}$-module with basis $\{[G/H]|(H) \in C(\mathfrak{X})\}$, where $C(\mathfrak{X})$ is the set of the G-conjugacy classes of a family $\mathfrak{X}$ of subgroups of G. The direct product $\prod_{(S)\in C(\mathfrak{X})} \mathbb{Z}$ of copies of the ring $\mathbb{Z}$ will be denoted by $\tilde{\Omega}(G, \mathfrak{X})$. Let φ_S denote the additive map from $\Omega(G, \mathfrak{X})$ to $\mathbb{Z}$ defined by $[G/H] \mapsto |(G/H)^S|$, where $|(G/H)^S|$ is the cardinality of the S-fixed points of the G-set G/H for a subgroup S of G. Thus we have an additive homomorphism relative to $\mathfrak{X}$

$$\varphi := (\varphi_S)_{(S)} : \Omega(G, \mathfrak{X}) \to \tilde{\Omega}(G, \mathfrak{X}) : x \mapsto (\varphi_S(x))$$

and φ is called a *mark homomorphism*. For any element $x \in \Omega(G, \mathfrak{X})$ and any subgroup S in $\mathfrak{X}$, we often write $x(S) = \varphi_S(x)$. For a prime p, let $\mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at p :

$$\mathbb{Z}_{(p)} := \{a/b|a \in \mathbb{Z},\ b \in \mathbb{Z}\backslash p\mathbb{Z}\} \subseteq \mathbb{Q}.$$

For a $\mathbb{Z}$-module M, we set $M_{(p)} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M$, and denote by $\varphi_{(p)} : \Omega(G, \mathfrak{X})_{(p)} \to \tilde{\Omega}(G, \mathfrak{X})_{(p)}$ the map induced by the mark homomorphism φ.

2.3. Condition $(\mathrm{C})_p$. Let p be a prime. We use the notation for a subgroup H of G that $\overline{H} := \cap\{S \in \mathfrak{X}|H \leq S\}$. We put $\overline{H} = G$ if there is no element $U \in \mathfrak{X}$ containing H. In [Yo90] Yoshida introduced the following condition:

$(\mathrm{C})_p$ $\quad gS \in (WS)_p,\quad S \in \mathfrak{X} \Rightarrow \overline{\langle g \rangle S} \in \mathfrak{X},$

where $(WS)_p$ is a Sylow p-subgroup of WS.

2.4. The Cauchy-Frobenius homomorphism. The direct product $\prod_{(S)\in C(\mathfrak{X})}(\mathbb{Z}/|WS|\mathbb{Z})$ of the quotient groups will be denoted by $\mathrm{Obs}(G, \mathfrak{X})$. The *Cauchy-Frobenius homomorphism* $\psi_{(p)}$ from $\tilde{\Omega}(G, \mathfrak{X})_{(p)}$ to $\mathrm{Obs}(G, \mathfrak{X})_{(p)}$ is defined by

$$(y(S))_{(S)} \longmapsto \left(\sum_{gS\in(WS)_p} y(\overline{\langle g \rangle S}) \mod |WS|_p \right)_{(S)}.$$

Theorem 2.5. (Yoshida [Yo90] 3.10, 3.11). *Let p be a prime. Then under the condition $(\mathrm{C})_p$, the following sequence of $\mathbb{Z}_{(p)}$-modules is exact:*

$$0 \longrightarrow \Omega(G, \mathfrak{X})_{(p)} \xrightarrow{\varphi_{(p)}} \tilde{\Omega}(G, \mathfrak{X})_{(p)} \xrightarrow{\psi_{(p)}} \mathrm{Obs}(G, \mathfrak{X})_{(p)} \longrightarrow 0. \tag{2.1}$$

Moreover, $\Omega(G, \mathfrak{X})_{(p)}$ has a unique ring structure such that $\varphi_{(p)}$ is a ring homomorphism.

Remark 2.6. If x and y are elements in $\Omega(G, \mathfrak{X})_{(p)}$, denote by $x \bullet y$ the product of x and y over $\Omega(G, \mathfrak{X})_{(p)}$ defined by

$$x \bullet y := (\varphi_{(p)})^{-1} (\varphi_{(p)}(x)\varphi_{(p)}(y)).$$

Definition 2.7. Let R be a commutative ring. The R-module $R \otimes_{\mathbb{Z}} \Omega(G, \mathfrak{X})$ is called a *generalized Burnside ring with respect to* $\mathfrak{X}$ provided it has ring structure with identity element such that the homomorphism

$$1 \otimes \varphi : R \otimes_{\mathbb{Z}} \Omega(G, \mathfrak{X}) \to R \otimes_{\mathbb{Z}} \widetilde{\Omega}(G, \mathfrak{X})$$

is an injective ring homomorphism.

Remark 2.8. If $\mathfrak{X}$ satisfies the condition $(\mathbf{C})_p$, and if the commutative ring R is p-torsion free and $|G|_{p'}$ is invertible in R, then by Theorem 2.5, $R \otimes_{\mathbb{Z}} \Omega(G, \mathfrak{X})$, particularly $\Omega(G, \mathfrak{X})_{(p)}$ is a generalized Burnside ring with respect to $\mathfrak{X}$.

Proposition 2.9. *Let* $\bullet$ *be the multiplication of* $\Omega(G, \mathfrak{X})_{(p)}$ *defined by Remark 2.6. Then* $x \bullet y = xy$ *in* $\Omega(G)_{(p)}$ *for* $x, y \in \Omega(G, \mathfrak{X})_{(p)}$ *if and only if* $\mathfrak{X}$ *is closed by intersection.*

Proof: If $x \bullet y = xy$ in $\Omega(G)_{(p)}$ for $x, y \in \Omega(G, \mathfrak{X})_{(p)}$, then we have that

$$[G/H] \bullet [G/K] = [G/H][G/K] = \sum_{g \in [H \backslash G / K]} [G/H \cap {}^gK]$$

for any $H, K \in \mathfrak{X}$ and $\Omega(G, \mathfrak{X})_{(p)}$ must contain $\sum_{g \in [H \backslash G / K]} [G/H \cap {}^gK]$. Hence the family $\mathfrak{X}$ must contain $H \cap {}^gK$ for any $g \in G$.

On the other hand, if $\mathfrak{X}$ is closed by intersection, then $\Omega(G, \mathfrak{X})$ contains $\sum_{g \in H \backslash G / K} [G/H \cap {}^gK]$. Since $\sum_{g \in H \backslash G / K} [G/H \cap {}^gK] = [G/H][G/K]$ in $\Omega(G)$, $\Omega(G, \mathfrak{X})_{(p)}$ contains $[G/H][G/K]$. Then we have $[G/H] \bullet [G/K] = [G/H][G/K]$, because $\varphi_{(p)}([G/H]) \cdot \varphi_{(p)}([G/K]) = \varphi_{(p)}([G/H][G/K])$. Proposition 2.9 follows by Remark 2.6. □

2.10. Condition $(\mathbf{C}')_p$. In [Yo90] Yoshida introduced the following condition:

$(\mathbf{C}')_p$ $\quad gS \in (WS)_p, \quad S \in \mathfrak{X} \Rightarrow \langle g \rangle S \in \mathfrak{X}.$

If $\mathfrak{X}$ satisfies the condition $(\mathbf{C}')_p$, then the condition $(\mathbf{C})_p$ holds trivially, and so $\Omega(G, \mathfrak{X})_{(p)}$ is a generalized Burnside ring with respect to $\mathfrak{X}$ by Theorem 2.5.

2.11. The equivalence relation $\sim_p$. We assume the condition $(\mathbf{C})_p$, so that by Theorem 2.5, $\Omega(G, \mathfrak{X})_{(p)}$ is a generalized Burnside ring with respect to $\mathfrak{X}$. Let $\sim_p$ be the equivalence relation on $C(\mathfrak{X})$ generated by the relation

$$\left(\overline{\langle g \rangle S}\right) \sim_p (S) \quad \text{for} \quad S \in \mathfrak{X},\ gS \in (WS)_p. \tag{2.2}$$

This relation can be lifted to $\mathfrak{X}$, that is, $S \sim_p T$ if and only if $(S) \sim_p (T)$.

2.12. Primitive idempotents. If $Q \in \mathfrak{X}$, denoted by e_Q^p the sum $\sum e_H$ of idempotents $e_H \in \mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G, \mathfrak{X})$, where $(H) \in C(\mathfrak{X})$ with $H \sim_p Q$ (see Theorem 4.2 of [Yo90]). Let $\mu_{\mathfrak{X}} : \mathfrak{X} \times \mathfrak{X} \to \mathbb{Z}$ be the Möbius function on the poset $\mathfrak{X}$ with the order relation by inclusion. Yoshida computed the idempotent e_Q^p of $\Omega(G, \mathfrak{X})_{(p)}$ for $Q \in \mathfrak{X}$ as follows:

$$e_Q^p = \sum_{(D) \in C(\mathfrak{X})} \frac{1}{|WD|} \left(\sum_{H \sim_p Q} \mu_{\mathfrak{X}}(D, H) \right) [G/D].$$

Theorem 2.13. (Yoshida [Yo90] 4.12). *Under the condition* $(\mathbf{C})_p$, *the element* e_Q^p *is a primitive idempotent of* $\Omega(G,\mathfrak{X})_{(p)}$, *and conversely any primitive idempotent of* $\Omega(G,\mathfrak{X})_{(p)}$ *has this form. Thus the set of primitive idempotents of* $\Omega(G,\mathfrak{X})_{(p)}$ *is bijectively corresponding to the equivalence classes of the equivalence relation* $\sim_p$ *in* $C(\mathfrak{X})$.

Yoshida determined the prime ideals of the generalized Burnside ring $\Omega(G,\mathfrak{X})_{(p)}$ by the method of Dress.

Theorem 2.14. (Yoshida [Yo90] 5.12 and 5.13). *Assume that the condition* $(\mathbf{C})_p$ *holds for* $\mathfrak{X}$. *Then there is a bijective correspondence between the connected components of prime ideals of* $\Omega(G,\mathfrak{X})_{(p)}$ *and* $\sim_p$*-equivalence classes. Moreover, the set* $\{(D) \in C(\mathfrak{X}) | WD \text{ is a } p'\text{-group } \}$ *is a complete set of representatives of* $\sim_p$*-equivalence classes.*

3. p-CENTRIC SUBGROUPS

Definition 3.1. A p-subgroup P of G is said to be *p-centric* if the centralizer $C_G(P)$ is the product of the center of P and a group of order prime to p. This is equivalent to the condition that the center $Z(P)$ of P be a Sylow p-subgroup of $C_G(P)$. The subgroup P is p-centric if and only if $Z(P) = C_S(P)$ for any Sylow subgroup S of G containing P. Denote by $\mathcal{C}_p(G)$ the set of all p-centric subgroups of G.

Lemma 3.2. (e.g. see Proposition 6 of [Sa06]).*Let* $\mathfrak{X}$ *be* $\mathcal{C}_p(G)$. *If* $Q \leq P$ *for* $Q \in \mathfrak{X}$ *and* P *is a p-subgroup of* G, *then* $P \in \mathfrak{X}$. *In particular, any Sylow p-subgroup is p-centric.*

Proof: Suppose that $Q \leq P$ for $Q \in \mathfrak{X}$ and $P \leq G$ is a p-subgroup. Then $C_G(P) \leq C_G(Q)$, and thus any p-element g in $C_G(P)$ is contained in $C_G(Q)$. Since Q is p-centric, we have $x \in Q \leq P$, which implies that P is p-centric. □

Proposition 3.3. *Let* $\mathfrak{X}$ *be* $\mathcal{C}_p(G)$. *Then* $\mathfrak{X}$ *satisfies the condition* $(\mathbf{C})_p$.

Proof: Let $P \in \mathfrak{X}$ and $gP \in (WP)_p$. The groups P and $(WP)_p$ are p-groups, so is $\langle g \rangle$. Since $P \leq \langle g \rangle P$ and $\langle g \rangle P$ is a p-group, $\langle g \rangle P \in \mathfrak{X}$ by Proposition 3.2. Hence $\mathfrak{X}$ satisfies the condition $(\mathbf{C}')_p$, hence also the condition $(\mathbf{C})_p$. □

Proposition 3.3 and Proposition 2.5 show the following corollary.

Corollary 3.4. *Let* $\mathfrak{X}$ *be* $\mathcal{C}_p(G)$. *Then* $\Omega(G,\mathfrak{X})_{(p)}$ *is a generalized Burnside ring with respect to* $\mathfrak{X}$. *In particular, the ring* $\Omega(G,\mathfrak{X})_{(p)}$ *has an identity element.*

If $\mathfrak{X} = \mathcal{C}_p(G)$, then we can determine the complete set of representatives of $\sim_p$-equivalence classes.

Proposition 3.5. *Let* $\mathfrak{X}$ *be* $\mathcal{C}_p(G)$. *Then the Sylow p-subgroups are the only p-centric subgroups of* G *such that the order* $|WQ|$ *is not divisible by* p *for* $Q \in \mathfrak{X}$.

Proof:Let S be a Sylow p-subgroup of G. Then $|WS|$ is not divisible by p. Let Q be a proper subgroup of S. Then $|WQ|$ is divisible by p because Q is a non maximal p-subgroup of G. □

Theorem 2.14, Proposition 3.5 and 2.12 show the following corollary.

Corollary 3.6. *Let $\mathfrak{X}$ be $\mathcal{C}_p(G)$. Then the generalized Burnside ring $\Omega(G,\mathfrak{X})_{(p)}$ with respect to $\mathfrak{X}$ is a local ring. The identity element of $\Omega(G,\mathfrak{X})_{(p)}$ is*

$$e^p_{G_p} = \sum_{(D)\in C(\mathfrak{X})} \frac{1}{|WD|}\left(\sum_{H\sim_p G_p} \mu_{\mathfrak{X}}(D,H)\right)[G/D].$$

Remark 3.7. Let $\mathcal{S}_p(G)$ be the family of all p-subgroups of G and let $\mathcal{C}^n_p(G)$ be the family $\mathcal{S}_p(G)\backslash\mathcal{C}_p(G)$ of non-p-centric p-subgroups of G. Since $\mathcal{S}_p(G)$ satisfies the condition $(\mathrm{C}')_p$, it satisfies the condition $(\mathrm{C})_p$. By Theorem 2.5, $\Omega(G,\mathcal{S}_p(G))_{(p)}$ is a generalized Burnside ring. The module $\Omega(G,\mathcal{C}^n_p(G))_{(p)}$ is an ideal of $\Omega(G,\mathcal{S}_p(G))_{(p)}$. Díaz and Libman introduced a quotient ring $\mathcal{A}^{p\text{-cent}}(G)_{(p)}$ whose free basis is $C(\mathcal{C}_p(G))$ as $\mathbb{Z}_p$-module (see 5.1 of [DL07]). Denote by H^g the subgroup $g^{-1}Hg$ of G for $g\in G$. The product of basis elements (P) and (Q) is $\sum_g(Q^g\cap P)$ where the sum ranges through the double cosets QgP such that $Q^g\cap P$ is p-centric. We can regard the quotient $\Omega(G,\mathcal{S}_p(G))_{(p)}/\Omega(G,\mathcal{C}^n_p(G))_{(p)}$ as a $\mathbb{Z}_{(p)}$-module $\mathcal{A}^{p\text{-cent}}(G)_{(p)}$ by identifying a representative $[G/P]$ of a basis of the quotient ring with an element (P), where $P\in\mathcal{C}_p(G)$. Moreover, the map is a ring isomorphism (see Corollary 3.11).

Lemma 3.8. *Let $Q\in\mathcal{C}^n_p(G)$. Then $\varphi_P([G/Q])=0$ for any $P\in\mathcal{C}_p(G)$.*

Proof: For a pair H and K of subgroups of G $\varphi_K([G/H]) = \sharp\mathrm{Map}_G(G/K,G/H)$, where $\mathrm{Map}_G(G/K,G/H)$ is the set of G-maps from G/K to G/H. Hence $\varphi_K([G/H])\neq 0$ if and only if $K\leq_G H$. If $Q\in\mathcal{C}^n_p(G)$ then P is not G-conjugate subgroup of Q for any $P\in\mathcal{C}_p(G)$. So $\varphi_P([G/Q])=0$. □

Lemma 3.9. *Let $Q\in\mathcal{S}_p(G)$. If $\varphi_P([G/Q])=0$ for any $P\in\mathcal{C}_p(G)$, then $Q\in\mathcal{C}^n_p(G)$.*

Proof: Let $Q\in\mathcal{C}_p(G)$. Then $\varphi_Q([G/Q]) = |WQ|\neq 0$. □

Theorem 3.10. *The generalized Burnside ring $\Omega(G,\mathcal{C}_p(G))_{(p)}$ is isomorphic to the quotient ring*
$\Omega(G,\mathcal{S}_p(G))_{(p)}/\Omega(G,\mathcal{C}^n_p(G))_{(p)}$.

Proof: We give a linear map ρ from $\Omega(G,\mathcal{S}_p(G))_{(p)}$ to $\Omega(G,\mathcal{C}_p(G))_{(p)}$. Let x be an element of $\Omega(G,\mathcal{S}_p(G))_{(p)}$. We note that $\varphi_Q([G/P])=0$ for $Q\in\mathcal{C}_p(G)$ and $P\in\mathcal{C}^n_p(G)$ by Lemma 3.8. Let χ be the element $(x(Q))_{(Q)\in C(\mathcal{C}_p(G))}$ in $\widetilde{\Omega}(G,\mathcal{C}_p(G))_p$, where $x(Q)$ is the image of x by $\Omega(G,\mathcal{C}_p(G))_{(p)}\hookrightarrow\Omega(G,\mathcal{S}_p(G))_{(p)}\xrightarrow{\varphi_Q}\mathbb{Z}_{(p)}$. Since $\mathcal{C}_p(G)$ satisfies the condition $(\mathrm{C}')_p$ by the proof of Proposition 3.3, $\overline{\langle g\rangle Q} = \langle g\rangle Q$ for any $S\in\mathcal{C}_p(G)$. We have that

$$\psi_{(p)}(\chi) = \sum_{gQ\in(WQ)_p}\chi(\overline{\langle g\rangle Q}) = \sum_{gQ\in(WQ)_p}\chi(\langle g\rangle Q)\equiv 0 \ (\mathrm{mod}\ \ |WQ|_p)$$

for any $Q\in\mathcal{C}_p(G)$ by the lemma of Cauchy-Frobenius. By Theorem 2.5, we have that χ is contained in $\Omega(G,\mathcal{C}_p(G))_{(p)}$. The linear map ρ is obtained by $\rho(x)=\chi$. Lemma 3.8 and

Lemma 3.9 show that $\mathrm{Ker}(\rho) = \Omega(G, \mathcal{C}_p^n(G))_{(p)}$. The map ρ makes the following diagram of $\mathbb{Z}_{(p)}$-modules commutative:

$$\begin{array}{ccc} \Omega(G, \mathcal{S}_p(G))_{(p)} & \xrightarrow{\rho} & \Omega(G, \mathcal{C}_p(G))_{(p)} \\ \downarrow{\scriptstyle \varphi'_{(p)}} & & \downarrow{\scriptstyle \varphi_{(p)}} \\ \widetilde{\Omega}(G, \mathcal{S}_p(G))_p & \xrightarrow{\pi} & \widetilde{\Omega}(G, \mathcal{C}_p(G))_{(p)}, \end{array}$$

where π is the projection.

