第30回代数的組合せ論シンポジウム報告集

2013年6月24日－26日

於　静岡大学・浜松キャンパス（佐鳴会館・会議室）

平成25年度JSPS科学研究補助金基盤研究(B)

（課題番号　24340002 千葉大学　北詰正顕）

まえがき

この報告集は2013年6月24日から26日にわたり、静岡大学・浜松キャンパス（佐鳴会館会議室）で行われた「第30回代数的組合せ論シンポジウム」の講演記録です。約50名の参加者により行われました。

本研究集会の報告集の作成、講演者の旅費および会議費を、平成25年度JSPS科学研究補助金

基盤研究（B）研究代表者：宮本雅彦（課題番号：22340002）
基盤研究（B）研究代表者：原田昌晃（課題番号：23340021）
基盤研究（B）研究代表者：北詰正顕（課題番号：24340002）

より援助をいただきましたので、お礼を申し上げます。

浜松市に関するパンフレットを浜松観光コンベンションビューローより提供していただきました。講演者、参加者の方々、会場準備を手伝ってくれた静岡大学情報学部・大学院情報学研究科の学生達、この研究集会に関係する皆様にここに改めてお礼を申し上げます。

2013年10月

北詰正顕（千葉大学）
原田昌晃（東北大学）
新谷　誠（静岡大学）

第３０回代数的組合せ論シンポジウム

世話人：北詰 正顕 (千葉大)
原田 昌晃 (山形大)
新谷　誠 (静岡大)

日程：２０１３年6月２４日(月)～２６日(水)
会場：静岡大学・浜松キャンパス（佐鳴会館・会議室）
住所：浜松市中区城北３－５－１
（ＪＲ東海・浜松駅からバスで約２０分「静岡大学」下車）

プログラム

6月 24日(月)

10:00-10:50 澤辺 正人（千葉大・教育学部）
有限群の Up-Down パスから得られる単体複体について

11:00-11:50 田中 康彦（大分大・工学部）
実例に見る quasithin 群の影のふるまい

12:00-12:30 藤田 亮介（獨協医科大）
On the finite space with a finite group action

14:00-14:50 島倉 裕樹（東北大・情報科学研究科）
Z_3 軌道体構成法と中心電荷 24 の正則頂点作用素代数

15:00-15:30 三枝崎 剛（山形大・地域教育文化学部）
The McKay-Thompson series of Mathieu Moonshine modulo two

15:50-16:20 入江 佑樹（千葉大・理学研究科）
Ternary Golay code が必勝形となる九つのゲーム

16:30-17:00 山口 正男（筑波大・数理物質科学研究科）
多重 p-角形の置換群について

6月 25日(火)

10:00-10:30 小林 みどり（静岡県立大・経営情報学部）
Dudeney の円卓問題

10:40-11:10 平峰 豊（熊本大・教育学部）
A construction of difference matrices using functions from $GF(q)$ to $GF(q)^*$ (joint work with C. Suetake)

11:20-11:50 谷口 浩朗（香川高専）
d-dimensional symmetric bilinear dual hyperovals in $V(((1/r)d^2+3d+2)/2,2)$ with $r>1$

12:00-12:30 中空 大幸（岡山大・自然科学研究科）
Extremal binary doubly even self-dual code から得られる t-design について

14:00–14:50 城本 啓介（熊本大・自然科学研究科）
The critical problem in coding theory
15:00–15:30 佐藤 重吾（金沢大・自然科学研究科）
TD-pairs of shape $1, 2, 2, \ldots, 2, 2, 1$ at $q = 1$
15:50–16:40 栗林 勝彦（信州大・理学部）
アソシエーションスキームの圏論的一般化について – スキーモイドとその圏 –
16:50–17:20 Gary Greaves（東北大・情報科学研究科）
On limit points of the least eigenvalue of a graph

18:00–20:00　懇親会（静岡大学生協北館食堂 1 階）

6 月 26 日 (水)
10:00–10:50 宗政 昭弘（東北大・情報科学研究科）
Complex Hadamard matrices and 3-class association schemes
11:00–11:50 Ferenc Szöllősi（東北大・情報科学研究科）
Equiangular lines and Seidel matrices with 3 different eigenvalues
(joint work with Gary Greaves)
12:00–12:30 谷口 哲至（松江高専）
Hoffman graphs and edge-signed graphs
14:00–14:50 田中 太初（東北大・情報科学研究科）
A cross-intersection theorem for vector spaces based on semidefinite programming
15:00–15:30 須田 庄（愛知教育大）
Weighing matrix と球面上のデザイン，アソシエーションスキームについて

目　次

有限群の Up-Down パスから得られる単体複体について

−共同研究：山口大学 飯寄信保 氏−

千葉大学（教育） 澤辺正人

1 はじめに

この報告文の概略は次の通りである。まず今回の話の背景を簡単に説明する。次に講演題目は “有限群の” Up-Down パスとなっているが、実際の設定は全て quiver 上で成されている。群はその具体例として存在する。つまり Up-Down パスは quiver 上で定義される対象であり、それを用いてパス複体というものを新たに導入する。パス複体はいわゆる部分群複体の概念を含んでおり、そのことを解説する。さらに部分群およびコセットから定義されるパス複体の連結性に関する結果を紹介する。本研究の全体については [1] を参照されたい。

■これまでのアイデアと今回の方向性 有限群 G に対して $\mathrm{Sgp}(G)$ を G の部分群全体とする。部分群族 $\mathfrak{X} \subseteq \mathrm{Sgp}(G)$ を通常の包含関係 $\leq$ と共に半順序集合 (poset) と見なす。このとき $(\mathfrak{X}, \leq)$ の順序複体を $\Delta(\mathfrak{X}) = \Delta(\mathfrak{X}, \leq)$ と表し、これを G の部分群複体と呼ぶ。即ち $\mathfrak{X}$ に属する部分群から成る包含列 $(H_0 > H_1 > \cdots > H_m)$ $(H_i \in \mathfrak{X})$ を単体とする有限抽象単体複体のことである。この様に部分群複体は部分群族 $\mathfrak{X} \subseteq \mathrm{Sgp}(G)$ を取るごとに定義される対象である。

今回の共同研究の発端は、部分群複体 $\Delta(\mathfrak{X})$ 或いは部分群束 $(\mathrm{Sgp}(G), \leq)$ をもっと良く知るために poset の表現論から何か新しい事が出来ないかということで始まった。これまでのアイデアは、まず poset $(\mathcal{P}, \leq)$ を自然に quiver $Q_{\mathcal{P}} = Q_{(\mathcal{P}, \leq)}$ と見なす。即ち頂点集合を $(Q_{\mathcal{P}})_0 := \mathcal{P}$ として要素 $a, b \in \mathcal{P}$ に対して $a > b$ なるとき矢印 $(a \to b)$ を定義する。$(Q_{\mathcal{P}})_1$ を矢印全体の集合とする。さらに写像 $s, r : (Q_{\mathcal{P}})_1 \longrightarrow (Q_{\mathcal{P}})_0$ を矢印 $\alpha = (a \to b) \in (Q_{\mathcal{P}})_1$ に対して $s(\alpha) := a \in \mathcal{P}$ および $r(\alpha) := b \in \mathcal{P}$ と定めることにより 4 つ組

$$Q_{\mathcal{P}} := \left((Q_{\mathcal{P}})_0, (Q_{\mathcal{P}})_1, s, r \right)$$

は quiver を成す。quiver $Q_{\mathcal{P}}$ があれば付随するパス代数 $RQ_{\mathcal{P}}$ が定義される。そこである $RQ_{\mathcal{P}}$-加群 M を構成し、さらにその自己準同型環の中から UD-代数 $\mathrm{UD}(Q_{\mathcal{P}}, w_{\mathcal{P}}; R) \subseteq \mathrm{End}(M)$ というものを新たに導入した。$w_{\mathcal{P}}$ は矢印上の重み関数である。そしてその代数構造と元の群 G との関係などを考察した。詳しくは [2, 3] を参照されたい。そこで今回はこの quiver $Q_{\mathcal{P}}$ から、パス代数へではなく、単体複体へ向かうルートを新たに開拓したということである。

■部分群 quiver とコセット quiver 有限群 G に付随する quiver を 2 つ導入する。まず $\mathrm{Coset}(G) := \bigcup_{L \in \mathrm{Sgp}(G)} G/L$ と定める。即ち L が G の部分群を全て動くときの左コセット $gL \in G/L$ 全体から成る集合を考える。これは通常の包含関係 $\subseteq$ と共に poset を与える。そこで部分群束 $(\mathrm{Sgp(G)}, \leq)$ と $(\mathrm{Coset}(G), \subseteq)$ に付随する quiver をそれぞれ

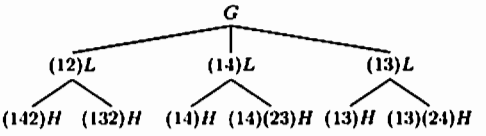
$$Q_G := Q_{(\mathrm{Sgp(G)}, \leq)}, \quad Q_{CG} := Q_{(\mathrm{Coset}(G), \subseteq)}$$

で表し G の**部分群 quiver** および**コセット quiver** と呼ぶことにする。ここで Q_G は Q_{CG} に含まれていることに注意する。一方、写像

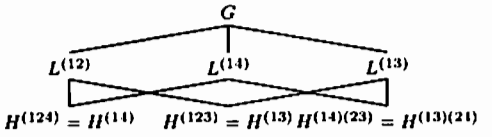
$$\varphi_G : \mathrm{Coset}(G) \longrightarrow \mathrm{Sgp}(G);\ gL \mapsto L^{g^{-1}}$$

1

を考えることにより Q_G は Q_{CG} を φ_G に従って貼り合わせることで実現される。具体的な状況を観察する。G を 4 次対称群 $\mathrm{Sym}(\{1,2,3,4\})$ としその部分群 $H := \mathrm{Sym}(\{3,4\}) < L := \mathrm{Sym}(\{2,3,4\}) < G$ を取る。このとき次は poset $(\mathrm{Coset}(G), \subseteq)$ の一部を描いたものである。



同時に上から下へ矢印を付けることによって quiver Q_{CG} を考えている。これを φ_G で移すと次の様になる。



これは部分群束 $(\mathrm{Sgp}(G), \leq)$ 或いは quiver Q_G の一部を与えている。以上のことから Q_G 或いは部分群束 $(\mathrm{Sgp}(G), \leq)$ （より一般には部分群複体）を単に眺めているよりも、張り合わせの情報を入れながら Q_{CG} 或いは poset $(\mathrm{Coset}(G), \subseteq)$ を考察することは有益であると思われる。さらにコセットから得られる自然な置換表現の情報も部分群複体等に引き戻せると思われる。いずれにしても、部分群だけでは無くコセットも重要な研究対象となる。

2 パス複体

以下 $Q = (Q_0, Q_1, (s : Q_1 \to Q_0), (r : Q_1 \to Q_0))$ を quiver とする。

2.1 Up-Down パス

各矢印 $\alpha = (a \to b) \in Q_1$ に対して記号 ${}^t\alpha$ を用意する。${}^t\alpha$ 全体の集合を $Q_1^{\mathrm{opp}} := \{{}^t\alpha \mid \alpha \in Q_1\}$ で表す。さらに元々の矢印と ${}^t\alpha$ 全体からなる集合を $Q_1^{\mathrm{ud}} := Q_1 \cup Q_1^{\mathrm{opp}}$ で表す。ここで s, r を Q_1^{ud} 上に拡張する。即ち $\alpha = (a \to b) \in Q_1$ に対して $s({}^t\alpha) := r(\alpha) = b$ および $r({}^t\alpha) := s(\alpha) = a$ と定める。つまり矢印で表せば ${}^t\alpha = (b \to a)$ ということになる。このとき 4 つ組

$$Q^{\mathrm{ud}} := \Big(Q_0,\ Q_1^{\mathrm{ud}},\ (s : Q_1^{\mathrm{ud}} \to Q_0),\ (r : Q_1^{\mathrm{ud}} \to Q_0) \Big)$$

は quiver を成す。$\mathsf{P}(Q^{\mathrm{ud}})$ で Q^{ud} のパス全体を表す。パスとは結合可能な矢印の列のことである。

定義 上記の記号の下で パス $\Delta \in \mathsf{P}(Q^{\mathrm{ud}})$ を Q の **Up-Down パス**（UD-パス）と呼ぶ。

先程の例で言えば、単に Q_{CG} では上から下に伸びる包含列のみがパスとなる。ところが Q_{CG}^{ud} においては $\big((142)H < (12)L < G > (13)L > (13)(24)H \big)$ などもパス（Q_{CG} の UD-パス）として考察出来るようになる。

2.2 パス複体

Q のパス $\Delta = (a_0 \to \cdots \to a_k) \in \mathsf{P}(Q)$ に対して $\mathsf{Ob}(\Delta) := \{a_0, \ldots, a_k\}$ を Δ を構成する頂点全体の集合とする。更にパスの族 $\mathcal{H} \subseteq \mathsf{P}(Q)$ を取る。このとき $\mathcal{H}$ に属するパス $\Delta \in \mathcal{H}$ に対してその

2

$\mathsf{Ob}(\Delta)$ の空でない部分集合を単体とするような単体複体を $\mathrm{T}_Q(\mathcal{H})$ で表す。つまり正確には次の様になる。

定義 上記の記号の下で

$$\bigcup_{\Delta\in\mathcal{H}}\mathsf{Ob}(\Delta)\subseteq Q_0,\quad \bigcup_{\Delta\in\mathcal{H}}\left(2^{\mathsf{Ob}(\Delta)}\setminus\{\emptyset\}\right)$$

をそれぞれ頂点集合および単体の集合として定義される単体複体を $\mathrm{T}_Q(\mathcal{H})$ で表す。これを $\mathcal{H}$ の Q に於ける**パス複体**と呼ぶ。

特に部分群 quiver Q_G の UD-パスの族 $\mathcal{H}\subseteq\mathsf{P}(Q_G^{\mathrm{ud}})$ に対してそのパス複体 $\mathrm{T}_{Q_G^{\mathrm{ud}}}(\mathcal{H})$ を改めて G の**部分群複体**と呼ぶことにする。つまり部分群の UD-パス上に乗っている部分群の subfamily を単体とする単体複体である。同様にコセット quiver Q_{CG} の UD-パスの族 $\mathcal{K}\subseteq\mathsf{P}(Q_{CG}^{\mathrm{ud}})$ に対してそのパス複体 $\mathrm{T}_{Q_{CG}^{\mathrm{ud}}}(\mathcal{K})$ を**コセット複体**と呼ぶことにする。さらに $\mathcal{K}\subseteq\mathsf{P}(Q_{CG}^{\mathrm{ud}})$ を上手く取ると先程の $\varphi_G:\mathrm{Coset}(G)\longrightarrow\mathrm{Sgp}(G)$ は G-複体の間の G-写像

$$\varphi_{G,\mathcal{K}}:\mathrm{T}_{Q_{CG}^{\mathrm{ud}}}(\mathcal{K})\longrightarrow\mathrm{T}_{Q_G^{\mathrm{ud}}}\left(\mathsf{P}(Q_G^{\mathrm{ud}})\right)$$

を誘導する。以上のことを踏まえて今回考察した内容は次の通りである（詳しくは [1] を参照）。

■考察内容（基礎の整備） まずパス複体 $\mathrm{T}_Q(\mathcal{H})$ の一般論としてその可縮性やホモロジー群などを考察した。また具体的な計算をする際にコセット quiver の UD-パスを一般に考えていては手が付かない。そこで部分群の UD-パスの族 $\mathcal{H}\subseteq\mathsf{P}(Q_G^{\mathrm{ud}})$ から得られるコセットの特別な UD-パスの族 $\widetilde{\mathfrak{G}}(\mathcal{H})\subseteq\mathsf{P}(Q_{CG}^{\mathrm{ud}})$ を導入した。しかしながらこの特別なもので本質的に十分ということになる。さらに UD-パスのある族 $\mathcal{K}\subseteq\mathsf{P}(Q_{CG}^{\mathrm{ud}})$ に対するコセット複体 $\mathrm{T}_{Q_{CG}^{\mathrm{ud}}}(\mathcal{K})$ のオイラー標数やホモロジー群の計算を行った。或いはいわゆるコセット幾何とコセット複体との関係についても追求した。またパス複体の連結性についての結果も得た。さらには G-写像 $\varphi_{G,\mathcal{K}}$ の逆像を決定した。これは今後議論するであろう fiber 定理等への応用に備えたものである。

この報告文では特にパス複体といわゆる部分群複体との関連について説明する。さらにパス複体の連結性に関する結果を紹介する。

3 通常の部分群複体との関係

G の部分群族 $\mathfrak{X}\subseteq\mathrm{Sgp}(G)$ を取る。これは部分群 quiver Q_G 或いはその UD-version Q_G^{ud} の頂点の部分集合を与えていることに注意する。ここで Q_G のパスの族を次のように定める。

$$\mathsf{P}(Q_G)\cap\mathfrak{X}:=\{\Delta\in\mathsf{P}(Q_G)\mid\mathsf{Ob}(\Delta)\subseteq\mathfrak{X}\}\subseteq\mathsf{P}(Q_G)$$

即ち上から下へ伸びる部分群の包含列であって、それを構成する部分群が全て $\mathfrak{X}$ に属するというものである。このパスの族から定義されるパス複体を

$$\mathrm{T}_{Q_G}(\mathfrak{X}):=\mathrm{T}_{Q_G}\left(\,\mathsf{P}(Q_G)\cap\mathfrak{X}\,\right)$$

で表す。即ちこれは包含列の部分集合を単体とする複体であることから先に述べた通常の部分群複体 $\Delta(\mathfrak{X})$ を与えていることになる。同様に Q_G^{ud} のパス（Q_G の UD-パス）の族を次のように定める。

$$\mathsf{P}(Q_G^{\mathrm{ud}})\cap\mathfrak{X}:=\{\Delta\in\mathsf{P}(Q_G^{\mathrm{ud}})\mid\mathsf{Ob}(\Delta)\subseteq\mathfrak{X}\}\subseteq\mathsf{P}(Q_G^{\mathrm{ud}})$$

3

即ち Up-Down する部分群の包含列であって、それを構成する部分群が全て $\mathfrak{X}$ に属するというものである。このパスの族から定義されるパス複体を

$$\mathrm{T}_{Q_G^{\mathrm{ud}}}(\mathfrak{X}) := \mathrm{T}_{Q_G^{\mathrm{ud}}}\big(\,\mathsf{P}(Q_G^{\mathrm{ud}}) \cap \mathfrak{X}\,\big)$$

で表す。これは $\mathrm{T}_{Q_G}(\mathfrak{X}) = \Delta(\mathfrak{X})$ を部分複体として含む。よって**我々のパス複体 $\mathrm{T}_Q(\mathcal{H})$ は通常の部分群複体とその拡張を自然に含んでいることになる。**ここで我々の記号を用いると Quillen の定理は次のように述べることが出来る。まず G の位数の素因子 p に対して $\mathcal{S}_p(G)$ を G の非自明な p-部分群全体とする。

命題 (Quillen の定理) $O_p(G) \neq 1$ ならば $\mathrm{T}_{Q_G}\big(\mathcal{S}_p(G)\big) = \Delta\big(\mathcal{S}_p(G)\big)$ は可縮である。

このときこの UD-version が成り立つ。

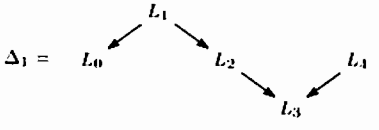
命題 (Quillen の定理の UD-version) $O_p(G) \neq 1$ ならば $\mathrm{T}_{Q_G^{\mathrm{ud}}}\big(\mathcal{S}_p(G)\big)$ は可縮である。

今後の課題の一つとして次を挙げることが出来る。即ち『部分群族 $\mathfrak{X}, \mathfrak{Y} \subseteq \mathrm{Sgp}(G)$ に対して通常の部分群複体 $\Delta(\mathfrak{X})$ と $\Delta(\mathfrak{Y})$ がホモトピー同値ならばその UD-version である $\mathrm{T}_{Q_G^{\mathrm{ud}}}(\mathfrak{X})$ と $\mathrm{T}_{Q_G^{\mathrm{ud}}}(\mathfrak{Y})$ もホモトピー同値になるか？』というものである。これが成立していれば非常に有力な道具となる。

4 複体の連結性

4.1 部分群の UD-パスから得られるコセットの UD-パス

部分群 quiver Q_G の UD-パス $\Delta = (L_0 - \cdots - L_k) \in \mathsf{P}(Q_G^{\mathrm{ud}})$ から得られるコセット quiver Q_{CG} の UD-パス $\Gamma \in Q_{CG}^{\mathrm{ud}}$ を導入する。Δ としては例えば次のような Δ_1 を想定すればよい。



ここで部分群 $L_0, L_1, \ldots, L_k$ の順序に従って対応するコセット $gL_i \in G/L_i$ $(0 \leq i \leq k)$ を繋げていった Q_{CG} の UD-パス全体を $\tilde{\mathfrak{S}}(\Delta)$ で表す。即ち

$$\tilde{\mathfrak{S}}(\Delta) := \big\{\ (X_0 - \cdots - X_k) \mid X_j \in G/L_j\ (0 \leq j \leq k)\ \big\} \subseteq \mathsf{P}(Q_{CG}^{\mathrm{ud}})$$

と定める。例として $\tilde{\mathfrak{S}}(\Delta_1)$ の様子を観察してみる。まず X_0 として任意のコセット $g_0L_0 \in G/L_0$ を取ることが出来る。$X_1 \in G/L_1$ は $X_0 = g_0L_0$ を含むことから $X_1 = g_0L_1$ のように一意的に定まる。次に $X_2 \in G/L_2$ は g_0L_1 に含まれることからその取り方は $|L_1 : L_2|$ 通りだけある。同様に X_2 に対して $X_3 \in G/L_3$ の取り方は $|L_2 : L_3|$ 通りである。さらに X_3 に対してそれを含む $X_4 \in G/L_4$ は一意的に定まる。従って $|\tilde{\mathfrak{S}}(\Delta_1)| = |G : L_0| \times 1 \times |L_1 : L_2| \times |L_2 : L_3| \times 1$ が成り立つ。この様に一般の $\tilde{\mathfrak{S}}(\Delta)$ の濃度も容易に書き上げることが出来る。

ここでコセットの間の包含関係 $aL_1 \subseteq bL_2$ があれば部分群の間の包含関係 $L_1 \leq L_2$ が得られることに改めて注意する。これを用いると コセットの UD-パス $\Gamma = (g_0L_0 - \cdots - g_kL_k) \in \mathsf{P}(Q_{CG}^{\mathrm{ud}})$ は部分群の UD-パス $\Delta = (L_0 - \cdots - L_k) \in \mathsf{P}(Q_G^{\mathrm{ud}})$ に対する $\tilde{\mathfrak{S}}(\Delta)$ に含まれる。つまり任意のコセットの UD-パスとして $\tilde{\mathfrak{S}}(\Delta)$ を扱ってよいことになる。

さて UD-パスの族 $\mathcal{D} \subseteq \mathsf{P}(Q_G^{\mathrm{ud}})$ に対して $\tilde{\mathfrak{S}}(\mathcal{D}) := \bigcup_{\Delta \in \mathcal{D}} \tilde{\mathfrak{S}}(\Delta) \subseteq \mathsf{P}(Q_{CG}^{\mathrm{ud}})$ と定義する。

4

4.2 2 つの結果

命題 (Proposition 7.18 in [1]) Q_G に於ける UD-パスの族 $\mathcal{D} \subseteq \mathsf{P}(Q_G^{\mathrm{ud}})$ に対して次は同値である。

(1) $\mathrm{T}_{Q_{CG}^{\mathrm{ud}}}\big(\widetilde{\mathfrak{S}}(\mathcal{D})\big)$ は連結である。
(2) $\mathrm{T}_{Q_G^{\mathrm{ud}}}(\mathcal{D})$ は連結であり、かつ $\big\langle \bigcup_{\Delta\in\mathcal{D}} \mathsf{Ob}(\Delta) \big\rangle = G$ が成り立つ。

■証明の概略 (1) ⇒ (2): 連結性については直ちに導かれる。実際に $\mathcal{D} \subseteq \widetilde{\mathfrak{S}}(\mathcal{D})$ より $\mathrm{K} := \mathrm{T}_{Q_G^{\mathrm{ud}}}(\mathcal{D})$ は $\mathrm{T} := \mathrm{T}_{Q_{CG}^{\mathrm{ud}}}\big(\widetilde{\mathfrak{S}}(\mathcal{D})\big)$ の部分複体である。仮定から T は連結であることから任意の 2 つの部分群はコセットの edge パスで結ばれている。ところがコセットの UD-パスは、前に注意した通り、そのまま部分群の UD-パスに落ちてくる。このことから K の連結性が導かれる。よって問題は G を生成する方となる。以下 $\mathcal{V} := \bigcup_{\Delta\in\mathcal{D}} \mathsf{Ob}(\Delta)$ および $N := \langle \mathcal{V} \rangle \leq G$ と置く。

Step1: コセットの UD-パス $(X_0 - \cdots - X_k) \in \widetilde{\mathfrak{S}}(\mathcal{D})$ を取る。このときある i に対して $X_i \subseteq N$ ならば全ての $0 \leq j \leq k$ に対して $X_j \subseteq N$ が成り立つ。

Step2: $\mathcal{C} \cap \mathcal{V} \neq \emptyset$ なる T の連結成分 $\mathcal{C}$ に対して $X \subseteq N$ $(^\forall X \in \mathcal{C})$ が成り立つ。

実際に $L \in \mathcal{C} \cap \mathcal{V}$ を取ると L と X はコセットの edge パスで結ばれている。ところが L は $\mathcal{V}$ に属している。つまり L は N に含まれていることから Step1 によって L と X を結ぶコセットは全て N に含まれることになる。

$N < G$ と仮定し $yN \cap N = \emptyset$ なる $y \in G$ を取る。Step2 に於ける T の連結成分 $\mathcal{C}$ を取ると Step2 の主張から任意の $X \in \mathcal{C}$ に対して $X \subseteq N$ かつ $yX \subseteq yN$ が成り立つ。即ち $\mathcal{C}$ に属するコセットは N に含まれ、また $y\mathcal{C}$ に属するコセットは yN に含まれる。ところが $yN \cap N = \emptyset$ であることから 2 つの連結成分 $\mathcal{C}$ と $y\mathcal{C}$ も互いに素となる。つまり連結成分が 2 つ以上となり T は非連結となる。これはそもそも T が連結であるという仮定に矛盾する。

(2) ⇒ (1): $\mathcal{V}$ はパス複体 $\mathrm{K} := \mathrm{T}_{Q_G^{\mathrm{ud}}}(\mathcal{D})$ の頂点集合である。さらに仮定から K は連結であり、またパス複体 $\mathrm{T} := \mathrm{T}_{Q_{CG}^{\mathrm{ud}}}\big(\widetilde{\mathfrak{S}}(\mathcal{D})\big)$ の部分複体である。よって $\mathcal{V} \subseteq \mathcal{C}$ なる T の連結成分を取ることが出来る。このとき $G = \langle \mathcal{V} \rangle \leq \mathrm{Stab}_G(\mathcal{C})$ を示す。すると $\mathcal{V}$ に属するコセットに G の要素を左から掛けたものが全て $\mathcal{C}$ に入る。従って $\mathcal{C}$ は T の頂点集合を含むことになり T の連結性が導かれる。□

前の命題では Q_G に於ける UD-パスの族 $\mathcal{D} \subseteq \mathsf{P}(Q_G^{\mathrm{ud}})$ を扱った。最後にこの特別な場合として一本の UD-パス $\Delta \in \mathsf{P}(Q_G^{\mathrm{ud}})$ を考える。

定理 (Theorem 7.20 in [1]) Q_G に於ける UD-パス $\Delta = (L_0 - \cdots - L_k) \in \mathsf{P}(Q_G^{\mathrm{ud}})$ に対して $\mathrm{T}_{Q_{CG}^{\mathrm{ud}}}\big(\widetilde{\mathfrak{S}}(\Delta)\big)$ の連結成分の個数は指数 $|G : H|$ で与えられる。ここで $H := \big\langle \mathsf{Ob}(\Delta) \big\rangle \leq G$ とする。

■証明の概略 まず $\mathsf{Ob}(\Delta) = \{L_0, \ldots, L_k\}$ は $\Delta \in \mathsf{P}(Q_G^{\mathrm{ud}}) \subseteq \mathsf{P}(Q_{CG}^{\mathrm{ud}})$ に沿って全て結ばれている。従って $\mathsf{Ob}(\Delta)$ は $\mathrm{T} := \mathrm{T}_{Q_{CG}^{\mathrm{ud}}}\big(\widetilde{\mathfrak{S}}(\Delta)\big)$ 内で連結である。即ち $\mathsf{Ob}(\Delta) \subseteq \mathcal{C}$ なる T の連結成分 $\mathcal{C}$ が存在する。ここで T の任意の頂点は $gL_i \in G/L_i \subseteq \bigcup_{i=0}^{k} G/L_i$ なる形をしている。さらに頂点 gL_i は連結成分 $g\mathcal{C}$ に含まれている。これは G が T の連結成分全体の上に可移に作用していることを表している。従って証明は $\mathrm{Stab}_G(\mathcal{C}) = H$ を示すことに帰着される。特に議論が必要な部分は $\mathrm{Stab}_G(\mathcal{C}) \leq H$ である。これを示すためには $\widetilde{\mathfrak{S}}(\Delta) \subseteq \mathsf{P}(Q_{CG}^{\mathrm{ud}})$ に含まれるパスの性質をある程度把握する必要が出てくる。詳しくは [1] を参照されたい。□

5

参考文献

[1] N. Iiyori and M. Sawabe, Simplicial complexes associated to quivers arising from finite groups, preprint.

[2] N. Iiyori and M. Sawabe, Representations of path algebras with applications to subgroup lattices and group characters, to appear in *Tokyo Journal of Mathematics*

[3] 澤辺正人, 有限群の部分群族とパス代数の表現, 第２９回代数的組合せ論シンポジウム（弘前大学）報告集.

Performance of lights and shadows for the quasithin groups

Yasuhiko Tanaka
Oita University

1 Even small groups

Let $\mathcal{F}$ be a set (of isomorphism classes) of known finite simple groups. If G is a finite group, then one of the following holds:

(1) G is a member of $\mathcal{F}$;

(2) G is not a member of $\mathcal{F}$, but the local structure of G is close to that of a member of $\mathcal{F}$;

(3) otherwise.

A group arising in the second case is called a *shadow* from $\mathcal{F}$, while a group arising in the first case is called a *light* from $\mathcal{F}$. Examples show that we have both simple and nonsimple shadows.

The purpose of this note is to give a short introduction to the classification of the simple quasithin groups. To be more precise, the author would like to show how shadows emerge in front of us to be obstructions in the whole classification process. The work of Aschbacher and Smith was published in a two-volume book [AS], which was full of traces of fights against various types of shadows. This note treats only a small number of ones because we should first become familiar with the notion.

Let us make a stop for a while to look back at the history. Revision projects to the existing classification had already begun before it was declared to have completed. It was around those days that an amalgam method appeared and started to expand in the world. Most people must have thought that the amalgam method was one of the most elegant approach in the final stage of the proof.

We know that we always had in mind a set $\mathcal{S}$ (of isomorphism classes) of simple groups for a classification problem beforehand. Of course, it was

expected to be the set of solutions to the problem. We often met with shadows from $\mathcal{S}$, which should be treated appropriately. We can now say that those shadows caused the proof long and complicated. Bender, known for long as a specialist of revision projects through his various results, told us in 1990's that the same would occur also in the approach by the amalgam method. The history proved that he was right indeed, which means we had to spend another decade for analysis. Those footprints left scattered on the sands make us recognize again that we must know how to control many kinds of shadows in the classification.

In the existing proof, the classification of the finite simple groups was divided into four classes: odd large groups, odd small groups, even large groups, and even small groups. We will follow the similar track. In order to do so, we need notions of 'characteristic' and 'rank' for the finite simple groups, corresponding to the inherent characteristic and rank of the Lie type groups. The definition given below is somewhat different from the classical (well-known) one.

A 2-local subgroup is, by definition, a normalizer of a nonidentity 2-subgroup. A finite group G is said to be *even* if $C_L(O_2(L)) \subseteq O_2(L)$ for all 2-local subgroups L of G of odd index. A finite even group G is said to be *quasithin* if $e(G) \leq 2$, where $e(G)$, the (Thompson) rank of G, is the maximum of the p-rank of L, where L ranges over the set of 2-local subgroups of G of odd index, and p ranges over the set of odd primes. We will focus our attention on the quasithin groups.

2 Minimal and maximal parabolics

Where do we come across shadows from the simple quasithin groups, and how? In order to explain that, we will consider the following theorem as an example although it is only a tiny part of the classification of the simple quasithin groups.

Theorem 1 *Let G be a simple quasithin group having a 'minimal parabolic' subgroup. Suppose that the condition*

$$C_L(O_2(L)) = O_2(L) \qquad (*)$$

holds for all minimal parabolic subgroups L of G. Then $G \cong PSL_3(q), PSp_4(q)'$, where q is a power of 2.

We will give a definition of a 'minimal parabolic' subgroup later.

Before we go to description of generic structure of simple quasithin groups, we review properties of Lie type groups because they behave as typical examples and solutions.

Let G be a Lie type group defined over a finite field of characteristic 2. A Borel subgroup of G is a normalizer of a Sylow 2-subgroup of G, and a parabolic subgroup of G is a subgroup containing a Borel subgroup. The most important property of the Lie type groups for us is described in the following. *If G has rank 2 or more, then G is generated by a minimal parabolic subgroup P and a maximal parabolic subgroup Q having a common Borel subgroup B:*

$$G = \langle P, Q \rangle \quad \textit{and} \quad B \subset P \subset G \supset Q \supset B.$$

How do we find similar structure in a simple even group? What is a minimal parabolic subgroup in a simple even group? What is a maximal parabolic subgroup in a simple even group?

Throughout the remainder of this section, let G be a finite even group, and let S be a Sylow 2-subgroup of G.

A subgroup P of G is said to be an *abstract minimal parabolic* over S if $1 \neq O_2(P) \subset S \subset P$ and S is contained in a unique maximal subgroup of P. An abstract minimal parabolic has a very restricted structure. In fact, we have the following for an abstract minimal parabolic P.

- If P is solvable, then P is a $\{2,p\}$-group for some odd prime p, $P = O_{2,p,2}(P)$, and the 2-group $S/O_2(P)$ acts irreducibly on the elementary abelian p-group $(O_{2,p}(P)/O_2(P))/\Phi(O_{2,p}(P)/O_2(P))$.
- If P is not solvable, then $P = O_{2,2',E,2}(P)$, and the 2-group $S/O_2(P)$ permutes the simple components of $P/O_{2,2'}(P)$.

A subgroup Q of G is said to be an *abstract maximal parabolic* over S if $1 \neq O_2(Q) \subset S \subset Q$ and Q is a uniqueness subgroup of G, plus some other technical conditions, if necessary. A subgroup Q of G is said to be a uniqueness subgroup if Q is contained in a unique maximal 2-local subgroup of G.

A pair (H,U) of subgroups of G is said to be a *min-max parabolic pair* over S if the following three conditions hold:

- H is an abstract minimal parabolic over S;
- U is an abstract maximal parabolic over S;
- $O_2(\langle H,U \rangle) = 1$.

It is a min-max parabolic pair over a Sylow 2-subgroup that plays a central role in our analysis.

3 Case division

Let G be a simple quasithin group, and let T be a Sylow 2-subgroup of G. Denote by $\mathcal{M}(T)$ the set of maximal 2-local subgroups of G containing T. There are obviously two cases where $|\mathcal{M}(T)| = 1$ and $|\mathcal{M}(T)| > 1$. The first case is called a uniqueness case, while the other is called an amalgam method case.

In this note, we focus our attention on the amalgam method case. So we can take a pair (M, N) of maximal 2-local 'overgroups' of T (subgroups containing T). Then we have $O_2(\langle M, N\rangle) = 1$. We must choose M and N carefully enough to find the precise structure of M and N. Possibly, we may have $G \neq \langle M, N\rangle$, but we do not care about that because M and N have sufficient information on 'saturated' structure of 2-local subgroups. The smaller both M and N, the better we have. Both $M/O_2(M)$ and $N/O_2(N)$ have restricted structure because they are quasithin themselves. The structure of the chief factors of M and N are restricted by analysis of the amalgams they form.

4 Reduction

We continue to use the same notation. The group G is a simple quasithin group with a Sylow 2-subgroup T.

In order to pin down the precise 2-local structure of G, we want to take a min-max parabolic pair rather than a pair of maximal 2-local overgroups. The next proposition enables us to take a desired one.

Theorem 2 *Let G be a simple quasithin group, and let T be a Sylow 2-subgroup of G. Suppose that $|\mathcal{M}(T)| > 1$. Then G has a min-max parabolic pair (H, U) over T.*

Let $M \in \mathcal{M}(T)$. For a while, M may be an arbitrary element of $\mathcal{M}(T)$. We will choose an appropriate subgroup for M later.

We first choose an abstract minimal parabolic H over T. Let $\mathcal{H} = \mathcal{H}_G$ be the set of subgroups H of G with $O_2(H) \neq 1$. If $H \in \mathcal{H}$, then H is strongly quasithin, namely, $m_p(H) \leq 2$ for all odd primes p. Let $\mathcal{H}(T; M) = \{H \in \mathcal{H} \mid T \subset H \subset M\}$, and let $\mathcal{H}^*(T; M)$ be the set of minimal elements of $\mathcal{H}(T; M)$ under inclusion. If $H \in \mathcal{H}^*(T; M)$, then H is an abstract minimal parabolic over T, and $O_2(\langle H, M\rangle) = 1$.

Suppose that there is a uniqueness subgroup U of M. Then $1 \neq O_2(U) \subset T \subset U$, U is an abstract maximal parabolic over T, and $O_2(\langle H, U\rangle) = 1$. This means that we have a min-max parabolic pair (H, U) over T. Thus

it suffices to prove that there is a maximal 2-local subgroup M having a uniqueness subgroup. We will show that there is a general way to construct a uniqueness subgroup of M for an appropriate choice of M. This is done by using 'component-like' subgroups.

Let K be a subgroup of G. Let $\mathcal{C} = \mathcal{C}_K$ be the set of *$\mathcal{C}$-components*, or subgroups L of K minimal subject to $1 \neq L = L' \lhd \lhd K$. Then the following hold.

- $K^\infty = \langle \mathcal{C}_K \rangle$.
- If $L_1, L_2 \in \mathcal{C}_K$ and $L_1 \neq L_2$, then $[L_1, L_2] \subset O_2(L_1) \cap O_2(L_2) \subset O_2(K)$.
- If $L \in \mathcal{C}_K$, then $L \lhd K$, or $|L^K| = 2$.

Let us consider subgroups like the Levi subgroups in the Lie type groups. Let $\mathcal{L}(G,T)$ be the set of subgroups L with $L \in \mathcal{C}_{\langle L,T\rangle}$, $T \in \mathrm{Syl}_2(\langle L,T\rangle)$, $O_2(\langle L,T\rangle) \neq 1$. Let $\mathcal{L}^*(G,T)$ be the set of maximal elements of $\mathcal{L}(G,T)$. If $L \in \mathcal{L}^*(G,T)$, then $\mathcal{M}(\langle L,T\rangle) = \{N_G(\langle L^T\rangle)\}$, which forces that $\langle L,T\rangle$ is a uniqueness subgroup of G.

We want to take a uniqueness subgroup rather than a maximal 2-local subgroup by the following reason. First of all, a maximal 2-local subgroup itself has too many possible structures. In order to determine possible structure of the maximal 2-local subgroup M by an amalgam method, we want to restrict it before analysis of amalgams. We must know interaction between M and other 2-locals. It is more appropriate if $|\mathcal{M}|$ is smaller, which necessarily demand M should contain many 2-local subgroups. If $\mathcal{M}(U) = \{M\}$ and W is a chief factor of U, then we have $O^2(C_G(W))U \subset N_G(W) \subset M$.

From now on, we will work under the following hypothesis, which is weaker than $(*)$ in the Theorem 1.

Hypothesis:

$$C_H(O_2(H)) = O_2(H) \quad \text{and} \quad C_U(O_2(U)) = O_2(U). \qquad (**)$$

In the course of analysis of 2-local subgroups, the main task is to obtain precise structure of 2-chief factors of them. To do so, we need various results concerning $GF(2)$-representation of even groups. Here, we raise one of the typical ones.

Let G be a group of even order with $O_2(G) = 1$, and let A be an abelian subgroup of G. A $GF(2)G$-module V is said to be an *FF-module* for G with an offending subgroup A if

$$|V : C_V(A)| \leq |A|.$$

Finite groups having an FF-module has a strictly restricted structure. In fact, the following theorem holds.

Theorem 3 *Let G be a group of even order with $O_2(G) = 1$. If G has an FF-module V with an offending subgroup A, then the following hold.*

- $|V : C_V(A)| = |A|$.
- $G \approx PSL_2(q) \times \cdots \times PSL_2(q)$, *where q is a power of* 2.
- $V \approx$ *the direct sum of the modules, each of which is induced by a standard module for the* $PSL_2(q)$.

Of course, the numbers of direct factors and direct summands coincide.

We have just used the symbol '$\approx$' in the above theorem, and will frequently do in the remainder of this note. It means as usual that both sides are close enough to be considered isomorphic for the present purpose.

5 Local structure

We are still proceeding under the same notation. The group G is a simple quasithin group with a Sylow 2-subgroup T. Take a min-max parabolic pair (H, U) over T. Define $Q = O_2(H)$ and $R = O_2(U)$.

Under the Hypothesis (**), we have the following.

- $|Q : Q \cap R| = |R : Q \cap R|$.
- $H/Q \approx PSL_2(q)$ or $PSL_2(q)$ wr Z_2, where q is a power of 2.
- H has a unique noncentral chief factor within Q.
- $U/R \approx PSL2(q)$ or $PSL_2(q) \times PSL_2(q)$, where q is a power of 2.
- $|T : QR|$ is small.

We can conclude that all the above statements are true by the Hypothesis (**) and the properties of groups having an FF-module. We should also remark that U is generated by abstract minimal parabolics even though it is not an abstract minimal parabolic itself.

By the above, we are reduced to one of the following.

- Case 1: $H/Q \approx PSL_2(q)$ and $U/R \approx PSL_2(q)$.
- Case 2: $H/Q \approx PSL_2(q)$ and $U/R \approx PSL2(q) \times PSL2(q)$.
- Case 3: $H/Q \approx PSL_2(q^2)$ and $U/R \approx PSL_2(q) \times PSL_2(q)$.
- Case 4: $H/Q \approx PSL_2(q)$ wr Z_2 and $U/R \approx PSL_2(q^2)$.
- Case 5: $H/Q \approx PSL_2(q)$ wr Z_2 and $U/R \approx PSL_2(q) \times PSL_2(q)$.

6 Shadows of quasithin groups

Before going to each case of the above, we recall the definition of lights and shadows of quasithin groups. Let $\mathcal{Q}$ be the (expected) set of (isomorphism classes of) simple quasithin groups. A 'light' from $\mathcal{Q}$ is an actual group contained in $\mathcal{Q}$, while a 'shadow' from $\mathcal{Q}$ is a group not contained in $\mathcal{Q}$, whose local structure is close to that of some group in $\mathcal{Q}$.

Now, we will give a short comment for each case.

In the Case 1, we have $H/Q \approx PSL_2(q)$ and $U/R \approx PSL_2(q)$.

This is a classical case, and we have examples included here. In fact, we have $G \approx PSL_3(q), PSp_4(q)'$ as the solutions of the Theorem 1. So, G is a light from $\mathcal{Q}$ in our terminology. If we ignore the Hypothesis (**) for now, then $G \approx$ a Lie type group over $GF(q)$ of Lie rank 2, or an exceptional groups. Thus G is a light from $\mathcal{Q}$ with some exceptions.

In the Case 2, we have $H/Q \approx PSL_2(q)$ and $U/R \approx PSL_2(q) \times PSL_2(q)$.

This is impossible under the Hypothesis (**). If we ignore the Hypothesis (**) for now, then $G \approx$ a Lie type group over $GF(q)$ of Lie rank 3, G is a light from $\mathcal{Q}$ if $G \approx PSL_4(2), PSp_6(2), PSU_4(3), \ldots$, but G is a shadow from $\mathcal{Q}$ otherwise.

In the Cases 3 and 4, we have either $H/Q \approx PSL_2(q^2)$ and $U/R \approx PSL_2(q) \times PSL_2(q)$, or $H/Q \approx PSL_2(q) \times PSL_2(q)$ and $U/R \approx PSL_2(q^2)$.

This is impossible under the Hypothesis (**). If we ignore the Hypothesis (**) for now, then $G \approx PSU_4(2), PSL_4(3)$ for $q = 2$. G is a light from $\mathcal{Q}$ if $G \approx PSU_4(2), PSL_4(3), \ldots$, but G is a shadow from $\mathcal{Q}$ if $G \approx \mathrm{Aut}(PSU_4(2)), \mathrm{Aut}(PSL_4(3)), \ldots$.

In the Case 5, we have $H/Q \approx PSL_2(q) \,\mathrm{wr}\, Z_2$ and $U/R \approx PSL_2(q) \times PSL_2(q)$.

This is impossible under the Hypothesis (**). If we ignore the Hypothesis (**) for now, then $G \approx L \,\mathrm{wr}\, Z_2$, where L is a Lie type group over $GF(q)$ of Lie rank 2. Anyway, G is a shadow from $\mathcal{Q}$.

7 Typical shadows

We have encountered four types of shadows in the course of analysis. Both shadows 'of automorphism type' and shadows 'of wreath product type' should finally be eliminated as they are not simple. Both shadows 'of rank 3 or more type' and shadows 'of odd type' are eliminated due to our restriction. If we deviate from the restriction of the quasithin groups and consider in a broader range of groups, we will probably obtain those groups as lights. Let us take a closer look at each type of shadows.

First, let L be a simple groups of Lie type of characteristic 2, and let t be an involution. A group 'of characteristic 2 like' is a group such as L, $G = L\langle t\rangle$, $H = (L \times L^t)\langle t\rangle$.

As you know, we have the following examples of small groups.

- $L = A_6 \cong Sp_4(2)'$, $G = S_6 \cong Sp_4(2)$.
- $L = A_5 \cong PSL_2(4)$, $G = S_5 \cong PSL_2(4)\langle f\rangle$, $H = A_5 \operatorname{wr} Z_2 \cong PSO_4^+(4)$, where f is a field automorphism of $PSL_2(4)$.
- $L = A_8 \cong PSL_4(2)$, $G = S_8 \cong PSL_4(2)\langle g\rangle$, where g is a graph automorphism of $PSL_4(2)$.

Those example show that we are sometimes unable to distinguish simple groups from nonsimple groups only by 2-local structure.

Next, let $G = PSL_4(q)$, where q is a power of 2 and larger than 2. Let M be a maximal parabolic subgroup of G. Let L be the uniqueness subgroup in M. Then $L/O_2(L) \cong PSL_3(q)$ or $PSL_2(q) \times PSL_2(q)$. Thus L is quasithin itself. This example shows that a simple quasithin group with a uniqueness subgroup isomorphic to L seems to be possible at first, which is finally eliminated, though.

The example shows that some even groups of rank 3 have similar 2-local structure with quasithin groups. We are often unable to distinguish quasithin groups from even groups of higher rank only by 2-local structure.

Finally, we raise examples of odd groups. The detailed information is obtained from the ATLAS [AT1, AT2].

- It is known that $P\Omega_7(3)$ has a $PSp_6(2)$-subgroup of odd index, where $PSp_6(2)$ is a quasithin group.
- It is also known that $P\Omega_8^+(3)$ has a $P\Omega_8^+(2)$-subgroup of odd index, where $P\Omega_8^+(2)$ is a group of rank 3.
- It is further known that $P\Omega_8^-(3)$ has an $\mathrm{Aut}(P\Omega_7(3))$-subgroup of odd index.

Those examples show that some odd groups have similar 2-local structure with even groups. In some cases, we cannot distinguish odd groups from even groups only by 2-local structure.

References

[AS] M. Aschbacher and S. D. Smith, *The classification of quasithin groups*, AMS Surveys and Monographs **111**, **112**, 2004.

[AT1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Clarendon Press, Oxford, 1985, 252pages.

[AT2] R. Abbott, J. Bray, S. Linton, S. Nickerson, S. Norton, R. Parker, I. Suleiman, J. Tripp, P. Walsh, and R. Wilson, *Atlas of finite group representations*, published electronically at `http://brauer.maths.qmul.ac.uk/Atlas/v3/`.

On the finite space with a finite group action

獨協医科大学基本医学基盤教育部門　藤田亮介 (Ryousuke Fujita)
Premedical Sciences, Dokkyo Medical University
大阪大学大学院理学研究科　河野進 (Susumu Kono)
Graduate School of Science, Osaka University

1 Introduction

The purpose of our presentation was to study actions of finite groups on finite T_0-spaces, i.e. topological spaces having finitely many points with the T_0-separation axioms. The definition of T_0-separation axiom is, for each pair of distinct points, there exists an open set containing one but not the other. A remarkable feature of a finite T_0-space is that it has the structure of a poset. Conversely, one can give any finite poset the structure of a finite T_0-space. The equvariant theory of finite T_0-spaces was first made by Stong [13]. His research motivation is an approach to the Quillen Conjecture, that is,

If a Quillen complex $\Delta(A_p(G))$ is contractible, then $O_p(G)$ is non-trivial,

where p is a prime number dividing the order of a finite group G, and $O_p(G)$ is the maximal normal p-subgroup of G. Moreover $\Delta(A_p(G))$ is the order complex of a poset

$$A_p(G) = \{\text{non-trivial elementary abelian } p\text{-subgroup of } G\},$$

ordered by inclusion. In [13], Stong viewed $A_p(G)$ as a finite T_0-G-space by conjugation and obtained the following result:

Proposition 1.1. *If a finite T_0-space $A_p(G)$ is contractible, then $O_p(G)$ is non-trivial.*

Therefore, the Quillen Conjecture is equivalent to

If the Quillen complex $\Delta(A_p(G))$ is contractible, then the finite T_0-space $A_p(G)$ is so.

Following McCord's result [11, Theorem 2], the Quillen complex $\Delta(A_p(G))$ is weak homotopy equivalent to the finite T_0-space $A_p(G)$. From a topological point of view, this problem deals with a difference between weak homotopy equivalence and homotopy equivalence.

First we define a simplicail complex induced from a finite T_0-space. Recall that a finite T_0-space has a poset structure (see Proposition 2.2). Let X be a finite poset. The *order complex* $\Delta(X)$ of X is the abstract simplicial complex on the vertex set X whose faces are the chains of X, including the empty chain. The *dimension* of a simplex is defined to be the length of the chain, where the length of a chain is one less than its number of elements. In particular, the length of the empty chain is -1. When the dimension of a simplex σ is k, we write $\dim \sigma = k$. Next we shall define the geometric realization $|\Delta(X)|$ of $\Delta(X)$ by

$$|\Delta(X)| = \{m : X \to [0,1] \mid \sum_{x \in X} m(x) = 1,\ \mathrm{supp}(m) \in \Delta(X)\},$$

where for a map $m : X \to [0,1]$, we mean that $\mathrm{supp}(m) = \{x \in X \mid m(x) > 0\}$. The numbers $(m(x) \mid x \in X)$ are the *barycentric coordinates* of m. For a simplex $\sigma \in \Delta(X)$, we put

$$|\sigma| = \{m \in |\Delta(X)| \mid \mathrm{supp}(m) = \sigma\}.$$

We can define a metric topology on $|\Delta(X)|$. In details, we have a metric d on $|\Delta(X)|$ defined by

$$d(m_1, m_2) = \left(\sum_{x \in X} (m_1(x) - m_2(x))^2 \right)^{\frac{1}{2}}.$$

Then we have $\overline{|\sigma|} = \{m \in |\Delta(X)| \mid \sum_{x \in \sigma} m(x) = 1\}$, where $\overline{|\sigma|}$ indicates the closure of $|\sigma|$. Moreover a metric space $|\Delta(X)|$ is equipped with a CW-complex structure whose n-cell is a set $\{|\sigma| \mid \sigma \in \Delta(X),\ \dim \sigma = n\}$. Let $(p_x \mid x \in X)$ be a family of points in euclidean n-space $\mathbb{R}^n$. Consider the continuous map

$$f : |\Delta(X)| \to \mathbb{R}^n, \qquad m \mapsto \sum_{x \in X} m(x) p_x.$$

If f is an embedding, we call the image of f a *simplicial polyhedron* in $\mathbb{R}^n$ of type $\Delta(X)$, that is, $f(|\Delta(X)|)$ is a realization of $\Delta(X)$ as a polyhedron in $\mathbb{R}^n$.

Now, we shall introduce McCord's result [11, Theorem 2], which provides insight into understanding relations between finite T_0-spaces and simplicial complexes.

Proposition 1.2. *There exists a correspondence that assigns to each finite T_0-space X a finite simplicial complex $\Delta(X)$, whose vertices are the points of X, such that the map $\mu_X : |\Delta(X)| \to X$ induced from the correspondence above is a weak homotopy equivalence. Moreover, each map $\varphi : X \to Y$ of finite T_0-spaces is also a simplicial map $\Delta(X) \to \Delta(Y)$, and $\varphi \mu_X = \mu_Y |\varphi|$ where $|\varphi| : |\Delta(X)| \to |\Delta(Y)|$ is a continuous map induced by φ.*

Let G be a finite group. In this note, we focus on the equivariant order complex $\Delta(X)$ of a finite T_0-G-space X, that is, a finite T_0-space with a G-action, and then its orbit space $\Delta(X)/G$. In particular, we are interested in the following questions:

(i) Does $|\Delta(X)|$ has a G-CW-complex structure?
(ii) Is there the orbit space version of Proposition 1.2?

Our results related the above questions are the following.

Theorem A. Let X be a finite T_0-G-space. Then $|\Delta(X)|$ is a finite G-CW-complex.

We will prepare the following technical condition:

(C) If $g_0, g_1, \cdots, g_k$ are elements of G and $(x_0, x_1, \cdots, x_k)$ and $(g_0 x_0, g_1 x_1, \cdots, g_k x_k)$ are both simplices of K, then there exists an element g of G such that $g x_i = g_i x_i$ for all i. Here overlaps of some of x_i are allowed.

Theorem B. If $\Delta(X)$ satisfies property (C), there exists a weak homotopy equivalence $\tilde{\mu}_X : |\Delta(X)|/G \to X/G$.

The rest of this note is organized as follows. In section 2, we briefly review finite (T_0-)space theory. In section 3, we investigate an equivariant version of finite T_0-spaces and prove Theorem A. The last section studies orbit spaces of equivariant complexes and prove Theorem B.

2 Finite (T_0-)spaces

In this section, we survey well-known properties about finite (T_0-)spaces. General reference may be found in [2], [7] and [12]. Let X denote a finite space, i.e. a topological space having finitely many points. Let a set U_x be the minimal open set which contains a point x of X, that is, U_x is the intersection of all open sets containing x. It is easy to see that a set $\{U_x\}_{x\in X}$ constitute a basis for the topology of X. Now we can define a *preorder* on X by

$$x \leq y \quad \text{if} \quad x \in U_y.$$

In other words, every open set containing y also contains x if and only if $x \leq y$.

Proposition 2.1. *Let x and y be elements of a finite space X. Then X is T_0-space if and only if $U_x = U_y$ implies $x = y$.*

Proposition 2.2. *A finite T_0-space with the above preorder $\leq$ is a poset.*

If X is now a finite preordered set, one can define a topology on X given by the basis $\{y \in X \mid y \leq x\}_{x\in X}$. Note that if $y \leq x$, then y is contained in every basic set containing x, and therefore $y \in U_x$. Conversely, if $y \in U_x$, then $y \in \{z \in X \mid z \leq x\}$. After all, $y \leq x$ if and only if $y \in U_x$. This shows that these two applications, relating topologies and preorders on a finite set, are mutually inverse. Thus we have

Proposition 2.3. *A finite T_0-space corresponds to a finite poset.*

Example 2.4. Let $X = \{a, b, c\}$ be a finite space whose topology is $\{\emptyset, \{a, b, c\}, \{b, c\}, \{b\}, \{c\}\}$. This space is T_0. Immediately, $U_a = \{a, b, c\}$, $U_b = \{b\}$ and $U_c = \{c\}$. Therefore $b \leq a$ and $c \leq a$, but there exists no order relation between b and c.

