第 36 回代数的組合せ論シンポジウム報告集

2019 年 6 月 17 日－19 日
於　長崎大学文教キャンパス

まえがき

令和元年 8 月 24 日に本報告集本欄の執筆依頼を受けた。過去の報告集をめくると、判で押したように形式的な文言が並び、

基盤研究 (B) 研究代表者：北詰正顕 (課題番号：24340002)

のように運営資金の援助者一覧が掲載されるのが常であった。今回はその前例を踏襲することが出来なくなったのは悲痛の極みである。

令和元年 6 月 17〜19 日の期間に長崎大学で開催された第 36 回代数的組合せ論シンポジウムの中日最終講演者は、胃と食道を摘出する大手術を経た後、食べ物の十分な摂取ができず、就寝時の逆流を防ぐための可動式寝台を備えるホテルに宿泊するほどの回復状況で、４０分間の講演を行い、誰よりも大きな拍手を浴びた。彼を知る聴衆のほとんどは痩せこけた彼の容貌に戸惑いながらも、病状が回復に向かうだろうと信じて疑わなかったはずである。それほどの力強い活舌と以前と変わらぬ精緻な説明だったのだ。

その願いも空しく、8 月 12 日に彼はこの世を去った。長年にわたって本研究集会の学術面と運営面においての彼の貢献そして尽力はこの共同体の誰もが知る所であり、もう二度と会えないという悲しみと喪失感もまたしかりである。

北詰先生、以前お会いした時に掛けていただいたお言葉が思い出されます。あれが最後になるとは夢にも思いませんでした。肉体は滅べど、先生の数字的業績、数々のご講演、そして気さくなお人柄は我々の心の中で生き続けるのです。天に召された先生にそのことをお知らせしようと思い、この報告集をしたためる次第です。

平坂　貢

本研究集会は次の援助を受けて開催されました。

- 科研費基盤研究 (B) 19H01802 「代数的符号理論の総合的研究 」 (代表者 : 原田 昌晃)
- 科研費基盤研究 (C) 18K03396 「Ramsey 的手法による極値組合せ論の研究 」（代表者：篠原 雅史）
- 科研費基盤研究 (C) 18K03245「組合せ構造のモジュラー表現の研究とその応用」（代表者：島袋 修）

2019 年 11 月

世話人

- 宗政 昭弘 (東北大学大学院情報科学研究科)
- 平坂 貢 (釜山大学校自然科学大数学科)
- 島倉 裕樹 (東北大学大学院情報科学研究科)
- 篠原 雅史 (滋賀大学教育学部)
- 島袋 修 (長崎大学教育学部)

第 36 回代数的組合せ論シンポジウム

標記の研究集会を以下の要領で開催しますので，ご案内申し上げます.

世話人: 宗政 昭弘 (東北大学)
平坂 貢 (釜山大学校)
島倉 裕樹 (東北大学)
篠原 雅史 (滋賀大学)
島袋 修 (長崎大学)

日時：2019 年 6 月 17 日 (月)–6 月 19 日 (水)
場所：長崎大学文教キャンパス工学部 21 番教室 (長崎県長崎市文教町 1-14)

プログラム

6 月 17 日 (月) 午後

12:50–13:30 吉野 聖人 (東北大学 D1)
Non 2-integrable lattices of dimension 12 and discriminant 15

13:40–14:20 佐竹翔平 (神戸大学 D3)
On expansion properties of some Abelian Cayley graphs

14:30–15:00 Himadri Shekhar Chakraborty (金沢大学 D1)
Enumeration Results of Moriyama's conjecture in coding theory
(joint with Y. Arike, T. Miezaki and M. Oura)

15:20–16:00 中空 大幸 (神戸学院大学)
符号のサポートデザインについて
(On the support designs of codes)

16:10–16:50 生田 卓也 (神戸学院大学)
Bordered complex Hadamard matrices and strongly regular graphs

6 月 18 日 (火) 午前

9:20–10:00 有家 雄介 (鹿児島大学)
Vertex operator algebras and modular linear differential equations

10:10–10:50 島倉裕樹 (東北大学)
On automorphism groups of the holomorphic VOAs associated with Niemeier lattices and the -1-isometries

11:00–11:40 田邊顕一朗 (北海道大学)
非退化偶格子に付随する頂点代数の不変部分代数の既約弱加群
（Irreducible weak modules for some fixed point subalgebra of the vertex algebra associated with a non-degenerate even lattice）

6 月 18 日 (火) 午後

13:40–14:20 籾原幸二 (熊本大学)
A big family of strongly regular graphs from three-valued Gauss periods

14:30–15:10 平尾将剛（愛知県立大学)
On QMC designs and related topics

15:20–16:00 東谷 章弘 (大阪大学)
Reflexive polytopes arising from finite graphs and the unimodality of h^*-vectors

16:10–16:50 北詰正顕 (千葉大学)
The Rudvalis group and the Hoffman-Singleton graph

6 月 19 日 (水) 午前

9:30-10:10 山口尚哉（長崎大学)
巡回群の群行列式の項数とある分割数について
(The number of terms of the group determinant of cyclic groups and some partition numbers)

10:20-11:00 花木章秀 (信州大学)
Frame numbers, splitting fields, and integral adjacency algebras of commutative association schemes

11:10-11:50 田上真 (九州工業大学)
Hamming scheme 上の調和指数 t-design について
(On Harmonic index t-designs in the Hamming scheme)

12:00-12:40 須田庄（愛知教育大学)
On tight 4-designs in Hamming association schemes

本研究集会は次の援助を受けて開催されます:

- 科研費基盤研究 (B) 19H01802「代数的符号理論の総合的研究 」(代表者 : 原田 昌晃)
- 科研費基盤研究 (C) 18K03396 「Ramsey 的手法による極値組合せ論の研究 」（代表者：篠原 雅史）
- 科研費基盤研究 (C) 18K03245 「組合せ構造のモジュラー表現の研究とその応用」（代表者：島袋 修）

目　次

Non 2-integrable lattices of dimension 12 and discriminant 15

吉野 聖人（東北大学）

1 はじめに

本稿は 2019 年 6 月 17 日に行った講演の内容に加筆したものである．

格子に関連する基本的な用語を定義する．まず n を正の整数とする．このとき，**格子**（*lattice*）とは $\mathbb{R}^n$ の部分集合 L であり，ある正の整数 $k \leq n$ と一次独立な元 $u_1, \ldots, u_k$ が存在して $L = \mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_k$ を満たすものである．以下，格子は全て**整格子**と仮定する．すなわち，格子の 2 元の内積は常に整数とする．格子 $L \subset \mathbb{R}^n$ に対して，その**双対** L^* は任意の L の元との内積が整数になるような $\mathbb{Q}L$ の元全体である．さらに，格子 L の *discriminant* とは，L^*/L の濃度であり，$\operatorname{disc} L$ と表される. 格子 L の部分格子 M に対して，M に直交する L の部分格子とは，M の任意の元と直交する L の元全体であり，$M^\perp$ と表される．

正の整数 s に対して，格子 L が *s-integrable* であるとは，ある正の整数 n が存在して $\sqrt{s}L$ が $\mathbb{Z}^n$ の部分格子と同形になることである．また，s-integrable でない格子の（$\mathbb{Z}$-加群としての）階数の最小値を $\phi(s)$ とする．Conway 氏と Sloane 氏によって，$\phi(1) = 6$, $\phi(2) = 12$，$\phi(3) = 14$ [2, Theorem 1] などが示されている．例えば，$\phi(1) = 6$ を与える non 1-integrable な階数 6 の格子としては，E_6 ルート格子がある．しかし，一般には $\phi(s)$ を決定することは難しく，$s \geq 4$ の時は決定されていない．彼らは $\phi(2) = 12$ を決定するために，階数 11 以下の格子は全て 2-integrable [2, Theorem 2] であることを示し，階数 12 の non 2-integrable 格子を 2 つ具体的に与えた．実際には，次の定義の下で定理 2 を証明した．

定義 1. 正の整数 n に対して，$\mathsf{A}_n := \{x \in \mathbb{Z}^{n+1} \mid (x, \mathsf{e}) = 0\}$ とする．ただし，e は成分が全て 1 のベクトルとする．また，$\mathsf{A}_{15}^+ := \langle \mathsf{A}_{15}, [4] \rangle$ とする．ただし，

$$[4] := \frac{1}{16}(4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, 4, -12, -12, -12, -12) \in \mathbb{R}^{16}.$$

定理 2 (Theorem 14 [2])**.** 格子 A_{15}^+ 内で，（ある基底に対応する）グラム行列として

$$\begin{bmatrix} 3 & 2 & 2 \\ 2 & 3 & 2 \\ 2 & 2 & 3 \end{bmatrix} \tag{1.1}$$

をもつ部分格子 M を任意にとる．この格子 M に直交する A_{15}^+ の部分格子 $M^\perp$ は階数 12，*discriminant* 7 かつ *non* 2*-integrable* である．

さらに定理 2 における格子 M は $\mathrm{Aut}(\mathsf{A}_{15}^{+})$ の作用を除いてちょうど 2 つであり，それぞれに直交する格子 L_{12} と L'_{12} は非同型であると述べられている．Conway 氏と Sloane 氏は階数が 12 の non 2-integrable 格子はこの 2 つだけかもしれないと述べていたが，新たにもう 2 つ階数 12 の non 2-integrable 格子を得た．これが主結果であり，定理 2 に対応して次のように述べる．

定理 3. 自己同型群 $\mathrm{Aut}(\mathsf{A}_{15}^{+})$ の作用を除いて，

$$\begin{bmatrix} 3 & 2 & 0 \\ 2 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix} \tag{1.2}$$

をグラム行列にもつ A_{15}^{+} の部分格子は $\langle a, b, c\rangle$ と $\langle a, b, c'\rangle$ のみである．ただし，

$$\begin{aligned} a &:= \frac{1}{4}(-3,-3,-3,-3,1,1,1,1,1,1,1,1,1,1,1,1) \in \mathsf{A}_{15}^{+}, \\ b &:= \frac{1}{4}(-3,-3,-3,1,-3,1,1,1,1,1,1,1,1,1,1,1) \in \mathsf{A}_{15}^{+}, \\ c &:= \frac{1}{4}(-3,1,1,1,1,-3,-3-3,1,1,1,1,1,1,1,1) \in \mathsf{A}_{15}^{+}, \\ c' &:= \frac{1}{4}(1,1,1,-3,-3,-3,-3,1,1,1,1,1,1,1,1,1) \in \mathsf{A}_{15}^{+}. \end{aligned}$$