We have to show that ρ is a ring homomorphism. Let $x, y \in \Omega(G, \mathcal{S}_p(G))_{(p)}$. We show that $\rho(x) \bullet \rho(y) = \rho(xy)$ in $\Omega(G, \mathcal{C}_p(G))_{(p)}$. We have that

$$\rho(x) \bullet \rho(y) = \varphi_{(p)}^{-1}(\varphi_{(p)}(\rho(x))\varphi_{(p)}(\rho(y))) = \varphi_{(p)}^{-1}(\pi\varphi'_{(p)}(x)\pi\varphi'_{(p)}(y)) = \varphi_{(p)}^{-1}\pi\varphi'_{(p)}(xy) = \rho(xy)$$

by Remark 2.6 and the commutativity of the diagram above. □

Corollary 3.11. *The generalized Burnside ring $\Omega(G, \mathcal{C}_p(G))_{(p)}$ is isomorphic to $\mathcal{A}^{p\text{-cent}}(G)_{(p)}$.*

Proof: There exists an isomorphisms of $\mathbb{Z}_p$-module from $\Omega(G, \mathcal{C}_p(G))_{(p)}$ to $\mathcal{A}^{p\text{-cent}}(G)_{(p)}$ defined by sending $[G/P]$ to (P) for $P \in \mathcal{C}_p(G)$. Since $\Omega(G, \mathcal{C}_p(G))_{(p)}$ is commutative and $[G/Q \cap {}^gP] = [G/Q^g \cap P]$ for any $g \in G$, so it suffices to show that $[G/Q] \bullet [G/P] = \sum_{g \in [Q\backslash \mathcal{C}_p(G)/P]} [G/Q \cap {}^gP]$, where $[Q\backslash \mathcal{C}_p(G)/P]$ is the subset of $[Q\backslash G/P]$ consisting of elements g such that $Q \cap {}^gP \in \mathcal{C}_p(G)$, by the note on the product of $\mathcal{A}^{p\text{-cent}}(G)_{(p)}$ in Remark 3.7. Let ρ be the surjective ring homomorphism from $\Omega(G, \mathcal{S}_p(G))_{(p)}$ to $\Omega(G, \mathcal{C}_p(G))_{(p)}$ in Theorem 3.10. Then

$$[G/Q] \bullet [G/P] = \rho([G/Q]) \bullet \rho([G/P]) = \rho([G/Q][G/P]) = \rho\left(\sum_{g \in [Q\backslash G/P]} [G/Q \cap {}^gP]\right)$$

$$= \sum_{g \in [Q\backslash G/P]} \rho([G/Q \cap {}^gP]) = \sum_{g \in [Q\backslash \mathcal{C}_p(G)/P]} \rho([G/Q \cap {}^gP]) = \sum_{g \in [Q\backslash \mathcal{C}_p(G)/P]} [G/Q \cap {}^gP],$$

because $\mathrm{Ker}(\rho) = \Omega(G, \mathcal{C}_p^n(G))$. □

In this paper, we use the following theorem.

Theorem 3.12. (Díaz and Libman [DL07] Theorem 5.11). *Let $\mathcal{F}$ be the fusion system associated to a finite group G and a Sylow p-subgroup S. Then the rings $\mathcal{A}(\mathcal{F})_{(p)}$ and $\mathcal{A}^{p\text{-cent}}(G)_{(p)}$ are isomorphic.*

Then we have the following theorems of Díaz and Libman those are restricted to the case of their assumption.

Theorem 3.13. *Let $\mathcal{F}$ be the fusion system associated to a finite group G and a Sylow p-subgroup S. Then the ring $\mathcal{A}(\mathcal{F})_{(p)}$ has a unit.*

Proof: Theorem 3.12, Corollary 3.11 and Corollary 3.4 show the theorem. □

Theorem 3.14. *Let $\mathcal{F}$ be the fusion system associated to a finite group G and a Sylow p-subgroup S. Then the ring $\mathcal{A}(\mathcal{F})_{(p)}$ is local.*

Proof: Theorem 3.12, Corollary 3.11 and Corollary 3.6 show the theorem. □

REFERENCES

[DL07] A. DÍAZ AND A. LIBMAN, The Burnside ring of fusion systems, *preprint.* (2007).

[Od96] F. ODA, A note on the decomposition of the Burnside rings of finite groups, *Hokkaido Math. J.* **25** (1996), no. 1, 93–96.

[Od] F. ODA, The generalized Burnside ring with respect to p-centric subgroups, *preprint.*

[OY01] F. ODA AND T. YOSHIDA, On the generalized Burnside ring with respect the Young subgroups of the symmetric group, *J. Algebra* **236** (2001), 349–354.

[Sa06] M. SAWABE, On the reduced Lefschetz module and the centric p-radical subgroups II., *J. London Math. Soc.(2)* **73** (2006), 126–140.

[Ta06] D. TAMBARA, A partial Burnside ring of $GL(n,q)$ relative to line stabilizers, *J. Algebra* **296** (2006), 301–322.

[Yo90] T. YOSHIDA, The generalized Burnside ring of a finite group, *Hokkaido Math. J.* **19** (1990), 509–574.

(F. Oda) DEPARTMENT OF LIBERAL ARTS, TOYAMA NATIONAL COLLEGE OF TECHNOLOGY, TOYAMA 939-8630, JAPAN

E-mail address: oda@toyama-nct.ac.jp

A Wei type duality for matroids*

愛知県立大学　情報科学部　城本 啓介 (Keisuke Shiromoto)
Department of Information Systems
Aichi Prefectural University

1 Introduction

本稿では，q-元体 $\mathbb{F}_q$ 上の n 次元ベクトル空間の k 次元部分空間 C を $[n,k]$（線形）符号と言い，以後使用する記号等を次のように定める．

任意のベクトル $\boldsymbol{x}=(x_1,\ldots,x_n),\boldsymbol{y}=(y_1,\ldots,y_n)\in\mathbb{F}_q^n$ に対して，

$$\begin{aligned}\mathrm{supp}(\boldsymbol{x}) &:= \{i : x_i\neq 0\},\\ \mathrm{wt}(\boldsymbol{x}) &:= |\mathrm{supp}(\boldsymbol{x})| = |\{i : x_i\neq 0\}|,\\ \boldsymbol{x}\cdot\boldsymbol{y} &:= \sum_{i=1}^{n} x_iy_i\end{aligned}$$

として，特に $\min\{\mathrm{wt}(\boldsymbol{x}) : 0\neq\boldsymbol{x}\in C\}=d$ の時，C を $[n,k,d]$ 符号と言う．さらに，符号 C に対して，

$$W_C(x,y) := \sum_{\boldsymbol{v}\in C} x^{n-\mathrm{wt}(\boldsymbol{v})}y^{\mathrm{wt}(\boldsymbol{v})} = \sum_{i=0}^{n} A_ix^{n-i}y^i$$

を重み多項式と言い，ここで $A_i=A_i(C)=|\{\boldsymbol{x}\in C : \mathrm{wt}(\boldsymbol{x})=i\}|$ である．また，符号 C の双対符号を

$$C^{\perp} := \{\boldsymbol{y}\in\mathbb{F}_q^n : \boldsymbol{x}\cdot\boldsymbol{y}=0,\ \forall\boldsymbol{x}\in C\}$$

とする．

本稿では，符号とその双対符号との関係を表すものを双対性 (duality) と言い，以下に良く知られたものを挙げる．

命題 1 (MacWilliams identity (cf. [2]))

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|}W_C(x+(q-1)y,x-y)$$

*本研究は Thomas Britz 氏 (University of New South Wales, Australia) との共同研究の一部である．

$[n,k]$ 符号 C と部分集合 $M \subseteq N = \{1,2,\ldots,n\}$ に対して，

$$\begin{aligned} C(M) &:= \{x \in C : \mathrm{supp}(x) \subseteq M\}, \\ C^* &:= \mathrm{Hom}_{\mathbf{F}_q}(C, \mathbf{F}_q) \end{aligned}$$

と定めたとき，

命題 2 (Yoshida's algebraic duality (cf. [8], [9]))

$$0 \longrightarrow C^{\perp}(M) \xrightarrow{\mathrm{inc}} \mathbf{F}_q^n(M) \xrightarrow{f} C^* \xrightarrow{\mathrm{res}} C(N-M)^* \longrightarrow 0$$

は完全系列である．ここで，$f : x \longmapsto (\hat{x} : y \mapsto x \cdot y)$ とする．

例えば命題2の双対性を用いて，命題1の恒等式やシングレトン限界式などについて，より代数的な別証を与えることができたり，命題1の恒等式から自己双対符号の最小ハミング重みに関する限界式や分類等を行うことができる．

一般化ハミング重み (generalized Hamming weights (GHW)) とは，通常，各符号語（ベクトル）に対して定義されているハミング重みを各部分符号（部分空間）に対して一般化して定義したものであり，V. Wei によって情報セキュリティ分野への応用を意識して導入された ([6])．$[n,k]$ 符号 C と整数 r $(1 \le r \le k)$ に対して，

$$d_r = d_r(C) := \min\{\mathrm{Wt}(D) : \dim(D) = r,\ D \le C\}.$$

で定める．ここで，

$$\mathrm{Wt}(D) = |\mathrm{Supp}(D)| = \left| \bigcup_{x \in D} \mathrm{supp}(x) \right|$$

とする．さらに，$\{d_1, d_2, \ldots, d_k\}$ を符号 C の weight hierarchy と言い，様々な符号に対して決定することが重要な問題とされている．例えば，ハミング符号や BCH 符号，MDS 符号などについては既に決定されている (cf. [6], [5])．

ここで，一般化ハミング重みに関する双対性の一つとして以下の恒等式が知られている．

命題 3 (Wei's duality for GHW ([6]))

$$\{d_r(C) : 1 \le r \le k\} = \{1,2,\ldots,n\} - \{n+1-d_{r'}(C^{\perp}) : 1 \le r' \le n-k\}.$$

本研究の目的としては，符号理論における様々な双対性をマトロイドへ拡張し，マトロイド理論における様々な問題を符号理論的考察によって新たな視点から検討することである．特に，本稿においては，上記の命題3の双対性をマトロイドへ一般化したものを紹介する．

2 Dualities in Matroid Theory

本題に入る前に，マトロイドの定義といくつかの双対性について紹介する．なお，マトロイド理論の詳細は [4] や [7] を参照されたい．

定義 4 マトロイドとは，有限集合 E とその部分集合族 $\mathcal{I}$ で以下の3つの条件を満たす組 $\mathcal{M}=(E,\mathcal{I})$ のことである．

(I1) $\emptyset \in \mathcal{I}$
(I2) $X \in \mathcal{I}$ かつ $Y \subseteq X$ ならば $Y \in \mathcal{I}$ である．
(I3) $|Y|<|X|$ である $X,Y \in \mathcal{I}$ に対して，$Y \cup \{e\} \in \mathcal{I}$ である $e \in X-Y$ が存在する．

特に，任意の $I \in \mathcal{I}$ を独立集合と言い，$D \notin \mathcal{I}$ を従属集合と言う．また，マトロイドにおける重要な構造として以下のものが挙げられる．

・極大な独立集合を $\mathcal{M}$ の基底と言い，それらの集合族を $\mathcal{B}$ で表す．
・極小な従属集合を $\mathcal{M}$ のサーキットと言い，それらの集合族を $\mathcal{C}$ で表す．
・$\mathcal{M}$ の rank function とは，以下に定義される関数 $\rho : 2^E \to \mathbb{Z}^+ \cup \{0\}$ のことである．

$$\rho(X)=\max\{|Y| : Y \subseteq X, Y \in \mathcal{I}\},\ \forall X \subseteq E$$

特に，$\rho(E)$ を $\mathcal{M}$ の階数とする．

マトロイドは，例えば基底族やサーキット族からも同様に一意的に定義することができる (cf. [4], [7])．

マトロイド理論における重要な問題の一つに，どのような組合せ構造からマトロイドを構成できるかということが挙げられる．例えば，A を $\mathbb{F}_q$ 上の $m \times n$ 行列とする．E を A の列番号の集合とし，$\mathcal{I}$ を A の列ベクトルの中で1次独立な列ベクトルの列番号の集合族とする．このとき，$(E,\mathcal{I})$ はマトロイドの定義を満たすことが直ちに分かるので一種のマトロイドである．このような構成法により構成されたマトロイドをベクトルマトロイドと言う．他にも，グラフのサイクル集合族から構成されるマトロイド等がある．

E 上のマトロイド $\mathcal{M}$ に対して，$\{E-B : B \in \mathcal{B}\}$ を基底族とするマトロイドを $\mathcal{M}$ の双対マトロイドと言い，$\mathcal{M}^*$ で表す．このとき，マトロイドとその双対マトロイドの間の双対性として以下のものが良く知られている．

補題 5 $\mathcal{M}^*$ の rank function を ρ^* とするとき，$X \subseteq E$ に対して，

$$\rho^*(X)=|X|-\rho(E)+\rho(E-X)$$

が成立する．

E 上のマトロイド $\mathcal{M}$ に対して，Tutte 多項式を次のように定義する．

$$T_{\mathcal{M}}(x,y) := \sum_{S \subseteq E}(x-1)^{\rho(E)-\rho(S)}(y-1)^{|S|-\rho(S)}.$$

このとき，以下の恒等式が成立する．

命題 6

$$T_{\mathcal{M}^*}(x,y)=T_{\mathcal{M}}(y,x).$$

符号理論とマトロイド理論の関係性は古くから研究がされており，特に上記の双対性を用いてマックリウィリアムズ恒等式を組合せ論的に証明することができる (cf. [1])．

3 A Wei type duality for matroids

$\mathcal{M}$ を E 上の階数 $\rho(E) = k$ であるマトロイドとし，$|E| = n$ とする．任意の i, j, $0 \leq i \leq k$, $0 \leq j \leq n-k$ に対して

$$\begin{aligned} f_i &:= \max\{|X| : X \subseteq E, \rho(X) = i\}, \\ f_j^* &:= \max\{|Y| : Y \subseteq E, \rho^*(Y) = j\} \end{aligned}$$

とする．このとき，以下の不等式が成立することが分かる．

補題 7

$$0 \leq f_0 < f_1 < f_2 < \cdots < f_k = n.$$

さらに，以下の集合を定める．

$$\begin{aligned} U_{\mathcal{M}} &:= \{n - f_{k-1}, n - f_{k-2}, \ldots, n - f_0\}, \\ V_{\mathcal{M}} &:= \{f_0^* + 1, f_1^* + 1, \ldots, f_{n-k-1}^* + 1\}. \end{aligned}$$

このとき，以下の定理が成立することが分かる．

定理 8 $U_{\mathcal{M}} \cup V_{\mathcal{M}} = \{1, 2, \ldots, n\}$ であり，$U_{\mathcal{M}} \cap V_{\mathcal{M}} = \emptyset$.

(証明の概要)

- $n - f_i = f_j^* + 1$ であるような i, j が存在すると仮定する．
- $|X| = f_i$ かつ $\rho(X) = i$ であるならば，$|E - X| = f_j^* + 1$ である．このとき，補題5から $\rho^*(E - X) \geq j + 1$ が成立する．
- ここで，$|E - X| - \rho(E) + \rho(X) = \rho^*(E - X)$ から

$$n - f_i - k + i \geq j + 1$$

  が得られる．
- 同様に，$-f_j^* + j + k \geq i + 1$ が得られる．
- 従って，上記の2式から $1 = n - f_i - f_j^* \geq 2$ となり，矛盾が生じる．

ここで，H を $[n, k]$ 符号 C のパリティ検査行列として，$\mathcal{M}$ を H から構成されるベクトルマトロイドとしたとき，

$$d_r = n - 1 - f_{k-r}$$

であることが分かる．よって，上記の定理は命題3の一般化であることが分かり，同時に命題3が組合せ論的に証明できることが分かる．

また，定理8から分かることとして，グラフ G に対して，

- b_i を i 個の極小カットセットの和集合における最小の辺の数
- c_j を j 個のサイクルの和集合における最小の辺の数

とする．このとき，

$$\begin{aligned} U_G &:= \{b_1, b_2, \ldots, b_k\}, \\ V_G &:= \{n + 1 - c_{n-k}, n + 1 - c_{n-k-1}, \ldots, n + 1 - c_1\} \end{aligned}$$

に対して，以下の等式が成立する．

系 9 $U_G \cup V_G = \{1, 2, \ldots, n\}$ であり，$U_G \cap V_G = \emptyset$.

今後の課題としては，定理8を用いてマトロイドにおける問題を再考察すること（例えば，Whitney numbers の考察等），他の符号理論における双対性（例えば，Yoshida's duality）をマトロイドに拡張することでマトロイドの表現問題（与えられたマトロイドが $\mathbb{F}_q$ 上の行列から構成できるかを検討する問題）等への新たなアプローチを行いたい．

References

[1] C. Greene, Weight enumeration and the geometry of linear codes, *Stud. Appl. Math.* **55** (1976), pp. 119–128.

[2] F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42** (1963), pp. 79–94.

[3] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, 16., North-Holland Publishing Company, Amsterdam (1978).

[4] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.

[5] M. A. Tsfasman and S. G. Vlădut, Geometric approach to higher weights, *IEEE Trans. Inform. Theory*, Vol. 41 (1995) pp. 1564–1588.

[6] V. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory*, **37** (1991), pp. 1412-1418.

[7] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

[8] T. Yoshida, The average of joint weight enumerators, *Hokkaido Math. J*, **18** (1989), pp. 217-222.

[9] T. Yoshida, MacWilliams identities for linear codes with group action, *Kumamoto Math. J*, **6** (1993), pp. 29-45.

On projective planes of order 12 with a collineation group of order 9

秋山献之　福岡大学理学部
Kenzi AKIYAMA
Faculty of Science, Fukuoka University

末竹千博　大分大学工学部
Chihiro SUETAKE
Faculty of Engineering, Oita University

この報告は，秋山と末竹との共著論文 [2] についての報告と解説である．

まず，有限射影平面についての定義から始めて，簡単な性質を述べ，この研究でのキーワードとなる対称横断デザインについて注意する．次に，位数 12 の射影平面についての研究状況を述べ，最後に，得られた結果とその証明の手法と証明の概略を紹介する．

1. 有限射影平面と対称横断デザイン

§1.1 射影平面の定義と記号

定義 1　空でない有限集合 $\mathcal{Q}$, $\mathcal{L}$ と $\mathcal{Q} \times \mathcal{L}$ の空でない部分集合 I の組 $\pi = (\mathcal{Q}, \mathcal{L}, I)$ を**結合構造** (incidence structure) という．このとき，$\mathcal{Q}$ の元 a を点，$\mathcal{L}$ の元 A を直線（あるいはブロック）といい，I の元 (a, A) を旗 (flag) という．$(a, A) \in I$ のとき，点 a は直線 A 上にある，あるいは点 a は直線 A を通る等という．

点 a に対して，$(a) = \{X \in \mathcal{L} | (a, X) \in I\}$,
直線 A に対して，$(A) = \{x \in \mathcal{Q} | (x, A) \in I\}$ と定義する．

結合構造 $\pi = (\mathcal{Q}, \mathcal{L}, I)$ が次の 3 条件をみたすとき，**有限射影平面** (finite projective plane) という．

(1) 任意の異なる 2 点 $a, b \in \mathcal{Q}$ に対して，$|(a) \cap (b)| = 1$
(2) 任意の異なる 2 直線 $A, B \in \mathcal{L}$ に対して，$|(A) \cap (B)| = 1$
(3) 異なる 4 点 a, b, c, d で，この中からどの異なる 3 点 x, y, z をとっても，$|(x) \cap (y) \cap (z)| = 0$ をみたすものが存在する．

以下，簡単のため有限射影平面を単に射影平面ということにする．また，射影平面について必要最小限の結果しか述べない．詳しくは，平峰 [6] を参照されたい．

射影平面 π に対して，任意の点 a と任意の直線 A に対して，$|(a)| = |(A)| = n+1$ をみたす正の整数 $n(\geq 2)$ が存在する．この n を射影平面 π の**位数** (order) という．このとき，$|\mathcal{Q}| = |\mathcal{L}| = n^2+n+1$ である．

§1.2　射影平面と対称 2-デザイン

定義 2　v, k, λ を正の整数で，$v > 2k$ をみたすとする．
結合構造 $\pi = (\mathcal{Q}, \mathcal{L}, I)$ が次の 3 条件をみたすとき，2-(v, k, λ) **デザイン**と（2-design）いう．
(1)　$|\mathcal{Q}| = v$
(2)　任意のブロック B に対して，$|(B)| = k$
(3)　任意の異なる 2 点 a, b に対して，$|(a) \cap (b)| = \lambda$

このとき，任意の点 a に対して，$|(a)| = \lambda(v-1)/(k-1)$,
$|L| = \lambda v(v-1)/k(k-1)$ であることが分かる．

2-(v, k, λ) デザイン π において，$|\mathcal{Q}| = |\mathcal{L}|$ が成り立つとき，π を**対称 2-(v, k, λ) デザイン**（symmetric 2-design）という．またこのとき，$n = k-\lambda$ を π の**位数**（order）という．

定理 1　n を 2 以上の正の整数，$\pi = (\mathcal{Q}, \mathcal{L}, I)$ を結合構造とする．このとき，π が位数 n の射影平面であることと，π が対称 2-$(n^2+n+1, n+1, 1)$ デザインであることとは，同値である．