Example 2.5. Let $X = \{a, b, c, d\}$ be a finite space whose topology is $\{\emptyset, \{a, b, c, d\}, \{b, c, d\}, \{b\}, \{b, c\}, \{b, d\}\}$. This space is also T_0. Immediately, $U_a = \{a, b, c, d\}$, $U_b = \{b\}, U_c = \{b, c\}$ and $U_d = \{b, d\}$. On the order relation, we see the following Hasse diagram:

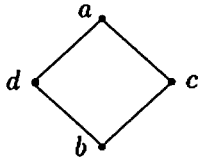


Figure 1.

Proposition 2.6. *Let X be a preordered set. A set $F_x = \{y \in X \mid x \leq y\}$ is a closed set of X. Moreover F_x is the closure of the set $\{x\}$.*

Definition 2.7. A subset U of a preordered set X is a *down-set* if for every $x \in U$ and $y \leq x$, it holds that $y \in U$. Dually, a subset F of a preordered set X is a *up-set* if for every $x \in F$ and $y \geq x$, it holds that $y \in F$. Open sets of finite spaces correspond to down-sets and closed sets to up-sets.

Proposition 2.8. *Let X and Y be finite spaces, and f be a map from X to Y. Then f is continuous if and only if f is an order-preserving map.*

Proposition 2.9. *Let X be a finite space, f a continuous map of X into itself. If f is either one-to-one or onto, then it is a homeomorphism.*

Next we state connectivity. First, for each U_x, we let $U_x \subset A \cup B$, where A and B are open sets of a finite space X. Then x is in one set, say $x \in A$, immediately $U_x \subset A$. Thus any finite space is locally connected.

Proposition 2.10. *Let x, y be two comparable points of a finite space X and $x \leq y$. Then there exists a path from x to y in X, that is, a map α from the unit interval I to X such that $\alpha(0) = x$ and $\alpha(1) = y$.*

Let X be a finite preordered set. A *fence* in X is a sequence $x_0, x_1, \cdots, x_n$ of points such that any two consecutive are comparable. X is *order-connected* if any two points $x, y \in X$ there exists a fence starting in x and ending in y.

Proposition 2.11. *Let X be a finite space. Then the following are equivalent:*
(i) X is a connected topological space.
(ii) X is an order-connected preordered set.
(iii) X is a path-connected topological space.

If X and Y are finite spaces, we can consider the finite set Y^X of continuous maps from X to Y with the pointwise order: $f \leq g$ if $f(x) \leq g(x)$ for every $x \in X$.

Proposition 2.12. *Let X and Y be two finite spaces. Then pointwise order on Y^X corresponds to the compact-open topology.*

Corollary 2.13. *Let $f, g : X \to Y$ be two maps between finite spaces. Then $f \simeq g$ if and only if there is a fence $f = f_0 \leq f_1 \geq f_2 \leq \cdots f_n = g$. Moreover, if $A \subset X$, then $f \simeq g$ rel A if and only if there exists a fence $f = f_0 \leq f_1 \geq f_2 \leq \cdots f_n = g$ such that $f_i|_A = f|_A$ for every $0 \leq i \leq n$.*

Any finite space is homotopy equivalent to a finite T_0-space.

Proposition 2.14. *Let X be a finite space. Let X_0 be the quotient $X/\sim$ where $x \sim y$ if $x \leq y$ and $y \leq x$. Then X_0 is T_0 and the quotient map $q : X \to X_0$ is a homotopy equivalence.*

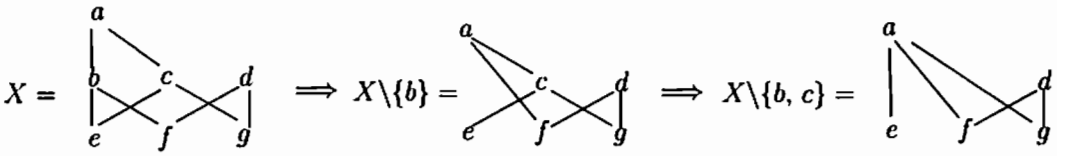
Therefore , when studying homotopy types of finite spaces, we can restrict our attention to finite T_0-spaces.

Definition 2.15. A point x in a finite T_0-space X is a *down beat point* if x cover one and only one element of X. This is equivalent to saying that the set $\hat{U}_x = U_x \backslash \{x\}$ has a maximum. Dually, $x \in X$ is an *up beat point* if x is covered by a unique element or equivalently if $\hat{F}_x = F_x \backslash \{x\}$ has a minimum, where F_x denotes the closure of the set $\{x\}$. In any of these cases, we say that x is a *beat point* of X.

Proposition 2.16. *Let X be a finite T_0-space and let $x \in X$ be a beat point. Then $X\backslash\{x\}$ is a strong deformation retract of X.*

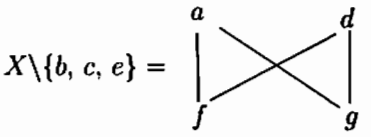
Definition 2.17. A finite T_0-space is a *minimal finite space* if it has no beat points. A *core* of a finite space X is a strong deformation retract which is a minimal finite space.

For example, we have the following:



b is a up beat poin. c is a up beat point. e is a up beat point.

After all,



is a minimal finite space.

Proposition 2.18. *Let X be a minimal finite space. A map $f : X \to X$ is homotopic to the identity if and only if $f = 1_X$.*

Immediately, we have the following corollary.

Corollary 2.19. (Classification Theorem) *A homotopy equivalence between minimal finite spaces is a homeomorphism. In particular, the core of a finite space is unique up to homeomorphism and two finite spaces are homotopy equivalent if and only if they have homeomorphic cores.*

By the Classification Theorem, a finite space is contractible if and only if its core is a point. In fact, a one-point finite space has a core of the one-point. Therefore any contractible finite space has a point which is a strong deformation retract.This property is false in general for non-finite spaces.

3 Finite T_0-G-spaces

In this section, we treat an equivariant version of finite T_0-spaces. Let G be a topological group (a group, for short) and X a finite T_0-space. A G-invariant subspace $A \subset X$ is an *equivariant strong deformation retract* if there is an equivariant retraction $r : X \to A$ such that ir is homotopic to 1_X via a G-homotopy which is stationary at A. A finite T_0-space which is a G-space will be *a finite T_0-G-space.*

Remark If a topological group G acts on a finite topological space effectively, then it must be a finite topological group [8, Proposition 3.9]. Therefore, from now on, we assume that G is finite.

Proposition 3.1. *Let X be a finite T_0-G-space. Then there exists a core of X which is G-invariant and an equivariant strong deformation retract of X.*

Proposition 3.2. *A contractible finite T_0-G-space has a point which is fixed by the action of G.*

This proposition deduces Stong's result stated in introduction. Note that $A_p(G)$ is a finite T_0-G-space by conjugation. If $A_p(G)$ is contractible, $A_p(G)$ has exactly one point core which is G-invariant. Therefore $A_p(G)$ has a fixed point by the action of G. Consequently, G has a non-trivial normal p-subgroup.

Proposition 3.3. *Let X and Y be finite T_0-G-spaces and let $f : X \to Y$ be a G-map which is a homotopy equivalence. Then f is an equivariant homotopy equivalence.*

Let X be a finite T_0-G-space and x, y points of X. If $x \in U_y$, then $gx \in gU_y = U_{gy}$. Therefore a G-action on a finite T_0-space X preserves the order. Thus $\Delta(X)$ is a G-simplicial complex (in short, G-complex). Let $\mathbb{N}_0$ be the union set of natural numbers $\{1, 2, 3, \cdots\}$ and $\{0\}$.

Definition 3.4. Let G be a finite group. A CW-complex Z with a G-action is called a *G-CW-complex* if it satisfies the following conditions:
(i) The G-action determines a cellular map, that is, for any $g \in G$, $gZ^i \subset Z^i$ for each $i \in \mathbb{N}_0$, where Z^i denotes the union of cells of dimension $\leq i$ and is called the *i-skeleton* of Z.
(ii) If $g(e) = e$, then g is trivial on $\bar{e}$, that is, $Z^g \supset \bar{e}$, where $\bar{e}$ is the closure of e.

Example 3.5. Let $x = (x_1, \cdots, x_n) \in \mathbb{R}^n$, then its *norm* is defined by $\|x\| = \sqrt{\sum_{i=1}^{n} x_i^2}$. For $G = \mathbb{Z}_2 = \{\pm 1\}$, the unit sphere $S^{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = 1\}$ together with the G-action given by scalar multiplication,

$$G \times S^{n-1} \to S^{n-1}, \quad (\lambda, x) \mapsto \lambda x, \quad \lambda \in G = \{\pm 1\} \subset \mathbb{R}, \quad x \in S^{n-1} \subset \mathbb{R}^n$$

is a free G-space. Then S^{n-1} becomes a G-CW-complex. Let us verify this. Observe that $S^{n-1} = E_+^{n-1} \cup E_-^{n-1}$, where E_+^{n-1}(respectively, E_-^{n-1}) is a upper(respectively, lower) closed hemisphere, and $E_+^{n-1} \cap E_-^{n-1} = S^{n-2}$(the equator). There are thus two $(n-1)$-cells e_1^{n-1} and e_2^{n-1} with $\overline{e_1^{n-1}} = E_+^{n-1}$, $\overline{e_2^{n-1}} = E_-^{n-1}$; one concludes by induction that S^{n-1} has a CW-decomposition with two i-cells in every dimension $0 \leq i \leq n-1$. For each $\lambda \in G$, λe_j^i $(j = 1, 2; i = 0, \cdots, n-1)$ is also a cell. If $\lambda(e_j^i) = e_j^i$, then $\lambda = 1$, and it is clearly trivial on $\overline{e_j^i}$. Thus S^{n-1} has a $\mathbb{Z}_2$-CW-complex structure.

A *G-CW-complex* was defined by Matumoto ([10]) and Illman ([5]) separately. Roughly speaking, a *finite* G-CW-complex is a compact Hausdorff G-space obtained by attaching a finite number of *G-cells* $G/H \times D$, where H is an arbitrary subgroup of G and D is an arbitrary finite dimensional, closed disk with trivial G-action. As sets, a finite G-CW-complex is a disjoint union of open G-cells $G/H \times \mathrm{Int}(D)$, where $\mathrm{Int}(D)$ denoted the interior of D. In particular, a 0-dimensional finite G-CW-complex is a finite G-set, and in general, a finite G-CW-complex is a finite cellular complex with regular G-action. A

G-action on a cellular complex X is said to be *regular* if, for each open cell e in X, ge is an open cell in X for any $g \in G$, and the isotropy subgroups appearing in e coincide with one another. As we saw above, S^{n-1} is a finite $\mathbb{Z}_2$-CW-complex.

Proof of Theorem A.

Proof. For $g \in G$ and $m \in |\Delta(X)|$, we define a map $g(m) : X \to [0,1]$ by

$$(g(m))(x) := m(g^{-1}(x)) \quad \text{for } x \in X.$$

Then we have

$$\sum_{x \in X} (g(m))(x) = \sum_{x \in X} m(g^{-1}(x)) = \sum_{g^{-1}(x) \in X} m(g^{-1}(x)) = 1,$$

on the other hand,

$$\begin{aligned} \mathrm{supp}(g(m)) &= \{x \in X \mid (g(m))(x) > 0\} \\ &= \{x \in X \mid m(g^{-1}(x)) > 0\} \\ &= \{x \in X \mid g^{-1}(x) \in \mathrm{supp}(m)\} \\ &= g(\mathrm{supp}(m)) \in \Delta(X). \end{aligned}$$

Therefore we have that $g(m) \in |\Delta(X)|$. Thus we can define a isometric map $g : |\Delta(X)| \to |\Delta(X)|$. For each $\sigma \in \Delta(X)$, it holds that $g(|\sigma|) = |g(\sigma)|$. In particular, a map g is a cellular map.

Let $g(|\sigma|) = |\sigma|$. Immediately, we have $g(\sigma) = \sigma$. Since g is an automorphism between totally ordered sets, it is an identity map. Therefore $g^{-1} : \sigma \to \sigma$ is also an identity map. Let m be any element of $\overline{|\sigma|}$.

Case $x \in \sigma$: It follows that $(g(m))(x) = m(g^{-1}(x)) = m(x)$.

Case $x \in X \backslash \sigma$: Since $g^{-1}(x) \in X \backslash g^{-1}(\sigma) = X \backslash \sigma$, we get that $(g(m))(x) = m(g^{-1}(x)) = 0 = m(x)$.

Therefore $g(m) = m$. Thus we obtain that $\overline{|\sigma|} \subset |\Delta(X)|^g$. □

Referring to [6, p.229], we now prepare the following technical properties concerning a G-complex K:

(P_1) For any $g \in G$ and simplex σ of K, g leaves $\sigma \cap g\sigma$ pointwise fixed.

(P_2) If $g_0, g_1, \cdots, g_k$ are elements of G and $(x_0, x_1, \cdots, x_k)$ and $(g_0x_0, g_1x_1, \cdots, g_kx_k)$ are both simplices of K, then there exists an element g of G such that $gx_i = g_ix_i$ for all i. Here overlaps of some of x_i are allowed.

(P_3) Let g be an element of G and σ a simplex of K. If $g(\sigma) = \sigma$, g leaves σ pointwise fixed.

Proposition 3.6. *It holds that* $(P_2) \Longrightarrow (P_1) \Longrightarrow (P_3)$.

Proposition 3.7. *Let X be a finite T_0-G-space. Then a G-complex $\Delta(X)$ holds both property (P_1) and property (P_3).*

On a G-complex, we can see a geometric simplex as a cell. One immediate consequence of this observation is the following.

Proposition 3.8. *Let $|K|$ be the geometric realization of a G-complex K with property (P_3). Then $|K|$ is a G-CW-complex.*

The following result is an equivariant version of Proposition 1.2 in a sense.

Proposition 3.9. *Let X be a finite T_0-G-space. For each subgroup H of G, it holds that $\Delta(X^H) = \Delta(X)^H$ and the map $\mu_X^H : |\Delta(X)|^H \to X^H$ is a weak homotopy equivalence.*

4 Orbit spaces

Next we will devote the study of the orbit space of a G-complex.

Proposition 4.1. *Let X be a finite T_0-G-space. Then the orbit space X/G is a finite T_0-space.*

Let X and Y be finite sets, and $\mathcal{P}(X)$ the power set of X. A map $f : X \to Y$ induces a map $\mathcal{P}(X) \to \mathcal{P}(Y)$, which we denote also by f. Let K be a simplicial complex such that X is the set of vertices of K. Then it is easy to see that the image $f(K)$ becomes a simplicial complex such that $f(X)$ is the set of vertices of $f(K)$. We apply this observation to our situation.

Let K be a G-complex and X be the set of vertices of K. Concerning the induced G-action on X. we consider its orbit space X/G and the orbit map $p : X \to X/G$. As observes above, p induced a map $\mathcal{P}(X) \to \mathcal{P}(X/G)$, which we denote by p as well and $p(K)$ becomes a simplicial complex such that X/G is the set of vertices of $p(K)$. For $s \in K$, we denote $p(s)$ by $\overline{s}$.

Next we consider another kind of orbit space. Let K be a G-complex. Denote by K/G the orbit space of the G-action on K and by $\pi : K \to K/G$ the orbit map. For $s \in K$, we denote $\pi(s)$ by $[s]$. Note that K/G is not a simplicial complex in general and K/G does not coincide with $p(K)$ in general.

Proposition 4.2. [6, Lemma 5.10] *Let K be a G-complex satisfying property (P_2) and X be the set of vertices of K. Then the orbit space K/G becomes a simplicial complex such that the set of vetrices K/G is X/G and K/G is naturally isomorphic to $p(K)$. Moreover the orbit map $\pi : K \to K/G$ is a simplicial map preserving dimension of simplexes.*

Corollary 4.3. *If K is a G-complex satisfying property (P_2), $|K|/G$ is homeomorphic to $|K/G|$.*

Furthermore, we add simplicial notion for both posets and (finite) cell complexes to investigate the simplicial structure of the orbit spaces in detail.

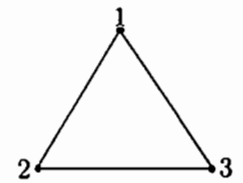
Definition 4.4. A *simplicial poset* P is a finite poset with a smallest element $\hat{0}$ such that every interval

$$[\hat{0}, y] = \{x \in P \mid \hat{0} \leq x \leq y\}$$

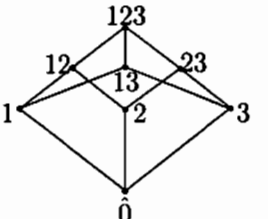
for $y \in P$ is a boolean algebra, i.e., $[\hat{0}, y]$ is isomorphic to the set of all subsets of a finite set, ordered by inclusion. When a boolean algebra is the set of all subsets of a finite set consisting of n elements, we denote the boolean algebra by B_n. Let x be an element of P

such that $[\hat{0}, x]$ is isomorphic to a boolean algebra B_n. Then the *dimension* of x is said to be $n-1$, denoted by $\dim x = n-1$. Remark that $\dim \hat{0} = -1$. Moreover, a simplicail poset P is *n-dimensional*, if it contains at least one point x such that $\dim x = n$ but no $(n+1)$-dimensional points.

The set of all faces of a (finite) simplicial complex with empty set added forms a simplicial poset ordered by inclusion, where the empty set is the smallest element. Such a simplicial poset is called the *face poset* of a simplicial complex, and two simplicial complexes are isomorphic if and only if their face posets are isomorphic. Therefore, a simplicial poset can be thought of as a generalization of a simplicial complex. Figure 2 shows that a 2-simplicial complex and its face poset.



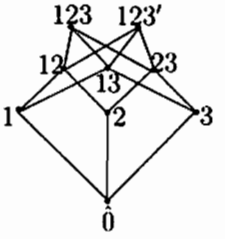
a 2-simplicial complex



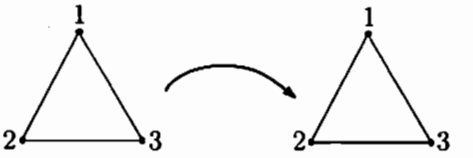
a face poset

Figure 2.

A CW-complex is said to be *regular* if all closed cells are homeomorphic to closed disks. Although a simplicial poset is not necessarilly the face poset of a simplicial complex, it is always the face poset of a regular CW-complex. Let P be a simplicial poset. To each element $y \in P\backslash\{\hat{0}\} = \overline{P}$, we assign a (geometric) simplex whose face poset is $[\hat{0}, y]$ and glue those geometric simplices according to the order relation in P. Then, we get the CW-complex in which the closure of each cell is identified with a simplex, the structure of faces being preserved; moreover, all characteristic mappings are embeddings. This CW-complex is called a *simplicial cell complex* associated to P and is denoted by $|P|$. For instance, if two 2-simplices are identified on their boundaries via the identity map, then it is not a simplicial complex but a CW-complex obtained from a simplicial poset (see Figure 3). Clearly, this CW-complex is homeomorphic to the 2-sphere S^2. The simplicial cell complex $|P|$ has a well-defined barycentric subdivision which is isomorphic to the order complex $\Delta(\overline{P})$ of the poset $\overline{P}$.



a simplicial poset P
($123'$ is a copy of 123)



a simplicial cell complex $|P|$

Two 2-simplicial complexes are identified on their boundaries.

Figure 3.

By definition, we have the following proposition.

Proposition 4.5. *Let S is a finite cell complex. Then S is simplicial if and only if for each cell $\sigma \subset S$, the closure $\overline{\sigma}$ of σ is isomorphic to a simplex Δ of the same dimension with σ as a cell complex.*

In a word, a simplicial cell complex is a cell complex such that each closed cell is a geometric simplex. Obviously, the geometric realization of any finite simplicial complex is a simplicial cell complex.

Definition 4.6. Let S be a simplicial cell complex and $V(S)$ the set of all 0-cells of S. Let σ be a cell of S. We put $V(\sigma) = V(S) \cap \overline{\sigma}$. For each cell $\sigma \subset S$, there is an embedding

$$\varphi_\sigma : \Delta^{\dim \sigma}(V(\sigma)) \to \overline{\sigma} \subset S,$$

where $\Delta^{\dim \sigma}(V(\sigma))$ is the $\dim \sigma$-simplex whose vertex set is $V(\sigma)$. We say φ_σ a *characteristic map* of σ.

Proposition 4.7. *A simplicial poset corresponds to a simplicial cell complex.*

Let P be a simplicial poset and $x \in P$. A half-open interval $(\hat{0}, x]$ is a subset $\{y \in P \,|\, \hat{0} \leq y \leq x\}$ of P.

Definition 4.8. Let P and Q be simplicial posets. A *simplicial poset map* $f : P \to Q$ is a map such that for any $x \in P$, $\dim f(x) \leq \dim x$ and $f((\hat{0}, x]) = (\hat{0}, f(x)]$.

For a simplicial poset P, we put $V(P) := \{x \in P \,|\, \dim x = 0\}$, which is called the *vertex set* of P. Similarly, for each $x \in P$, $V(x) := V([\hat{0}, x]) = [\hat{0}, x] \cap V(P)$, which is also called the *vertex set* of x. A simplicial poset map f is order-preserving and satisfies $f(V(x)) = V(f(x))$ for $x \in P$. Note that $V(P) = \bigcup_{x \in P} V(x)$. Moreover we put

$$K_P := \{V(x) \,|\, x \in P\},$$

which is a simplicial complex whose vertex set is $V(P)$. Here we see K_P as a simplicial poset, so that a surjection $\varphi_P : P \to K_P$ defined by $\varphi_P(x) = V(x)$ is a simplicial poset map.

Definition 4.9. Let X and Y be simplicial cell complexes. A *simplicial cell complex map* $f : X \to Y$ is a cellular map such that for any cell $\sigma \in X$, $f(\sigma)$ is a cell of Y and $f|_{\overline{\sigma}} : \overline{\sigma} \to \overline{f(\sigma)} \subset Y$ extends linearly the map $f|_{V(\sigma)} : V(\sigma) \to V(f(\sigma)) \subset Y$. Note that $f(\overline{\sigma})$ is the compact set of a Hausdorff space Y.

Let X and Y be simplicial cell complexes. Let $\mathcal{F}(X)$ (*respectively*, $\mathcal{F}(Y)$) be a simplicial poset corresponding to X (*respectively*, Y). A simplicial cell complex map $f : X \to Y$ defines a simplicial poset map $\mathcal{F}(f) : \mathcal{F}(X) \to \mathcal{F}(Y)$ by $\sigma \mapsto f(\sigma)$ for each cell $\sigma \in X$. Conversely, we have the following.

Proposition 4.10. *For any simplicial poset map $\alpha : \mathcal{F}(X) \to \mathcal{F}(Y)$, there exists uniquely a simplicial cell complex map $f : X \to Y$ such that $\mathcal{F}(f) = \alpha$. In particular, if a simplicial poset map $\alpha : \mathcal{F}(X) \to \mathcal{F}(Y)$ is bijective, then f is an isomorphism from X to Y.*

Proposition 4.11. *For any simplicial poset P, there exists some simplicial cell complex X with $\mathcal{F}(X) \cong P$.*

From the above two propositions, there is uniquely an isomorphism class $[X]$ such that $\mathcal{F}(X) \cong P$. Then a simplicial cell complex X is said to be *a realization* of P, denoted by $|P|$ as well. Under this notation, we have a simplicail cell complex map $|\varphi_P| : |P| \to |K_P|$.

Let K be a G-complex. Now, we shall investigate the structure of the orbit space K/G. Let σ and τ be simplices of K. We define a partial ordering on K/G as follows:

$$\pi(\tau) \leq \pi(\sigma) \text{ if and only if there exists an element } g \in G \text{ such that } g(\tau) \subset \sigma,$$

where the map $\pi : K \to K/G$ is the orbit map. Note that the orbit space K/G has the minimum $\hat{0} = \pi(\emptyset)$. Moreover we denote the orbit map from $|K|$ to $|K|/G$ by π as well.

Proposition 4.12. *If a G-complex K has property (P_1), K/G is a simplicial poset. Moreover $|K|/G$ is a simplicial cell complex such that $\{\pi(|\sigma|) \,|\, \sigma \in K \backslash \{\emptyset\}\}$ is the set of all cells of $|K|/G$.*

Proposition 4.13. *If a G-complex K has property (P_1), it holds that $|K|/G \cong |K/G|$ as a simplicial cell complex.*

Corollary 4.14. *Let X be a finite T_0-G-space. The orbit space $|\Delta(X)|/G$ is a finite simplicial cell complex associated to a simplicial poset $\Delta(X)/G$. Moreover we have $|\Delta(X)|/G \cong |\Delta(X)/G|$.*

Let X be a finite T_0-G-space. Since the orbit map $p : X \to X/G$ is continuous, it is an order-preserving map. It determines a simplicial map

$$\Delta(p) : \Delta(X) \to \Delta(X/G),$$

and also a continuous map $|\Delta(p)| : |\Delta(X)| \to |\Delta(X/G)|$. Noting $|\Delta(X/G)|$ is a G-space with a trivial G-action, we have a continuous map $\tilde{p} : |\Delta(X)|/G \to |\Delta(X/G)|$ such that the following diagram commutes

$$\begin{array}{ccc} |\Delta(X)| & & \\ {\scriptstyle q}\downarrow & \searrow^{|\Delta(p)|} & \\ |\Delta(X)|/G & \xrightarrow[\tilde{p}]{} & |\Delta(X/G)| \end{array}$$

where q is the orbit map from $|\Delta(X)|$ to $|\Delta(X)|/G$.

Proposition 4.15. *Let X be a finite T_0-G-space. A simplicial complex $K_{\Delta(X)/G}$ concides with $\Delta(X/G)$.*

In consequence we have the following commutative diagram:

$$\begin{array}{ccc} |\Delta(X)|/G & \xrightarrow{\cong} & |\Delta(X)/G| \\ {\scriptstyle \tilde{p}}\downarrow & & \downarrow{\scriptstyle |\varphi_{\Delta(X)/G}|} \\ |\Delta(X/G)| & \xrightarrow[id]{} & |\Delta(X/G)|\,. \end{array}$$

A simplicial action of G on a simplicial complex K is called *regular in the sense of Bredon* if K possesses property (P_2) for the action of each subgroups of G. Now, we shall present an interesting example.

Example 4.16. Let n be an integer larger than one. Let X_{2n+2} be a set consisting of $2n+2$ elements as follows:

$$X_{2n+2} =: \bigcup_{i=1}^{n+1} \{x_i, x_{-i}\}.$$

We set

$$\begin{cases} U(x_i) := \{x_i\} \bigcup_{j=1}^{i-1} \{x_j, x_{-j}\}, & \text{and} \\ U(x_{-i}) := \{x_{-i}\} \bigcup_{j=1}^{i-1} \{x_j, x_{-j}\}, \end{cases}$$

for $i = 1, 2, \cdots, n+1$. First note that each point x_i determines the smallest open set $U(x_i)$ on X_{2n+2}, that is, $U_{x_i} = U(x_i)$. Therefore we define a T_0-topology on X_{2n+2}. Let g be a map from X_{2n+2} to itself by $g(x_i) = x_{-i}$. We set $G := \langle g \rangle$(that is, a group is generated by g). Evidently, G is a cyclic group whose order is two. Since $|\Delta(X_{2n+2})|$ is homeomorphic to the n-sphere S^n, it holds that $|\Delta(X_{2n+2})|/G \cong \mathbb{R}P^n$, where $\mathbb{R}P^n$ is the n-dimensional real projective space. Note that $|\Delta(X_{2n+2})|/G$ is a simplicial cell complex by Proposition 4.12. On the other hand, X_{2n+2}/G is a totally ordered set with $n+1$ elements. Therefore $|\Delta(X_{2n+2}/G)|$ is homeomorphic to a n-simplex $\Delta^n(X_{2n+2}/G)$. Since the map $\tilde{p} : |\Delta(X_{2n+2})|/G \to |\Delta(X_{2n+2}/G)|$ is not a weak homotopy equivalence, $\tilde{p}$ is not an isomorphism between simplicial cell complexes. If $\Delta(X_{2n+2})/G$ is a simplicial complex, the map $|\varphi_{\Delta(X_{2n+2})/G}|$ is an isomorphism, and $\tilde{p}$ is also an isomorphism. This is a contradiction. Hence $\Delta(X_{2n+2})/G$ is not a simplicial complex, thereby G-action on $\Delta(X_{2n+2})$ is not regular in the sense of Bredon.

Proof of Theorem B.

Let X be a finite T_0-G-space. By Proposition 1.2, there is a weak homotopy equivalence $\mu_X : |\Delta(X)| \to X$. Then μ_X determines a continuous map $\tilde{\mu}_X : |\Delta(X)|/G \to X/G$ such that the following diagram commutes.

$$\begin{array}{ccc} |\Delta(X)|/G & \xrightarrow{\tilde{p}} & |\Delta(X/G)| \\ & \searrow^{\tilde{\mu}_X} & \downarrow{\scriptstyle \mu_{X/G}} \\ & & X/G \end{array}$$

Therefore $\tilde{p}$ is a weak homotopy equivalence if and only if $\tilde{\mu}_X$ is so. In general, $\tilde{\mu}_X$ is not a weak homotopy equivalence (see Example 4.16).

Remark that both $|\Delta(X)|/G$ and $|\Delta(X/G)|$ are CW-complexes. Therefore, we have

Claim 1. $\tilde{\mu}_X$ is a weak homotopy equivalence if and only if $\tilde{p}$ is a homotopy equivalence.

We consider the case where $\tilde{p}$ is a homeomorphism.

Claim 2. Let X be a finite T_0-G-space. Then the following conditions are equivalent:
(1) $\tilde{p}$ is a homeomorphism.
(2) $\Delta(X)/G$ is a simplicial complex.
(3) $\Delta(X)$ has property (P_2).

Proof. (1) $\Longrightarrow$ (2) Since $\tilde{p}$ is a homeomorphism, $\varphi_{\Delta(X)/G}$ is injective. Let U be a subset of X/G. Then there exists only one element s of $\Delta(X)/G$ at most with $V(s) = U$. Therefore $\Delta(X)/G$ is a simplicial complex. (2) $\Longrightarrow$ (1) Since $\Delta(X)/G$ is a simplicial complex, it holds that $|\Delta(X)/G| = |\Delta(X/G)|$. Noting that $\varphi_{\Delta(X)/G}$ is surjective, $\tilde{p}$ is also surjective. By Proposition 2.9, $\tilde{p}$ is a homeomorphism. (2) $\Longrightarrow$ (3) Let $\sigma = \{x_i \,|\, i = 0, \cdots, k\}$ and $\tau = \{g_i x_i \,|\, g_i \in G,\ i = 0, \cdots, k\}$ be simplices of $\Delta(X)$. If $x_i = x_j$, then

$$g_j x_j = (g_j g_i^{-1})(g_i x_i) \in \tau \cap (g_j g_i^{-1})\tau.$$

Since a G-complex $\Delta(X)$ has property (P_1), we have $g_j x_j = (g_j g_i^{-1})^{-1}(g_j x_j) = g_i x_j$, so that $g_i x_i = g_i x_j = g_j x_j$. Hence we assume that each x_i $(i = 0, \cdots, k)$ is distinct, then both σ and τ are k-simplices of $\Delta(X)$. Therefore both $\pi(\sigma)$ and $\pi(\tau)$ are elements of $\Delta(X)/G$ such that $V(\pi(\sigma)) = V(\pi(\tau)) = \{\pi(x_i) \,|\, i = 0, \cdots, k\}$. By assumption, $\pi(\sigma) = \pi(\tau)$. In consequence there is some $g \in G$ such that $\tau = g(\sigma)$ and $g_i x_i = g x_i$ $(i = 0, \cdots, k)$. (3) $\Longrightarrow$ (2) It follows from Proposition 4.2. □

Combining Claim 1 and Claim 2, we obtain Theorem B. □

ACKNOWLEDGEMENTS. We would like to Professor Masaaki Kitazume, Professor Masaaki Harada and Professor Makoto Araya for inviting us to the 30th Symposium on Algebraic Combinatorics.

References

[1] Buchstaber, V.M. and Panov, T,E., *Combinatorics of simplicial cell complexes and torus actions*, Proc. Steklov Inst. Math. **247** (2004), 1-17.

[2] Barmak, J., *Algebraic Topology of Finite Topological Spaces and Applications*, Lecture Notes in Math, 2032, Springer-Verlag, 2011.

[3] Björner, A., *Posets, regular CW complexes and Bruhat order*, European. J. Combinatorics. **5** (1984), 7-16.

[4] Ginsburg, J., *A structure theorem in finite topology*, Canad. Math. Bull. **26 (1)** (1983), 121-122.

[5] Illman, S., *Equivariant singular homology and cohomology for actions of comapct Lie groups*, Lecture Notes in Math, 298, Springer-Verlag, Berlin-Heidelberg-New York, 403-415, 1972

[6] Kawakubo K., *The Theory of Transformation Groups*, Oxford University Press, London, 1991.

[7] Kono, S. and Ushitaki, F., *Geometry of finite topological spaces and equivariant finite topological spaces*, in: Current Trends in Transformation Groups, ed. A.Bak, M.Morimoto and F.Ushitaki, pp.53-63, Kluwer Academic Publishers, Dordrecht, 2002.

[8] Kono, S. and Ushitaki, F., *Homeomorphism groups of finite topological spaces*, RIMS Kokyuroku, **1290** (2002), 131-142.

[9] Kono, S. and Ushitaki, F., *Homeomorphism groups of finite topological spaces and Group actions*, RIMS Kokyuroku, **1343** (2003), 1-9.

[10] Matumoto, T., *On G-CW-complexes and a theorem of J.H.C. Whitehead*, J. Fac. Sci. Univ. of Tokyo, **18** (1971), 363-374.

[11] McCord, M.C., *Singular homotopy groups and homotopy groups of finite topological spaces*, Duke. Math. J. **33** (1966), 465-474.

[12] Stong, R.E., *Finite topological spaces*, Trans.Amer.Math.Soc. **123** (1966), 325-340.

[13] Stong, R.E., *Group actions on finite spaces*, Discrete Math. **49** (1984), 95-100.

$\mathbb{Z}_3$-軌道体構成法と中心電荷 24 の正則頂点作用素代数

島倉 裕樹 (Hiroki Shimakura)

東北大学大学院情報科学研究科
純粋・応用数学研究センター
Research Center for Pure and Applied Mathematics,
Graduate School of Information Sciences, Tohoku University
e-mail: shimakura@m.tohoku.ac.jp

本稿では佐垣大輔氏 (筑波大学) と石井基裕氏 (筑波大学) と筆者の共同研究 [SS, ISS] の解説を行う.

1 序

本稿で取り扱う正則 VOA とは, 既約加群がただ一つで自分自身と同型となるような VOA である. 例えば, モンスター単純群を自己同型群に持つムーンシャイン VOA は正則である.

二元符号, 格子, 頂点作用素代数[1] (VOA) の間に様々な類似があることはよく知られている. 正則に対応する二元符号における概念は自己双対, 格子における概念はユニモジュラであると思われる.[2] この根拠の一つとして, 次の (古典的な) 定理における対応がある.

定理 1.1. (1) 長さ n の重偶自己双対二元符号が存在するための必要十分条件は $n \in 8\mathbb{Z}_{>0}$.

(2) 階数 n のユニモジュラ偶格子が存在するための必要十分条件は $n \in 8\mathbb{Z}_{>0}$.

(3) 中心電荷 n の正則 VOA が存在するための必要十分条件は $n \in 8\mathbb{Z}_{>0}$.

これらの証明 (の一つの方法) にはそれぞれ, 符号の重み多項式, 格子のテータ級数, VOA の指標, におけるある種の群作用による不変性が用いられることを注意しておく.

各 $n \in 8\mathbb{Z}_{>0}$ に対して, これらの符号, 格子, VOA の同型類 (同値類) の分類問題を考えたい. 符号については $n \leq 32$, 格子については $n \leq 24$, VOA については $n \leq 16$ で分類されている. 特に, $n = 8, 16$ においては次のような完全な対応がある.

[1] 本稿では VOA は単純, 有理的, C_2-有限, CFT 型を仮定している. VOA の定義は [Bo86, FLM88] を参照せよ.

[2] 二元符号における重偶, 格子における偶に対応する VOA の性質は「整数による次数付け」であると思われる. これは VOA の公理に含まれている.

定理 1.2. (1) 長さ 8, 16 の重偶自己双対二元符号は同値を除いて丁度三つあり, e_8, e_8^2, d_{16}^+ である.

(2) 階数 8, 16 のユニモジュラ偶格子は同型を除いて丁度三つあり, E_8, E_8^2, D_{16}^+ である.

(3) 中心電荷 8, 16 の正則 VOA は同型を除いて丁度三つあり, V_{E_8}, $V_{E_8^2}$, $V_{D_{16}^+}$ である.

ここで, 中心電荷 8, 16 の正則 VOA は格子 VOA であり, それぞれ階数 8, 16 のユニモジュラ偶格子から得られる. これは, 階数 8, 16 のユニモジュラ偶格子はそれぞれ長さ 8, 16 の重偶自己双対二元符号から構成法 A によって得られることに対応していると考えられる.

次の $n = 24$ の場合は, 重偶自己双対符号とユニモジュラ偶格子は分類されている:

定理 1.3. 長さ 24 の重偶自己双対符号の同値類は 9 個あり, それぞれの同値類は重さ 4 の符号語の成す tetrad system によって一意的に定まる.

定理 1.4. [Ni73] 階数 24 のユニモジュラ偶格子の同型類は 24 個あり, それぞれの同型類はノルム 2 のベクトルの成すルート系によって一意的に定まる.

VOA の共形重みは 1 の空間には (VOA の積を用いて) リー代数の構造が入る. したがって, 対応する頂点作用素代数の問題は次の通りである.

問題 1.5.
- 中心電荷 24 の正則 VOA の同型類を決定せよ.
- それぞれの同型類は共形重み 1 の空間が成すリー代数構造から一意的に決まるか?

この問題は次の有名な予想を含む.

予想 1.6. [FLM88] 共形重み 1 の空間が 0 である中心電荷 24 の正則 VOA はムーンシャイン VOA $V^\natural$ と同型である.

この予想は Golay 符号の一意性, Leech 格子の一意性に対応する主張であることを注意しておく.

さて, 問題 1.5 を考える前に, Venkov による階数 24 のユニモジュラ偶格子の分類の証明を紹介しよう.

定理 1.7. [Ve78] L を階数 24 のユニモジュラ偶格子として, R をそのルート系とする. このとき, 次が成立する:

(1) $R = \emptyset$ または R の生成する部分格子の階数は 24;

(2) R の各既約部分ルート系に対して, $h = \frac{|L(2)|}{24}$. ただし, h はコクセター数である.

この定理 (とルート系の分類) から, ユニモジュラ偶格子のルート系は (空集合も含めて) 24 通りの可能性しかないことが示せる. さらに各ルート系をノルム 2 のベクトルの集合として持つユニモジュラ偶格子が (同型を除いて) ただ一つ存在することがわかる.

同様な手法による中心電荷 24 の正則 VOA の分類の研究が行われている.

定理 1.8. [Sc93, DM04b, DM06] V を中心電荷 24 の正則 VOA とする.

(1) $V_1 = 0$ または V_1 が生成する部分 VOA の中心電荷は 24.

(2) $V_1 \neq 0$ かつ V_1 が可換ならば, $\dim V_1 = 24$ であり, V はリーチ格子 VOA と同型.

(3) V_1 が非可換ならば, V_1 は半単純である. さらに V_1 の全ての単純イデアル $\mathfrak{g}$ に対して, $\frac{\check{h}}{k} = \frac{\dim V_1}{24} - 1$ となる. ただし, $\check{h}$ は $\mathfrak{g}$ の双対コクセター数であり, k は $\mathfrak{g}$ の V 上のアファイン表現のレベルである.

(4) (3) におけるレベル k は正の整数である.

アファイン VOA の既約加群は一般には単純カレントではないため, V_1 が生成するアファイン VOA の拡大として正則 VOA を構成するのは難しい. 同様に VOA 構造の一意性についても格子 VOA の場合 ([DM04a]) を除いては証明されていない.

また, この結果と単純リー代数の分類結果を合わせても 221 個[3]の可能性までしか減らせない. だたし "さらなる計算"[4]によって, リー代数の可能性を絞り込む事が出来, そうして得られる 71 通りのリストが [Sc93] にまとめられている.

そこで, 中心電荷 24 の正則 VOA の分類へ向けて, まずは次の問題を考えたい.

問題 1.9. [Sc93] のリストにある 71 個のリー代数に対して, それを共形重み 1 の空間にもつ中心電荷 24 の正則 VOA を構成せよ.

既に述べたように, リー代数を出発点とした正則 VOA の構成は非常に難しい. そこで, ユニモジュラ偶格子から別のユニモジュラ偶格子を作る一つの手法である p-neighbor の理論[5]の VOA 版である $\mathbb{Z}_p$-軌道体構成法を用いた正則 VOA の構成を考える. これは正則 VOA V と位数 p の自己同型 g に対して, 固定点として得られる部分 VOA V^g の拡大として別の正則 VOA $\tilde{V}^g$ を構成する方法[6]である. そして, いくつかの VOA とその自己同型に対しては $\mathbb{Z}_p$ 軌道体構成法が確立されており[7], 次の中心電荷 24 の正則 VOA が構成されている:

- 24 (合計 24): Niemeier 格子に付随する正則格子 VOA ([Bo86, FLM88, Do93]).
- 15 (合計 39): $\mathbb{Z}_2$-軌道体構成法を Niemeier 格子 VOA と -1 倍する自己同型の持ち上げに適用 [8] ([FLM88, DGM96]).

[3] [Sc93] による. 筆者は未確認

[4] [Sc93] による. 筆者は未確認

[5] ユニモジュラ格子 L と L' が p-neighbor とは $|L/(L \cap L')| = |L'/(L \cap L')| = p$. このとき, $(L \cap L')^*/(L \cap L')$ は位数 p^2 の可換群であり, $L \cap (L \cap L')$ と $L'/(L \cap L')$ は位数 p の部分群である.

[6] 殆どの場合は次の "良い" 状況を考えている: V^g の既約加群の同型類が丁度 p^2 個あり, 分岐則によって同型類の集合に位数 p^2 の可換群の構造が入り, V と $\tilde{V}^g$ の部分 V-可群の同型類は位数 p の部分群となる. 特に, V^g-既約加群は単純カレント.

[7] 一般の VOA の理論の確立に必要であった V^g の C_2-有限性が最近に [Mi] で証明された.

[8] 9 個の Niemeier 格子の場合は格子 VOA と同型になる.

- 17 (合計 56): 長さ 48 の三重偶符号 ([BM12]) に付随する枠付正則 VOA[9] ([La11, LS12, LS]).

- 1 (合計 57): $\mathbb{Z}_3$-軌道体構成法を E_6^4 型の Niemeier 格子とある位数 3 に自己同型へ適用 ([Mi13]).

今回の研究の主結果は, 宮本氏によって確立された正則格子 VOA への $\mathbb{Z}_3$-軌道体構成法 ([Mi13]) を全ての Niemeier 格子と全ての位数 3 の自己同型に対して適用して, この方法で得られる新しい中心電荷 24 の正則 VOA を全て決めた事である.

定理 1.10. [SS, ISS] L を Niemeier 格子とし, $\sigma \in \mathrm{Aut}L$ を位数 3 とする. さらに, $L^\sigma = \{v \in L \mid \sigma(v) = v\}$ とし, $\mathrm{rank}\, L^\sigma \in 6\mathbb{Z}$ とする[10]. このとき, $\mathbb{Z}_3$-軌道体構成法を V_L と σ に適用[11]して得られる正則 VOA $\tilde{V}_L^\sigma$ は次のいずれかを満たす.

(1) 格子 VOA と同型;

(2) $(\tilde{V}_L^\sigma)_1$ のリー代数構造は 0, $A_{2,3}^6$, $E_{6,3}G_{2,1}^3$, $A_{5,3}D_{4,3}A_{1,1}^3$ のいずれかと同型.

さらに, (2) の各リー代数を持つ V_L^σ が (少なくとも一つは) 存在する.

[Mi13] で $E_{6,3}G_{2,1}^3$ を持つ正則 VOA は構成されているため, 新たに見つけたのは二つである.[12] よって, 次の系を得る.

系 1.11. 中心電荷 24 の正則 VOA は (少なくとも) 59 個存在する.

したがって, 残されている問題は次の通りである.

- Schellekens のリストにある残り 12 個のリー代数に対して, それを持つ中心電荷 24 の正則 VOA を構成せよ.

- Schellekens のリストの (簡単な) 証明を与えよ.

- 各リー代数に対して, それをもつ中心電荷 24 の正則 VOA の (同型を除いた) 一意性 (もしくは分類).

[9] 既に得られていた 39 個も枠付 VOA である. 困難の一つである VOA 構造が入ることは (ヴィラソロ枠に自明に作用する位数 2 の自己同型に付随する) $\mathbb{Z}_2$-軌道体構成法 [LY08] を用いて解決している.

[10] この仮定は twisted 加群に整数の共形重みが現れることと同値. すなわち, $\mathbb{Z}_3$-軌道体構成法が適用できるための必要十分条件.

[11] 奇数位数の格子の自己同型は (位数を保ったまま) 格子 VOA の自己同型に持ち上げることが出来る.

[12] "新しい" 正則 VOA であることは, リー代数のレベルに 3 冪が現れていることから分かる. これは, 枠付正則 VOA のリー代数のレベルが 2 冪 ([LS12]) から従う.

2 $\mathbb{Z}_3$-軌道体構成法を用いた中心電荷 24 の正則 VOA の構成

この章では [SS] の結果を簡単に紹介する.
まずは, 宮本氏によって確立された次の結果を思いだそう.

定理 2.1. [Mi13] L をユニモジュラ偶格子, $\sigma \in \mathrm{Aut}\ L$ を位数 3, $\mathrm{rank}\ L^\sigma \in 6\mathbb{Z}$ とする. $V_L(\sigma^i)$ を V_L の既約 σ^i-twisted 加群とし, $V_L(\sigma^i)_{\mathbb{Z}}$ を $V_L(\sigma^i)$ の共形重みが整数である部分空間とする. このとき, $\tilde{V}_L^\sigma = V_L^\sigma \oplus V_L(\sigma)_{\mathbb{Z}} \oplus V_L(\sigma^2)_{\mathbb{Z}}$ は (C_2-有限な) 正則 VOA となる.

この応用として宮本氏は次の結果を得ている.

定理 2.2. [Mi13] L を E_6^4 型の Niemeier 格子とし, $\sigma_6 \in \mathrm{Aut}\ L$ を

$$\begin{array}{cc} & E_6 \oplus E_6 \oplus E_6 \ominus \quad E_6 \\ \sigma_6 : & \text{3-cycle} \qquad \text{fixed point free} \end{array}$$

で与えられる L の位数 3 の自己同型とする. このとき, $\mathrm{rank}\ L^{\sigma_6} = 6$ であり, $(\tilde{V}_L^{\sigma_6})_1 \cong E_{6,3}G_{2,1}^3$

注意 2.3. [Mi13] L をリーチ格子とし, $\sigma_7 \in \mathrm{Aut}\ L$ を共役類 3A に属する元とする. このとき, $\mathrm{rank}\ L^{\sigma_7} = 0$ であり, $(\tilde{V}_L^{\sigma_7})_1 = 0$.

ここから, $\mathbb{Z}_3$-軌道体構成法を適用して格子 VOA 以外が得られる自己同型 σ_i $(1 \le i \le 5)$ を挙げていく.

L を D_4^6 型の Niemeier 格子とし, $\sigma_2, \sigma_3, \sigma_4 \in \mathrm{Aut}\ L$ を次を満たす位数 3 の自己同型とする:

$$\begin{array}{cc} & D_4 \oplus D_4 \oplus D_4 \oplus D_4 \oplus D_4 \oplus D_4 \\ \sigma_2 : & \varphi \quad \varphi \quad \varphi \quad \varphi \quad \varphi \quad \varphi \\ \sigma_3 : & \varphi \quad \varphi \quad \varphi \quad \omega \quad \omega \quad \omega \\ \sigma_4 : & \text{3-cycle} \qquad\quad \varphi \quad \varphi^{-1} \quad \psi \end{array}$$

ただし $\varphi, \omega \in \mathrm{Aut}\ D_4 \setminus W(D_4)$, $\psi \in W(D_4)$ は位数 3 で $\mathrm{rank}\ D_4^\varphi = 0$, $\mathrm{rank}\ D_4^\omega = \mathrm{rank}\ D_4^\psi = 2$ を満たす. このとき, $\mathrm{rank}\ L^{\sigma_2} = 0$, $\mathrm{rank}\ L^{\sigma_3} = \mathrm{rank}\ L^{\sigma_4} = 6$ となる.

定理 2.4. [SS] $(\tilde{V}_L^{\sigma_2})_1 \cong A_{2,3}^6$, $(\tilde{V}_L^{\sigma_3})_1 \cong E_{6,3}G_{2,1}^3$, $(\tilde{V}_L^{\sigma_4})_1 \cong A_{5,3}D_{4,3}A_{1,1}^3$.

$N(Q)$ でルート系 Q に対応する Niemeier 格子を表すことにする. $\sigma_1 \in \mathrm{Aut}\ N(A_2^{12})$ を次を満たす位数 3 の自己同型とする:

$$\begin{array}{cc} & A_2^3 \oplus A_2^3 \oplus A_2^3 \oplus \quad A_2^3 \\ \sigma_1 : & \text{3-cycle} \qquad \text{fixed point free} \end{array}$$

$\sigma_5 \in \mathrm{Aut}\ N(A_5^4D_4)$ を次で定義される位数 3 の自己同型とする:

$$A_5 \oplus A_5 \oplus A_5 \oplus A_5 \oplus D_4$$
$$\sigma_5 : \quad 3\text{-cycle} \qquad \eta \quad \varphi$$

ただし $\eta \in W(A_5)$ は rank $A_5^\eta = 1$ を満たす位数 3 の自己同型とする. このとき, rank $\mathrm{Ni}(A_2^{12})^{\sigma_1} = \mathrm{rank}\ \mathrm{Ni}(A_5^4 D_4)^{\sigma_5} = 6$ となる.

定理 2.5. [SS] $(\tilde{V}^{\sigma_1}_{N(A_2^{12})})_1 \cong A^6_{2,3}$, $(\tilde{V}^{\sigma_5}_{N(A_5^4 D_4)})_1 \cong A_{5,3} D_{4,3} A^3_{1,1}$.

これらの定理の証明の鍵は次の事である.

- $\tilde{V}_L^\sigma$ は $\mathbb{Z}_3$-grading を持つ.
- $V_L(\sigma)$, $V_L(\sigma^2)$ は [Le85, DL96] で構成されており, V_L^σ の作用が具体的に書ける.
- $(\tilde{V}_L^\sigma)_1$ は可換でなければ半単純である. さらに, 各単純イデアルに対して, 定理 1.8 (3) が成立している.

単純リー代数の分類から, 各々の場合においてリー代数の可能性は数通りで, さらに, 上に挙げた性質から可能性を一つに絞り込んだ.

注意 2.6.
- 各リー代数に対して, それを持つ VOA の構成法が二通りあるが, これら VOA が同型かどうかは (現時点では) わかっていない.
- これらの証明には Schellekens のリストを用いていない.

3 Weyl 群の元に付随する $\mathbb{Z}_p$-軌道体構成法

Niemeier 格子 VOA に $\mathbb{Z}_3$-軌道体構成法を適用して得られる正則 VOA のリー代数の可能性について調べたい. まずは, Weyl 群に属する自己同型を考察する. そのために, もっと一般的な自己同型である共形重み 1 の元の 0-積の exponential として得られる自己同型について考察する.

定理 3.1. L をユニモジュラ偶格子とし, $N(V_L) = \langle \exp a_{(0)} \mid a \in (V_L)_1 \rangle$ とする. $g \in N(V_L)$ を有限位数とする.

(1) $|L : M| = |g|$ となる L の部分格子 M が存在し, $V_L^g \cong V_M$.

(2) $\mathbb{Z}_p$-軌道体構成法を V_L と g に適用して得られる正則 VOA $\tilde{V}_L^g$ が存在するとする. このとき, $|N : M| = |g|$ となる偶格子 N が存在して, $\tilde{V}_L^g \cong V_N$. 特に, L と N は $|g|$-neighbor である.

$N(V_L)$ はリー代数 $(V_L)_1$ の内部自己同型群と思える. 有限次元リー代数の有限自己同型は [K90] の 8 章で分類されており, g はあるカルタン部分代数の元の exponential と書くことが出来る. $N(V_L)$ はカルタン部分代数へ可移に作用することと, 標準的なカルタン部分代数の元の exponential による固定部分 VOA の計算によって (1) が証明される. また, 格子 VOA の既約加群は単純カレントであり, その単純カレント拡大は格子 VOA となる. よって (2) が証明される.

特に, L の Weyl 群 (の持ち上げ) は $N(V_L)$ に入るため, 次が得られる.

系 3.2. $L = N(Q)$ を Niemeier 格子とし, $\sigma \in W(Q)$ とする. このとき, $\tilde{V}_L^\sigma$ は格子 VOA となる.

4 Niemeier 格子の位数 3 の自己同型の分類とその応用

前章の結果から, 次の分類問題を解決し, それぞれの場合に $\tilde{V}_L^\sigma$ を考察すれば良い.

問題 4.1. 次を満たす $L = N(Q)$ の位数 3 の自己同型を分類せよ:

$$\text{rank } L^\sigma \in 6\mathbb{Z} \qquad \text{and} \qquad \sigma \notin W(Q).$$

Weyl 群に属さない自己同型は, ルート系上に置換として作用するか, グラフ自己同型として作用する. また, Niemeier 格子の自己同型群の情報は [CS99] に書かれている. これらを基にして, それぞれの場合で計算をすることで, 次の結果を得ることが出来る:

定理 4.2. $L = N(Q)$ が

$$\text{rank } L^\sigma \in 6\mathbb{Z} \qquad \text{and} \qquad \sigma \notin W(Q)$$

を満たす位数 3 の自己同型 σ を持つならば

$$Q = \emptyset,\ A_1^{24},\ A_2^{12},\ A_3^8,\ D_4^6,\ A_5^4D_4,\ A_6^4,\ D_6^4,\ E_6^4.$$

さらに, このような自己同型の共役類の数は表で与えられる.

2 章で述べた σ_i が属する共役類については, $(\tilde{V}_L^\sigma)_1$ のリー代数の構造が決定されている. また, リーチ格子 Λ に付随する V_Λ と $\text{rank } \Lambda^\sigma = 6$ の場合は $\tilde{V}_\Lambda^\sigma \cong V_\Lambda$ となることが容易に証明できる. 残る場合は次の命題により解決される:

命題 4.3. Niemeier 格子 $L = N(Q)$ の位数 3 の自己同型 σ が $\text{rank } L^\sigma = 12$ を満たすならば, $\tilde{V}_L^\sigma$ は格子 VOA と同型である.

[DM04a] によって, 共形重み 1 の空間のリー代数のランクが 24 ならば格子 VOA と同型となることが知られている. これらの場合に, 表による具体的な自己同型の記述を用いて, 24 次元のカルタン部分代数を見つける. ここでも, [K90] の 8 章の内容を用いる.

以上から主結果である定理 1.10 が証明される.

Q	$\emptyset$	A_1^{24}	A_2^{12}	A_3^8	D_4^6	$A_5D_4^4$	A_6^4	D_6^4	E_6^4
rank $L^\sigma = 0$	1 σ_7	0	0	0	1 σ_2	0	0	0	0
rank $L^\sigma = 6$	1	0	1 σ_1	0	2 σ_3, σ_4	1 σ_5	0	0	1 σ_6
rank $L^\sigma = 12$	1	1	1	1	2	1	1	1	1

5 今後の課題

1章の最後で今後の課題について述べている. 最初の問題である残り 12 個のリー代数を持つ正則 VOA の構成に関しては, いくつかのアイデアがある.

一つは宮本氏の理論を $\mathbb{Z}_5$ の場合に拡張することである. これによって, 新しい正則 VOA が少なくとも一つ構成できることを確認している. あとは実際に VOA 構造が入ることを証明し, 他に新しい正則 VOA が構成できるかを確認する必要がある. これは佐垣氏を含めたグループによって研究予定である.

もう一つは枠付 VOA の置換自己同型に付随する $\mathbb{Z}_p$-軌道体構成法の確立である. これによって, 新しい正則 VOA が出来るであろうと予想している. VOA 構造が入ることを証明し, リー代数構造を決定しなくてはいけない. これは Lam 氏との共同研究の予定である.

実際に 71 個を構成するためには $\mathbb{Z}_2$- 及び $\mathbb{Z}_3$-軌道体構成法が確立されれば十分であることが Montague によって示唆されている ([Mo98]). しかしながら, 現段階では一般の VOA に対する軌道体構成法が確立されていない. この理論の進展があれば, さらに多くの正則 VOA が構成できると思われる.

参考文献

[BM12] K. Betsumiya and A. Munemasa, On triply even binary codes, *J. Lond. Math. Soc.* **86** (2012), 1–16.