さらに，非同型な格子 $\langle a, b, c\rangle^{\perp}$ と $\langle a, b, c'\rangle^{\perp}$ は階数 12，*discriminant* 15 かつ *non 2-integrable* である．

どのようにして，新たな non 2-integrable 格子を発見したかを説明する．まず [2] において，任意の階数 12 の non 2-integrable 格子は A_{15}^{+} の部分格子であることが示されているため，A_{15}^{+} の中から探した．もちろん A_{15}^{+} の部分格子は多数あるため，定理 2 の方法の類似を考察した． まずノルム 3 のベクトルから成る基底をもつ階数 3 の部分格子全体 $\mathcal{L}$ を $\mathrm{Aut}(\mathsf{A}_{15}^{+})$ の作用を除いて構成する（2 章）．そして，

$$\mathcal{L}^{\perp} = \{M^{\perp} \subset \mathsf{A}_{15}^{+} \mid M \in \mathcal{L}\}$$

の中から non 2-integrable な格子を探し，主結果の格子を得た．特に，$\mathcal{L}^{\perp}$ の元で non 2-integrable な格子は定理 2 と定理 3 に現れるもののみである．その際，non 2-integrable であることはコンピュータによる判定（補題 10）と，証明（4 章）をそれぞれ与えた．

注意 4. 講演時は階数 12 の non 2-integrable 格子は，Conway 氏と Sloane 氏の見つけたものと合わせても 4 しか見つかっていなかった．しかし，以下に述べる方法で多数発見した．ただし，それらは既に得られた階数 12 の non 2-integrable 格子から得られ，特に Conway 氏らの格子と主結果で得た格子はある意味で極小なものであることも明らかにした．

どのように新たな格子を構成したかを説明する．まず，階数 n の格子 L に対してグラム行列 $G \in M_n(\mathbb{Z})$ が取れる．正の整数 s とベクトル $v_1, \ldots, v_k \in \mathbb{Z}^n$ に対して，

$$G + \frac{1}{s}\sum_{i=1}^{k} v_i v_i^{\top}$$

の成分が全て整数のとき，この行列をグラム行列に持つ格子 M が存在する．Conway 氏と Sloane 氏は，L が s-integrable のとき M もそうであることを示した [2]．従って，このような方法で non s-integrable な格子 M を構成するためには，L が non s-integrable である必要がある．そこで，すでに発見していた 4 つの格子を L としてとり，さらに適当に $v_1, \ldots, v_k$ をとることで，non 2-integrable な格子を 10^4 個以上得た．ただし，2-integrability かの判定にはコンピュータを用いた．このようにして，non 2-integrable 格子の無限列が構成できると予想するが示せていない．

2 格子 A_{15}^{+}

第 1 章で述べた格子の集合

$$\mathcal{L} := \{M \subset \mathsf{A}_{15}^{+} \mid M \text{ はノルム } 3 \text{ のベクトルで生成される階数 } 3 \text{ の格子 }\}/\operatorname{Aut}(\mathsf{A}_{15}^{+})$$

を具体的に決定する方法を説明する．まず 16 次対称群 S_{16} は自然に A_{15}^{+} に作用する．さらに，$\operatorname{Aut}(\mathsf{A}_{15}^{+}) = \langle -1, S_{16} \rangle$ であることが分かる．また，相異なる整数 $i_1, \ldots, i_4 \in \{1, \ldots, 16\}$ に対して，

$$e_{i_1,i_2,i_3,i_4} = e_{\{i_1,i_2,i_3,i_4\}} = \frac{1}{4}\mathsf{e} - e_{i_1} - e_{i_2} - e_{i_3} - e_{i_4}$$

と定める．ただし，e は成分が全て 1 のベクトル，e_j は j 番目の成分が 1 かつ他の成分が 0 のベクトルを表す．単純な計算で，

$$T := \{x \in \mathsf{A}_{15}^{+} \mid (x,x) = 3\} = \{\pm e_I \mid I \subset \{1, \ldots, 16\}, |I| = 4\}$$

であることが分かる．さらに，濃度 4 の $I, J \subset \{1, \ldots, 16\}$ に対して

$$(e_I, e_J) = -1 + |I \cap J|$$

が成り立つ．以上のことから，$\mathcal{L}$ を決定することが出来る．なぜならば，ノルム 3 のベクトルから成る基底をもつ階数 3 の格子のグラム行列は少数しかなく，そのグラム行列を与えるベクトルは $\operatorname{Aut}(\mathsf{A}_{15}^{+})$ の作用を除いて次の例のように決定できるためである．

例 5. 行列 (1.2) をグラム行列に持つような 格子は $\operatorname{Aut}(\mathsf{A}_{15}^{+})$ の作用を除いて，$\langle a, b, c \rangle$ と $\langle a, b, c' \rangle$ であることを示す．行列 (1.2) をグラム行列として与えるベクトル $x, y, z \in \mathsf{A}_{15}^{+}$ を決定すればよい．まず，$\operatorname{Aut}(\mathsf{A}_{15}^{+}) \simeq \langle -1, S_{16} \rangle$ はノルム 3 ベクトル全体の集合 $T \subset \mathsf{A}_{15}^{+}$ に推移的に作用する．従って，$x = e_{1,2,3,4} = a$ と仮定してよい．さらに $(x, y) = 2$ より，$y = e_{1,2,3,5} = b$ としてよい．最後に，$(x, z) = (y, z) = 0$ なる z のとり方は，$\operatorname{Aut}(\mathsf{A}_{15}^{+})$ の作用を除いて

$$z = e_{1,6,7,8} = c \text{ と } z = e_{4,5,6,7} = c'$$

の 2 通りある．

例 5 は定理 3 の前半の主張である．また，2 つの格子が非同型であることは，kissing number を数えることで従う．これより，その 2 つに直交する A_{15}^{+} の部分格子が non 2-integrable であることを示せば主定理が従う．

3 s-integrablity の同値条件

格子の s-integrability を証明するため，或いは計算機で判定するために同値条件を述べる．

定義 6. 正の整数 s を固定する．正の整数 $n \leq m$ に対して，$\mathbb{R}^m$ からその n 次元部分空間への直交射影を p とおく．このとき，$p(\sqrt{s}\cdot e_1), \ldots, p(\sqrt{s}\cdot e_m)$ からなる多重集合を *(n 次元) スケール s の eutactic star* という．

補題 7 (Theorem 3 [2])**.** 正の整数 s を固定する．階数 n の格子 L が *s-integrable* であることの必要十分条件は，その双対 L^* が n 次元スケール s の *eutactic star* を含むことである．

与えられたベクトルが eutactic star であるかは次の補題によって判別できる．

補題 8 (pp. 215–216 [2])**.** ベクトル $s_1, \ldots, s_m \in \mathbb{R}^n$ が n 次元スケール s の *eutactic star* を成すことの必要十分条件は，任意の $w \in \mathbb{R}^n$ に対して

$$\sum_{i=1}^{m} (w, s_i)^2 = s(w, w) \tag{3.1}$$

が成り立つことである．

注意 9. Conway 氏と Sloane 氏は定理 2 において格子の non 2-integrability を証明するために，補題 7，8 を用いた．まず，補題 7 によって，non 2-integrability をスケール 2 の eutactic star の非存在性に帰着した．その後，eutactic star が存在が存在すると仮定すると，それらは (3.1) を満たさないことを適当なテストベクトル w をとることで証明し，補題 8 により矛盾を得た．その際，テストベクトルのとり方は自然であったが，(3.1) が満たされないことは直ちには従わない．加えて，格子によって異なる議論が必要であった．本稿では，定理 3 における格子が non 2-integrable であることの証明の概略を与えるが，まったく同様の方法で Conway 氏らの格子が non 2-integrable であることも証明できる．特に，後に与える補題 12 によって，テストベクトルのとり方や方程式を満たすかどうかという議論は不要になる．また補題 12 は 3 つの仮定を要請するが，実際に確認が必要な 2 つの仮定は Conway 氏らの証明でも必要であり証明を複雑にしない．

次に述べる補題によって，s-integrable かどうか判定する問題は線形方程式系の非負整数解の有無に帰着される．従って，方程式系の変数が少ない場合はコンピュータで判別することが出来る．実際に主定理が与える格子の non 2-integrability は，プログラミング言語 Magma [1] を用いて確かめた．一般に線形方程式系の変数が多くなる場合は，整数計画問題ソルバーの SCIP [3] を用いることで計算が可能になる場合がある．また次の補題の証明は補題 7，8 を組み合わせることで直ちに得られる．

補題 10. 正の整数 s を固定する．ベクトル $w_1, \ldots, w_n$. を基底に持つ格子 L をとる．さらに，ベクトル $u_1, \ldots, u_N$ はノルム s 以下の相異なる L^* の元全てを表す．このとき，L が

s-integrable であることの必要十分条件は，次の線形方程式系が非負整数解 $(x_1, \ldots, x_N)$ を持つことである*:*

$$\sum_{k=1}^{N} (w_i + w_j, u_k)^2 x_k = s(w_i + w_j, w_i + w_j) \quad (i, j = 1, \ldots, n). \tag{3.2}$$

4 主定理の証明の概略

第 2 章で述べたように主定理を示すためには次を示せばよい.

命題 11. 格子 A_{15}^{+} の部分格子 $\langle a, b, c\rangle^{\perp}$ と $\langle a, b, c'\rangle^{\perp}$ は *non* 2*-integrable* である

次の補題をその 2 つの格子に適用することで命題 11 を証明することが出来る．またコンピュータを用いると補題 10 によって s-integrability が判別できると述べていたが，新たな補題を用いることでより少ない計算量で判別可能である.

補題の主張で必要な記号を導入する．まず，格子 A_{15}^{+} のノルム 2 の元全体から成る集合を R で表す．また，ベクトル $u \in \mathbb{R}^n$ に対して，その**サポート**を

$$\operatorname{supp} u := \{i \in \{1, \ldots, n\} \mid u_i \neq 0\}$$

で定める.

補題 12. 集合 $\{1, \ldots, 16\}$ の部分集合を X，A_{15}^{+} の部分格子を N， A_{15}^{+} から $\mathbb{Q}N$ への直交射影を p とする. 次の条件を仮定する：

(1) N^* の非零元のノルムは 1 より大きい.