例 1　q を素数べきとし，$F = GF(q)$, V を F 上の 3 次元線形空間とする．このとき，$\mathcal{Q}$ を V の 1 次元部分空間全体，$\mathcal{L}$ を V の 2 次元部分空間全体，結合関係を包含関係とする結合構造は位数 q の射影平面である．しかし，素数べきでない位数について，射影平面の存在は知られていない．

射影平面の存在に関して，次の定理が基本的である．
定理 2　(Bruck, Ryser [4]) n を 2 以上の正の整数とする．
$n \equiv 1$ または $2 \pmod 4$ で，$n = x^2 + y^2$ をみたす整数解 (x, y) が存在しないとする．このとき，位数 n の射影平面は存在しない．
定理 3　(Lam, Thiel, Swiercz [19]) 位数 10 の射影平面は存在しない．

定理 2 より，位数 6, 14, 21, 22 等の射影平面が存在しないことが分かる．これより，存在，非存在が知られていない射影平面の位数 n を小さい順にあげると，$n = 12, 15, 18, 20, 24, 26, 28, \cdots$ である．

§1.3　射影平面の自己同型

定義 3　$\pi=(\mathcal{Q},\mathcal{L},I)$ を位数 n の射影平面とする．点集合 $\mathcal{Q}$ 上の置換 φ で，これから直線集合 $\mathcal{L}$ 上に自然に定義される写像が $\mathcal{L}$ 上の置換を引き起こすとき，φ を π の**自己同型** (automorphism) という．π の自己同型全体は写像の合成で群をなす．この群を π の**全自己同型群**（full automorphism group）といい，$\mathrm{Aut}(\pi)$ で表す．また，その部分群を π の**自己同型群**（automorphism group）という．

π の自己同型群 G に対して，G の固定点集合，固定直線集合を次の記号で表す．

$F_{\mathcal{Q}}(G)=\{a\in\mathcal{Q}|$ すべての $\varphi\in G$ に対して，$a^{\varphi}=a\}$,
$F_{\mathcal{L}}(G)=\{A\in\mathcal{L}|$ すべての $\varphi\in G$ に対して，$A^{\varphi}=A\}$

射影平面 $\pi=(\mathcal{Q},\mathcal{L},I)$ の自己同型で次のものが重要である．
π の自己同型 φ に対して，

$$(a,A)\in I,\ F_{\mathcal{Q}}(\varphi)\subseteq(A),\ F_{\mathcal{L}}(\varphi)\subseteq(a)$$

をみたす点 $a\in F_{\mathcal{Q}}(\varphi)$ と直線 $A\in F_{\mathcal{L}}(\varphi)$ が存在するとき，φ を π の**一般相応**（generalized elation）という．特に，上の 2 つの包含関係でいずれも等号が成り立つとき，φ を**相応**（elation）という．

同様に，π の自己同型 φ に対して，

$$(a,A)\notin I,\ F_{\mathcal{Q}}(\varphi)\subseteq(A)\cup\{a\},\ F_{\mathcal{L}}(\varphi)\subseteq(a)\cup\{A\}$$

をみたす点 $a\in F_{\mathcal{Q}}(\varphi)$ と直線 $A\in F_{\mathcal{L}}(\varphi)$ が存在するとき，φ を π の**一般ホモロジー**（generalized homology）という．特に，上の 2 つの包含関係でいずれも等号が成り立つとき，φ を**ホモロジー**（homology）という．

π の自己同型群 G(あるいは自己同型 φ（このとき，$G=\langle\varphi\rangle$ とおく））に対して，π の部分構造 $(F_{\mathcal{Q}}(G),F_{\mathcal{L}}(G),I')(I'=(F_{\mathcal{Q}}(G)\times F_{\mathcal{L}}(G))\cap I)$ が射影平面であるとき，G(あるいは φ）を**平面的**（planar）という．

定理 4　$\pi=(\mathcal{Q},\mathcal{L},I)$ を位数 n の射影平面とし，$\varphi(\neq 1)$ を π の自己同型で，$F_{\mathcal{Q}}(\varphi)$ は空集合でない（あるいは $F_{\mathcal{L}}(\varphi)$ は空集合でない）とする．このとき，φ は一般相応，一般ホモロジー，平面的のいずれかである．

§1.4　射影平面，アフィン平面と対称横断デザイン

位数 n の射影平面に関連するデザインについて述べる．

定義 4　n を 2 以上の正の整数とする．2-$(n^2,n,1)$ デザインを，**位数 n のアフィン平面**（affine plane of order n）という．

定理5 nを2以上の正の整数とする．このとき，位数nの射影平面が存在することと，位数nのアフィン平面が存在することとは，同値である．

定義5 k,u,λを正の整数とする．結合構造$\mathcal{D}=(\mathcal{P},\mathcal{B},J)$が次の3つの条件をみたすとき，$\mathcal{D}$をパラメータ$k,u,\lambda$をもつ**対称横断デザイン**（symmetric transversal design）といい，$STD_\lambda[k;u]$で表す．

(1) 任意の点pと任意のブロックBに対して，$|(p)|=|(B)|=k$

(2) $\mathcal{P}$の分割$\mathcal{P}=\mathcal{P}_0\cup\mathcal{P}_1\cup\cdots\cup\mathcal{P}_{k-1}$が存在して，次が成り立つ．
$|\mathcal{P}_i|=u(0\leq i\leq k-1)$,
$\mathcal{P}$の異なる2点$p\in\mathcal{P}_i$, $q\in\mathcal{P}_j$に対して，

$$|(p)\cap(q)|=\begin{cases}0\ (i=j)\\ \lambda\ (i\neq j)\end{cases}$$

(3) $\mathcal{B}$の分割$\mathcal{B}=\mathcal{B}_0\cup\mathcal{B}_1\cup\cdots\cup\mathcal{B}_{k-1}$が存在して，次が成り立つ．
$|\mathcal{B}_j|=u(0\leq j\leq k-1)$,
$\mathcal{B}$の異なる2つのブロック$B\in\mathcal{B}_i$, $C\in\mathcal{B}_j$に対して，

$$|(B)\cap(C)|=\begin{cases}0\ (i=j)\\ \lambda\ (i\neq j)\end{cases}$$

ここで，$\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}$を$\mathcal{D}$の**点クラス**（point classes），
$\mathcal{B}_0,\mathcal{B}_1,\cdots,\mathcal{B}_{k-1}$を$\mathcal{D}$の**ブロッククラス**（block classes）という．

このとき，$k=\lambda u,|\mathcal{P}|=|\mathcal{B}|=ku$. また，任意の点$p$と任意のブロッククラス$\mathcal{B}_j(0\leq j\leq k-1)$に対して，$|(p)\cap\mathcal{B}_j|=1$，任意のブロック$B$と任意の点クラス$\mathcal{P}_i(0\leq i\leq k-1)$に対して，$|(B)\cap\mathcal{P}_i|=1$

定理6 nを2以上の正の整数とする．このとき，位数nの射影平面が存在することと，対称横断デザイン$STD_1[n;n]$が存在することとは，同値である．

対称横断デザインについて次が成り立つ．
定理7 (Akiyama, Suetake [1]) $\mathcal{D}=(\mathcal{P},\mathcal{B},J)$を$STD_\lambda[k;u]$とする．
$\Omega=\{\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}\}$を点クラスの集合，
$\Delta=\{\mathcal{B}_0,\mathcal{B}_1,\cdots,\mathcal{B}_{k-1}\}$をブロッククラスの集合とする．
φを$\mathcal{D}$の自己同型，Gを$\mathcal{D}$の自己同型群とする．このとき，φおよびG

はそれぞれ，Ω 上，Δ 上に作用し，次が成り立つ．
(1) $\theta_{\mathcal{P}}(\varphi)+\theta_{\Delta}(\varphi)=\theta_{\mathcal{B}}(\varphi)+\theta_{\Omega}(\varphi)$,
ただし，$\theta_{\mathcal{P}}(\varphi)=|\{x\in\mathcal{P}\mid x^{\varphi}=x\}|$ で，$\theta_{\Delta}(\varphi)$,
$\theta_{\mathcal{B}}(\varphi)$, $\theta_{\Omega}(\varphi)$ も同様である．
(2) $t_{\mathcal{P}}(G)+t_{\Delta}(G)=t_{\mathcal{B}}(G)+t_{\Omega}(G)$,
ただし，$t_{\mathcal{P}}(G)$ は G を $\mathcal{P}$ 上に作用させたときの $G-$ 軌道の個数で，$t_{\Delta}(G)$, $t_{\mathcal{B}}(G)$, $t_{\Omega}(G)$ も同様である．

2. 位数 12 の射影平面

§2.1 位数 12 の射影平面の研究

現在のところ，存在，非存在が知られていない射影平面の最小位数は 12 である．自己同型群の存在の仮定なしではほとんど手掛りがないので，自明でない自己同型群を仮定してその存在を調べることが広く行われている．

最初の組織的な位数 12 の射影平面の研究は，Janko と T.van Trung による 1980 年から 1984 年にかけての研究である．その一連の研究によって次の結果が得られた．

定理 8 (Janko, T.van Trung [11] - [18])

(1) 位数 12 の射影平面の全自己同型群は，$\{2,3\}$-群である．
(2) 位数 12 の射影平面は，位数 27 の群，位数 6 の非可換群，位数 4 の基本可換群を自己同型群としてもたない．
(3) 位数 12 の射影平面は位数 3 の相応をもたない．

その後，Horvic-Baldasar と Kramer と Matulic-Bedenic によって 1986 年から 1987 年にかけて研究が続けられ，次の結果が得られた．

定理 9 (Horvic-Baldasar, Kramer, Matulic-Bedenic [8], [9])
位数 12 の射影平面の全自己同型群の位数は，$2^a(0\leq a\leq 4)$ または $3^b(0\leq b\leq 2)$ である．

末竹と秋山による 2004 年から始まった研究によって，さらに次の結果が得られた．

定理 10 (Akiyama, Suetake [20], [1])
位数 12 の射影平面は，位数 16，位数 8 の自己同型群をもたない．

今回得られた結果は次のものである．

定理（Akiyama, Suetake [2])
位数 12 の射影平面の位数 9 の自己同型群は，基本可換群で，平面的でない．

§2.2 証明の手法

$\pi = (\mathcal{Q}, \mathcal{L})$ を位数 12 の射影平面とする. G を π のある条件 $(*)$ を満たす位数 9 の自己同型群で, π のある旗 (r_∞, L_∞) を固定するとする. 以下このような G が存在しないことを示したい. このとき, π から L_∞ 上のすべての点と r_∞ を通るすべての直線を除いて得られる π の部分構造を $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ とすると, $\mathcal{D}$ は $STD_1[12; 12]$ になる. G は旗 (r_∞, L_∞) を固定するので, G は $\mathcal{D}$ の自己同型群を導入する. ここで, G は $\mathcal{D}$ 上なるべく多くの長さ $|G|$ の点軌道とブロック軌道を持つことが望ましいことを注意しておく. この仮定のもとで以下の議論をする.

(1) G の $\mathcal{P}$ 上および $\mathcal{B}$ 上の作用 $(\dagger)$ を決定する.

(2) $\mathcal{P}$ 上の長さ $|G|$ の G-軌道の集合を求め, その完全代表系 $\{q_i\}(0 \leq i \leq s)$ を一つ定める. 同様に, $\mathcal{B}$ 上の G の作用についても同様に議論し, その完全代表系 $\{C_j\}(0 \leq j \leq t)$ を一つ定める.

(3) $D_{ij} = \{\alpha \in G \mid q_i^\alpha \in (C_j)\}(0 \leq i \leq s,\ 0 \leq j \leq t)$ と定義し, $m_{ij} = |D_{ij}|$ とおく.
$0 \leq i,\ i' \leq s$ に対して, $\sum_{0 \leq j \leq t} D_{ij} D_{i'j}^{(-1)}$ を決定する.

(4) $M = (m_{ij})_{0 \leq i \leq s, 0 \leq j \leq t}$ を決定する.

(5) $D = (D_{ij})_{0 \leq i \leq s, 0 \leq j \leq t}$ を決定する.

(6) 長さが $|G|$ でない G-軌道の作用も調べ, 対称横断デザイン $STD_1[12; 12]$ を決定する. (長さが $|G|$ である G-軌道がなるべく多い方が良いという理由は, この復元をし易くするためである.)

(7) 対称横断デザイン $STD_1[12; 12]$ を位数 12 の射影平面 π に拡大する.

このような方法を何故わざわざ使うのか. 何故位数 12 の射影平面をそのまま扱わずに, わざわざ遠回りしてその部分構造である対称横断デザイン $STD_1[12; 12]$ を扱うのか. 一歩譲ったとして, 何故部分構造である位数 12 のアファイン平面を利用しないのか. 理由は対称横断デザインが射影平面の良さとアファイン平面の良さの両方を兼ね備えているからである. 前者は点とブロックの対称性であり, 後者は点と直線の平行類を持つという点である. このことは, 対称横断デザインの自己同型群の点上とブロック上の作用が調べ易いということを意味している. 実際, 定理 7 はこのことを示す 1 つの例である. なお我々の証明では上記の手続き (5) までを調べることにより (つまり $\mathcal{D}$ の非存在を主張する), 条件 $(*)$ を満た G が存在しないことを示している. 従って (6),(7) は, 実は不要である.

§2.3　定理の証明の概略

定理を示すには，　次の命題を示せばよい．

命題　$\pi = (\mathcal{Q}, \mathcal{L}, I)$ を位数 12 の射影平面, $G = \mathrm{Aut}(\pi)$ とし, G は次の条件 $(*)$ をみたすとする．

$(*)$　$|G| = 9$,　$G \cong Z_3 \times Z_3$, G は平面的ではない

このとき, π は存在しない

この射影平面の命題は，　次のようにして対称横断デザインの問題に変換できる．条件 $(*)$ から,

点 $r_\infty \in F_{\mathcal{Q}}(G)$ とブロック $L_\infty \in F_{\mathcal{L}}(G)$ で, $r_\infty \in (L_\infty)$ みたすものが存在する．ここで,

$(L_\infty) = \{r_0, r_1, \cdots, r_{11}, r_\infty\}$, $(r_\infty) = \{L_0, L_1, \cdots, L_{11}, L_\infty\}$,

$\mathcal{P} = \mathcal{Q} - (L_\infty)$,　$\mathcal{B} = \mathcal{L} - (r_\infty)$,　$J = (\mathcal{P} \times \mathcal{B}) \cap I$,

$\mathcal{P}_i = (L_i) - \{r_\infty\}$ $(0 \le i \le 11)$, $\mathcal{B}_j = (r_j) - \{L_\infty\}$ $(0 \le j \le 11)$

$\mathcal{D} = (\mathcal{P}, \mathcal{B}, J)$ とおく．このとき, $\mathcal{D}$ は対称横断デザイン $STD_1[12; 12]$ で, G は $\mathcal{D}$ の位数 9 の自己同型群となる．さらに, 条件 $(*)$ から, G は次の条件 $(\dagger)$ のいずれか一つをみたす．

条件 $(\dagger)$：

(i)　$G = \langle \varphi \mid \varphi^9 = 1 \rangle$ は巡回群, $F_{\mathcal{Q}}(G) = \{r_\infty\}$,　$F_{\mathcal{L}}(G) = \{L_\infty\}$,
$\varphi^{(L_\infty)} = (r_0, r_1, \cdots, r_8)(r_9, r_{10}, r_{11})(r_\infty)$,
$\varphi^{(r_\infty)} = (L_0, L_1, \cdots, L_8)(L_9, L_{10}, L_{11})(L_\infty)$,
(i.a)　φ^3 は一般相応　または
(i.b)　φ^3 は平面的

(ii)　$G = \langle \varphi \mid \varphi^9 = 1 \rangle$ は巡回群,
$F_{\mathcal{Q}}(G) = \{r_9, r_{10}, r_{11}, r_\infty\}$, $F_{\mathcal{L}}(G) = \{L_9, L_{10}, L_{11}, L_\infty\}$,
$\varphi^{(L_\infty)} = (r_0, r_1, \cdots, r_8)(r_9)(r_{10})(r_{11})(r_\infty)$,
$\varphi^{(r_\infty)} = (L_0, L_1, \cdots, L_8)(L_9)(L_{10})(L_{11})(L_\infty)$,
φ^3 は平面的

(iii)　G は平面的,
(iii.a)　$G = \langle \varphi \mid \varphi^9 = 1 \rangle$ または
(iii.b)　$G = \langle \varphi, \tau \mid \varphi^3 = \tau^3 = 1, \varphi\tau = \tau\varphi \rangle$

(i.a) の場合の証明

$\mathcal{D} = (\mathcal{P}, \mathcal{B}, J)$ の点と点クラスおよびブロックとブロッククラスを次のように定める．

$\mathcal{P} = \{p_0, p_1, \cdots, p_{143}\}$,
$\mathcal{P}_0 = \{p_0, p_1, \cdots, p_{11}\}$, $\mathcal{P}_1 = \{p_{12}, p_{13}, \cdots, p_{23}\}$,

$\cdots, \mathcal{P}_{11} = \{p_{132}, p_{133}, \cdots, p_{143}\}$,

$\mathcal{B} = \{B_0, B_1, \cdots, B_{143}\}$,

$\mathcal{B}_0 = \{B_0, B_1, \cdots, B_{11}\}$, $\mathcal{B}_1 = \{B_{12}, B_{13}, \cdots, B_{23}\}$,

$\cdots, \mathcal{B}_{11} = \{B_{132}, B_{133}, \cdots, B_{143}\}$

また, $\Omega = \{\mathcal{P}_0, \mathcal{P}_1, \cdots, \mathcal{P}_{11}\}$, $\Delta = \{\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_{11}\}$ とおく.

(1) φ の $\mathcal{P}$ 上および $\mathcal{B}$ 上の作用

$\varphi^{\mathcal{P}}$(あるいは $\varphi^{\mathcal{B}}$)$= (x_0, x_{12}, x_{24}, x_{36}, x_{48}, x_{60}, x_{72}, x_{84}, x_{96})$
$(x_1, x_{13}, x_{25}, x_{37}, x_{49}, x_{61}, x_{73}, x_{85}, x_{97})$
$(x_2, x_{14}, x_{26}, x_{38}, x_{50}, x_{62}, x_{74}, x_{86}, x_{98})$
$(x_3, x_{15}, x_{27}, x_{39}, x_{51}, x_{63}, x_{75}, x_{87}, x_{99})$
$(x_4, x_{16}, x_{28}, x_{40}, x_{52}, x_{64}, x_{76}, x_{88}, x_{100})$
$(x_5, x_{17}, x_{29}, x_{41}, x_{53}, x_{65}, x_{77}, x_{89}, x_{101})$
$(x_6, x_{18}, x_{30}, x_{42}, x_{54}, x_{66}, x_{78}, x_{90}, x_{102})$
$(x_7, x_{19}, x_{31}, x_{43}, x_{55}, x_{67}, x_{79}, x_{91}, x_{103})$
$(x_8, x_{20}, x_{32}, x_{44}, x_{56}, x_{68}, x_{80}, x_{92}, x_{104})$
$(x_9, x_{21}, x_{33}, x_{45}, x_{57}, x_{69}, x_{81}, x_{93}, x_{105})$
$(x_{10}, x_{22}, x_{34}, x_{46}, x_{58}, x_{70}, x_{82}, x_{94}, x_{106})$
$(x_{11}, x_{23}, x_{35}, x_{47}, x_{59}, x_{71}, x_{83}, x_{95}, x_{107})$
$(x_{108}, x_{120}, x_{132}, x_{109}, x_{121}, x_{133}, x_{110}, x_{122}, x_{134})$
$(x_{111}, x_{123}, x_{135}, x_{112}, x_{124}, x_{136}, x_{113}, x_{125}, x_{137})$
$(x_{114}, x_{126}, x_{138}, x_{115}, x_{127}, x_{139}, x_{116}, x_{128}, x_{140})$
$(x_{117}, x_{129}, x_{141}, x_{118}, x_{130}, x_{142}, x_{119}, x_{131}, x_{143})$,

ただし, x は p または B を表す.