[Bo86] R.E. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster, *Proc. Nat'l. Acad. Sci. U.S.A.* **83** (1986), 3068–3071.

[CS99] J.H. Conway and N.J.A. Sloane, Sphere packing, lattices and groups, Third edition, Grundlehren der Mathematischen Wissenschaften, Vol. 290, Springer-Verlag, New York, 1999.

[DGM96] L. Dolan, P. Goddard and P. Montague, Conformal field theories, representations and lattice constructions, *Comm. Math. Phys.* **179** (1996), 61–120.

[Do93] C. Dong, Vertex algebras associated with even lattices, *J. Algebra* **161** (1993), 245–265.

[DL96] C. Dong and J. Lepowsky, The algebraic structure of relative twisted vertex operators, *J. Pure Appl. Algebra* **110** (1996), 259–295.

[DM04a] C. Dong and G. Mason, Rational vertex operator algebras and the effective central charge, *Int. Math. Res. Not.* (2004), 2989–3008.

[DM04b] C. Dong and G. Mason, Holomorphic vertex operator algebras of small central charge, *Pacific J. Math.* **213** (2004), 253–266.

[DM06] C. Dong and G. Mason, Integrability of C_2-cofinite vertex operator algebras. *Int. Math. Res. Not.* (2006), Art. ID 80468, 15 pp.

[FLM88] I. Frenkel, J. Lepowsky and A. Meurman, Vertex operator algebras and the Monster, Pure and Appl. Math., Vol.134, Academic Press, Boston, 1988.

[ISS] M. Ishii, D. Sagaki and H. Shimakura, Application of a $\mathbb{Z}_3$-orbifold construction to the lattice vertex operator algebras associated to Niemeier lattices, Part II, in preparation.

[K90] V.G. Kac, Infinite-dimensional Lie algebras, Third edition, Cambridge University Press, Cambridge, 1990

[La11] C.H Lam, On the constructions of holomorphic vertex operator algebras of central charge 24, *Comm. Math. Phys.* **305** (2011), 153–198

[LS12] C.H. Lam and H. Shimakura, Quadratic spaces and holomorphic framed vertex operator algebras of central charge 24, *Proc. Lond. Math. Soc.* **104** (2012), 540–576.

[LS] C.H. Lam and H. Shimakura, Classification of holomorphic framed vertex operator algebras of central charge 24, preprint, arXiv:1209.4677.

[LY08] C. Lam and H. Yamauchi, On the structure of framed vertex operator algebras and their pointwise frame stabilizers, *Comm. Math. Phys.* **277** (2008), 237–285.

[Le85] J. Lepowsky, Calculus of twisted vertex operators, *Proc. Nat. Acad. Sci. U.S.A.* **82** (1985), 8295–8299.

[Mi13] M. Miyamoto, A $\mathbb{Z}_3$-orbifold theory of lattice vertex operator algebra and $\mathbb{Z}_3$-orbifold constructions, *in* "Symmetries, Integrable Systems and Representations", Springer Proceedings in Mathematics and Statistics Vol. 40, pp.319–344, Springer-Verlag, London, 2013.

[Mi] M. Miyamoto, C_2-cofiniteness of cyclic-orbifold models, preprint, arXiv:1306.5031.

[Mo98] P.S. Montague, Conjectured Z_2-orbifold constructions of self-dual conformal field theories at central charge 24 - the neighborhood graph, *Lett. Math. Phys.* **44** (1998), 105–120.

[Ni73] H-V. Niemeier, Definite quadratische Formen der Dimension 24 und Diskriminante 1, *J. Number Theory* **5** (1973), 142–178.

[SS] D. Sagaki and H. Shimakura, Application of a $\mathbb{Z}_3$-orbifold construction to the lattice vertex operator algebras associated to Niemeier lattices, Part I, preprint, arXiv:1302.4826.

[Sc93] A.N. Schellekens, Meromorphic $c = 24$ conformal field theories, *Comm. Math. Phys.* **153** (1993), 159–185.

[Ve78] B.B. Venkov,On the classification of integral even unimodular 24-dimensional quadratic forms, *Trudy Mat. Inst. Steklov.* **148** (1978), 65–76, 273.

The McKay–Thompson series of Mathieu Moonshine modulo two

山形大学・地域教育文化学部　三枝崎　剛

1　はじめに

本稿の目的は，近年発見された Mathieu Moonshine 現象 [7]，Umbral Moonshine 現象 [2] に現れるモックテータ関数のフーリエ係数の合同式，特に偶素数に関する合同式を調べ，その合同式の Cheng-Duncan-Harvey による予想 [2] への応用を紹介することである．

本稿の結果は，部分的に Matthias Waldherr 氏 (University of Cologne)，Thomas Creutzig 氏 (Technische Universität Darmstadt)，Gerald Höhn 氏 (Kansas State University) との共同研究である．

2　Moonshine 現象

$E_4(\tau)$ を Eisenstein 級数，$\eta(\tau)$ を Dedekind η-関数とする：

$$E_4(\tau) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n,$$

$$\eta(\tau) = q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n),$$

ここで，$\sigma_3(n) = \sum_{m|n} m^3$．そのとき，$j$-関数は次のように定義される：

$$\begin{aligned} j(\tau) &= \frac{E_4(\tau)^3}{\eta(\tau)^{24}} = \frac{1}{q} + 744 + 196884q + \cdots \\ &= \sum_{n=-1}^{\infty} c(n)q^n. \end{aligned}$$

McKay は，$c(1) = 196884$ が Monster 単純群の非自明な既約表現の最小次元 196883 とほとんど等しい事に気付き，いわゆる Moonshine 現象を発見した．これらは，Conway と Norton により，Moonshine conjecture として纏められ，現在では Borcherds によって証明されている [5, 1]．この様に j-関数の Fourier 係数 $c(n)$ は種々の興味深い性質をもつが，特に次の合同式を満たす事が知られている [14]：$a \geq 1$ に対し，

$$\begin{cases} n \equiv 0 \pmod{2^a} & \Rightarrow c(n) \equiv 0 \pmod{2^{3a+8}} \\ n \equiv 0 \pmod{3^a} & \Rightarrow c(n) \equiv 0 \pmod{3^{2a+3}} \\ n \equiv 0 \pmod{5^a} & \Rightarrow c(n) \equiv 0 \pmod{5^{a+1}} \\ n \equiv 0 \pmod{7^a} & \Rightarrow c(n) \equiv 0 \pmod{7^a} \\ n \equiv 0 \pmod{11^a} & \Rightarrow c(n) \equiv 0 \pmod{11^a}. \end{cases}$$

3 Mathieu Moonshine現象

さて最近，Mathieu moonshine現象が発見された [7]．$\vartheta_1(z;\tau)$ と $\mu(z;\tau)$ を次に定める関数とする：

$$\vartheta_1(z;\tau) = -\sum_{n=-\infty}^{\infty} e^{\pi i\tau(n+\frac{1}{2})^2+2\pi i(n+\frac{1}{2})(z+\frac{1}{2})},$$

$$\mu(z;\tau) = \frac{ie^{\pi iz}}{\vartheta_1(z;\tau)}\sum_{n\in\mathbf{Z}}(-1)^n\frac{q^{\frac{1}{2}n(n+1)}e^{2\pi inz}}{1-q^ne^{2\pi iz}}.$$

それらを用いて $\Sigma(\tau)$ を次のように定義する：

$$\begin{aligned}\Sigma(\tau) &:= 8\sum_{z\in\{1/2,\tau/2,(1+\tau)/2\}}\mu(z;\tau)\\ &= q^{-\frac{1}{8}}\left(2-\sum_{n=1}^{\infty}A(n)q^n\right)\ \text{(say)}\\ &= -q^{-\frac{1}{8}}(-2+90q+462q^2+1540q^3+4554q^4+11592q^5+27830q^6+\cdots).\end{aligned}$$

Mathieu moonshine現象とは最初の5個のフーリエ係数を2で割ったもの：

$$\{45, 231, 770, 2277, 5796\},$$

が24次のMathieu群 M_{24} の既約表現の次元に等しく，更に他の係数も M_{24} の既約表現の次元の正の整数係数線形結合で書けている，というものであった．このミステリアスな現象は，ごく最近になって，[9] によって証明された．(しかし，この現象の背景に存在するであろう代数構造までは，解明されていない．)

さて，このフーリエ係数の合同式を調べようということが目的である．筆者は，j-関数の様な合同式を持たないか調べる中で，j-関数の類似とも思える，次の合同式を発見した：

$$\begin{cases} n\equiv 1,2 \pmod 3 & \Rightarrow A(n)\equiv 0 \pmod 3\\ n\equiv 1,3 \pmod 5 & \Rightarrow A(n)\equiv 0 \pmod 5\\ n\equiv 2,3,5 \pmod 7 & \Rightarrow A(n)\equiv 0 \pmod 7\\ n\equiv 2,3,4,6,9 \pmod{11} & \Rightarrow A(n)\equiv 0 \pmod{11}\\ n\equiv 4,5,6,7,9,11,12,15,16,19,21 \pmod{23} & \Rightarrow A(n)\equiv 0 \pmod{23}. \end{cases} \tag{1}$$

モジュラー形式のフーリエ係数の合同式を示すには，スツルムの定理という強力な道具がある．スツルムの定理は，最初の有限項のみ合同式を確認すれば，全てのフーリエ係数で正しいことがわかることを主張する．しかし，$\Sigma(\tau)$ はもはやモジュラー形式でなく，モックテータ関数である．つまりスツルムの定理を用いることが出来ない．筆者は，Matthias Waldherr氏との共同研究において，スツルムの定理をモックテータ関数へ拡張し，これらの合同式を示した：

定理 3.1 ([10],[12]). (1) の合同式は正しい．

面白いことに，法として現れる素数は，$\sharp M_{24}$ を割る奇素数として特徴づけられる．
本稿の目的である偶素数2に関する合同式については後程述べる．

4 Mathieu Moonshine現象のMcKay–Thompson級数

さて，トレースが$\Sigma(\tau)$となるM_{24}-加群$K=\oplus_{n=-1}^{\infty}K_n$に対し，$M_{24}$の共役類$\ell X$の元$g$のMcKay-Thompson級数を定義しよう [6, 8]：

$$\Sigma_{\ell X}(\tau)=\sum_{n=-1}^{\infty}\mathrm{tr}(g|K_n)\,q^{n/8}=\sum_{n=-1}^{\infty}A_{\ell X}(n)\,q^{n/8}\ (\text{say}).$$

このとき [11] において，$A_{\ell X}(n)$も (1) と同じ型の合同式を持つことが示された．2つのtypeに分けているが，大雑把にいって$\Sigma_{\ell X}(\tau)$がモックテータ関数のとき "Type I"，モジュラー関数のとき "Type II"と名付けている：

定理 4.1. $g\in M_{24}$に対し$A_g(n)$は次の合同式を持つ：

- **Type I:**

1A

$$n\equiv\begin{cases}1 \pmod 3\\ 1,3 \pmod 5\\ 2,3,5 \pmod 7\\ 2,3,4,6,9 \pmod{11}\\ \begin{cases}4,5,6,7,9,\\ 11,12,15,16,19,21\end{cases}\pmod{23}\end{cases}\Rightarrow A_{1A}(n)\equiv 0\begin{cases}\pmod{3^2}\\ \pmod 5\\ \pmod 7\\ \pmod{11}\\ \pmod{23}.\end{cases}$$

2A

$$n\equiv\begin{cases}1 \pmod 3\\ 2,3,5 \pmod 7\end{cases}\Rightarrow A_{2A}(n)\equiv 0\begin{cases}\pmod 3\\ \pmod 7\end{cases}$$

3A

$$n\equiv\begin{cases}1,2 \pmod 3\\ 1,3 \pmod 5\end{cases}\Rightarrow A_{3A}(n)\equiv 0\begin{cases}\pmod 3\\ \pmod 5\end{cases}$$

5A

$$n\equiv\begin{cases}1 \pmod 3\\ 1,3 \pmod 5\end{cases}\Rightarrow A_{5A}(n)\equiv 0\begin{cases}\pmod 3\\ \pmod 5\end{cases}$$

7A

$$n\equiv\begin{cases}2 \pmod 3\\ 2,3,5 \pmod 7\end{cases}\Rightarrow A_{7A}(n)\equiv 0\begin{cases}\pmod 3\\ \pmod 7\end{cases}$$

6A

$$n \equiv 1 \pmod 3 \Rightarrow A_{6A}(n) \equiv 0 \pmod 3$$

11A

$$n \equiv 2,3,4,6,9 \pmod{11} \Rightarrow A_{11A}(n) \equiv 0 \pmod{11}$$

14A

$$n \equiv 2,3,5 \pmod 7 \Rightarrow A_{14A}(n) \equiv 0 \pmod 7$$

15A

$$n \equiv \begin{cases} 1 \pmod 3 \\ 1,3 \pmod 5 \end{cases} \Rightarrow A_{15A}(n) \equiv 0 \begin{cases} \pmod 3 \\ \pmod 5 \end{cases}$$

23A

$$n \equiv \begin{cases} 4,5,6,7,9, \\ 11,12,15,16,19,21 \end{cases} \pmod{23} \Rightarrow A_{23A}(n) \equiv 0 \pmod{23}$$

- **Type II:**

2B

$$n \equiv \begin{cases} 2 \pmod 3 \\ 1,3 \pmod 5 \end{cases} \Rightarrow A_{2B}(n) \equiv 0 \begin{cases} \pmod 3 \\ \pmod 5 \end{cases}$$

4A

$$n \equiv 1 \pmod 3 \Rightarrow A_{4A}(n) \equiv 0 \pmod 3$$

4C

$$n \equiv 1 \pmod 3 \Rightarrow A_{4C}(n) \equiv 0 \pmod 3$$

3B

$$n \equiv \begin{cases} 1,2 \pmod 3 \\ 2,3,5 \pmod 7 \end{cases} \Rightarrow A_{3B}(n) \equiv 0 \begin{cases} \pmod 3 \\ \pmod 7 \end{cases}$$

6B

$$n \equiv 2 \pmod 3 \Rightarrow A_{6B}(n) \equiv 0 \pmod 3$$

12B

$$n \equiv 2 \pmod 3 \Rightarrow A_{12B}(n) \equiv 0 \pmod 3$$

10A

$$n \equiv 1,3 \pmod 5 \Rightarrow A_{10A}(n) \equiv 0 \pmod 5$$

12A

$$n \equiv 1 \pmod 3 \Rightarrow A_{12A}(n) \equiv 0 \pmod 3$$

21A

$$n \equiv \begin{cases} 2 \pmod 3 \\ 2,3,5 \pmod 7 \end{cases} \Rightarrow A_{21A}(n) \equiv 0 \begin{cases} \pmod 3 \\ \pmod 7 \end{cases}$$

$A(n)(= A_{1A}(n))$ と同じく，法として現れる素数は，$\sharp C_{M_{24}}(\ell X)$ を割る奇素数として特徴づけられる [11]．更に他の奇素数に関しては，(1) のような合同式は持たないと予想される．この予想を解決することは，モックテータ関数と M_{24} との関係を更に明らかにするという意味において，大切な問題である．

5 フーリエ係数の偶奇性

では最後に，Fourier 係数の偶奇を調べたい．以下では，記号は [3] に従う．実は [10, 11, 12] において，偶奇は詳しく調べなかった．というのは，全ての ℓX に対し $2 | \sharp C_{M_{24}}(\ell X)$ であり，すると上に挙げた特徴づけを信じるならば，全ての ℓX に対し，$A_{\ell X}(n)$ の偶奇は規則的なはずである．確かに計算してみると，ほぼ全ての $A_{\ell X}(n)$ は偶数だが，しかし奇数も一部の ℓX に対し存在し，なかなか良い特徴づけが見つからなかったからである．ところが，[2] において提出された一つの予想と思わぬ関係が見つかり，それにより Fourier 係数の偶奇の特徴づけも成功したので報告する．その予想とは，次のようなものである：

予想 5.1 ([2], Conj. 5.11)．$n = \ell m^2 \equiv 7 \pmod 8$ とする．K_n は次の複素共役な既約表現のペアを含む：

- For $\ell = 7$, one of the pairs (χ_3, χ_4), (χ_{12}, χ_{13}) or (χ_{15}, χ_{16});
- for $\ell = 15$, the pair (χ_5, χ_6);
- for $\ell = 23$, the pair (χ_{10}, χ_{11}).

この予想に現れる数 "7, 15, 23" が，偶奇の特徴づけに必要だったのである．$A_{\ell X}(n)$ に関する偶奇性は，次のように述べられる：

定理 5.1 ([4]). M_{24} の共役類 ℓX に対し，$A_{\ell X}(n)$ が奇数である必要十分条件は，$\ell X \in \{7A, 7B, 14A, 14B, 15A, 15B, 23A, 23B\}$ かつ奇数 m を用いて，$n = \ell m^2$ と書ける，もしくは，$\ell X \in \{21A, 21B\}$ かつ 3 で割れない奇数 m を用いて，$n = \ell m^2$ と書けることである．

定理5.1を用いて，予想5.1を含むような次の系が得られた：

系 5.1 ([4]). $n = \ell m^2 \equiv 7 \pmod 8$ とする．$n = \ell m^2 \equiv 7 \pmod 8$ とする．K_n は次の複素共役な既約表現のペアを重複度奇数で含む：

- For $\ell = 7$, the total number of pairs (χ_3, χ_4) and (χ_{12}, χ_{13});
- for $\ell = 7$ and m divisible by 3, the pair (χ_{15}, χ_{16});
- for $\ell = 15$, the pair (χ_5, χ_6);
- for $\ell = 23$, the pair (χ_{10}, χ_{11}).

6 Remarks

- [2] により，Umbral Moonshine 現象が見つかった．この現象に現れるモックテータ関数に対しても数多くの興味ある合同式を発見している．特に，ラマヌジャンの発見した多数のモックテータ関数が登場し，それらのフーリエ係数の合同式に現れる法が，対応する群の位数と関係することも確認している．古典的なラマヌジャンのモックテータ関数が，由緒正しい有限群達と関係することが明らかになったのである．これについて，論文を作成中である．

- 証明について触れなかったが，簡単に述べておく．既に述べたように，保型形式のフーリエ係数の合同式を示す際，スツルムの定理 [13] を用いることは定石である．しかし，我々の考えている McKay–Thompson 級数は一般に保型形式でなくモックテータ関数なので，スツルムの定理が使えない．我々は，スツルムの定理をモックテータ関数に一般化することに成功した．それを用いてこれら数多くの合同式の証明に成功した．

  また，モックテータ関数となる McKay–Thompson 級数を，モジュラー形式や良く知られた形式の和として表示できる場合が，少なからずある．このような場合は，通常はスツルムの定理を使えばよい．

  詳しくは論文を参照して頂きたい [10, 12, 2].

参考文献

[1] R.E. Borcherds, Monstrous moonshine and monstrous Lie superalgebras, *Invent. Math.* **109** (1992), no. 2, 405–444.

[2] M. C. N. Cheng, J. F. R. Duncan and J. A. Harvey, Umbral Moonshine, preprint (2012), arXiv:1204.2779.

[3] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups, Oxford University Press, 1985.

[4] T. Creutzig, G. Höhn and T. Miezaki, The McKay-Thompson series of Mathieu Moonshine modulo two, submitted (2012), arXiv:1211.3703.

[5] J. H. Conway and S. P. Norton, Monstrous Moonshine, *Bull. Lond. Math. Soc.* **11** (1979), 308–339.

[6] T. Eguchi and K. Hikami, Note on twisted elliptic genus of $K3$ surface, *Phys. Lett. B* **694** (2011), no. 4-5, 446–455, arXiv:1008.4924.

[7] T. Eguchi, H. Ooguri and Y. Tachikawa, Notes on the $K3$ surface and the Mathieu group M_{24}, *Exp. Math.* **20** (2011), no. 1, 91–96, arXiv:1004.0956.

[8] M. R. Gaberdiel, S. Hohenegger and R. Volpato, Mathieu Moonshine in the elliptic genus of $K3$, *J. High Energy Phys.* (2010), no. 10, **062**, 24 pp, arXiv:1008.3778.

[9] T. Gannon, Much ado about Mathieu, preprint (2012), arXiv:1211.5531.

[10] T. Miezaki, On the Mathieu mock theta function, *Proc. Japan Acad. Ser. A Math. Sci.* **88** (2012), no. 2, 28–30.

[11] T. Miezaki, Congruences on the Fourier coefficients for mock theta functions, which relate finite groups, preprint.

[12] T. Miezaki, M. Waldherr, Congruence of the Fourier coefficients of the Mathieu mock theta function, submitted.

[13] K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[14] J.-P. Serre, *A course in arithmetic*, Translated from the French, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973.

Ternary Golay code が必勝形となる九つのゲーム

入江 佑樹 （千葉大学理学研究科）

ゲームの必勝形全体が良い組合せ構造を持つ場合があることが知られている [2]. 本稿では, そのような例として必勝形全体が ternary Golay code となるゲームを紹介する. さらに, その際に得られた線形性の判定条件も述べる.

1 ゲームの構成

まず, ゲームを構成しよう. 本稿ではゲームとは有向閉路を持たない有限有向グラフを指すことにする. $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ で位数 p (素数) の有限体を表し, $0 < 1 < \cdots < p-1$ で順序が入っているとする. 簡単のため, 線形空間 $\mathbb{F}_p^n$ の順序付基底 $(b_1, b_2 \ldots, b_n)$ を行列 $B := \begin{pmatrix} b_1 & b_2 & \cdots & b_n \end{pmatrix}^T$ で表すことにする.

基底 B を使って $\mathbb{F}_p^n$ に辞書式に順序を入れる. $\mathbb{F}_p^n$ の相異なる 2 つの元 $x = \sum x_i b_i, y = \sum y_i b_i$ に対して成分が異なる最大の添字を m とする ($m := \max\{i \in \{1, 2, \ldots, n\} \mid x_i \neq y_i\}$). このとき, もし $x_m < y_m$ ならば $x <_B y$ と定めることで $<_B$ は全順序になる. この順序 $<_B$ を B 順序と呼ぶことにする.

では, B 順序を用いてゲームを構成する. d を 2 以上の自然数とし, 頂点集合 V を $\mathbb{F}_p^n$ とする. 2 点 x, y に対して, x と y の Hamming 距離 $d(x, y)$ が d 未満でかつ $y <_B x$ のとき, x から y に矢を作る. すなわち, 辺集合 E を次とする:

$$E := \left\{ (x, y) \in V^2 \;\middle|\; y <_B x,\ d(x, y) < d \right\}.$$

この有向グラフ (V, E) は, B 順序で小さい方向にしか矢が走らないため, 有向閉路を持たない. 以下, 有向グラフ (V, E) を $\mathbb{F}_p$ 上の B 順序 d ゲームと呼ぶことにする.

このゲームは 2 人対戦のゲームで次のように遊ぶことができる. まず, 開始地点となる点 v_0 を選ぶ. 先手は, v_0 から $(v_0, v_1) \in E$ となる v_1 へ移動する. 後手は v_1 から $(v_1, v_2) \in E$ となる 点 v_2 へ移動する. あとはこの繰り返しで, 交互に点から点へと矢に沿って移動していき, 移動できる点がなくなった方が負けである.

2 必勝形

それでは, B 順序 d ゲームの後手必勝形全体を構成しよう. ここで後手必勝形とは, その点から始めると必ず後手が勝つことができる戦略がある点とする. 以下, 単に必勝形といった場合, 後手必勝形を指すことにする. $w(0) := (0, \cdots, 0) \in \mathbb{F}_p^n$ とする. そして, $w(m)$ を $w(0), w(1), \ldots, w(m-1)$ との距離が d 以上なものの中で, B 順序について最小のものと定義する. すなわち, 再帰的に次で定義する:

$$w(m) := \min_{<_B} \left\{ x \in \mathbb{F}_p^n \;\middle|\; d(x, w(i)) \geq d \ (0 \leq \forall i < m) \right\}.$$

ただし, 右辺の集合 $\left\{ x \in \mathbb{F}_p^n \;\middle|\; d(x, w(i)) \geq d \ (0 \leq \forall i < m) \right\}$ はいつかは空集合になるため, そのような最小の m を $m_0 + 1$ とし, $w(m_0 + 1)$ 以降は定義しないものとする. このとき $W := \{w(0), w(1), \ldots, w(m_0)\}$ が

ゲームの必勝形全体となる. 実際, まず $w(0)$ から始めたら必ず後手の勝ちのため, $w(0)$ は必勝形であることがわかる. ここで, W の点からは他の W の点へは移動できず, かつ, W に含まれない点からは W の点 へ移動できる. よって W の点から始めると, 後手は常に W の点に移動することができ, かつ, 先手は常に W の点に移動できない. さらに $w(0) \in W$ であることから, 後手はいつか $w(0)$ に移動できるため, W は必勝形である. また, W に含まれない点から始めると, 同様の方法で先手が必ず勝てるため, 必勝形全体は W になることがわかる.

3 ゲームと符号

$\mathbb{F}_2$ 上の B 順序 d ゲームの必勝形について次の結果が知られている [3, 2, 1].

定理 3.1 (Levenshtein '60, Conway-Sloan '86, Brualdi-Pless '93). $\mathbb{F}_2$ 上の B 順序 d ゲームの必勝形全体は線形符号になる.

この定理の $\mathbb{F}_p$ への一般化を次節で与える.

さて, 具体的にどのような線形符号が B 順序 d ゲームから得られるかというと, B を $\mathbb{F}_2$ 上の n 次単位行列とするとき, $n = 2^m, d = 4$ のとき extended Hamming code, $n = 24, d = 8$ のとき extended Golay code が得られる. それでは, ternary Golay code も同じように得られるのだろうか. 実際に同じように B を $\mathbb{F}_3$ 上の 12 次単位行列, $d = 6$ として必勝形全体を計算すると ternary Golay code にならないばかりか, 線形にもならないことがわかる. しかし, B を少しだけ変えることによって次の結果を得た:

定理 3.2. B_{ij} を $\mathbb{F}_3$ 上の 12 次単位行列の (i, j) 成分を 1 に変えた行列とする. このとき B_{ij} 順序 6 ゲームの必勝形全体が線形となる必要十分条件は $i = 1, 2, \ldots, 9$ かつ $j = 10$ である. さらに, これら 9 つの符号は全て, extended ternary Golay code になる.

すなわち下の X の部分に 1 を 1 つだけいれたとき, extended ternary Golay code が得られる.

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & X & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & X & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & X & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & X & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & X & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & X & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & X & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & X & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & X & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix}$$

4 線形性の判定条件

上の定理を示すにはいつ線形になるかが判定できれば良い. そこで判定条件を与えるため, 記号を準備する. $\{ 0^{M_0}, 1^{M_1}, \ldots, (p-1)^{M_{p-1}} \}$ によって $\alpha \in \mathbb{F}_p$ を M_α 個含む多重集合を表すことにする. また, 部分集合に元の和が 0 となるものをもつ多重集合全体を $\mathcal{M}_0$ で表す:

$$\mathcal{M}_0 := \left\{ M = \{ 0^{M_0}, 1^{M_1}, \ldots, (p-1)^{M_{p-1}} \} \mid \emptyset \neq \exists \{0^{N_0}, \ldots, (p-1)^{N_{p-1}}\} \subset M \text{ s.t. } \sum_{\alpha \in \mathbb{F}_p} N_\alpha \alpha = 0 \right\}.$$

このとき次で線形性を判定できる:

定理 4.1. B 順序 d ゲームの必勝形全体 W が線形になる必要十分条件は, 任意の $\sum_{i=0}^{k} a_i p^i \in \mathcal{I}$ に対して次が成り立つことである:

$$w\left(\sum_{i=0}^{k} a_i p^i\right) = a_k w\left(p^k\right) + w\left(\sum_{i=0}^{k-1} a_i p^i\right).$$

但し, 基底 B を使って $w(m) = \sum w(m,j) b_j$ と表すとき, $\mathcal{I}$ は次の集合である:

$$\mathcal{I} := \left\{ \sum_{i=0}^{k} a_i p^i < \#W \;\middle|\; \exists j \text{ s.t. } \{w(p^0,j)^{a_0}, \ldots, w(p^k,j)^{a_k}\} \notin \mathcal{M}_0 \right\}.$$

この定理の判定条件は少し複雑だが, 主張を弱めると次のわかりやすい判定条件が得られる:

系 4.2. B 順序 d ゲームの必勝形全体 W が線形になる必要十分条件は, 任意の $\sum_{i=0}^{k} a_i \leq p-1$, $\sum_{i=0}^{k} a_i p^i < \#W$ に対して次が成り立つことである:

$$w\left(\sum_{i=0}^{k} a_i p^i\right) = a_k w\left(p^k\right) + w\left(\sum_{i=0}^{k-1} a_i p^i\right).$$

すなわち, 係数の和が $p-1$ 以下の部分だけ確認すれば良い. 例えば, $p=3$ の場合は $w(3^k+3^h) = w(3^k)+w(3^h)$ ならば線形符号であるため, ternary Golay code の定理を示す際には, この部分だけ確認すれば良い. また, 上述した $p=2$ の場合に線形符号になることもここからわかる.

最後に, d を変えて同じことを行うとどこまで線形符号が得られるか, 調べた結果を紹介する. $k(n,d,i,j)$ で $\mathbb{F}_p$ 上 n 次の B_{ij} 順序 d ゲームの必勝形の次元を表すことにする. ただし, 線形でない場合はその次元は 0 とする. さらに, $h_d := \max\{k(n,d,i,i) \mid 1 \leq i \leq n\}$, $k_d := \max\{k(n,d,i,j) \mid 1 \leq i \leq n, 1 \leq j \leq n\}$ とすると次の結果が得られた:

定理 4.3.

$$h_d \begin{cases} = 1 & (d \equiv 1,2 \pmod 3), \\ \leq 3 & (d \equiv 0 \pmod 3). \end{cases}$$

$$k_d \begin{cases} = 1 & (d \equiv 1,2 \pmod 3, d \neq 5), \\ \leq 3 & (d \equiv 0 \pmod 3, d \neq 6), \\ = 6 & (d = 5,6). \end{cases}$$

すなわち, 今回の方法では ternary Golay code 以外には次元の高い線形符号は得られない.

参考文献

[1] R. Brualdi and V. S. Pless. Greedy codes. *Journal of Combinatorial Theory, Series A*, 64(1):10–30, Sept. 1993.

[2] J. H. Conway and N. J. A. Sloane. Lexicographic codes: Error-correcting codes from game theory. *IEEE Transactions on Information Theory*, 32(3):337–348, May 1986.

[3] V. Levenshtein. A class of systematic codes. *Soviet Mathematics Doklady*, 1(1):368–371, 1960.

多重p-角形の置換群について

筑波大学数理物質科学研究科数学専攻博士前期課程
山口 正男

1 導入

有限群Gに対して、Gの自己同型写像全体を$Aut(G)$とし、整数p個のGの直積群を$G^{\times p}$とする。さらに、Gの元で位数が整数nの約数であるもの全体を$\Omega_n(G)$とする(つまり$\Omega_n(G)=\{g\in G|g^n=e\}$)。以下、$p$を奇素数とする。さらに、位数$p$の巡回群を$C_p$とし、その生成元を一つとり$\sigma_p$とする。この時有限群$G$に対して、次のような$C_p$から$Aut(G^{\times p})$への自然な単射$\phi:C_p\to Aut(G^{\times p})$が存在する。

$$\phi(\sigma_p)(g_1,g_2,\cdots,g_p):=(g_{\tau(1)},g_{\tau(2)},\cdots,g_{\tau(2)})=(g_p,g_1,\cdots,g_{p-1})$$

(ここでτは巡回置換$(1,p,\cdots,2)$とする。) これより、$G^{\times p}$とC_pに半直積が定義でき、その半直積群を$G\wr C_p$とする。ここで、さらに、$G\wr C_p$の元を次のように表す。

$$(g_1,g_2,\cdots,g_p;g)$$

(ここで、$g_i\in G, g\in C_p$) このとき、次のように帰納的に$G_p(n)$を定義する。

定義 1.1 $G_p(1)$をC_pとする。$n\geq 2$に対して、$G_p(n)$を次の$L_{p,n}$と$R_{p,n}$で生成された$G_p(n-1)\wr C_p$の部分群とする。

$$L_{p,1}:=\sigma_p\in G_p(1)\quad and\quad L_{p,n}:=(L_{p,n-1},e,\cdots,e;\sigma_p)$$

$$R_{p,1}:=\sigma_p{}^{-1}\in G_p(1)\quad and\quad R_{p,n}:=(R_{p,n-1},e,\cdots,e;\sigma_p{}^{-1})$$

以下、この$G_p(n)$の性質について詳しい証明はせず述べる。さらに$G_p(n)$が作用する多重p-角形についても割愛するが最後に$G_5(1)$、$G_5(2)$と$G_5(3)$が作用する多重五角形のグラフを載せておく。さて$n\geq 2$に対して、この$G_p(n)$は非可換な二元生成p-群であることは簡単な計算によりわかる。さて有限群Gに対して$G^{\times p}$は$G\wr C_p$の正規部分群と同一視でき、この同一視により$G\wr C_p$の部分群Hに対して、$H\cap G^{\times p}$はHの正規部分群となる。

定義 1.2 これより$n\geq 2$に対して、$G_p(n)\cap G_p(n-1)^{\times p}$は$G_p(n)$の正規部分群となり、この部分群を$H_p(n)$と表す。さらに、$G_p(n)$の交換子群を$G_p{}'(n)$と表す。

補題 1.3 $n\geq 2$に対して$G_p(n)$と$H_p(n)$の指数はpである。

さらに、$g \in G_p(n)$ に対して $g^{L_{p,n}}$ と $g^{R_{p,n}}$ は次のようになる。

$$g^{L_{p,n}} = \begin{cases} (g_2, \cdots, g_p, (g_1)^{L_{p,n-1}}; e) & if \quad i = 0 \\ (g_2, \cdots g_{i+1} L_{p,n-1}, \cdots, g_p, L_{p,n-1}^{-1} g_1; \sigma_p^i) & if \quad i \neq 0 \end{cases}$$

$$g^{R_{p,n}} = \begin{cases} (g_p, (g_1)^{R_{p,n-1}}, g_2 \cdots, g_{p-1}; e) & if \quad i = 0 \\ (g_p R_{p,n-1}, R_{p,n-1}^{-1} g_1, g_2, \cdots, g_{p-1}; {\sigma_p}^{-1}) & if \quad i = p-1 \\ (g_p, R_{p,n-1}^{-1} g_1, g_2, \cdots g_{i+1} R_{p,n-1}, \cdots, g_{p-1}; {\sigma_p}^i) & if \quad i \neq 0, p-1 \end{cases}$$

証明 定義 1.1 から、直接計算によりわかる。□

2 $G_p(n)$ とその部分群

ここでは $G_p(2)$ の構造を決定する。まず、定義より $G_p(2)$ は $G_p(1) \wr C_p$ の部分群であり

$$|G_p(n)| \leq p^{p+1}$$

$$|L_{p,2}| = |R_{p,2}| = p^2$$

である。さて、定義 1.2 から $H_p(2)$ は ${C_p}^{\times p}$ の部分群である。この時、

$$L_{p,2} R_{p,2} = (\sigma_p, \sigma_p^{-1}, e, \cdots, e; e) \in H_p(2)$$

である。特に、補題 1.3 から $H_p(2)$ は ${C_p}^{\times p-1}$ と同型であり、$G_p(2)$ の位数は p^p である。さらに、簡単な計算により $G_p(2)$ の中心は $L_{p,2}^p$ で生成された位数 p の巡回群である。

次に $G_p(2)$ の交換子群 ${G_p}'(2)$ について考察する。$G_p(2)$ が二元生成であるため ${G_p}'(2)$ は $[L_{p,2}, R_{p,2}]$ の $G_p(2)$-共役類で生成される $H_p(2)$ の部分群である。つまり、

$${G_p}'(2) = \{[L_{p,2}, R_{p,2}]^g | g \in G_p(2)\} \subset H_p(2)$$

である。さらに

$$[L_{p,2}, R_{p,2}] = (\sigma_p^2, \sigma_p^{-1}, e, \cdots, e, \sigma_p^{-1}; e)$$

より、補題 1.3 から ${G_p}'(2)$ の位数は p^{p-2} である。特に次が成り立つ。

$$H_p(2)/{G_p}'(2) = \langle L_{p,2} R_{p,2} {G_p}'(2) \rangle \simeq C_p$$

$$G_p(2)/{G_p}'(2) = \langle L_{p,2} {G_p}'(2) \rangle \times \langle L_{p,2} R_{p,2} {G_p}'(2) \rangle \simeq {C_p}^{\times 2}$$

上記をまとめると

命題 2.1 p を奇素数とする。このとき、$G_p(2)$ は位数 p^p の二元生成非可換群であり、$\Omega_p(G_p(2))$ はちょうど $H_p(2)$ である。さらに

$$G_p(2)/{G_p}'(2) = \langle L_{p,2}{G_p}'(n)\rangle \times \langle L_{p.2}R_{p.2}{G_p}'(2)\rangle \simeq {C_p}^{\times 2}$$
$$H_p(2)/{G_p}'(2) = \langle L_{p.2}R_{p.2}{G_p}'(2)\rangle \simeq C_p$$
$$Z\left(G_p(2)\right) = \langle L_{p.2}^p\rangle \simeq C_p$$

である。

特に、$n \geq 3$ に対しても次のような命題 2.1 と同様のことが成り立つ。

定理 2.2 $n \geq 2$ に対して次が成り立つ。

(1) $G_p(n)$ は指数 p^n の二元生成 p-群

(2) $\Omega_p(G_p(n))$ が $G_p(n)$ の基本アーベル正規 p-部分群である。さらに q を p 冪とすると $\Omega_q(G_p(n))$ が $G_p(n)$ の部分群となる。

(3) $\ker(\pi_n) = \Omega_p(G_p(n))$

(4) $G_p(n)$ の中心が常に $(L_{p,n})^{p^{n-1}}$ (もしくは $(R_{p,n})^{p^{n-1}}$) で生成される位数 p の巡回群である。

ここで、$\pi_n\colon G_p(n) \to G_p(n-1)$ は次のような準同型写像である。

$$\pi_n\colon G_p(n) \to G_p(n-1)$$
$$L_{p,n} \mapsto L_{p,n-1}$$
$$R_{p,n} \mapsto R_{p,n-1} \qquad for \quad n \geq 2$$

証明 定義から明らかに (1) が成り立ち、π_n は全射準同型である。さらに命題 2.1 より、$n = 2$ のときは示された。故に、$n \geq 3$ とし帰納的に示す。

(2) と (3) については、次の等式から得られる。

$$\pi_n = (\pi_{n-1}, \pi_{n-1}, \cdots, \pi_{n-1}; 1)$$

この等式は定義から明らかである。

さて、g を $Z(G_p(n))$ の元とすると、$\pi_n(g)$ は $Z(G_p(n-1))$ の元である。特に $Z(G_p(n-1))$ は $H_p(n-1)$ の部分群であるから、$\pi_n(g)$ は $H_p(n-1)$ の元である。故に、g は $H_p(n)$ の元である。さらに、帰納法の仮定から g は次のように表せる。

$$g = (g_1, g_2, \cdots, g_p; e) \quad (g_i \in Z(G_p(n-1)), 1 \leq i \leq p)$$

あとは、$g_i = g_j (1 \leq i, j \leq p)$ を示せば十分であるが、補題 1.3 から明らかである。□

(ここで $(L_{p,n})^{p^{n-1}}$ の逆元はちょうど $(R_{p,n})^{p^{n-1}}$ である。)

3 $G_p(n)$ の位数

最後に $G_p(n)$ の位数と $G_p(n)/G_p'(n)$ の構造を決定する。既に、命題 2.1 で $n=2$ のときは示した。$n \geq 3$ に関して、位数と構造を決定するためにいくつかの補題を紹介する。以下、$n \geq 3$ とする。

補題 3.1 $H_p(n) = \langle (L_{p,n})^p, (R_{p,n})^p, (L_{p,n})^i (R_{p,n})^i | 1 \leq i \leq p-1 \rangle$

補題 3.2 $H_p'(n) = \left(G_p'(n-1)\right)^{\times p}$ であり、$(L_{p,n})^p H_p'(n)$ と $(R_{p,n})^p H_p'(n)$ は $G_p(n)/H_p'(n)$ の中心に含まれる。

補題 3.3 さらに、$g_{p,n}(0) = (g_1, g_2, \cdots, g_p; \tilde{g})$ を次のように定める。

$$\begin{aligned} g_{p,n}(1) =& (g_1, g_2, \cdots, g_p; \tilde{g}) \\ :=& \left(L_{p,n}(n-1)H_p'(n), R_{p,n-1}{L_{p,n}}^{-1}(n-1)H_p'(n), {R_{p,n}}^{-1}(n-1)H_p'(n), e, \cdots, e; e\right) \end{aligned}$$

さらに、$2 \leq i \leq p$ に対して

$$g_{p,n}(i) := (g_{\tau^{i-1}(1)}, g_{\tau^{i-1}(2)}, \cdots, g_{\tau^{i-1}(p)}; e)$$

とする。(ここで $\tau = (1, p, \cdots, 2)$ であった。)

この時、$\{g_{p,n}(i)\}_{1 \leq i \leq p-1}$ は $G_p'(n)/H_p'(n)$ を生成する。

これらの補題と先の命題から次の定理が成り立つ。

定理 3.4 $n \geq 2$ に対して、$G_p(n)/G_p'(n)$ はそれぞれ位数が $p^{\lfloor \frac{n+1}{2} \rfloor}$ と $p^{\lfloor \frac{n}{2} \rfloor}$ の二つの巡回群 $\langle L_{p,n} G_p'(n) \rangle$ と $\langle L_{p,n} R_{p,n} G_p'(n) \rangle$ の直積である。さらに次が成り立つ。

$$H_p(n)/G_p'(n) \simeq G_p(n-1)/G_p'(n-1) \tag{3.1}$$

and

$$G_p'(n)/H_p'(n) \simeq \left(G_p(n-1)/G_p'(n-1)\right)^{\times \frac{p-1}{2}} \tag{3.2}$$

である。(ここで $[\,]$ は Gauss 記号とする。)

証明 命題 2.1 から $n=2$ の場合は既に示されている。故に、$n \geq 3$ として帰納的に示す。さて、帰納法の仮定から

$$\begin{aligned} G_p(n)/G_p'(n-1) &= \langle L_{p,n-1} G_p'(n-1) \rangle \times \langle L_{p,n-1} R_{p,n-1} G_p'(n-1) \rangle \\ &\simeq \mathbb{Z}_{p^{\lfloor \frac{n}{2} \rfloor}} \times \mathbb{Z}_{p^{\lfloor \frac{n-1}{2} \rfloor}} \end{aligned}$$

である。このとき、$G_p(n)/G_p'(n-1)$ から $\mathbb{Z}_{p^{\lfloor \frac{n}{2} \rfloor}} \times \mathbb{Z}_{p^{\lfloor \frac{n-1}{2} \rfloor}}$ への自然な同型写像を ι とする。さらに、補題 3.2 から $H_p(n)/H_p'(n)$ は $\left(G_p(n-1)/G_p'(n-1)\right)^{\times p}$ の部分群と同一視することによって、$H_p(n)/H_p'(n)$ から $\left(\mathbb{Z}_{p^{\lfloor \frac{n}{2} \rfloor}} \times \mathbb{Z}_{p^{\lfloor \frac{n-1}{2} \rfloor}}\right)^{\prime p}$ への自然な単射準同型 $\tilde{\iota}$ がある。

$$\begin{aligned} \tilde{\iota} : H_p(n)/H_p'(n) &\longrightarrow \left(\mathbb{Z}_{p^{\lfloor \frac{n}{2} \rfloor}} \times \mathbb{Z}_{p^{\lfloor \frac{n-1}{2} \rfloor}}\right)^{\prime p} \\ (\tilde{g_1}, \tilde{g_2}, \cdots, \tilde{g_p}; e) &\longmapsto (\iota(\tilde{g_1}), \iota(\tilde{g_2}), \cdots, \iota(\tilde{g_p})) \end{aligned}$$

この時 $\iota(L_{p,n-1}G_p{}'(n)) = (1,0)$ と $\iota(R_{p,n-1}G_p{}'(n)) = (-1,1)$ であるから $L_{p,n}R_{p,n}H_p{}'(n)$ の像は次のようになる（ここで、ι による像の第一成分は $\mathbb{Z}_{p^{[\frac{n}{2}]}}$ とし、第二成分は $\mathbb{Z}_{p^{[\frac{n-1}{2}]}}$ である)。

$$\tilde{\iota}(L_{p,n}R_{p,n}H_p{}'(n)) = ((1,0),(-1,1),(0,0),\cdots,(0,0))$$

である。
さて、初めに (3.2) を示す。補題 3.3 から $\{g_{p,n}(i)\}_{1\leq i\leq p-1}$ は $G_p{}'(n)/H_p{}'(n)$ の生成元である。さらに、$\{g_{p,n}(i)\}_{1\leq i\leq p-1}$ の定義から

$$\tilde{\iota}(g_{p,n}(1)) = ((1,0),(-2,1),(1,-1),(0,0),\cdots,(0,0))$$

$$\begin{aligned}\sum_{i=1}^{p-1} a_i\tilde{\iota}(g_{p,n}(i)) =&((a_1+a_{p-1},-a_{p-1}),(-2a_1+a_2,a_1),(a_1-2a_2+a_3,-a_1+a_2)\\ &,\cdots,(a_j-2a_{j+1}+a_{j+2},-a_j+a_{j+1}),\cdots\\ &,(a_{p-3}-2a_{p-2}+a_{p-1},-a_{p-3}+a_{p-2}),(a_{p-2}-2a_{p-1},-a_{p-2}+a_{p-1}))\end{aligned}$$

(ここで、$a_i \in \mathbb{Z}$) である。このとき、$h_{p,n}(1)$ を $\prod_{i=1}^{p-1}(g_{p,n})^i$ とすると

$$\begin{aligned}\tilde{\iota}(h_{p,n}(1)) &= \sum_{i=1}^{p-1} i\tilde{\iota}(g_{p,n}(i))\\ &= ((p,1-p),(0,1),\cdots,(0,1),(-p,1))\end{aligned}$$

である。$h_{p,n}(1) = (h_1,h_2,\cdots,h_p;e)$ とするとき、$\{h_{p,n}(i)\}_{2\leq i\leq p-1}$ を次のように定める。

$$h_{p,n}(i) := (h_{\tau^{i-1}(1)},h_{\tau^{i-1}(2)},\cdots,h_{\tau^{i-1}(p)};e) \ for\ 2\leq i\leq p-1$$

この時、$\tilde{\iota}$ による像の各成分を比較すると $\{g_{p,n}(2i-1),h_{p,n}(2i-1)\}_{1\leq i\leq\frac{p-1}{2}}$ は $G_p{}'(n)/H_p{}'(n)$ の独立生成系であることがわかる。さらに $g_{p,n}(i)$ と $h_{p,n}(i)$ の位数はそれぞれ $p^{[\frac{n}{2}]}$ と $p^{[\frac{n-1}{2}]}$ であるから (3.2) が成り立つ。
次に (3.1) を示す。簡単な計算により $(L_{p,n})^pG_p{}'(n)$ と $L_{p,n}R_{p,n}G_p{}'(n)$ の位数はそれぞれ $p^{[\frac{n-1}{2}]}$ と $p^{[\frac{n}{2}]}$ であり

$$\begin{aligned}\langle L_{p,n}R_{p,n}H_p{}'(n)\rangle \cap G_p{}'(n)/H_p{}'(n) &= \{e\}\\ \langle (L_{p,n})^pH_p{}'(n)\rangle \cap G_p{}'(n)/H_p{}'(n) &= \langle (L_{p,n})^{p^{(1+[\frac{n-1}{2}])}}H_p{}'(n)\rangle\\ \langle L_{p,n}R_{p,n}G_p{}'(n)\rangle \cap \langle (L_{p,n})^pG_p{}'(n)\rangle &= \{e\}\end{aligned}$$

である。
これより

$$H_p(n)/G_p{}'(n) = \langle (L_{p,n})^pG_p{}'(n)\rangle \times \langle L_{p,n}R_{p,n}G_p{}'(n)\rangle$$

である。さらに $G_p(n)$ と $H_p(n)$ の指数が p より

$$G_p(n)/{G_p}'(n) = \langle L_{p,n}{G_p}'(n)\rangle \times \langle (L_{p,n}R_{p,n}){G_p}'(n)\rangle$$

であり、$L_{p,n}{G_p}'(n)$ と $(L_{p,n}R_{p,n}){G_p}'(n)$ の位数はそれぞれ $p^{[\frac{n+1}{2}]}$ と $p^{[\frac{n}{2}]}$ である。 □

故に定理 3.4 から、$G_p(n)$ の位数に関して次のような漸化式が得られる。

系 3.5 $|G_p(1)| = p, |G_p(2) = p^p$ である。さらに $n \geq 3$ に対して

$$|G_p(n)| = p|G_p(n-1)|^p / p^{\frac{(n-1)(p-1)}{2}}$$

である。

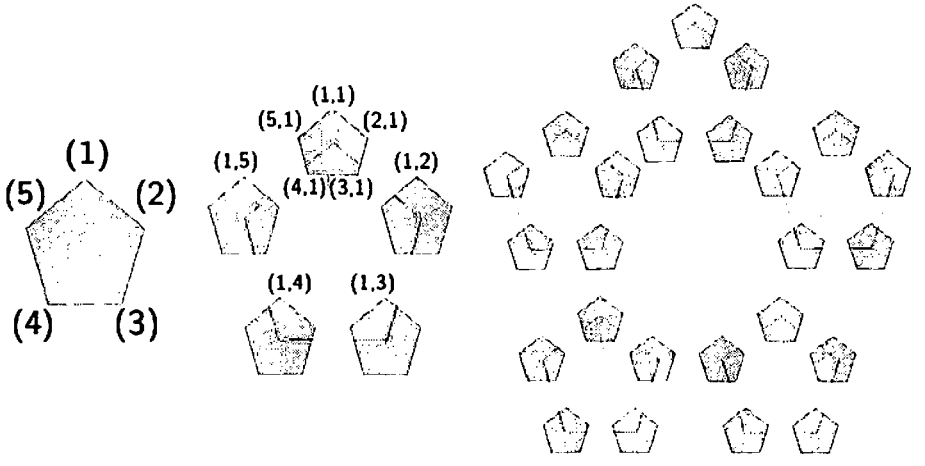
さらに、この漸化式を解くことにより $G_p(n)$ の位数は

$$|G_p(1)| = p$$
$$|G_p(2)| = p^p$$
$$|G_n| \text{の指数} = p^{n-1} - p^{n-2} + \frac{1}{2}\sum_{k=0}^{n-3} p^k + \frac{n}{2} \ (n \geq 3)$$

である。

4 備考

$p = 5$ のときの $G_5(1)$、$G_5(2)$ と $G_5(3)$ が作用する多重五角形はそれぞれ以下のグラフである。



$G_5(1)$ $G_5(2)$ $G_5(3)$

Dudeneyの円卓問題 − A survey −

静岡県立大学　小林みどり

1 Dudeneyの円卓問題とは

Dudeneyの円卓問題とは次の問題である.

「n 人の人を何回か円卓に座らせる. その際, どの人についても, 自分以外の任意の2人が自分の両隣りにちょうど1回くるようにしたい. その座らせ方を求めよ.」

このように n 人を座らせるには, 自分以外の任意の2人を選ぶ選び方の数である ${}_{n-1}C_2$ 回座らせる必要がある.

Dudeneyの円卓問題の解は, n が小さいときは次のように求められる. n 人の人を $1,2,\ldots,n$ とする. $n=3$ のときは1回座らせればよく, 解は $\{(1,2,3)\}$ であり, $n=4$ のときは3回で, 解は $\{(1,2,3,4),(1,2,4,3),(1,3,2,4)\}$ である. ここで, $(1,2,3,4)$ 等は巡回列を表しており, 4から1へ戻るものとする. $n=5$ のときは6回で, 解は $\{(1,2,3,4,5),(1,2,4,5,3),(1,2,5,3,4),(1,3,2,5,4),(1,4,2,3,5),(1,5,2,4,3)\}$ であり, $n=6$ のときは10回で, 解は $\{(1,2,3,6,4,5),(1,3,4,2,5,6),(1,4,5,3,6,2),(1,5,6,4,2,3),(1,6,2,5,3,4),(1,2,4,5,6,3),(1,3,5,6,2,4),(1,4,6,2,3,5),(1,5,2,3,4,6),(1,6,3,4,5,2)\}$ などである.

すべての n について, このような座らせ方があるか, あればそれを求めよ, というのが問題であり, 現在まで未解決の問題である.

グラフの言葉では, Dudeneyの円卓問題とは次の集合を求める問題である.「完全グラフ K_n のすべての2-path（長さ2のpath）をちょうど1回ずつ含むHamilton cycleの集合を求めよ.」このようなHamilton cycleの集合をDudeney setと呼ぶ. つまり, Dudeneyの円卓問題とは, すべての n について K_n のDudency setを求める問題である.

2 Dudeneyの円卓問題の歴史

1899年, Judsonが Amer. Math. Monthly に次の問題を載せた [14].

「7人の人が, 夏にリゾートで会った. 毎日1回, 7人で円卓を囲んで会食する. その際, テーブルの席順は, どの人についても, 自分以外の任意の2人が自分の両隣りにちょうど1回くるようにする (左右は無視する). こうして15日間滞在した. この席順を示せ.」

翌1900年, Judsonが同じ Amer. Math. Monthly に,「7人のときの解が得られないため, 6人と8人の解を示す」として, 6人と8人の解を載せた [15]. Editorが, 7人のときの解に懸賞をつけた (懸賞は, この雑誌の1年間無料購読であった).

1904年, Saffordが Amer. Math. Monthly に7人のときの解を示し, 7人のときの解はuniqueであると予想した. またJudsonの6人の解の別解を示し, 6人の解はこの2個のみであろうと述べた [32]. 実際に, この2個の解は非同型であり, 6人の解はこの2個のみであることが, SaffordとDicksonにより示された [33, 5].

1905年, Dicksonは Judsonの問題を n 人の場合に一般化し, 群論を用いて考察し, $n=4,5,6,8,10,12$ の解を求めた [6].

同じ1905年にDudeneyは，イギリスの新聞 Daily Mail に6人の問題を載せた．1907年，Dudeneyは自著“Canterbury Puzzles”[7] (No. 90) に7人の問題を載せた．その中で，「この問題は，Bergholtが$n = p + 1$のときに解いた．Bewleyはすべての偶数について解をみつけた．そして，ついに私が，すべての数について解をみつけた.」と書いている．

1917年，Dudeneyは彼の本“Amusements in Math.”[8] (No. 273) にもn人の問題を載せた．しかし，その本には，Bewleyがすべての偶数について解をみつけたことも自分がすべての数について解を見つけたことも書かれていない．その後もDudeneyは解を発表していないようである．このようなわけで現在でも解は分からないままである．そのため，次をDudeneyの予想と呼ぶことにする．

Dudeneyの予想 Dudeneyの円卓問題は，すべてのnに対して解が存在する．

3 Dudeneyの円卓問題が解けているn

本節では，Dudeneyの円卓問題が解けているnを，解決された時間順に並べる．

1. $n = p + 1$ (p is a prime) [1]
2. $n = 2p$ (p is a prime) [30, 2, 3] [2]
3. $n = p^e + 1$ (p is a prime, $e \geq 1$) [31]
4. $n = p + 2$ (p is an odd prime and 2 is a primitive root of $GF(p)$) [9]
5. $n = p^e + 1$, $n = pq + 1$ (p, q are odd primes, $e \geq 1$); $n = p^e q^f + 1$ (p, q are odd primes with $p \geq 5$, $q \geq 11$, and $e, f \geq 1$) [10]
6. n is even [17]
7. $n = p + 2$ (p is an odd prime and -2 is a primitive root of $GF(p)$) [16]
8. $n = p + 2$ (p is an odd prime, 2 is the square of a primitive root of $GF(p)$ and $p \equiv 3 \pmod 4$) [16]
9. $n = p + 2$ (p is an odd prime, 2 is the square of a primitive root of $GF(p)$, $p \equiv 1 \pmod 4$, 3 is not a quadratic residue modulo p) [21]
10. $n = p + 2$ (p is an odd prime, -2 is the square of a primitive root of $GF(p)$, and either

    (10-1) $p \equiv 1 \pmod 4$ and 3 is not a quadratic residue modulo p, or

    (10-2) $p \equiv 3 \pmod 4$ [21]

[1] 文献は [13, 35] などがあるが，$n = p + 1$ (p is a prime) のときは，古くからいろいろな人により解かれていると思われる．

[2] Nakamura は [30] において perfect 1-factorization (P1F) を定義し，P1F から Dudeney set が導かれることを示し，K_{p+1} と K_{2p} の P1F を構成した．Anderson は [2, 3] において K_{p+1} と K_{2p} の P1F を構成した．

11. some sporadic cases ($n = 11, 23, 45$ [9]; $27, 29, 35, 37$ [29]; $75, 91$ [18]).