(2) N^* のノルムが 2 以下の非零元は $p(\mathsf{R})$ に含まれる.

(3) $|X| \geq 3$，かつ N はサポートが X に含まれる R の元を全て含む.

格子 N が 2*-integrable* ならば, ある一次独立な R の元 u と v が存在して，以下を満たす :

(4) $\operatorname{supp} u \cap \operatorname{supp} v \cap X \neq \emptyset$.

(5) $p(u)$ と $p(v)$ に対応するグラム行列 G に対して，$2I - G$ は半正値行列である.

この補題の証明は，補題 7 を用いることで得られるがいくつかの準備が必要になるため省略する.

命題 11 の証明の概略. まず

$$(N, X) = (\langle a, b, c\rangle^{\perp}, \{9, \ldots, 16\}) \text{ or } (\langle a, b, c'\rangle^{\perp}, \{8, \ldots, 16\})$$

とする．いずれの場合も補題 12 の 3 つの仮定を満たすことが以下のように確かめられる．まず，条件 (3) は定義から直ちに従う．$N = \langle a, b, c\rangle^{\perp}$ の場合で，残り 2 つの条件

を確かめる．格子 $\langle a, b, c\rangle$ を M とおく．このとき $\operatorname{disc} M = 15$ は square-free であるから，M は primitive である．そのため，

$$N^* \perp M^* = (M^\perp)^* \perp M^* = \mathsf{A}_{15}^+ + M^* = \bigoplus_{u+M \in M^*/M} \left(u + \mathsf{A}_{15}^+\right).$$

が成立する．ここで，M^*/M の完全代表系をノルムが 0 か 1 未満になるように取れる．格子 A_{15}^+ の最小ノルムは 2 であるから，$N = M^\perp$ の双対の最小ノルムは 1 より大きい．即ち，条件 (1) が満たされることが確かめられた．同様の理由から，条件 (2) も従い仮定は確かめられる．残りの $N = \langle a, b, c'\rangle^\perp$ の場合も全く同じ議論で仮定が確かめられる．これにより，補題 12 が (N, X) に適用できる．

格子 N が non 2-integrable であることを示すためには，補題 12 の条件 (4)，(5) を同時に満たす一次独立な $u, v \in \mathsf{R}$ が存在しないことを証明すればよい．即ち，任意の一次独立な $u, v \in \mathsf{R}$ が

$$\operatorname{supp} u \cap \operatorname{supp} v \cap X \neq \emptyset$$

を満たすとき，

$$2I - \begin{bmatrix} (p(u), p(u)) & (p(u), p(v)) \\ (p(v), p(u)) & (p(v), p(v)) \end{bmatrix}$$

が半正値でないことを証明すれば十分である．候補となる u, v のペアは多数あるが，対称性を加味することで数パターンを確かめればよいと分かり結果が従う． □

謝辞

シンポジウムにおいて発表と議論の場を与えてくださった世話人・関係者の皆様方に感謝いたします．

参考文献

[1] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[2] J. H. Conway, N. J. A. Sloane, Low-dimensional lattices V: Integral coordinates for integral lattices. *Proc. Roy. Soc. London Ser. A* **426** (1989), no. 1871, 211–232.

[3] A. Gleixner, M. Bastubbe, L. Eifler, T. Gally, G. Gamrath, R. L. Gottwald, G. Hendel, C. Hojny, T. Koch, M. E. Lübbecke, S. J. Maher, M. Miltenberger, B. Müller, M. E. Pfetsch, C. Puchert, D. Rehfeldt, F. Schlösser, C. Schubert, F. Serrano, Y. Shinano, J. M. Viernickel, M. Walter, F. Wegscheider, J. T. Witt, and J. Witzig, *The SCIP Optimization Suite 6.0*. ZIB-Report 18-26, Zuse Institute Berlin (2018).

On expansion properties of some Abelian Cayley graphs

佐竹 翔平 (Shohei Satake)*

概　　要

本稿では, 有限体のトレース関数で定義される Cayley ダイグラフの第 2 固有値を評価し, その応用として, 有限体のトレース関数に関するある整数論的問題に対する結果を与える.

1. 序

群 Γ とその部分集合 X に対して, Cayley ダイグラフ $Cay(\Gamma, X)$ は, 頂点集合に Γ を持ち, 2 頂点 u, v に対し, $u - v \in X$ であるときに限り (有向) 辺 (u, v) を定義することで得られるダイグラフである. 本稿では, 群 Γ が位数 q^r の有限体 $\mathbb{F}_{q^r}$ の乗法群 $\mathbb{F}_{q^r}^*$ の場合を考える. さらに, X として $\mathbb{F}_{q^r}$ から $\mathbb{F}_q$ へのトレース関数 $\mathrm{T} = \mathrm{T}_{q^r/q}$ と $A \subset \mathbb{F}_q$ で定義される以下の $\mathbb{F}_{q^r}^*$ の部分集合 T_A を考える.

$$T_A = \{x \in \mathbb{F}_{q^r}^* \mid \mathrm{T}(x) \in A\}. \tag{1}$$

ただし, $\mathrm{T}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{r-1}}$ である. 本稿では, Cayley ダイグラフ $Cay(\mathbb{F}_{q^r}^*, T_A)$ の隣接行列の固有値 (の絶対値) を求め, その結果を用いて Swaenepoel [9] によるある結果 (を一般化した形の定理) のグラフ理論的な証明を与える.

Swaenepoel [9] の結果を説明する前にその背景を以下で述べる. まず整数論においては, 整数の b 進表示における digit の持つ情報から, 整数の性質を調べる研究が盛んに行われてきた. 中でも, b 進表示における digit の総和から整数の性質を調べる研究に関しては, 多くの論文が出版されている (最も身近な例としては, 整数 x の 10 進表示において, digit の総和が 9 の倍数である場合, x は 9 の倍数となる事実などが上げられる).

こうした研究を (有理) 整数の世界から, 有限体上に初めて持ち込んだのが, Dartyge-Sárközy [6] である. 彼らは "digit" を次のように定義した. まず, 有限体 $\mathbb{F}_{q^r}$ は $\mathbb{F}_q$ 上の r 次元ベクトル空間の構造を持つため, ある基底 $\mathcal{B} = \{e_1, e_2, \ldots, e_r\}$ が取れ (以下基底 $\mathcal{B}$ は固定されるものとする), $\mathbb{F}_{q^r}$ の元 x は一次結合 $x = c_1e_1 + c_2e_2 + \cdots + c_re_r$ $(c_1, c_2, \ldots, c_r \in \mathbb{F}_q)$ の形で表される. この $c_1, c_2, \ldots, c_r$ を x の digit とよぶ. Dartyge-Sárközy [6] では, x の digit の総和

$$s_{\mathcal{B}}(x) = c_1 + c_2 + \cdots + c_r \tag{2}$$

を固定した状況で, x の持つ種々の性質に関して調べている. ここで, x の digit の総和 $s_{\mathcal{B}}(x)$ は, $\mathbb{F}_q$-線形形式であることに注意されたい. 有限体の場合, すべての $\mathbb{F}_q$-線形形式 f は, ある $a \in \mathbb{F}_{q^r}$ とトレース関数を用いて $f(x) = \mathrm{Tr}(ax)$ と表示できる. したがって, $s_{\mathcal{B}}(x)$ もトレース関数を用いて表現できる.

* 〒 657-8501 神戸市灘区六甲台町 1-1 神戸大学 大学院システム情報学研究科 情報科学専攻
e-mail: 155x601x@stu.kobe-u.ac.jp

一方で, Rivat-Sárközy [8] は, 有理整数の設定で, 自然数の集合 $\{1,2,\dots,n\}$ の大きな2つの部分集合 S, T に対して, 2つの自然数 $s \in S$, $t \in T$ の積 st の digit の総和の値は法 m において均等に分布することを次の意味で示した.

定理 1.1 ([8])**.** 任意の自然数 $b \geq 2$ に対して, $s_b(x)$ を自然数 x の b 進展開における *digit* の総和とおく. このとき, ある $C_b > 0$ が存在し, 任意の自然数 $m \geq 2$, $0 \leq a \leq m-1$ に対して, 以下が成り立つ : 任意の $S, T \subset \{1,2,\dots,n\}$ に対して,

$$\left|\#\{(s,t) \in S \times T \mid s_b(st) \equiv a \pmod m\} - \frac{|S||T|}{m}\right| \ll \Big(1 - \frac{1}{m}\Big) n^{2(1-C_b)} \log n.$$

上の定理において, $|S||T|/m$ という量は順序対 $(s,t) \in S \times T$ を確率 $1/m$ で独立ランダムに選んだ際の, $s_b(st) \equiv a \pmod m$ なる (s,t) の総数の期待値であることを注意しておく.

この定理の有限体類似が本稿で扱う Swaenepoel [9] による次の定理である.

定理 1.2 ([9])**.** 有限体 $\mathbb{F}_{q^r}^*$ の2つの部分集合 S, T および $a \in \mathbb{F}_q$ に対して, $\mathcal{E}_{\{a\}}(S,T) = \{(s,t) \in S \times T \mid \mathrm{Tr}(st) = a\}$ とする. このとき,

$$\left||\mathcal{E}_{\{a\}}(S,T)| - \frac{q^{r-1}}{q^r-1} \cdot |S||T|\right| \leq q^{\frac{r-1}{2}} \cdot \sqrt{|S||T|\Big(1 - \frac{|S|}{q^r-1}\Big)\Big(1 - \frac{|T|}{q^r-1}\Big)}. \quad (3)$$

実は, 定理 1.2 は, 先述した $Cay(\mathbb{F}_{q^r}^*, T_A)$ の「第2固有値」を上から評価することで, グラフ理論的に証明できる. 第2固有値は, エクスパンダーダイグラフやダイグラフの擬ランダムネスにおける重要な量であり, 定理 1.2 は, $Cay(\mathbb{F}_{q^r}^*, T_A)$ のエクスパンダーダイグラフの良さまたはその擬ランダムネスを測ることで得られる. そこで, まず第2節で第2固有値を定義し, そこからエクスパンダーダイグラフの良さまたはその擬ランダムネスを測れることを説明する. その上で, 第3節で $Cay(\mathbb{F}_{q^r}^*, T_A)$ の隣接行列の固有値を調べることで, 定理 1.2 の一般形である定理 3.1 の証明を与える. さらに, 特別な A に対する結果も与える. 最後に第4節でいくつかの注意を述べて, 本稿を締めくくる.