(2) $\mathcal{P}$ 上あるいは $\mathcal{B}$ 上の長さ 9 の G-軌道とその代表元

$\mathcal{P}$ 上 (あるいは $\mathcal{B}$ 上) の長さ 9 の G-軌道を $\mathcal{Y}_i = z_i{}^G (0 \leq i \leq 15)$ とする. ただし, $z_i = x_i (0 \leq i \leq 11)$, $z_{12} = x_{108}$, $z_{13} = x_{111}$, $z_{14} = x_{114}$, $z_{15} = x_{117}$. また, $(\mathcal{Y}, x, z) = (\mathcal{Q}, p, q)$ または $(\mathcal{C}, B, C)$ である.

(3) $D_{ij} (0 \leq i, j \leq 15)$ の関係式

$0 \leq i, i' \leq 11$ に対して,

$$\sum_{0 \leq j \leq 15} D_{ij} D_{i'j}^{(-1)} = \begin{cases} G - \{1\} (i \neq i' \text{のとき}) \\ 12 \quad (i = i' \text{のとき}) \end{cases}$$

(4) $M = (m_{ij})_{0 \leq i,j \leq 15}$ の決定

$m_{ij} (0 \leq i, j \leq 11)$ は次の条件をみたす.

$$\sum_{0 \leq j \leq 15} m_{ij} = 12 \ (0 \leq i \leq 15),$$

$$\sum_{0\le j\le 15} m_{ij}m_{i'j} = 8 \quad (0 \le i, i'(\neq) \le 11)$$

$$\sum_{0\le j\le 15} m_{ij}^2 = 12 \quad (0 \le i \le 11)$$

ここで，列の適当な置換によって，

$$(m_{ij})_{0\le i\le 3, 0\le j\le 15} = \begin{pmatrix} 0000 & 1111 & 1111 & 1111 \\ 1111 & 0000 & 1111 & 1111 \\ 1111 & 1111 & 0000 & 1111 \\ 1111 & 1111 & 1111 & 0000 \end{pmatrix}$$

と出来る．しかし，5番目の行を条件をみたすように定めることが出来ないので，$M = (m_{ij})$ は非存在で，この場合は位数 12 の射影平面は存在しない．

(i.a) 以外の場合の証明

命題の (i.a) 以外の場合は，議論はより複雑で，$M = (m_{ij})$ を決定するための工夫とより多くの計算機の利用が必要である．

(i.b), (iii.a), (iii.b) の場合についても，それぞれ (i.a) の場合と同様に M の非存在がいえる．

しかし (ii) の場合は，非同値な 4 個の M が存在するが，最終的には $D = (D_{ij})$ の非存在が示され，命題が証明される．

参考文献

[1] K.Akiyama and C.Suetake, The nonexistence of projective planes of order 12 with a collineation group of order 8, *J.Combin.Des.* **16**(2008),411-430.

[2] K.Akiyama and C.Suetake, On projective planes of order 12 with a collineation group of order 9, to appear.

[3] T.Beth, D.Jungnickel and H.Lenz, Design Theory, Cambridge U.P. 2nd ed.(1999).

[4] R.H.Bruck and H.J.Ryser, The nonexistence of certain finite projective planes, *Canad.J.Math.***1**(1949),88-93.

[5] C.J. Colbourn and J.H. Dinitz, Handbook of combinatorial dsigns, Chapman & Hall /CRC, 2nd ed.(2007)

[6] Y.Hiramine, A survey on finite projective planes, *RIMS Kokyuroku* **1214**(2001), 46-61.

[7] Y.Hiramine and C.Suetake, A contraction of divisible designs, *Disc.Math.***308**(2008), 3257-3264.

[8] K.Horvtic-Baldasar, E.Kramer and I.Matulic-Bedenic, Projective planes of order 12 do not have an abelian group of order 6 as a collineation group, *Punime Mat.* **1**(1986),75-81.

[9] K.Horvtic-Baldasar, E.Kramer and I.Matulic-Bedenic, On the full collineation group of projective planes of order 12, *Punine Mat.* **2**(1987),9-11.

[10] Y.J.Ionin and M.S.Shrikhande, Combinatorics of Symmetric Designs, Cambridge U.P.(2006).

[11] Z.Janko and T.van Trung, On Projective planes of order 12 which have a subplanes of order three I, *J.Combin.Theory(A)* **29**(1980), 254-256.

[12] Z.Janko and T.van Trung, Projective planes of order 12 do not have a non-abelian group of order 6 as a collineation group, *J.Reine Angew. Math.***326**(1981),152-157.

[13] Z.Janko and T.van Trung, Projective planes of order 12 do not possess an elation of order 3, *Stud.Sci.Math.***16**(1981),115-118.

[14] Z.Janko and T.van Trung, On projective planes of order 12 with an automorphism of order 13. Part I.Kirkman designs of order 27, *Geom.Dedicata* **11**(1981),257-284.

[15] Z.Janko and T.van Trung, On projective planes of order 12 with an automorphism of order 13. Part II.Orbit matrices and conclusion, *Geom.Dedicata* **12**(1982),87-99.

[16] Z.Janko and T.van Trung, The full collineation group of any projective pkanes of order 12 is a 2,3 group, *Geom. Dedicata* **12**(1982), 101-110.

[17] Z.Janko and T.van Trung, A generalization of a result of L.Baumert and M.Hall about projective planes of order 12, *J.Combin.Theory(A)* **32**(1982),378-385.

[18] Z.Janko and T.van Trung, Projective planes of order 12 do not have a four group as a collineation group, *J.Combin.Theory(A)* **32**(1982),401-404.

[19] C.W.Lam, L.Thiel and S.Swiercz, The nonexistence of finite projective planes of order 10, *Canad.J.Math.***41**(1989),1117-1123.

[20] C.Suetake, The nonexistence of projective planes of order 12 with a collineation group of order 16, *J. Combin. Theory(A)* **107**(2004), 21-48.

The nonexistence of $\mathrm{STD}_2[12;6]$'s with an automorphism group of order 9

Chihiro Suetake
(Oita University)

25th Algebraic Combinatorics

Hokkaido University(June 25, 2008)

§1 Motivation

We assume that all sets are finite sets.

1.1 Definition
Let $\pi = (\mathcal{P}, \mathcal{B}, I)$ be an incidence structure.
$\mathcal{D}$ is a **symmetric transversal design**(STD) $\mathrm{STD}_\lambda[k;u]$.
$\overset{\text{def.}}{\Longleftrightarrow}$
(i) For $B \in \mathcal{B}$, $|(B)| = |\{x \in \mathcal{P} |\ xIB\}| = k$.
(ii) There exists a partition $\mathcal{P} = \mathcal{P}_0 \cup \mathcal{P}_1 \cup \cdots \cup \mathcal{P}_{k-1}$ ($|\mathcal{P}_i| = u$ for $0 \leq i \leq k-1$) such that for $p, q(\neq) \in \mathcal{P}$

$$|(p) \cap (q)| = \begin{cases} 0 & \text{if } p, q \in \mathcal{P}_i \text{ for some } i, \\ \lambda & \text{otherwise.} \end{cases}$$

($\mathcal{P}_0, \cdots, \mathcal{P}_{k-1}$ are said to be the **point classes** of $\mathcal{D}$.)
(iii) The dual structure $\mathcal{D}^d$ of $\mathcal{D}$ satisfies (i) and (ii).
The point classes of $\mathcal{D}^d$ are said to be the **block classes** of $\mathcal{D}$.
This definition yields $k = \lambda u$.

1.2 Example
Let $\mathcal{P} = \{p_0, p_1, \cdots, p_{17}\}$ and $\mathcal{B} = \{B_0, B_1, \cdots, B_{17}\}$. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be an incidence structure defined by the following incidence matrix M. Then $\mathcal{D}$ is an $\mathrm{STD}_2[6;3]$.

$$M = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc}
1&0&0&1&0&0&1&0&0&1&0&0&1&0&0&1&0&0\\
0&1&0&0&1&0&0&1&0&0&1&0&0&1&0&0&1&0\\
0&0&1&0&0&1&0&0&1&0&0&1&0&0&1&0&0&1\\
\hline
1&0&0&1&0&0&0&1&0&0&1&0&0&0&1&0&0&1\\
0&1&0&0&1&0&0&0&1&0&0&1&1&0&0&1&0&0\\
0&0&1&0&0&1&1&0&0&1&0&0&0&1&0&0&1&0\\
\hline
1&0&0&0&1&0&1&0&0&0&0&1&0&1&0&0&0&1\\
0&1&0&0&0&1&0&1&0&1&0&0&0&0&1&1&0&0\\
0&0&1&1&0&0&0&0&1&0&1&0&1&0&0&0&1&0\\
\hline
1&0&0&0&1&0&0&0&1&1&0&0&0&0&1&0&1&0\\
0&1&0&0&0&1&1&0&0&0&1&0&1&0&0&0&0&1\\
0&0&1&1&0&0&0&1&0&0&0&1&0&1&0&1&0&0\\
\hline
1&0&0&0&0&1&0&1&0&0&0&1&1&0&0&0&1&0\\
0&1&0&1&0&0&0&0&1&1&0&0&0&1&0&0&0&1\\
0&0&1&0&1&0&1&0&0&0&1&0&0&0&1&1&0&0\\
\hline
1&0&0&0&0&1&0&0&1&0&1&0&0&1&0&1&0&0\\
0&1&0&1&0&0&1&0&0&0&0&1&0&0&1&0&1&0\\
0&0&1&0&1&0&0&1&0&1&0&0&1&0&0&0&0&1
\end{array}\right).$$

For example $(B_3) = \{p_0, p_3, p_8, p_{11}, p_{13}, p_{16}\}$ and $(p_5) = \{B_2, B_5, B_6, B_9, B_{13}, B_{16}\}$.
The point classes are $\mathcal{P}_0 = \{p_0, p_1, p_2\}, \cdots, \mathcal{P}_5 = \{p_{15}, p_{16}, p_{17}\}$.
The block classes are $\mathcal{B}_0 = \{B_0, B_1, B_2\}, \cdots, \mathcal{B}_5 = \{B_{15}, B_{16}, B_{17}\}$.

1.3 Example
Let $\Pi = (\mathcal{Q}, \mathcal{L})$ be a projective plane of order n and $p \in \mathcal{Q}$, $L \in \mathcal{L}$, $p \in (L)$. Set $\mathcal{P} = \mathcal{Q} - (L)$ and $\mathcal{B} = \mathcal{L} - (p)$. Then the substructure $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ of Π is an $\mathrm{STD}_1[n; n]$ with the point classes $(X) - \{p\}$ $(X \in (p))$ and the block classes $(x) - \{L\}$ $(x \in (L))$.
(The converse is also true.)

Therefore,
$\exists$a projective plane of order $n \Longleftrightarrow \exists$ an $\mathrm{STD}_1[n; n]$.

1.4 Example (a generalization of 1.3)
Let G be an elation group with a fixed center p and a fixed axis L of a projective plane $\Pi = (\mathcal{Q}, \mathcal{L})$ of order n.
Set $|G| = \lambda$. Then $\lambda | n$. Let $\mathcal{P}$ =(the set of G-orbits on $\mathcal{Q} - (L)$) and $\mathcal{B}$ =(the set of G-orbits on $\mathcal{L} - (p)$). For $\alpha \in \mathcal{P}$, $\Gamma \in \mathcal{B}$,

$$\alpha I_1 \Gamma \overset{\text{def.}}{\Longleftrightarrow} aIC \quad \text{for some a} \in \alpha,\ \mathrm{C} \in \Gamma.$$

Then, $(\mathcal{P}, \mathcal{B}, I_1)$ is an $\mathrm{STD}_\lambda[n; n/\lambda]$.

1.5 Remark
Let n be a non square positive integer. Let φ be an automorphism of order 2 of a projective plane Π of order n. Then, φ is an elation of Π.

1.6 Example
If there exists a projective plane of order 12 with an automorphism of order 2, then there exists an $\mathrm{STD}_2[12;6]$.

1.7 Remark
The point class size u of any known $\mathrm{STD}_\lambda[k;u]$ is a prime power. It is unknown whether there exists an $\mathrm{STD}_\lambda[k;u]$ or not which u is not a prime power. The smallest such STD is an $\mathrm{STD}_2[12;6]$.

In this note, we prove (i) of the following theorem.

1.8 Theorem
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an $\mathrm{STD}_2[12;6]$. *Let G be an automorphism group of $\mathcal{D}$. Then, the following statements hold.*
(i) $|G| = 2^\alpha 3^\beta$, *where α is a non negative integer and $\beta \in \{0,1\}$.*
(ii) *If $|G| = 4$, then G is not semiregular on $\mathcal{P} \cup \mathcal{B}$.*
((ii) *was proved by Akiyama and S in* [*AS*].)

§2 Preliminaries

In this section we note several theorems which will be used to prove 1.8 Theorem (i).

2.1 Notation
Assume that a finite group G acts on a finite set Λ. Let $\varphi \in G$.
Then, set $F_\Lambda(\varphi) = \{x \in \Lambda | x^\varphi = x\}$, $\theta_\Lambda(\varphi) = |F_\Lambda(\varphi)|$ and let $t_\Lambda(G) = t_\Lambda$ be the number of orbits of (G, Λ).

2.2 Theorem(Akiyama, S, 2008[AS])
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an STD, *Ω the set of point classes of $\mathcal{D}$, Δ the set of block classes of $\mathcal{D}$ and $\varphi \in$* Aut *$\mathcal{D}$. Then,*

$$\theta_\mathcal{P}(\varphi) + \theta_\Delta(\varphi) = \theta_\mathcal{B}(\varphi) + \theta_\Omega(\varphi).$$

2.3 Theorem(Akiyama, S, 2008[AS])

Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an STD. *Let Ω be the set of point classes of $\mathcal{D}$, Δ the set of block classes of $\mathcal{D}$ and G an automorphism group of $\mathcal{D}$. Then,*

$$t_{\mathcal{P}} + t_{\Delta} = t_{\mathcal{B}} + t_{\Omega}.$$

2.4 Theorem(S, 2008[S])
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an STD. *Let Ω be the set of point classes of $\mathcal{D}$, Δ the set of block classes of $\mathcal{D}$ and $\varphi \in \mathrm{Aut}\ \mathcal{D}$.*
(i) *If $\theta_{\Omega}(\varphi) \neq 0$, $\theta_{\Delta}(\varphi) \neq 0$ and $\theta_{\mathcal{Q}_0}(\varphi) = 1$ for some $\mathcal{Q}_0 \in F_{\Omega}(\varphi)$ or $\theta_{\mathcal{C}_0}(\varphi) = 1$ for some $\mathcal{C}_0 \in F_{\Delta}(\varphi)$, then $\theta_{\mathcal{P}}(\varphi) = \theta_{\Omega}(\varphi)$, $\theta_{\mathcal{B}}(\varphi) = \theta_{\Delta}(\varphi)$, $\theta_{\mathcal{Q}}(\varphi) = 1$ for $\mathcal{Q} \in F_{\Omega}(\varphi)$ and $\theta_{\mathcal{C}}(\varphi) = 1$ for $\mathcal{C} \in F_{\Delta}(\varphi)$.*
(ii) *If $\theta_{\Omega}(\varphi) \neq 0$, $\theta_{\Delta}(\varphi) \neq 0$ and $\theta_{\mathcal{Q}_0}(\varphi) \geq 2$ for some $\mathcal{Q}_0 \in F_{\Omega}(\varphi)$ or $\theta_{\mathcal{C}_0}(\varphi) \geq 2$ for some $\mathcal{C}_0 \in F_{\Delta}(\varphi)$, then $\theta_{\mathcal{P}}(\varphi) = \theta_{\mathcal{B}}(\varphi)$, $\theta_{\Omega}(\varphi) = \theta_{\Delta}(\varphi)$ and $\theta_{\mathcal{Q}}(\varphi) = \theta_{\mathcal{C}}(\varphi)$ for $\mathcal{Q} \in F_{\Omega}(\varphi)$ and for $\mathcal{C} \in F_{\Delta}(\varphi)$, where the value $\theta_{\mathcal{Q}}(\varphi) = \theta_{\mathcal{C}}(\varphi)$ is constant.*
(iii) *If $\theta_{\Omega}(\varphi) = 0$, then $\theta_{\mathcal{P}}(\varphi) = 0$ and $\theta_{\mathcal{B}}(\varphi) = \theta_{\Delta}(\varphi)$.*
(iv) *If $\theta_{\Delta}(\varphi) = 0$, then $\theta_{\mathcal{B}}(\varphi) = 0$ and $\theta_{\mathcal{P}}(\varphi) = \theta_{\Omega}(\varphi)$.*

We define a sub STD of an STD.

2.5 Definition
Let $\mathcal{D}$ be an $\mathrm{STD}_{\lambda}[\lambda u; u]$ and $\mathcal{E}$ a substructure of $\mathcal{D}$, then
$\mathcal{E}$ **is a sub STD** of $\mathcal{D}$
$\overset{\text{def.}}{\Longleftrightarrow}$
(i) $\mathcal{E}$ is an $\mathrm{STD}_{\lambda}[\lambda v; v]$ for some $v(\leq u)$.
(ii) Any point class of $\mathcal{E}$ is contained in a point class of $\mathcal{D}$ and any block class of $\mathcal{E}$ is contained in a block class of $\mathcal{D}$.

2.6 Theorem
Let $\mathcal{D}$ be an $\mathrm{STD}_{\lambda}[\lambda u; u]$ and $\mathcal{E}$ a sub STD of $\mathcal{D}$. If $\mathcal{E}$ is an $\mathrm{STD}_{\lambda}[\lambda v; v]$ with $v < u$, then

$$u \geq \lambda v^2.$$

2.7 Remark
2.6 Theorem is a partial generalization of the Bruck theorem in finite projective planes.

2.8 Theorem
Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be an $\mathrm{STD}_{\lambda}[\lambda u; u]$ *and $\varphi(\neq 1) \in \mathrm{Aut}\mathcal{D}$. If any prime divisor of $o(\varphi)$ is greater than λ, $\theta_{\Omega}(\varphi) \geq 2$, $\theta_{\Delta}(\varphi) \geq 2$ and $\theta_{\mathcal{Q}_0}(\varphi) \geq 2$ for some*

$\mathcal{Q}_0 \in F_\Omega(\varphi)$ *or* $\theta_{\mathcal{C}_0}(\varphi) \geq 2$ *for some* $\mathcal{C}_0 \in F_\Delta(\varphi)$, *then* $\mathcal{D}_1 = (F_\mathcal{P}(\varphi), F_\mathcal{B}(\varphi))$ *is a sub* STD *of* $\mathcal{D}$. *Actually,* $\mathcal{D}_1$ *is an* $\mathrm{STD}_\lambda[\lambda v; v]$, *where* $|\mathcal{Q}_0 \cap F_\mathcal{P}(\varphi)| = v$.

§3 $\mathrm{STD}_2[12; 6]$

Throughout this section let $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ be an $\mathrm{STD}_2[12; 6]$, Ω the set of point classes of $\mathcal{D}$ and Δ the set of block classes of $\mathcal{D}$.

3.1 Lemma
Let $\varphi \in \mathrm{Aut}\mathcal{D}$ *such that* $o(\varphi) = 3$. *Then, the following statements hold.*
(i) $\langle\varphi\rangle$ *acts semiregularly on* $\mathcal{P} \cup \mathcal{B}$.
(ii) $\theta_\Omega(\varphi) = \theta_\Delta(\varphi) \in \{0, 3, 6, 9\}$ *and* $\theta_\mathcal{P}(\varphi) = \theta_\mathcal{B}(\varphi) = 0$.

Proof 2.8 Theorem, 2.6 Theorem, 2.2 Theorem and [HS].

3.2 Assumption
Assume that $\mathcal{D}$ has an automorphism group of order 9.

Let $\Omega = \{\mathcal{P}_0, \cdots, \mathcal{P}_{11}\}$, $\Delta = \{\mathcal{B}_0, \cdots, \mathcal{B}_{11}\}$ and $\mathcal{P}_0 = \{p_0, p_1, \cdots, p_5\}, \cdots, \mathcal{P}_{11} = \{p_{66}, p_{67}, \cdots, p_{71}\}$, $\mathcal{B}_0 = \{B_0, B_1, \cdots, B_5\}, \cdots, \mathcal{B}_{11} = \{B_{66}, B_{67}, \cdots, B_{71}\}$.