以上をまとめると，n が even のとき Dudeney の円卓問題は解けているが，n が odd のときは，$n = 2^e + 1$ $(e \geq 1)$ と，$n = p + 2$ (p is an odd prime) の一部が解けているのみである．ただし，n が odd のとき，「二重」の解は得られている [20]．ここで「二重」の解とは，もともとの問題の「ちょうど 1 回」を「ちょうど 2 回」に変えた問題の解のことである．

4 Dudeney design – Dudeney の円卓問題の一般化 –

Dudeney の円卓問題とは，前述したように，完全グラフ K_n の Dudeney set を求める問題であり，一言でいえば「完全グラフにおける Hamilton cycle による 2-path の uniform covering」を求める問題である．

この問題における完全グラフを，完全二部グラフや完全有向グラフに変えたり，Hamilton cycle を，Hamilton path，k-cycle，k-circuit，k-path に変えた問題を考えることは自然なことである．そのため，次のように Dudeney design を定義する[3]．G を graph，H を G の subgraph とするとき，Dudeney design $D(G, H, \lambda)$ とは，H と同型な G の subgraphs の集まりであり，その中にグラフ G のすべての 2-path がちょうど λ 回ずつ含まれているものである．Dudeney design $D(G, H, \lambda)$ が resolvable であるとは，その subgraph の集まりが，いくつかの class に分解でき，それぞれの class には K_n の頂点が 1 回ずつ含まれているもののことである．それぞれの class を parallel class と呼ぶ．

本稿では，G が完全グラフ K_n，完全二部グラフ $K_{n,n}$ の場合，そして H が Hamilton cycle，Hamilton path，k-cycle C_k，k-path P_k の場合について考える．ここで，k-cycle とは頂点数 k のサイクル（長さ k のサイクル），k-path とは頂点数 k のパス（長さ $k-1$ のパス）のことである．なお Dudeney の円卓問題は $D(K_n, C_n, 1)$ design を求める問題のことである．

5 Dudeney design についての知られている結果

次の Dudeney design はすでに解決されている．「解決されている」とは，その design が存在するための必要十分条件が得られていることである．

1. $D(K_n, P_3, \lambda)$ designs (trivial) and resolvable $D(K_n, P_3, \lambda)$ designs [11] (Th. 2.9)
2. $D(K_n, C_3, \lambda)$ designs (trivial) and resolvable $D(K_n, C_3, \lambda)$ designs [11] (Th. 2.9)
3. $D(K_n, P_4, 1)$ designs [11] (Th. 2.20)
4. $D(K_n, C_4, \lambda)$ designs [12] and resolvable $D(K_n, C_4, 1)$ designs [23]
5. $D(K_n, P_5, 1)$ designs [24]
6. $D(K_n, P_6, 1)$ designs [27, 28]

[3] Heinrich らは，さらに一般化して (G, H, K, λ)-design を定義した [11].

7. $D(K_n, C_6, 1)$ designs [25]

8. $D(K_n, P_7, 1)$ designs [1]

9. $D(K_{n,n}, P_4, 1)$ designs and resolvable $D(K_{n,n}, P_4, 1)$ designs [11] (Th. 3.3)

10. $D(K_{n,n}, C_4, 1)$ designs and resolvable $D(K_{n,n}, C_4, 1)$ designs [11] (Th. 3.1)

11. $D(K_{n,n}, P_{2n}, \lambda)$ designs [26].

以下の Dudeney design については，次のように部分的に解決されている．

1. $D(K_n, C_n, 1)$ design は n が even のとき存在し [17]，n が odd のとき $D(K_n, C_n, 2)$ design が存在する [20].

2. $D(K_n, P_n, 1)$ design は $n \equiv 0, 1, 3 \pmod 4$ のとき存在し，$n \equiv 2 \pmod 4$ のとき $D(K_n, P_n, 2)$ design が存在する [26].

3. $D(K_{n,n}, C_{2n}, 1)$ design は $n \equiv 0, 1, 3 \pmod 4$ のとき存在し，$n \equiv 2 \pmod 4$ のとき $D(K_{n,n}, C_{2n}, 2)$ design が存在する [26].

6 Dudeney design に関する open problems

本節では Dudeney design に関する主な未解決問題について述べる．最初の 3 つの問題は前節の未解決の部分である．問題 1 が解ければ問題 2, 3 が解けることが分かっている．その意味で $D(K_n, C_n, 1)$ design，すなわち Dudeney の円卓問題がこれらの 3 つの問題の中で一番基本的で重要で難しい問題であるといえる．

問題 1 n が odd のとき，$D(K_n, C_n, 1)$ design を構成せよ．

問題 2 $n \equiv 2 \pmod 4$ のとき，$D(K_n, P_n, 1)$ design を構成せよ．

問題 3 $n \equiv 2 \pmod 4$ のとき，$D(K_{n,n}, C_{2n}, 1)$ design を構成せよ．

次の 2 つの問題が解ければ，n が even のときの Dudeney の円卓問題の解を得ることができる．n が even のときの Dudeney の円卓問題の解はすでに得られているが（前節参照），その構成は複雑であるため simple な構成法が求められており，その点で意味のある問題である．また問題自体も興味ある問題である．

問題 4 n が even のとき，K_n の perfect 1-factorization を構成せよ．

ここで，K_n の 1-factorization が perfect であるとは，その中の任意の 2 つの 1-factor の union が K_n の Hamilton cycle となるもののことである．K_n の perfect 1-factorization $\mathcal{F}$ が構成できれば，K_n の Dudeney の円卓問題の解が $\mathcal{D} = \{F \cup F' \mid F, F' \in \mathcal{F}\}$ と得られることはすぐ分かるが，K_n の perfect 1-factorization の構成は Dudeney の円卓問題より難し

い問題であり，現在，無限系列では $n = p + 1$ (p is a prime) と $n = 2p$ (p is a prime) の場合しか構成されていない [34].

問題5 n が odd (≥ 5) のとき，K_n の 2-perfect Hamilton decomposition を構成せよ.

K_n の Hamilton decomposition が i-perfect ($2 \leq i \leq (n-1)/2$) であるとは，その中に含まれるすべての Hamilton cycle の i-chord (長さ i の chord) 全体が K_n の枝集合と一致することである．K_n の 2-perfect Hamilton decomposition が構成できれば K_{n+1} の Dudeney の円卓問題の解が導かれることが示されている [22]．なお，K_n の i-perfect Hamilton decomposition の構成については，$i = 3$ の場合に構成されているのみで [4, 19]，それ以外の i についてはまだ構成されていない.

K_n の Hamilton decomposition が，すべての i ($2 \leq i \leq (n-1)/2$) について i-perfect であるとき，Steiner Hamilton decomposition と呼ばれる．n が素数のとき K_n に Steiner Hamilton decomposition は存在するが，それ以外の n については何も分かっていない．そこで最後に，Steiner Hamilton decomposition についての問題を載せておく.

問題6 n を奇数とする．K_n に Steiner Hamilton decomposition が存在すれば，n は素数であることを証明せよ.

謝辞 本稿では Dudeney の円卓問題を中心にその歴史と既知の結果，そして未解決問題について述べた．このテーマで長年共同研究を行いました故喜安善市氏，中村義作氏，武藤伸明氏に謝意を表します.

参考文献

[1] J. Akiyama, M. Kobayashi and G. Nakamura, Uniform coverings of 2-paths with 6-paths in the complete graph, J. Akiyama et al. (Eds.): Combinatorial Geometry and Graph Theory, IJCCGGT 2003, Lecture Notes in Computer Science, Springer-Verlag, 3330 (2005) 25–33.

[2] B. A. Anderson, Finite topologies and hamiltonian path, *J. Combin. Theory* (B) **14** (1973) 87–93.

[3] B. A. Anderson, Symmetry groups of some perfect 1-factorizatoins of complete graphs, *Discrete Math.* **18** (1977) 227–234.

[4] M. Buratti, G. Rinaldi and T. Traetta, Some results on 1-rotational hamiltonian cycle systems, *J. Combin. Designs*, to appear.

[5] L. E. Dickson, Solutions of Problems (Algebra), *Amer. Math Monthly* **11** (1904) 170.

[6] L. E. Dickson, Application of groups to a complex problem in arrangements, *Ann. of Math.* **6** (1905) 31–44.

[7] H. E. Dudeney, "The Canterbury Puzzles", W. Heinemann, London, 1907; Dover, New York, 2002.

[8] H. E. Dudeney, "Amusements in Mathematics", Thomas Nelson and Sons, 1917; Dover, New York, 1970.

[9] K. Heinrich, M. Kobayashi and G. Nakamura, Dudeney's Round Table Problem, *Annals of Discrete Math.* **92** (1991) 107–125.

[10] K. Heinrich, M. Kobayashi and G. Nakamura, A Solution of Dudeney's Round Table Problem for $p^r q^l + 1$, *Ars Combin.* **43** (1996) 3–16.

[11] K. Heinrich, D. Langdeau and H. Verrall, Covering 2-paths uniformly, *J. Combin. Des.* **8** (2000) 100–121.

[12] K. Heinrich and G. Nonay, Exact coverings of 2-paths by 4-cycles, *J. Combin. Theory* (A) **45** (1987) 50–61.

[13] C. Huang and A. Rosa, On sets of orthogonal hamiltonian circuits, Proceedings of the Second Manitoba Conference on Numerical Mathematics, October 5-7, 1972, Utilitas Mathematica Pub. (Congressus Numerantium 7) (1973) 327–332.

[14] C. H. Judson, Problems for Solution (Algebra), *Amer. Math Monthly* **6** (1899) 92.

[15] C. H. Judson, Problems for Solution (Algebra), *Amer. Math Monthly* **7** (1900) 72–73.

[16] M. Kobayashi, J. Akiyama and G. Nakamura, On Dudeney's round table problem for $p + 2$, *Ars Combin.* **62** (2001) 145–154.

[17] M. Kobayashi, Kiyasu-Z. and G. Nakamura, A solution of Dudeney's round table problem for an even number of people, *J. Combin. Theory* (A) **63** (1993) 26–42.

[18] M. Kobayashi, B. D. McKay, N. Mutoh and G. Nakamura, Black 1-factors and Dudeney sets, *J. Combin. Math. Combin. Comput.* **75** (2010) 167–174.

[19] M. Kobayashi, B. D. McKay, N. Mutoh G. Nakamura and C. Nara, 3-Perfect hamiltonian decomposition of the complete graph, *Australas. J. Combin.*, accepted.

[20] M. Kobayashi, N. Mutoh, Kiyasu-Z. and G. Nakamura, Double coverings of 2-paths by Hamilton cycles, *J. Combin. Designs* **10** (2002) 195–206.

[21] M. Kobayashi, N. Mutoh, Kiyasu-Z. and G. Nakamura, New series of Dudeney sets for $p + 2$ vertices. *Ars Combin.* 65 (2002) 3–20.

[22] M. Kobayashi, N. Mutoh and G. Nakamura, Dudeney's round table problem and neighbour-balanced Hamilton decompositions, *J. Combin. Math. Combin. Comput.*, to appear.

[23] M. Kobayashi and G. Nakamura, Resolvable coverings of 2-paths by 4-cycles, *J. Combin. Theory* (A) **60** (1992) 295–297.

[24] M. Kobayashi and G. Nakamura, Uniform coverings of 2-paths by 4-paths, *Australas. J. Combin.* **24** (2001) 301–304.

[25] M. Kobayashi and G. Nakamura, Uniform coverings of 2-paths with 6-cycles in the complete graph, *Australas. J. Combin.* **34** (2006) 299–304.

[26] M. Kobayashi and G. Nakamura, Uniform coverings of 2-paths in the complete graph and the complete bipartite graph, *J. Combin. Math. Combin. Comput.*, to appear.

[27] M. Kobayashi, G. Nakamura and C. Nara, Uniform coverings of 2-paths with 5-paths in K_{2n}, *Australas. J. Combin.* **27** (2003) 247–252.

[28] M. Kobayashi, G. Nakamura and C. Nara, Uniform coverings of 2-paths with 5-paths in the complete graph, *Discrete Mathematics* **299** (2005) 154–161.

[29] N. Mutoh, Some results on symmetry Dudeney sets, Manuscript (2002).

[30] G. Nakamura, Dudeney's round table problem and the edge-coloring of the complete graph (in Japanese), *Sugaku Seminar* No. 159 (1975) 24–29.

[31] G.Nakamura, Kiyasu-Z. and N.Ikeno, Solution of the round table problem for the case of $p^k + 1$ persons, *Commentarii Mathematici Universitatis Santi Pauli* **29** (1980) 7–20.

[32] F. H. Safford, Solutions of Problems (Algebra), *Amer. Math Monthly* **11** (1904) 87–88.

[33] F. H. Safford, Solutions of Problems (Algebra), *Amer. Math Monthly* **11** (1904) 169–170.

[34] E. Seah, Perfect one factorizations of the complete graph – A survey, *Bulletin Inst. Combin. Appl.* **1** (1991) 59 70.

[35] T. Shimauchi and K. Namba, Arrangements of chairs (in Japanese), *Sugaku Seminar* No. 129 (1972) 40–45.

A construction of difference matrices using functions from $GF(q)$ to $GF(q)^*$

Yutaka Hiramine
Kumamoto University

Chihiro Suetake
Oita University

1 Introduction

Definition 1.1. ([1]) Let $k > 0, \lambda > 0$ be integers and U a group of order u. A $k \times u\lambda$ matrix $\begin{bmatrix} d_{1,1} & \cdots & d_{1,u\lambda} \\ \vdots & & \vdots \\ d_{k,1} & \cdots & d_{k,u\lambda} \end{bmatrix}$ $(d_{ij} \in U)$ is called a (u, k, λ)-difference matrix over U ((U, k, λ)-DM for short) if $d_{i,1}{d_{\ell,1}}^{-1} + \cdots + d_{i,u\lambda}{d_{\ell,u\lambda}}^{-1} = \lambda U$ for any i, ℓ with $1 \leq i \neq \ell \leq k$.

Example 1.2. The following is a $(\mathbb{Z}_9, 3, 1)$-DM.

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 0 & 2 & 1 & 6 & 8 & 7 & 3 & 5 & 4 \end{bmatrix}$$

Open Question. Find the maximum number k for given U and λ.

Result 1.3. (D. Jungnickel [3]) $k \leq u\lambda$.

If the equality holds, the matrix is called *a generalized Hadamard matrix* and denoted by $\mathrm{GH}(u, \lambda)$.

Definition 1.4. (1) If p and q are primes and $q = 2p + 1$, then p is called a Sophie Germain prime ([4]) $(q = 3, 5, 7, 11, 23, \cdots)$.

(2) In this talk we weaken slightly the assumption that q is a prime by assuming that q is a power of a prime. If p is a prime and $q := 2p+1$ is a power of a prime, we call p *a quasi* Sophie Germain prime. We note that $13, 1093, 797161, \cdots$ are not Sophie Germain primes but quasi Sophie Germain primes.

In this talk we prove the following results.

Theorem 1.5. *Let $p > 3$ be a* (quasi) *Sophie Germain prime and set $q = 2p+1$. Then there exists a $(\mathbb{Z}_p, (p-1)q/2, q)$-DM.*

Theorem 1.6. *Let q be a power of a prime with $q \equiv 3 \pmod 4$. Then there exists a $(\mathbb{Z}_{(q-1)/2}, q, q)$-DM.*

We note that $q \in \{19, 31, 43, 67, \cdots\}$ is not a quasi Sophie Germain prime, but satisfies the condition of Theorem 1.6.

Theorem 1.7. *Let p be a Mersenne prime and set $q = p+1$. Then there exists a $(\mathbb{Z}_p, pq, q)$-DM,* i. e. *$GH(p, q)$.*

Remark 1.8. The GH matrices with the same parameters as in Theorem 1.7 are also obtained by T. Feng's (pq, p, pq, q)-RDSs ([5]).

Result 1.9. ([2]) If there exist (G, k, λ_1)-DM and (G, k, λ_2)-DM, then there exists a $(G, k, \lambda_1 + \lambda_2)$-DM.

Using Result 1.9, we check $(\mathbb{Z}_{23}, k, 47)$- and $(\mathbb{Z}_{29}, k, 59)$-DMs.

Example 1.10. (1) Set $p = 23$. As there exist a $(\mathbb{Z}_{23}, 529, 23)$-DM and a $(\mathbb{Z}_{23}, 184, 24)$-DM, by Result 1.9 there exists a $(\mathbb{Z}_{23}, \min\{529, 184\}, 23 + 24)$-DM, i.e. a $(\mathbb{Z}_{23}, 184, 47)$-DM. On the other hand, applying Theorem 1.5, we obtain $(\mathbb{Z}_{23}, 517, 47)$-DM, since $(p-1)q/2 = (23-1)47/2 = 517 > 184$.
(2) Set $p = 29$. As there exist a $(\mathbb{Z}_{29}, 232, 24)$-DM and a $(\mathbb{Z}_{29}, 232, 35)$-DM, by Result 1.9 there exists a $(\mathbb{Z}_{29}, \min\{232, 232\}, 24 + 35)$-DM, i.e. a $(\mathbb{Z}_{29}, 232, 59)$-DM. On the other hand, applying Theorem 1.5, we obtain $(\mathbb{Z}_{29}, 826, 59)$-DM, since $(p-1)q/2 = (29-1)59/2 = 826 > 232$.

Definition 1.11. An incidence structure $\mathcal{D} = (\mathbb{P}, \mathbb{B})$ is called a *transversal design* $\mathrm{TD}_\lambda(k, u)$ if the following conditions are satisfied.

(i) There exists a partition $\mathbb{P} = C_1 \cup \cdots \cup C_k$ into k point classes, where $|\forall C_i| = u$.

(ii) $\mathbb{B} = \{B_1, \cdots, B_{u^2\lambda}\}$, $|\forall B_i| = k$

(iii) The number of blocks containing two points $\forall a \neq b \in \mathbb{P}$

$$= \begin{cases} 0 & \text{if } a, b \in C_i\,,\ \exists i, \\ \lambda & \text{otherwise.} \end{cases}$$

Example 1.12. $\mathrm{TD}_2(3, 2) : \mathbb{P} = \{1, \cdots, 6\}$, $\mathbb{B} = \{B_1, \cdots, B_8\}$

$\mathbb{P} = C_1 \cup C_2 \cup C_3$ (point classes)

$C_1 = \{1, 2\}$, $C_2 = \{3, 4\}$, $C_3 = \{5, 6\}$

$B_1 = \{1, 4, 6\}$, $B_2 = \{2, 3, 6\}$, $B_3 = \{2, 4, 5\}$, $B_4 = \{2, 4, 6\}$

$B_5 = \{2, 3, 5\}$, $B_6 = \{1, 4, 5\}$, $B_7 = \{1, 3, 6\}$, $B_8 = \{1, 3, 5\}$

$\mathrm{Aut}(\mathbb{P}, \mathbb{B}) \geq U = \{1, s\} \simeq \mathbb{Z}_2$, $s = (1,2)(3,4)(5,6)$

U acts regulary on each point class — $U$is called a *class regular group.*

$B_1^U = \{B_1, B_5\}$, $B_2^U = \{B_2, B_6\}$, $B_3^U = \{B_3, B_7\}$, $B_4^U = \{B_4, B_8\}$.

Example 1.13. We note that a difference matrix $M = (d_{ij})$ obtained from a class regualr group. Let notations be as in Example 1.12.

$\{1, 3, 5\}$: a set of representatives of the point classes

$\{B_1, B_2, B_3, B_4\}$: a set of representatives of U-orbits on $\mathbb{B}$,

where $B_1 = \{1,4,6\}$, $B_2 = \{2,3,6\}$, $B_3 = \{2,4,5\}$, $B_4 = \{2,4,6\}$) and $s = (1,2)(3,4)(5,6)$). Moreover,

$1^1 \in B_1$, $1^s \in B_2$, $1^s \in B_3$, $1^s \in B_4$,
$3^s \in B_1$, $3^1 \in B_2$, $3^s \in B_3$, $3^s \in B_4$,
$5^1 \in B_1$, $5^1 \in B_2$, $5^s \in B_3$, $5^1 \in B_4$.

Then we have a $(2,3,2)$-DM $M = \begin{bmatrix} 1 & s & s & s \\ s & 1 & s & s \\ 1 & 1 & s & 1 \end{bmatrix}$.

In general, the following result is well known.

Result 1.14. There exists a $\mathrm{TD}_\lambda(k,u)$ admitting a class regular automorphism group U if and only if there exists a (u,k,λ)-DM over a group U

2 Functions from $GF(q)$ to $GF(q)^*$ and a TD

Notation 2.1. Throughout we use the following notations.

(i) $2 \nmid p \in \mathbb{N}$, $m \in \mathbb{N}$ and $q = mp+1$ is a prime power.

(ii) Set $I_t := \{0, \cdots, t-1\}$, $t \leq p$ and assume p is a prime when $t > 1$.

(iii) Set $F = GF(q)$, $F^* = \langle \omega \rangle$ and $U = \langle \omega^m \rangle \simeq \mathbb{Z}_p$.

Hypothesis 2.2. A group $G = U \times F \times U$ of order p^2q is defined by

$$(y_1,x_1,z_1)(y_2,x_2,z_2) = (y_1y_2, x_1y_2 + x_2, z_1z_2),$$
$$\forall (y_1,x_1,z_1), \quad (y_2,x_2,z_2) \in G.$$

We often identify $(1,0,z)$ $(\in G)$ with z $(\in U)$ and so often regard U as a subgroup $\{1\} \times \{0\} \times U$ of G.

Our method for constructing difference matrices is as follows:

a group G of order p^2q with $G \rhd U \simeq \mathbb{Z}_p$
$\longrightarrow$ a dual $\mathrm{TD}_q(tq,p)$ admitting G as its automorphism group for some t $(\leq p)$, where U is class regular
$\longrightarrow$ a $(\mathbb{Z}_p, tq, q)$-DM

Remark 2.3. In our construction, G is regular on the set of points. But G is not regular on the set of blocks.

Hypothesis 2.4. Let notations be as in Notation 2.1. Let functions $f_j : F \longrightarrow U$ $(j \in I_t)$ and a bijection $g : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p$ satisfy the following:

(A) $\#\{(y,x) \in U \times F \mid y^{g(j_2)-g(j_1)} f_{j_1}(x) f_{j_2}(cy+x)^{-1} = k\} = q$
$\forall j_1, j_2 \in I_t, \quad c,k \in U$

Under Hypothesis 2.4 we define a pq-subset $D_{j,a}$ of G $(j \in I_t,\ a \in F)$ in the following way :

$$D_{j,a} = \{(y, x, y^{g(j)} f_j((x-a)y^{-1})) \mid y \in U,\ x \in F\} \ (\subset G).$$

Note that $D_{j,a} \cdot (y,x,z) = D_{j,ay+x} \cdot zy^{-g(j)}, \quad zy^{-g(j)} \in U.$

Here we identify $(1,0,zy^{-g(j)})$ with $zy^{-g(j)} \in U$.

Then the incidence structure $\mathcal{D}(\mathbb{P},\mathbb{B})$ defined by

$$\mathbb{P} = G, \qquad \mathbb{B} = \{D_{j,x}\, z \mid j \in I_t,\ x \in F,\ z \in U\}$$

satisfies the following lemma.

An incidence structure $\mathcal{D}(\mathbb{P},\mathbb{B})$

Lemma 2.5. *Let notations be as above. Then the following holds.*
(i) $|\mathbb{P}| = p^2q, \quad |\mathbb{B}| = tpq, \quad |B| = pq \ \ (\forall B \in \mathbb{B})$
(ii) $|D_{j_1,x_1}z_1 \cap D_{j_2,x_2}z_2| = \begin{cases} 0 & \text{if } (j_1,x_1) = (j_2,x_2),\ z_1 \neq z_2, \\ q & \text{if } (j_1,x_1) \neq (j_2,x_2). \end{cases}$
(iii) *Set* $\mathcal{B}_{j,a} = \{D_{j,a}z \mid z \in U\}$ $(j \in I_t,\ a \in F)$. *Then* $|\mathcal{B}_{j,a}| = p$ *and* U *acts regularly on* $\mathcal{B}_{j,a}$.

Definition 2.6. We define a $pq \times tq$ matrix $M = [M_{(y,x_1),(j,x_2)}]$ $((y,x_1) \in U \times F,\ (j,x_2) \in I_t \times F)$ over U by

$$M_{(y,x_1),(j,x_2)} = y^{g(j)} f_j\,((x_1 - x_2)y^{-1}) \ \ (\in U)$$

The following holds.

Proposition 2.7. (i) *The dual of* $\mathcal{D}$ *is a* $TD_q(tq,p)$.
(ii) M^T *is a* $(\mathbb{Z}_p, tq, q)$*-difference matrix.*
(iii) G *is regular on* $\mathbb{P}$, *but non-regular on* $\mathbb{B}$. *Actually,*
$G_{(y,x,z)} = \{(1,0,1)\}$ *and*
$G_{D_{j,x}z} = \{(y, x - xy, y^{g(j)}) \mid y \in U\} \simeq \mathbb{Z}_p$.

3 Sophie Germain primes and DMs

In this section we assume Hypothesis 2.4 and that $m = 2$ and $q = 2p + 1$ is a power of a prime. Moreover, p is an odd prime if $t > 1$. Note that $q \equiv 3 \pmod 4$ and $U = \langle w^2 \rangle, F^* = -U \cup U$.

We can show the following.

Lemma 3.1. *The condition* (A) *is satisfied if it is true for* $c \in \{\pm 1\}$, *i. e.*

$$\textbf{(A)}\ \#\{(y,x) \in U \times F \mid y^{g(j_2)-g(j_1)} f_{j_1}(x) f_{j_2}(cy + x)^{-1} = k\} = q$$
$$\forall j_1,\ j_2 \in I_t,\ \ k \in U, c \in \{\pm 1\}$$

Lemma 3.2. *Assume* $\gcd(2\ell, q-1) = 2$ *and let* $h(x) = x^{2\ell}$ *be a function from* F^* *to* U. *Then* $h|_U$ *and* $h|_{-U}$ *are bijections.*
In particular, $x^{2\ell} = k \in U \iff \exists_1 h \in U; x = \pm h,\ k = h^{2\ell}$

We now define functions f_j and g as follows. Set $g(i) = 2i$ and $f_j(x) = (x^2 + 1)^{2j+2}$ for j with $0 \le j \le (p-3)/2$. Then $\gcd(p, 2j+2) = 1$. Moreover, in the present condition, (A) is represented in the following form.

$$\textbf{(A)}\ \#\{(y,x) \in U \times F \mid y^{2n-2m}(x^2+1)^{2m}((cy+x)^2+1)^{-2n} = k\} = q$$
$$(m = j_1 + 1,\ n = j_2 + 1, \forall j_1,\ j_2 \in I_{(p-1)/2},\ \ c \in \{\pm 1\},\ k \in U)$$

Case $m = n$:

$$(\text{A}')\ \#\left\{(y,x) \in U \times F \mid \left(\tfrac{(cy+x)^2+1}{x^2+1}\right)^{2n} = h^{2n}\right\} = q, \qquad ((c,h) \in \{\pm 1\} \times U).$$

Case $m \neq n$:

$$(\mathrm{A}'')\ \#\left\{(y,x) \in U \times F \mid \left(\frac{x^2+1}{y}\right)^{2m} = \left(\frac{(cy+x)^2+1}{y}h\right)^{2n}\right\} = q, \quad ((c,h) \in \{\pm 1\} \times U)$$

$$\because \left(\frac{x^2+1}{y}\right)^{2m} \Big/ \left(\frac{(cy+x)^2+1}{y}\right)^{2n} = h^{2n}, \qquad \exists 1\, h \in U \ \text{ s.t. } \ k = h^{2n}$$

Case $m = n$

First we consider the case $m = n$.

$$(\mathrm{A}')\ \#\left\{(y,x) \in U \times F \mid \left(\frac{(cy+x)^2+1}{x^2+1}\right)^{2n} = h^{2n}\right\} = q,\ h \in U$$

As $x^{2n}|_U : U \to U$ is a bijection, (A′) is equivalent to

$$\#\left\{(y,x) \in U \times F \,\middle|\, 2cxy + y^2 = (\pm h - 1)(x^2+1)\right\} = q, \qquad (\forall c \in \{\pm 1\},\ \ \forall h \in U) \tag{1}$$

Fix $h \in U$ and $c \in \{\pm 1\}$. For each $\varepsilon \in \{\pm 1\}$, set

$$\varphi_{c,\varepsilon,h}(x,y) = -(\varepsilon h - 1)x^2 + 2cxy + y^2 - (\varepsilon h - 1)$$

and $N_{c,\varepsilon,h} = \#\{(x,y) \in F \times U \mid \varphi_{c,\varepsilon,h}(x,y) = 0\}$. Then (1) is equivalent to $N_{c,1,h} + N_{c,-1,h} = q$.
We can prove the following.

Lemma 3.3. $N_{c,1,h} + N_{c,-1,h} = q. \qquad (\forall c \in \{\pm 1\},\ \ \forall h \in U)$

Case $m \neq n$

We now consider the case $m \neq n$ for a fixed $(h,c) \in U \times \{\pm 1\}$.

$$(\mathrm{A}'')\ \#\left\{(y,x) \in U \times F \,\middle|\, \left(\frac{x^2+1}{y}\right)^{2m} = \left(\frac{(cy+x)^2+1}{y}h\right)^{2n}\right\} = q$$

In this case $p > 3$ and , $m-1\ (= j_1),\ n-1\ (= j_2) \in I_{(p-1)/2}$. Hence p is a prime by assumption. As $1 \leq m, n \leq (p-1)/2$, we have $\gcd(p, 2m) = \gcd(p, 2n) = 1$. Let $t \in \mathbb{Z}_p$ such that $2nt \equiv 1 \mod p$.

Remark 3.4. $a, b \in U,\ \ a^{2m} = b^{2n} \implies a = b^{2mt}$.

Lemma 3.5. (A″) *holds if and only if, for any* $h \in U$, *the number of solutions* $(a,x,y) \in U \times F \times U$ *to the following simultaneous equations is* q.

$$\frac{x^2+1}{y} = \sigma a, \qquad \sigma = \pm 1 \tag{2}$$

$$\frac{(cy+x)^2+1}{y}h = \tau a^{2mt}, \qquad \tau = \pm 1 \tag{3}$$

Proof. By the previous lemma on the function $h(x) = x^{2\ell}$ with $\gcd(2\ell, q-1) = 2$, there exists a unique $(a,b) \in U \times U$ such that $\left(\frac{x^2+1}{y}\right)^{2m} = \left(\frac{(cy+x)^2+1}{y}h\right)^{2n} = (\pm a)^{2m} = (\pm b)^{2n}$. As $a^{2m} = b^{2n}, a, b \in U$ and $2nt \equiv 1 \pmod p$, $b = a^{2mt}$. Therefore the lemma holds. □

Lemma 3.6. *Set $s = 2mt$. Then (2)(3) are equivalent to the following simultaneous equations.*

$$y^2 - 2(a\sigma + \tau a^s h^{-1})y + (\sigma a - \tau a^s h^{-1})^2 + 4 = 0 \quad (4)$$
$$2cx = -y + h^{-1}\tau a^s - \sigma a \quad (5)$$

For a fixed $(h, c) \in U \times \{\pm 1\}$, let $N_{h,c}$ be the number of solutions $(a, y, x) \in U \times U \times F$ to (4)(5). Then we can show the following.

Lemma 3.7. *$N_{h,c} = q$ for any $(h, c) \in U \times \{\pm 1\}$.*

DMs obtained from Sophie Germain primes

By Proposition 2.7 and Lemmas 3.3, 3.7 we have the following.

Theorem 3.8. *Let p be an odd prime with $q = 2p + 1$ a power of a prime. Let $f_i(t) = (t^2 + 1)^{2i+2}$ be functions from $F = GF(q)$ to $U = (F^*)^{(2)}$ for $i \in I_{(p-1)/2}$. Then, $(p-1)q/2 \times pq$ matrix M over $\mathbb{Z}_p$ defined by the following is a $(\mathbb{Z}_p, (p-1)q/2, q)$-DM.*

$$M_{(i,z),(y,x)} = y^{-2i} f_i((x - z)y) \quad ((i, z) \in I_{(p-1)/2} \times F, \quad (y, x) \in U \times F)$$

Theorem 3.9. *Let $q \equiv 3 \pmod 4$ be a power of a prime. Set $F = GF(q)$ and $U = (F^*)^{(2)}$. Then $q \times rq$ matrix M over $\mathbb{Z}_r$ with $r = (q-1)/2$ defined by the following is a $(\mathbb{Z}_r, q, q)$-DM.*

$$M_{z,(y,x)} = \left(((x - z)y)^2 + 1\right)^2 \quad z \in F, \quad (y, x) \in U \times F$$

Example 3.10. A $(\mathbb{Z}_{15}, 12, 31)$-DM is listed in Table 17.43 of [2]. On the other hand, Theorem 3.9 implies the existence of a $(\mathbb{Z}_{15}, 31, 31)$-DM.

Mersenne prime p $(= q - 1)$ and GH(p, q)

Theorem 3.11. *Let $p = q - 1$ be a Mersenne prime. Set $F = GF(q)$, $F^* = \langle\omega\rangle$ and let f be a function form F to F^* defined by $f(0) = 1$ and $f(x) = x^{\log(x) \pmod p}$ for $x \in F^*$. Then a matrix $H = (h_{(i,x),(j,y)})$ over F^* defined by the following is a GH(p, q).*

$$h_{(i,x),(j,y)} = \omega^{-2ij} f((x - y)\omega^{-i-j}) \quad ((i, x), (j, y) \in \mathbb{Z}_p \times F)$$

Remark 3.12. The functions corresponding to (A) are given by

$$f_i(x) = f(x\omega^{-i}), \quad i \in I_p.$$

T. Feng's (pq, p, pq, q)-RDS ([5])

In [5] T. Feng constructed a (pq, p, pq, q)-RDS, which also gives the following GH(p, q).

$$H = (h_{(s_1,x_1),(s_2,x_2)}) \quad ((s_1, x_1), (s_2, x_2) \in F_p \times F_q)$$

$$h_{(s_1,x_1),(s_2,x_2)} = \begin{cases} (s_2 - s_1)^2 & (x_1 = x_2), \\ (s_2 - s_1)\tau(x_2 - x_1) - \frac{1}{4}\tau(x_2 - x_1)^2 & (x_1 \neq x_2), \end{cases}$$

where $\tau : F_q^* \to F_p$ is any bijection.

Remark on (p, k, λ)-DMs over $\mathbb{Z}_p$

Remark 3.13. We now compare the bound in [2] with our new bound. In the following table, "$*$" denotes the bound in Table 17.42-43 of [2] and "†" denotes the bound obtained from Theorems 3.8, 3.9.

*(5,17,11)-DM	†(5,33,11)-DM	*(7,26,8)-DM	†(7,56,8)-DM	* (9,3,19)-DM	†(9,19,19)-DM

*(11,44,23)-DM	†(11,115,23)-DM	* (13,65,27)-DM	†(13,162,27)-DM

* (15,12,31)-DM	†(15,31,31)-DM	* (31,496,32)-DM	†(31,992,27)-DM

Let p be a quasi Sophie Germain prime and set $q = 2p + 1$. By Theorem 3.8, there exists a $(p, (p-1)q/2, q)$-DM over $\mathbb{Z}_p$. In connection with this result we would like to raise the following question.

Question. Does there exist a (p, pq, q)-DM (i.e. GH(p, q)) over $\mathbb{Z}_p$?

References

[1] T. Beth, D. Jungnickel and H. Lenz, "Design Theory" Volume I, Second Edition, Cambridge University Press, 1999.

[2] C.J. Colbourn and J.H. Dinitz, "The CRC Handbook of Combinatorial Designs", Second Edition, Chapman & Hall/CRC Press, Boca Raton, 2007.

[3] D. Jungnickel, On difference matrices, resolvable transversal designs and generalised Hadamard matrices, Math. Z., Vol. 167 (1979), 49-60.

[4] Richard K. Guy, "Unsolved Problems in Number Theory", Third Edition, Chapman & Hall/CRC Press, Boca Raton, 2007.

[5] Tao Feng, Relative (pn, p, pn, n)-difference sets with $\gcd(p, n) = 1$, J. Algebraic Combinatorics (2009) Vol. 29, p91-106.

d-dimensional symmetric bilinear dual hyperovals in $V(((1/r)d^2+3d+2)/2,2)$

香川高専 (高松キャンパス)　谷口浩朗 (Hiroaki Taniguchi)*

1　はじめに

C. Huybrechts と A. Pasini [5] により, ベクトル空間 $V(m,2)$ 内の高次元双対超卵形 (dimensional dual hyperoval, DHO) は定義されました。

m-次元ベクトル空間 $V(m,2)$ における d-次元部分空間の集合 S が, $V(m,2)$ における d-次元双対超卵形 (DHO) であるとは，以下が成り立つことである:
(1) S に属するどの 2 個の d-部分空間も 1 次元部分ベクトル空間で交わり,
(2) S に属するどの異なる 3 個の d-部分空間も，それらの共有ベクトル空間は 0-ベクトル空間であり,
(3) S に属する d-部分空間達は $V(m,2)$ を生成し,
(4) S は 2^{d+1} 個の d-部分空間から成る。

以下 $d\geq 3$ とする. $GF(2)$ 上の d-次元 DHO が生成する射影空間の次元 m については，$2d+1\leq m\leq (d+1)(d+2)/2$ であろうと予想されている [11]. その最大の次元と考えられる $V((d+1)(d+2)/2,2)$ には，現在
（1）Huybrechts' DHO [4],
（2）Buratti-Del Fra's DHO [1],[2],
（3）Veronesean DHO [10], [11],
（4）Veronesean DHO の変形 [6],
の 4 種類の（同型でない）双対超卵形 (DHO) が知られている。

ところで，ごく最近私が $m=3d-3, m=4d-2$ などで simply connected な例を構成する [7] まで，$2d+2<m<(d+1)(d+2)/2$ における DHO の例はすべて以上の 4 種類の DHO の quotient(projection の像) になっているものしか知られていなかった。今回，またこれらとは別に，$d=lr\geq 4$(ただし l,r は自然数) に対して $m=((1/r)d^2+3d+2)/2$ であるような例 S_c(ただし

*taniguchi@t.kagawa-nct.ac.jp　(アドレスが変わっています)

$c \in GF(2^r)$) を構成したのでそれを報告したい。この例は一言で言えば「(A) 吉荒-谷口による Buratti-Del Fra の例の再構成 [9]」と「(B)Dempwolff による $m = 2d + 1$ の例 [3]」を結びつけたもので, 結びつけるという発想があればだれにでも簡単に構成できると思う。実際 $r = 1$ の時には (A) となり $l = 1$ の時には (B) となっている。どちらかというと苦労をした（時間をかけた）のは後半で，これらの例が $r \geq 2$, $l \geq 2$ でかつ $GF(2^r) \ni c \neq 1$ の時には上記の 4 種類の DHO の quotient(projection の像) になっていないことを示す場面であった。その場面で有用な命題（上記 4 種類の DHO の quotient に関する）を示すことができたと思う。しかしながら，ページ数があまり増えすぎる（実際, 後半は上記 4 種類の DHO の細かい性質が必要となる）と思うので，この報告では構成しか説明できない。お許し願いたい。さらに興味を持たれた方は私に現在作成中の preprint[8] のご請求お願いしたい。

講演の機会を与えてくださった先生方，ご推薦くださった先生方に感謝をいたします。また，この DHO の自己同型がどうなるかという座長の末竹先生のご質問にはまだ答えられていないが，([2] のまねをすれば) たぶん難しくないだろうと考えています。同様アフィン拡大 $A_f(S_c)$ の Universal cover の探求も [9] に準じて調べれば難しくないだろうと考えています。

なお、これらの例は広い意味での Buratti-Del Fra DHO の一族（定義はありませんが, たとえばアフィン拡大の universal cover が halved hypercube であるとかいう可能性も考えられる）をなすのではないか、と考えています。

2 DHO S_c for $c \in GF(2^r)$ with $Tr(c) = 1$

Let $l \geq 1$ and $r \geq 1$ be integers with $d = lr \geq 4$, and $GF(2^r)$ a finite field of 2^r elements. The letter I is used to denote the set of integers i with $0 \leq i \leq l$, and we set $I_0 := I \backslash \{0\}$. Let V_1 be a l-dimensional vector space over $GF(2^r)$ with a basis $\{e_i \mid i \in I_0\}$ and V_2 a $(l+1)$-dimensional vector space over $GF(2^r)$ with a basis $\{e_i \mid i \in I\}$. Let $V \subset V_2$ be a $(rl+1)$-dimensional $GF(2)$-vector space generated by V_1 and e_0. Note that $V = V_1 \oplus \langle e_0 \rangle$ as $GF(2)$-vector space.

Let $c \in GF(2^r)$ be a non-zero element such that the equation $x^2 + (x/c) + 1 = 0$ has no solution in $GF(2^r)$.

注意 . *If there exists an* $x \in GF(2^r)$ *with* $x^2 + (x/c) + 1 = 0$, *then, if we put* $y := cx$, *we have* $y^2 + y + c^2 = 0$, *hence the absolute trace* $Tr(c) = 0$. *Conversely, if* $Tr(c) = 0$, *there exists a* $y \in GF(2^r)$ *with* $y^2 + y + c^2 = 0$, *hence there exists an* $x \in GF(2^r)$ *with* $x^2 + (x/c) + 1 = 0$, *by additive form of*

Hilbert's Theorem 90. Therefore, for $c \in GF(2^r)$, *we have* $x^2 + (x/c) + 1 \neq 0$ *for any* $x \in GF(2^r)$ *if and only if* $Tr(c) = 1$ *in* $GF(2)$.

Let $V_2 \otimes V_2$ be the tensor product of V_2 and V_2 over $GF(2^r)$. We define the action of $a \in GF(2^r)$ on $V_2 \otimes V_2$ as $a(x \otimes y) = (ax) \otimes y = x \otimes (ay)$. Inside $V_2 \otimes V_2$, let W_c be a $GF(2^r)$-vector subspace generated by

$$(e_i \otimes e_j) + (e_j \otimes e_i) \text{ for all } i, j \in I \text{ with } i < j,$$
$$e_0 \otimes e_0 \text{ and } c(e_i \otimes e_i) + (e_0 \otimes e_i) \text{ for all } i \in I_0.$$

We denote by $x \otimes_c y$ the image $x \otimes y + W_c$ of a vector $x \otimes y \in V_2 \otimes V_2$ under the cannonical projection of $V_2 \otimes V_2$ onto $(V_2 \otimes V_2)/W_c$. Then $x \otimes_c y = y \otimes_c x$ and $(x_1 + x_2) \otimes_c y = x_1 \otimes_c y + x_2 \otimes_c y$ for any $x, x_1, x_2, y \in V_2$. We notice that

$$x \otimes_c e_0 = e_0 \otimes_c x = (cx) \otimes_c x = x \otimes_c (cx) \quad \text{for any } x \in V_1 \text{ and}$$
$$e_0 \otimes_c e_0 = 0 \quad \text{in } (V_2 \otimes V_2)/W_c.$$

Hence $\{e_i \otimes_c e_j \mid i, j \in I_0, i \leq j\}$ generate $(V_2 \otimes V_2)/W_c$ as a $GF(2^r)$-vector space. The symmetric tensor space $Sym(V_1) := (V_1 \otimes V_1)/W$ over $GF(2^r)$, where $W \subset V_1 \otimes V_1$ is a $GF(2^r)$-vector subspace defined by $W := \langle (e_i \otimes e_j) + (e_j \otimes e_i) \mid i, j \in I_0 \text{ with } i < j \rangle$. We regard $V_1 \otimes V_1 \subset V_2 \otimes V_2$ naturally. Then, $\langle W_c, V_1 \otimes V_1 \rangle / (V_1 \otimes V_1) \simeq \langle e_0 \otimes e_0 \rangle \oplus \langle c(e_i \otimes e_i) + (e_0 \otimes e_i) \mid i \in I_0 \rangle \oplus \langle e_i \otimes e_0 + e_0 \otimes e_i \mid i \in I_0 \rangle$ as $GF(2^r)$-vector spaces, and since $\langle W_c, V_1 \otimes V_1 \rangle / (V_1 \otimes V_1) \simeq W_c / W_c \cap (V_1 \otimes V_1)$, we must have $W_c \cap (V_1 \otimes V_1) = W$. Hence natural injection $V_1 \otimes V_1 \to V_2 \otimes V_2$ induces an isomorphism $Sym(V_1) \simeq (V_2 \otimes V_2)/W_c$. Therefore $\{e_i \otimes_c e_j \mid i, j \in I_0, i \leq j\}$ is a basis of $(V_2 \otimes V_2)/W_c$ as a $GF(2^r)$-vector space. Thus the dimension of the vector space $(V_2 \otimes V_2)/W_c$ over $GF(2^r)$ is $l(l+1)/2$, and $rl(l+1)/2$ over $GF(2)$.

補題 1. *Let* $x, y \in V_1$. *If* $x \otimes_c y + c(x + y) \otimes_c (x + y) = 0$, *then* $x = y = 0$.

Proof. Let us express $x, y \in V_1$ as $x = \sum_{i \in I_0} x_i e_i$ and $y = \sum_{i \in I_0} y_i e_i$ with $x_i, y_i \in GF(2^r)$. Then, by easy calculations, we have

$$x \otimes_c y + c(x + y) \otimes_c (x + y) = \sum_{i<j, i,j \in I_0} (x_i y_j + x_j y_i)(e_i \otimes_c e_j)$$
$$+ \quad c \left(\sum_{i \in I_0} ({x_i}^2 + (x_i y_i / c) + {y_i}^2)(e_i \otimes_c e_i) \right) = 0.$$

Recall $\{e_i \otimes_c e_j \mid i,j \in I_0, i \leq j\}$ is a basis of $(V_2 \otimes V_2)/W_c$ as a $GF(2^r)$-vector space. Hence, if $x \otimes_c y + c(x+y) \otimes_c (x+y) = 0$, then ${x_i}^2 + (x_i y_i/c) + {y_i}^2 = 0$ for any $i \in I_0$. If $(x_i, y_i) \neq (0,0)$ for some $i \in I_0$, for example $y_i \neq 0$, then $(x_i/y_i)^2 + (x_i/cy_i) + 1 = 0$ gives a solution $x_i/y_i \in GF(2^r)$ for the equation $x^2 + (x/c) + 1 = 0$, contradicts our assumption on $c \in GF(2^r)$. Hence $(x_i, y_i) = (0,0)$ for any $i \in I_0$, thus $x = y = 0$. □

補題 2. *Let $x, y \in V_1$ and $y \neq 0$. If $x \otimes_c y = 0$, then $x = 0$.*

Proof. Let $x, y \in V_1$ and $y \neq 0$. Let $x = \sum_{i \in I_0} x_i e_i$ and $y = \sum_{i \in I_0} y_i e_i$ with $x_i, y_i \in GF(2^r)$. Then we have $\sum_{i<j, i,j \in I_0} (x_i y_j + x_j y_i)(e_i \otimes_c e_j) + \sum_{i \in I_0} x_i y_i (e_i \otimes_c e_i) = 0$. Hence $x_i y_j + x_j y_i = 0$ for $i \neq j$ with $i, j \in I_0$ and $x_i y_i = 0$ for $i \in I_0$. Since $y \neq 0$, we have $y_i \neq 0$ for some i. We fix this i. Then we have $x_i = 0$ from $x_i y_i = 0$. From $x_i y_j + x_j y_i = 0$ for $j \neq i$ with $j \in I_0$, we have $x_j y_i = 0$, hence $x_j = 0$ for any $j \neq i$ with $j \in I_0$. Thus we have $x = 0$. □

補題 3. *Let $x, y \in V$ with $x, y \notin V_1$. If $x \otimes_c y = 0$, then $x = y = e_0$.*

Proof. Recall that $V = V_1 \oplus \langle e_0 \rangle \subset V_2$ as $GF(2)$-vector space. Since $x, y \notin V_1$, x and y have expressions $x = x_0 + e_0$ and $y = y_0 + e_0$ with $x_0, y_0 \in V_1$. Assume $x \otimes_c y = 0$. Then, since $e_0 \otimes_c e_0 = 0$, we have $x_0 \otimes_c y_0 + e_0 \otimes_c (x_0 + y_0) = x_0 \otimes_c y_0 + c(x_0 + y_0) \otimes_c (x_0 + y_0) = 0$. Hence $x_0 = y_0 = 0$ by Lemma 1, and $x = y = e_0$. □

補題 4. *Let $x, y \in V$ with $x \notin V_1$ and $y \in V_1 \backslash \{0\}$. Then $x \otimes_c y = 0$ if and only if $x = cy + e_0$.*

Proof. Let $y \in V_1 \backslash \{0\}$ with $y = \sum_{i \in I_0} y_i e_i$, $y_i \in GF(2^r)$. From $ce_i \otimes_c e_i + e_0 \otimes_c e_i = 0$ for all $i \in I_0$, we see that $cy \otimes_c y + e_0 \otimes_c y = 0$. Hence $(cy + e_0) \otimes_c y = 0$. Now, let $x \otimes_c y = 0$ with $x \in V \backslash \{0\}$. We must have $x = x_0 + e_0$ for some $x_0 \in V_1$ from Lemma 2. Adding these equations, we have $(x_0 + cy) \otimes_c y = 0$ with $x_0 + cy \in V_1$, hence $x_0 + cy = 0$ by Lemma 2, and we have $x = x_0 + e_0 = cy + e_0$. □

Let $y \in V = V_1 \oplus \langle e_0 \rangle$ with $y \notin V_1$ and $y \neq e_0$. Express y as $y := y_0 + e_0$ with $y_0 \in V_1 \backslash \{0\}$. Then by Lemma 4, we have $(y_0 + e_0) \otimes_c c^{-1} y_0 = 0$, that is, $y \otimes_c c^{-1}(y + e_0) = 0$. By the same way, we have the following lemma.

補題 5. *Let $x, y \in V$ with $x \in V_1 \backslash \{0\}$ and $y \notin V_1$. Then $x \otimes_c y = 0$ if and only if $x = c^{-1}(y + e_0)$.*

Thus, we have the following proposition.

命題 1. *For non-zero $x, y \in V$, we have $x \otimes_c y = 0$ if and only if $x = cy + e_0 \notin V_1$ in case $y \in V_1$, $x = c^{-1}(y + e_0) \in V_1$ in case $y \notin V_1$ with $y \neq e_0$, and $x = e_0$ in case $y = e_0$.*

Set $d := rl$. The dimension of $V \oplus ((V_2 \otimes V_2)/W_c)$ over $GF(2)$ is $(rl+1)+rl(l+1)/2 = (rl^2+3rl+2)/2 = (1/2r)d^2+(3/2)d+1 = ((1/r)d^2+3d+2)/2$. Inside the vector space $V(((1/r)d^2+3d+2)/2, 2) := V \oplus ((V_2 \otimes V_2)/W_c)$, for each $t \in V$, define a $(d+1)$-dimensional vector subspace $X_c(t)$ by

$$X_c(t) := \{(x, x \otimes_c t) \mid x \in V\}.$$

定理 1. *$S_c := \{X_c(t) \mid t \in V\}$ is a d-dimensional symmetric bilinear dual hyperoval in $V(((1/r)d^2+3d+2)/2, 2)$.*

Proof. Since $(V_2 \otimes V_2)/W_c \simeq (V_1 \otimes V_1)/W = Sym(V_1)$ and $V_1 \subset V$, $V(((1/r)d^2+3d+2)/2, 2) = V \oplus ((V_2 \otimes V_2)/W_c)$ is generated by $\{(x, 0) \mid x \in V\} = X_c(0)$ and $\{(x, x \otimes_c t) \mid x \in V\} = X_c(t)$ for $t \in V \backslash \{0\}$. Hence the ambient space of S_c is $V(((1/r)d^2+3d+2)/2, 2)$. For $s \neq t \in V$, let $X_c(s) \cap X_c(t) \ni (x, x \otimes_c s) = (x, x \otimes_c t)$ with $x \neq 0$. Then we have $x \otimes_c s = x \otimes_c t$, i.e., $x \otimes_c (s+t) = 0$. From $x \otimes_c (s+t) = 0$ and Proposition 1, we have $x = c(s+t) + e_0 \notin V_1$ if $s+t \in V_1$, $x = c^{-1}(s+t+e_0) \in V_1$ if $s+t \notin V_1$ with $s+t \neq e_0$, and $x = e_0$ if $s+t = e_0$. Hence any two members $X_c(s)$ and $X_c(t)$ with $s \neq t$ intersect in one dimensional subspace. For mutually distinct elements $s, t_1, t_2 \in V$, we have $X_c(s) \cap X_c(t_1) \neq X_c(s) \cap X_c(t_2)$ from the above result. Hence $X_c(s) \cap X_c(t_1) \cap X_c(t_2) = \{0\}$. There are $|V| = 2^{d+1}$ members in S_c ($|V|$ is the cardinality of V). By the definition of W_c, we have $B(x, y) := x \otimes_c y$ is symmetric and bilinear. Therefore, S_c is a symmetric bilinear dual hyperoval in $V(((1/r)d^2+3d+2)/2, 2)$. □

注意 . *If $r = 1$, then $GF(2^r) = GF(2)$, $c = 1$ and $((1/r)d^2+3d+2)/2 = (d+1)(d+2)/2$, and S_c is the Buratti-Del Fra DHO in [9]. If $l = 1$, the dimension of the ambient space $((1/r)d^2+3d+2)/2 = 2r+1 = 2d+1$, and S_c is DHO constructed by U. Dempwolff in Example 3.4 of [3].*

References

[1] M. Buratti and A. Del Fra, Semi-Boolean quadruple systems and dimensional dual hyperovals, Advances in Geometry, 3 (2003), 245–253.

[2] A. Del Fra and S. Yoshiara, Dimensional dual hyperovals associated with Steiner systems, European Journal of Combinatorics, 26 (2005), 173–194.

[3] U. Dempwolff, Symmetric extensions of bilinear dual hyperovals, Finite Fields and their Applications, 22 (2013), 51–56.

[4] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AC^*$ geometries, Discrete Mathematics, 255 (2002), 503–532.

[5] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, Contribution to Algebra and Geometry, 40 (1999), 503–532.

[6] H. Taniguchi, A new family of dual hyperovals in $PG(d(d+3)/2, 2)$ with $d \geq 3$, Discrete Mathematics, 309 (2009), 418–429.

[7] H. Taniguchi, Some examples of simply connected dual hyperovals, Finite Fields and their Applications, 22 (2013), 45–50.

[8] H. Taniguchi, d-dimensional symmetric bilinear dual hyperovals in $V(((1/r)d^2 + 3d + 2)/2, 2)$ for $d = lr \geq 4$, preprint.

[9] H. Taniguchi and S. Yoshiara, A new construction of the d-dimensional Buratti-Del Fra dual hyperoval, European Journal of Combinatorics, 33 (2012), 1030–1042.

[10] J. Thas and H. van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, The Quarterly Journal of Mathematics, Oxford. 55 (2004), 99–113.

[11] S. Yoshiara, Ambient spaces of dimensional dual arcs, Journal of Algebraic Combinatorics, 19 (2004), 5–23.