2. ダイグラフの第2固有値

まず, n 頂点ダイグラフ D の隣接行列 M_D とは, 行と列ぞれぞれが D の頂点でラベル付けされた n 次 0-1 正方行列であり, その (u,v)-成分は (u,v) が D の辺となる場合に限り 1 となる. 以下, D を d-正則 (各頂点の入次数と出次数がともに d) であると仮定する. このとき, d の固有ベクトルとしてオール 1 ベクトルが取れる事実と, Perron-Frobenius の定理から, d は絶対値が最大となる M_D の固有値となる. いま, $d = \lambda_1, \lambda_2, \dots, \lambda_n$ を M_D の固有値とおく. 一般に M_D は対称ではないため, 固有値は複素数となる. そこで, 固有値の絶対値の大小関係に着目し, D の第2固有値を $\lambda(D) = \max_{2 \leq i \leq n} |\lambda_i|$ とおく.

次に, エクスパンダーダイグラフにおいて, 第2固有値が重要な量であることを説明する. まず, n 頂点ダイグラフ $D = (V,E)$ において, サイズが $n/2$ 以下の任意の頂点部分集合 U に対し, $|N_D^-(U)| \geq c|U|$ となるとき, D を c-エクスパンダーとよぶ. ただし, $N_D^-(U) = \{v \in V \setminus U \mid \exists u \in U \text{ s.t. } (u,v) \in E\}$ とおく. この c の値が大きさが, エクスパンダーダイグラフとしての良さを測る一つの尺度となる. さて, D の隣接行列 M_D に適切な条件を課すことで, Alon-Spencer [1] の 9.2 節と議論と全く同様にして, 次の定理が証明される.

定理 2.1 ([1] を参照)**.** D を n 頂点 d-正則ダイグラフとし, 隣接行列 M_D は正規行列であると仮定する. このとき, D は $(d-\lambda(D))/2d$-エクスパンダーとなる.

上の定理から $\lambda(D)$ の値が小さいほど, D はよいエクスパンダーダイグラフとなることが保証される. このことから, 第2固有値がエクスパンダーダイグラフのよさを示す重要な量となる.

一方で, 第2固有値の小ささは, そのダイグラフがいかにランダムダイグラフに「近い」のかも示してくれる. この事実は, よいエクスパンダーダイグラフがランダムダイグラフに「近い」ことを示すものである. ここで, 辺確率 p のランダムダイグラフは, 大雑把に言えば, 異なる各2頂点 u, v の順序対 (u, v) において, 辺 (u, v) を確率 p で選ぶ試行を, 順序対ごとに独立に行うことで得られる. ダイグラフとランダムダイグラフの「近さ」を与える尺度が, 擬ランダムネスとよばれるものであり, 次の jumbled property で説明される. 任意の D の頂点部分集合 S, T に対して, 次を満たすとき, D は (p, α)-jumbled であるという.

$$\Big|e_D(S,T) - p|S||T|\Big| \le \alpha \cdot \sqrt{|S||T|}.$$

ここで, $e_D(S,T)$ は S から T に向かう D の辺の数であり, $p|S||T|$ という量は, ランダムダイグラフにおいて A から B に向かうの辺の数の期待値を表す. よって, この性質において, p に応じて α をどこまで小さく抑えられるかで, いかに辺確率 p のランダムダイグラフに近いかを表現できる. さらに, 辺確率 p の n 頂点ランダムダイグラフは, Chernoff の不等式から, 高い確率で $(p, O(\sqrt{np}))$-jumbled $(n \to \infty)$ となり, $(p, O(\sqrt{np}))$-jumbled である n 頂点ダイグラフの無限列は, ランダムダイグラフに近しいとみなせる. 次の expander-mixing lemma とよばれる補題は, 第2固有値と擬ランダムネスの関係を表す重要な補題である.

補題 2.2 ([10], [1])**.** D を n 頂点 d-正則ダイグラフとし, 隣接行列 M_D は正規行列であると仮定する. このとき, 任意の D の頂点部分集合 S, T に対して,

$$\left|e_D(S,T) - \frac{d}{n}|S||T|\right| \le \lambda(D) \cdot \sqrt{|S||T|\Big(1-\frac{|S|}{n}\Big)\Big(1-\frac{|T|}{n}\Big)}.$$

3. 主結果

本節では, 以下の定理の証明の概略を説明する.

定理 3.1. 有限体 $\mathbb{F}_{q^r}^*$ の2つの部分集合 S, T および $A \subset \mathbb{F}_q^*$ に対して, $\mathcal{E}_A(S,T) = \{(s,t) \in S \times T \mid \mathrm{Tr}(st) \in A\}$ とする. このとき,

$$\begin{aligned}\left||\mathcal{E}_A(S,T)| - \frac{|A|q^{r-1}}{q^r-1} \cdot |S||T|\right| \le{}& \max\Big\{\max_{\chi \in \widehat{\mathbb{F}_{q^r}^*}, \chi|_{\mathbb{F}_q^*} \neq 1} |\chi(A)| \cdot q^{\frac{r-1}{2}}, |A| \cdot q^{\frac{r}{2}-1}\Big\} \\ &\cdot \sqrt{|S||T|\Big(1-\frac{|S|}{q^r-1}\Big)\Big(1-\frac{|T|}{q^r-1}\Big)}.\end{aligned} \tag{4}$$

ただし, 有限体 $\mathbb{F}_{q^r}$ の乗法指標 χ (すなわち, 乗法群 $\mathbb{F}_{q^r}^*$ から複素数体の乗法群 $\mathbb{C}^*$ への群準同型) の全体がなす群を $\widehat{\mathbb{F}_{q^r}^*}$ (ただし, 単位元は自明な乗法指標 1) と記し, $\chi(A) = \sum_{x \in A} \chi(x)$ とおく.

注意 3.2. Swaenepoel による定理 1.2 は, 上の定理の q が素数かつ A が 1 点集合の場合である.

本稿冒頭でも述べたように, まず $Cay(\mathbb{F}_{q^r}^*, T_A)$ の第 2 固有値を評価する.

補題 3.3. *Cayley* ダイグラフ $Cay(\mathbb{F}_{q^r}^*, T_A)$ の隣接行列の各固有値は, ある $\chi \in \widehat{\mathbb{F}_{q^r}^*}$ に対する指標和 $\chi(T_A) = \sum_{x \in T_A} \chi(x)$ の形で表される. 特に最大の固有値 (次数) は, χ が自明な乗法指標 1 の場合の指標和 $1(T_A) = |T_A|$ に対応する.

証明. 隣接行列および Cayley ダイグラフそれぞれの定義から, $\chi(T_A)$ は固有ベクトル $v_\chi = (\chi(x))_{x \in \mathbb{F}_{q^r}^*}$ に対応する隣接行列の固有値である. 上の事実と指標の直交関係から, 補題の前半部分が示される. 後半部分は明らかである. □

補題 3.4.

$$\lambda(Cay(\mathbb{F}_{q^r}^*, T_{\mathcal{A}})) = \max\Big\{ \max_{\chi \in \widehat{\mathbb{F}_{q^r}^*}, \chi|_{\mathbb{F}_q^*} \neq 1} |\chi(A)| \cdot q^{\frac{r-1}{2}},\ |A| \cdot q^{\frac{r}{2}-1} \Big\}. \tag{5}$$

証明. 補題 3.3 より, $\chi(T_A)$ を評価することで, 求めたい第 2 固有値を評価することができる. まず, $a \in \mathbb{F}_q^*$ に対して, $\chi(T_{\{a\}}) = \chi(a) \cdot \chi(T_{\{1\}})$ が成り立つ事実 (例えば, [2, Chapter 12] などを参照) から, 本稿冒頭の T_A の定義より,

$$\chi(T_A) = \sum_{a \in A} \chi(T_{\{a\}}) = \sum_{a \in A} \chi(a)\chi(T_{\{1\}}) = \chi(A)\chi(T_{\{1\}})$$

が成り立つ. 補題の主張は, 上の等式と Gauss 和を用いた $\chi(T_{\{1\}})$ に関する以下の評価 (例えば, [2, Chapter 12]) を組み合わせることで得られる.

$$|\chi(T_{\{1\}})| = \begin{cases} q^{\frac{r-1}{2}} & \chi \text{ および } \chi|_{\mathbb{F}_q^*} \text{ は非自明;} \\ q^{\frac{r}{2}-1} & \chi \text{ は非自明だが, } \chi|_{\mathbb{F}_q^*} \text{ は自明;} \\ q^{r-1} & \chi \text{ は自明.} \end{cases}$$

□

以上で定理 3.1 の証明の準備が整った.

定理 3.1 の証明. 補題 3.4 を用いて, $D = Cay(\mathbb{F}_{q^r}^*, T_A)$ として expander-mixing lemma (補題 2.2) を適用する. ($\mathcal{E}_A(S,T) = e_D(S, T^{-1})$ であることに注意されたい. ただし, $T^{-1} = \{t^{-1} \mid t \in T\}$ とする.) ここで, M_D が正規行列であることを調べる必要があるが, D が Abel 群上の Cayley ダイグラフであることに着目して M_D とその転置の積を計算することで, 正規性を証明できる. □

また, Swaenepoel [9] では, q が素数の場合に, A として 1 点集合だけでなく, k 乗剰余全体の集合および $\mathbb{F}_q^*$ の生成元の集合などの乗法的な構造を持つ部分集合が考えられている. これらの場合, $\max_{\chi \in \widehat{\mathbb{F}_{q^r}^*}, \chi|_{\mathbb{F}_q^*} \neq 1} |\chi(A)| = |A|$ となり, $\chi(A)$ に関しては, 自明な評価しか得られない.

その一方で, A として加法的な構造を持つ部分集合を考えると, $\max_{\chi \in \widehat{\mathbb{F}_{q^r}^*}, \chi|_{\mathbb{F}_q^*} \neq 1} |\chi(A)| \ll |A|$ という非自明な評価から, 定理 3.1 の右辺をより小さく評価できる場合がある. 以下の系はその一例である.