Case A G is cyclic.
Let $G = \langle\varphi\rangle$. We may assume that
$\varphi^\Omega = (\mathcal{P}_0, \mathcal{P}_1, \cdots, \mathcal{P}_8)(\mathcal{P}_9, \mathcal{P}_{10}, \mathcal{P}_{11})$ and $\varphi^\Delta = (\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_8)(\mathcal{B}_9, \mathcal{B}_{10}, \mathcal{B}_{11})$.
Therefore we may assume that
$\varphi^\mathcal{X} = (x_0, x_6, x_{12}, x_{18}, x_{24}, x_{30}, x_{36}, x_{42}, x_{48})$
$(x_1, x_7, x_{13}, x_{19}, x_{25}, x_{31}, x_{37}, x_{43}, x_{49})$
$(x_2, x_8, x_{14}, x_{20}, x_{26}, x_{32}, x_{38}, x_{44}, x_{50})$
$(x_3, x_9, x_{15}, x_{21}, x_{27}, x_{33}, x_{39}, x_{45}, x_{51})$
$(x_4, x_{10}, x_{16}, x_{22}, x_{28}, x_{34}, x_{40}, x_{46}, x_{52})$
$(x_5, x_{11}, x_{17}, x_{23}, x_{29}, x_{35}, x_{41}, x_{47}, x_{53})$
$(x_{54}, x_{60}, x_{66}, x_{55}, x_{61}, x_{67}, x_{56}, x_{62}, x_{68})$
$(x_{57}, x_{63}, x_{69}, x_{58}, x_{64}, x_{70}, x_{59}, x_{65}, x_{71})$,
where $(x, \mathcal{X}) \in \{(p, \mathcal{P}), (B, \mathcal{B})\}$.
Set
$\mathcal{Y}_0 = \{x_0, x_6, x_{12}, x_{18}, x_{24}, x_{30}, x_{36}, x_{42}, x_{48}\}$,
$\mathcal{Y}_1 = \{x_1, x_7, x_{13}, x_{19}, x_{25}, x_{31}, x_{37}, x_{43}, x_{49}\}$,
$\mathcal{Y}_2 = \{x_2, x_8, x_{14}, x_{20}, x_{26}, x_{32}, x_{38}, x_{44}, x_{50}\}$,
$\mathcal{Y}_3 = \{x_3, x_9, x_{15}, x_{21}, x_{27}, x_{33}, x_{39}, x_{45}, x_{51}\}$,
$\mathcal{Y}_4 = \{x_4, x_{10}, x_{16}, x_{22}, x_{28}, x_{34}, x_{40}, x_{46}, x_{52}\}$,
$\mathcal{Y}_5 = \{x_5, x_{11}, x_{17}, x_{23}, x_{29}, x_{35}, x_{41}, x_{47}, x_{53}\}$,

$\mathcal{Y}_6 = \{x_{54}, x_{60}, x_{66}, x_{55}, x_{61}, x_{67}, x_{56}, x_{62}, x_{68}\}$ and
$\mathcal{Y}_7 = \{x_{57}, x_{63}, x_{69}, x_{58}, p_{64}, x_{70}, x_{59}, x_{65}, x_{71}\}$,
where $(x, \mathcal{Y}) \in \{(p, \mathcal{Q}), (B, \mathcal{C})\}$. These sets are G-orbits on $\mathcal{P}$ and $\mathcal{B}$.

Set $q_0 = p_0, q_1 = p_1, \cdots, q_5 = p_5$ and $C_0 = B_0, C_1 = B_1, \cdots, C_5 = B_5, C_6 = B_{54}, C_7 = B_{57}$.

For $0 \leq i \leq 5,\ 0 \leq j \leq 7$, set $m_{ij} = |\mathcal{Q}_i \cap (C_j)|$, $D_{ij} = \{\alpha \in G | q_i{}^{\alpha} \in (C_j)\}$ and $M = (m_{ij})_{0 \leq i \leq 5, 0 \leq j \leq 7}$.

Then $m_{ij} = |D_{ij}|$.

3.3 Lemma
(i) *For* $0 \leq i \neq i' \leq 5$,

$$\sum_{0 \leq j \leq 7} D_{ij} D_{i'j}{}^{-1} = 2(G - \{1\}).$$

(ii) *For* $0 \leq i \leq 5$,

$$\sum_{0 \leq j \leq 7} D_{ij} D_{ij}{}^{-1} = 12 + 2(G - \{1\}).$$

By considering the action of the trivial character of G on the equations of 3.3 Lemma we have the folowing lemma.

3.4 Lemma
(i) *For* $0 \leq i \neq i' \leq 5$,

$$\sum_{0 \leq j \leq 7} m_{ij} m_{i'j} = 16.$$

(ii) *For* $0 \leq i \leq 5$,

$$\sum_{0 \leq j \leq 7} m_{ij}{}^2 = 28.$$

(iii) *For* $0 \leq i \leq 7$,

$$\sum_{0 \leq j \leq 7} m_{ij} = 12.$$

3.5 Lemma
For $0 \leq i \leq 5$, $(m_{i\,0}, m_{i\,1}, \cdots, m_{i\,7})$ *is equal to* $(0,1,1,1,1,2,2,4)$ *or* $(0,0,1,1,2,2,3,3)$ *up to ordering.*

3.6 Definition
Let Ω be the set of 6×8 matrices with entries from $\{0,1,2,3,4\}$ satisfying:
(i) For $0 \leq i \leq 5$,
$(x_{i\,0}, x_{i\,1}, \cdots, x_{i\,7})$ is equal to $(0,1,1,1,1,2,2,4)$ or $(0,0,1,1,2,2,3,3)$ up to ordering.
(ii) For $0 \leq r \neq s \leq 5$,

$$\sum_{0 \leq j \leq 7} x_{r\,j} x_{s\,j} = 16.$$

3.7 Definition
Let $X = (x_{ij})_{0 \leq i \leq 5,\ 0 \leq j \leq 7}$, $Y = (y_{ij})_{0 \leq i \leq 5,\ 0 \leq j \leq 7} \in \Omega$. Then,
X is **equivalent** to Y(we denote this by $X \sim Y$)
$\overset{\text{def.}}{\Longleftrightarrow} Y = (y_{ij}) = (x_{i^\alpha j^\beta})$ for some $\alpha \in \mathrm{Sym}\{0,1,\cdots,5\}$, $\beta \in \mathrm{Sym}\{0,1,\cdots,7\}$.

An extensive computer search yields the following lemma.

3.8 Lemma
There are 171 *representatives of* $\Omega/\sim$. $(D_{ij})_{0 \leq i \leq 5, 0 \leq j \leq 7}$*'s corresponding to these do not exist.*

3.9 Lemma
There is no $\mathrm{STD}_2[12;6]$ *admitting an automorphism group of order* 9 *which is cyclic.*

Case B G is an elementary abelian group of order 9.
We consider the following two cases.

Case B-1 The size of any G-orbit on Ω is equal to 3.
In this case we have to consider 10 types of actions of G on $\mathcal{P} \cup \mathcal{B}$. For each type of these actions, we define subsets of G D_{ij} $(0 \leq i, j \leq 7)$ and a 8×8 matrix M by a similar argument as in Case A. But for each type of these actions of G, there does not exist M.

Case B-2 G has a G-orbit of size 9 on Ω.
In this case we can show that it is sufficient to consider 171 representatives of $\Omega/\sim$ of 3.8 Lemma. Using a computer it follows that there is no $(D_{ij})_{0\leq i\leq 5,\ 0\leq j\leq 7}$ corresponding to each representative M, where any D_{ij} is a subset of the elemetary abelian group G of order 9.

3.10 Lemma
There is no $\mathrm{STD}_2[12;6]$ *admitting an automorphism group of order* 9 *which is elementary abelian.*

Proof of 1.8 Theorem: 3.9 Lemma, 3.10 Lemma, [S], [AS].

3.11 Problem
Is there an $\mathrm{STD}_2[12;6]$ $\mathcal{D}$ admitting an automorphism group of order 6?

References
[AS] K. Akiyama and C. Suetake, The nonexistence of projective planes of order 12 with a collineation group of order 8, *J. Combin. Designs* **16**, (2008), 411–430.

[HS] Y. Hiramine and C. Suetake, A contraction of square transversal designs, *Discrete Math.* **308**, (2008), 3257–3264.

[S] C. Suetake, Automorphism groups of a symmetric transversal design $\mathrm{STD}_2[12;6]$, to appear in *J. Statistical Theory and Practice.*

On some equations over finite fields of characteristic 2 and a construction of APN functions

Nobuo Nakagawa
nakagawa@math.kindai.ac.jp

Department of Mathematics, Faculty of Science and Technology, Kinki University, 3-4-1 Kowakae, Higashi Osaka, Osaka 577-8502 Japan

This is a joint work with Lilya Budaghyan and Claude Carlet.

1 Introduction

Importance of functions on a finite fields with high nonlinearity has been recognized in recent applications to cryptgraphy.

Let f be a function on $GF(2^n)$ (from $GF(2^n)$ to itself). For an element $a \in GF(2^n)$, a function $D_a(f)$ is defined as

$$D_a(f)(x) := f(x+a) + f(x).$$

It is easily shown that $D_a(f)^{-1}(b) = \emptyset$ or $|D_a(f)^{-1}(b)| \geq 2$ for any $b \in GF(2^n)$. A function f on $GF(2^n)$ is called an almost perfect nonlinear (APN) function if $D_a(f)^{-1}(b) = \emptyset$ or $|D_a(f)^{-1}(b)| = 2$ for any $b \in GF(2^n)$ and any nonzero element $a \in GF(2^n)$. Then $x \mapsto D_a(f)(x)$ is a two to one mapping from $GF(2^n)$ to $\mathrm{Im}(D_a(f))$ for any $a \in GF(2^n)^\times$.

Recently several quadratic APN functions have been constructed ([1],[2]). We are interested in a construction of APN functions starting from a finite geometric object, finite semifields planes. We deduce a function

$$f(x) = x^3 + \alpha x^{2t+1} + \alpha x^{3t} + \alpha^{t+1} x^{t+2}$$

on $GF(2^{2e})$ where $t = 2^e$, $\alpha \in GF(2^{2e})$ from the cubic function $f(x) = (x \circ x) \circ x$ of certain Albert's semifields. It is proved in [4] that the function $f(x)$ above is a differentially 4-uniform function.

We consider more generally functions as follows;

$$f(x) = x^3 + Ax^{2t+1} + Bx^{t+2} + Cx^{3t}$$

on $GF(2^{2e})$ where $t = 2^e$ and $A, B, C \in GF(2^{2e})$ which are named cubic type of semifields.

We made sure by computers that there are many APN functions of cubic type for $3 \leq e \leq 8$. And we proved that some cubic type functions are APN functions.

Theorem 1
Let $f(x) = x^3 + x^{2t+1} + \gamma x^{t+2}$, $g(x) = x^3 + x^{2t+1} + \gamma x^{3t}$ be functions on $GF(2^{2e})$ where $t = 2^e$. Suppose that $2k$ is a divisor of e for a positive integer $k > 1$ and $\gamma \in GF(2^k) \setminus GF(2)$. Then $f(x)$ and $g(x)$ are APN functions on $GF(2^{2e})$.

We observed these functions are extended affine equivalent to Gold functions.

Theorem 2
Let $f(x) = x^3 + ux^{2t+1} + ux^{t+2} + (u+1)x^{3t}$ be functions on $GF(2^{2e})$ where $t = 2^e$. Suppose that e is even and $u \in GF(2^e) \setminus GF(2)$. Then $f(x)$ is an APN function on $GF(2^{2e})$.

The following lemma is the key lemma to obtain the theorems above.

Lemma 3(See Theorem 2 in [5])
let $x^{2t} + \alpha x^t + \beta x^2 + \delta x = 0$ be an equation on $GF(2^{2e})$ where $\delta = \alpha + \beta + 1$ and $t = 2^e$. Suppose that $\alpha \neq 1$, $\beta^{t+1} \neq 1$ and $\beta^t \neq (\alpha+1)^{t-1}$. Set

$$Q := ((\delta^t + \beta^t \alpha)(\alpha^{t+1} + \delta^{t+1}))/(1 + \beta^{2t+2}).$$

Then the above equation has just two solutions $x = 0$ and $x = 1$ in $GF(2^{2e})$ if and only if

$$Q + Q^2 + Q^4 + \cdots + Q^{t/2} \neq (Q^t + \beta Q)/(\alpha + 1).$$

2 Proof of Theorem 1 and Theorem 2

Proof of Theorem 1

Take any $a \in GF(2^{2e})$ such that $a \neq 0$.

$$f(x+a) + f(x) + f(a) = (a^2 x + a^2 x) + (a^{2t} x + a x^{2t}) + \gamma(a^t x^2 + a^2 x^t).$$

We may prove that the equation

$$(a^2 x + a^2 x) + (a^{2t} x + a x^{2t}) + \gamma(a^t x^2 + a^2 x^t) = 0$$

has just two solutions in $GF(2^{2e})$. Put $y := x/a$. Then we have

$$a^3(y + y^2) + a^{2t+1}(y + y^{2t}) + \gamma a^{t+2}(y^2 + y^t) = 0.$$

Multiple a^{-3} to both side of the equation above then set $b := a^{t-1}$ and rewrite x instead of y. Then we have

$$b^2 x^{2t} + \gamma b x^t + (1 + \gamma b)x^2 + (1 + b^2)x = 0.$$

Divide by b^2 bothside above and put $c := b^{-1}$. Then

$$x^{2t} + \gamma c x^t + (c^2 + \gamma c)x^2 + (c^2 + 1)x = 0. \tag{1}$$

Here we denote by K the subgroup of $GF(2^{2e})^\times$ of order $t+1$ and by H the subgroup of $GF(2^{2e})^\times$ of order $t-1$. We have $K \cap H = \{1\}$ trivially.

We remark that $c \in K$ and $\gamma \in H$. Therefore $c^{t+1} = 1$ and $\gamma^t = \gamma$.

We adopt **Lemma 3** here. Then

$$\alpha = \gamma c, \quad \beta = c^2 + \gamma c, \quad \delta = c^2 + 1.$$

We have $\alpha \neq 1$. Because suppose that $\alpha = 1$. Then $c = \gamma^{-1} \in H \cap K$ and $\gamma = 1$, a contradiction. We have $\beta^{t+1} \neq 1$. Because suppose that $\beta^{t+1} = 1$. $(c^{2t} + c^t\gamma)(c^2 + c\gamma) = 1$ Since $c^{2t+2} = 1$, $c^{2t+1} = c^t$, $c^{t+2} = c$, $c^t + c + \gamma = 0$. Since $GF(2^{2k})$ is the quadratic extension of $GF(2^k)$ and $c^2 + c + \gamma = 0$ is a quadratioc equation over $GF(2^k)$, $c \in GF(2^{2k})$, thus $c \in GF(2^e)$ because of $2k|e$. Therefore $c \in H$. Namely $c \in H \cap K$. Thus $c = 1$, implies $\gamma = 0$, a contradiction.

We have $\beta^t \neq (\alpha+1)^{t-1}$. Because we suppose that $\beta^t = (\alpha+1)^{t-1}$. Then $(\alpha+1)\beta^t = (\alpha+1)^t = (\alpha^t+1)$. Therefore $(c\gamma+1)(c^{2t}+c^t\gamma) = (c^t\gamma+1)$. Thus $\gamma c^t + \gamma^2 + c^{2t} + \gamma c^t = \gamma c^t + 1$ because of $c^{t+1} = 1, \gamma^t = \gamma$. We have $(c^t)^2 + \gamma c^t + (\gamma^2+1) = 0$. Because $GF(2^{2k})$ is the quadratic extension of $GF(2^k)$ and $\gamma \in GF(2^k)$, $c^t \in GF(2^{2k})$, that is $c^t \in GF(2^e)$. Hence $c^t \in H \cap K$. Therefore $c^t = 1$, which implies $\gamma^2 + \gamma = 0$. This is a contradiction.

Above all, We have $\alpha \neq 1$, $\beta^{t+1} \neq 1$ and $\beta^t \neq (\alpha+1)^{t-1}$. Hence the theorem is verifies if we prove that

$$Q + Q^2 + \cdots + Q^{t/2} \neq (Q^t + \beta Q)/(\alpha+1)$$

from **Lemma 3**. It holds that $(\beta^{2t+2}+1) = \gamma^2 c^{2t} + \gamma^2 c^2 + \gamma^4$ as we proved in previous parts.

On the other hand

$$\alpha^{t+1} + \delta^{t+1} = c^{t+1}\gamma^{t+1} + (c^2+1)^{t+1} = \gamma^2 + (c^{2t}+1)(c^2+1) = \gamma^2 + c^{2t} + c^2.$$

Therefore

$$(\alpha^{t+1} + \delta^{t+1})/(\beta^{2t+2}+1) = 1/\gamma^2.$$

Moreover

$$\delta^t + \alpha\beta^t = (c^2+1)^t + c\gamma(c^{2t} + c^t\gamma) = c^{2t} + 1 + \gamma c^t + \gamma^2.$$

Then we have

$$Q = (c^{2t} + \gamma c^t + (\gamma^2+1))/\gamma^2.$$

Thus

$$Q + Q^2 + \cdots + Q^{t/2} =$$

$$\frac{1}{\gamma^2}(c^{2t}+\gamma c^t+(\gamma^2+1)) + \frac{1}{\gamma^4}(c^{4t}+\gamma^2 c^{2t}+(\gamma^4+1)) + \frac{1}{\gamma^8}(c^{8t}+\gamma^4 c^{4t}+(\gamma^8+1)) + \cdots + \frac{1}{\gamma^t}(c^{t^2}+\gamma^{t/2}c^{t^2/2}+(\gamma^t+1))$$

$$= \frac{1}{\gamma}c^t + \frac{1}{\gamma}c + \mathrm{Tr}_{(GF(2^e)/GF(2))}(\gamma).$$

Remark that e is even.

Here $\mathrm{Tr}_{(GF(2^e)/GF(2))}(\gamma) = 0$ because $\gamma + \gamma^2 + \cdots + \gamma^{2^{k-1}} = 1$ or 0. Now we have

$$Q + Q^2 + \cdots + Q^{t/2} = \frac{1}{\gamma}(c + c^t).$$

On the other hand

$$(Q^t + \beta Q)/(\alpha + 1) = \frac{1}{\gamma^2}(c^2 + c + \gamma^2 + 1 + (c^2 + \gamma c)(c^{2t} + c^t + \gamma^2 + 1))/(\gamma c + 1).$$

Thus

$$(Q^t + \beta Q)/(\alpha + 1) = (\gamma c^t + \gamma^2 c^2 + \gamma^3 c + \gamma c)/(\gamma^3 c + \gamma^2).$$

Suppose that

$$Q + Q^2 + \cdots + Q^{t/2} = (Q^t + \beta Q)/(\alpha + 1).$$

Then

$$(c^t + c)(\gamma^2 c + \gamma) = \gamma c^t + \gamma^2 c^2 + \gamma^3 c + \gamma c.$$

Therefore $\gamma c = 1$. Thus $c \in H \cap K = \{1\}$, which means that $\gamma = 1$, a contradiction. Hence we have

$$Q + Q^2 + \cdots + Q^{t/2} \neq (Q^t + \beta Q)/(\alpha + 1),$$

namely the equation (1) has just two solutions at $GF(2^{2e})$ from **Lemma 3.** Therefore $f(x)$ in the theorem is an APN function.
It is proved that a function $g(x) = x^3 + x^{2t+1} + \gamma x^{3t}$ on $GF(2^{2e})$ is APN by the similar arguments as we did concerning $f(x)$.

Proof of Theorem 2.

Take any $a \in GF(2^{2e})$ such that $a \neq 0$.

$$f(x + a) + f(x) + f(a) = (a^2 x + a x^2) + u(a^{2t} x + a x^{2t}) + u(a^2 x^t + a^t x^2) + (u + 1)(a^{2t} x^t + a^t x^{2t}).$$

We may prove that the equation

$$(a^2 x + a x^2) + u(a^{2t} x + a x^{2t}) + u(a^2 x^t + a^t x^2) + (u + 1)(a^{2t} x^t + a^t x^{2t}) = 0.$$

has just two solutions in $GF(2^{2e})$. Set $b := a^{t-1}$.