「Extremal binary doubly even self-dual codeから得られるt-designについて」

中空　大幸
(岡山大学)

1　序文

t-(v,k,λ) design において、$\lambda=1$ のとき Steiner System と呼ばれる。1938 年に Witt system 5-(24, 8, 1) design が発見されているように 5-design の例は古くから知られているが、$t\geq 6$ になると現在において Steiner System の存在は知られていなく、古典的な未解決問題として知られる。

Steiner System でなくても $t\geq 6$ のデザインの存在は以下のように歴史的に有名な問題であった。

- t 重可移群 (非自明) が存在 $\Rightarrow$ t-design が存在 (Mathieu 群と Witt system, 1938 年)
- Assmus-Mattson の定理により、コードから 5-design が得られる。 ([1], 1969 年)
- 6 重可移群の非存在が示される。(1982 年)
- (simple) 6-(33, 8, 36) design が構成される。 (Magliveras, Leavitt [7], 1983 年)
- 任意の t に対して、t-$(v,t+1,\lambda)$ design が存在する。 (Teirlinck [8], 1987 年)

自明な多重可移群とは n 次対称群と n 次交代群でそれぞれ n 重可移と $(n-2)$ 重可移である。有限単純群の分類の時代に自明でない 6 重可移群が無さそうなことから、6-design は存在しないだろうと思われていたこともあったようである。しかし、有限単純群の分類が完成し自明でない 6 重可移群の存在が否定されたが、6-design の例は構成されてその数年後に任意の t に対して t-design の存在が示されたことになる。

コードから Assmus-Mattson の定理から得られるデザインについても類似性が見られる。Golay code から Witt system 5-(24, 8, 1) design 他には QR_{48} code から 5-(48, 12, 8) design が得られるように 5-design の例は幾つか知られているが、t が 6 以上のデザインの例は知られていなく、その存在・非存在は未解決である。

本稿では Extremal binary doubly even self-dual code から Assmus-Mattson の定理によって得られるデザインについて述べる。このコードの系列は TypeII とも呼ばれ特に長さが 24 の倍数の時は前述の Golay code および QR_{48} code を含み最も重要なコードの系列の一つと言われている。このコードの系列からは Assmus-Mattson の定理によって (長さを n とすると) (i) n=24m の場合 5-design, (ii) $n=24m+8$ の場合 3-design, (iii) $n=24m+16$ の場合 1-design が得られる。

今回はこのコードの系列でかつ Minimum weight から得られる t-design についてであるが、t の値についてある上限を得たので報告させて頂く。また今回の内容はすでに論文で発表しているので詳細は [5] をご覧ください。

2 知られていた諸結果

長さ n の extremal binary doubly even self-dual code を C とする。ここで C の minimum weight は $d(C) = 4[n/24] + 4$ である。長さが $n = 24m$ の場合存在が知られているのは $24, 48$ のときだけであり、特に長さ 72 の場合は有名な未解決問題である。また、非存在については Zhang [11] より (i) $n = 24m$ の場合 $m \geq 154$, (ii) $n = 24m + 8$ の場合 $m \geq 159$, (iii) $n = 24m + 16$ の場合 $m \geq 164$ で非存在が分かっている。

ここでは $n = 24m$ のときについて述べる。よって、C を extremal binary doubly-even $[24m, 12m, 4m + 4]$ code とする。

$c = (c_1, \ldots, c_n) \in C$, $(c_i \in \mathbb{F}_2)$ に対して、$supp(c) = \{i : c_i \neq 0\}$ を c のサポートと呼ぶ。X を C の n 個の座標、$\mathcal{B}$ を weight w のコードワード全体のサポートとする。すると、結合構造 $D_w = (X, \mathcal{B})$ を C の weight w のサポートデザインという。ここで $w \equiv 0 \pmod 4$, $4[n/24] + 4 \leq w \leq 24m - (4[n/24] + 4)$ である。

さらに、ここでは minimum weight $4m + 4$ に対するサポートデザインを $D(= D_{4m+4})$ そのパラメータを t-$(24m, 4m + 4, \lambda_t)$ とする。すると、主に次のことが知られている。

1. 先に述べた Zhang の結果から D が存在するならば $1 \leq m \leq 153$ より、t の値は高々有限である。

2. Assmus-Mattson theorem より、D は 5-$(24m, 4m + 4, \binom{5m-2}{m-1})$ design である。

3. $\lambda_t = \binom{5m-2}{m-1}\binom{4m-1}{t-5}/\binom{24m-5}{t-5}$ は正の整数である。$(t \geq 6)$

4. A strengthening of the Assmus-Mattson theorem (Calderbank, Delsarte and Sloane [4], 1991) より、D は $\{1, 2, 3, 4, 5, 7\}$-design である。
   言い換えると、6-design $\Longleftrightarrow$ 7-design が得られる。

   $1 \leq m \leq 153$ に対して、λ_6 と λ_7 の値が両方とも正の整数ならば、
   $m \in \{5, 8, 15, 19, 35, 40, 41, 42, 50, 51, 52, 55, 57, 59, 60, 63, 65, 74, 75, 76, 80, 86, 90, 93, 100, 101, 104, 105, 107, 118, 125, 127, 129, 130, 135, 143, 144, 150, 151\}$.

5. 2006年の (Bannai-Koike-Shinohara-Tagami [2]) の論文 Section 3 において上限 $t \leq 8$ が与えられた。また、$1 \leq m \leq 153$ のうち、$t \geq 6$ の t-design になる可能性について 38 個の m が与えられた。まとめると次の表のとおりである。

t-design	m	total
5-design	$1 \leq m \leq 153$	153
7-design (6-design)	8, 15, 19, 35, 40, 41, 42, 50, 51, 52, 55, 57, 59, 60, 63, 65, 74, 75, 76, 80, 86, 90, 93, 100, 101, 104, 105, 107, 118, 125, 127, 129, 130, 135, 143, 144, 150, 151	38
8-design	8, 42, 63, 75, 130	5

3 手法と t の上限

D の t の上限を与えた結果とその手法についての概要を述べる。

C_u を C の weight u のコードワード全体の集合とする。$(4m + 4 \leq u \leq 20m - 4)$ $a \in C_u$ に対して、$n_j^u := \left|\{c \in C_{4m+4} : |supp(a) \cap supp(c)| = j\}\right|$ と定義する。

すると、$s = 0, 1, \ldots, t$ に対して、$\displaystyle\sum_{j=0}^{4m+4} \binom{j}{s} n_j^u = \binom{u}{s} \lambda_s$ が成り立つ。

次に $0 \le s \le t$ に対して、$A_s^u = \sum_{j=0}^{4m+4} (j)_s n_j^u = (u)_s \lambda_s$ とおく。
($(i)_s = i(i-1)\cdots(i-s+1)$)

ここで、D の 7-design になる可能性について調べるため

$$F(m,u;[x_1,x_2,x_3,x_4,x_5,x_6,x_7]) = \sum_{j=0}^{4m+4} (j-x_1)(j-x_2)\cdots(j-x_7)n_i^u$$

と定義すると、

- $S(\alpha,\beta)$: 第 2 種 Stirling numbers $x^\alpha = \sum_{\beta=0}^{\alpha} S(\alpha,\beta)(x)_\beta$ と
- $\sigma_{\theta,\tau}$: elementary symmetric polynomials　を用いて

$$F(m,u;[x_1,x_2,x_3,x_4,x_5,x_6,x_7]) = \sum_{\theta=0}^{7}(-1)^\theta \sigma_{\theta,7}\left(\sum_{h=0}^{7-\theta} S(7-\theta,h)A_h^u\right)$$

が得られる。すると、次のような計算ができる。

$$\begin{aligned}
&F(m,u;[0,2,4,6,8,10,12])\\
&= \sum_{j=0}^{4m+4} j(j-2)(j-4)(j-6)(j-8)(j-10)(j-12)n_j^u\\
&= 10395A_1^u - 10395A_2^u + 4725A_3^u - 1260A_4^u + 210A_5^u - 21A_6^u + A_7^u.
\end{aligned}$$

ここで、n_{14}^u について解くと (n_j^u は定義より、正の整数である)

$$n_{14}^u = \frac{F(m,u;[0,2,4,6,8,10,12])}{645120} - 8n_{16}^u - 36n_{18}^u - \cdots - \binom{2m+2}{7} n_{4m+4}^u$$

- $m \in \{8,40,42,50,74,76,80,86,100,130,144,150\}$ のとき、$\frac{F(m,4m+4;[0,2,4,6,8,10,12])}{645120}$ は整数でない。よって、このとき D は 7-design でない。
- $m \in \{5,19,35,41,51,65,75,101,129\}$ のとき、$\frac{F(m,4m+8;[0,2,4,6,8,10,12])}{645120}$ は整数でない。よって、このとき D は 7-design でない。

最後に、8-design の可能性の残った $m = 63$ に対して、

$$\begin{aligned}
F(m,4m+4;[x_1,x_2,x_3,x_4,x_5,x_6,x_8]) &= \sum_{i=0}^{4m+4} (i-x_1)(i-x_2)\cdots(i-x_8)n_i\\
&= \sum_{\theta=0}^{8}(-1)^\theta \sigma_{\theta,8}\left(\sum_{h=0}^{8-\theta} S(8-\theta,h)A_h\right).
\end{aligned}$$

から計算し、n_{16}^u について解くと

$$n_{16} = \frac{F(m,4m+4;[0,2,4,6,8,10,12,14])}{10321920} - 9n_{18} - 45n_{20} - \cdots - \binom{2m+2}{8} n_{4m+4}.$$

$m = 63$ のとき、$\frac{F(m,4m+4;[0,2,4,6,8,10,12,14])}{10321920}$ は整数でない。よって、このとき D は 8-design でない。

以上より、次の主結果を得る。

Theorem 3.1 (N. Horiguchi, T. Miezaki and H. Nakasora). D の上限は $t \leq 7$ である。また、*7-design* になる可能性のある m については以下の表の通りである。

t-design	m	total
5-design	$1 \leq m \leq 153$	153
7-design (6-design)	15, 52, 55, 57, 59, 60, 63, 90, 93, 104, 105 107, 118, 125, 127, 135, 143, 151	18

また、他の長さ $n = 24m + 8$, $24m + 16$ についても同様な手法で次のような結果を得た。

Theorem 3.2. *[N. Horiguchi, T. Miezaki and H. Nakasora] Let D_1 and D_2 be the support t-designs of the minimum weight of an extremal binary doubly even self-dual $[24m + 8, 12m + 4, 4m + 4]$ code ($m \leq 158$) and $[24m + 16, 12m + 8, 4m + 4]$ code ($m \leq 163$), respectively.*

(1) D_1 の上限は $t \leq 7$ である。

t-design	m	total
3-design	$1 \leq m \leq 158$	158
5-design (4-design)	15, 35, 45, 58, 75, 85, 90, 95, 113, 115, 120, 125	12
6-design	58, 90, 113	3
7-design	58	1

(2) D_2 の上限は $t \leq 5$ である。

t-design	m	total
1-design	$1 \leq m \leq 163$	163
3-design (2-design)	5, 10, 20, 23, 25, 35, 44, 45, 50, 55, 60, 70, 72, 75, 79, 80, 85, 93, 95, 110, 118, 120, 121, 123, 125, 130, 142, 144, 145, 149, 150, 155, 156, 157, 160, 163	36
4-design	10, 79, 93, 118, 120, 123, 125, 142	8
5-design	79, 93, 118, 120, 123, 125, 142	7

References

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combinatorial Theory* **6** (1969), 122-151.

[2] E. Bannai, M. Koike, M. Shinohara and M. Tagami, Spherical designs attached to extremal lattices and the modulo p property of Fourier coefficients of extremal modular forms, *Mosc. Math. J.* **6** (2006), 225-264.

[3] W. Bosma, J. Cannon and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp.*, 24, 3/4:235-265, 1997.

[4] A. R. Calderbank, P. Delsarte and N. J. A. Sloane, A strengthening of the Assmus-Mattson theorem, *IEEE Trans. Inform. Theory* **37** (1991), 1261-1268.

[5] N. Horiguchi, T. Miezaki and H. Nakasora, On the support designs of extremal binary doubly even self-dual codes, *Des. Codes Cryptogr.*, published online (2012).

[6] H. Koch, On self-dual doubly-even extremal codes, *Discrete Math.* **83** (1990), no. 2-3, 291-300.

[7] S.S. Magliveras and D.W. Leavitt, Simple six designs exist, *Congressus Numerantium* Vol. 40 (1983), 195-205.

[8] L. Teirlinck Non-trivial t-designs without repeated blocks exist for all t, *Discrete Math.* Vol. 306, (2006), 1060-1067.

[9] V. D. Tonchev, *Combinatorial configurations designs, codes, graphs,* Translated from the Bulgarian by Robert A. Melter. Pitman Monographs and Surveys in Pure and Applied Mathematics, 40. Longman Scientific & Technical, Harlow; John Wiley & Sons, Inc., New York, 1988.

[10] E. W. Weisstein, "Stirling Number of the Second Kind." From MathWorld–A Wolfram Web Resource.
`http://mathworld.wolfram.com/StirlingNumberoftheSecondKind.html`.

[11] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999), 277-286.

The Critical Problem in Coding Theory

Keisuke Shiromoto (keisuke@kumamoto-u.ac.jp)
Department of Mathematics and Engineering,
Kumamoto University,
2-39-1, Kurokami, Kumamoto 860-8555, Japan

1 Preliminaries

Let E be a finite set and $\rho : 2^E \to \mathbb{Z}^+ \cup \{0\}$ be a function. $M = (E, \rho)$ is called a *matroid* if M has the following properties:

(R1) If $X \subseteq E$, then $0 \leq \rho(X) \leq |X|$.

(R2) If $X \subseteq Y \subseteq E$, then $\rho(X) \leq \rho(Y)$.

(R3) If X and Y are subsets of E, then

$$\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y).$$

We refer the reader to [9] and [11] for the basic definitions in matroid theory.

For a matroid $M = (\rho, E)$, the *characteristic polynomial* $p(M; \lambda)$ of M is defined by

$$p(M; \lambda) = \sum_{X \subseteq E} (-1)^{|X|} \lambda^{\rho(E) - \rho(X)}.$$

Let M be a matroid representable over $GF(q) = \mathbb{F}_q$. It is well known that $p(M; q^k) \geq 0$, for all $k \in \mathbb{Z}^+$. Then the *critical exponent* $c(M; q)$ of M is defined by

$$c(M; q) = \begin{cases} \infty, & \text{if } M \text{ has a loop;} \\ \min\{j \in \mathbb{Z}^+ \ : \ p(M; q^j) > 0\}, & \text{otherwise.} \end{cases}$$

Thus if M has no loops, then $p(M; q^k) > 0$ for all $k \geq c(M; q)$. For a matroid M which is representable over $\mathbb{F}_q$, one of the critical problems is the problem of determining the critical exponent $c(M; q)$ (cf. [6, 1]). However, this is difficult in general.

The *support* and *weight* of each vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_q^n$ is given by

$$\begin{aligned} \mathrm{supp}(\boldsymbol{x}) &:= \{ i \ : \ x_i \neq 0 \}; \\ \mathrm{wt}(\boldsymbol{x}) &:= |\mathrm{supp}(\boldsymbol{x})|. \end{aligned}$$

Similarly, the *support* and *weight* of each subset $B \subseteq \mathbb{F}_q^n$ are defined as follows:

$$\mathrm{Supp}(B) := \bigcup_{\boldsymbol{x} \in B} \mathrm{supp}(\boldsymbol{x});$$
$$\mathrm{wt}(B) := |\mathrm{Supp}(B)|.$$

Let C be an $[n,k]$ code over $\mathbb{F}_q$, that is, a k-dimensional subspace of the vector space $\mathbb{F}_q^n$. Let G be a generator matrix of C, that is, a $k \times n$ matrix over $\mathbb{F}_q$ whose rows form a basis for C. Set $E := \{1, 2, \ldots, n\}$. For each subset $X \subseteq E$, the *punctured code*, denoted by $C \setminus X$, is the linear code obtained by deleting the coordinate X from each codeword in C. It is easy to check that if we define a function ρ by $\rho(X) = \dim C \setminus (E - X)$, for any $X \subseteq E$, then $M_C = (E, \rho)$ is a matroid, conversely, if M is a representable matroid over $\mathbb{F}_q$, then there exists a linear code C such that $M = M_C$ (cf. [11, 9]). Thus, for an $[n,k]$ code over $\mathbb{F}_q$, the *characteristic polynomial* $p(C;\lambda)$ of C is defined by

$$p(C;\lambda) = \sum_{X \subseteq E} (-1)^{|X|} \lambda^{k - \dim C \setminus X},$$

and the *critical exponent* $c(C;q)$ of C is defined by

$$c(C;q) = \begin{cases} \infty, & \text{if } \mathrm{Supp}(C) \neq E; \\ \min\{j \in \mathbb{Z}^+ \ : \ p(C;q^j) > 0\}, & \text{otherwise.} \end{cases}$$

For any subset $X \subseteq E$, the *shortened code*, denoted by C/X, is the linear code obtained by deleting the (zero) coordinates X from each codewords $\boldsymbol{x} \in C$ with $\mathrm{supp}(\boldsymbol{x}) \cap X = \emptyset$. Crapo and Rota ([4]) prove the following theorem widely known as the *Critical Theorem* (cf. Theorem 2 in [1]).

Lemma 1 (The Critical Theorem) *Let C be an $[n,k]$ code over $\mathbb{F}_q$. For any $X \subseteq E$ and any $m \in \mathbb{Z}^+$, the number of ordered m-tuples $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m)$ of codewords $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ in C with $\mathrm{supp}(\boldsymbol{v}_1) \cup \cdots \cup \mathrm{supp}(\boldsymbol{v}_m) = X$ is $p(C/X; q^m)$.*

From Lemma 1, if there exists at least one set of m codewords $V = \{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m\}$ in C with $\mathrm{Supp}(V) = E$, then $p(C;q^m) > 0$ and so $c(C;q) \leq m$. For $0 \leq r \leq k$ and any $X \subseteq E$, let $A_X^{(r)}$ be the number of r-dimensional subcodes D of C with $\mathrm{Supp}(D) = X$. We note that the polynomial

$$W_C^{(r)}(x,y) = \sum_{i=0}^{n} A_i^{(r)} x^{n-i} y^i$$

is the r-th *support weight enumerator* of C, where $A_i^{(r)} \sum_{X \in \binom{E}{i}} A_X^{(r)}$ (cf. [5]).

Then we have the following result:

Proposition 2 *Let C be an $[n,k]$ code over $\mathbb{F}_q$ having generator matrix G and set $E = \{1, 2, \ldots, n\}$. The following are equivalent:*

(1) $c(C;q) = m$.

(2) $\min\{r : 0 \le r \le k,\ A_E^{(r)} \neq 0\} = m$.

(3) *m is the smallest positive integer such that there exists a $(k-m)$-dimensional subspace U of $\mathbb{F}_q^k$ which does not contain any of the n column vectors of G.*

Example 3 Let C be the binary $[10, 4]$ code having generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

If we take a 3-dimensional subcode

$$B = \langle (1,1,1,1,0,0,1,1,0,0), (1,0,0,0,1,1,1,0,0,0), (1,0,1,0,0,1,0,1,1,1) \rangle$$

of C, then $\mathrm{Supp}(B) = \{1,2,3,4,5,6,7,8,9,10\} = E$. And there does not exist any 2-dimensional subcode of C whose support is equal to E. From Proposition 2, it follows that $c(M_C; 2) = 3$.

2 Bounds on Critical Exponents

Let G be a $k \times n$ matrix over $\mathbb{F}_q$ which contains as columns exactly one multiple of each nonzero vector in $\mathbb{F}_q^k$. Then the $[n = (q^k - 1)/(q-1), k]$ code C having generator matrix G is a dual Hamming code and $C^\perp$ is a $[n, n-k, 3]$ Hamming code. It is also known that, for any r, $1 \le r \le k$,

$$\sum_{X \in \binom{E}{i}} A_X^{(r)} = \begin{cases} \begin{bmatrix} k \\ r \end{bmatrix}_q & i = (q^k - q^{k-r})/(q-1), \\ 0 & \text{otherwise,} \end{cases}$$

where $\begin{bmatrix} k \\ r \end{bmatrix}_q$ denotes the Gaussian binomial coefficient (cf. [5]). So we have that $i = n$ if and only if $r = k$.

Proposition 4 *If C is a dual Hamming $[n, k]$ code over $\mathbb{F}_q$, then*

$$\min\{r : 0 \le r \le k,\ A_E^{(r)} \neq 0\} = k.$$

A *maximum distance separable* (MDS) code over $\mathbb{F}_q$ is an $[n, k]$ code over $\mathbb{F}_q$ whose minimum Hamming weight is $n - k + 1$. According to Theorem 6, p. 321, in [7], the number A_w of codewords of weight w in an MDS $[n, k]$ code over $\mathbb{F}_q$ is given by

$$A_w = \binom{n}{w}(q-1)\sum_{j=0}^{w-d}(-1)^j \binom{w-1}{j} q^{w-d-j}, \tag{1}$$

for $d \le w \le n$, where $d = n - k + 1$.

Theorem 5 *Let C be an MDS $[n,k]$ code over $\mathbb{F}_q$. Then*

$$c(C;q) \leq 2.$$

Remark 6 From Proposition 4, for a $[q+1,2]$ MDS code C over $\mathbb{F}_q$, we have that $c(C;q)=2$. So the bound is sharp.

It is known that a uniform matroid $U_{n,m}$ representable over $\mathbb{F}_q$ is corresponding to a matroid obtained by an MDS $[n,m]$ code over $\mathbb{F}_q$ (cf. [9]). As a corollary of the above theorem, we have the following.

Corollary 7

$$c(U_{n,m};q) \leq 2.$$

In general, we have the following bound on critical exponents for linear codes over finite fields.

Theorem 8 *Let C be an $[n,k]$ code over $\mathbb{F}_q$ having generator matrix G. If $d^\perp > q$, then*

$$c(C;q) \leq k - d^\perp + 2,$$

except when C is a binary codes such that $d^\perp = n$ is odd or such that $n = 2^k - 1$ and $d^\perp = 3$ in which case $c(C;q) = k - d^\perp + 3$, where $C^\perp$ denotes the minimum Hamming weight of the dual code $C^\perp$.

As a corollary of the above theorem, we have the following bound on critical exponents for representable matroids over finite fields.

Corollary 9 *Let M be a rank k representable simple matroid over $\mathbb{F}_q$ with girth g. If $g > q$, then*

$$c(M;q) \leq k - g + 2,$$

except when M is a binary matroid isomorphic to $U_{2l+1,2l}$ or $PG(k-1,2)$ in which case $c(M;q) = k - g + 3$.

Example 10 Let C be the ternary $[11,5]$ code having generator matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 & 1 & 2 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 & 1 & 0 & 1 \end{pmatrix}.$$

Then the dual code $C^\perp$ is an $[11,6,5]$ quadratic residue code. By a Magma calculation, we have that

$$A_E^{(1)} = 0,\ A_E^{(2)} = 330,\ A_E^{(3)} = 825,\ A_E^{(4)} = 110,\ A_E^{(5)} = 1,$$

where $E = \{1,2,\ldots,11\}$. If M_C is the vector matroid obtained from G, then $c(M_C;3) = 2 (= 5-5+2)$ and so M_C holds the equality in Theorem 8.

3 A construction of tangential blocks

As defined in [3, 6], for $1 \leq r \leq k-1$, a set M of points of the projective geometry $PG(k-1,q)$ is an *r-block* over $\mathbb{F}_q$ if every $(k-r)$-dimensional subspace in $PG(k-1,q)$ contains at least one point in M. If X is a flat in M, a *tangent* of X is a $(k-r)$-dimensional subspace U in $PG(k-1,q)$ such that

$$M \cap U = X.$$

An r-block M is called to be *minimal* if every point in M has a tangent, and to be *tangential* if every proper nonempty flat in M of rank not exceeding $k-r$ has a tangent.

Alternatively, a matroid M is a *tangential r-block* over $\mathbb{F}_q$ if the following conditions hold:

(i) M is simple and representable over $\mathbb{F}_q$.

(ii) $p(M;q^r) = 0$.

(iii) $p(M/F;q^r) > 0$ whenever F is a proper nonempty flat of M.

Proposition 11 *For any positive integer k, set $K := \{1,2,\ldots,k\}$. For an m $(1 \leq m \leq k)$, we take an m elements subset $T \in \binom{K}{m}$ and a family $\mathcal{V}$ of $(m-1)$ distinct points $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{m-1} \in PG(k-1,q)$ with $\mathrm{supp}(\boldsymbol{v}_i) \cap T = \emptyset$, $i = 1,2,\ldots,m-1$. Define*

$$X^T := \{\boldsymbol{x} \in PG(k-1,q) \ : \ \mathrm{supp}(\boldsymbol{x}) \cap T = \emptyset\},$$
$$Y_{\mathcal{V}}^T := \{\boldsymbol{x} \in PG(k-1,q) \ : \ |\mathrm{supp}(\boldsymbol{x}) \cap T| = 1\} \setminus \{\boldsymbol{v}_i + \lambda \boldsymbol{e}_j \ : \ \boldsymbol{v}_i \in \mathcal{V},\ \lambda \in \mathbb{F}_q - \{0\},\ j \in T\},$$
$$Z^T := \{\boldsymbol{x} \in PG(k-1,q) \ : \ \mathrm{supp}(\boldsymbol{x}) \in \binom{T}{2}\}.$$

Then $M := X^T \cup Y_{\mathcal{V}}^T \cup Z^T$ is a $(k-m)$-block over $\mathbb{F}_q$.

Then we can give a construction of tangential blocks as follows:

Theorem 12 *Let M be the set of points in $PG(k-1,q)$ defined in Proposition 11. If $m-1 \leq q^{k-m-1}$, then M is a tangential $(k-m)$-block over $GF(q)$.*

From the definition, M is a minimal r-block over $\mathbb{F}_q$ if and only if $c(C;q) = r+1$ for the linear code having generator matrix G whose column vectors are all points in M (cf. p. 168 in [3]).

Corollary 13 *Let M be the set of points defined in Proposition 11. If $m = 2$, then the linear code C over $\mathbb{F}_q$ whose generator matrix obtained from M attains the bound in Theorem 8.*

Proof. From the definition of M, it finds that $d^{\perp} = 3$, since there exist three column vectors in G which are linearly dependent. Thus we have that

$$k-2+1 = k-1 = c(C;q) \leq k-3+2 = k-1.$$

□

Example 14 Let C be the binary $[22,5]$ code over $\mathbb{F}_q$ having generator matrix

$$G = \begin{pmatrix} 1&0&0&0&0&0&1&1&1&1&1&1&1&0&0&0&0&1&1&0&0&0 \\ 0&1&0&0&0&1&1&1&0&1&1&0&0&1&1&0&0&1&1&1&1&0 \\ 0&0&1&0&0&1&1&0&1&0&0&1&1&0&0&1&1&1&1&1&1&0 \\ 0&0&0&1&0&0&0&0&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \\ 0&0&0&0&1&0&0&0&0&0&1&0&1&0&1&0&1&0&1&0&1&1 \end{pmatrix}.$$

From Theorem 12, G forms a binary tangential 3-block. Moreover, we have that

$$\begin{aligned} p(M_C;\lambda) &= \lambda^5 - 22\lambda^4 + 175\lambda^3 - 610\lambda^2 + 9 - 4\lambda - 448 \\ &= (\lambda-1)(\lambda-2)(\lambda-4)(\lambda-7)(\lambda-8). \end{aligned}$$

If M_C is the vector matroid obtained from G, then $c(M_C;2) = 4(= 5-3+2)$ and so M_C holds the equality in Theorem 8.

References

[1] T. Britz, Extensions of the critical theorem, *Discrete Mathematics* **305** (2005), pp.55–73.

[2] T. Britz, Higher support matroids, *Discrete Mathematics* **307** (2007), pp.2300–2308.

[3] T. Brylawski and J. Oxley, The Tutte polynomial and its applications; *Matroid applications*, pp. 123–225, Cambridge Univ. Press, Cambridge, 1992.

[4] H. Crapo and G.-C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial geometries*, MIT Press, Cambridge, MA, London, 1970 (Preliminary Edition).

[5] T. Kløve, Support weight distribution of linear codes, *Discrete Mathematics* **106/107** (1992), pp. 311–316.

[6] J. P. S. Kung, Critical problems, in: *Matroid Theory*, Seattle, WA, 1995, *Contemporary Mathematics*, **197**, American Mathematical Society, Providence, RI, 1996, pp. 1–127.

[7] F. J. MacWilliams and N. J. A. Sloane, *TheTheory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1977.

[8] J. Oxley, Colouring, packing and the critical problem, *Quart. J. Math. Oxford* (2), **29** (1978), pp. 11–22.

[9] J. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.

[10] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, 2003.

[11] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

TD-pairs of shape 1, 2, 2, ..., 2, 2, 1 at $q = 1$

佐藤重吾（金沢大学大学院自然科学研究科）

Abstract

shape 1, 2, 2, ..., 2, 2, 1, type II というクラスの TD-pairs の分類を行ったので，それを報告する．

この報告では，まず，TD-pairs の定義し，次に，TD-pair の type および shape について説明する．最後に，TD-pairs の shape 1, 2, 2, ..., 2, 2, 1, type II を分類した結果を述べる．

TD-pairs

まず，TD-pairs を定義する．V を複素数体上の有限次元ベクトル空間，A, A^* を V 上の線型変換で対角化可能なものとする．A, A^* の固有値をそれぞれ $\theta_0, \theta_1, \ldots, \theta_d$; $\theta_0^*, \theta_1^*, \ldots, \theta_d^*$ とし，これらの固有値に関する固有空間をそれぞれ，$V_0, V_1 \ldots, V_d$; $V_0^*, V_1^* \ldots, V_{d^*}^*$ とおく：

$$V = \bigoplus_{j=0}^{d} V_j, \quad A|V_j = \theta_j,$$

$$V = \bigoplus_{j=0}^{d^*} V_j^*, \quad A^*|V_j^* = \theta_j^*.$$

次の三つをみたすとき，(A, A^*) を V 上の *TD-pair* (*tridiagonal pair*) と呼ぶ：

(i) 次をみたす A の固有空間 $V_0, V_1, \ldots, V_d$ の順序づけが存在する：任意の $j = 0, 1, \ldots, d$ に対して，$A^*V_j \subseteq V_{j-1} + V_j + V_{j+1}$. ただし，$V_{-1} = 0$, $V_{d+1} = 0$ である．

(ii) 次をみたす A^* の固有空間 $V_0^*, V_1^*, \ldots, V_d^*$ の順序づけが存在する：任意の $j = 0, 1, \ldots, d^*$ に対して，$AV_j^* \subseteq V_{j-1}^* + V_j^* + V_{j+1}^*$. ただし，$V_{-1}^* = 0$, $V_{d^*+1}^* = 0$ である．

(iii) V は (A, A^*)-module として既約である．すなわち，V の部分空間で A-不変かつ A^*-不変であるのは，0 と V に限る．

(A, A^*) が TD-pair ならば，$d = d^*$ が成り立つ．この整数 d を TD-pair の *diameter* と呼ぶ．

次に TD-pair の同型を定義する．(B, B^*) を複素数体上の有限次元ベクトル空間 W 上の TD-pair とする．二つの TD-pairs (A, A^*), (B, B^*) が同型であるとは，

$$B = \varphi A \varphi^{-1}, \quad B^* = \varphi A^* \varphi^{-1}$$

をみたす線形空間としての同型写像 $\varphi: V \longrightarrow W$ が存在することをいう．

Type of TD-pairs

次に，TD-pairs の type を定義する．そのために，TD-pair の固有値列に関する事実を二つ紹介する．

(A, A^*) を diameter d の TD-pair とし，θ_j を A の V_j 上での固有値，θ_j^* を A^* の V_j^* 上での固有値とする．

Fact 1. $d \geq 3$ のとき，次をみたす複素数 β が一意的に存在する：任意の $j = 1, 2, \ldots, d-2$ に対して，

$$\begin{aligned} \beta &= \frac{\theta_{j+2} - \theta_{j+1} + \theta_j + \theta_{j-1}}{\theta_{j+1} - \theta_j} \\ &= \frac{\theta_{j+2}^* - \theta_{j+1}^* + \theta_j^* + \theta_{j-1}^*}{\theta_{j+1}^* - \theta_j^*}. \end{aligned}$$

Fact 2. A, A^* の固有値列は次のいずれか（$q + q^{-1} = \beta$）である：

$$\text{(I) } q \neq \pm 1 \quad \begin{cases} \theta_j = \alpha_1 + \alpha_2 q^j + \alpha_3 q^{-j} \\ \theta_j^* = \alpha_1^* + \alpha_2^* q^j + \alpha_3^* q^{-j} \end{cases}$$

$$\text{(II) } q = +1 \quad \begin{cases} \theta_j = \alpha_1 + \alpha_2 j + \alpha_3 j^2 \\ \theta_j^* = \alpha_1^* + \alpha_2^* j + \alpha_3^* j^2 \end{cases}$$

$$\text{(III) } q = -1 \quad \begin{cases} \theta_j = \alpha_1 + \alpha_2 (-1)^j + \alpha_3 j (-1)^j \\ \theta_j^* = \alpha_1^* + \alpha_2^* (-1)^j + \alpha_3^* j (-1)^j \end{cases}$$

for $j = 0, 1, \ldots, d$. ここで，$\alpha_1, \alpha_2, \alpha_3; \alpha_1^*, \alpha_2^*, \alpha_3^*$ は j に依らない定数である．

TD-pair は，$q \neq \pm 1$ のとき type I, $q = +1$ のとき type II, $q = -1$ のとき type III と呼ばれる．

Type I の TD-pairs は分類済みである（ただし，発表されているのは，$q \neq$ root of unity の場合のみ）．

Shape of TD-pairs

次に，TD-paris の shape を定義する．type は TD-pair の固有値列に関することであった．shape は TD-pair の固有空間の次元に関することである．

TD-pair の固有空間の次元に関して，$\dim V_j = \dim V_j^*$ が成り立つことが知られている．そこで，$\rho_j = \dim V_j$ と置き，固有空間の次元の列 $\rho_0, \rho_1, \ldots, \rho_d$ を TD-pair の *shape* と呼ぶ．shape は一般に symmetric かつ unimodal であることがわかっている，すなわち，

$$\rho_j = \rho_{d-j}$$

$$\rho_0 \leq \rho_1 \leq \rho_2 \leq \cdots \geq \rho_{d-2} \geq \rho_{d-1} \geq \rho_d$$

が成り立つ．さらに，$\rho_0 = 1$ が成り立つこと（shape conjecture と呼ばれていた）がわかっている．

とくに，shape が 1, 1, ..., 1 の TD-pairs は *L-pairs* (*Leonard pairs*) と呼ばれている．L-pairs は分類済みであり，{L-pairs } $\longleftrightarrow$ { Askey-Wilson polynomials} という全単射な対応があることがわかっている．

L-pairs の次のクラス——次に簡単なクラス——は，shape 1, 2, 2, ..., 2, 2, 1 の TD-pairs である．われわれは，この shape の TD-pair を扱う．

TD-pairs of shape 1, 2, 2, ..., 2, 2, 1

われわれの問題は，'shape 1, 2, 2, ..., 2, 2, 1 の TD-pairs of type II を分類せよ' である．type I の TD-pair は分類済みであることに注意する．

TD-pair (A, A^*) の固有値列

$$\begin{cases} \theta_i = \alpha_1 + \alpha_2 i + \alpha_3 i^2 \\ \theta_i^* = \alpha_1^* + \alpha_2^* i + \alpha_3^* i^2 \end{cases}$$

に現れる係数のペア (α_3, α_3^*) によって三つの場合に分ける：

(1) $\alpha_3 \neq 0, \alpha_3^* \neq 0$

(2) $\alpha_3 \neq 0, \alpha_3^* = 0$

(3) $\alpha_3 = 0, \alpha_3^* = 0$

定理. Shape 1, 2, 2, ..., 2, 2, 1 の TD-pair of type II は，次の行列のペア (A, A^*) と同型である：

$$A = \begin{pmatrix}
\theta_0 & & & & & \\
\lambda_0 & \theta_1 & & & & \\
\xi_1 & & \theta_1 & & & \\
 & \xi_1 & \lambda_1 & \theta_2 & & \\
 & & \xi_2 & & \theta_2 & \\
 & & & \ddots & \ddots & \ddots \\
 & & & & \ddots & & \ddots \\
 & & & & \xi_{d-2} & \lambda_{d-2} & \theta_{d-1} & \\
 & & & & & \xi_{d-1} & & \theta_{d-1} & \\
 & & & & & & \xi_{d-1} & \lambda_{d-1} & \theta_d
\end{pmatrix}$$

$$A^* = \begin{pmatrix}
\theta_0^* & \mu_0 & \eta_1 & & & & \\
 & \theta_1^* & & \eta_1 & & & \\
 & & \theta_1^* & \mu_1 & \eta_2 & & \\
 & & & \theta_2^* & & \ddots & \\
 & & & & \theta_2^* & \ddots & \ddots & \\
 & & & & & \ddots & & \eta_{d-2} & \\
 & & & & & & \ddots & \mu_{d-2} & \eta_{d-1} & \\
 & & & & & & & \theta_{d-1}^* & & \eta_{d-1} \\
 & & & & & & & & \theta_{d-1}^* & \mu_{d-1} \\
 & & & & & & & & & \theta_d^*
\end{pmatrix}$$

（ただし，空白部は 0 を表す.）行列の各成分は次のように表される：

(1) $\alpha_3 \neq 0, \alpha_3^* \neq 0$ のとき，

$$\begin{cases}
\theta_i = hi(i+1+\omega) + \theta_0 & (0 \leq i \leq d) \\
\lambda_i = h(2i+1+b+\Omega) & (0 \leq i \leq d-1) \\
\xi_i = hi(i+a+\Omega+d/2) & (1 \leq i \leq d-1)
\end{cases}$$

$$\begin{cases}
\theta_i^* = h^* i(i+1+\omega^*) + \theta_0^* & (0 \leq i \leq d) \\
\mu_i = -h^*(2i+1-b+\Omega) & (0 \leq i \leq d-1) \\
\eta_i = h^*(i-d)(i-a+\Omega+d/2) & (1 \leq i \leq d-1)
\end{cases}$$

where $\Omega = 1 + (\omega + \omega^*)/2$

(2) $\alpha_3 \neq 0$, $\alpha_3^* = 0$ のとき,

$$\begin{cases} \theta_i = hi(i+1+\omega) + \theta_0 \quad (0 \leq i \leq d) \\ \lambda_i = h(2i+1+b) \quad (0 \leq i \leq d-1) \\ \xi_i = hi(i+a+d/2) \quad (1 \leq i \leq d-1) \end{cases}$$

$$\begin{cases} \theta_i^* = h^* i + \theta_0^* \quad (0 \leq i \leq d) \\ \mu_i = -h^* \quad (0 \leq i \leq d-1) \\ \eta_i = h^*(i-d) \quad (1 \leq i \leq d-1) \end{cases}$$

(3) $\alpha_3 = 0$, $\alpha_3^* = 0$ のとき,

$$\begin{cases} \theta_i = hi + \theta_0 \quad (0 \leq i \leq d) \\ \lambda_i = hb \quad (0 \leq i \leq d-1) \\ \xi_i = hai \quad (1 \leq i \leq d-1) \end{cases}$$

$$\begin{cases} \theta_i^* = h^* i + \theta_0^* \quad (0 \leq i \leq d) \\ \mu_i = -h^* \quad (0 \leq i \leq d-1) \\ \eta_i = h^*(i-d) \quad (1 \leq i \leq d-1) \end{cases}$$

ただし，いずれの場合も $\xi_i, \eta_i \neq 0$ である.

参考文献

[1] T. Ito and P. Terwilliger. The augmented tridiagonal algebra. *Kyushu Journal of Mathematics*, 64(1):81–144, 2009.

アソシエーションスキームの圏論的一般化について
— スキーモイドとその圏 —

栗林 勝彦 (信州大学)
2013年6月25日

1. はじめに

本報告集の内容は第３０回代数的組合せ論シンポジウムにおける講演内容とプレプリント [8] の内容に基づいている。特に本稿は [8] で導入した (擬) スキーモイドとそれらがつくる圏の解説とその基本性質の概説を目的とする[*1]。現状を概観する場面や展望, 希望を語る場面では些か「押しつけ」の感が強い。著者が夢を語っている箇所とご理解頂きお許し願いたい。

有限群は群環を経由することで圏論的表現論の道具を用いて有限次元代数の表現論と共通の枠組みで研究が進められている。また分類空間を経由して位相空間の圏上でホモトピー論を用いてその性質が解明されてきた。代数的組合せ論における重要な研究対象であるアソシエーションスキームは有限群の一般化とも考えられる。したがって, それらの特性の解明や, 分類は私たちの興味をそそる非常に重要な問題である。アソシエーションスキームの研究をさらに進めるためには, 有限群の研究の歴史が示すように圏論的枠組みを構築しその研究に必要な道具を整備すること, また分類問題を考察するために適切な不変量を定義することが重要であろう。

一方で小圏のホモトピー論はある意味, 位相空間のホモトピー論と等価である。より正確には小圏の圏と位相空間のつくる圏には Quillen の意味のモデル圏構造が定まり, それらのホモトピー圏は互いに同値になる ([9])。よってトポロジー研究に現れる多くの対象 (CW 複体, シンプレクテック多様体や Lie 群など) はホモトピー論的には小圏に適切な条件を付加して記述できるものと等価であると言って良い。しかしながら, 小圏には「顔」がない。半順序集合 (posets) や亜群等のホモトピー論, 圏論的研究はあるものの, どのような小圏が特別なのかという議論は多くはない。小圏にある特別な性質「顔」を持たせ議論することそして上記のようなアソシエーションスキームの圏論的枠組の構築を目的として本研究プロジェクトは始まった。このような試みの一部を本稿で概説する。

第2章ではアソシエーションスキームを一般化した**スキーモイド**の概念を導入しそれらがつくる圏を定義する。スキーモイドとは小圏の射全体がつくる集合に適切な分割を与える (色分けを行なう) ことで構成されるもので, それらがつくる圏には Hanaki によるアソシエーションスキームの圏や French により導入された圏が埋め込まれる。さらにアソシエーションスキームに Bose-Mesner 代数が同伴するように, スキーモイドに対しても自然に代数が付随して現れる。この代数がスキーモイドに対する基礎圏の圏代数の部分代数として現れることは, 圏論的表現論の道具を用いてスキーモイドが考察できることを示唆している。

第3章では French により導入されたアソシエーションスキームの間の許容写像をスキーモイドの場合に一般化し, その基本性質を述べる。第4章ではスキーモイドの拡張やそれらの分類を Baues-Wirsching の小圏の拡張理論を用いて展開する。第5章ではアソシエーションスキームを完全グラフと考えることで, 小圏とみなしそこからスキーモイドを構成する方法を述べる。今後の展望は第6章で述べられる。

[8] ではさらに thin スキームに対応する thin スキーモイドの概念とそれらがつくるスキーモイドの適切な部分圏と亜群がつくる圏との同値性が述べられている。これらも重要な結果ではあるが, 本稿ではその説明は割愛した。

2. (擬) スキーモイドとスキーモイドの圏

私たちが導入するスキーモイドとの比較のために, まずアソシエーションスキームの定義を思い出す。

[*1] 述べられる定理, 命題等の証明はすべて省略します。[8] を参照してください。

有限集合 X と直積集合 $X\times X$ の分割 S, すなわち巾集合 $2^{X\times X}$ の部分集合であり $X\times X=\amalg_{\sigma\in S}\sigma$ をみたすものを考える。また $g\in S$ に対して

$$g^*:=\{(y,x)\mid (x,y)\in g\}$$

とおき, 対角写像 $\{(x,x)\mid x\in X\}$ を 1_X で表す。分割 S が次の 3 条件をみたすとき組 (X,S) を**アソシエーションスキーム** (AS と以下略記) という。

(1) $1_X\in S$,
(2) $g\in S$ に対して $g^*\in S$,
(3) 任意の $e,f,g\in S$ に対して非負の整数 p^g_{ef} が定まり, 任意の $(x,z)\in g$ に対して

$$p^g_{ef}=\sharp\{y\in X\mid (x,y)\in e \text{ かつ } (y,z)\in f\}.$$

ここで p^g_{ef} は元 $(x,z)\in g$ の取り方に無関係に定まる非負整数であることに注意する。

例えば, 有限群 G を考えるとき $[G]:=\{G_h\}$, $G_h:=\{(k,l)\in G\times G\mid k^{-1}l=h\}$ と定義すると $(G,[G])$ は $p^{G_{fg}}_{G_fG_g}=1$, $h\neq fg$ のとき $p^{G_h}_{G_fG_g}=0$ となり AS となる。

上記 (3) の条件を圏論的な条件に書き換えることで, 擬スキーモイドが定義される。以後, 圏 $\mathcal{C}$ の射 $u:x\to y$ に対して $x=s(u)$, $y=t(u)$ と表す場合がある。

定義 2.1. $\mathcal{C}$ を小圏, すなわち $\mathcal{C}$ の対象全体がつくる類が集合であるとする。$S:=\{\sigma_l\}_{l\in I}$ を $\mathcal{C}$ の射全体がつくる集合 $mor(\mathcal{C})$ の分割であるとする。次の条件をみたすとき, 圏 $\mathcal{C}$ と分割の対 $(\mathcal{C},S)$ を**擬スキーモイド** (quasi-schemoid) と呼ぶ。($\mathcal{C}$ はこの擬スキーモイドの基礎圏とよばれる。)

任意の $\sigma,\tau,\mu\in S$ と μ の任意の射 f, g に対して, 集合としての同型

$$(\pi^\mu_{\sigma\tau})^{-1}(f)\cong(\pi^\mu_{\sigma\tau})^{-1}(g),$$

が成り立つ。ただし, $\pi^\mu_{\sigma\tau}:\pi^{-1}_{\sigma\tau}(\mu)\to\mu$ は結合写像

$$\pi_{\sigma\tau}:\sigma\times_{ob(\mathcal{C})}\tau:=\{(u,v)\in\sigma\times\tau\mid s(u)=t(v)\}\to mor(\mathcal{C})$$

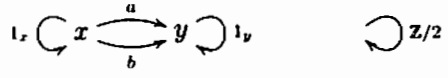
を制限して定義される写像を表している。以下 $(\pi^\mu_{\sigma\tau})^{-1}(f)$ の濃度を $p^\mu_{\sigma\tau}$ と表す。

小圏を対象とし小圏の間の関手を射として得られる圏を Cat, その充満部分圏である亜群 (groupoid) [*2]の圏を Gpd と表す。

例 2.2. (i)(離散的スキーモイド) $\mathcal{C}$ を小圏とし $mor(\mathcal{C})$ の分割 S を $S=\{\{f\}\}_{f\in mor(\mathcal{C})}$ で与えるとき, 対 $K(\mathcal{C}):=(\mathcal{C},S)$ は擬スキーモイドとなる。こうして小圏から自然に擬スキーモイドが得られる。

(ii) (シューアスキーモイド) G を (有限とは限らない) 群とする。G を一つの対象 $\bullet$ のみをもち, 射の集合が G である亜群と考える。G-圏 $\mathcal{D}$, すなわち関手 $F:G\to$ Cat が存在して $\mathcal{D}=F(\bullet)$ となる圏 $\mathcal{D}$ を考える。このとき集合 $mor(\mathcal{D})$ の G による軌道全体がつくる集合を S とするとき, $(\mathcal{D},S)$ は擬スキーモイドとなる。実際これはシューア的 AS が (3) の条件をみたすことを確かめる場合と同じように示せる。

例えば, $\mathcal{D}$ が次の図式で与えられる小圏であり, $\mathbb{Z}/2$ は a を b に 1_x, 1_y は変えずに $\mathcal{D}$ に作用しているとする。



このとき擬スキーモイド $(\mathcal{C},\{\{1_x,1_y\},\{a,b\}\})$ を得る。

擬スキーモイドに AS の定義の条件 (1) と (2) を一般化したものを付加してスキーモイドを定義する。

[*2]全ての射が可逆である小圏

定義 2.3. 擬スキーモイド $(\mathcal{C}, S)$ が次の２条件をみたすとき**アソシエーションスキーモイド** (スキーモイド (schemoid)) という[*3]。

(i) 任意の $\sigma \in S$ と集合 $J := \amalg_{x \in ob(\mathcal{C})} \mathrm{Hom}_{\mathcal{C}}(x,x)$ に対して，もし $\sigma \cap J \neq \phi$ ならば $\sigma \subset J$.

(ii) 反変関手 $T : \mathcal{C} \to \mathcal{C}$ で $T^2 = id_{\mathcal{C}}$ をみたすものが存在する。さらに任意の $\sigma \in S$ に対して

$$\sigma^* := \{T(f) \mid f \in \sigma\}$$

は S に属する。反変関手 T を持つこのスキーモイドを $(\mathcal{C}, S, T)$ と表す。

例 2.4. (i)(AS からの構成) アソシエーションスキーム (X, S) を考える。このとき小圏 $\mathcal{C}$ を $ob(\mathcal{C}) = X$, $\mathrm{Hom}_{\mathcal{C}}(y,x) = \{(x,y)\} \subset X \times X$, 合成を $(z,x) \circ (x,y) = (z,y)$ と定義する。このとき $U = S$, 反変関手 $T : \mathcal{C} \to \mathcal{C}$ を $T(x) = x$, $T(x,y) = (y,x)$ で定義すると，$j(X,S) := (\mathcal{C}, U, T)$ はスキーモイドとなる。

(ii)(亜群からの構成) $\mathcal{H}$ を亜群とする。小圏 $\widetilde{\mathcal{H}}$ を $ob(\widetilde{\mathcal{H}}) := mor(\mathcal{H})$, そして射に関しては

$$\mathrm{Hom}_{\widetilde{\mathcal{H}}}(g,h) = \begin{cases} \{(h,g)\} & \text{if } t(h) = t(g) \\ \varnothing & \text{otherwise.} \end{cases}$$

と定義する。さらに $mor(\widetilde{\mathcal{H}})$ の分割 $S = \{\mathcal{G}_f\}_{f \in mor(\mathcal{H})}$ を $\mathcal{G}_f = \{(k,l) \mid k^{-1}l = f\}$, 反変関手を $(f,g) \in mor(\widetilde{\mathcal{H}})$ に対して $T((f,g)) = (g,f)$ と定義する。このとき $\widetilde{S}(\mathcal{H}) := (\widetilde{\mathcal{H}}, S, T)$ はスキーモイドとなる。これは群 G から得られるアソシエーションスキーム $S(G)$ の場合と同様に確かめられる。

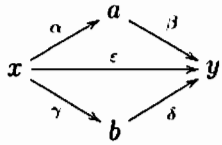
さらに体系的な (擬) スキーモイドの構成方については第５章で述べる。ここでは次にアドホックな方法で得られるスキーモイドの例をあげる。

例 2.5. G を群とし，$\mathcal{C}$ を次の図式で与えられる小圏とする。

$$G \circlearrowright x \xrightarrow{f} y \circlearrowright G^{\mathrm{op}}$$

すなわち，$ob(\mathcal{C}) = \{x, y\}$ であり，$\mathrm{Hom}_{\mathcal{C}}(x,x) = G$, $\mathrm{Hom}_{\mathcal{C}}(y,y) = G^{\mathrm{op}}$, $\mathrm{Hom}_{\mathcal{C}}(x,y) = \{f\}$ になる。このとき $(\mathcal{C}, S, T)$ はスキーモイドである。ただし，$mor(\mathcal{C})$ の分割は $S = \{S_g\}_{g \in G} \cup \{S_f\}$, $S_g := \{g, g^{\mathrm{op}}\}$, $S_f := \{f\}$, 反変関手は $T(x) := y$, $T(y) := x$ で定義されている。

例 2.6. 次で定義される３系 $(\mathcal{D}, \{S^i\}_{0 \le i \le 3}, T)$ はスキーモイドとなる。ここで基礎圏 $\mathcal{D}$ は図式



$$; \ \beta\alpha = \varepsilon = \delta\gamma;$$

で定義される。さらに $mor(\mathcal{D})$ の分割と $\mathcal{D}$ 上の反変関手 $T : \mathcal{D} \to \mathcal{D}$ はそれぞれ $S = \{S^i\}_{i=0,1,2,3}$ $S^1 = \{\alpha, \gamma\}$, $S^2 = \{\beta, \delta\}$, $S^3 = \{\varepsilon\}$, $S^0 = \{1_x, 1_y, 1_a, 1_b\}$ そして $T(a) = b$, $T(\varepsilon) = \varepsilon$, $T(\alpha) = \delta$, $T(\beta) = \gamma$ で定義されている。

アソシエーションスキーム (X, S) に Bose-Mesner 代数 $\mathcal{A}(X, S)$ が付随して現れた様に，擬スキーモイドからも自然に代数が定義できる。まず圏代数を思い出そう。$\mathcal{C}$ を小圏とし，$\mathbb{K}$ を単位元を持つ可換環とする。このとき**圏代数** (category algebra) とは自由 $\mathbb{K}$-加群 $\mathbb{K}\mathcal{C} := \mathbb{K}\langle f \mid f \in mor(\mathcal{C})\rangle$ であり

$$\alpha\beta = \begin{cases} \alpha \circ \beta & s(\alpha) = t(\beta) \\ 0 & \text{その他.} \end{cases}$$

[*3] この定義からスキーモイドは実際，coherent configuration の一般化になっていることがわかる。

4

により定義される積をもつ $\mathbb{K}$-代数である。圏代数は一般的には非可換であり単位元を持たない。$\mathcal{C}$ を基礎圏として持つ擬スキーモイド $(\mathcal{C},S)$ が与えられたとする。分割 S の元はすべて有限集合であると仮定する。このとき任意の S の元 σ,τ に対して圏代数 $\mathbb{K}\mathcal{C}$ 上で

$$(\sum_{s\in\sigma} s)\cdot(\sum_{t\in\tau} t)=\sum_{\mu\in S} p^{\mu}_{\sigma\tau}(\sum_{u\in\mu} u)$$

が成立する。すなわち自由 $\mathbb{K}$-加群

$$\mathbb{K}(\mathcal{C},S):=\mathbb{K}(\sum_{s\in\sigma} s \mid \sigma\in S)$$

は圏代数 $\mathbb{K}\mathcal{C}$ 部分代数となる。そこで $\mathbb{K}(\mathcal{C},S)$ を擬スキーモイド $(\mathcal{C},S)$ の **Bose-Mesner 代数**とよぶ。この代数が単位元を持つときはどのような場合かが直ぐわかる。

圏 $\mathcal{C}$ に対して, $mor(\mathcal{C})$ 部分集合 J_0 を

$$J_0:=\{1_x \mid x\in ob(\mathcal{C})\}$$

と定義する。(擬) スキーモイド $(\mathcal{C},S)$ に対して, $\alpha\in S$ かつ $\alpha\cap J_0\neq\phi$ ならば $\alpha\subset J_0$ をみたすとき, $(\mathcal{C},S)$ は**単位的** (unital) であるという。

補題 2.7. [8, Lemma 2.4] $(\mathcal{C},S)$ を擬スキーモイド, その基礎圏 $\mathcal{C}$ は有限とする。このとき *Bose-Mesner* 代数 $\mathbb{K}(\mathcal{C},S)$ が単位元を持つための必要十分条件は $(\mathcal{C},S)$ が単位的であることである。

Hanaki が定義したの AS の圏 AS([4] 参照) の定義を自然に拡張して (擬) スキーモイドの圏を定義する。

定義 2.8. (i) $(\mathcal{C},S)$ と $(\mathcal{E},S')$ を擬スキーモイドとする。このとき関手 $F:\mathcal{C}\to\mathcal{E}$ が任意の $\sigma\in S$ に対して $\tau\in S'$ が存在して $F(\sigma)\subset\tau$ をみたすとき F を擬スキーモイドの射といい $F:(\mathcal{C},S)\to(\mathcal{E},S')$ と表す。

(ii) $(\mathcal{C},S,T)$ と $(\mathcal{E},S',T')$ をスキーモイド, $F:(\mathcal{C},S)\to(\mathcal{E},S')$ を擬スキーモイドの射とする。$FT=T'F$ をみたすとき $F:(\mathcal{C},S,T)\to(\mathcal{E},S',T')$ と表して, F をスキーモイドの射と呼ぶ。

記号の乱用はあるが, F が擬スキーモイドの射であり $F(\sigma)\subset\tau$ をみたしているとき, F を分割の間の写像と考えて $F(\sigma)=\tau$ と表示する。

擬スキーモイドの圏, スキーモイドの圏を以下それぞれ qASmd, ASmd と表す。

例 2.2(i), 2.4 で与えた対象間の対応は圏の間の関手を生み出す。こうして次の可換図式を得る。

(2.1)
$$\begin{array}{ccccccc} \mathsf{Gpd} & \xrightarrow{\widetilde{S}(\ )} & \mathsf{ASmd} & \xrightarrow{k} & q\mathsf{ASmd} & \underset{K}{\overset{U}{\rightleftarrows}} & \mathsf{Cat}. \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle j} & & & & \\ \mathsf{Gr} & \xrightarrow{S(\ )} & \mathsf{AS} & & & & \end{array}$$

ただし U は基礎圏を取り出す忘却関手, k は自然な忘却関手そして Gr は有限群の圏を表す。$S(\ )$ は関しては第 2 章の始めので与えた対象間の対応であるがこれも関手となる。ここで合成 $Uk\widetilde{S}(\ )$ が自然な埋め込み $\mathsf{Gpd}\to\mathsf{Cat}$ には なっていない ということに注意する。

定理 2.9. [8, Theorem 3.2] (i) 関手 $S(\ )$ は $\widetilde{S}(\ )$ は忠実である。
(ii) 関手 i,j および K は充満忠実埋め込みである。

この定理によりスキーモイドは AS の一般化であることが分り, さらに擬スキーモイドが小圏の拡張であることがわかる。後ほど概説されるように, 関手 $\widetilde{S}(\ )$ により表されるスキーモイドは thin スキーモイドとして特徴づけられる。したがってスキーモイドは亜群の一般化でもある。