系 3.5. q を素数とし, $c, d \in \mathbb{F}_q^*$ に対して, A を (加法に関して) 等差数列をなす $\mathbb{F}_q^*$ の元の集合 $\{c, c+d, c+2d, \dots, c+(|A|-1)d\}$ とする. また, S, T を $\mathbb{F}_{q^r}^*$ の部分集合とする. このとき, 任意の $l \geq 1$ に対して, ある (どのパラメータにも依存しない) 定数 $K > 0$ があって

$$\left| |\mathcal{E}_A(S,T)| - \frac{|A|q^{r-1}}{q^r-1} \cdot |S||T| \right| \leq K|A|^{1-\frac{1}{l+1}} q^{\frac{r-1}{2}+\frac{1}{4l}} \log q \cdot \sqrt{|S||T|\Big(1-\frac{|S|}{q^r-1}\Big)\Big(1-\frac{|T|}{q^r-1}\Big)}. \tag{6}$$

上の系において, A が $|A| \gg q^{\frac{l+1}{4l}} (\log q)^{l+1}$ のようにある程度大きい部分集合であれば, $\max_{\chi \in \widehat{\mathbb{F}_{q^r}^*}, \chi|_{\mathbb{F}_q^*} \neq 1} |\chi(A)| \ll |A|$ となり, 非自明な評価となる. ここで, $\max_{\chi \in \widehat{\mathbb{F}_{q^r}^*}, \chi|_{\mathbb{F}_q^*} \neq 1} |\chi(A)|$ の評価として, Burgess [4] の部分指標和の結果を用いた.

4. 諸注意

- Swaenepoel [9] の定理 1.2 の原証明は, 本質的には expander-mixing lemma の証明における議論の特別な場合を用いている. (少なくともこの事実は言及されておらず, 指標和の技術的な計算の形の証明になっている). 今回筆者は, (部分的に, 固有値の評価に関して Swaenepoel と同様に指標和の評価を用いるものの) Swaenepoel の証明をグラフ理論の見地から与えた. これにより, Swaenepoel の整数論的な結果が, エクスパンダーダイグラフまたは擬ランダムネスなどを通して組合せ論的な見地から捉えられることを明らかにした.

- Abel 群 Γ とその部分集合 X に対して, Cayley 和グラフ $CayS(\Gamma, X)$ は, 頂点集合に Γ を持ち, 2 頂点 u, v に対し, $u+v \in X$ であるときに限り辺 $\{u, v\}$ を定義することで得られるグラフである. 定理 3.1 は, $CayS(\mathbb{F}_{q^r}^*, T_A)$ に対してグラフ版の expander-mixing lemma を用いることでも証明できる.

- Mattheus [7] は筆者とは別に, 定理 1.2 の一般形の証明を与えている. 彼の証明は, 今回用いた $Cay(\mathbb{F}_{q^r}^*, T_A)$ とは別のある 2 部グラフに対して, 2 部グラフ版の expander-mixing lemma を応用するものである. その 2 部グラフの隣接行列の固有値の評価では, 指標和の評価を全く用いることなく組合せ論的な証明を行っている. その一方で, 定理 3.1 とは異なり, A が 1 点集合でない場合において, $|\mathcal{E}_A(S,T)|$ と $\frac{|A|q^{r-1}}{q^r-1} \cdot |S||T|$ の誤差は, A のいかなる構造に対しても一様にしか与えられない.

- 一般の素数べき q の場合の系 3.5 に対応する結果も, Davenport-Lewis [5] の結果を応用して得られる.

- Swaenepoel [9] では, 具体的な $S, T \subset \mathbb{F}_q^*$ を構成することで, 定理 1.2 における右辺の最適性も議論されている. 一方で, エクスパンダーグラフの構成に関する Bilu-Linial [3] の仕事で証明された expander-mixing lemma の「逆」の形の補題を用いることで, 十分大な q とすべての互いに素な $S, T \subset \mathbb{F}_{q^r}^*$ に対して, 右辺の $q^{\frac{r-1}{2}}$ の項は, いかなる $\varepsilon > 0$ に対しても, $q^{\frac{r-1}{2}-\varepsilon}$ の形には改良できないことも証明できる.

謝辞

今回講演の機会をくださった世話人の皆様ならびに講演をご静聴くださった参加者の皆様に心より御礼申し上げます. さらに, 事前にメールをいただき, 本年6月の国際会議 “F_q14” で議論させていただいたSam Mattheus氏にも感謝致します. 本研究はJSPS特別研究員奨励費 (課題番号:18J11282) の助成を受けております.

参考文献

[1] N. Alon, J. H. Spencer, The Probabilistic Method, John Wiley & Sons, Inc., 2016.

[2] B. Berndt, R. J. Evans, K. S. Williams, Gauss and Jacobi Sums, John Wiley & Sons, Inc., New York, 1998.

[3] Y. Bilu, N. Linial, Lifts, discrepancy and nearly optimal spectral gap, *Combinatorica*, **26** (2006), 495-519.

[4] D. A. Burgess, On character sums and primitive roots, *Proc. London Math. Soc. (3)* **12** (1962), 179–192.

[5] H. Davenport, D. J. Lewis, Character sums and primitive roots in finite fields, *Rend. Circ. Mat. Palermo (2)* **12** (1963), 129–136.

[6] C. Dartyge, A. Sárközy, The sum of digits function in finite fields, *Proc. Am. Math. Soc.*, **141** (2013), 4119–4124.

[7] S. Mattheus, private communication.

[8] J. Rivat, A. Sárközy, On arithmetic properties of products and shifted products, In *Analytic Number Theory*, Springer, 2015, 345–355.

[9] C. Swaenepoel, Trace of products in finite fields, *Finite Fields Appl.* **51** (2018), 93–129.

[10] V. H. Vu, Sum-product estimates via directed expanders, *Math. Res. Lett.* **15** (2008), no. 2, 375–388.

Enumeration results of Moriyama's conjecture in binary codes *

Yusuke Arike †, Himadri Shekhar Chakraborty ‡, Tsuyoshi Miezaki §, and Manabu Oura ¶

Abstract

Let L be a Euclidean integral lattice. Moriyama's conjecture says that the map from the harmonic polynomial P, which is invariant of $\mathrm{Aut}(L)$, to the theta series associated with P is injective. We state an analogy of Moriyama's conjecture for codes and we also show some enumeration results of this conjecture.

Key Words: Theta series, weight enumerators, trace functions.

2010 *Mathematics Subject Classification.* Primary 11T71; Secondary 94B05, 11F11.

1 Introduction

A lattice in $\mathbb{R}^n$ is a subset $\Lambda \subset \mathbb{R}^n$ with the property that there exists a basis $\{e_1, \cdots, e_n\}$ of $\mathbb{R}^n$ such that $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$, namely, Λ consists of all

*This work was supported by JSPS KAKENHI (19K03406, 18K03217, 17K05164).

†Faculty of Education, Kagoshima University, Kagoshima 890-0065, Japan, arike@edu.kagoshima-u.ac.jp,

‡Graduate School of Natural Science and Technology, Kanazawa University, Ishikawa 920-1192, Japan, himadri38@gmail.com,

§Faculty of Education, University of the Ryukyus, Okinawa 903-0213, Japan, miezaki@edu.u-ryukyu.ac.jp, Telephone: +81-98-897-8883, Fax: +81-98-897-8883 (Corresponding author)

¶Graduate School of Natural Science and Technology, Kanazawa University, Ishikawa 920-1192, Japan, oura@se.kanazawa-u.ac.jp, Telephone: +81-76-264-5635, Fax: +81-76-264-6065

integral linear combinations of the vectors $e_1, \cdots, e_n$. The dual lattice Λ is the lattice

$$\Lambda^\sharp := \{y \in \mathbb{R}^n \mid (y, x) \in \mathbb{Z},\ \forall x \in \Lambda\},$$

where (x, y) is the standard inner product. In this paper, we assume that the lattice Λ is integral, that is, $(x, y) \in \mathbb{Z}$ for all x, $y \in \Lambda$. An integral lattice Λ is called even if $(x, x) \in 2\mathbb{Z}$ for all $x \in \Lambda$, and it is odd otherwise. An integral lattice Λ is called unimodular if $\Lambda^\sharp = \Lambda$.

Let $\mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ be the upper half-plane. We denote by $\mathrm{Harm}_j(\mathbb{R}^n)$ the set of homogeneous harmonic polynomials of degree j on $\mathbb{R}^n$.

Definition 1.1. Let Λ be the lattice of $\mathbb{R}^n$. Then for a polynomial $P \in \mathrm{Harm}_j(\mathbb{R}^n)$, the function

$$\vartheta_{\Lambda,P}(z) := \sum_{x \in \Lambda} P(x) e^{i\pi z(x,x)}$$

is called the theta series of Λ weighted by P.

The theta series of Λ weighted by P is a modular form for some subgroup Γ_L of $SL_2(\mathbb{R})$ with some character χ_L. For the detailed expression of modular forms, see [3, 7, 8, 12, 13]. We denote by $M_k(\Gamma, \chi)$ (resp. $S_k(\Gamma, \chi)$) the space of modular forms (resp. cusp forms) with respect to Γ with the character χ. The following Moriyama's Conjecture is due to [16].

Conjecture 1.1. Let L be a integral lattice of rank n. Let $\mathrm{Harm}_j(\mathbb{R}^n)^{\mathrm{Aut}(L)}$ be a set of harmonic polynomimals, which is an invariant polynomial of $\mathrm{Aut}(L)$. Then the following map is injective:

$$\mathrm{Harm}_j(\mathbb{R}^n)^{\mathrm{Aut}(L)} \to M_{n/2+j}(\Gamma_L, \chi_L); P \mapsto \vartheta_{L,P}.$$

In [9], it is showed that for $L = E_8$-lattice and $\deg(P) < 20$, the Conjecture 1.1 is true. But in [17], it is showed for $L = E_8$-lattice that if $\deg(P) = 24$ then

$$\dim \mathrm{Harm}_{24}(\mathbb{R}^8)^{\mathrm{Aut}(E_8)} \neq \dim M_{24+4}(\Gamma_{E_8}, \chi_{E_8}).$$

Hence in general the Conjecture 1.1 is not true. The main purposes of the present paper is to state an analogy of Moriyama's conjecture in coding theory and to show that some enumeration results of the conjecture.

2 Harmonic Weight Enumerator

In this section, we review the concept of the harmonic weight enumerators.