By the same arguments of theorem 1, we may prove that the equation

$$((u + 1)b^3 + ub^2)x^{2t} + ((u + 1)b^3 + ub)x^t + (1 + ub)x^2 + (1 + ub^2)x = 0 \qquad (2)$$

has just two solusions, namely $x = 0, 1$ in $GF(2^{2e})$. We denote by H the subgroup of $GF(2^{2e})^\times$ of order $t - 1$ and by K the subgroup of $GF(2^{2e})^\times$ of order $t + 1$. Note that $b \in K$ and $u \in H$. Hence $b^{t+1} = 1$, $u^t = u$.

Suppose that $(u+1)b^3+ub^2=0$. Then $b=\frac{u}{u+1}\in H\cap K=\{1\}$. Thus $b=1$ and $u=u+1$, a contradiction. Therefore $(u+1)b^3+ub^2\neq 0$.

We have

$$x^{2t}+\alpha x^t+\beta x^2+\delta x=0 \tag{3}$$

where

$$\alpha=((u+1)b^3+ub)/((u+1)b^3+ub^2),\ \beta=(1+ub)/((u+1)b^3+ub^2),\ \delta=(1+ub^2)/((u+1)b^3+ub^2).$$

Suppose that $\alpha=1$. Then $ub=ub^2$, so $b=1$. Substitute $b=1$ to (2). Then we obtain

$$x^{2t}+x^t+(u+1)x^2+(u+1)x=0.$$

Hence

$$(x^2+x)\{(x^2+x)^{t-1}+(u+1)\}=0.$$

If this equation has a solusion which is an elemennt of $GF(2^{2e})\backslash GF(2)$, $(u+1)\in(GF(2^{2e})^\times)^{t-1}$, namely $(u+1)^{t+1}=1$. Thus $(u+1)\in H\cap K=\{1\}$. Therefore $u=0$, a contradiction.

Hence $\alpha\neq 1$.

Suppose that $\beta^{t+1}=1$. Then

$$(1+u^tb^t)(1+ub)=((u+1)^tb^{3t}+u^tb^{2t})((u+1)b^3+ub^2).$$

Therefore $1+b^t+b=0$, thus $b^2+b+1=0$, which means that $b\in GF(4)\subset GF(2^e)$ as e is even. Thus $b\in H\cap K$ and $b=1$. We have a contradiction again as we see above.

Hence $\beta^{t+1}\neq 0$.

Suppose that $\beta^t=(\alpha+1)^{t-1}$. Then $(\alpha+1)\beta^t=(\alpha+1)^t=(\alpha^t+1)$. Therfore

$$(ub+ub^2)/((u+1)b^3+ub^2)\times(1+u^tb^t)/((u+1)^tb^{3t}+u^tb^{2t})=(u^tb^t+u^tb^{2t})/(((u+1)^tb^{3t}+u^tb^{2t}).$$

We have $u^2(b^2+b)=0$ from this equation. Hence $b=1$ a contradiction.

Above all, We have $\alpha\neq 1$, $\beta^{t+1}\neq 1$ and $\beta^t\neq(\alpha+1)^{t-1}$. Hence the theorem is verifies if we prove that

$$Q+Q^2+\cdots+Q^{t/2}\neq(Q^t+\beta Q)/(\alpha+1)$$

from **Lemma 3.**

Now we calculate

$$Q=(\alpha^{t+1}+\delta^{t+1})(\delta^t+\alpha\beta^t)/(\beta^{2t+2}+1).$$

$$(\beta^{2t+2}+1)=\{(1+u^{2t}b^{2t})(1+u^2b^2)\}/\{((u+1)^{2t}b^{6t}+u^{2t}b^{4t})((u+1)^2b^6+u^2b^4)\}+1$$

$$=u^4(1+b^2+b^{2t})/(1+(u^2+u^4)b^2+(u^2+u^4)b^{2t}).$$

5

Next,

$$(\alpha^{t+1}+\delta^{t+1}) = \{(1+u^tb^{2t})(1+ub^2)+((u+1)^tb^{3t}+u^tb^t)((u+1)b^3+ub)\}/\{((u+1)^tb^{3t}+u^tb^{2t})((u+1)b^3+ub^2)\}$$

$$= u^2(1+b^2+b^{2t})/(1+(u+u^2)b+(u+u^2)b^t).$$

Thus

$$(\alpha^{t+1}+\delta^{t+1})/(\beta^{2t+2}+1) = (1+(u+u^2)b+(u+u^2)b^t)/u^2.$$

Moreover

$$\delta^t+\alpha\beta^t = (1+u^tb^{2t})/((u+1)^tb^{3t}+u^tb^{2t})+((u+1)b^3+ub)/(u+1)b^3+ub^2)\times(1+u^tb^t)/((u+1)^tb^{3t}+u^tb^{2t})$$

$$= u^2(b+b^2)/(1+(u+u^2)b+(u+u^2)b^t).$$

Therefore

$$Q = (1+(u+u^2)b+(u+u^2)b^t)/u^2 \times u^2(b+b^2)/(1+(u+u^2)b+(u+u^2)b^t) = b+b^2.$$

Therefore we obtain

$$Q+Q^2+Q^4+\cdots+Q^{t/2} = b+b^t.$$

On the other hand,

$$(Q^t+\beta Q)/(\alpha+1) = \{b^t+b^{2t}+(b+b^2)\frac{1+ub}{(u+1)b^3+ub^2}\} \times ((u+1)b^3+ub^2)/(ub+ub^2)$$

$$= (1+b^3)/(b+b^2).$$

Suppose that

$$Q+Q^2+Q^4+\cdots+Q^{t/2} = (Q^t+\beta Q)/(\alpha+1).$$

Then

$$b+b^t = (1+b^3)/(b+b^2),$$

which implies $b=1$. This is also a contradiction again. Hence we have

$$Q+Q^2+Q^4+\cdots+Q^{t/2} \neq (Q^t+\beta Q)/(\alpha+1),$$

namely the equation (2) has just two solutions at $GF(2^{2e})$ from **Lemma 3**. Therefore $f(x)$ in the theorem is an APN function.

3 Discussions

We like to consider the general form of the functions on $GF(2^{2e})$ of the cubic type as follows

$$f(x) = x^3+ax^{2t+1}+bx^{t+2}+cx^3.$$

Deliberate the equation

$$f(x+u)+f(x)+f(u)=0$$

for any $u \in GF(2^{2e})$ such that $u \neq 0$. Then from this equation we have the equation

$$x^t+\alpha x^t+\beta x^2+\gamma x=0$$

where $t=2^e$, $\alpha=(bv+cv^3)/(av^2+cv^3)$, $\beta=(1+bv)/(av^2+cv^3)$ and $\gamma=(1+av^2)/(av^2+cv^3)$ for $v:=u^{t-1}$ if it holds $(av^2+cv^3)\neq 0$. Moreover

$$Q=(\alpha^{t+1}+\gamma^{t+1})(\gamma^t+\alpha\beta^t)/(1+\beta^{2t+2})=A/B$$

where

$$A=\{(1+a^{t+1}+b^{t+1}+c^{t+1})+(a+cb^t)v^2+(a^t+bc^t)v^{2t}\}\{(a^{t+1}+b^{t+1})+(b+a^tc)v+(a+b^tc)v^2\},$$

$$B=(1+a^{2t+2}+b^{2t+2}+c^{2t+2})+(b^2+c^2a^{2t})v^2+(b^{2t}+a^2c^{2t})v^{2t}.$$

Here suppose that

$$1+a^{t+1}+b^{t+1}+c^{t+1}=0, \text{ and } a+cb^t=b^2+c^2a^{2t}.$$

Then

$$Q=(1+c^{t+1})+(b+a^tc)v+((b+a^tc)v)^2.$$

Therefore

$$Q+Q^2+Q^4+\cdots+Q^{t/2}=(b+a^tc)v+((b+a^tc)v)^t$$

because of $s+s^2+s^4+\cdots+s^{t/2}=0$ for $s\in GF(2^e)$. In this case there are a few possibility to construct APN functions of the cubic type.

Edel,Kyureghyan and Pott proved that a function $f(x)=x^3+ux^{36}$ on $GF(2^{10})$ is an APN function if $u\notin GF(2^5)$ in [3]. We consider a function

$$f(x)=x^3+ux^{t+4}$$

on $GF(2^{2p})$ where p is an odd prime and $t=2^p$ in general. We have a equation

$$(X+X^2)+ua^{t+1}(X^t+X^4)=0$$

from $f(x+a)+f(x)+f(a)=0$ for $a\neq 0$. Note to $X:=x/a$. Here consider the function

$$g(x)=(x^t+x^4)/(x^2+x)$$

from $GF(2^{2p})$ to $GF(2^{2p})$. We define $g(1)=g(0)=0$. We would like to give a conjecture here in this situation as follows.

Conjecture BCN:

$$GF(2^p)\mathrm{Im}(g)\neq GF(2^{2p})$$

If this conjecture holds, then a function $f(x)=x^3+ux^{t+4}$ is APN for $u\in GF(2^{2e})\setminus GF(2^p)\mathrm{Im}(g)$. For $p=3$ set $GF(64)=GF(2)(\theta)$ where $\theta^6=\theta+1$. Note that θ is a generator of $GF(64)^\times$. Now we can check easily that $GF(8)\mathrm{Im}(g)=<\theta^3>\cup\{0\}$.

References

[1] Budaghyan,L.,Carlet,C. and Leander,G. A class of quadratic APN binomials in equivalent to power functions(submitted).

[2] Budaghyan,L.,Carlet,C. and Pott,A. New classes of almost perfect nonlinear functions, Trans. Inform. Theory 52(3), 1141-1152 (2006).

[3] Edel,Y.,Kyureghyan,G. and Pott,A. A new APN function which is not equivalent to a power mapping, IEEE Trans. Inform. Theory 52, 744-747(2006).

[4] Nakagawa,N.and Yoshiara, S. A Construction of Differentially 4-Uniform Functiopns from Commutative Semifields of Characteristic 2, LNCS 4547(Proceedings of First International Workshop,WAIFI 2007), 134-146(2007).

[5] Nakagawa,N. Report of talk given at Kyoto RIMS on December 17-19,2007 for the Conference on finite groups and algebraic combinatorics ,Sugaku Kokyuroku 1593(ed. by Harada,M.)

Virasoro Frames and Frame Stabilizers for Framed Vertex Operator Algebras

Ching Hung Lam

National Cheng Kung University
Tainan, Taiwan 701

This manuscript is based on the sildes of my talk given at Hokkaido Uinversity on June 2008.

1 Virasoro Vertex operator algebra

Let $Vir = \bigoplus_{n\in\mathbb{Z}} \mathbb{C}L_n \bigoplus \mathbb{C}\mathbf{c}$ be a Virasoro algebra, i.e.,

$$\begin{aligned} [L_m, L_n] &= (m-n)\,L_{m+n} + \frac{1}{12}\left(m^3 - m\right)\delta_{m+n,0}\mathbf{c}; \\ [L_m, \mathbf{c}] &= 0. \end{aligned}$$

Let $L(c,h)$ be an irreducible highest weight module of Vir of central charge c and highest weight h. That means $L(c,h)$ is irreducible and generated by a single vector $\mathbf{1}$. Moreover,

$$\begin{aligned} L_n \cdot \mathbf{1} &= 0 \text{ for } n \geq 1 \\ L_0 \cdot \mathbf{1} &= h \cdot \mathbf{1} \text{ and } \mathbf{c} \cdot \mathbf{1} = c\mathbf{1}. \end{aligned}$$

When $c = 1/2, h = 0$, $L\left(\frac{1}{2}, 0\right)$ is a rational VOA and it has exactly 3 irreducible modules, namely

$$L\left(\frac{1}{2}, 0\right), \quad L\left(\frac{1}{2}, \frac{1}{2}\right), \quad \text{and} \quad L\left(\frac{1}{2}, \frac{1}{16}\right)$$

where $0, \frac{1}{2}$ and $\frac{1}{16}$ are highest weights.

Its fusion product is given as:

$$L\left(\frac{1}{2},\frac{1}{2}\right)\times L\left(\frac{1}{2},\frac{1}{2}\right)=L\left(\frac{1}{2},0\right),$$

$$L\left(\frac{1}{2},\frac{1}{2}\right)\times L\left(\frac{1}{2},\frac{1}{16}\right)=L\left(\frac{1}{2},\frac{1}{16}\right),$$

$$L\left(\frac{1}{2},\frac{1}{16}\right)\times L\left(\frac{1}{2},\frac{1}{16}\right)=L\left(\frac{1}{2},0\right)+L\left(\frac{1}{2},\frac{1}{2}\right),$$

and $L\left(\frac{1}{2},0\right)$ acts as an identity. Note that the fusion product gives a group structure on $(\{0,1/2\},\times)$ and $\{0,1/2,1/16\}/\{0,1/2\}$. In fact, $(\{0,1/2\},\times)\cong\mathbb{Z}_2$, and $\{0,1/2,1/16\}/\{0,1/2\}\cong\mathbb{Z}_2$.

2 Miyamoto involutions

Definition. Let $V=\oplus_{n\geq 0}V_n$ be a VOA. An element $e\in V_2$ is called an *Ising vector* if the subVOA $\mathrm{Vir}(e)$ generated by e is isomorphic to $L(1/2,0)$.

Let $e\in V$ be an Ising vector. Then, $\mathrm{Vir}(e)\simeq L(1/2,0)$. Define τ_e on V by

$$\tau_e=\begin{cases}1 & \text{on } V_e(0)\oplus V_e(1/2),\\ -1 & \text{on } V_e(1/16),\end{cases}\quad\in \mathrm{Aut}(V)\quad\text{(Miyamoto)}$$

where $V_e(h)$ be the sum of all irreducible $\mathrm{Vir}(e)$-submodules of V isomorphic to $L(1/2,h)$ for $h=0,1/2,1/16$.

On the fixed point subalgebra $V^{\langle\tau_e\rangle}=V_e(0)\oplus V_e(1/2)$, one can define another linear automorphism σ_e by

$$\sigma_e=\begin{cases}1 & \text{on } V_e(0),\\ -1 & \text{on } V_e(1/2).\end{cases}$$

Then σ_e also defines an automorphism on $V^{\langle\tau_e\rangle}$.

Theorem: (Conway-Miyamoto) There is a one to one correspondence between the Ising vectors in $V^\natural$ and the elements in the $2A$ conjugacy class of the Monster.

$$e \quad\longleftrightarrow\quad \tau_e$$

3 Framed vertex operator algebra

Definition. A *framed vertex operator algebra* V is a simple vertex operator algebra which contains a subVOA F called a Virasoro frame isomorphic to a tensor product of n-copies of the simple Virasoro VOA $L(1/2, 0)$, i.e., $F = L(1/2, 0)^{\otimes n}$, such that $\mathrm{rank}(V) = \mathrm{rank}(F) = n/2$.

Examples.

1. the Moonshine VOA $V^\natural$ constructed by Frenkel-Lepowsky-Meurman, whose full automorphism group $\mathrm{Aut}\, V^\natural$ =Monster

2. the lattice VOA $V_{\sqrt{2}A_1}$, and

$$V_{\sqrt{2}A_1} \cong L(\frac{1}{2}, 0) \otimes L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{1}{2}, \frac{1}{2})$$

3. Many lattice VOAs and their twisted versions.

Example. Let $L = \sqrt{2}A_1 = \mathbb{Z}\alpha$, $(\alpha, \alpha) = 4$ and $L^* = \{\beta \in \mathbb{Q} \otimes_{\mathbb{Z}} L | (\beta, \alpha) \in \mathbb{Z}\} = \frac{1}{4}L$ its dual lattice. Then $L^*/L \cong \mathbb{Z}_4$ and $L^* = L \cup \{\frac{1}{4}\alpha + L\} \cup \{\frac{1}{2}\alpha + L\} \cup \{-\frac{1}{4}\alpha + L\}$. There is a nice correspondence.

$$\begin{aligned}
0 &\longleftrightarrow \quad V_L \quad = L(\frac{1}{2}, 0) \otimes L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{1}{2}, \frac{1}{2}), \\
1 &\longleftrightarrow V_{\frac{1}{4}\alpha+L} = L(\frac{1}{2}, \frac{1}{16}) \otimes L(\frac{1}{2}, \frac{1}{16}), \\
2 &\longleftrightarrow V_{\frac{1}{2}\alpha+L} = L(\frac{1}{2}, \frac{1}{2}) \otimes L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, 0) \otimes L(\frac{1}{2}, \frac{1}{2}), \\
3 &\longleftrightarrow V_{-\frac{1}{4}\alpha+L} = L(\frac{1}{2}, \frac{1}{16}) \otimes L(\frac{1}{2}, \frac{1}{16})
\end{aligned}$$

$$\begin{aligned}
0 &\longleftrightarrow (0,0), (1/2, 1/2), \\
2 &\longleftrightarrow (1/2, 0), (0, 1/2) \\
1 \text{ or } 3 &\longleftrightarrow (1/16, 1/16)
\end{aligned}$$

Important facts.

1. All framed VOAs are rational. [DGH]

2. If V is framed and $V_1 = 0$, then $\mathrm{Aut}\, V$ is a finite group.[Miy]

Remark. The subalgebra F is not unique. In general, there are many subalgebra $\cong L(1/2, 0)^{\otimes n}$ in V. In fact, there may be infinitely many.

Questions:

1. Characterizes all Virasoro frames of V (up to the actions of $\mathrm{Aut}(V)$).
2. Compute the frame stabilizer of a given frame F, i.e., the subgroup of all automorphisms of V which stabilizes the frame F setwise

4 Frame stabilizers and Pointwise Frame stabilizers

Definition. Let V be a framed VOA with a frame F. The *frame stabilizer* of F is the subgroup of all automorphisms of V which stabilizes the frame F setwise. The *pointwise frame stabilizer* is the subgroup of $\mathrm{Aut}(V)$ which fixes F pointwise.

The frame stabilizer and the pointwise frame stabilizer of F are denoted by $\mathrm{Stab}_V(F)$ and $\mathrm{Stab}_V^{\mathrm{pt}}(F)$, respectively.

Structure codes

We shall associate two binary codes C and D to V and F as follows.

Let $F \simeq L(1/2,0)^{\otimes n}$ (rational). Therefore

$$V = \bigoplus_{h_i \in \{0,1/2,1/16\}} m_{h_1,\dots,h_n} L(1/2,h_1) \otimes \cdots \otimes L(1/2,h_n),$$

where $m_{h_1,\dots,h_r} \geq 0$ is the multiplicity of $L(1/2,h_1) \otimes \cdots \otimes L(1/2,h_n)$ in V. Note that all the multiplicities are finite and $m_{h_1,\dots,h_r} \leq 1$ if all h_i are different from $1/16$.

Let $M = L(1/2,h_1) \otimes \cdots \otimes L(1/2,h_n)$ be an irreducible module over F. The $1/16$-word (or τ-word) $\tau(M)$ of M is a binary codeword $\beta = (\beta_1,\dots,\beta_n) \in \mathbb{Z}_2^n$ such that

$$\beta_i = \begin{cases} 0 & \text{if } h_i = 0 \text{ or } 1/2, \\ 1 & \text{if } h_i = 1/16. \end{cases}$$

For any $\alpha \in \mathbb{Z}_2^n$, define

V^α =the sum of all irreducible submodules M of V such that $\tau(M) = \alpha$.

Denote $D := \{\alpha \in \mathbb{Z}_2^n \mid V^\alpha \neq 0\}$. Then D is an even linear subcode of $\mathbb{Z}_2^n$ and $V = \oplus_{\alpha \in D} V^\alpha$. Moreover, V^0 is a subalgebra of V.

For any $\gamma = (\gamma_1,\dots,\gamma_n) \in \mathbb{Z}_2^n$, denote $V(\gamma) = L(1/2,h_1) \otimes \cdots \otimes L(1/2,h_n)$ where $h_i = 1/2$ if $\gamma_i = 1$ and $h_i = 0$ elsewhere.

Set $C := \{\gamma \in \mathbb{Z}_2^n \mid m_{\gamma_1/2,\dots,\gamma_n/2} \neq 0\}$. Then C is an even linear code also.

Note that $V(0) = F$ and $V^0 = \oplus_{\gamma \in C} V(\gamma)$. V^0 is called a code VOA associated with C. The codes C and D are called the structures codes of V with respect to the frame F.

As a summary, we have:

1. A code $D \longleftrightarrow$ the positions of 1/16. (triply even)
2. A code $C \longleftrightarrow$ the positions of 1/2 if there is no 1/16. (even)

Remark. The codes (C, D) depend on the choice of the frame F. Different frames may give different codes.