3. 許容写像と基礎的スキーモイド

残念ながら Bose-Mesner 代数を与える対象の間の対応

$$\mathcal{A}(\ ) : \mathsf{AS} \rightsquigarrow \mathsf{Alg}$$

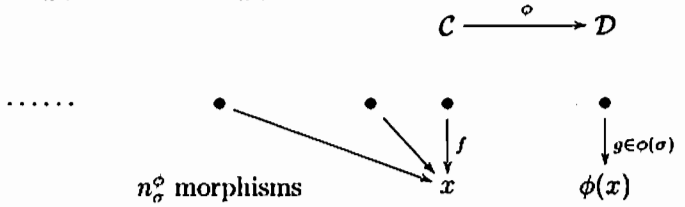
は一般に関手を与えない。そこで, French[3] は AS の射を"許容写像"[*4]に制限することで圏 $\mathcal{S}$ を導入し, 次を示した。

定理 3.1. [3, Corollaries 6.4, 6.6] 対象の間の対応 $\mathcal{A}(\ ) : \mathcal{S} \to \mathsf{Alg}$ は自然に関手を引き起こす。

許容写像の定義を圏論的に書き換えて一般化することで, 定理 3.1 は擬スキーモイドの世界で一般化されることになる。その一般化のために圏 $\mathcal{S}$ を拡大する。

定義 3.2. 擬スキーモイド $(\mathcal{C}, S)$ が基本的であるとは以下の (i), (ii) をみたすことである。
(i) $\alpha \in S$ に対して $\alpha \cap J_0 \neq \phi$ ならば $\alpha \subset J_0$, ただし $J_0 := \{1_x \mid x \in ob(\mathcal{C})\}$ である。
(ii) 基礎圏 $\mathcal{C}$ は亜群である。

定義 3.3. 擬スキーモイドの射 $\phi : (\mathcal{C}, S) \to (\mathcal{D}, T)$ は次をみたすとき許容的 (admissible) と呼ばれる。任意の $x \in ob(\mathcal{C})$, $\sigma \in S$ そして $t(g) = \phi(x)$ をみたす $g \in \phi(\sigma)$ に対して, $f \in \sigma$ が存在して $t(f) = x$ および $\phi(f) = g$ となる。



注意 3.4. 定義 3.3 において, $(\mathcal{D}, T)$ は基本的であり, $(\mathcal{C}, S)$ が有限な擬スキーモイドで基礎圏が亜群である場合 f の個数は有限でその値は ϕ と σ のみにより決まり x, g の取り方にはよらない ([8, Lemma 6.5] 参照)。その数を以下 n_σ^ϕ と表す。

有限な基本的擬スキーモイドと許容的射がつくる圏を $\mathcal{B}$ と表す。

ここで, 第 2 章で導入した擬スキーモイドにその Bose-Mesner 代数を定める対応 $\mathbb{K}(\ )$ を思い出す。French の結果をスキーモイドの言葉で述べると以下のようになる。

命題 3.5. [8, Proposition 6.7] $(\mathcal{D}, T)$ を有限な基本的擬スキーモイド, $(\mathcal{C}, S)$ は有限な擬スキーモイドであり基礎圏 $\mathcal{C}$ は亜群であるとする。さらに $\phi : (\mathcal{C}, S) \to (\mathcal{D}, T)$ を許容的写像とする。 このとき $\mathbb{K}(\phi)(s_\sigma) = n_\sigma^\phi s_{\phi(\sigma)}$ で定義される写像 $\mathbb{K}(\phi) : \mathbb{K}(\mathcal{C}, S) \to \mathbb{K}(\mathcal{D}, T)$ は代数の準同型写像となる, ただし $s_\sigma = \sum_{p \in \sigma} p$ である。

こうして定理 3.1 の一般化が得られる。

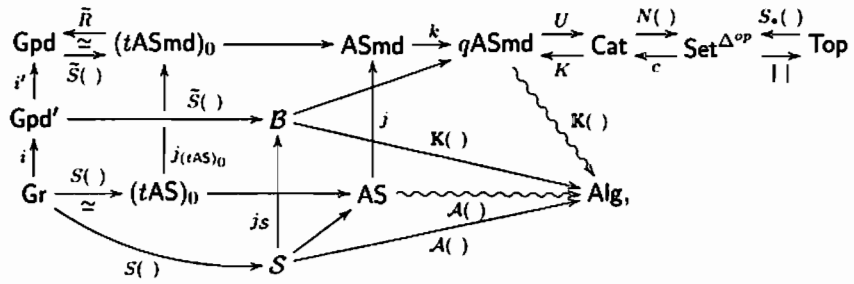
定理 3.6. [8, Theorem 6.9] 命題 *3.5* で与えられる対応 $\mathbb{K}(\ ) : \mathcal{B} \to \mathsf{Alg}$ は関手を誘導する。

さらに充満忠実関手 $j : \mathsf{AS} \to \mathsf{ASmd}$ は $j_{\mathcal{S}} : \mathcal{S} \to \mathcal{B}$ に制限されやはり充満忠実となる。
基点付き thin スキーモイドおよびその圏 $t(\mathsf{ASmd})_0$ も定義でき[*5], この圏は関手 $\widetilde{S}(\ )$ により亜群の圏 Gpd と同値になることがわかる ([8, Theorem 4.11])。

[*4] 擬スキーモイドの場合に拡張した定義を以下に述べるため AS の場合の定義は省略する。
[*5] 詳細は [8, Section 4] 参照。

既知の事実及び今まで述べた圏と関手についてまとめると次の図式を得る。

(3.1)



ただし波矢印は関手ではなく単に対象上の対応である。また K と垂直方向の矢印 j, j_S, $j_{(tAS)_0}$ は充満忠実関手 (fullly faithful functor) である。定理 2.9 を参照。射 $N(\ )$ と c は, それぞれナーブ構成関手と圏化関手 ([6]) を意味している。さらに $|\ |$, $S_*(\ )$ は実現関手, 特異単体集合を与える関手である。平行ライン上に表されている関手は, 下の射が上の射の左随伴であることに注意する。狭義には関手 $\widetilde{S}(\ ) : \mathrm{Gpd}' \to \mathcal{B}$ と $q\mathrm{ASmd}$ から Alg への対応 $\mathbb{K}(\ )$ はそれぞれ有限亜群の圏と有限擬スキーモイドの圏に制限されるべきである。ここで, Gpd′ は対象上で単射となる射に制限してえられる, Gpd の部分圏である。

(3.1) の右上段に位置する 3 つの圏 Cat, $\mathrm{Set}^{\Delta^{op}}$(単体的集合の圏) そして Top(位相空間の圏) を考える。Thomason([9]) の結果から それらのホモトピー圏は上の図式上に置かれている関手 $N(\ )$, $S_*(\ )$ により同値になる。関手 K は充満忠実であるからある意味, 擬スキーモイド "位相空間の一般化" とも言えよう。従って第 6 章でも繰り返し言及されることであるが, qASmd におけるホモトピー論を展開することは重要な意味を持つ。

Zicschang [13], Hanaki [4] により有限群の圏 Gr と基点付きの thin AS がつくる AS の部分圏 $(tAS)_0$ とは圏として同値となる (図式左下) ことが示されている。先に述べたように, この事実は拡張されて, (3.1) 上段の同値を与える。

4. スキーモイドの拡張と許容写像

(擬) スキーモイドを系統的に作り出すことは圏 ASmd, qASmd を豊かにすることになり特に重要である。ここでは Baues-Wrisching の圏の線形拡張を利用して (擬) スキーモイドを拡大していくことを考える。

$F(\mathcal{C})$ を $\mathcal{C}$ の分解圏とする, すなわち $ob(F(\mathcal{C})) = mor(\mathcal{C})$, 射 $(\alpha, \beta) : f \to g$ は $mor(\mathcal{C})$ の対であり, 図式

$$\begin{array}{ccc} t(f) & \xrightarrow{\alpha} & t(g) \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle g} \\ s(f) & \xleftarrow[\beta]{} & s(g) \end{array}$$

を可換にするものである。$F(\mathcal{C})$ 上の射の合成は $(\alpha', \beta') \circ (\alpha, \beta) = (\alpha'\alpha, \beta\beta')$ で定義される。

定義 4.1. ([1, (2.2) Definition]) $\mathcal{C}$ と $\mathcal{E}$ を小圏とする。 さらに $D : F(\mathcal{C}) \to \mathbb{K}\text{-Mod}$ を自然系 (natural system), すなわち, $F(\mathcal{C})$ から $\mathbb{K}$-加群の圏 $\mathbb{K}$-Mod への関手とする。このとき次の (a), (b), (c) が成り立つとき

$$D_+ \to \mathcal{E} \xrightarrow{q} \mathcal{C}$$

を自然系 D による $\mathcal{C}$ の線形拡張 (linear extension) という。

(a) $\mathcal{E}$ と $\mathcal{C}$ の対象の集合は同じで q は対象の上では恒等的な充満関手。

(b) $\mathcal{C}$ 上の任意の射 $f : A \to B$ に対して, アーベル群 D_f は推移的かつ効果的に $mor(\mathcal{E})$ の部分集合 $q^{-1}(f)$ に作用する。 $\alpha \in D_f$ の $f_0 \in q^{-1}(f)$ 上の作用を $f_0 + \alpha$ と表す。

(c) (b) の作用は線形分配法則 (*linear distributivity law*):

$$(f_0 + \alpha)(g_0 + \beta) = f_0 g_0 + f_* \beta + g^* \alpha,$$

をみたす, ただし $f_\bullet = D(f,1)$, $g^\bullet = D(1,g)$ である。

命題 4.2. [8, Proposition 5.2]　小圏 $\mathcal{C}$ 上の線形拡張 $D_+ \to \mathcal{E} \xrightarrow{q} \mathcal{C}$ を考える。$(\mathcal{C}, S)$ を擬スキーモイドとする。さらに任意の射 $f \in mor(\mathcal{C})$ に対して準同型写像 $f^\bullet$ と $f_\bullet$ は同型写像となり任意の $\sigma \in S$, $f, g \in \sigma$ に対して $D_{1_{s(f)}} \cong D_{1_{s(g)}}$ が成り立つとする。このとき $\mathcal{E}$ には q が $mor(\mathcal{E})$ の分割上では単射かつスキーモイドの間の射となるような擬スキーモイド構造が一意に定まる。

命題 4.2 でいう線形拡張を**スキーモイド拡張**そしてその射影 q を以下, **固有射** (proper morphism) とよぶ。

注意 4.3. 底小圏 $\mathcal{C}$ にスキーモイドの構造が入るある特別な場合には, $\mathcal{E}$ にもスキーモイド構造が定義できる ([8, Theorem 5.5] 参照)。

任意の $\mathbb{Z}$-加群 M に対して, 自然系 $\underline{M} : F(\mathcal{C}) \to \mathbb{Z}\text{-Mod}$ (自明表現) を $x \in ob(\mathcal{C})$ と $f \in mor(\mathcal{C})$ に対して $\underline{M}(x) = M$, $\underline{M}(f) = id_M$ 定義する。このとき Baues-Wirsching コホモロジー $H^*_{BW}(\mathcal{C}, D)$ が次で定義される。

$$H^*_{BW}(\mathcal{C}, D) := \mathrm{Ext}^*_{\mathbf{Func}(F(\mathcal{C}),\mathbb{Z}\text{-Mod})}(\underline{\mathbb{Z}}, D).$$

本来 Baues-Wirsching コホモロジーは適切なチェイン複体により定義されていることに注意する ([1, (1.4) Definition] 参照)。

Baues-Wirsching による結果 [1, (2.3) Theorem] は 2 次 Baues-Wirsching コホモロジーが小圏上の線形拡張を分類するということを主張している。したがって, 命題 4.2 から次の結果を得る。

定理 4.4. [8, Theorem 5.7] $(\mathcal{C}, S)$ を擬スキーモイド, $D : F(\mathcal{C}) \to \mathbb{Z}\text{-Mod}$ を自然系で, $f \in mor(\mathcal{C})$ に対して $f_\bullet$, $f^\bullet$ は同型写像, さらに $\sigma \in S$, $f, g \in \sigma$ に対して, $D_{1_{s(f)}} \cong D_{1_{s(g)}}$ が成り立つとする。このとき *Baues-Wirsching* コホモロジー $H^2_{BW}(\mathcal{C}; D)$ は射影 q が固有射であるスキーモイド拡張 $D_+ \to \mathcal{E} \xrightarrow{q} \mathcal{C}$ を分類する。

系 4.5. [8, Corollary 5.8] (X, S) をアソシエーションスキームとする。スキーモイド $j(X, S)$ 上のすべてのスキーモイド拡張は分裂する。

$j(X, S)$ は圏としては完全グラフから得られる圏となるため, 自明な圏と同値となる。したがって任意の自然系 D に対して $H^*_{BW}(j(X, S), D) = 0$ $(* > 0)$. これより上の系が従う。

ある条件下で, スキーモイド拡張の固有射は前章で導入した許容写像になる。さらにその固有射は Bose-Mesner 代数上に同型写像を誘導することがわかる ([8, Propositions 6.6, 6.11, Corollary 6.13] 参照)。これらの事実から基礎圏が圏としては同型ではないが, それぞれの Bose-Mesner 代数は同型であるスキーモイドを得ることができる。

例 4.6. [8, Remark 6.14] まず, 一般に群 G に対して $G^\bullet := (G, \{G\}, T))$ はスキーモイドであることに注意する, ただし反変関手 T は $T(g) = g^{-1}$ で与えられる。

(X, S) をアソシエーションスキームとし, $\mathcal{E}_0$ と $\mathcal{E}_1$ をそれぞれ積スキーモイド[*6] $j(X, S) \times (\mathbb{Z}/2)^\bullet$ 上の自明表現 $\mathbb{Z}/2$ による自明なスキーモイド拡張と非自明なものとする[*7]。このとき $ch(\mathbb{K}) \neq 2$ ならば, 代数として

$$\mathbb{K}(\mathcal{E}_1) \cong \mathbb{K}(\mathcal{E}_0) \cong \mathbb{K}(j(X, S) \times (\mathbb{Z}/2)^\bullet) \cong \mathbb{K}(j(X, S)) \cong \mathcal{A}((X, S))$$

となる[*8]。しかし, 先にも述べたように $j(X, S)$ が対象が一点である自明な圏と圏として同値, すなわちその分類空間は可縮となる。また分類空間 $B(\mathbb{Z}/2)$ は無限次元射影空間 $\mathbb{R}P^\infty$

[*6] スキーモイドの積はそれぞれの分割の積を用いて自然にスキーモイドになる。

[*7] $j(X, S)$ は自明な圏と同値であった。したがって $H^*_{BW}(j(X, S) \times (\mathbb{Z}/2)^\bullet, \underline{\mathbb{Z}/2}) \cong H^*_{BW}((\mathbb{Z}/2)^\bullet, \underline{\mathbb{Z}/2}) \cong H^*(\mathbb{Z}/2, \mathbb{Z}/2)$ となる。$H^2(\mathbb{Z}/2, \mathbb{Z}/2) = \mathbb{Z}/2$ より線形拡張の分類定理からスキーモイド拡張として自明なものとそうでないもの 2 つが現れる

[*8] ここで 2 番目の同型は $j(X, S)$ 上の自明表現 $\underline{\mathbb{Z}/2}$ によるスキーモイド拡張が分裂し $j(X, S) \times (\mathbb{Z}/2)^\bullet$ という形のスキーモイドと同型であるという事実を用いている。

となるから可縮ではない。このことから $j(X,S)\times(\mathbb{Z}/2)^\bullet$ と $j(X,S)$ は圏として同値ではないことがわかる。

5. スキーモイドの構成方法

前章に引き続き, (擬) スキーモイドの構成方法について考える。ここではBerger-Leinsterによる方法に基づき正方行列から小圏を構成し, そこにスキーモイドの構造を入れるという構成方法を紹介する。

$Z=(z_{ij})$ を非負整数を成分とする正方行列とする。Z は推移的すなわち, $z_{ij},z_{jk}\geq 1$ ならば $z_{jk}\geq 1$ をみたすとする。さらに対角成分は全て2以上であるとする。このときBerger-Leinster[2] は, 圏の行列が Z である有限小圏 $\mathcal{C}_Z$ を次のように構成した[*9]。

$\mathcal{C}_Z$ の対象がつくる集合を順序集合 $\{i\}_{i\in ob(\mathcal{C}_Z)}$ とする。$z_{ij}=\sharp\mathrm{Hom}_{\mathcal{C}}(i,j)$ とし, 各 i,j に対して $z_{ij}\neq 0$ のとき恒等射ではない $\phi_{ij}:i\to j$ を一つ選ぶ。射の合成 $i\xrightarrow{\alpha}j\xrightarrow{\beta}k$ を $\alpha\neq 1$ かつ $\beta\neq 1$ のとき $\beta\circ\alpha=\phi_{ik}$ で定める。このとき $\mathcal{C}_Z$ は圏となる。以下では $\{\phi_{ij}\}_{ij}$ を $\mathcal{C}_Z$ の**枠**と呼ぶ。射の合成を全て枠に"押し込める"ことで圏 $\mathcal{C}_Z$ は得られていると言ってよい。

$(X,P=\{P_l\}_{l=0,\dots,s})$ をアソシエーションスキームで $\{(R_l)\}$ をその隣接行列とする。すなわち R_l の (i,j) 成分を $R_l(i,j)$ とすると

$$R_l(i,j)=\begin{cases}1 & \text{if } (i,j)\in P_l,\\ 0 & \text{otherwise}\end{cases}$$

である。$\{(R_l)\}$ を用いてスキーモイドが構成できる。

定理 5.1. [8, Theorem 7.5] 上の記号のもと, 正数 $z_0,\dots,z_s$ に対して

$$Z:=z_0R_0+z_1R_1+\cdots+z_sR_s+\mathrm{diag}(1,1,\dots,1).$$

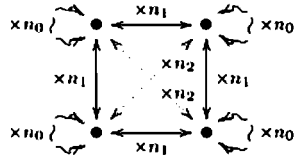
とおく。$S=\{\sigma_l\}_{l=0,1,\dots,s}$ を $\mathcal{C}_Z$ の枠 $\{\phi_{ij}\}_{ij}$ の分割とする, ただし $\sigma_0=\{\phi_{ii}\mid i=1,\dots,m\}$, $\sigma_l=\{\phi_{ij}\mid (j,i)\in P_l\}$ である。このとき S を含む $mor(\mathcal{C})$ の分割 Σ が存在して[*10] $(\mathcal{C}_Z,\Sigma)$ は擬スキーモイドになる。さらに $z_0=\cdots=z_s$ であるとき, $(\mathcal{C}_Z,\Sigma)$ は単位的スキーモイド構造をもつ。

定理5.1の基礎圏 $\mathcal{C}_Z$ は始めに与えられるASを完全グラフと考えたときその射の集合を"太らせて"得られている。

例 5.2. $H(2,2)$ を $(2,2)$ 型のHammingスキームとする。このとき定理5.1の構成にしたがって得られる擬スキーモイドを $(\mathcal{C}_Z,\Sigma)$ とする。その基礎圏 $\mathcal{C}_Z$ は 4×4 行列

$$Z=\sum_{i=0}^{2}n_iR_i+\mathrm{diag}(1,1,1,1)=\begin{pmatrix}n_0+1 & n_1 & n_1 & n_2\\ n_1 & n_0+1 & n_2 & n_1\\ n_1 & n_2 & n_0+1 & n_1\\ n_2 & n_1 & n_1 & n_0+1\end{pmatrix}.$$

を用い, 上述のBerger-Leinsterの手続きに沿って得られる。さらに Σ は次の図が示すような $mor(\mathcal{C}_Z)$ の分割である。



+4 white identities.

[*9] 圏の行列 C から圏のEuler標数が2つ定義される。これらの性質が[2]で考察されている。

[*10] Σ の定義は[8, Proposition 7.4]参照。

6. 展望

(擬) スキーモイドを研究する上での今後の展望を述べてこの稿をおえる。

• Bose-Mesner 代数を経由した圏論的表現論を用いたスキーモイドのホモロジー論的考察: スキーモイドから得られる Bose-Mesner 代数の導来同値の考察など。

• Cat の Quillen モデル圏構造, (コ) ファイブレーション圏構造から qASmd に付加される構造をもとにしたスキーモイドのホモトピー論的考察: 具体的なシリンダー対象を与えた抽象ホモトピー論の展開と qASmd の 2-圏構造を用いたホモトピー論的考察およびホモトピー不変量[*11]の導入など。

上の 2 つの考察は決して独立して進むわけではない。実際 qASmd の 2-圏構造を利用すれば適切な擬スキーモイド $(\mathcal{C}, S)$ からベクトル空間の圏への関手圏を考えることで Mitchell 対応を模倣できる。すなわち Bose-Mesner 代数 $\mathbb{K}(\mathcal{C}, S)$ 上で圏論的表現論, コホモロジー論的表現論の展開が期待できる。(2.1) の図式およびその後のコメントが示すように有限群は AS を経由してスキーモイドの圏に運ばれる。しかし Cat まで持っていった場合それは常に対象が一点である圏と同値になってしまい, そこから面白い表現論, コホモロジー論は展開できない。Webb [10], Xu[11, 12] 等により有限群のコホモロジー論を拡張した小圏のコホモロジー論の研究も進んでいるが, これをそのまま AS に適用することはできない。小圏のコホモロジー論を再構築して別系列のスキーモイドのコホモロジー論をつくる必要があろう。そのキーワードが上述の Mitchell 対応であると考える。

また qASmd の 2-圏構造は Cat のそれを拡張して得られる。すなわち上述の充満忠実関手 K : Cat $\to$ qASmd は 2-圏の関手となる ([7, Theorem 3.9])。従って Hardie, Kamps, Marcum [5] により圏論的に考察される Toda の積を用いて擬スキーモイドのホモトピー集合を考察することも可能になろう。そうして得られる非自明な元が持つ幾何学的, 代数的組合せ論的意味を探ることにも意味がある。

アソシエーションスキームの研究では閉集合の概念や, Bose-Mesner 代数の表現論的な性質が重要な役割を果たしている ([14])。こうした概念をスキーモイドの場合に一般化しそれらが qASmd や ASmd 内でどのように振る舞うかの研究も重要であろう。実際, 図式 (3.1) 内を移動しながらの考察が再び AS に戻ってくる可能性もある。一般化からの還元も期待できる。

(擬) スキーモイドは [8] ではじめて導入された概念である。まだまだ若く, その性質はほとんど解っていないと言って良い。ホモトピー論的, ホモロジー論的性質の解明やアソシエーションスキームのように代数的組合せ論, デザイン, 符号理論にこの新しい対象が応用されること強く願う。

謝辞 第３０回という記念すべき回に伝統ある代数的組合せ論シンポジウムに参加しそして講演出来たことは私にとって非常に光栄なことでした。また講演者, 参加者の方々とアソシエーションスキームの一般化について議論できたこと, さらに今後研究を進める上で重要な助言をして頂いたことは私にとって大きな収穫となりました。最後になりましたが, 講演の機会を与えて頂きました世話人方々, 北詰正顕氏, 原田昌晃氏, 新谷誠氏そして講演者として推薦して頂いた花木章秀氏に感謝いたします。

References

[1] H. J. Baues and G. Wirsching, Cohomology of small categories, J. Pure Appl. Algebra **38** (1985), 187-211.

[2] C. Berger and T. Leinster, The Euler characteristic of a category as the sum of a divergent series, Homology, Homotopy and App. **10** (2008), 41-51.

[*11] [7] では擬スキーモイド間の自己ホモトピー同値写像がつくる群を考察している。

[3] C. French, Functors from association schemes, J. Combin. Theory Ser. A **120** (2013), 1141-1165.
[4] A. Hanaki, A category of association schemes, J. Combin. Theory Ser. A **117** (2010), 1207-1217.
[5] K. A. Hardie, K. H. Kamps and H. J. Marcum, A categorical approach to matrix Toda brackets. Trans. Amer. Math. Soc. **347** (1995), 4625-4649.
[6] P. Gabriel and M. Zisman, Calculus of fractions and homotopy theory, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 35 Springer-Verlag New York, Inc., New York 1967.
[7] K. Kuribayashi, On the strong homotopy for quasi-schemoids, preprint, 2013.
[8] K. Kuribayashi and K. Matsuo, Association schemoids and their categories, to appear in Applied Categorical Structures, preprint (2013). `arXiv:1304.6883 math.CT`.
[9] R. W. Thomason, Cat as a closed model category, Cahirs de topologie et géométrie différentielle catégoriques, **21**(1980), 305-324.
[10] P. Webb, An introduction to the representations and cohomology of categories. Group representation theory, 149-173, EPFL Press, Lausanne, 2007.
[11] F. Xu, Representations of categories and their applications. J. Algebra **317** (2007), 153-183.
[12] F. Xu, Hochschild and ordinary cohomology rings of small categories. Adv. Math. **219** (2008), 1872-1893.
[13] P. -H. Zieschang, Homogeneous coherent configurations as generalized groups and their relationship to buildings, Journal of algebra, **178** (1995), 677-709.
[14] P. -H. Zieschang,Theory of association schemes, Springer Monographs in Math., Springer-Verlag, Berlin, 2005.

EDGE-SIGNED GRAPHS WITH SMALLEST EIGENVALUE GREATER THAN -2

GARY GREAVES*, JACK KOOLEN†, AKIHIRO MUNEMASA, YOSHIO SANO, AND TETSUJI TANIGUCHI††

ABSTRACT. We give a structural classification of edge-signed graphs with smallest eigenvalue greater than -2. We prove a conjecture of Hoffman about the smallest eigenvalue of the line graph of a tree that was stated in the 1970s. Furthermore, we prove a more general result extending Hoffman's original statement to all edge-signed graphs with smallest eigenvalue greater than -2. Our results give a classification of special graphs of fat Hoffman graphs with smallest eigenvalue greater than -3.

1. INTRODUCTION

The (adjacency) eigenvalues of a graph G on n vertices are defined as the eigenvalues of its adjacency matrix A. Since A is a real symmetric matrix, its eigenvalues $\lambda_i(A)$ are real; we arrange them as follows

$$\lambda_1(A) \leqslant \lambda_2(A) \leqslant \cdots \leqslant \lambda_n(A).$$

For convenience we will sometimes also refer to each $\lambda_i(A)$ as $\lambda_i(G)$. Much attention has been directed towards the study of graphs with smallest eigenvalue at least -2 [2, 6, 15, 18]. Most of this attention has centred around the beautiful theorem of Cameron, Goethals, Shult, and Seidel [3], which classifies graphs having smallest eigenvalue at least -2. In the late 1970s Hoffman [10] studied graphs G with $\lambda_1(G) \geqslant -1-\sqrt{2}$ and later Woo and Neumaier [19] furthered Hoffman's work, introducing the so-called Hoffman graph. Recently, Jang, Koolen, Munemasa, and Taniguchi [13] proposed a programme to classify fat Hoffman graphs with smallest eigenvalue at least -3. The present work fills a part of this programme, and includes the results of [17].

*GG was supported by JSPS KAKENHI; grant number: 24-02789.

†Part of this work was done while JHK was visiting Tohoku University with a JSPS visitors grant. Also he greatly appreciates support from the '100 talent' grant of the Chinese government.

††TT was supported by JSPS KAKENHI; grant number: 25400217.

In this article we classify, up to switching equivalence, edge-signed graphs with smallest eigenvalue greater than -2. In particular, we recover as a special case the classification of graphs with smallest eigenvalue greater than -2 given earlier by Doob and Cvetković [6]. As an application, we classify the special graphs of fat Hoffman graphs with smallest eigenvalue greater than -3. Some of such graphs are related to the modified adjacency matrix that appeared in Hoffman [9]. Below we describe the conjecture Hoffman made about these modified adjacency matrices.

Let T be a tree on $n \geqslant 2$ vertices with line graph $\mathfrak{L}(T)$ and let e be an end-edge of T (one of whose vertices has valency 1). Then e is a vertex of $\mathfrak{L}(T)$. Define $\hat{A}(\mathfrak{L}(T), e)$ to be the adjacency matrix of $\mathfrak{L}(T)$, modified by putting a -1 in the diagonal position corresponding to e. In one of his papers [9], Hoffman conjectured that $\lambda_1(\hat{A}(\mathfrak{L}(T), e)) < \lambda_1(\mathfrak{L}(T))$ for all trees T and end-edges e. In Section 4 we prove this conjecture, which we record as the following theorem.

Theorem 1. *Let T be a tree and let e be an end-edge of T. Then $\lambda_1(\hat{A}(\mathfrak{L}(T), e)) < \lambda_1(\mathfrak{L}(T))$.*

Furthermore, using the classification of edge-signed graphs (see Theorem 6) with smallest eigenvalue greater than -2, we prove a generalised version of Hoffman's conjecture (see Theorem 15).

In Section 2 we give our preliminaries. In Section 3 we prove the main part of the classification theorem of edge-signed graphs with smallest eigenvalue greater than -2 leaving the exceptional case to Section 5. In Section 4 we prove Theorem 1 and its generalised version, and in Section 6 we comment on the application to Hoffman graphs with smallest eigenvalue greater than -3.

2. Edge-signed graphs and representations

In this section we introduce some terminology that we use in our results. An **edge-signed graph** G is a triple (V, E^+, E^-) of a set V of vertices, a set E^+ of 2-subsets of V (called **(+)-edges**), and a set E^- of 2-subsets of V (called **(−)-edges**) such that $E^+ \cap E^- = \emptyset$.

Let G be an edge-signed graph. We denote the set of vertices of G by $V(G)$, the set of (+)-edges of G by $E^+(G)$, and the set of (−)-edges of G by $E^-(G)$. By a **subgraph** $G' = (V(G'), E^+(G'), E^-(G'))$ of G we mean a vertex induced edge-signed subgraph, i.e., $V(G') \subseteq V(G)$, $E^\pm(G') = \{\{x, y\} \in E^\pm(G) \mid x, y \in V(G')\}$. The **underlying graph** $U(G)$ of G is the unsigned graph $(V(G), E^+(G) \cup E^-(G))$.

Two edge-signed graphs G and G' are said to be **isomorphic** if there exists a bijection $\phi : V(G) \to V(G')$ such that $\{u, v\} \in E^+(G)$ if and

only if $\{\phi(u), \phi(v)\} \in E^+(G')$ and that $\{u, v\} \in E^-(G)$ if and only if $\{\phi(u), \phi(v)\} \in E^-(G')$.

A **switching** at vertex v is the process of swapping the signs of each edge incident to v. Two edge-signed graphs G and G' are said to be **switching equivalent** if there exists a subset $W \subset V(G)$ such that G' is isomorphic to the graph obtained by switching at each vertex in W. Note that switching equivalence is an equivalence relation that preserves eigenvalues.

For an edge-signed graph G, we define its **signed adjacency matrix** $A(G)$ by

$$(A(G))_{uv} = \begin{cases} 1 & \text{if } \{u, v\} \in E^+(G), \\ -1 & \text{if } \{u, v\} \in E^-(G), \\ 0 & \text{otherwise.} \end{cases}$$

To ease language, we will refer to the signed adjacency matrix simply as the adjacency matrix.

Let G be an edge-signed graph with smallest eigenvalue at least -2. A **representation** of G is a mapping ϕ from $V(G)$ to $\mathbb{R}^n$ for some positive integer n, such that $(\phi(u), \phi(v)) = \pm 1$ if $\{u, v\} \in E^{\pm}(G)$ respectively, and $(\phi(u), \phi(v)) = 2\delta_{u,v}$ otherwise, where $\delta_{u,v}$ is Kronecker's delta, i.e., $\delta_{u,v} = 1$ if $u = v$ and $\delta_{u,v} = 0$ if $u \neq v$. Since, for A the adjacency matrix of G, the matrix $A + 2I$ is positive semidefinite, $A + 2I$ is the Gram matrix of a set S of vectors $\mathbf{x}_1, \ldots, \mathbf{x}_m$. These vectors satisfy $(\mathbf{x}_i, \mathbf{x}_i) = 2$ and $(\mathbf{x}_i, \mathbf{x}_j) = 0, \pm 1$ for $i \neq j$. Sets of vectors satisfying these conditions determine line systems. We denote by $[\mathbf{x}]$ the line determined by a nonzero vector $\mathbf{x}$, in other words, $[\mathbf{x}]$ is the one-dimensional subspace spanned by $\mathbf{x}$. We say that G is **represented by** the line system S if G has a representation ϕ such that $S = \{[\phi(v)] : v \in V(G)\}$.

Below we give descriptions of three line systems, A_n, D_n and E_8. Let $\mathbf{e}_1, \ldots, \mathbf{e}_n$ be an orthonormal basis for $\mathbb{R}^n$.

$$A_n = \{[\mathbf{e}_i - \mathbf{e}_j] : 1 \leqslant i < j \leqslant n+1\} \quad (n \geqslant 1).$$

$$D_n = A_{n-1} \cup \{[\mathbf{e}_i + \mathbf{e}_j] : 1 \leqslant i < j \leqslant n\} \quad (n \geqslant 4),$$

$$E_8 = D_8 \cup \left\{ [\frac{1}{2} \sum_{i=1}^{8} \epsilon_i \mathbf{e}_i] : \epsilon_i = \pm 1, \prod_{i=1}^{8} \epsilon_i = 1 \right\}.$$

These line systems are used in the following classical result of Cameron, Goethals, Shult, and Seidel.

Theorem 2 ([3]). *Let G be a connected edge-signed graph with $\lambda_1(G) \geqslant -2$. Then G is represented by a subset of either D_n or E_8.*

Let G be an edge-signed graph represented by a line system S. If S embeds into $\mathbb{Z}^n$ for some n, then we say that G is **integrally represented** or that G has an **integral representation**. By Theorem 2, for an edge-signed graph G with $\lambda_1(G) \geqslant -2$, G has an integral representation if and only if G is represented by a subset of D_n for some n. We record this observation as the following corollary.

Corollary 3. *Let G be a connected edge-signed graph with $\lambda_1(G) \geqslant -2$. Then G has no integral representation if and only if G is represented by a subset of E_8 but not by a subset of D_n for any n.*

Corollary 3 motivates our next definition. Let G be a connected edge-signed graph with $\lambda_1(G) \geqslant -2$. We call G **exceptional** if it does not have an integral representation. Clearly there are only finitely many exceptional edge-signed graphs.

3. Classification of edge-signed graphs with $\lambda_1 > -2$

In this section we classify integrally represented edge-signed graphs with smallest eigenvalue greater than -2. We leave the exceptional case until Section 5.

Lemma 4. *Let G be an edge-signed graph whose underlying graph is a cycle. Then $\lambda_1(G) > -2$ if and only if the number of $(+)$-edges of G is odd.*

Proof. If the number of $(+)$-edge is even, then G is switching equivalent to the edge-signed cycle in which all edges are $(-)$-edges, hence $\lambda_1(G) = -2$. Conversely, suppose G has an odd number of $(+)$-edges. If the length of G is odd, then G has an even number of $(-)$-edges, hence G is switching equivalent to an unsigned cycle. Thus $\lambda_1(G) > -2$. If the length of G is even, then, up to switching, $A(G) = B^{\mathsf{T}}B - 2I$ where

$$B = \begin{pmatrix} 1 & 0 & \cdots & 0 & -1 \\ 1 & 1 & \ddots & & 0 \\ 0 & 1 & 1 & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 1 & 1 \end{pmatrix}.$$

Since this matrix is nonsingular, $\lambda_1(G) > -2$. □

Let G be an edge-signed graph with smallest eigenvalue greater than -2. Assume that G has an integral representation ϕ. This means that, with $m = |V(G)|$, there exists an $n \times m$ matrix

$$M = (\mathbf{v}_1 \ \cdots \ \mathbf{v}_m),$$

with entries in $\mathbb{Z}$, such that $(\mathbf{v}_i, \mathbf{v}_j) = \pm 1$ if $\{i, j\} \in E^{\pm}(G)$ respectively, and $(\mathbf{v}_i, \mathbf{v}_j) = 2\delta_{i,j}$ otherwise. We may assume that M has no rows consisting only of zeros. Since $\mathbf{v}_i \in \mathbb{Z}^n$, $\mathbf{v}_i$ has two entries equal to ± 1, and all other entries 0. This means that we can regard M as an signed incidence matrix of a graph H and the underlying graph of G is the line graph of H. More precisely, H is a graph with n vertices, and the vertices i and j are joined by the edge k whenever $\{i, j\} = \mathrm{supp}(\mathbf{v}_k)$. Note that the graph H may have multiple edges. A graph without multiple edges is called **simple**. We call H the **representation graph** of G associated with the representation ϕ. Note that H has no isolated vertex. If G is connected, then so is H.

Lemma 5. *Let G be an m-vertex connected edge-signed graph having an integral representation ϕ and smallest eigenvalue greater than -2. Let H be the n-vertex representation graph of G associated with the representation ϕ. Then $n \in \{m, m+1\}$. Moreover, if $n = m$, then H is a unicyclic graph or a tree with a double edge and if $n = m+1$, then H is a tree.*

Proof. Since $M^{\top}M = A(G) + 2I$ is positive definite, M has rank m. This implies $n \geqslant m$. If H is disconnected, then so is G, which is absurd. Thus H is connected, which forces $n \leqslant m + 1$. □

Let G be the line graph of a unicyclic graph whose unique cycle has at least 4 vertices. For each edge e of G there exists a unique maximal clique that contains e. For such a graph G, we denote by $\mathfrak{C}_G(uu')$ the unique maximal clique of G containing the edge uu'.

Theorem 6. *Let G be a connected integrally represented edge-signed graph having smallest eigenvalue greater than -2. Let H be the representation graph of G for some integral representation. Then one of the following statements holds:*

(i) *H is a simple tree or H is unicyclic with an odd cycle, and G is switching equivalent to the line graph $\mathfrak{L}(H)$,*

(ii) *H is unicyclic with an even cycle C, and G is switching equivalent to the edge-signed graph (V, E^+, E^-), where $V = V(\mathfrak{L}(H))$,*

$$E^- = \{uv \in E(\mathfrak{L}(H)) \mid v \in \mathfrak{C}_G(uu')\}$$

where uu' is an edge of $\mathfrak{L}(C)$, and $E^+ = E(\mathfrak{L}(H)) \backslash E^-$.

(iii) *H is a tree with a double edge, and G is switching equivalent to the edge-signed graph obtained from the line graph $\mathfrak{L}(H)$, by attaching a new vertex u', and join u' by $(+)$-edges to every vertex of a clique in the neighbourhood of u, $(-)$-edges to every*

vertex of the other clique in the neighbourhood of u, where u is a fixed vertex of $\mathfrak{L}(H)$.

Conversely, if G is an edge-signed graph described by (i), (ii), *or* (iii) *above, then G is integrally represented and has smallest eigenvalue greater than -2.*

Proof. By Lemma 5, we can divide the proof into three cases.
Case 1: H is a simple tree. Since G has smallest eigenvalue greater than -2, G cannot contain a triangle switching equivalent to one with three $(-)$-edges. By repeatedly applying switching, one can move the locations of $(-)$-edges toward an end block, and eventually end up with an unsigned graph. Therefore, G is switching equivalent to $\mathfrak{L}(H)$.
Case 2: H is unicyclic. We prove either (i) or (ii) holds by induction on the number of vertices of H minus the length of the cycle in H. First suppose that H is a cycle. By Lemma 4, G is either an odd cycle with an even number of $(-)$-edges, or G is an even cycle with odd number of $(-)$-edges. In the former case, G is switching equivalent to an unsigned odd cycle. In the latter case, G is switching equivalent to an even cycle with one $(-)$-edge and the clique of the underlying graph of G containing the $(-)$-edge is then switching equivalent to the one described in (ii).

Now suppose that H is not a cycle. Let ϕ be the integral representation of G to which H is associated. Then H has a vertex of v of degree 1. Let H' be the graph obtained from H by removing the vertex v, and set $G' = \mathfrak{L}(H')$. Then G' may be regarded as a subgraph of G, and H' is the representation graph of the representation ϕ restricted to G'. By induction, (i) or (ii) holds for (G', H'). The edges of G not in G' have the same sign, so we may assume that these are all $(+)$-edges by applying switching if necessary. Also, we may assume the unique vertex of H closest to v is not incident with $(-)$-edges, by applying switching if necessary. Then (i) or (ii) holds.
Case 3: H is a tree with a double edge. If H has a double edge, then the matrix M has a submatrix

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Let u' (resp. u) denote the vertex of G corresponding to the first (resp. second) column of this matrix (which in turn correspond to a column of M), and let v^+ (resp. v^-) denote the vertex of H corresponding to the first (resp. second) row of this matrix (which in turn correspond to a row of M). Let $G' = G - u'$. Then the graph H' obtained from G' is a tree. We have already shown that, in this case, we may take

G' to be the unsigned line graph of H'. Let K^+ (resp. K^-) be the clique of G in the neighbourhood of u consisting of vertices u'' with $M_{v^+,u''} = 1$ (resp. $M_{v^-,u''} = -1$). Then in the graph G, u' is joined to every vertex of K^+ by (+)-edges, and u' is joined to every vertex of K^- by (−)-edges. Therefore (iii) holds.

Conversely, suppose G is described by (i), (ii), or (iii). First, we describe how to construct M for each case. For (i), M is the incidence matrix of H. For (ii), let v be the vertex incident to both the edges u and u' of H. Then M is the incidence matrix of H adjusted so that $M_{v,u} = -1$. For (iii), let v and w be incident to the edge u in H. Then M is the incidence matrix of H together with an extra column for u' with $M_{v,u'} = 1$, $M_{w,u'} = -1$, and the remaining entries 0.

To prove the converse, it suffices to show that, in each case, $M^\top M$ is positive definite. If G is the line graph of a tree then this is well known. Thus we can immediately restrict our attention to when $n = m$. We will show that, in both remaining cases, $M^\top M$ has determinant 4. We inductively show that $\det(M^\top M) = 4$ for H unicyclic. Suppose that the underlying graph of G is the line graph of a unicyclic graph. If H is a cycle then, by Lemma 4, M is nonsingular. Hence the rows of M are a basis for D_n, which has discriminant 4. Thus M has determinant ± 2. Otherwise, H has a vertex v of degree 1. Let M' be a the matrix obtained by removing v. Then $\det(M) = \pm\det(M')$. Hence $M^\top M$ is positive definite, as required. The same inductive approach can be applied when starting with the double-edge where M is the matrix

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

which has determinant 2. □

Note that, if G is represented by the line system A_n, then one can relax the assumption of Theorem 6 to having smallest eigenvalue *at least* -2. Ishihara [12] shows that, in this case, the underlying graph of G is a claw-free block graph.

4. Hoffman's conjecture

In this section we settle Hoffman's conjecture, i.e., we prove Theorem 1. Moreover, we prove a stronger version of Hoffman's conjecture extended to edge-signed graphs.

Lemma 7. *Let M be an $n \times m$ real matrix. Then $M^\top M$ and $MM^\top$ have the same nonzero eigenvalues (including multiplicities). More explicitly, for any nonzero eigenvalue θ of $M^\top M$, the multiplication by*

M gives a linear map from $\ker(M^\top M - \theta I)$ *to* $\ker(MM^\top - \theta I)$ *whose inverse is given by* $\mathbf{v} \mapsto \theta^{-1} M^\top \mathbf{v}$.

Proof. Follows from [1, Lemma 2.9.2]. □

Lemma 8. *Let* $A = (a_{i,j})$ *be a real symmetric matrix, and let* $A' = (a'_{i,j})$ *be the matrix defined by* $a'_{i,j} = a_{i,j} - \delta_{i,1}\delta_{j,1}$. *Suppose there exists an eigenvector* $\mathbf{x}$ *of* A *belonging to the eigenvalue* $\lambda_1(A)$ *with* $x_1 \neq 0$. *Then* $\lambda_1(A) > \lambda_1(A')$.

Proof. We may assume without loss of generality that $\|\mathbf{x}\| = 1$. Then $\lambda_1(A) = \mathbf{x}^\top A\mathbf{x} = \mathbf{x}^\top A'\mathbf{x} + x_1^2 \geqslant \lambda_1(A') + x_1^2 > \lambda_1(A')$. □

Remark 9. One might wonder if Theorem 1 can be proved by showing that the adjacency matrix of $\mathfrak{L}(T)$ satisfies the assumption of Lemma 8 when we take the first entry to correspond to an end-edge of T. This approach, however, does not work. In fact, let T be the Dynkin diagram E_6, and let the first entry of A correspond to the unique end edge attached to the vertex of degree 3. Then the smallest eigenvalue $-(\sqrt{5}+1)/2$ of $\mathfrak{L}(T)$ has multiplicity 1, and the eigenvector has 0 in its first entry.

Lemma 10. *Let* G *be a connected bipartite graph on* m *vertices and* n *edges, with oriented incidence matrix* B. *Let* A *be the adjacency matrix of the line graph of* G, *and let* L *be the Laplacian matrix of* G. *Then for each* $i \in \{2, \ldots, m\}$, $B\ker(A - \lambda_{i+n-m}(A)I) = \ker(L - \lambda_i(L)I)$ *and* $\ker(A - \lambda_{i+n-m}(A)I) = B^\top \ker(L - \lambda_i(L)I)$.

Proof. Since G is connected, the multiplicity of 0 as an eigenvalue of L is 1. Since $B^\top B = A + 2I$ and $BB^\top = L$, Lemma 7 implies that $\lambda_i(L) = \lambda_{i+n-m}(A + 2I) = \lambda_{i+n-m}(A) + 2$ for $1 < i \leq m$. Moreover, Lemma 7 implies $B\ker(B^\top B - \lambda_{i+n-m}(B^\top B)I) = \ker(L - \lambda_i(L)I)$ and $\ker(B^\top B - \lambda_{i+n-m}(B^\top B)I) = B^\top \ker(L - \lambda_i(L)I)$. Since $B^\top B - \lambda_{i+n-m}(B^\top B)I = A - \lambda_{i+n-m}(A)I$, we obtain the desired result. □

Let G be a graph and let v be a vertex of G. Recall that $\hat{A}(G, v)$ is the adjacency matrix of G, modified by putting a -1 in the diagonal position corresponding to v.

Lemma 11 ([9, Lemma 2.1]). *Let* T *be a tree and let* e *be an end-edge of* T. *Then* $\lambda_1(\hat{A}(\mathfrak{L}(T), e)) > -2$.

We are now ready to prove Theorem 1.

Proof of Theorem 1. Let T be a tree on $n+1$ vertices and n edges, and let A denote the adjacency matrix of the line graph $\mathfrak{L}(T)$ of T. Since

T is bipartite, one can orient its edges so that its oriented incidence matrix B satisfies

$$B^\top B = A + 2I.$$

We also have $BB^\top = L$, the Laplacian matrix of T.

Let r and s be the vertices of the end-edge e, and assume r has valency 1 in T. We may choose B so that the first row and column correspond to r and e respectively, and the second row corresponds to s. Let the columns vectors $\mathbf{e}_i$ be the canonical basis of the Euclidean space $\mathbb{R}^m$ where m should be clear from context. Without loss of generality, we assume $B\mathbf{e}_1 = \mathbf{e}_1 - \mathbf{e}_2$ and $B^\top \mathbf{e}_1 = \mathbf{e}_1$.

We obtain the matrix C from B by setting $b_{1,1} = 0$. Define matrices A' and L' by

$$C^\top C = A' + 2I, \text{ and } CC^\top = L'.$$

Then A' can be obtained from A by setting $a_{1,1} = -1$, that is, $A' = \hat{A}(\mathfrak{L}(T), e)$. The matrix L' can be obtained from L by setting all entries of the first row and column to zero.

By Lemma 11, $C^\top C$ is positive definite. It then follows from Lemma 7 that L' is a positive semidefinite $(n+1) \times (n+1)$ matrix with rank n. Let X be the principal submatrix of L' obtained by removing the first row and column of L'. Since the matrix L' has only zeros in its first row and column, the matrix X is positive definite.

Moreover, X is an M-matrix, that is, in addition to being positive definite, its off-diagonal entries are non-positive. By [11, Theorem 2.5.3], X^{-1} is a non-negative matrix. By the Perron-Frobenius theorem (see, for example, [8]), any eigenvector corresponding to the smallest eigenvalue of X has no zero entry.

By Lemma 7, $\lambda_1(A'+2I) = \lambda_2(L') = \lambda_1(X)$, and $\lambda_1(A+2I) = \lambda_2(L)$. Thus, to prove Theorem 1, it suffices to show that $\lambda_1(X) < \lambda_2(L)$. By Lemma 8, we can assume $\ker(A - \lambda_1(A)I) \subset \mathbf{e}_1^\perp$.

Let $\mathbf{w}$ be an eigenvector of L belonging to the eigenvalue $\lambda_2(L)$. Then

$$\begin{aligned} B^\top \mathbf{w} &\in B^\top \ker(L - \lambda_2(L)I) \\ &= \ker(A - \lambda_1(A)I) \qquad \text{(by Lemma 10)} \\ &\subset \mathbf{e}_1^\perp. \end{aligned}$$

Thus $\mathbf{w} \in (B\mathbf{e}_1)^\perp = (\mathbf{e}_1 - \mathbf{e}_2)^\perp$. Therefore $w_1 = w_2$.

On the other hand, again by Lemma 10, the eigenvector $\mathbf{w}$ can be written as $B\mathbf{v}$ where $\mathbf{v}$ is in $\ker(A - \lambda_1(A)I) \subset \mathbf{e}_1^\perp$. Then $w_1 = \mathbf{e}_1^\top B\mathbf{v} = \mathbf{e}_1^\top \mathbf{v} = 0$. Hence $w_1 = w_2 = 0$. Since the first row of L is given by

$\mathbf{e}_1^\top - \mathbf{e}_2^\top$, we have

$$L\mathbf{w} = \begin{pmatrix} 0 \\ X\mathbf{y} \end{pmatrix},$$

where $\mathbf{w}^\top = (0, \mathbf{y}^\top)$. Hence, $\mathbf{w}$ restricts to an eigenvector $\mathbf{y}$ of X. But the first entry of $\mathbf{y}$ is zero. Since X is an M-matrix, $\lambda_2(L)$ is not the smallest eigenvalue of X. This implies $\lambda_1(X) < \lambda_2(L)$. □

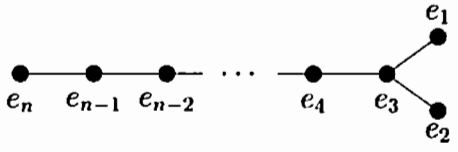


FIGURE 1. The graph $\mathcal{X}_n^{(1)} (n \geqslant 3)$

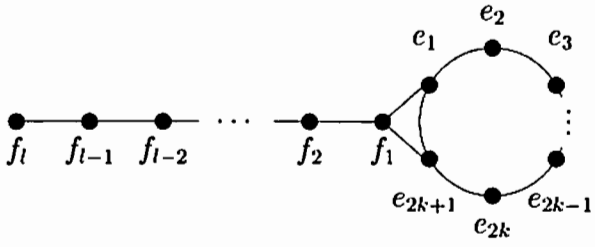


FIGURE 2. The graph $\mathcal{X}_{k,l}^{(2)} (k, l \geqslant 1)$

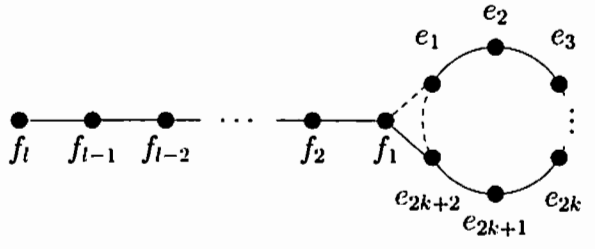


FIGURE 3. The graph $\mathcal{X}_{k,l}^{(3)} (k, l \geqslant 1)$

Lemma 12. *The matrices $\hat{A}(\mathcal{X}_n^{(1)}, e_n)$, $\hat{A}(\mathcal{X}_{k,l}^{(2)}, f_l)$, and $\hat{A}(\mathcal{X}_{k,l}^{(3)}, f_l)$ (see Figures 1, 2, and 3) have smallest eigenvalue -2.*

Proof. We give the eigenvectors corresponding to the eigenvalue -2 of each matrix in the statement of the lemma.

- $\hat{A}(\mathcal{X}_n^{(1)}, e_n)$: set $e_1, e_2 = -1$, and $e_j = (-1)^{j+1} \cdot 2$ for $j \in \{3, \ldots, n\}$.
- $\hat{A}(\mathcal{X}_{k,l}^{(2)}, f_l)$: set $e_j = (-1)^{j+1}$ for $j \in \{1, \ldots, 2k+1\}$ and set $f_j = (-1)^j \cdot 2$ for $j \in \{1, \ldots, l\}$.
- $\hat{A}(\mathcal{X}_{k,l}^{(3)}, f_l)$: set $e_j = (-1)^j$ for $j \in \{1, \ldots, 2k+2\}$ and set $f_j = (-1)^j \cdot 2$ for $j \in \{1, \ldots, l\}$.

Deleting the row and column containing the -1 on the diagonal, we obtain the adjacency matrix of a graph with smallest eigenvalue greater than -2. This is immediate for $\mathcal{X}_n^{(1)}$ since the obtained graph has spectral radius less than 2. As for $\mathcal{X}_{k,l}^{(2)}$ and $\mathcal{X}_{k,l}^{(3)}$, the result follows from (i) and (ii), respectively, of Theorem 6. By interlacing, $\hat{A}(\mathcal{X}_n^{(1)}, e_n)$, $\hat{A}(\mathcal{X}_{k,l}^{(2)}, f_l)$, and $\hat{A}(\mathcal{X}_{k,l}^{(3)}, f_l)$ have at most one eigenvalue less than or equal to -2. This implies that -2 is indeed the smallest eigenvalue. □

Theorem 13. *Let G be a connected edge-signed graph and let $v \in V(G)$ such that $\lambda_1(\hat{A}(G, v)) \geqslant -2$. Then G is integrally represented.*

Proof. Suppose that $\hat{A}(G, v) + 2I$ is positive semidefinite. Then we can write $\hat{A}(G, v) + 2I = U^\top U$ for some matrix U. Label the columns of U as $\mathbf{u}_1, \ldots, \mathbf{u}_n$ where $\|\mathbf{u}_1\| = 1$ and $\|\mathbf{u}_i\|^2 = 2$ for $i \in \{2, \ldots, n\}$. Let $\Lambda = \bigoplus_{i=1}^n \mathbb{Z}\mathbf{u}_i$ and let $B = \{\mathbf{v} \in \Lambda \mid \|\mathbf{v}\| = 1\}$. Clearly $B = \{\pm\mathbf{v}_1, \ldots, \pm\mathbf{v}_m\}$ for some m with $(\mathbf{v}_i, \mathbf{v}_j) = \delta_{ij}$. Define Λ' as the $\mathbb{Z}$-span of the vectors of B and set $X = \Lambda \cap (\Lambda')^\perp$. It is easily checked that a vector $\mathbf{v} \in \Lambda$ with $\|\mathbf{v}\|^2 = 2$ and $\mathbf{v} \notin \Lambda'$ is orthogonal to Λ'. Hence we can write Λ as the orthogonal sum $\Lambda = \Lambda' \perp X$ and so $\mathbf{v} \in X$. Unless either $\Lambda' = 0$ or $X = 0$, this orthogonal decomposition of Λ violates our assumption that G is connected. Since $\mathbf{u}_1 \in \Lambda'$, we must have $X = 0$. Therefore $\Lambda = \Lambda' \cong \mathbb{Z}^m$.

Finally, the vectors

$$\begin{pmatrix} 1 \\ \mathbf{u}_1, \end{pmatrix}, \begin{pmatrix} 0 \\ \mathbf{u}_2, \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \mathbf{u}_n \end{pmatrix}$$

all have norm $\sqrt{2}$ and their Gram matrix gives $A + 2I$. Clearly these vectors are contained in a $\mathbb{Z}$-lattice and this lattice represents G. □

Remark 14. The proof of Theorem 13 is essentially the same as that of [13, Theorem 3.7].

Theorem 15. *Let G be an edge-signed graph with $\lambda_1(G) > -2$, and let $v \in V(G)$. Then $\lambda_1(G) > \lambda_1(\hat{A}(G, v))$. Furthermore, $\lambda_1(\hat{A}(G, v)) >$*

-2 if and only if the underlying graph of G is the line graph of a tree T and v corresponds to an end-edge of T. Otherwise, $\lambda_1(\hat{A}(G,v)) \leqslant -2$.

Proof. By Theorem 2, G is represented by D_n or E_8. We may assume that G is represented by D_n, otherwise by Corollary 3 and Theorem 13 we would have $\lambda_1(\hat{A}(G,v)) < -2$ in which case the theorem holds. Therefore the structure of G can be described by Theorem 6.