Let C be a code of length n. The weight distribution of a code C is the sequence $\{A_i \mid i = 0, 1, \ldots, n\}$, where A_i is the number of codewords of weight i. The polynomial

$$w_C(x, y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$$

is called the weight enumerator of C. The weight enumerator of a code C and its dual $C^\perp$ are related. The following theorem, due to MacWilliams, is called the MacWilliams identity:

Theorem 2.1 ([14]). *Let $w_C(x, y)$ be the weight enumerator of an $[n, k]$ code C over $\mathbb{F}_q$ and let $w_{C^\perp}(x, y)$ be the weight enumerator of the dual code $C^\perp$. Then*

$$w_{C^\perp}(x, y) = q^{-k} W_C(x + (q-1)y, x - y).$$

A striking generalization of the MacWilliams identity was obtained by Bachoc [1], who gave the concept of harmonic weight enumerators and a generalization of the MacWilliams identity. The harmonic weight enumerators have many applications; particularly, the relations between coding theory and design theory are reinterpreted and progressed by the harmonic weight enumerators [1, 2]. For the reader's convenience, we quote the definitions and properties of discrete harmonic functions from [1, 4].

Let $\Omega = \{1, 2, \ldots, n\}$ be a finite set (which will be the set of coordinates of the code) and let X be the set of its subsets, while, for all $k = 0, 1, \ldots, n$, X_k is the set of its k-subsets. We denote by $\mathbb{R}X$, $\mathbb{R}X_k$ the real vector spaces spanned by the elements of X, X_k, respectively. An element of $\mathbb{R}X_k$ is denoted by

$$f = \sum_{z \in X_k} f(z) z$$

and is identified with the real-valued function on X_k given by $z \mapsto f(z)$.

Such an element $f \in \mathbb{R}X_k$ can be extended to an element $\widetilde{f} \in \mathbb{R}X$ by setting, for all $u \in X$,

$$\widetilde{f}(u) = \sum_{z \in X_k, z \subset u} f(z).$$

If an element $g \in \mathbb{R}X$ is equal to some $\widetilde{f}$, for $f \in \mathbb{R}X_k$, we say that g has degree k. The differentiation γ is the operator defined by the linear form

$$\gamma(z) = \sum_{y \in X_{k-1}, y \subset z} y$$

for all $z \in X_k$ and for all $k = 0, 1, \ldots n$, and Harm_k is the kernel of γ:

$$\mathrm{Harm}_k = \ker(\gamma|_{\mathbb{R}X_k}).$$

In [1], the harmonic weight enumerator associated with a binary linear code C was defined as follows:

Definition 2.1. Let C be a binary code of length n and let $f \in \mathrm{Harm}_k$. The harmonic weight enumerator associated with C and f is

$$w_{C,f}(x, y) = \sum_{\mathbf{c} \in C} \widetilde{f}(\mathbf{c}) x^{n - \mathrm{wt}(\mathbf{c})} y^{\mathrm{wt}(\mathbf{c})}.$$

Bachoc proved the following MacWilliams-type identity:

Theorem 2.2 ([1])**.** *Let $w_{C,f}(x, y)$ be the harmonic weight enumerator associated with the code C and the harmonic function f of degree k. Then*

$$w_{C,f}(x, y) = (xy)^k Z_{C,f}(x, y)$$

where $Z_{C,f}$ is a homogeneous polynomial of degree $n - 2k$, and satisfies

$$Z_{C^\perp,f}(x, y) = (-1)^k \frac{2^{n/2}}{|C|} Z_{C,f}\left(\frac{x + y}{\sqrt{2}}, \frac{x - y}{\sqrt{2}}\right).$$

Let S_n be the symmetric group of n positions. For a permutation $\sigma \in S_n$, and $f \in \mathbb{R}X_k$, define $f^\sigma \in \mathbb{R}X_k$ by

$$f^\sigma = \sum_{z \in X_k} f(z) z^\sigma$$

Now for a binary code C of length n, a code C^σ, which may or may not be exactly the same code as C. If $C^\sigma = C$, we call C^σ an *automorphism* of C, and in any case we refer to C and C^σ as equivalent codes. We call

$$\mathrm{Aut}(C) = \{\sigma \in S_n \mid C = C^\sigma\}$$

the *automorphism group* of the code C. By $\mathrm{Harm}_k^{\mathrm{Aut}(C)}$ we denotes the set of elements in Harm_k which are invariant under $\mathrm{Aut}(C)$, that is,

$$\mathrm{Harm}_k^{\mathrm{Aut}(C)} := \{f \in \mathrm{Harm}_k \mid f = f^\sigma \text{ for all } \sigma \in \mathrm{Aut}(C)\}$$

Conjecture 2.1. [16] Let C be a $\mathbb{F}_q$-code of length n. Let $\mathrm{Harm}_j(\mathbb{R}^n)^{\mathrm{Aut}(C)}$ be a set of harmonic polynomials, which is an invariant polynomial of $\mathrm{Aut}(C)$. Then the following map is injective:

$$\mathrm{Harm}_j(\mathbb{R}^n)^{\mathrm{Aut}(C)} \to \mathbb{C}[x,y]; f \mapsto w_{C,f}.$$

2.1 Method of Computation

In [11] the Hahn polynomials is defined in terms of the generalized hypergeometric series:

$${}_3F_2(a_1,a_2,a_3;b_1,b_2;z) = \sum_{i=0}^{\infty} \frac{(a_1)_i(a_2)_i(a_3)_i}{(b_1)_i(b_2)_i}.\frac{z^i}{i!}$$

where $(a)_0 = 1$ and $(a)_i = a(a+1)(a+2)\dots(a+i-1)$ for $i \geq 1$. The series terminates if one of the a_i is zero or a negative integer. For real α, β and for positive integer N, the Hahn polynomials $Q_m(x) \equiv Q_m(x;\alpha,\beta,N)$ are defined by hypergeometric series as:

$$Q_m(x) = {}_3F_2(-m,-x,m+\alpha+\beta+1;\alpha+1,-N+1;1)$$

for $m = 0,1,\dots,N-1$. The explicit formula for the Hahn polynomials given in [11] as follows:

$$Q_m(x) \equiv Q_m(x;\alpha,\beta,N) = \sum_{i=0}^{m} \frac{(-m)_i(-x)_i(m+\alpha+\beta+1)_i}{(\alpha+1)_i(-N+1)_i} \cdot \frac{1^i}{i!}.$$

From the explicit formula it can be seen at once that $Q_m(x)$ is a polynomial in the variable x with degree exactly m.

Theorem 2.3 ([1], Proposition 5.1)**.** *Let T be a t-subset of $\{1,2,\dots,n\}$. For all k, $1 \leq k \leq t \leq n/2$, let $H_{k,T} \in \mathbb{R}X_t$ be given by:*

$$H_{k,T}(u) = Q_k^t(t - |u \cap T|)$$

for all t-set u, where $Q_k^t(x) \equiv Q_k(x;t-n-1,-t-1,t+1)$ are orthogonal Hahn polynomials. Then $H_{k,T} \in \mathrm{Harm}_k$.

By Theorem 2.3 we can form a square matrix of order $\binom{n}{t}$, say, $H = [H_{k,T}(u)]$ for t-subsets T and u . Using elementary row operations we compute

$H_{k,T} \in \mathrm{Harm}_k$ such that $H_{k,T}$ is independent. Also compute the rank of matrix H which is equal to

$$m_k = \binom{n}{k} - \binom{n}{k-1}, \text{ where } k = 1, 2, \ldots, n/2.$$

Now let B_H be a basis of Harm_k. Again let $H_{k,T} \in B_H$ for some t-subset, T. Then $H_{k,T}(u)$ for all t-subset u forms an independent row in the matrix H. Therefore $\dim(\mathrm{Harm}_k) = m_k$.

Let $H_{k,T_i} \in B_H$ for $i = 1, 2, \ldots, m_k$. Then an element $f \in \mathrm{Harm}_k$ can be written as follows

$$f = \sum_{i=1}^{m_k} \alpha_i H_{k,T_i} = \sum_{i=1}^{m_k} \alpha_i \left(\sum_{u \in X_t} H_{k,T_i}(u) u \right) = \sum_{u \in X_t} \left(\sum_{i=1}^{m_k} \alpha_i H_{k,T_i}(u) \right) u.$$

where $\alpha_i \in \mathbb{R}$ and

$$f^\sigma = \sum_{i=1}^{m_k} \alpha_i H^\sigma_{k,T_i} = \sum_{i=1}^{m_k} \alpha_i \left(\sum_{u \in X_t} H_{k,T_i}(u) u^\sigma \right) = \sum_{u \in X_t} \left(\sum_{i=1}^{m_k} \alpha_i H_{k,T_i}(u) \right) u^\sigma$$

Now let $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$. Therefore for all $u \in X_t$ we have,

$$\sum_{i=1}^{m_k} \alpha_i H_{k,T_i}(u) = \sum_{i=1}^{m_k} \alpha_i H_{k,T_i}(v),$$

where $u = v^\sigma$ for some $v \in X_t$. Therefore the number of equations we have is $\gamma|X_t|$, where γ denotes the number of generators of $\mathrm{Aut}(C)$. Applying matrix row operations on $\gamma|X_t|$ equations, we evaluate linearly independent equations with m_k unknowns. Let the number of linearly independent equations be m_e. Our computation shows that $m_e \leq m_k$. Therefore

$$\dim\left(\mathrm{Harm}_k^{\mathrm{Aut}(C)}\right) = m_c = m_k - m_e$$

Now we have the following Theorem.

Theorem 2.4. *Let $C = \mathbb{F}_2^n$. Then $\mathrm{Aut}(C) = S_n$. We have*

$$\mathrm{Harm}_j(\mathbb{R}^n)^{\mathrm{Aut}(C)} = \{\mathbf{0}\}.$$

This means that Conjecture 2.1 is true for the case $C = \mathbb{F}_2^n$.

Proof. For a symmetric polynomial f, we have that $\gamma(f) \neq 0$. The proof is completed. □

2.2 Length 8

For $n = 8$ we have $C = e_8$ with $\gamma = 6$, the number of generators of $\mathrm{Aut}(C)$. Here we have the following observations:

n	$1 \le k \le n/2$	$k \le t \le n/2$	$\lvert X_t \rvert$	m_k	m_e	m_c
8	1	1	8	7	7	0
	2	2	28	20	20	0
	3	3	56	28	28	0
	4	4	70	14	13	1

Table 1: Data Table for Length 8

For $k = 1, 2, 3$ we compute $w_{C,f} = 0$ for $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$.