Proposition: Let F and F' be Virasoro frames of V. Suppose that there is $g \in \mathrm{Aut}(V)$ such that $F' = g(F)$. Then $C(F) \cong C(F')$ and $D(F') \cong D(F)$.

Basic facts about Frame stabilizers and Pointwise stabilizers

Let (C, D) be the structure code of V with respect to F. Then we have the followings.

1. $\mathrm{Stab}_V^{\mathrm{pt}}(F) \lhd \mathrm{Stab}_V(F)$.
2. The group $\mathcal{T} = \{\tau_\gamma | \, \gamma \in \mathbb{Z}_2^n\} \cong \mathbb{Z}_2^n / D^\perp$ is in the center of $\mathrm{Stab}_V^{\mathrm{pt}}(F)$.
3. $\mathrm{Stab}_V^{\mathrm{pt}}(F)/\mathcal{T} < Hom(C, \{\pm 1\}) = \{\varphi_x \, | x \in \mathbb{Z}_2^n, \varphi_x(y) = (-1)^{(x,y)}, y \in C\}$. In fact,
$$\mathrm{Stab}_V^{\mathrm{pt}}(F)/\mathcal{T} = \{\varphi_x \mid x \in P\},$$
where $P := \{\xi \in \mathbb{Z}_2^n \mid \alpha \cdot \xi \in C \text{ for all } \alpha \in D\}$.
4. $\mathrm{Stab}_V(F)/\mathrm{Stab}_V^{\mathrm{pt}}(F) < \mathrm{Aut}(C)$ and $\mathrm{Stab}_V(F) < \infty$.

Question: What are the possible choices for the codes C and D? We will show that they satisfy some "duality" conditions.

Structure Codes

The structure codes (C, D) actually satisfy some "duality" conditions.

Theorem[L-Yamauchi]. Let $V = \oplus_{\beta \in D} V^\beta$ be a framed VOA with the structure codes C and D. Then for any $\beta \in D$, the code $C_\beta = \{\alpha \in C | \, \mathrm{supp}\, \alpha \subset \mathrm{supp}\, \beta\}$ contains a doubly even self-dual subcode w.r.t. β. As a consequence, all V^β are simple current modules.

Fact. A framed VOA V with structure codes (C, D) is holomorphic (i.e, V is the only irreducible V-module) if and only if $C = D^\perp$.

As a consequence, we also have

Theorem. Let V be a holomorphic framed VOA with the structure codes C and D. Then

(1) the length of C and D are divisible by 16 and $C = D^\perp$;

(2) C is even and every codeword of D has a weight divisible by 8;

(3) for any $\alpha \in D$, the subcode C_α of C contains a doubly even self-dual subcode w.r.t. α.

Remark. The above conditions are also sufficient. That means if C and D are binary codes satisfy the condition (1),(2), and (3), then there exists a holomorphic framed VOA whose structure codes are C and D.

Theorem. Let $n = 16k$ and D is a linear code of length n.
Suppose $(1^n) \in D$ and for any $\alpha \in D$, the weight of α is divisible by 8. Then $C = D^\perp$ and D satisfy the condition (1),(2), and (3) above. D is called admissible in this case.

5 $\mathbb{Z}_4$-codes and Framed VOA

Let Z be a self-orthogonal linear code over $\mathbb{Z}_4$. Define

$$A_4(Z) = \frac{1}{2}\{(x_1, \ldots, x_n) \in \mathbb{Z}^n | (x_1, \ldots, x_n) \in Z \mod 4\}.$$

Then $A_4(Z)$ is an even lattice. It is also well-known that $A_4(Z)$ is unimodular iff Z is self-dual.

Note that if $Z = 0$, then $A_4(Z) \cong \sqrt{2}A_1^n$. Hence the lattice VOA $V_{A_4(Z)}$ is framed for any Z.

Let Z be a self-dual $\mathbb{Z}_4$ code. Denote

$$Z_0 = \{(\alpha_1, \ldots, \alpha_n) \in \{0,1\}^n | (2\alpha_1, \ldots, 2\alpha_n) \in Z\},$$
$$Z_1 = \{\alpha \in \{0,1\}^n | \alpha \equiv \beta \mod 2 \text{ for some } \beta \in Z\}.$$

Then Z_1 is doubly even and $Z_0^\perp = Z_1$.

The structure codes of the lattice VOA $V = V_{A_4(Z)}$ is given by

$$D = d(Z_1) \quad \text{and} \quad C = D^\perp \supset \{(0,0),(1,1)\}^n,$$

where $d : 0 \to 00, 1 \to 11$.

Let $\delta = (10)^n$. Then $\tilde{D} =< d(Z_1), (10)^n >$ is also tribly even. Therefore, there exists holomorphic framed VOA with structure codes $(\tilde{D}^\perp, \tilde{D})$.

$\mathbb{Z}_2$-orbifold.

Let V be a framed VOA with the structure codes (C, D),i.e., $V = \oplus_{\alpha \in D} V^\alpha$, and $V^0 = M_C$. For a binary codeword $\beta \in \mathbb{Z}_2^n$, we define a linear map $\tau_\beta : V \to V$ by

$$\tau_\beta = (-1)^{\langle \alpha, \beta \rangle} v, \quad \text{for } v \in V^\alpha.$$

Then τ_β is an automorphism of V and is often called a τ-involution.

Theorem: Let $V = \oplus_{\alpha \in D} V^\alpha$ be a holomorphic framed VOA with structure codes (C, D). For any $\delta \in \mathbb{Z}_2^n$, denote

$$D^0 = \{\alpha \in D \mid \langle \alpha, \delta \rangle = 0\} \quad \text{and} \quad D^1 = \{\alpha \in D \mid \langle \alpha, \delta \rangle \neq 0\}.$$

Define

$$V(\tau_\delta) = \begin{cases} (\bigoplus_{a\in D^0} V^a) \oplus (\bigoplus_{a\in D^1} M_{\delta+C} \times_{M_C} V^a) & \text{if wt}\,\delta \text{ is odd,} \\ (\bigoplus_{a\in D^0} V^a) \oplus (\bigoplus_{a\in D^0} M_{\delta+C} \times_{M_C} V^a) & \text{if wt}\,\delta \text{ is even.} \end{cases}$$

Then $V(\tau_\delta)$ is also a holomorphic framed VOA.

Let $\tilde{D} =< d(Z_1), (10)^n >$ and $\tilde{C} = \tilde{D}^\perp$. Let V be a holomorphic VOA with the structure codes $(\tilde{C}, \tilde{D})$. Set $\delta = (1100\ldots0)$. Then $V(\tau_\delta)$ is isomorphic to a lattice VOA associated with a self dual $\mathbb{Z}_4$-code.

Conjecture: Let D be a non-decomposable triply even binary code of length $16k$. Then D is a subcode of $< d(C), (01)^{8k} >$, where C is a double even self-dual codes of length $8k$.

The conjecture hold for $k = 1, 2$ but is not proved for $k \geq 3$.

The conjecture implies that the dual code $C = D^\perp$ of D always contains a subcode isomorphic to $d(E_{8k})$, where E_{8k} is the subcode of $\mathbb{Z}_2^{8k}$ which consists of all even words.

Therefore, there are two kinds of structure codes (C, D) with $C = D^\perp$.

1. C contains a subcode isomorphic to $d(\mathbb{Z}_2^{8k})$. In this case, V contains a subalgebra isomorphic to $V_{\sqrt{2}A_1}^{8k}$ and V is a lattice VOA associated with a unimodular lattice.

2. C contains a subcode isomorphic to $d(E_{8k})$ but does not have a subcode isomorphic to $d(\mathbb{Z}_2^{8k})$. Then V is isomorphic to a $\mathbb{Z}_2$-orbifold of a lattice VOA.

When $k = 1$, the only holomorphic framed VOA is V_{E_8}. There are five possible tribly even codes (up to isomorphisms). All of them are subcodes of $RM(1,4)$.

Theorem (Griess-Höhn) There are exactly 5 Virasoro frames in V_{E_8} (up to the action of V_{E_8}). They can be characterized by the dimension k of the code D. Moreover, the frame stablizer G has the shape

1. If $k = 1$, then $G \cong 2^{1+14}Sym_{16}$.
2. If $k = 2$, then $G \cong 2^{2+12}[Sym_8 \wr 2]$
3. If $k = 3$, then $G \cong 2^{4+16}[Sym_3 \wr Sym_4]$
4. If $k = 4$, then $G \cong 2^{4+5}[2 \wr AGL(3,2)]$
5. If $k = 5$, then $G \cong 2^5 AGL(4,2)$.

When $k = 2$, there are 2 holomorphic framed VOA of rank 16, $V_{E_8} \otimes V_{E_8}$ and $V_{D_{16}^+}$.

If $V = V_{E_8} \otimes V_{E_8}$, then the structure codes (C, D) are decomposable, i.e., $C = C_1 \oplus C_2$ and $D = D_1 \oplus D_2$, where $C_1 = D_1^\perp$ and $C_2 = D_2^\perp$.

Theorem: Let D be any triply even codes of length 32 and $(1,\ldots,1) \in D$ and let $C = D^{\perp}$. Then there is a Virasoro frame F of $V_{D_{16}^+}$ such that the structure codes associated with F are (C, D) unless $D =< (1^{16}0^{16}), (0^{16}1^{16}) >$.

Let F be a Virasoro frame of $V = V_{D_{16}^+}$ and (C, D) the structure codes associated with F. Suppose that C contains a subcode K isomorphic to $d(\mathbb{Z}_2^{16})$. Then K determines a subVOA $M_K \cong V_{\sqrt{2}A_1}{}^{\otimes 16}$ in V and gives a selfdual $\mathbb{Z}_4$-codes associated to the coset structure of V/M_K.

Theorem: Let $g \in \mathrm{Aut}C$. Then, g lifts to an automorphism of V if and only if the $\mathbb{Z}_4$-codes associated to V/M_K and $V/M_{g(K)}$ are isomorphic.

Proposition: Let F be a Virasoro frame defined as above and F' another Virasoro frame of V. Suppose that there exits $g \in \mathrm{Aut}(V)$ such that $F' = g(F)$. Then the $\mathbb{Z}_4$-codes associated to V/M_K and $V/g(M_K)$ have the same symmetric weight enumerator.

Mass Formula for Self-Orthogonal Codes over $\mathbf{Z}_{p^2}$

ROWENA ALMA L. BETTY [1]

Graduate School of Information Sciences
Tohoku University
Sendai 980-8579, Japan

AKIHIRO MUNEMASA

Graduate School of Information Sciences
Tohoku University
Sendai 980-8579, Japan

Abstract

In this talk, we establish a mass formula for self-orthogonal codes over $\mathbf{Z}_{p^2}$, where p is a prime. As a consequence, we can also derive the known mass formulas for self-dual codes over $\mathbf{Z}_{p^2}$. We also establish a mass formula for even quaternary codes.

1 Definitions and Preliminaries

Establishing a mass formula for self-orthogonal codes over $\mathbf{Z}_{p^2}$, where p is a prime, means finding a number $M(n)$ such that

$$M(n) = \sum_{C} \frac{|E|}{|\operatorname{Aut} C|}$$

[1]On study leave from the Department of Mathematics, University of the Philippines-Diliman, Quezon City 1101 Philippines

where C runs through the equivalence classes of self-orthogonal codes of length n over $\mathbf{Z}_{p^2}$, E is the full group of all transformations that we allow in defining equivalence for code C, and $\mathrm{Aut}\,C$ is the automorphism group of C. The mass formula gives the total number of distinct self-orthogonal codes. Mass formulas for self-orthogonal p-ary codes, with p an odd prime were given in [4, 5], quaternary self-dual and Type II codes were given in [3], while for odd primes p, a mass formula for self-dual codes over $\mathbf{Z}_{p^2}$ was given in [1, 2].

For a positive integer m, we denote by $\mathbf{Z}_m$ the ring of integers modulo m. A code C of length n over $\mathbf{Z}_m$ is a submodule of $\mathbf{Z}_m^n$. For a matrix $G \in M_{k\times n}(\mathbf{Z})$, we denote by $\mathbf{Z}_m^k G$ the code $\{aG \bmod m \mid a \in \mathbf{Z}^k\}$ of length n over $\mathbf{Z}_m$. A generator matrix of a code C of length n over $\mathbf{Z}_m$ is a matrix $G \in M_{k\times n}(\mathbf{Z})$ such that $C = \mathbf{Z}_m^k G$. Since we deal with codes over $\mathbf{Z}_p$ and $\mathbf{Z}_{p^2}$ at the same time, we adopt this non-standard convention to avoid cumbersome notation.

We denote by $x \cdot y$ the standard inner product of vectors x, y in $\mathbf{Z}_m^n$, and by $C^\perp$ the dual code of a code C over $\mathbf{Z}_m$ with respect to this inner product. A code C is said to be self-orthogonal (respectively self-dual) if $C \subset C^\perp$ (respectively $C = C^\perp$) holds.

Let p be a prime, and consider the exact sequence

$$0 \to \mathbf{Z}_p \xrightarrow{\iota} \mathbf{Z}_{p^2} \xrightarrow{\pi} \mathbf{Z}_p \to 0,$$

where ι is the composition of the isomorphism $\mathbf{Z}_p \to p\mathbf{Z}_{p^2}$ and the embedding $p\mathbf{Z}_{p^2} \to \mathbf{Z}_{p^2}$, and π is the canonical homomorphism. For a positive integer n, by abuse of notation, we denote the cartesian product of the mappings ι and π by the same symbols. For a code C over $\mathbf{Z}_{p^2}$, $\pi(C)$ is called the residue code of C, and $\iota^{-1}(C)$ is called the torsion code of C. Since $\iota \circ \pi = p$, we have $\pi(C) \subset \iota^{-1}(C)$. Moreover, since $\mathrm{Im}\,\iota = \mathrm{Ker}\,\pi$, we have

$$|C| = |\pi(C)||\iota^{-1}(C)|. \tag{1}$$

Note that $C \subset C^\perp$ if and only if $\pi(C) \subset \iota^{-1}(C) \subset \pi(C)^\perp$. Furthermore, when $p = 2$, $\pi(C)$ is doubly-even.

Every code of length n over $\mathbf{Z}_{p^2}$ is equivalent to a code C with generator matrix

$$\begin{bmatrix} I_{k_1} & A \\ 0 & pB \end{bmatrix}$$

where $A \in M_{k_1 \times (n-k_1)}(\mathbf{Z})$, $B \in M_{k_2 \times (n-k_1)}(\mathbf{Z})$. Note that

$$\begin{bmatrix} I_{k_1} & A \end{bmatrix}$$

is a generator matrix of the residue code of C, and

$$\begin{bmatrix} I_{k_1} & A \\ 0 & B \end{bmatrix}$$

is a generator matrix of the torsion code of C. We say that the code C has type $(p^2)^{k_1}p^{k_2}$. Unlike mass formulas for codes over finite fields, our mass formula for self-orthogonal codes over $\mathbf{Z}_{p^2}$ is given as the sum of mass formulas over some finer classes of codes of a given type, where we use the type in place of the dimension for codes over finite fields. The type of a code over $\mathbf{Z}_{p^2}$ is determined by the dimensions of its residue and torsion. We shall determine the number of self-orthogonal codes over $\mathbf{Z}_{p^2}$ with given residue and torsion. We say that the code C is free if $k_2 = 0$, or equivalently, $\pi(C) = \iota^{-1}(C)$.

2 Codes over $\mathbf{Z}_{p^2}$ with prescribed residue and torsion

Let p be a prime, and C_1, C_2 codes of length n over $\mathbf{Z}_p$ such that C_1 has generator matrix

$$\begin{bmatrix} I & A \end{bmatrix}, \tag{2}$$

C_2 has generator matrix

$$\begin{bmatrix} I & A \\ 0 & B \end{bmatrix}, \tag{3}$$

$A \in M_{k_1 \times (n-k_1)}(\mathbf{Z})$, $B \in M_{k_2 \times (n-k_1)}(\mathbf{Z})$ and $\dim C_1 = k_1$, $\dim C_2 = k_1 + k_2$.

Lemma 2.1. *If C is a code of length n over $\mathbf{Z}_{p^2}$ satisfying $\pi(C) = C_1$ and $\iota^{-1}(C) = C_2$, then there exists a matrix $N \in M_{k_1 \times n-k_1}(\mathbf{Z})$ such that*

$$\begin{bmatrix} I & A + pN \\ 0 & pB \end{bmatrix}$$

is a generator matrix of C. Moreover, if $k_2 = 0$, that is, $\pi(C) = \iota^{-1}(C) = C_1$, such a matrix N is unique modulo p.

For the remainder of this section, we assume $C_1 \subset C_2 \subset C_1^{\perp}$. This implies

$$I + AA^t \equiv 0 \pmod{p} \tag{4}$$

and

$$AB^t \equiv 0 \pmod{p}. \tag{5}$$

Moreover, when $p = 2$, we further assume C_1 to be doubly even, or equivalently,

$$\mathrm{diag}(I + AA^t) \equiv 0 \pmod{4}. \tag{6}$$

Lemma 2.2. *The number of free self-orthogonal codes $C \subseteq \mathbf{Z}_{p^2}^n$ such that $\pi(C) = \iota^{-1}(C) = C_1$ is $p^{k_1(2n-3k_1-1)/2}$ for odd primes p and $2^{k_1(2n-3k_1+1)/2}$ for $p = 2$.*

These results were obtained by counting N such that

$$I + AA^t + p(AN^t + NA^t) \equiv 0 \pmod{p^2}.$$

Let us consider sets

$$X = \{C \mid C \text{ is self-orthogonal, } \pi(C) = \iota^{-1}(C) = C_1\} \text{ and}$$
$$X' = \{C' \mid C' \text{ is self-orthogonal, } \pi(C') = C_1, \iota^{-1}(C') = C_2\}.$$

By Lemma 2.2, we have $|X| = p^{k_1(2n-3k_1-1)/2}$ if p is odd and $|X| = 2^{k_1(2n-3k_1+1)/2}$ if $p = 2$. To obtain $|X'|$, we need the following lemmas.

Lemma 2.3. *If $C \in X$, then there exists a unique $C' \in X'$ containing C.*

Lemma 2.4. *Let $C' \in X'$. Then $|\{C \in X \mid C \subset C'\}| = p^{k_1 k_2}$.*

Theorem 2.5. *Let C_1 and C_2 be codes of length n over $\mathbf{Z}_p$ where $C_1 \subset C_2 \subset C_1^{\perp}$. Assume further that C_1 is doubly even when $p = 2$. If $\dim C_1 = k_1$, $\dim C_2 = k_1 + k_2$, then*

$$|X'| = \begin{cases} p^{k_1(2n-3k_1-1-2k_2)/2} & \text{for odd primes } p, \\ 2^{k_1(2n-3k_1+1-2k_2)/2} & \text{for } p = 2. \end{cases}$$

3 Main Results

Let $\sigma(n, k_1)$ denote the number of distinct doubly even binary codes of length n and dimension k_1, and let $\sigma_p(n, k_1)$ be the number of distinct self-orthogonal p-ary codes, with p an odd prime, of length n and dimension k_1. For $k \leq n$, we define the Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_p$ as

$$\begin{bmatrix} n \\ k \end{bmatrix}_p = \frac{(p^n - 1)(p^n - p) \cdots (p^n - p^{k-1})}{(p^k - 1)(p^k - p) \cdots (p^k - p^{k-1})}.$$

Corollary 1. *The number of distinct self-orthogonal codes of length n over $\mathbf{Z}_{p^2}$ of type $(p^2)^{k_1} p^{k_2}$ is*

$$M_{p^2}(k_1, k_2) = \sigma_p(n, k_1) \begin{bmatrix} n - 2k_1 \\ k_2 \end{bmatrix}_p p^{k_1(2n - 3k_1 - 1 - 2k_2)/2}, \tag{7}$$

for odd primes p, and

$$M_4(k_1, k_2) = \sigma(n, k_1) \begin{bmatrix} n - 2k_1 \\ k_2 \end{bmatrix}_2 2^{k_1(2n - 3k_1 + 1 - 2k_2)/2}, \tag{8}$$

for $p = 2$.