First suppose G is of type (i) from Theorem 6. Suppose G is the line graph of a tree T. If v is not an end-edge of T then $\hat{A}(G,v)$ contains $\hat{A}(\mathcal{X}_3^{(1)}, e_3)$ as a principal submatrix, hence $\lambda_1(\hat{A}(G,v)) \leqslant -2$. If v is an end-edge of T, then $\lambda_1(G) > \lambda_1(\hat{A}(G,v))$ by Theorem 1, and $\lambda_1(\hat{A}(G,v)) > -2$ by Lemma 8. Next suppose G is of type (i) but not the line graph of a tree T. That is, G is the line graph of a unicyclic graph with an odd cycle (and G is not equal to C_3). Then $\hat{A}(G,v)$ contains (as a principal submatrix) either $\hat{A}(\mathcal{X}_3^{(1)}, e_3)$ or $\hat{A}(\mathcal{X}_{k,l}^{(2)}, f_l)$ for some k and l.

Suppose G is of type (ii). Then $\hat{A}(G,v)$ contains (as a principal submatrix) either $\hat{A}(\mathcal{X}_3^{(1)}, e_3)$ or $\hat{A}(\mathcal{X}_{k,l}^{(3)}, f_l)$ for some k and l.

Suppose G is of type (iii). Then G contains $\mathcal{X}_n^{(1)}$ for some n. Therefore, by Lemma 11, we have $\lambda_1(\hat{A}(G,v)) \leqslant -2$ for these cases. □

Remark 16. A special case of Theorem 15 for unsigned graphs is given in [17, Theorem 5.2].

5. Exceptional graphs

In this section we enumerate the exceptional edge-signed graphs with smallest eigenvalue greater than -2, i.e., those that are not integrally represented. In the tables in the appendix we list (up to switching) every such edge-signed graph. We generalise the following result about graphs with smallest eigenvalue greater than -2.

Theorem 17 ([2, 6]). *Let G be an exceptional graph having smallest eigenvalue greater than -2. Then G is one of*

(i) 20 *graphs on* 6 *vertices;*
(ii) 110 *graphs on* 7 *vertices;*
(iii) 443 *graphs on* 8 *vertices.*

To describe our results, we need a list of 120 lines of the root system E_8. Such a list can be found in [7, Appendix B], and this is also sufficient to describe our results for E_6 and E_7, since these root systems can be embedded in E_8. Each of the 120 lines are determined by a vector $\beta = \sum_{i=1}^{8} b_i \alpha_i$ and the coefficients $(b_1, \ldots, b_8)$ for each β are given in [7,

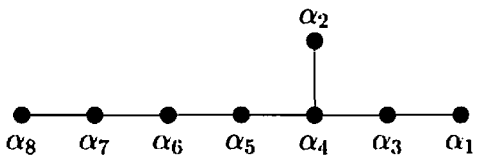


FIGURE 4. The simple roots of E_8

Appendix B]. The inner products among the basis vectors $\alpha_1, \ldots, \alpha_8$ are described by Figure 4, where $(\alpha_i, \alpha_i) = 2$ for all $i \in \{1, \ldots, 8\}$, $(\alpha_i, \alpha_j) = -1$ if α_i and α_j are adjacent, $(\alpha_i, \alpha_j) = 0$ otherwise. The lines determined by E_6 are precisely the 36 lines with $b_7 = b_8 = 0$, and the lines determined by E_7 are precisely the 63 lines with $b_8 = 0$.

Remark 18. The numbering of the 120 lines of E_8 in [7, Appendix B] is the natural one in the following sense. Every line can be represented by a vector $\alpha = \sum_{i=1}^{8} a_i \alpha_i$ with $\|\alpha\|^2 = 2$ and $a_i \geqslant 0$ for all i. We assign a total ordering to the lines as follows. Let $\alpha = \sum_{i=1}^{8} a_i \alpha_i$, $\beta = \sum_{i=1}^{8} b_i \alpha_i$. We define $[\alpha] \prec [\beta]$ if either

$$\sum_{i=1}^{8} a_i < \sum_{i=1}^{8} b_i;$$

or

$$\sum_{i=1}^{8} a_i = \sum_{i=1}^{8} b_i \text{ and}$$
$$a_1 = b_1, \ldots, a_i = b_i, a_{i+1} > b_{i+1}.$$

Note that this ordering on the set of lines is the default ordering given by MAGMA [14] on the set of positive roots of the root system E_8 (which are in one-to-one correspondence with the lines of the line system E_8).

Let $n = 7$ or 8 and let G be an n-vertex exceptional edge-signed graph. By [18, Theorem 1.10], G can be obtained from an $(n-1)$-vertex exceptional edge-signed graph H by attaching a vertex to H.

In the tables in the appendix we describe, up to switching equivalence, the edge-signed graphs that are not integrally represented. Each edge-signed graph is described by referring to the lines used to construct it and each line is referred to by its number in [7, Appendix B], or equivalently, by its position in the total ordering. Clearly, exceptional edge-signed graphs with smallest eigenvalue greater than -2 must have at least 6 vertices and at most 8 vertices. In Table 1 the 32 exceptional switching classes $\mathcal{S}_{6,i}$ $(1 \leqslant i \leqslant 32)$ of 6-vertex edge-signed graphs are described. The first 20 out of the 32 consist of those classes which contain an unsigned graph, and these ordered according to [4, Table A2], in which graphs are ordered by the number of edges. The remaining 12 switching classes are also ordered by the number of edges.

In Table 2 the 233 exceptional switching classes $\mathcal{S}_{7,i}$ $(1 \leqslant i \leqslant 233)$ of 7-vertex edge-signed graphs are described. Each switching class $\mathcal{S}_{7,i}$ is obtained by adding a line l to $\mathcal{S}_{6,k}$. In Table 2, the triples i, l, k are listed, and the first 110 switching classes consist of those classes which contain an unsigned graph, and these ordered according to [4, Table A2]. Similarly, in Tables 3, 4, 5, 6, and 7, the 1242 exceptional switching classes $\mathcal{S}_{8,i}$ $(1 \leqslant i \leqslant 1242)$ of 8-vertex edge-signed graphs are described. Each switching class $\mathcal{S}_{8,i}$ is obtained by adding a line l to $\mathcal{S}_{7,k}$ and these triple i, k, l are given in the tables. As before, in the tables the 443 unsigned graphs in [4, Table A2] come first.

We can summarise the tables below in the following theorem.

Theorem 19. *Let G be an exceptional edge-signed graph having smallest eigenvalue greater than -2. Then G is one of*

(i) 32 *edge-signed graphs on 6 vertices;*
(ii) 233 *edge-signed graphs on 7 vertices;*
(iii) 1242 *edge-signed graphs on 8 vertices.*

6. Hoffman graphs

A **Hoffman graph** $\mathfrak{H}$ is defined as a graph (V, E) with a distinguished coclique $V_f(\mathfrak{H}) \subset V$ called **fat** vertices, the remaining vertices $V_s(\mathfrak{H}) = V \backslash V_f(\mathfrak{H})$ are called **slim** vertices. For more background on Hoffman graphs see some of the authors' previous papers [13, 16, 17]. Let $\mathfrak{H}$ be a Hoffman graph and suppose its adjacency matrix A has the following form

$$A = \begin{pmatrix} A_s & C \\ C^{\mathsf{T}} & 0 \end{pmatrix},$$

where the fat vertices come last. Define $B(\mathfrak{H}) := A_s - CC^{\mathsf{T}}$. The eigenvalues of $\mathfrak{H}$ are defined to be the eigenvalues of $B(\mathfrak{H})$. A Hoffman graph $\mathfrak{H}$ is called **fat** if every slim vertex of $\mathfrak{H}$ has at least one fat neighbour. In this section we show how our results relate to the classification of fat Hoffman graphs with smallest eigenvalue greater than -3.

It is shown in [17] that if $\lambda_1(B(\mathfrak{H})) > -3$ then every slim vertex is adjacent to at most two fat vertices and at most one slim vertex can be adjacent to more than one fat vertex. It therefore follows that if a fat Hoffman graph $\mathfrak{H}$ has smallest eigenvalue $\lambda_1(\mathfrak{H}) > -3$ then the diagonal of $B(\mathfrak{H}) + I$ consists of at most one -1 entry and the remaining entries 0. In other words, $B(\mathfrak{H}) + I$ is either the adjacency matrix $A(G)$ of a signed graph G, or the modified adjacency matrix $\hat{A}(G, v)$ of G with respect to some vertex v. The **special graph** $\mathcal{S}(\mathfrak{H})$ of a Hoffman

graph $\mathfrak{H}$ is the edge-signed graph whose adjacency matrix has the same off-diagonal entries as $B(\mathfrak{H})$ and zeros on the diagonal.

Theorem 20. *Let $\mathfrak{H}$ be a fat Hoffman graph in which every slim vertex has exactly one fat neighbour. Then $\mathfrak{H}$ has smallest eigenvalue greater than -3 if and only if $\mathcal{S}(\mathfrak{H})$ is switching equivalent to one of the edge-signed graphs in Theorem 6 or Theorem 19.*

Proof. Since every slim vertex has exactly one fat neighbour, $B(\mathfrak{H})+I$ is the adjacency matrix of $\mathcal{S}(\mathfrak{H})$. Thus $\mathfrak{H}$ has smallest eigenvalue greater than -3 if and only if $\mathcal{S}(\mathfrak{H})$ has smallest eigenvalue greater than -2. The result then follows since Theorems 6 and 19 give a classification of edge-signed graphs with smallest eigenvalues greater than -2. □

Lemma 21. *Let $\mathfrak{H}$ be a fat Hoffman graph in which every slim vertex has exactly one fat neighbour. Then in the special graph $\mathcal{S}(\mathfrak{H})$ of $\mathfrak{H}$, there are no $(+)$-edges in the neighbourhood of any fat vertex. In particular, $\mathcal{S}(\mathfrak{H})$ does not contain a cycle in which all but one edge are $(-)$-edges.*

Proof. Let N be the set of neighbours of a fat vertex. Then the off-diagonal entry of $B(\mathfrak{H})$ corresponding to two vertices of N cannot be 1. This shows the first claim. Suppose that $\mathcal{S}(\mathfrak{H})$ contains a cycle $v_0, v_1, \ldots, v_n, v_0$ such that all but the edge $\{v_n, v_0\}$ are $(-)$-edges. Then v_i, v_{i+1} have a common fat neighbour for $i = 0, 1, \ldots, n-1$. Since every slim vertex has exactly one fat neighbour, it follows that $v_0, \ldots, v_n$ have a common fat neighbour. But this contradicts the first claim. □

Lemma 21 implies that not every edge-signed graph can be the special graph of a fat Hoffman graph in which every slim vertex has exactly one fat neighbour.

For an edge-signed graph $\mathcal{S} = (V, E^+, E^-)$, we denote by $\mathcal{S}^-$ the unsigned graph (V, E^-). Let $\mathcal{S}$ be an edge-signed graph that is switching equivalent to one of the edge-signed graphs in Theorem 6 or Theorem 19, and $\mathcal{S}$ has no cycle in which all but one edge are $(-)$-edges. Then every fat Hoffman graph $\mathfrak{H}$ in which every slim vertex has exactly one fat neighbour, satisfying $\mathcal{S}(\mathfrak{H}) = \mathcal{S}$ is obtained as follows. Let

$$V(\mathcal{S}) = \bigcup_{i=1}^{n} V_i \quad \text{(disjoint)}$$

be a partition satisfying

(i) for all $i \in \{1, \ldots, n\}$, the subgraph induced on V_i contains no $(+)$-edges,

(ii) every connected component of $\mathcal{S}^-$ is contained in V_i for some $i \in \{1, \ldots, n\}$.

Define a Hoffman graph $\mathfrak{H}$ as follows. The vertex set of $\mathfrak{H}$ consists of the set of slim vertices $V(\mathcal{S})$ and the set of fat vertices $\{f_1, \ldots, f_n\}$. The edges are $\{f_i, u\}$ with $u \in V_i$, $1 \leq i \leq n$; $\{u, v\}$ with $u, v \in V_i$, $1 \leq i \leq n$, $\{u, v\} \notin E(\mathcal{S})$; and $\{u, v\}$ with $u \in V_i$, $v \in V_j$, $1 \leq i, j \leq n$, $i \neq j$, $\{u, v\} \in E(\mathcal{S})$. Observe that for $u, v \in V_i$, $\{u, v\} \notin E(\mathcal{S})$ if and only if $\{u, v\} \notin E^-(\mathcal{S})$, and for $u \in V_i$, $v \in V_j$ with $i \neq j$, $\{u, v\} \in E(\mathcal{S})$ if and only if $\{u, v\} \in E^+(\mathcal{S})$. Then $\mathcal{S}(\mathfrak{H}) = \mathcal{S}$ holds, and $\lambda_1(\mathfrak{H}) = \lambda_1(\mathcal{S}) - 1$.

In general, given an edge-signed graph $\mathcal{S}$, there are a number of fat Hoffman graphs $\mathfrak{H}$ with $\mathcal{S}(\mathfrak{H}) = \mathcal{S}$, satisfying the condition that every slim vertex of $\mathfrak{H}$ has exactly one fat neighbour. For example, consider the simplest case where $\mathcal{S}$ is a path consisting only of (+)-edges. Then such Hoffman graphs are in one-to-one correspondence with partitions of the vertex-set into cocliques.

REFERENCES

[1] A.E. Brouwer and W.H. Haemers. *Spectra of Graphs*. Universitexts. Springer, 2012.

[2] F.C. Bussemaker and A. Neumaier. Exceptional graphs with smallest eigenvalue -2 and related problems. *Math. Comp.*, 59(200):583–608, 1992.

[3] P.J. Cameron, J.M. Goethals, E.E. Shult and J.J. Seidel. Line graphs, root systems, and elliptic geometry. *J. Algebra* 43(1):305–327, 1976.

[4] D. Cvetković, P. Rowlinson and S. Simić. *Spectral Generalizations of Line Graphs*. London Math. Soc. Lecture Note Ser. 314. Cambridge Univ. Press, 2004.

[5] M. Doob. An interrelation between line graphs, eigenvalues, and matroids. *J. Combin. Theory B*, 15:40–50, 1973.

[6] M. Doob and D. Cvetković. On spectral characterizations and embeddings of graphs. *Linear Algebra Appl.*, 27:17–26, 1979.

[7] A.-S. Gleitz. On the KNS conjecture in type *E*. *Preprint.*, arXiv:1307.2738v1.

[8] C.D. Godsil and G. Royle. *Algebraic Graph Theory*. Graduate Texts in Mathematics. New York: Springer, 2000.

[9] A.J. Hoffman. On limit points of the least eigenvalue of a graph. *Ars Combin.*, 3:3–14, 1977.

[10] A.J. Hoffman. On graphs whose least eigenvalue exceeds $-1 - \sqrt{2}$. *Linear Algebra Appl.*, 16:153–165, 1977.

[11] R.A. Horn and C.R. Johnson. *Matrix Analysis*. Cambridge University Press. 1985

[12] T. Ishihara. Signed graphs associated with the lattice A_n. *J. Math. Univ. Tokushima*, Vol. 36 (2002), 1–6.

[13] H.J. Jang, J. Koolen, A. Munemasa and T. Taniguchi. On fat Hoffman graphs with smallest eigenvalue at least -3. *Ars Math. Contemp.*, 7:105–121, 2014.

[14] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.). Handbook of Magma functions. Edition 2.18, 5017 pages. 2013.

[15] J. McKee and C. Smyth. Integer symmetric matrices having all their eigenvalues in the interval $[-2, 2]$. *J. Algebra*, 317:260–290, 2007.

[16] A. Munemasa, Y. Sano and T. Taniguchi. Fat Hoffman graphs with smallest eigenvalue at least $-1 - \tau$, *Ars Math. Contemp.*, 7:247–262, 2014.

[17] A. Munemasa, Y. Sano and T. Taniguchi. Fat Hoffman graphs with smallest eigenvalue greater than -3. *Preprint*, arXiv:1211.3929v2.

[18] G.R. Vijayakumar. Algebraic equivalence of signed graphs with all eigenvalues ≥ -2. *Ars Combin.*, 35:173–191, 1993.

[19] R. Woo and A. Neumaier. On graphs whose smallest eigenvalue is at least $-1 - \sqrt{2}$. *Linear Algebra Appl.*, 226-228:577–591, 1995.

APPENDIX

TABLE 1. Switching classes $\mathcal{S}_{6,i}$ $(i = 1, \ldots, 32)$

i	lines	i	lines
1	1, 2, 3, 4, 44, 48	17	1, 2, 3, 11, 19, 63
2	1, 2, 3, 4, 6, 24	18	1, 3, 5, 11, 17, 27
3	1, 3, 4, 6, 17, 18	19	1, 2, 3, 11, 18, 27
4	1, 2, 3, 4, 12, 69	20	1, 3, 5, 11, 17, 52
5	1, 3, 4, 17, 18, 26	21	1, 3, 4, 6, 30, 48
6	1, 2, 3, 4, 6, 12	22	1, 2, 3, 4, 18, 48
7	1, 2, 3, 4, 24, 52	23	1, 3, 4, 5, 6, 18
8	1, 2, 3, 11, 30, 48	24	1, 2, 3, 4, 6, 30
9	1, 3, 4, 10, 18, 20	25	1, 3, 4, 5, 6, 30
10	1, 2, 3, 4, 12, 45	26	1, 2, 3, 11, 12, 48
11	1, 2, 3, 4, 25, 48	27	1, 2, 3, 4, 12, 26
12	1, 2, 3, 4, 37, 52	28	1, 2, 3, 4, 19, 20
13	1, 3, 4, 17, 18, 33	29	1, 2, 3, 11, 18, 20
14	1, 2, 3, 4, 24, 33	30	1, 2, 3, 4, 19, 27
15	1, 3, 5, 11, 17, 20	31	1, 2, 3, 11, 18, 31
16	1, 2, 3, 4, 12, 20	32	1, 3, 5, 11, 17, 45

RESEARCH CENTER FOR PURE AND APPLIED MATHEMATICS, GRADUATE SCHOOL OF INFORMATION SCIENCES, TOHOKU UNIVERSITY, SENDAI 980-8579, JAPAN
E-mail address: grwgrvs@ims.is.tohoku.ac.jp

SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA, HEFEI, ANHUI, 230026, P.R. CHINA
E-mail address: koolen@ustc.edu.cn

RESEARCH CENTER FOR PURE AND APPLIED MATHEMATICS, GRADUATE SCHOOL OF INFORMATION SCIENCES, TOHOKU UNIVERSITY, SENDAI 980-8579, JAPAN
E-mail address: munemasa@math.is.tohoku.ac.jp

DIVISION OF INFORMATION ENGINEERING, FACULTY OF ENGINEERING, INFORMATION AND SYSTEMS, UNIVERSITY OF TSUKUBA, IBARAKI 305-8573, JAPAN
E-mail address: sano@cs.tsukuba.ac.jp

MATSUE COLLEGE OF TECHNOLOGY, MATSUE 690-8518, JAPAN
E-mail address: tetsuzit@matsue-ct.ac.jp

TABLE 2. Switching classes $\mathcal{S}_{7,i}$ $(1 \leqslant i \leqslant 233)$ where $i \equiv i' \pmod{100}$

$1 \leqslant i \leqslant 50$			$51 \leqslant i \leqslant 100$			$101 \leqslant i \leqslant 150$			$151 \leqslant i \leqslant 200$			$201 \leqslant i \leqslant 233$		
i'	k	l	i'	k	l	i'	k	l	i'	k	l	i'	k	l
1	1	80	51	8	61	1	12	41	51	25	70	1	16	49
2	1	75	52	7	97	2	15	59	52	5	85	2	26	41
3	2	58	53	9	59	3	16	28	53	26	76	3	29	93
4	1	55	54	2	41	4	19	46	54	27	61	4	30	75
5	3	7	55	9	58	5	20	85	55	24	66	5	16	34
6	1	59	56	12	76	6	16	41	56	28	14	6	7	49
7	2	89	57	5	41	7	20	41	57	6	76	7	27	35
8	3	70	58	8	76	8	19	35	58	8	89	8	30	39
9	1	85	59	8	66	9	20	66	59	23	41	9	30	85
10	3	80	60	9	28	10	20	59	60	29	7	10	31	89
11	3	14	61	6	70	11	1	82	61	28	97	11	28	93
12	4	7	62	6	71	12	1	49	62	29	21	12	15	55
13	3	34	63	13	80	13	1	97	63	23	89	13	15	53
14	6	97	64	16	97	14	3	46	64	23	58	14	28	28
15	1	64	65	6	28	15	23	97	65	26	49	15	29	66
16	6	21	66	10	59	16	21	58	66	25	75	16	31	46
17	2	71	67	12	28	17	21	75	67	21	59	17	27	41
18	2	28	68	13	89	18	2	75	68	25	97	18	30	28
19	6	61	69	8	93	19	23	82	69	13	76	19	28	53
20	7	7	70	7	59	20	24	21	70	25	61	20	17	97
21	4	75	71	9	41	21	1	89	71	25	71	21	29	59
22	6	93	72	9	53	22	23	7	72	4	89	22	11	46
23	6	14	73	15	34	23	21	49	73	29	55	23	28	64
24	8	7	74	16	93	24	4	14	74	9	46	24	30	34
25	4	64	75	17	75	25	26	97	75	28	55	25	31	59
26	9	97	76	12	97	26	22	49	76	27	64	26	31	66
27	1	41	77	18	7	27	27	97	77	24	64	27	30	93
28	3	58	78	6	41	28	4	34	78	26	66	28	31	41
29	8	21	79	18	70	29	23	46	79	25	55	29	18	53
30	3	93	80	14	85	30	6	49	80	28	59	30	32	93
31	7	76	81	10	28	31	23	61	81	27	39	31	32	53
32	4	93	82	18	85	32	22	75	82	8	58	32	16	46
33	7	93	83	15	28	33	23	21	83	13	46	33	20	53
34	8	55	84	18	71	34	21	85	84	5	39			
35	4	85	85	8	46	35	24	97	85	24	76			
36	6	53	86	12	53	36	23	28	86	27	71			
37	11	80	87	8	35	37	23	34	87	25	66			
38	5	28	88	13	28	38	4	97	88	29	82			
39	11	97	89	12	59	39	5	46	89	8	39			
40	8	97	90	13	93	40	25	39	90	24	41			
41	12	80	91	14	28	41	21	89	91	23	71			
42	5	93	92	18	21	42	3	39	92	28	80			
43	3	41	93	11	41	43	3	76	93	30	21			
44	4	71	94	19	89	44	23	80	94	11	49			
45	13	97	95	13	59	45	24	80	95	22	46			
46	13	7	96	20	71	46	25	89	96	25	53			
47	7	28	97	20	75	47	23	14	97	13	49			
48	7	53	98	18	49	48	24	85	98	31	97			
49	10	97	99	19	58	49	24	71	99	28	89			
50	8	53	0	17	66	50	25	21	0	12	49			

TABLE 3. Switching classes $\mathcal{S}_{8,i}$ $(1 \leqslant i \leqslant 250)$

$1 \leqslant i \leqslant 50$			$51 \leqslant i \leqslant 100$			$101 \leqslant i \leqslant 150$			$151 \leqslant i \leqslant 200$			$201 \leqslant i \leqslant 250$		
i'	k	l	i'	k	l	i'	k	l	i'	k	l	i'	k	l
1	1	8	51	14	90	1	5	50	51	45	74	1	64	47
2	1	118	52	16	116	2	42	74	52	27	95	2	19	36
3	2	118	53	5	106	3	44	68	53	58	8	3	58	74
4	1	96	54	1	50	4	14	84	54	46	118	4	28	50
5	1	92	55	28	74	5	44	8	55	5	105	5	69	78
6	5	8	56	14	106	6	43	8	56	14	77	6	60	116
7	1	95	57	6	102	7	45	87	57	28	79	7	36	84
8	6	118	58	27	8	8	20	95	58	15	102	8	58	77
9	6	8	59	4	62	9	32	118	59	59	8	9	28	84
10	4	96	60	6	105	10	21	79	60	14	78	10	65	47
11	3	106	61	17	74	11	19	68	61	45	103	11	71	8
12	7	8	62	9	117	12	24	87	62	43	74	12	61	87
13	8	74	63	8	77	13	22	47	63	44	103	13	73	118
14	1	90	64	19	74	14	25	47	64	59	116	14	62	106
15	9	8	65	19	118	15	10	78	65	45	92	15	64	74
16	10	74	66	31	8	16	48	96	66	64	8	16	74	74
17	5	118	67	9	103	17	37	118	67	65	118	17	65	117
18	5	117	68	32	68	18	17	84	68	16	36	18	75	8
19	12	8	69	32	8	19	9	50	69	31	77	19	41	74
20	6	62	70	19	117	20	39	116	70	32	90	20	75	118
21	14	8	71	8	84	21	40	87	71	36	68	21	64	90
22	15	118	72	2	108	22	21	105	72	48	62	22	77	117
23	5	42	73	3	77	23	37	92	73	52	116	23	24	105
24	13	8	74	28	77	24	23	108	74	31	95	24	26	103
25	16	118	75	2	50	25	12	90	75	21	47	25	28	106
26	9	96	76	10	106	26	5	78	76	52	95	26	78	116
27	3	78	77	4	36	27	25	102	77	35	105	27	79	74
28	9	62	78	11	108	28	50	118	78	52	78	28	30	79
29	7	74	79	21	103	29	35	103	79	37	77	29	47	77
30	11	74	80	27	62	30	9	90	80	52	92	30	33	36
31	12	68	81	28	117	31	25	105	81	39	68	31	54	78
32	7	90	82	34	118	32	37	78	82	51	118	32	32	79
33	4	117	83	7	84	33	16	105	83	34	42	33	32	105
34	9	78	84	30	77	34	26	105	84	51	62	34	51	42
35	19	8	85	35	68	35	10	50	85	66	96	35	49	105
36	10	42	86	4	47	36	2	36	86	59	87	36	51	96
37	20	8	87	36	118	37	12	78	87	24	95	37	48	79
38	3	108	88	14	92	38	53	77	88	36	90	38	53	102
39	14	116	89	35	8	39	40	77	89	20	74	39	67	92
40	20	62	90	22	106	40	25	95	90	55	79	40	58	108
41	12	118	91	13	108	41	55	74	91	34	62	41	50	62
42	14	74	92	1	36	42	55	77	92	22	77	42	67	116
43	4	103	93	30	118	43	41	92	93	42	103	43	49	102
44	13	117	94	36	8	44	21	96	94	36	79	44	23	105
45	12	96	95	39	92	45	22	79	95	67	118	45	24	79
46	22	74	96	23	106	46	43	117	96	22	78	46	53	79
47	1	79	97	25	106	47	41	95	97	39	95	47	50	56
48	6	103	98	27	78	48	23	117	98	45	84	48	50	102
49	5	108	99	11	117	49	44	102	99	25	108	49	75	68
50	12	103	0	41	8	50	43	42	0	63	42	50	71	116

TABLE 4. Switching classes $\mathcal{S}_{8,i}$ $(251 \leqslant i \leqslant 500)$

$251 \leqslant i \leqslant 300$			$301 \leqslant i \leqslant 350$			$351 \leqslant i \leqslant 400$			$401 \leqslant i \leqslant 450$			$451 \leqslant i \leqslant 500$		
i'	k	l	i'	k	l	i'	k	l	i'	k	l	i'	k	l
51	7	50	1	82	68	51	68	79	1	97	116	51	1	68
52	76	47	2	63	78	52	95	77	2	94	79	52	1	42
53	53	42	3	91	62	53	35	36	3	71	84	53	114	74
54	37	90	4	36	78	54	90	106	4	103	105	54	4	92
55	54	74	5	83	42	55	36	50	5	106	74	55	111	74
56	29	79	6	60	108	56	79	106	6	77	79	56	122	8
57	56	95	7	52	105	57	62	77	7	103	77	57	1	106
58	57	42	8	20	50	58	40	43	8	78	50	58	1	84
59	76	95	9	91	118	59	74	84	9	107	118	59	116	8
60	75	96	10	85	74	60	75	77	10	89	105	60	118	118
61	74	90	11	74	79	61	57	50	11	90	79	61	3	116
62	11	105	12	56	108	62	101	92	12	98	106	62	117	8
63	60	42	13	76	78	63	44	36	13	92	106	63	116	92
64	64	105	14	92	118	64	102	118	14	91	36	64	119	74
65	78	117	15	34	43	65	97	92	15	99	106	65	1	87
66	36	108	16	88	42	66	62	78	16	107	92	66	112	62
67	82	8	17	41	105	67	78	84	17	107	110	67	115	47
68	22	50	18	76	68	68	65	36	18	95	79	68	16	42
69	43	84	19	76	102	69	31	50	19	87	43	69	130	118
70	38	79	20	61	36	70	92	92	20	108	118	70	2	84
71	84	8	21	94	74	71	83	56	21	109	8	71	10	90
72	78	74	22	39	108	72	94	84	22	100	77	72	122	118
73	61	84	23	59	105	73	95	84	23	98	79	73	4	42
74	58	56	24	89	103	74	87	108	24	98	102	74	13	116
75	27	36	25	59	102	75	98	74	25	86	50	75	121	87
76	27	108	26	42	105	76	99	77	26	100	102	76	5	47
77	85	92	27	62	84	77	90	78	27	89	50	77	129	74
78	63	102	28	90	118	78	81	78	28	102	79	78	6	77
79	86	92	29	96	8	79	97	47	29	110	77	79	4	77
80	64	103	30	43	50	80	58	110	30	107	87	80	9	74
81	86	118	31	96	68	81	78	77	31	107	79	81	115	92
82	26	84	32	46	50	82	54	50	32	105	102	82	111	56
83	87	78	33	68	106	83	73	105	33	96	105	83	122	74
84	88	8	34	50	110	84	72	108	34	103	36	84	122	116
85	88	118	35	81	95	85	88	108	35	108	108	85	122	42
86	42	79	36	83	92	86	86	105	36	105	105	86	134	8
87	89	118	37	54	77	87	103	47	37	106	36	87	7	118
88	90	74	38	67	36	88	105	68	38	104	43	88	137	8
89	70	77	39	82	90	89	59	43	39	107	102	89	133	87
90	66	77	40	84	116	90	65	50	40	110	50	90	12	42
91	61	105	41	83	116	91	90	102	41	109	102	91	118	62
92	81	47	42	81	77	92	91	105	42	110	106	92	123	92
93	69	68	43	83	96	93	98	95	43	110	105	93	12	62
94	55	105	44	59	110	94	49	50	44	112	8	94	117	77
95	67	103	45	94	103	95	52	50	45	111	8	95	122	110
96	67	102	46	71	102	96	85	79	46	113	8	96	119	47
97	71	42	47	93	78	97	73	106	47	1	74	97	122	47
98	51	68	48	71	103	98	92	116	48	121	8	98	116	77
99	81	96	49	85	77	99	101	95	49	4	116	99	113	106
0	68	102	50	67	105	0	102	36	50	6	87	0	113	56

TABLE 5. Switching classes $\mathcal{S}_{8,i}$ ($501 \leqslant i \leqslant 750$)

$501 \leqslant i \leqslant 550$			$551 \leqslant i \leqslant 600$			$601 \leqslant i \leqslant 650$			$651 \leqslant i \leqslant 700$			$701 \leqslant i \leqslant 750$		
i'	k	l	i'	k	l	i'	k	l	i'	k	l	i'	k	l
1	116	96	51	119	90	1	138	96	51	132	106	1	154	96
2	119	87	52	143	118	2	124	95	52	122	108	2	139	108
3	115	77	53	119	102	3	16	96	53	133	92	3	151	96
4	140	118	54	132	103	4	137	68	54	14	110	4	37	42
5	119	79	55	120	92	5	163	87	55	148	106	5	123	79
6	122	77	56	11	47	6	14	56	56	173	116	6	125	117
7	119	36	57	131	74	7	151	8	57	30	95	7	182	78
8	111	90	58	122	92	8	113	79	58	181	74	8	121	108
9	6	117	59	132	116	9	131	118	59	159	96	9	161	118
10	4	43	60	160	8	10	168	47	60	45	110	10	192	74
11	111	103	61	121	68	11	130	68	61	124	62	11	37	106
12	127	8	62	144	87	12	161	8	62	188	74	12	164	87
13	115	96	63	117	96	13	176	96	63	14	62	13	155	117
14	145	106	64	140	47	14	114	102	64	144	77	14	114	50
15	120	116	65	164	118	15	143	116	65	36	96	15	42	77
16	130	8	66	127	116	16	164	77	66	133	50	16	115	43
17	122	36	67	12	74	17	124	74	67	164	110	17	132	102
18	12	116	68	160	117	18	114	84	68	158	116	18	138	105
19	128	8	69	9	84	19	168	42	69	114	78	19	184	8
20	142	74	70	122	79	20	13	47	70	112	110	20	20	68
21	4	84	71	114	77	21	24	50	71	139	62	21	119	117
22	121	105	72	134	96	22	131	68	72	28	90	22	157	56
23	111	87	73	127	87	23	120	103	73	142	106	23	146	77
24	113	116	74	135	84	24	148	84	74	123	43	24	123	84
25	127	74	75	15	106	25	153	118	75	167	47	25	41	118
26	8	103	76	124	106	26	191	74	76	10	43	26	122	84
27	123	87	77	132	56	27	160	118	77	14	43	27	125	84
28	4	106	78	162	117	28	136	117	78	172	8	28	114	62
29	168	8	79	154	8	29	136	36	79	28	96	29	192	117
30	122	43	80	16	43	30	124	103	80	13	102	30	44	116
31	18	62	81	150	42	31	39	118	81	140	92	31	141	79
32	136	74	82	9	56	32	122	90	82	131	90	32	158	74
33	123	96	83	6	106	33	180	74	83	137	79	33	157	87
34	16	79	84	120	79	34	189	118	84	139	90	34	147	116
35	157	74	85	168	87	35	165	92	85	127	78	35	27	87
36	115	42	86	116	79	36	16	92	86	125	90	36	159	92
37	25	68	87	111	79	37	141	62	87	114	56	37	159	79
38	29	117	88	145	74	38	124	92	88	132	96	38	174	92
39	149	87	89	124	56	39	172	68	89	115	95	39	189	116
40	117	84	90	129	92	40	117	102	90	178	8	40	28	103
41	13	56	91	122	50	41	126	87	91	45	96	41	153	92
42	125	78	92	132	77	42	165	68	92	156	117	42	26	110
43	131	116	93	149	116	43	144	106	93	23	96	43	46	116
44	137	92	94	122	117	44	132	79	94	129	117	44	153	68
45	123	116	95	153	8	45	169	117	95	134	118	45	129	50
46	5	84	96	21	42	46	125	77	96	135	42	46	129	68
47	148	8	97	142	77	47	157	79	97	134	77	47	143	42
48	123	106	98	15	77	48	156	106	98	156	74	48	113	36
49	123	77	99	148	116	49	45	118	99	154	74	49	19	102
50	6	110	0	22	96	50	21	116	0	137	117	50	143	84

TABLE 6. Switching classes $\mathcal{S}_{8,i}$ $(751 \leqslant i \leqslant 1000)$

$751 \leqslant i \leqslant 800$			$801 \leqslant i \leqslant 850$			$851 \leqslant i \leqslant 900$			$901 \leqslant i \leqslant 950$			$951 \leqslant i \leqslant 1000$		
i'	k	l	i'	k	l	i'	k	l	i'	k	l	i'	k	l
51	131	117	1	185	79	51	156	62	1	33	42	51	123	110
52	154	62	2	131	78	52	147	77	2	189	106	52	185	77
53	187	8	3	203	92	53	183	103	3	175	92	53	40	42
54	138	74	4	154	68	54	162	108	4	209	92	54	174	87
55	166	47	5	119	105	55	155	79	5	64	42	55	155	96
56	159	74	6	162	77	56	143	102	6	212	78	56	156	36
57	122	103	7	188	118	57	44	42	7	166	68	57	130	105
58	7	47	8	194	77	58	134	95	8	36	103	58	152	84
59	161	74	9	163	116	59	122	78	9	169	95	59	145	36
60	124	47	10	202	103	60	209	74	10	212	42	60	177	90
61	136	43	11	207	118	61	124	43	11	135	50	61	152	50
62	187	47	12	123	56	62	116	68	12	183	68	62	52	103
63	41	42	13	200	8	63	161	68	13	222	118	63	153	42
64	25	110	14	197	118	64	124	79	14	178	90	64	156	84
65	45	90	15	157	90	65	172	62	15	199	68	65	21	43
66	186	118	16	188	62	66	177	74	16	62	96	66	179	106
67	155	68	17	180	47	67	172	74	17	216	103	67	31	90
68	135	68	18	196	118	68	165	84	18	62	103	68	50	103
69	147	50	19	17	103	69	186	79	19	191	50	69	161	108
70	61	56	20	156	42	70	177	62	20	203	118	70	155	77
71	150	50	21	158	68	71	136	90	21	209	84	71	174	102
72	41	56	22	179	84	72	189	92	22	194	62	72	164	108
73	209	8	23	161	79	73	158	95	23	211	90	73	200	95
74	46	95	24	193	106	74	34	36	24	163	84	74	194	84
75	53	62	25	187	74	75	177	79	25	218	8	75	160	42
76	131	62	26	127	42	76	144	108	26	176	90	76	169	84
77	124	77	27	54	62	77	178	78	27	180	106	77	167	110
78	172	118	28	156	90	78	117	68	28	147	84	78	190	84
79	185	84	29	190	87	79	155	78	29	192	105	79	173	108
80	173	68	30	42	90	80	161	84	30	174	47	80	44	110
81	123	78	31	146	84	81	160	68	31	157	95	81	40	50
82	140	95	32	150	79	82	50	84	32	223	118	82	217	8
83	120	95	33	147	56	83	141	108	33	156	79	83	201	116
84	210	8	34	139	36	84	130	36	34	204	92	84	221	118
85	161	62	35	143	95	85	167	84	35	188	84	85	76	96
86	205	8	36	159	43	86	122	95	36	37	62	86	197	77
87	144	78	37	60	62	87	43	56	37	207	79	87	148	108
88	161	77	38	163	47	88	189	87	38	154	43	88	157	62
89	23	62	39	139	105	89	150	77	39	175	42	89	180	77
90	21	110	40	164	36	90	169	62	40	196	96	90	189	96
91	156	95	41	143	103	91	183	102	41	216	118	91	181	79
92	150	84	42	183	116	92	183	110	42	169	103	92	186	102
93	183	92	43	158	102	93	199	90	43	187	106	93	158	47
94	40	106	44	154	102	94	151	110	44	66	42	94	71	68
95	39	56	45	189	117	95	206	92	45	171	117	95	182	87
96	193	47	46	145	77	96	172	105	46	213	8	96	128	43
97	206	118	47	194	106	97	201	62	47	147	117	97	159	50
98	178	68	48	208	74	98	164	106	48	191	43	98	159	84
99	207	116	49	139	50	99	204	56	49	131	103	99	183	90
0	148	78	50	154	90	0	219	8	50	60	90	0	199	118

TABLE 7. Switching classes $\mathcal{S}_{8,1000+i}$ $(1 \leqslant i \leqslant 242)$

$1 \leqslant i \leqslant 50$			$51 \leqslant i \leqslant 100$			$101 \leqslant i \leqslant 150$			$151 \leqslant i \leqslant 200$			$201 \leqslant i \leqslant 242$		
i'	k	l	i'	k	l	i'	k	l	i'	k	l	i'	k	l
1	175	84	51	71	56	1	224	118	51	213	110	1	191	105
2	30	102	52	212	36	2	143	105	52	206	43	2	101	90
3	61	95	53	85	103	3	182	79	53	58	90	3	232	103
4	133	95	54	149	105	4	227	116	54	153	110	4	221	105
5	127	36	55	205	79	5	226	74	55	218	87	5	226	95
6	57	77	56	209	90	6	224	90	56	185	103	6	221	95
7	167	95	57	199	79	7	196	68	57	225	92	7	218	108
8	202	68	58	208	77	8	180	43	58	94	62	8	200	50
9	211	118	59	174	110	9	90	90	59	172	43	9	197	105
10	31	56	60	175	43	10	188	106	60	193	43	10	226	62
11	71	90	61	196	117	11	184	47	61	77	87	11	198	42
12	43	95	62	207	78	12	206	102	62	184	84	12	96	108
13	197	95	63	209	105	13	205	43	63	71	47	13	232	62
14	221	8	64	217	79	14	193	110	64	194	110	14	103	43
15	201	92	65	160	43	15	211	103	65	185	50	15	82	108
16	179	50	66	204	68	16	199	84	66	89	90	16	219	110
17	148	105	67	187	43	17	219	68	67	197	108	17	229	95
18	146	95	68	202	62	18	226	36	68	97	68	18	212	106
19	65	96	69	215	118	19	205	84	69	69	47	19	205	50
20	44	84	70	227	106	20	67	90	70	85	84	20	230	110
21	226	8	71	194	79	21	230	8	71	216	62	21	232	79
22	87	103	72	202	90	22	178	110	72	199	103	22	105	47
23	84	77	73	218	47	23	232	118	73	222	90	23	229	106
24	149	36	74	182	106	24	229	77	74	227	77	24	104	62
25	210	96	75	228	118	25	66	92	75	103	42	25	225	105
26	161	36	76	175	36	26	173	110	76	197	47	26	226	50
27	78	62	77	87	117	27	93	42	77	218	36	27	214	110
28	79	92	78	199	95	28	210	95	78	216	79	28	227	42
29	182	36	79	178	102	29	69	90	79	196	105	29	218	110
30	201	77	80	217	74	30	84	62	80	100	74	30	97	43
31	162	106	81	51	90	31	200	90	81	233	8	31	89	43
32	153	105	82	176	103	32	199	36	82	208	50	32	227	108
33	222	105	83	209	103	33	211	79	83	64	36	33	233	108
34	159	95	84	217	62	34	67	74	84	212	105	34	231	116
35	176	42	85	223	90	35	225	84	85	97	108	35	232	84
36	206	42	86	163	78	36	216	90	86	205	110	36	226	43
37	155	103	87	52	36	37	77	108	87	227	103	37	229	43
38	217	68	88	201	90	38	205	77	88	216	105	38	110	62
39	207	103	89	223	47	39	186	84	89	101	42	39	107	108
40	226	92	90	221	92	40	173	43	90	223	95	40	233	106
41	201	47	91	194	103	41	50	90	91	217	105	41	109	108
42	210	84	92	148	95	42	49	36	92	226	90	42	233	105
43	212	116	93	198	74	43	213	68	93	224	36			
44	223	117	94	226	117	44	200	78	94	219	36			
45	219	92	95	181	36	45	63	47	95	227	47			
46	174	108	96	48	90	46	95	62	96	225	90			
47	169	79	97	32	110	47	146	103	97	222	62			
48	47	103	98	178	77	48	201	103	98	96	62			
49	42	47	99	147	103	49	83	108	99	83	110			
50	211	105	0	50	50	50	209	36	0	221	102			

Complex Hadamard matrices and 3-class association schemes

Akihiro Munemasa

(joint work with Takuya Ikuta)

June 26, 2013

The 30th Algebraic Combinatorics Symposium

Shizuoka University

A *(real) Hadamard* matrix of order n is an $n \times n$ matrix H with entries ± 1, satisfying $HH^\top = nI$. A *complex* Hadamard matrix of order n is an $n \times n$ matrix H with entries in $\{\zeta \in \mathbb{C} \mid |\zeta| = 1\}$, satisfying $HH^* = nI$, where $*$ means the conjugate transpose.

We propose a strategy to construct infinite families of complex Hadamard matrices using association schemes, and demonstrate a successful case. If we consider circulant Hadamard matrices, then

$$H = \begin{bmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \\ & \ddots & \ddots & \ddots \\ a_1 & & & a_0 \end{bmatrix} = \sum_{i=0}^{n-1} a_i A^i, \quad A = \begin{bmatrix} & 1 & & \\ & & 1 & \\ & & & \ddots \\ 1 & & & \end{bmatrix}.$$

Instead of n^2 entries, there are only n entries to determine. This simplifies the search.

Björck–Fröberg [1] classified circulant Hadamard matrices of order $n \leq 8$,

Faugère [4] classified circulant Hadamard matrices of order $n = 9, 10$.

On the other hand, it is conjectured that no circulant real Hadamard matrix of order > 4 exists.

Goethals–Seidel [5] symmetric regular (real) Hadamard matrix necessarily comes from a strongly regular graph (SRG) on $4s^2$ vertices

de la Harpe–Jones [6] SRG n: prime $\equiv 1 \pmod 4$ implies the existence of a symmetric circulant complex Hadamard matrix

Munemasa–Watatani [7] doubly regular tournament (DRT) n: prime $\equiv 3 \pmod 4$ implies the existence of a non-symmetric circulant complex Hadamard matrix

The last two results are of the following form:

$$H = \alpha_0 A_0 + \alpha_1 A_1 + \alpha_2 A_2, \quad A_0 = I$$

$$A_1^\top = A_1,\ A_2^\top = A_2 \quad \text{(G.–J., de la H.–J.)}$$

$$A_1^\top = A_2, \quad \text{(M.–W.)}$$

Unifying principle is: association schemes (strongly regular graphs is a special case).

Godsil–Chan (2010), and Chan (2011) classified complex Hadamard matrices of the form:

$$H = \alpha_0 I + \alpha_1 A_1 + \alpha_2 A_2 \quad \text{(we may assume } \alpha_0 = 1)$$

where $|\alpha_1| = |\alpha_2| = 1$, and

$$A_1 = \text{adjacency matrix of a SRG } \Gamma,$$
$$A_2 = \text{adjacency matrix of } \overline{\Gamma}.$$

also found a complex Hadamard matrix of the form

$$H = I + \alpha_1 A_1 + \alpha_2 A_2 + \alpha_3 A_3$$

of order 15 from the line graph $L(O_3)$ of the Petersen graph O_3.

The Bose–Mesner algebra of a symmetric association scheme of class d

$$\langle A_0, A_1, \ldots, A_d \rangle = \langle E_0, E_1, \ldots, E_d \rangle$$

is a commutative semisimple algebra with primitive idempotents $E_0, E_1, \ldots, E_d$.

$$\sum_{i=0}^{d} A_i = J, \quad \sum_{i=0}^{d} E_i = I, \quad A_0 = I,\ nE_0 = J.$$

$$A_j \circ A_k = \delta_{jk} A_j, \quad E_j E_k = \delta_{jk} E_j$$

$$A_j = \sum_{i=0}^{d} p_{ij} E_i, \quad A_i^{\mathsf{T}} = A_i, \quad p_{ji} \in \mathbb{R}.$$

When is $H = \sum_{i=0}^{d} \alpha_i A_i$ with $|\alpha_i| = 1$ a complex Hadamard matrix?

$$\begin{aligned}
HH^* = nI &\iff (\sum_{i=0}^{d} \alpha_i \sum_{k=0}^{d} p_{ki} E_k)\overline{(\sum_{j=0}^{d} \alpha_j \sum_{k=0}^{d} p_{kj} E_k)} = nI \\
&\iff (\sum_{i=0}^{d} \alpha_i \sum_{k=0}^{d} p_{ki} E_k)(\sum_{j=0}^{d} \overline{\alpha_j} \sum_{k=0}^{d} p_{kj} E_k) = nI \\
&\iff \sum_{k=0}^{d} \sum_{i=0}^{d} \sum_{j=0}^{d} \alpha_i \overline{\alpha_j} p_{ki} p_{kj} E_k = nI \\
&\iff \sum_{k=0}^{d} \sum_{i=0}^{d} \sum_{j=0}^{d} \alpha_i \overline{\alpha_j} p_{ki} p_{kj} E_k = n \sum_{k=0}^{d} E_k \\
&\iff \sum_{i=0}^{d} \sum_{j=0}^{d} \alpha_i \overline{\alpha_j} p_{ki} p_{kj} = n \quad (\forall k) \\
&\iff \sum_{i=0}^{d} \sum_{j=0}^{d} \frac{\alpha_i}{\alpha_j} p_{ki} p_{kj} = n \quad (\forall k) \\
&\iff \sum_{0 \le i < j \le d} \left(\frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i} \right) p_{ki} p_{kj} = n - \sum_{i=0}^{d} p_{ki}^2 \quad (\forall k)
\end{aligned}$$

Consider a system of linear equations

$$\sum_{0 \le i < j \le d} a_{ij} p_{ki} p_{kj} = n - \sum_{i=0}^{d} p_{ki}^2 \quad (\forall k) \tag{1}$$

in

$$a_{ij} = \frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i} \quad (0 \le i < j \le d). \tag{2}$$

Step 1 Solve the system of linear equations (1) in $\{a_{ij}\}$

Step 2 Find $\{\alpha_i\}$ from $\{a_{ij}\}$ by (2).

Problem is: given $\{a_{ij}\}$, when do there exist $\{\alpha_i\}$ satisfying (2)? This can be formulated in terms of a rational mapping defined as follows:

$$\begin{aligned} f : (S^1)^{d+1} &\to \mathbb{R}^{d(d+1)/2}, \\ \{\alpha_i\}_{i=0}^{d} &\mapsto \{\tfrac{\alpha_i}{\alpha_j} + \tfrac{\alpha_j}{\alpha_i}\}_{0 \le i < j < d}. \end{aligned}$$

where $S^1 = \{\zeta \in \mathbb{C} \mid |\zeta| = 1\}$. If we can describe the image of f, then the problem will be solved. Instead of considering $f : (S^1)^{d+1} \to \mathbb{R}^{d(d+1)/2}$, consider

$$\begin{aligned} f : (\mathbb{C}^\times)^{d+1} &\to \mathbb{C}^{d(d+1)/2}, \\ \{\alpha_i\}_{i=0}^{d} &\mapsto \{\tfrac{\alpha_i}{\alpha_j} + \tfrac{\alpha_j}{\alpha_i}\}_{0 \le i < j < d}. \end{aligned}$$

For example, for $d = 2$:

$$\begin{aligned} f : (\mathbb{C}^\times)^3 &\to \mathbb{C}^3, \\ (x, y, z) &\mapsto (\tfrac{x}{y} + \tfrac{y}{x}, \tfrac{x}{z} + \tfrac{z}{x}, \tfrac{y}{z} + \tfrac{z}{y}) \end{aligned}$$

This is not surjective. Indeed, let

$$g(X, Y, Z) = X^2 + Y^2 + Z^2 - XYZ - 4.$$

Then

$$g(\frac{x}{y} + \frac{y}{x}, \frac{x}{z} + \frac{z}{x}, \frac{y}{z} + \frac{z}{y}) = 0$$

Actually, one can prove that the image of f coincides with the zeros of g.

Next consider the case $d = 3$.

$$\begin{aligned} f : (\mathbb{C}^\times)^4 &\to \mathbb{C}^6, \\ (x_0, x_1, x_2, x_3) &\mapsto (\tfrac{x_i}{x_j} + \tfrac{x_j}{x_i})_{0 \le i < j \le 3} \end{aligned}$$

Then

$$g_{i,j,k} = g(\frac{x_i}{x_j} + \frac{x_j}{x_i}, \frac{x_i}{x_k} + \frac{x_k}{x_i}, \frac{x_j}{x_k} + \frac{x_k}{x_j}) = 0$$

One might expect that the image of f coincides with the zeros of $\{g_{i,j,k}\}$. This is not true. We need to define another polynomial

$$\begin{aligned} h = &(X_{03}^2 - 4)X_{12} - X_{03}(X_{01}X_{23} + X_{02}X_{13}) \\ &+ 2(X_{01}X_{02} + X_{13}X_{23}), \end{aligned}$$

where

$$X_{ij} = \frac{x_i}{x_j} + \frac{x_j}{x_i}$$

(and similar polynomials obtained by permuting indices). Then the image of f coincides with the zeros of g, h. The same is true for $\forall m \geq 4$.

Theorem 1. *Let*

$$\begin{aligned} f : (\mathbb{C}^\times)^{d+1} &\to \mathbb{C}^{d(d+1)/2}, \\ (\alpha_0, \alpha_1, \ldots, \alpha_d) &\mapsto (\tfrac{\alpha_i}{\alpha_j} + \tfrac{\alpha_j}{\alpha_i})_{0 \leq i < j \leq d} \end{aligned}$$

The image of f coincides with the set of zeros of the ideal I in the polynomial ring $\mathbb{C}[X_{ij} : 0 \leq i < j \leq d]$ generated by

$$\begin{aligned} &g(X_{ij}, X_{ik}, X_{jk}), \\ &h(X_{ij}, X_{ik}, X_{il}, X_{jk}, X_{jl}, X_{kl}), \end{aligned}$$

where i, j, k, l are distinct, $X_{ij} = X_{ji}$, and

$$\begin{aligned} g &= X^2 + Y^2 + Z^2 - XYZ - 4, \\ h &= (Z^2 - 4)U - Z(XW + YV) + 2(XY + VW). \end{aligned}$$

Given a zero (a_{ij}) of the ideal I, we know that there exists $(\alpha_i) \in (\mathbb{C}^\times)^{d+1}$ such that

$$a_{ij} = \frac{\alpha_i}{\alpha_j} + \frac{\alpha_j}{\alpha_i} \quad (0 \leq i < j \leq d). \tag{3}$$

The next question is: how do we find (α_i), and when does $(\alpha_i) \in (S^1)^{d+1}$ hold?

Observe, for $\alpha \in \mathbb{C}^\times$,

$$|\alpha| = 1 \iff -2 \leq \alpha + \frac{1}{\alpha} \leq 2.$$

So we need $-2 \leq a_{ij} \leq 2$. Moreover, if $a_{ij} \in \{\pm 2\}$ for all i, j, then $\alpha_i = \pm \alpha_j$ so the resulting matrix is a scalar multiple of a real Hadamard matrix (cf. Goethals–Seidel (1970)).

Theorem 2. *Let*

$$\begin{aligned} f : (\mathbb{C}^\times)^{d+1} &\to \mathbb{C}^{d(d+1)/2}, \\ (\alpha_0, \alpha_1, \ldots, \alpha_d) &\mapsto (\tfrac{\alpha_i}{\alpha_j} + \tfrac{\alpha_j}{\alpha_i})_{0 \leq i < j \leq d} \end{aligned}$$

Suppose (a_{ij}) *belongs to the image of* f, $a_{ij} \in \mathbb{R}$, *and there exist* $0 \le i_0 < i_1 \le d$ *such that* $-2 < a_{i_0,i_1} < 2$. *Let* $\alpha_{i_0}, \alpha_{i_1}$ *be complex numbers satisfying*

$$a_{i_0,i_1} = \frac{\alpha_{i_0}}{\alpha_{i_1}} + \frac{\alpha_{i_1}}{\alpha_{i_0}} = \frac{\alpha_{i_0}}{\alpha_{i_1}} + \left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right)^{-1}$$

Define α_i $(0 \le i \le n,\ i \ne i_0, i_1)$ *by*

$$\alpha_i = \frac{\alpha_{i_0}(a_{i_0,i_1}\alpha_{i_1} - 2\alpha_{i_0})}{a_{i_1,i}\alpha_{i_1} - a_{i_0,i}\alpha_{i_0}}.$$

Then $|\alpha_i| = |\alpha_j|$ *and* (3) *holds. Conversely, every* (α_i) *satisfying* (3) *is obtained in this way.*

Using Theorem 2, the strategy of finding a complex Hadamard matrix in a Bose–Mesner algebra is as follows:

Step 1 Solve the system of equations

$$g(X_{ij}, X_{ik}, X_{jk}) = 0,$$
$$h(X_{ij}, X_{ik}, X_{il}, X_{jk}, X_{jl}, X_{kl}) = 0,$$
$$\sum_{0 \le i < j \le d} X_{ij} p_{ki} p_{kj} = n - \sum_{i=0}^{d} p_{ki}^2$$

Step 2 List all solutions a_{ij} with $-2 \le a_{ij} \le 2$.

Step 3 Find (α_i) by

$$\alpha_i = \frac{\alpha_{i_0}(a_{i_0,i_1}\alpha_{i_1} - 2\alpha_{i_0})}{a_{i_1,i}\alpha_{i_1} - a_{i_0,i}\alpha_{i_0}}.$$

where $a_{i_0,i_1} \ne \pm 2$,

$$\frac{\alpha_{i_0}}{\alpha_{i_1}} + \frac{\alpha_{i_1}}{\alpha_{i_0}} = a_{i_0,i_1}.$$

In many known examples of association schemes with $d = 3$, Step 2 failed.

Theorem 3 (Chan [2]). *There are only finitely many antipodal distance-regular graphs of diameter* 3 *whose Bose–Mesner algebra contains a complex Hadamard matrix.*

But Chan did find an example, $L(O_3)$: the line graph of the Petersen graph. This graph belongs to an infinite family described below.

- q: a power of 2, $q \geq 4$,
- $\Omega = \mathrm{PG}(2, q)$: the projective plane over $\mathbb{F}_q$,
- $Q = \{[a_0, a_1, a_2] \in \Omega \mid a_0^2 + a_1 a_2 = 0\}$: quadric,
- $X = \{[a_0, a_1, a_2] \in \Omega \setminus Q \mid [a_0, a_1, a_2] \neq [1, 0, 0]\}$,
- $|X| = q^2 - 1$.