For $k = 4$ we compute $\dim(\mathrm{Harm}_k^{\mathrm{Aut}(C)}) = 1$. This implies $\mathrm{Harm}_k^{\mathrm{Aut}(C)} = \langle f_1 \rangle$ for some $f_1 \in \mathrm{Harm}_k$. That is,

$$\mathrm{Harm}_k^{\mathrm{Aut}(C)} \ni f = Af_1 \text{ for } A \in \mathbb{R}.$$

The harmonic weight enumerator for $k = 4$, $C = e_8$ and $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$ is

$$w_{C,f} = \frac{14}{3} A x^4 y^4.$$

Hence we have the following Theorem.

Theorem 2.5. *For $C = e_8$, Conjecture 2.1 is true. That is, the following map is injective:*

$$\mathrm{Harm}_j(\mathbb{R}^n)^{\mathrm{Aut}(e_8)} \to \mathbb{C}[x, y]; f \mapsto w_{e_8,f}.$$

2.3 Length 16

For $n = 16$ we have two cases

(i) $C = d_{16}^+$ with $\gamma = 8$ and

(ii) $C = e_8^2$ with $\gamma = 13$,

n	$1 \leq k \leq n/2$	$k \leq t \leq n/2$	$\lvert X_t \rvert$	m_k	m_e	m_c
16	1	1	16	15	15	0
	2	2	120	104	103	1
	3	3	560	440	440	0

Table 2: Data Table for Length 16

where γ is the number of generators of $\mathrm{Aut}(C)$. Here we have the following observations for both the cases:

For $k = 1, 3$ we compute $w_{C,f} = 0$ for $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$ for both $C = d_{16}^+$ and $C = e_8^2$.

For $k = 2$ and both the codes, we compute $\dim(\mathrm{Harm}_k^{\mathrm{Aut}(C)}) = 1$. This implies $\mathrm{Harm}_k^{\mathrm{Aut}(C)} = \langle f_1 \rangle$ for some $f_1 \in \mathrm{Harm}_k$. That is,

$$\mathrm{Harm}_k^{\mathrm{Aut}(C)} \ni f = Af_1 \text{ for } A \in \mathbb{R}.$$

The harmonic weight enumerator for $k = 2$ and $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$ is

$$[C = d_{16}^+] \quad w_{C,f} = \frac{336}{13}Ax^{12}y^4 - \frac{672}{13}Ax^8y^8 + \frac{336}{13}Ax^4y^{12}.$$

$$[C = e_8^2] \quad w_{C,f} = \frac{672}{13}Ax^{12}y^4 - \frac{1344}{13}Ax^8y^8 + \frac{672}{13}Ax^4y^{12}.$$

Therefore the Conjecture 2.1 is true for $n = 16$ and $k = 1, 2, 3$. But for $n = 16$, we need further computation to establish the Conjecture 2.1 true.

References

[1] C. Bachoc, On harmonic weight enumerators of binary codes, *Des. Codes Cryptogr.* **18** (1999), no. 1-3, 11-28.

[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] J. H. Conway, N.J.A. Sloane, *Sphere Packings Lattices and Groups*, third edition, Springer, New York, 1999.

[4] P. Delsarte, Hahn polynomials, discrete harmonics, and t-designs, *SIAM J. Appl. Math.* **34** (1978), no. 1, 157-166.

[5] P. Delsarte, J.-M. Goethals, and J. J. Seidel, Spherical codes and designs, Geom. Dedicata 6 (1977), 363–388.

[6] A. Erdélyi, W. Magnus, F. Oberhettinger, F.G. Tricomi, *Higher transcendental functions. Vols. II*, McGraw-Hill Book Company, Inc., New York-Toronto-London, 1953.

[7] E. Freitag, *Siegelsche Modulfunktionen. (German)*, Grundlehren der Mathematischen Wissenschaften, 254. Springer-Verlag, Berlin, 1983.

[8] E. Freitag, *Singular modular forms and theta relations*, Lecture Notes in Mathematics, 1487. Springer-Verlag, Berlin, 1991.

[9] Y. Funada, master thesis, *Osaka University* (2016, March).

[10] E. Hecke, Mathematische Werke, Vandenhoeck & Ruprecht, Göttingen, 1983.

[11] S. Karlin, and J. McGregor, *The Hahn polynomials, formulas and an application*, Scripta Math., Vol.26 (1961), 33-46.

[12] H. Klingen, *Introductory lectures on Siegel modular forms*, Cambridge Studies in Advanced Mathematics, 20. Cambridge University Press, Cambridge, 1990.

[13] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, Berlin/New York, 1984.

[14] J. Macwilliams, A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42** (1963), 79-84.

[15] T.Miyake *Modular forms*, Translated from the Japanese by Yoshitaka Maeda. Spring-Verlag, Berlin, 1989.

[16] T. Moriyama, Talk at Hokuriku Number theory seminar, (26 May, 2016).

[17] T. Moriyama, Theta series constructed from invariant E_8-Harmonic polynomials.

[18] C. Pache, Shells of selfdual lattices viewed as spherical designs, International Journal of Algebra and Computation 5 (2005), 1085–1127.

[19] B. Schoeneberg, Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen. (German) Math. Ann. 116 (1939), no. 1, 511–523.

[20] B. Schoeneberg, "Elliptic modular functions: an introduction," Translated from the German by J. R. Smart and E. A. Schwandt. Die Grundlehren der mathematischen Wissenschaften, Band 203. Springer-Verlag, New York-Heidelberg, 1974.

[21] B. B. Venkov, Even unimodular extremal lattices. (Russian) Algebraic geometry and its applications. Trudy Mat. Inst. Steklov. 165 (1984), 43–48; translation in Proc. Steklov Inst. Math. 165 (1985) 47–52.

[22] B. B. Venkov, "Boris Réseaux et designs sphériques," (French) [Lattices and spherical designs] Réseaux euclidiens, designs sphériques et formes modulaires, 10–86, Monogr. Enseign. Math., 37, Enseignement Math., Geneva, 2001.

「符号のサポートデザインについて」
On the support designs of codes

中空　大幸
(Hiroyuki Nakasora)
神戸学院大学
(Kobe Gakuin University)

1　序文

本稿は講演の内容に加筆したものである。また，一連の論文 [7], [9],[10] を基に構成している。

C を binary code とする。$c = (c_1, c_2, \ldots, c_n) \in C$, $(c_i \in \mathbb{F}_2)$ に対して，$supp(c) = \{i : c_i \neq 0\}$ を c の support と呼ぶ。$X = \{1, 2, \ldots, n\}$，$\mathcal{B}$ を weight w のコードワード全体の support とする。すると，結合構造 $D_w = (X, \mathcal{B})$ を C の weight w の support design という。この support design について次の Assmus-Mattson の定理 [1] が重要である。

Theorem 1.1 ([1]). *Let C be an $[n, k, d]$ linear code over $\mathbb{F}_q$ and $C^\perp$ be the dual $[n, n-k, d^\perp]$ code. Denote by n_0 the largest integer $\leq n$ such that $n_0 - \frac{n_0+q-2}{q-1} < d$, and define $n_0^\perp$ similarly for the dual code $C^\perp$. Suppose that for some integer $t, 0 < t < d$, there are at most $d - t$ non-zero weights w in $C^\perp$ such that $w \leq n - t$. Then:*

(1) *the support design for any weight u, $d \leq u \leq n_0$ in C is a t-design;*

(2) *the support design for any weight w, $d^\perp \leq w \leq \min\{n - t, n_0^\perp\}$ in $C^\perp$ is a t-design.*

ある linear code C の support design D_w が Assmus-Mattson の定理によって t-design $(t > 0)$ となるならば，その符号を applicable to the Assmus–Mattson theorem と呼ぶ。

ここで，D_w について次のような定義を与える。

$$\delta(C) := \max\{t \in \mathbb{N} \mid \forall w, D_w \text{ is a } t\text{-design}\}$$
$$s(C) := \max\{t \in \mathbb{N} \mid \exists w, \text{ s.t. } D_w \text{ is a } t\text{-design}\}$$

この定義から明らかに $\delta(C) \leq s(C)$ である。2016 年の我々の論文 [9] において次のような問題を提起した。

Problem 1.2. $s(C)$ の上限を求めよ。

Problem 1.3. $\delta(C) < s(C)$ となる場合はどこで起こり得るか？

Problem 1.2 について，$t \geq 6$ の t-design の実例は現在知られていない。これら 2 つの問題に対して，まずは極めて重要な符号のクラスである extremal Type II code について調べた。

2 Extremal Type II codeのサポートデザイン

長さ n の extremal Type II code を C とする。ここで C の minimum weight は $d(C) = 4[n/24]+4$ である。また，Zhang [14] 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 $m \geq 164$ で非存在が知られている。

$\delta(C)$ と $s(C)$ の値の可能性について N. Horiguchi, T. Miezaki and H. Nakasora [7] と T. Miezaki and H. Nakasora [9] から次の結果を得ている。

Theorem 2.1. *Let C be an extremal Type II code of length n.*

(1) *If $n = 24m$, then $\delta(C) = s(C) = 5$ or $\delta(C) = s(C) = 7$.*

(2) *If $n = 24m + 8$, then $\delta(C) = s(C) = 3$ or $5 \leq \delta(C) \leq s(C) \leq 7$.*

(3) *If $n = 24m + 16$, then $\delta(C) = s(C) = 1$ or $3 \leq \delta(C) \leq s(C) \leq 5$.*

Problem 1.2 について，extremal Type II code において $s(C) \leq 7$ である。Problem 1.3 について，Theorem 2.1(1) の n が 24 の倍数のときは $\delta(C) < s(C)$ となる場合が起きないことが分かる。次の命題で $\delta(C) < s(C)$ が起きる可能性がある場合について述べる。

Proposition 2.2. *If the case $\delta(C) < s(C)$ occurs, then one of the following holds:*

(1) *$n = 24m + 8$, $m = 58$, $\delta(C) = 6$ and $s(C) = 7$ with $w = n/2$;*

(2) *$n = 24m + 16$, $m \in \{10, 23, 79, 93, 118, 120, 123, 125, 142\}$, $\delta(C) = 4$ and $s(C) = 5$ with $w = n/2$.*