Proof. Given a self-orthogonal $[n, k_1]$ code C_1, we have $\begin{bmatrix} n - 2k_1 \\ k_2 \end{bmatrix}_p$ codes C_2 such that $C_1 \subseteq C_2 \subseteq C_1^{\perp}$. The result follows from Theorem 2.5. □

As an example, let $n = 4$, $k_1 = k_2 = 1$, and $p = 3$, C_1, C_2, C_3, C_4 be the self-orthogonal codes over $\mathbf{Z}_9$ of type $9^1 3^1$ with generator matrices

$$\begin{bmatrix} 1 & 1 & 4 & 0 \\ 0 & 3 & 6 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 4 & 3 \\ 0 & 3 & 6 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 4 & 6 \\ 0 & 3 & 6 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 7 & 7 & 0 \\ 0 & 0 & 0 & 3 \end{bmatrix},$$

respectively. Computing the orders of automorphism groups of each code, we have

$$\begin{aligned} \sum_{i=1}^{4} \frac{|E|}{|\operatorname{Aut} C_i|} &= \frac{2^4 4!}{24} + \frac{2^4 4!}{12} + \frac{2^4 4!}{4} + \frac{2^4 4!}{8} \\ &= 16 + 32 + 96 + 48 = 192. \end{aligned}$$

Using Corollary 1, we have

$$M_9(1,1) = \sigma_3(4,1) \begin{bmatrix} 4-2 \\ 1 \end{bmatrix}_3 3^{3-1-1}$$
$$= 16 \cdot 4 \cdot 3 = 192.$$

This implies that $\{C_1, C_2, C_3, C_4\}$ is a complete set of representatives for equivalence classes of self-orthogonal codes of length 4 and type $9^1 3^1$ over $\mathbf{Z}_9$. As a consequence of Corollary 1, we have

Corollary 2. *The number of distinct self-dual codes over $\mathbf{Z}_{p^2}$ of length n is*

$$\sum_{0 \le k_1 \le \lfloor \frac{n}{2} \rfloor} M_{p^2}(k_1, n-2k_1). \tag{9}$$

Corollary 2 agrees with previous known results on the number of distinct self-dual quaternary codes in [3] and the number of distinct self-dual codes over $\mathbf{Z}_{p^2}$, where p is an odd prime in [1], and [2].

4 Even Quaternary Codes

We define the Euclidean weight in $\mathbf{Z}_4$ by $\mathrm{wt}_e(0) = 0$, $\mathrm{wt}_e(1) = \mathrm{wt}_e(3) = 1$ and $\mathrm{wt}_e(2) = 4$. The Euclidean weight of a vector $x = (x_1, \ldots, x_n) \in \mathbf{Z}_4^n$ is defined by $\mathrm{wt}_e(x) = \sum_{i=1}^n \mathrm{wt}_e(x_i)$. A quaternary code is said to be even if the Euclidean weight of every codeword is divisible by 8. Every quaternary even code is self-orthogonal. If a quaternary even code contains a codeword all of whose coordinates are ± 1, then the length is divisible by 8. A quaternary even self-dual code is also called a quaternary Type II code. We are mainly concerned with the enumeration of codes containing the vector $\mathbf{1}$, or codes containing a vector each of whose coordinate is 1 or -1. This restriction forces the length of a code to be a multiple of 8.

First, let us consider such codes containing $\mathbf{1}$. Let $n \in 8\mathbf{Z}$, $1 \le k_1 \le \frac{n}{2}$, C_1, C_2 binary codes of length n such that C_1 is doubly even and has generator matrix

$$\begin{bmatrix} 1 & \mathbf{1} & \mathbf{1} \\ 0 & I_{k_1-1} & A \end{bmatrix}, \tag{10}$$

C_2 has generator matrix

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & I_{k_1-1} & A \\ 0 & 0 & B \end{bmatrix}, \tag{11}$$

$A \in M_{k_1-1\times(n-k_1)}(\mathbf{Z})$, $B \in M_{k_2\times(n-k_1)}(\mathbf{Z})$ and $\dim C_1 = k_1$, $\dim C_2 = k_1 + k_2$. Moreover, we assume that $C_1 \subset C_2 \subset C_1^{\perp}$ and C_1 is doubly even. Then the matrices A and B satisfy (4)–(6). We may assume without lost of generality that the entries of the matrix A are all 0 or 1. Then $1 + 1A^t \equiv 0 \pmod 4$.

Lemma 4.1. *The number of free quaternary even codes C of length n containing* $\mathbf{1}$ *such that $\pi(C) = \iota^{-1}(C) = C_1$ is $2^{(k_1-1)(2n-3k_1-2)/2}$.*

Using this lemma and applying similar methods as in Theorem 2.5, we have

Theorem 4.2. *Let C_1 and C_2 be binary codes of length n where $C_1 \subset C_2 \subset C_1^{\perp}$. If C_1 is doubly even and $\dim C_1 = k_1$ and $\dim C_2 = k_1 + k_2$, then the number of quaternary even codes C*

1. *containing* $\mathbf{1}$ *such that $\pi(C) = C_1$ and $\iota^{-1}(C) = C_2$ is $2^{(k_1-1)(2n-3k_1-2-2k_2)/2}$,*
2. *containing an element of $\{\pm 1\}^n$ such that $\pi(C) = C_1$ and $\iota^{-1}(C) = C_2$ is $2^{(n-k_1)+(k_1-1)(2n-3k_1-2-2k_2)/2}$.*

References

[1] J.M.P. Balmaceda, R.A.L. Betty and F.R. Nemenzo, On the number of distinct self-dual codes over $\mathbf{Z}_9$, Matimyas Matematika 26 (2003), 9-17.

[2] J.M.P. Balmaceda, R.A.L. Betty and F.R. Nemenzo, Mass formula for self-dual codes over $\mathbf{Z}_{p^2}$, Discrete Math., to appear.

[3] P. Gaborit, Mass formulas for self-dual codes over $\mathbf{Z}_4$ and $\mathbf{F}_q + u\mathbf{F}_q$ rings, IEEE Trans. Inform. Theory, 42 (1996), 1222–1228.

[4] V.S. Pless, The number of isotropic subspaces in a finite geometry, Atti. Accad. Naz. Lincei Rendic39 (1965) 418-421.

[5] V.S. Pless, On the uniqueness of the Golay codes, *J. Combin. Theory* 5 (1968) 215-228.

A partial generalization of the Livingstone-Wagner theorem

Yasuhiro Nakashima

Abstract

For a transitive permutation group G on a finite set Ω, the Livingstone–Wagner Theorem states that if G is k-homogeneous then G is $(k-1)$-transitive. It can be conjectured that the number of G-orbits on k-subsets of Ω is greater than or equal to the one on ordered $(k-1)$-tuples of Ω, if $|\Omega|$ is sufficiently large. For the simplest case $k=3$, we prove this by establishing a result on edge-colorings of complete digraphs.

1 Introduction

Let G be a permutation group on a finite set Ω. Denote by $G\backslash\Omega$ the set of G-orbits on Ω. Let $\Omega_{(k)}, \Omega_{[l]}$ denote the family of all k-subsets of Ω, the family of all l-tuples of distinct elements of Ω, respectively. The group G is said to be k-homogeneous, l-transitive, if G acts transitively on $\Omega_{(k)}$, $\Omega_{[l]}$, respectively.

Livingstone and Wagner [2, Theorem 1,2] showed that for any group G acting on Ω,

1. $|G\backslash\Omega_{(k)}|$ is greater than or equal to $|G\backslash\Omega_{(k-1)}|$, hence in particular k-homogeneity implies also $(k-1)$-homogeneity.

2. If G is k-homogeneous then G is $(k-1)$-transitive.

3. For $k \geq 5$, if G is k-homogeneous then G is k-transitive.

Martin and Sagan [1, Theorem 2] generalized (1) by introducing the concept of λ-transitivity as follows. Let S_λ be the set of all partitions of Ω of shape λ. If a permutation group G on Ω acts transitively on S_λ, then G is said to be λ-transitive. Let $\trianglelefteq$ denote the dominance order on the set of partitions of $|\Omega|$. Martin and Sagan proved that $\lambda \trianglelefteq \mu$ implies $|G\backslash S_\lambda| \geq |G\backslash S_\mu|$, in particular λ-transitivity implies also μ-transitivity. Let us consider a natural extension problem of (2), that is, for an integer k, whether $|G\backslash\Omega_{(k)}| \geq |G\backslash\Omega_{[k-1]}|$ holds. Since $|\Omega_{(k)}| \geq |\Omega_{[k-1]}|$ holds when $|\Omega|$ is large enough, one may expect this to be true for $|\Omega|$ sufficiently large. By the definition, $\Omega_{(k)}$, $\Omega_{[k-1]}$ are identified with $S_{[|\Omega|-k,k]}$, $S_{[|\Omega|-k+1,1^{k-1}]}$ as G-sets, respectively. Since $[|\Omega|-k,k]$ and $[|\Omega|-k+1,1^{k-1}]$ are incomparable with respect to the dominance order, the result of [1] does not apply. For the simplest case $k=3$, we prove $|G\backslash\Omega_{(3)}| \geq$

$|G\backslash\Omega_{[2]}|$ provided $|\Omega| \geq 11$, by counting certain configurations in a regular edge-coloring of a complete digraph, the definition of which is given in the next section. Here we only note that every transitive permutation group G on Ω induces a regular edge-coloring (Ω, C, ϕ, Ψ), and the number $|\Omega_{(3)}/\sim|$ of equivalence classes is at least $|G\backslash\Omega_{(3)}|$. There are regular edge-coloring which are not induced by transitive permutation groups (see Example 3.3). We prove the following in section 3.

Theorem 1.1. *Let (Ω, C, ϕ, Ψ) be a regular edge-coloring. If $|\Omega| \geq 11$ then $|\Omega_{(3)}/\sim| \geq |C|$ unless the coloring is the one given in Example 3.3.*

Corollary 1.2. *For any transitive permutation group G on Ω with $|\Omega| \geq 11$, $|G\backslash\Omega_{(3)}| \geq |G\backslash\Omega_{[2]}|$ holds.*

For some permutation groups of degree less than 11, Corollary 1.2 fails to hold. In fact, the counterexamples are C_6, $C_3 \rtimes S_2$, $C_3 \wr S_2$, of degree 6, C_7 of degree 7, $C_4 \wr S_2$ of degree 8, and $C_5 \wr S_2$ of degree 10.

2 Preliminaries

Let Ω, C be finite sets, and $\phi : \Omega_{[2]} \to C$ be a surjective mapping. We call (Ω, C, ϕ, Ψ) a regular edge-coloring if

(R1) For each $c \in C$, the color valency δ_c is independent of points:

$$\forall\alpha \in \Omega,\ \sharp\{\beta \in \Omega \mid \phi(\alpha, \beta) = c\} = \delta_c.$$

(R2) There is a bijective mapping $\Psi : C \to C$, which maps a color of an edge to that of its opposite:

$$\forall(\alpha, \beta) \in \Omega_{[2]},\ (\Psi \circ \phi)(\alpha, \beta) = \phi(\beta, \alpha).$$

Let G be a transitive permutation group on Ω. Then we obtain a regular edge-coloring induced by G, denoted (Ω, C, ϕ, Ψ), as follows. Let $C = G\backslash\Omega_{[2]}$, and define $\phi : \Omega_{[2]} \to C$ by $\phi(\alpha, \beta) = G(\alpha, \beta)$ for $(\alpha, \beta) \in \Omega_{[2]}$, where $G(\alpha, \beta)$ denotes the G-orbit of (α, β). Define Ψ by $\Psi(\phi(\alpha, \beta)) = \phi(\beta, \alpha)$. Then (R2) holds, and by transitivity of G, (R1) holds. Thus (Ω, C, ϕ, Ψ) is a regular edge-coloring.

For the remainder of this section, we assume that a regular edge-coloring (Ω, C, ϕ, Ψ) is given. We define an equivalence relation on $\Omega_{(3)}$ as follows. For $A, B \in \Omega_{(3)}$ we write $A \sim B$ if there exists a bijection π from A to B such that $\phi(\pi(\alpha), \pi(\alpha')) = \phi(\alpha, \alpha')$ for any distinct $\alpha, \alpha' \in A$. Let $[A]$ denote the equivalence class of A. For $a, b, c \in C$ we define $[a, b, c] = \{\{\alpha, \beta, \gamma\} \in \Omega_{(3)} \mid \phi(\alpha, \beta) = a,\ \phi(\beta, \gamma) = b,\ \phi(\gamma, \alpha) = c\}$. This set becomes an equivalence class, unless it is empty. By the definition, every equivalence class is of this form. For $c, d \in C$, let us define a set $T_{c,d}$ by

$$T_{c,d} = \Big\{\{\alpha, \beta, \gamma\} \in \Omega_{(3)} \mid \phi(\alpha, \beta) = c,\ \phi(\alpha, \gamma) = d\Big\}.$$

It is easy to see that $T_{c,d} = T_{d,c} = \bigcup_{x \in C}[c, x, \Psi(d)]$.

Lemma 2.1. *For $a, b, c, d, e \in C$ with $[a, b, c] \neq \varnothing$, we have*

$$[a, b, c] \subset T_{d,e} \iff \{d, e\} \in \Big\{\{a, \Psi(c)\}, \{b, \Psi(a)\}, \{c, \Psi(b)\}\Big\}.$$

For $\mathcal{D} \subset C$ let us define $f(\mathcal{D})$ and $\Delta(\mathcal{D})$ by $f(\mathcal{D}) = 2 + 2\sum_{d \in \mathcal{D}} \delta_d$ and $\Delta(\mathcal{D}) = \bigcup_{x,y,z \in C \setminus \mathcal{D}} [x, y, z]$.

Lemma 2.2. *Let $\mathcal{D} \subset C$. If $f(\mathcal{D}) < |\Omega|$, then for any $c \in C$ there exist $d, e \in C \setminus \mathcal{D}$ such that $[c, d, \Psi(e)] \neq \varnothing$. If moreover $\mathcal{D} = \Psi(\mathcal{D})$, then $\Delta(\mathcal{D}) \neq \varnothing$.*

Lemma 2.3. *For distinct $\{a, b\}, \{c, d\} \in C_{(1)} \cup C_{(2)}$, we have*

$$\{\Psi(a), \Psi(b)\} \cap \{c, d\} = \varnothing \Longrightarrow T_{a,b} \cap T_{c,d} = \varnothing.$$

Lemma 2.4. *Let $\{c_1, d_1\}, \ldots, \{c_s, d_s\} \in C_{(1)} \cup C_{(2)}$ be distinct, and assume $T_{c_i,d_i} \neq \varnothing$ for all i. Then we have*

$$\left| \bigcup_{1 \leq i \leq s} T_{c_i,d_i} / \sim \right| \geq \left\lceil \frac{s}{3} \right\rceil.$$

Lemma 2.5. *If $|\Omega| \geq 8$ and $|C| \geq 6$, then $|\Omega_{(3)}/\sim| \geq |C|$ holds.*

3 Proof of the main result

Let a regular edge-coloring (Ω, C, ϕ, Ψ) be given. We define subsets $\mathcal{K}, \mathcal{L}$ of C by

$$\mathcal{K} = \{c \in C \mid \Psi(c) \neq c\}, \ \mathcal{L} = \{c \in C \mid \Psi(c) = c\}.$$

Lemma 3.1. *If $|\Omega| \geq 11$ and $\mathcal{L} = \varnothing$, then $|\Omega_{(3)}/\sim| \geq |C|$.*

Lemma 3.2. *If $|\Omega| \geq 11$ and $\mathcal{K} = \varnothing$, then $|\Omega_{(3)}/\sim| \geq |C|$.*

Proof of Theorem 1.1. By Lemmas 2.5, 3.1 and 3.2 we only need to treat the cases $(k, l, |C|) = (1, 1, 3), (1, 2, 4), (1, 3, 5), (2, 1, 5)$. We omit the details. □

Example 3.3. Let $t \geq 3$ be an integer, $\Omega = \{\alpha_1, \beta_1, \ldots, \alpha_t, \beta_t\}$, $C = \{\overrightarrow{1}, \overleftarrow{1}, 1\}$, $\Psi(\overrightarrow{1}) = \overleftarrow{1}$, $\Psi(\overleftarrow{1}) = \overrightarrow{1}$, $\Psi(1) = 1$. Consider the regular edge-coloring (Ω, C, ϕ, Ψ) defined by $\Omega = \{\alpha_1, \beta_1, \ldots, \alpha_t, \beta_t\}$, $C = \{\overrightarrow{1}, \overleftarrow{1}, 1\}$, and for $1 \leq i < j \leq t$, $\phi(\alpha_i, \beta_i) = \phi(\beta_i, \alpha_i) = 1$, $\phi(\alpha_j, \alpha_i) = \phi(\beta_j, \beta_i) = \phi(\alpha_i, \beta_j) = \phi(\beta_i, \alpha_j) = \overrightarrow{1}$, $\phi(\alpha_i, \alpha_j) = \phi(\beta_i, \beta_j) = \phi(\alpha_j, \beta_i) = \phi(\beta_j, \alpha_i) = \overrightarrow{1}$ (see Figure 1). Then $\Omega_{(3)}/\sim = \{1, \overrightarrow{1}, \overrightarrow{1}\}, \{\overrightarrow{1}, \overrightarrow{1}, \overleftarrow{1}\}$, and so $|\Omega_{(3)}/\sim| = 2 < 3 = |C|$.

Proposition 3.4. *The regular edge-coloring given in Example 3.3 cannot be induced by a transitive permutation group on Ω.*

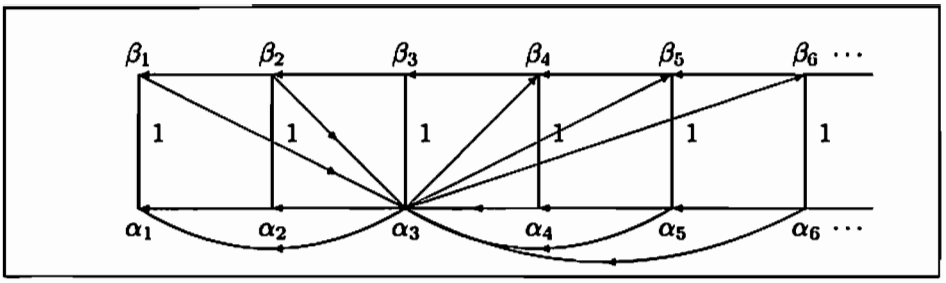


Figure 1: Exceptional example

Proof. Let $(\Omega, \mathcal{C}, \phi, \Psi)$ be as in Example 3.3, and suppose that $(\Omega, \mathcal{C}, \phi, \Psi)$ is induced by a transitive permutation group G on Ω. Let α_1, α_2, $\alpha_3 \in \Omega$ be as in Figure 1. Since $\phi(\alpha_2, \alpha_1) = \phi(\alpha_3, \alpha_1) = \overrightarrow{1}$, there exists $g \in G$ such that $g(\alpha_3, \alpha_1) = (\alpha_2, \alpha_1)$. Since $\phi(g(\alpha_2), \alpha_1) = \phi(g(\alpha_2), g(\alpha_1)) = \phi(\alpha_2, \alpha_1) = \overrightarrow{1}$, we have $g(\alpha_2) \in \{\alpha_3, \ldots, \alpha_t\}$. But then $\overrightarrow{1} = \phi(g(\alpha_2), \alpha_2) = \phi(g(\alpha_2), g(\alpha_3)) = \phi(\alpha_2, \alpha_3) = \overleftarrow{1}$. This is a contradiction. □

Proof of Corollary 1.2. Let $(\Omega, \mathcal{C}, \phi, \Psi)$ be the regular edge-coloring induced by G. By the definition of induced regular edge-coloring, $|\mathcal{C}| = |G\backslash\Omega_{[2]}|$ holds. For $A, B \in \Omega_{(3)}$, if $g(A) = B$ for some $g \in G$, then $[A] = [B]$, hence $|\Omega_{(3)}/\sim| \leq |G\backslash\Omega_{(3)}|$ holds. Therefore, the assertion follows from Theorem 1.1 and Proposition 3.4. □

Acknowledgment The author would like to thank his supervisor Akihiro Munemasa for valuable suggestions and comments.

References

[1] W. J. Martin and B. E. Sagan, A new notion of transitivity for groups and sets of permutations, J. London Math. Soc. (2) 73 (2006) 1–13.

[2] D. Livingstone and A. Wagner, Transitivity of finite permutation groups on unordered sets, Math. Zeitschr. 90 (1965), 393–403.