For $x, y \in X$, denote by $x + y$ the line through x, y. Define

$$(A_i)_{xy} = \begin{cases} 1 & \text{if } i = 0,\ x = y, \\ 1 & \text{if } i = 1,\ |(x+y) \cap Q| = 2, \\ 1 & \text{if } i = 2,\ |(x+y) \cap Q| = 0, \\ 1 & \text{if } i = 3,\ |(x+y) \cap Q| = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Then the matrices $A_0, \ldots, A_3$ generate a Bose–Mesner algebra of a commutative association scheme, and there exists a complex Hadamard matrix in this Bose–Mesner algebra.

Theorem 4. *The matrix $H = I + \alpha_1 A_1 + \alpha_2 A_2 + \alpha_3 A_3$ is a complex Hadamard matrix if and only if*

(i) *H belongs to the subalgebra forming the Bose–Mesner algebra of a strongly regular graph (precise description omitted, already done by Chan–Godsil [3]),*

(ii)
$$\alpha_1 + \frac{1}{\alpha_1} = -\frac{2}{q}, \quad \alpha_2 = \frac{1}{\alpha_1}, \quad \alpha_3 = 1,$$

(iii)
$$\alpha_1 + \frac{1}{\alpha_1} = \frac{(q-1)(q-2) - (q+2)r}{q},$$

where $r = \sqrt{(q-1)(17q-1)}$.

The case (ii) with $q = 4$ was found by Chan [2].

References

[1] G. Björck and R. Fröberg, A faster way to count the solutions of inhomogeneous systems of algebraic equations, with applications to cyclic n-roots, J. Symb. Comp., 12 (1991), 329–336.

[2] A. Chan, Complex Hadamard matrices and strongly regular graphs, preprint `arXiv:1102.5601v1`.

[3] A. Chan and C.D. Godsil, Type-II matrices and combinatorial structures, Combinatorica 30 (1) (2010), 1–24.

[4] J.-C. Faugère, Finding all the solutions of Cyclic 9 using Gröbner basis techniques, Computer Mathematics (Matsuyama, 2001), Lecture Notes Ser. Comput., 9, World Sci. Publ., 2001, pp.1–12.

[5] J.-M. Goethals and J.J. Seidel, Strongly regular graphs derived from combinatorial designs, Canad. J. Math. 22 (1970) 597–614.

[6] P. de la Harpe and V. Jones, Paires de sous-algèbres semi-simples et graphes fortement réguliers, C. R. Acad. Sci. Paris Sér. I Math. 311 (1990), no. 3, 147–150.

[7] A. Munemasa and Y. Watatani, Paires orthogonales de sous-algèbres involutives, C. R. Acad. Sci. Paris Sér. I Math. 314 (1992), no. 5, 329–331.

EQUIANGULAR LINES AND SEIDEL MATRICES WITH THREE EIGENVALUES I

FERENC SZÖLLŐSI

ABSTRACT. We discuss some preliminary results on equiangular lines in $\mathbb{R}^d$ whose Seidel matrix has three different eigenvalues.

2010 Mathematics Subject Classification. Primary 05B20, secondary 05B40.
Keywords and phrases. *Equiangular lines, Seidel matrix, Switching, Two-graph*

1. INTRODUCTION AND MAIN RESULTS

This paper is based on a talk given at Shizuoka university, and describes some preliminary results from a forthcoming paper jointly with Gary Greaves and Akihiro Munemasa [1].

A set of $n \geq 1$ lines, represented by the unit vectors $v_1, \ldots, v_n \in \mathbb{R}^d$, is called equiangular if there exists a constant $\alpha > 0$ for which $|\langle v_i, v_j \rangle| = \pm\alpha$ holds for every $1 \leq i < j \leq n$. Such lines arise in many applications [2]. The main question we are concerned with is the determination of the maximal number of equiangular lines in a given dimension d. For the state of the art of this question see [3]. The Gram matrix of the equiangular line system $[G]_{i,j} := \langle v_i, v_j \rangle$, $1 \leq i, j \leq n$, is of fundamental interest, since it contains all the relevant information and thus study of equiangular lines via matrix theoretical and linear algebraic tools is possible. It is, however, more convenient to consider the *Seidel matrix* $S := (G - I)/\alpha$ instead, which is a symmetric matrix with zero diagonal and ± 1 entries otherwise. The algebraic multiplicity of the smallest eigenvalue λ_0 of S describes the smallest possible dimension d where the line system fits in with common angle $\alpha = -1/\lambda_0$. Seidel matrices are the central objects of this work. We remark here that there is an ambient graph $\Gamma(S)$ associated with each Seidel matrix, whose adjacency matrix A can be obtained from the formula $A := (J - S - I)/2$.

One of the fundamental results in the area is the following conditional upper bound.

Proposition 1.1 (The relative bound, [4]). *Assume that there exist n equiangular lines in $\mathbb{R}^d$ with common angle $\alpha \leq 1/\sqrt{d+2}$. Then*

$$n \leq \frac{d(1-\alpha^2)}{1-d\alpha^2},$$

and equality holds if and only if the corresponding Seidel matrix has two distinct eigenvalues.

There are a number of interesting strongly regular graphs corresponding to the equality case above, e.g. the Petersen graph on 10 vertices in $\mathbb{R}^5$. However, when the bound is not an integer number, it is unclear what is the "best" combinatorial object providing the largest number of equiangular lines. Therefore we seek for a relaxed concept, and begin to investigate Seidel matrices with three different eigenvalues. This concept is non vacuous.

Date: October 8, 2013.
Contribution to the 30th Algebraic Combinatorics Symposium, Shizuoka University.

Lemma 1.2. *There exists mn equiangular lines in $\mathbb{R}^{mn-m+1}$ with common angle $\alpha = 1/(2n-1)$ for every $m, n \geq 2$. Moreover we can assume that the corresponding Seidel matrix has spectrum $\{[1-2n]^{m-1}, [1]^{m(n-1)}, [n(m-2)+1]^1\}$.*

Proof. It is easy to see, by using properties of the Kronecker product, that the $mn \times mn$ matrix $S := J_n \otimes (J_m - 2I_m) + I_{mn}$ has the desired spectrum. Under the assumptions on m and n its smallest eigenvalue is $1-2n$, hence the result follows. □

The Paley matrices of prime orders $p \equiv 1 \pmod 4$ form another series of examples with spectrum $\{[-\sqrt{p}]^{(p-1)/2}, [0]^1, [\sqrt{p}]^{(p-1)/2}\}$. We have the following result characterizing Seidel matrices with three distinct eigenvalues.

Theorem 1.3. *Let $d \geq 1$ and let S be a Seidel matrix of order $n \geq 2$ with smallest eigenvalue λ_0 with multiplicity $n - d \geq 1$. Assume that it has another eigenvalue μ with multiplicity $1 \leq m \leq d$. Then*

$$\left|\mu + \frac{\lambda_0(n-d)}{d}\right| \leq \frac{\sqrt{n(d(n-1) - \lambda_0^2(n-d))}}{d} \cdot \sqrt{\frac{d-m}{m}}. \tag{1}$$

Equality holds if and only if S has at most three distinct eigenvalues.

The proof is standard, and follows the spectral analysis of [4].

Proof. First note that the right hand side is well-defined by [4, Lemma 6.1]. Let us denote the remaining eigenvalues of S by $\lambda_1, \lambda_2, \ldots, \lambda_{d-m}$, respectively. Then, by using that $\mathrm{Tr}S = 0$ and $\mathrm{Tr}S^2 = n(n-1)$ we find, after an application of the Cauchy–Schwartz inequality, that

$$((n-d)\lambda_0 + m\mu)^2 = \left(\sum_{i=1}^{d-m} \lambda_i\right)^2 \leq (d-m)\sum_{i=1}^{d-m} \lambda_i^2 = (d-m)\left(n(n-1) - (n-d)\lambda_0^2 - m\mu^2\right).$$

The result follows after some algebraic manipulations. □

Theorem 1.3 can be used to tabulate feasible parameter sets of Seidel matrices with 3 different eigenvalues. Some of these are highlighted in Appendix A. The main result is the following connection between Seidel matrices with two and three eigenvalues.

Theorem 1.4. *Let S be a Seidel matrix of order $n \geq 2$ with two eigenvalues $\{[\lambda_0]^{n-d}, [\lambda_1]^d\}$ with $\lambda_1 \leq \min\{d-1, n-d-1\}$ and assume that it admits the block partition*

$$S = \begin{bmatrix} J_{\lambda_1+1} - I_{\lambda_1+1} & * \\ * & S' \end{bmatrix}.$$

Then the spectrum of S' is $\{[\lambda_0]^{n-d-\lambda_1}, [\lambda_1]^{d-\lambda_1-1}, [\lambda_0+\lambda_1+1]^{\lambda_1}\}$.

Proof. See [1]. □

We have the following interesting consequence.

Remark 1.5. One can see the following by the repeated application of Theorem 1.4. Assume that there exists a Seidel matrix of order 96 with spectrum $\{[-5]^{76}, [19]^{20}\}$ containing a $J_{20} - I_{20}$ principal minor. Then, there exists a Seidel matrix of order 76 with spectrum $\{[-5]^{57}, [15]^{19}\}$. If, in addition, this latter contains a $J_{16} - I_{16}$ principal minor, then there further exists a Seidel matrix of order 60 with spectrum $\{[-5]^{42}, [11]^{15}, [15]^3\}$.

The examples, described in Remark 1.5 would correspond to 96, 76 and 60 equiangular lines in $\mathbb{R}^{20}, \mathbb{R}^{19}$ and in $\mathbb{R}^{18}$, respectively improving upon earlier constructions. We suspect that most of the indicated cases, as well as those in Appendix A are in fact nonexistent, but hopefully the others will lead to some new and exciting examples of equiangular lines.

Acknowledgments

This work was supported by the Hungarian National Research Fund OTKA K-77748 and by the JSPS KAKENHI Grant Number 24 · 02807.

References

[1] G. Greaves, A. Munemasa and F. Szöllősi: Equiangular lines in real Euclidean spaces, in preparation (2013).
[2] R. B. Holmes, V. I. Paulsen: Optimal frames for erasures, *Linear Algebra Appl.*, **377**, 31-51 (2004).
[3] P. W. H. Lemmens, J. J. Seidel: Equiangular lines, *J. Algebra*, **24**, 494-512 (1973).
[4] J. H. van Lint, J. J. Seidel: Equilateral point sets in elliptic geometry, *Indag. Math.*, **28**, 335–348 (1966).
[5] E. Spence: The strongly regular $(40, 12, 2, 4)$ graphs, *Electron. J. Combin.*, **7**, #22, 4 pp. (electronic) (2000).
[6] D. E. Taylor: Some topics in the theory of finite groups, PhD thesis, University of Oxford (1972).
[7] J. C. Tremain: Concrete constructions of equiangular line sets, *arXiv:0811.2779 [math.MG]*, (2008).

Appendix A. A supplementary table

Here we display a list of feasible spectrum of Seidel matrices whose existence might reach, or improve upon the maximum number of equiangular lines in dimensions 14, 16-20.

n	d	λ	μ	ν	Exist?	Remark
28	14	$[-5]^{14}$	$[3]^{7}$	$[7]^{7}$	Y	[7]
30	14	$[-5]^{16}$	$[5]^{9}$	$[7]^{5}$	?	
40	16	$[-5]^{24}$	$[5]^{6}$	$[9]^{10}$	?	
40	16	$[-5]^{24}$	$[7]^{15}$	$[15]^{1}$	Y	[5]
42	16	$[-5]^{26}$	$[7]^{7}$	$[9]^{9}$	?	
48	17	$[-5]^{31}$	$[7]^{8}$	$[11]^{9}$	Y	[3]
49	17	$[-5]^{32}$	$[9]^{16}$	$[16]^{1}$	?	
48	18	$[-5]^{30}$	$[3]^{6}$	$[11]^{12}$	?	
48	18	$[-5]^{30}$	$[7]^{16}$	$[19]^{2}$	?	
54	18	$[-5]^{36}$	$[7]^{9}$	$[13]^{9}$	?	
60	18	$[-5]^{42}$	$[11]^{15}$	$[15]^{3}$	?	Remark 1.5
72	19	$[-5]^{53}$	$[13]^{16}$	$[19]^{3}$	Y	[6]
75	19	$[-5]^{56}$	$[10]^{1}$	$[15]^{18}$	?	
90	20	$[-5]^{70}$	$[13]^{5}$	$[19]^{15}$	?	
95	20	$[-5]^{75}$	$[14]^{1}$	$[19]^{19}$	?	

Table 1. Feasible parameter sets of Seidel matrices with 3 distinct eigenvalues.

F. Sz.: Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan
E-mail address: szoferi@gmail.com

Hoffman graphs and edge-signed graphs

谷口 哲至 (松江工業高等専門学校)

1 はじめに

ラングラフの最小固有値が -2 以上であることは良く知られている。これにより、最小固有値によるグラフの階層構造を知ろうという問題が自然と生じるのだが、(良く知られている) ラングラフの構成法では最小固有値が -2 よりも小さいグラフを構成する事はできない。そこで R. Woo と A. Neumaier [6] は、グラフの「辺」を「点」で置き換えるという単純な作業であるラングラフの構成法を高度に一般化し、最小固有値が -2 よりも小さいグラフの構成法を定式化した。[6] では、最小固有値 $-1-\sqrt{2}$ 以上のグラフが分類されている。それには (9 種類の) ホフマングラフと呼ばれる特別なグラフ達の和の概念が用いられており、そこにホフマングラフの既約性と共にルート系との関わりも生じる。これこそ最小固有値によるグラフの階層構造を解明する道であり、更に階層を降りる為にもっと多くのホフマングラフを知る必要がある。

現在目標としているのは、最小固有値が -3 以上のグラフの分類である。しかしながら、この様なグラフはあまりにも多くあり、途方に暮れるばかりである。そこで、まずはその様なホフマングラフの分類を行う事にする。ここで、スペシャルグラフを導入する事により、ホフマングラフの分類をより簡易なものにする事ができる。スペシャルグラフと辺符号グラフ (edge-signed graph) には密接な関係がある。今回、最小固有値が -2 より大きい辺符号グラフの分類を与え、ホフマングラフとの関係を示す。

これらのことについて、宗政昭弘氏[1]、J. Koolen 氏[2]、佐野良夫氏[3]、G. Greaves 氏[1]らと共同で進めている。

2 辺符号グラフ (edge-signed graph)

定義 2.1. グラフ S と写像 $\mathrm{sgn} : E(S) \to \{+,-\}$ のペア (S,sgn) を辺符号グラフ *(edge-signed graph)* とよぶ。辺符号グラフ $\mathcal{S} = (S,\mathrm{sgn})$ に対し、$V(\mathcal{S}) := V(S)$, $E^+(\mathcal{S}) := \mathrm{sgn}^{-1}(+)$, $E^-(\mathcal{S}) := \mathrm{sgn}^{-1}(-)$ とする。$E^+(\mathcal{S})$ $(E^-(\mathcal{S}))$ の要素を $\mathcal{S}$ の $(+)$-*edge* $((-)$-*edge*$)$ と呼ぶ。また、辺符号グラフ $\mathcal{S}$ を $(V(\mathcal{S}), E^+(\mathcal{S}), E^-(\mathcal{S}))$ で表す。

[1]東北大学大学院 情報科学研究科
[2]中国科学技術大学/浦項工科大学
[3]筑波大学 システム情報系

辺符号グラフ $S' = (S', \mathrm{sgn}')$ において、グラフ S' が S の誘導部分グラフで、S' の任意の辺 e で $\mathrm{sgn}(e) = \mathrm{sgn}'(e)$ が成り立つなら、S' を $S = (S, \mathrm{sgn})$ の**誘導辺符号部分グラフ** *(induced edge-signed subgraph)* と呼ぶ。

全単射 $\phi : V(S) \to V(S')$ が存在して、

(i) $\{u, v\} \in E^+(S) \iff \{\phi(u), \phi(v)\} \in E^+(S')$

(ii) $\{u, v\} \in E^-(S) \iff \{\phi(u), \phi(v)\} \in E^-(S')$

の両方が成立するなら、二つの辺符号グラフ S、S' は同型であるという。

グラフ $(V(S), E^+(S) \cup E^-(S))$ が連結（非連結）であるとき辺符号グラフ S は連結（非連結）であるという。

定義 2.2. 辺符号グラフ S に対し、その隣接行列 $A(S)$ を次で定義する：

$$(A(S))_{uv} = \begin{cases} 1 & \text{if } \{u, v\} \in E^+(S), \\ -1 & \text{if } \{u, v\} \in E^-(S), \\ 0 & \text{otherwise.} \end{cases}$$

固有値：

$$\lambda_{\max}(A(S)) = \lambda_1(A(S)) \geq \lambda_2(A(S)) \geq \cdots \geq \lambda_n(A(S)) = \lambda_{\min}(A(S))$$

を $\lambda_{\max}(S)$、$\lambda_i(S)$、$\lambda_{\min}(S)$ で表す。但し $n = |V(S)|$ とする。

頂点 v のスイッチングとは、v と接続するすべての辺の符号を入れ替える操作である。ある G の頂点集合 $V(G)$ の部分集合 W が存在して、W の各頂点でスイッチングをしたグラフが G' と同型になる時、二つの辺符号グラフ G と G' がスイッチング同値であるという。スイッチング同値なグラフ同士は同じ固有値を持つ。

総ての辺の符号が $+$ の場合で、辺符号グラフを通常のグラフとみなす。通常のグラフのうち、E-型についての先行研究では、以下の結果がよく知られている：

定理 2.3 ([1, 2]). *Let G be a connected exceptional graph having smallest eigenvalue greater than -2. Then G is one of*

(i) 20 *graphs on* 6 *vertices;*

(ii) 110 *graphs on* 7 *vertices;*

(iii) 443 *graphs on* 8 *vertices.*

定理 2.3 を辺符号グラフに拡張すると以下のようになる：

定理 2.4 ([3]). *Let G be a connected exceptional edge-signed graph having smallest eigenvalue greater than -2. Then G is one of*

(i) 32 *edge-signed graphs on* 6 *vertices;*

(ii) 233 *edge-signed graphs on* 7 *vertices;*

(iii) 1242 *edge-signed graphs on* 8 *vertices.*

E-型でないとき、以下の定理を得る：

定理 2.5 ([3]). *Let G be a connected integrally represented edge-signed graph having smallest eigenvalue greater than -2. Let H be the representation graph of G for some integral representation. Then one of the following statements holds:*

(i) H is a simple tree or H is unicyclic with an odd cycle, and G is switching equivalent to the line graph $\mathfrak{L}(H)$,

(ii) H is unicyclic with an even cycle C, and G is switching equivalent to the edge-signed graph (V, E^+, E^-), where $V = V(\mathfrak{L}(H))$,

$$E^- = \{uv \in E(\mathfrak{L}(H)) \mid v \in \mathfrak{C}_G(uu')\}$$

where uu' is an edge of $\mathfrak{L}(C)$, and $E^+ = E(\mathfrak{L}(H))\backslash E^-$.

(iii) H is a tree with a double edge, and G is switching equivalent to the edge-signed graph obtained from the line graph $\mathfrak{L}(H)$, by attaching a new vertex u', and join u' by $(+)$-edges to every vertex of a clique in the neighbourhood of u, $(-)$-edges to every vertex of the other clique in the neighbourhood of u, where u is a fixed vertex of $\mathfrak{L}(H)$.

Conversely, if G is an edge-signed graph described by (i), (ii), *or* (iii) *above, then G is integrally represented and has smallest eigenvalue greater than -2.*

※ integrally represented とは、例外型ルート格子を張らないときのこと。これらは今回の主結果である。

3 ホフマングラフ (Hoffman graph)

定義 3.1. 条件 (i)、(ii) を満たすグラフ $H = (V, E)$ とラベリング $\mu : V \to \{f, s\}$ とのペア $\mathfrak{H} = (H, \mu)$ を**ホフマングラフ**という:

(i) ラベル f の総ての頂点は、少なくとも一つラベル s の頂点と隣接する;

(ii) ラベルが f の頂点は互いに非隣接である。

ラベル s の頂点を **slim 頂点**と呼び、それらから成る $\mathfrak{H}$ の頂点集合を $V^s(\mathfrak{H})$ で表す。また、ラベル f の頂点を **fat 頂点**と呼び、それらから成る $\mathfrak{H}$ の頂点集合を $V^f(\mathfrak{H})$ で表す。また、どの slim 頂点も、ある fat 頂点と隣接するとき、$\mathfrak{H}$ を fat-ホフマングラフと呼ぶ。更に、ホフマングラフの固有値を次で与える [6]:

定義 3.2. A を次の様なホフマングラフ $\mathfrak{H}$ の隣接行列とする:

$$A = \begin{pmatrix} A_s & C \\ C^T & O \end{pmatrix}$$

但し、A_s は slim 頂点の隣接関係を表し、C は slim 頂点と fat 頂点の隣接関係を表す。ここで、実対称行列 $B(\mathfrak{H}) = A_s - CC^T$ の固有値を $\mathfrak{H}$ の固有値と呼ぶ。

定理 3.3 (Hoffman [4]). $\mathfrak{H}$ をホフマングラフとする。更に Γ^n を、各 *fat* 頂点 f を *slim n-clique* $K(f)$ で置き換え、f の総ての隣接点と $K(f)$ の総ての頂点を互いに辺で結ぶことで $\mathfrak{H}$ から得られるグラフとする。このとき、以下二式が成り立つ:

$$\lambda_{\min}(\Gamma^n) \geq \lambda_{\min}(\mathfrak{H}) \tag{1}$$

$$\lim_{n\to\infty} \lambda_{\min}(\Gamma^n) = \lambda_{\min}(\mathfrak{H}) \tag{2}$$

特に、任意の $\epsilon > 0$ に対し、Γ^n を誘導部分グラフとして含む総ての *slim* グラフ Δ が

$$\lambda_{\min}(\Delta) \leq \lambda_{\min}(\mathfrak{H}) + \epsilon.$$

を満たすように、自然数 n をとれる。

定理 3.3 から、ホフマングラフとはグラフの最小固有値における極限構造であり、Woo 氏、Neumaier 氏 [6] らは上手く導入したと言えよう。

3.1 ホフマングラフの表現

グラフの最小固有値を考える時に、よく知られた構造（ルート格子等）上で議論を展開する為に、Woo 氏、Neumaier 氏 [6] らはホフマングラフの表現を導入した。これに少し手を加え、以下の新しい表現を導入する。

定義 3.4. ホフマングラフ $\mathfrak{H}$ と正の整数 n に対し、以下を満たす写像 $\phi : V^s(\mathfrak{H}) \to \mathbf{R}^n$ をノルム m の被約表現と呼ぶ:

$$(\psi(x), \psi(y)) = \begin{cases} m - |N^f_{\mathfrak{H}}(x)| & \text{if } x = y; \\ 1 - |N^f_{\mathfrak{H}}(x,y)| & \text{if } \{x,y\} \in E(\mathfrak{H}); \\ -|N^f_{\mathfrak{H}}(x,y)| & \text{その他.} \end{cases}$$

但し、$N^f_{\mathfrak{H}}(x)$ は x と隣接する fat 頂点の集合を表し、$N^f_{\mathfrak{H}}(x,y)$ は x, y の両方に隣接する fat 頂点の集合を表す。更に、$\{\psi(x) \mid x \in V_s(\mathfrak{H})\}$ で生成される格子を $\Lambda^{\mathrm{red}}(\mathfrak{H}, m)$ で表す。

これで最小固有値が -2 を下回った時にも、ルート格子の理論を用いる事が出来るようになった。

3.2 ホフマングラフの和

定義 3.5. $\mathfrak{H}$ をホフマングラフとし、$\mathfrak{H}^1$、$\mathfrak{H}^2(\neq \emptyset)$ を $\mathfrak{H}$ の二つの誘導部分グラフとする。以下の条件を満たすとき、$\mathfrak{H}$ は $\mathfrak{H}^1$ と $\mathfrak{H}^2$ の和であると言い、$\mathfrak{H} = \mathfrak{H}^1 \uplus \mathfrak{H}^2$ で書き表す:

(i) $V(\mathfrak{H}) = V(\mathfrak{H}^1) \cup V(\mathfrak{H}^2)$;

(ii) $V^s(\mathfrak{H}) = V^s(\mathfrak{H}^1) \cup V^s(\mathfrak{H}^2)$,
$V^s(\mathfrak{H}^1) \cap V^s(\mathfrak{H}^2) = \emptyset$;

(iii) $x \in V^s(\mathfrak{H}^i)$, $y \in V^f(\mathfrak{H})$, $\{x, y\} \in E(\mathfrak{H}) \Longrightarrow y \in V^f(\mathfrak{H}^i)$;

(iv) $x \in V^s(\mathfrak{H}^1)$, $y \in V^s(\mathfrak{H}^2) \Longrightarrow |N^f_{\mathfrak{H}}(x, y)| \leq 1 \wedge (|N^f_{\mathfrak{H}}(x, y)| = 1 \Longleftrightarrow \{x, y\} \in E(\mathfrak{H}))$.

$\mathfrak{H}$ がホフマングラフ $\mathfrak{H}^1$、$\mathfrak{H}^2(\neq \emptyset)$ で $\mathfrak{H} = \mathfrak{H}^1 \uplus \mathfrak{H}^2$ と表されるなら、$\mathfrak{H}$ は分解可能であるという。非連結なホフマングラフは明らかに分解可能である。

これより、ホフマングラフの既約性の概念が生じる。これまでに得た成果の 1 つを紹介する。

定理 3.6 ([5]). $\mathfrak{H}$ を分解出来ない *fat*-ホフマングラフで、$V^s = V^s(\mathfrak{H})$、最小固有値が -3 以上とする。このとき、総ての *slim* 頂点は高々3 個の *fat* と隣接する。更に、以下の主張が成立する:

(i) $\exists x \in V^s\ (|N^f_{\mathfrak{H}}(x)| = 3) \Longrightarrow \mathfrak{H} \cong \mathfrak{H}^{(3)}$

(ii) $\forall x \in V^s\ (|N^f_{\mathfrak{H}}(x)| \leq 2) \wedge \exists x \in V^s\ (|N^f_{\mathfrak{H}}(x)| = 2) \Longrightarrow \exists n \geq 0$ $(\Lambda^{\mathrm{red}}(\mathfrak{H}, 3) \simeq \mathbb{Z}^n)$

(iii) $\forall x \in V^s\ (|N^f_{\mathfrak{H}}(x)| = 1) \Longrightarrow \Lambda^{\mathrm{red}}(\mathfrak{H}, 3)$: 既約ルート格子.

但し、$\mathfrak{H}^{(3)}$ は *slim* 頂点が 1 つで、3 つの *fat* 頂点をその隣接点に持つホフマングラフである。

3.3 ホフマングラフのスペシャルグラフ

定義 3.7. ホフマングラフ $\mathfrak{H}$ のスペシャルグラフとは、以下を満たす辺符号グラフ $\mathcal{S}(\mathfrak{H}) := (V(\mathcal{S}(\mathfrak{H})), E^+(\mathcal{S}(\mathfrak{H})), E^-(\mathcal{S}(\mathfrak{H})))$ のことである:

$V(\mathcal{S}(\mathfrak{H})) := V^s(\mathfrak{H})$,
$E^+(\mathcal{S}(\mathfrak{H})) := \{\{u, v\} \mid u, v \in V^s(\mathfrak{H}), u \neq v, \{u, v\} \in E(\mathfrak{H}), N^f_{\mathfrak{H}}(u) \cap N^f_{\mathfrak{H}}(v) = \emptyset\}$,
$E^-(\mathcal{S}(\mathfrak{H})) := \{\{u, v\} \mid u, v \in V^s(\mathfrak{H}), u \neq v, \{u, v\} \notin E(\mathfrak{H}), N^f_{\mathfrak{H}}(u) \cap N^f_{\mathfrak{H}}(v) \neq \emptyset\}$.

補題 3.8 ([5, Lemma 3.4]). ホフマングラフ $\mathfrak{H}$ が分解できない事は、そのスペシャルグラフ $\mathcal{S}(\mathfrak{H})$ が連結である為の必要かつ十分条件である。

補題 3.9. $\mathcal{S}'$ が辺符号グラフ $\mathcal{S}$ の誘導辺符号部分グラフなら、$\lambda_{\min}(\mathcal{S}') \geq \lambda_{\min}(\mathcal{S})$ である。

補題 3.10. *fat* ホフマングラフ $\mathcal{G}$ が -3 より大きい最小固有値をもつなら、$\lambda_{\min}(\mathcal{S}(\mathcal{G})) \geq \lambda_{\min}(\mathcal{G}) + 1$ が成り立つ。

以下は、最小固有値が -3 より大きい時の、分類ているである：

定理 3.11. *fat* ホフマングラフ $\mathcal{G}$ において、どの *slim* 頂点も丁度 1 つの *fat* 頂点と隣接するものとする。このとき、$\mathcal{G}$ の最小固有値が -3 より大きい事は、$\mathcal{S}(\mathcal{G})$ が *Theorem 2.5* 又は *Theorem 2.4* の中の辺符号グラフの一つとスイッチング同値である為の必要かつ十分条件である。

4 最後に

現在、定理 3.6 の分類を元に、最小固有値が -3 より大きなグラフの特徴付けを与える研究を行っており、(ii) について成果を得ている（未出版）。(iii) については、未だ結果は得ていないが進行中である。最小固有値が -3 に等しい時は、その特徴付けは難しいと考えられているが、ホフマングラフと関係の深い辺符号グラフの分類から、何か得られないか模索中である。

参考文献

[1] F.C. Bussemaker and A. Neumaier. *Exceptional graphs with smallest eigenvalue -2 and related problems*, Math. Comp. 59(200) (1992), 583–608.

[2] M. Doob and D. Cvetković. *On spectral characterizations and embeddings of graphs*, Linear Algebra Appl. 27 (1979), 17–26.

[3] G. Greaves, J. Koolen, A. Munemasa, Y. Sano and T. Taniguchi, *graphs with smallest eigenvalue greater than -2*, in preparation.

[4] A. J. Hoffman, *On graphs whose least eigenvalue exceeds $-1-\sqrt{2}$*, Linear Algebra Appl. 16 (1977), 153–165.

[5] H. J. Jang, J. Koolen, A. Munemasa and T. Taniguchi, *On fat Hoffman graphs with smallest eigenvalue at least -3*, Ars Mathematica Contemporanea, 7:105–121, 2014.

[6] R. Woo and A. Neumaier, *On graphs whose smallest eigenvalue is at least $-1-\sqrt{2}$*, Linear Algebra Appl. 226-228 (1995), 577–591.

A cross-intersection theorem for vector spaces based on semidefinite programming

須田 庄
愛知教育大学 数学教育講座
suda@auecc.aichi-edu.ac.jp

田中 太初
東北大学 大学院情報科学研究科
純粋・応用数学研究センター
htanaka@m.tohoku.ac.jp

V を有限体 $\mathbb{F}_q$ 上の n 次元ベクトル空間とする。また、Ω をその部分空間全体の集合とし、特に k 次元部分空間全体の集合を Ω_k で表す ($k=0,\dots,n$)。二つの部分空間族 $\mathscr{F}\subseteq\Omega_k, \mathscr{G}\subseteq\Omega_\ell$ が **cross-intersecting** であるとは、任意の $x\in\mathscr{F}, y\in\mathscr{G}$ について $x\cap y\neq 0$ が成り立つこととする。本稿の主結果は次の定理である：

Theorem 1. *Let $\mathscr{F}\subseteq\Omega_k$ and $\mathscr{G}\subseteq\Omega_\ell$ be a pair of cross-intersecting families. Suppose that $n\geqslant 2k$ and $n\geqslant 2\ell$. Then*[1]

$$|\mathscr{F}||\mathscr{G}|\leqslant \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}\begin{bmatrix} n-1 \\ \ell-1 \end{bmatrix},$$

and equality holds if and only if either (i) there is $z\in\Omega_1$ such that $\mathscr{F}=\{x\in\Omega_k : z\subseteq x\}$ and $\mathscr{G}=\{x\in\Omega_\ell : z\subseteq x\}$, or (ii) $n=2k=2\ell$ and there is $z\in\Omega_{2k-1}$ such that $\mathscr{F}=\mathscr{G}=\{x\in\Omega_k : x\subseteq z\}$.

この定理は、n 点集合の二つの部分集合族に関する Pyber [10] 及び Matsumoto-Tokushige [8] の結果の q-類似である[2]。彼らの証明は Kruskal-Katona の定理 (cf. [4]) に基づいている。一方、Kruskal-Katona の定理の q-類似については、現時点ではまだ弱い形のものしか得られておらず (cf. [1])、Theorem 1 を証明するには十分ではない (と思われる)。Theorem 1 は Erdős-Ko-Rado の定理 [3] の q-類似の拡張でもある。Erdős-Ko-Rado の定理やその q-類似は、Delsarte [2] の**線形計画限界**を応用することによって初めて完全な形で証明された (cf. [16, 13, 14])。線形計画限界は、グラフの Shannon 容量に関する Lovász の ϑ-限界と密接に関係しているが、そこに現れる半正定値計画問題は、association scheme の正則性をフルに活用することによって線形計画問題に帰着されるのである (cf. [11])。我々は ϑ-限界のある種の "2 部グラフ版" を導入することによって Theorem 1 を証明する。

まず記号の準備を行う。行と列が Ω で添字付けられた実行列全体の集合を $\mathbb{R}^{\Omega\times\Omega}$ とする。二つの行列 $Y,Z\in\mathbb{R}^{\Omega\times\Omega}$ に対し、その内積を $Y\bullet Z=\mathrm{trace}(Y^{\mathsf{T}}Z)$ で表す。また、$\mathbb{R}^{\Omega\times\Omega}$ の中の対称行列全体の集合を $S\mathbb{R}^{\Omega\times\Omega}$ と書くことにする。各 $k,\ell=0,\dots,n$ に対し、行列 $W_{k,\ell},\overline{W}_{k,\ell}\in\mathbb{R}^{\Omega\times\Omega}$ を次で定義する：

$$(W_{k,\ell})_{x,y}=\begin{cases}1 & \text{if } x\in\Omega_k,\ y\in\Omega_\ell,\ x\cap y\in\Omega_{\min\{k,\ell\}},\\ 0 & \text{otherwise,}\end{cases}$$

$$(\overline{W}_{k,\ell})_{x,y}=\begin{cases}1 & \text{if } x\in\Omega_k,\ y\in\Omega_\ell,\ x\cap y\in\Omega_0,\\ 0 & \text{otherwise.}\end{cases}$$

[1] ここで $\begin{bmatrix} a \\ b \end{bmatrix}=\begin{bmatrix} a \\ b \end{bmatrix}_q$ は通常の q-二項係数を表す：$\begin{bmatrix} a \\ b \end{bmatrix}=\prod_{i=0}^{b-1}((q^{a-i}-1)/(q^{b-i}-1))$.
[2] Theorem 1 の $k=\ell$ の場合は最近 Tokushige [15] により証明された。

ここで $W_{k,\ell} = W_{\ell,k}^{\mathsf{T}}$, $\overline{W}_{k,\ell} = \overline{W}_{\ell,k}^{\mathsf{T}}$ に注意する。また、$I_k := W_{k,k}$ は $\mathbb{R}^{\Omega_k} \subseteq \mathbb{R}^{\Omega}$ への直交射影であり、$\overline{W}_{k,k}$ は (本質的に) q-Kneser グラフ $qK_{n:k}$ の隣接行列である。最後に、$J \in \mathbb{R}^{\Omega\times\Omega}$ を成分が全て 1 の行列とし、各 $k,\ell = 0,\dots,n$ に対して $J_{k,\ell} := I_k J I_\ell$ とする。

以下 $k,\ell = 1,\dots,\lfloor \frac{n}{2} \rfloor$ を固定し、$k > \ell$ と仮定する[3]。空でない部分空間族 $\mathscr{F} \subseteq \Omega_k$, $\mathscr{G} \subseteq \Omega_\ell$ が cross-intersecting であるとし、$\varphi, \psi \in \mathbb{R}^{\Omega}$ をそれぞれ $\mathscr{F}, \mathscr{G}$ の特性 (列) ベクトルとする。このとき、

$$X_{\mathscr{F},\mathscr{G}} = \left(\frac{\varphi}{\|\varphi\|} + \frac{\psi}{\|\psi\|}\right)\left(\frac{\varphi}{\|\varphi\|} + \frac{\psi}{\|\psi\|}\right)^{\mathsf{T}} \in S\mathbb{R}^{\Omega\times\Omega}$$

は次の半正定値計画問題の、目的値 $|\mathscr{F}|^{\frac{1}{2}}|\mathscr{G}|^{\frac{1}{2}}$ の実行可能解を与えることが直ちに確かめられる：

$$\begin{aligned}
\text{(P):}\quad \text{maximize}\quad & \frac{1}{2}(J_{k,\ell} + J_{\ell,k}) \bullet X \\
\text{subject to}\quad & I_k \bullet X = I_\ell \bullet X = 1, \\
& (\overline{W}_{k,\ell} + \overline{W}_{\ell,k}) \bullet X = 0, \\
& X \succcurlyeq 0,\ X \geqslant 0.
\end{aligned}$$

ここで $X \in S\mathbb{R}^{\Omega\times\Omega}$ が変数であり、また $X \succcurlyeq 0$, $X \geqslant 0$ はそれぞれ X が半正定値及び非負であることを意味する。この問題の双対問題は次で与えられる：

$$\begin{aligned}
\text{(D):}\quad \text{minimize}\quad & \alpha + \beta \\
\text{subject to}\quad & S := \alpha I_k + \beta I_\ell - \frac{1}{2}(J_{k,\ell} + J_{\ell,k}) - \gamma(\overline{W}_{k,\ell} + \overline{W}_{\ell,k}) - A \succcurlyeq 0, \\
& A \geqslant 0.
\end{aligned}$$

ここで $\alpha,\beta,\gamma \in \mathbb{R}$ 及び $A \in S\mathbb{R}^{\Omega\times\Omega}$ が変数である[4]。実際、(P) と (D) の任意の実行可能解に対して、

$$\begin{aligned}
\alpha + \beta - \frac{1}{2}(J_{k,\ell} + J_{\ell,k}) \bullet X &= \left(\alpha I_k + \beta I_\ell - \frac{1}{2}(J_{k,\ell} + J_{\ell,k})\right) \bullet X \\
&\geqslant (\gamma(\overline{W}_{k,\ell} + \overline{W}_{\ell,k}) + A) \bullet X \\
&= A \bullet X \\
&\geqslant 0
\end{aligned}$$

となる。特に、$(\alpha+\beta)^2$ は $|\mathscr{F}||\mathscr{G}|$ の上界を与える。さらに、$\alpha + \beta = \frac{1}{2}(J_{k,\ell} + J_{\ell,k}) \bullet X$ となる場合には $S \bullet X = A \bullet X = 0$ が成り立たなければならないことも分かる。次の 1 パラメータ族を考える：

$$\alpha = \beta = \frac{1}{2}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}^{\frac{1}{2}}\begin{bmatrix} n-1 \\ \ell-1 \end{bmatrix}^{\frac{1}{2}},\quad \gamma = b(\lambda),\quad A = a(\lambda)\overline{W}_{k,k} + \lambda\overline{W}_{\ell,\ell}. \tag{1}$$

ただしここで $\lambda \in \mathbb{R}$ であり、$a(\lambda)$, $b(\lambda)$ は

$$\begin{aligned}
q^{k^2}(q^k-1)\begin{bmatrix} n-k \\ k \end{bmatrix} a(\lambda) &= \frac{1}{2}q^{\ell}(q^{k-\ell}-1)\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}^{\frac{1}{2}}\begin{bmatrix} n-1 \\ \ell-1 \end{bmatrix}^{\frac{1}{2}} + q^{\ell^2}(q^{\ell}-1)\begin{bmatrix} n-\ell \\ \ell \end{bmatrix}\lambda, \\
q^{k\ell}\begin{bmatrix} n-k \\ \ell \end{bmatrix} b(\lambda) &= -\frac{1}{2}q^{\ell}\begin{bmatrix} n-1 \\ \ell \end{bmatrix} - q^{\ell^2}\begin{bmatrix} n-\ell \\ \ell \end{bmatrix}\begin{bmatrix} n-1 \\ \ell-1 \end{bmatrix}^{\frac{1}{2}}\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}^{-\frac{1}{2}}\lambda
\end{aligned}$$

によって定める。このとき次の定理が示される：

[3] この仮定 ($k > \ell$) は単に記述を簡単にするためのものであり、本質的では全くない。すなわち、$k = \ell$ の場合には Ω_ℓ を Ω_k の異なる "コピー" とし、行と列が $\Omega \cup \Omega_\ell$ で添字付けられた行列を考えることになる。いずれにせよ、この場合は Tokushige [15] により既に解決されている。

[4] これらの制約条件から、x,y のいずれか一方が $\Omega_k \cup \Omega_\ell$ に含まれない場合には $A_{x,y} = 0$ となる。

Theorem 2. *For sufficiently small $\lambda > 0$, (1) gives a feasible solution to (D).*

Theorem 2 の証明は、双対問題 (D) を一般線形群 $GL(n,q)$ の対称性によって "ブロック対角化" することによって行う。詳細については [12] をご覧いただきたい。ここでは 2 種類の次元 (k,ℓ) の部分空間族を考えているので、Erdős-Ko-Rado の定理やその q-類似の証明の場合のように線形計画問題まで帰着することはできず、2×2 行列による制約条件が残ってしまう。従って状況はより複雑であるが、Frankl-Wilson [5] の計算を少々拡張することによって解決される。Theorem 1 は、Theorem 2 (及び前述のコメント) より示される：

Proof of Theorem 1. まず上界 $|\mathscr{F}||\mathscr{G}| \leqslant (\alpha+\beta)^2 = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}\begin{bmatrix} n-1 \\ \ell-1 \end{bmatrix}$ が直ちに従う。次に等号が成立すると仮定すると、$0 = A \bullet X_{\mathscr{F},\mathscr{G}} = a(\lambda)\,\overline{W}_{k,k} \bullet X_{\mathscr{F},\mathscr{G}} + \lambda\,\overline{W}_{\ell,\ell} \bullet X_{\mathscr{F},\mathscr{G}}$ となる。しかしながら、$\lambda > 0$ のときは常に $a(\lambda) > 0$ であるので、この場合には結局 $\overline{W}_{k,k} \bullet X_{\mathscr{F},\mathscr{G}} = \overline{W}_{\ell,\ell} \bullet X_{\mathscr{F},\mathscr{G}} = 0$ となる。すなわち、$\mathscr{F}$ と $\mathscr{G}$ はいずれも Erdős-Ko-Rado の定理の q-類似に於ける交叉族となる。従って $|\mathscr{F}| = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$, $|\mathscr{G}| = \begin{bmatrix} n-1 \\ \ell-1 \end{bmatrix}$ が得られ、さらに $\mathscr{F}$ と $\mathscr{G}$ の記述も同じ定理より容易に確認される (cf. [9, 6, 13])。 □

参考文献

[1] A. Chowdhury and B. Patkós, Shadows and intersections in vector spaces, J. Combin. Theory Ser. A 117 (2010) 1095–1106.

[2] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Rep. Suppl. No. 10 (1973).

[3] P. Erdős, C. Ko and R. Rado, Intersection theorems for systems of finite sets, Quart. J. Math. Oxford Ser. (2) 12 (1961) 313–320.

[4] P. Frankl and N. Tokushige, The Kruskal–Katona theorem, some of its analogues and applications, Extremal problems for finite sets (P. Frankl, Z. Füredi, G. Katona and D. Miklós, eds.), János Bolyai Mathematical Society, Budapest, 1994, pp. 229–250.

[5] P. Frankl and R. M. Wilson, The Erdős–Ko–Rado theorem for vector spaces, J. Combin. Theory Ser. A 43 (1986) 228–236.

[6] C. D. Godsil and M. W. Newman, Independent sets in association schemes, Combinatorica 26 (2006) 431–443; arXiv:math/0311535.

[7] L. Lovász, On the Shannon capacity of a graph, IEEE Trans. Inform. Theory 25 (1979) 1–7.

[8] M. Matsumoto and N. Tokushige, The exact bound in the Erdős–Ko–Rado theorem for cross-intersecting families, J. Combin. Theory Ser. A 52 (1989) 90–97.

[9] M. W. Newman, Independent sets and eigenspaces, Ph.D. Thesis, University of Waterloo, 2004.

[10] L. Pyber, A new generalization of the Erdős–Ko–Rado theorem, J. Combin. Theory Ser. A 43 (1986) 85–90.

[11] A. Schrijver, A comparison of the Delsarte and Lovász bounds, IEEE Trans. Inform. Theory 25 (1979) 425–429.

[12] S. Suda and H. Tanaka, A cross-intersection theorem for vector spaces based on semidefinite programming, preprint; arXiv:1304.5466.

[13] H. Tanaka, Classification of subsets with minimal width and dual width in Grassmann, bilinear forms and dual polar graphs, J. Combin. Theory Ser. A 113 (2006) 903–910.

[14] H. Tanaka, The Erdős–Ko–Rado theorem for twisted Grassmann graphs, Combinatorica 32 (2012) 735–740; arXiv:1012.5692.

[15] N. Tokushige, The eigenvalue method for cross t-intersecting families, J. Algebraic Combin. 38 (2013) 653–662.

[16] R. M. Wilson, The exact bound in the Erdős–Ko–Rado theorem, Combinatorica 4 (1984) 247–257.

Weighing matirxと球面上のデザイン, アソシエーションスキームについて

愛知教育大学　須田庄

1 序

Hadamard行列の一般化であるWeighing matrixについて, 本報告集ではHadamard行列とアソシエーションスキームの関係性をweighing行列へ拡張することを目標とする．またMUBの一般化として, mutually unbiased weighing matricesについても同様のことを考察する．本研究は愛知教育大の野崎寛氏との共同研究に基づく．本文で省略された証明は[5]を参照ください。

2 Weighing matrix

W を成分を $0, \pm 1$ とする d 次の正方行列とする．W が重さ k のweighing matrixであるとは, $WW^T = kI$ を満たすこととする．ここで, I は単位行列とする．定義から明らかなように $k = d$ となるweighing matrixは位数 d のHadamard matrixに一致する．

まず, Hadamard matrixとアソシエーションスキームの関連性について述べる．位数 d のHadamard matrix H から d 次元の実球面 S^{d-1} 上の有限集合 X を以下のようにして作る．$X_0 = \{\pm e_1, \ldots, \pm e_d\}$, $X_1 = \{\pm \frac{1}{\sqrt{d}} h_1, \ldots, \pm \frac{1}{\sqrt{d}} h_d\}$ (e_i は第 i 成分が1の単位ベクトル, h_i は H の第 i 行とする) とし, $X = X_0 \cup X_1$ とおく．このとき X の内積集合 $A(X) := \{\langle x, y\rangle \mid x, y \in X, x \neq y\}$ は $A(X) = \{\pm \frac{1}{\sqrt{d}}, 0, -1\}$ で与えられる．$\alpha_0 = 1, \alpha_1 = -1, \alpha_2 = \frac{1}{\sqrt{d}}, \alpha_3 = \frac{-1}{\sqrt{d}}, \alpha_4 = 0$ とおく．このとき,

$$R_i = \{(x, y) \in X \times X \mid \langle x, y\rangle = \alpha_i\} \qquad (i = 0, 1, \ldots, 4)$$

とおくことで $(X, \{R_i\}_{i=0}^4)$ はアソシエーションスキームになる．

しかしWeighing matrixに対して同様の方法ではアソシエーションスキームにはならないことが容易にわかる．これは, Hadamard matrixに対しては X_0 と X_1 の間に0の二点が現れないのに対し, weighing matrixに対してはそうではないことに由来する．従って, 重さ k のweighing matrix W に対して, $X_1 = \{\pm \frac{1}{\sqrt{k}} w_1, \ldots, \pm \frac{1}{\sqrt{k}} w_d\}$ (w_i は W の第 i 行) とし, $X = X_0 \cup X_1$ に対し $A(X) = \{\pm \frac{1}{\sqrt{k}}, 0, -1\}$ であるので．$\beta_0 = 1, \beta_1 = -1, \beta_2 = \frac{1}{\sqrt{k}}, \beta_3 =$

$\frac{-1}{\sqrt{k}}, \beta_4 = 0$ とおく．このとき，

$$R_i = \{(x,y) \in X \times X \mid \langle x,y \rangle = \beta_i\} \qquad (i = 0,1,2,3)$$
$$R_4 = \{(x,y) \in X \times X : \langle x,y \rangle = 0, x \in X_i, y \in X_j \text{ for } i \neq j\},$$
$$R_5 = \{(x,y) \in X \times X : \langle x,y \rangle = 0, x,y \in X_i \text{ for } i = 1,2\}.$$

のように，内積0から定まる二項関係を分割することが自然である．しかし，このような二項関係を考えても次のような W は X 上にアソシエーションスキームを定めない：

$$W = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & -1 & 0 & -1 & 0 & 1 & 0 \\ 1 & 0 & 0 & -1 & 0 & -1 & -1 & 0 \\ 0 & 1 & -1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 & 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & -1 & 1 & -1 \end{pmatrix}.$$

ではどのような W に対してはアソシエーションスキームを定めるかについては次のような特徴づけが得られた．定理の証明には球面上のデザインの理論が用いられる．

Theorem 2.1. W を重さ k で d 次の *weighing matrix (ただし, $k < d$)* とし，X, R_i は上記のように定義する．このとき次の二条件は同値である：

(i) $(X, \{R_i\}_{i=0}^5)$ はアソシエーションスキームである，

(ii) W は *balanced generalized weighing matrix* である．

ここで位数 d, 重さ k の weighing matrix$W$ が balanced generalized weighing matrix であるとは次の条件をみたすことである: 任意の相異なる $i,j \in \{1,\dots,d\}$ に対して，多重集合として $\{W_{ik}W_{jk}^{-1} \mid 1 \leq k \leq d, W_{ik} \neq 0 \neq W_{jk}\} = \frac{\lambda}{2}\{1,-1\}$ $(\lambda = \frac{k(k-1)}{d})$ が成り立つ．

Remark 2.2. 講演後，花木章秀さん、田中太初さんから上記の定理は有限アーベル群上の balanced generalized weiging matrix に拡張されると指摘がありました．実際，その通りに拡張ができたので詳しくは [5] を参照してください．

3 Mutually unbiased weighing matrices

はじめに mutually unbiased bases(MUB) について述べる．位数が d の Hadamard matrices H_1, H_2 が unbiased であるとは，$\frac{1}{\sqrt{d}}H_1H_2^T$ が Hadamard matrix になることとし，MUB とは Hadamard matrices $H_1,\dots,H_f$ であって，任意の相異なる i,j に対して H_i, H_j が unbiased であることとする．

MUB の一般化として，mutually unbiased weighing matrices が Holzmann, Kharaghani, Orrick によって次のように与えられている [2]. 位数 d, 重さ k の weighing matrices W_1, W_2

が unbiased であるとは, $\frac{1}{\sqrt{k}}H_1H_2^T$ が重さ k の weighing matrix になることとし, mutually unbiased weighing matrices (MUWM) とは重さ k の weighing matrices $W_1,\dots,W_f$ であって, 任意の相異なる i,j に対して W_i,W_j が unbiased であることとする.

MUWM に関する基本的な問題は位数 d, 重さ k の mutually unbiased weighing matrices $W_1,\dots,W_f$ の個数 f に関する上限を決定することである. $X_0=\{\pm e_1,\dots,\pm e_d\}$, $X_i=\{\pm\frac{1}{\sqrt{k}}w_{i,1},\dots,\pm\frac{1}{\sqrt{k}}w_{i,d}\}$ ($w_{i,j}$ は W_i の第 j 行) とし, $X=\cup_{i=0}^{f}X_i$ とおく. すると X の内積集合は $A(X)=\{\pm 1/\sqrt{k},0,-1\}$ であるので, 線形計画法を用いることで次のような不等式が得られる.

Proposition 3.1. $\{W_1,\dots,W_f\}$ を位数 d, 重さ k の *mutually unbiased weighing matrices* とする. もし $\frac{d}{3}+1\le k$ であれば, $f\le\frac{k(d-1)}{3k-d-2}$ が成り立つ.

講演の際には上記の不等式を満たす例を挙げられなかったが, Best, Kharaghani, Ramp による最近のプレプリント [1] には E_7,E_8 ルート系を正規直交基底に分解をすることで上記の不等式を達成する例が与えられている.

講演後, 野崎寛氏との共同研究を進めて MUWM を得るために [5] では mutually quasi-unbiased という概念を次のように定義した. 位数 d, 重さ k の weighing matrices W_1,W_2 が quasi-unbiased for parameters (d,k,l,a) であるとは $1/\sqrt{a}W_1W_2^T$ が重さ l の weighing matrix であることとし, mutually quasi-unbiased もこれまでと同様に定義する. 定義から容易にわかるように, mutually quasi-unbiased weighing matrices for parameters (d,k,l,a) $W_1,\dots,W_f$ に対して, $(1/\sqrt{a})W_2W_1^T,\dots,(1/\sqrt{a})W_fW_1^T$ は重さ l の MUWM になる. さらに [5] では $(d,k,l,a)=(2^{2t+1},2^{2t+1},2^{2t},2^{2t+2})$ (t は正の整数), $(d,2,4,1)$ に対して mutually quasi-unbiased weighing matrices の個数の上限を決定した.

MUB とアソシエーションスキームの関係は以下のようにして与えられる [3]. 位数 d の MUB $H_1,\dots,H_f$ から d 次元の実球面 S^{d-1} 上の有限集合 X を以下のようにして作る. $X_0=\{\pm e_1,\dots,\pm e_d\}$, $X_i=\{\pm\frac{1}{\sqrt{d}}h_{i,1},\dots,\pm\frac{1}{\sqrt{d}}h_{i,d}\}$ ($h_{i,j}$ は H_i の第 j 行) とし, $X=\cup_{i=0}^{f}X_i$ とおく. このとき,

$$R_i=\{(x,y)\in X\times X\mid\langle x,y\rangle=\alpha_i\}\qquad(i=0,1,\dots,4)$$

とおくことで $(X,\{R_i\}_{i=0}^4)$ はアソシエーションスキームになる.

MUWM に対しては, X_i の内部に現れるか否かに応じて内積 0 から定まる二項関係を以下のように分解する:

$$\begin{aligned}
&R_i=\{(x,y)\in X\times X\mid\langle x,y\rangle=\beta_i\},\\
&\tilde{R}_i=R_i\text{ for }i\in\{0,1,2,3\},\\
&\tilde{R}_4=R_4\cap\bigcup_{i\neq j}(X_i\times X_j),\\
&\tilde{R}_5=R_4\setminus\tilde{R}_4.
\end{aligned}$$

この分解によりアソシエーションスキームに関する定理が得られる.

Theorem 3.2. $(X,\{R_i\}_{i=0}^4)$ がアソシエーションスキームであれば $(X,\{\tilde{R}_i\}_{i=0}^5)$ もアソシエーションスキームである.

この定理を E_7, E_8 ルート系から得られる MUWM とパラメータ $(2^{2t+1}, 2^{2t+1}, 2^{2t}, 2^{2t+2})$ の mutually quasi-unbiased weighing matrices から得られる MUWM に適用することでクラスが 5 のアソシエーションスキームが得られる

4 今後の研究課題

最後に MUWM について考察したい問題を挙げることで報告集を終える.

(1) Porposition 3.1 では条件 $\frac{d}{3}+1 \leq k$ の下で f の上界が与えられている. $\frac{d}{3}+1 > k$ の場合には [4, Theorem 3.3] により, $f \leq \frac{(d+5)(d-2)}{6}$ が得られる. この不等式を満たす例は存在するか?

(2) Mutually quasi-unbiased weighing matrices (d, k, l, a) の weighing matrices に対する個数の上界を与えよ. これから得られる MUWM に対して線形計画法は適用されるが, より良い不等式が得られることが望まれる.

参考文献

[1] D. Best, H. Kharaghani, and H. Ramp, Mutually Unbiased Weighing Matrices, preprint, arXiv:1307.8161.

[2] W. H. Holzmann, H. Kharaghani and W. Orrick, On the real unbiased Hadamard matrices, Combinatorics and graphs, 243–250, Contemp. Math. 531, Amer. Math. Soc., Providence, RI, 2010.

[3] N. LeCompte, W. J. Martin, W. Owens, On the equivalence between real mutually unbiased bases and a certain class of association schemes, *Europ. J. Combin*, 31, no. 6 (2010) 1499–1512.

[4] H. Nozaki and M. Shinohara, On a generalization of distance sets, J. Combin. Theory Ser. A 117 (2010), no.7, 810–826.

[5] H. Nozaki and S. Suda, Association schemes related to weighing matrices, preprint, arXiv:1309.3892.