注意として extremal Type II code において，$\delta(C) < s(C)$ となる実例は知られていなく未解決問題である。

$\delta(C) < s(C)$ の場合の重要性は,「符号とサポートデザインの関係」と次に述べる「格子と spherical t-design の関係」との類似性によることが挙げられる。

Theorem 2.3 ([13])**.** *Let L be an extremal Type II lattice of rank n and $L_{2m} := \{x \in L : (x, x) = 2m\}$. If $L_{2m} \neq \phi$, then L_{2m} is a spherical*

$$\begin{cases} 11\text{-}design & (n \equiv 0 \pmod{24}), \\ 7\text{-}design & (n \equiv 8 \pmod{24}), \\ 3\text{-}design & (n \equiv 16 \pmod{24}). \end{cases}$$

例えば，$(E_8)_{2m}$ は spherical 7-design である。そして，次の Ramanujan τ 函数との関係がある。

Theorem 2.4 ([13])**.** *$(E_8)_{2m}$ is a spherical 8-design if and only if $\tau(m) = 0$, where*

$$q\prod_{m=1}^{\infty}(1-q^m)^{24} = \sum_{m=0}^{\infty}\tau(m)q^m.$$

有名な Lehmer 予想が関係している。

Conjecture 2.5 ([8])**.** For all m,

$$\tau(m) \neq 0.$$

この Lehmer 予想を extremal Type II code とサポートデザインに言い換えると

$$\delta(C) = s(C)$$

である。よって，$\delta(C) < s(C)$ はどこで起こっているのか? extremal Type II code の枠組を外して $\delta(C) < s(C)$ の起こる場合について探索を始めた。

3 長さ 48 の triply even code のサポートデザイン

知られている $\delta(C) < s(C)$ の例は 1984 年の Dillion-Schatz [6] がある。それは binary $[2^{2m}, 2m+2]$ code C でその weight enumerator は

$$1 + 2^{2m}x^{2^{2m-1}-2^{m-1}} + (2^{2m+1}-2)x^{2^{2m-1}} + 2^{2m}x^{2^{2m-1}+2^{m-1}} + x^{2m}$$

である。weight $2^{2m-1} \pm 2^{m-1}$ に対しては support 2-design で，weight 2^{2m-1} に対しては support 3-design となっている。すなわち，$2 = \delta(C) < s(c) = 3$ である。我々は Dillion-Schatz の符号とは本質的に異なる例を長さ 48 の triply even codes の中から見つけた。

長さ 48 の triply even codes は [4] で分類がされている。別宮先生のウェブサイト [3] で用いられている記号 ⟨Dimension, Code Id, [Generators]⟩ を本稿では ⟨Dimension, [Code Id]⟩ で表す。

Proposition 3.1. *If a triply even code of length* 48 C *is applicable to the Assmus–Mattson theorem, then one of the following:*

(A) $\langle 7, [144]\rangle$, $\langle 8, [129, 130, 131, 132, 133]\rangle$,
$\langle 9, [59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 1109, 1712, 1714, 1716, 1960]\rangle$,
$\langle 10, [16, 17, 18, 19, 20, 21, 22, 549, 550, 554, 1001, 1245, 1246, 1247]\rangle$,
$\langle 11, [6, 7, 154, 520]\rangle$, $\langle 12, [3]\rangle$, $\langle 13, [1]\rangle$.

(B) $\langle 2, [1]\rangle, \langle 3, [4]\rangle, \langle 4, [7]\rangle, \langle 5, [12]\rangle$

Proof. Assmus-Mattson の定理の条件 $d^\perp - t = |\{wt(u) : u \in C, wt(u) \neq 0, 48\}|$ において，
(A) は $4 - t = 3$ より，$t = 1$ を得る。
(B) は $2 - t = 1$ より，$t = 1$ を得る。

□

主定理は次である。

Theorem 3.2. *Let C be a triply even code length* 48 *in Proposition 3.1. Let D_w and $D_w^\perp$ be the support t-design of weight w of C and $C^\perp$.*

(1) *For all w, D_w and $D_w^\perp$ are* 1*-designs.*

(2) *If C is a code in Proposition 3.1 (A) except for $\langle 13, [1]\rangle$, $D_6^\perp$ (and also $D_{42}^\perp$) is a* 2*-design but is not a* 3*-design. For the other cases, D_w and $D_w^\perp$ are not* 2*-designs.*

この定理は最初はコンピュータ (MAGMA) の計算によって確認した。しかし，weight 6 に起きている現象の原因が分かり，証明は理論的に行った。この証明の概要については次節で述べる。この定理において重要な例を 2 つ挙げる。

Example 3.3. Proposition 3.1 (A) の 1 つである $\langle 7, [144]\rangle$ の triply even code を C とする。その weight enumerator は

$$W_C(x,y) = x^{48} + 3x^{32}y^{16} + 120x^{24}y^{24} + 3x^{16}y^{32} + y^{48}$$

である。C の双対符号 $C^{\perp}$ は Miyamoto's moonshine code [12] と呼ばれる。

Proposition 3.1 と Theorem 3.2 から，すべての weight w に対して，D_w と $D_w^{\perp}$ は 1-design である。さらに，双対符号の weight 6 は特別で $D_6^{\perp}$ は 2-$(48, 6, 2520)$ design となっている。($D_{42}^{\perp}$ は 2-$(48, 6, 2520)$ design の complement である。)

Example 3.4. Theorem 3.2 (2) で除いた $\langle 13, [1]\rangle$ の triply even code は extended doubling $\mathcal{D}(\mathcal{G}_{24})$ である。また，$\mathrm{Aut}\,\mathcal{D}(\mathcal{G}_{24}) = 2^{12}.M_{24}$ である。$\mathcal{D}(\mathcal{G}_{24}) = C'$ とおく。その weight enumerator は

$$W_{C'}(x,y) = x^{48} + 759x^{32}y^{16} + 6672x^{24}y^{24} + 759x^{16}y^{32} + y^{48}$$

である。

MacWilliams 恒等式

$$W_{C'^{\perp}}(x,y) = 2^{-13}W_{C'}(x+y, x-y)$$

から双対符号の $C'^{\perp}$ のコードワードの個数を計算すると weight 6 のコードワードの個数が $A_6^{\perp} = 0$ である。よって，$D_6^{\perp}$ はブロックの集合が空集合である自明なデザインであることが分かる。双対符号の weight 6 を除いたすべての weight w に対して，Proposition 3.1 と Theorem 3.2 から，D_w と $D_w^{\perp}$ は 1-design である。

表 1 には Theorem 3.2 で得られる双対符号の weight 6 の support 2-deign についてまとめている。また，三枝崎氏のホームページにはこれらの符号とデザインに関するデータ [11] が与えられている。

4 Theorem 3.2 の証明概要

今節では Theorem 3.2 の証明の概要について述べる。詳しい証明は [10] を参照頂きたい。まず，準備として harmonic weight enumerator の定義から始める。

Definition 4.1. 長さ n の binary code を C，$f \in \mathrm{Harm}_k$ とする。C と f に関する harmonic weight enumerator は

$$W_{C,f}(x,y) = \sum_{\mathbf{c}\in C} \widetilde{f}(\mathbf{c}) x^{n-\mathrm{wt}(\mathbf{c})} y^{\mathrm{wt}(\mathbf{c})}$$

である。

次に harmonic weight enumerator と t-design の関係は次の Delsarte [5] による。

表 1: weight 6 の support 2-deign について

次元	[Code Id] Weight distribution (i, A_i) for $A_i \neq 0$	2-(v, k, λ) 個数
7	[144] $(0,1),(16,3),(24,120),(32,3),(48,1)$	2-$(48,6,2520)$ 1
8	[129,130,131,132,133] $(0,1),(16,15),(24,224),(32,15),(48,1)$	2-$(48,6,1240)$ 5
9	[59,60,61,62,63,64,65,66,67,68,69,1109,1712,1714,1716,1960] $(0,1),(16,39),(24,432),(32,39),(48,1)$	2-$(48,6,600)$ 16
10	[16,17,18,19,20,21,22,549,550,554,1001,1245,1246,1247] $(0,1),(16,87),(24,848),(32,87),(48,1)$	2-$(48,6,280)$ 14
11	[6,7,154,520] $(0,1),(16,183),(24,1680),(32,183),(48,1)$	2-$(48,6,120)$ 4
12	[3] $(0,1),(16,375),(24,3344),(32,375),(48,1)$	2-$(48,6,40)$ 1
13	[1] $(0,1),(16,759),(24,6672),(32,759),(48,1)$	- 0

Theorem 4.2 ([5]). *D_w が t-design になることと，任意の $f \in \mathrm{Harm}_k$, $1 \leq k \leq t$ に対して $\sum_{b \in D_w} \widetilde{f}(b) = 0$ を満たすことは同値である。*

Bachoc [2] は次のような MacWilliams 型の恒等式を示した。

Theorem 4.3 ([2]). *$W_{C,f}(x,y)$ を binary code C と degree k の harmonic function f に関する harmonic weight enumerator とする。*

$$W_{C,f}(x,y) = (xy)^k Z_{C,f}(x,y)$$

そこで，$Z_{C,f}$ は degree $n-2k$ の homogeneous polynomial である。すると，次を満たす。

$$Z_{C^\perp,f}(x,y) = (-1)^k \frac{2^{n/2}}{|C|} Z_{C,f}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$$

C を Proposition 3.1 (A) の triply even code とする。ただし $\langle 13, [1] \rangle$ を除く。すると，Assmus-Mattson の定理よりすべての weight w に対して，D_w と $D_w^\perp$ は 1-design である。この時 $D_6^\perp$ が 2-design になることを示す。

$W_{C,f}(x,y)$ を C と degree 2 の harmonic function f に関する harmonic weight enumerator とする。

$$\begin{aligned} W_{C,f}(x,y) &= \sum_{\mathbf{c} \in C} \widetilde{f}(c) x^{48-wt(c)} y^{wt(c)} \\ &= ax^{32}y^{16} + bx^{24}y^{24} + ax^{16}y^{32} \\ &= (xy)^2(ax^{30}y^{14} + bx^{22}y^{22} + ax^{14}y^{30}) \\ &= (xy)^2 Z_{C,f}(x,y) \end{aligned}$$

ここで，$a, b \neq 0$ である。

Theorem 4.3 より，つぎの等式をみたす係数 a', b' が存在する。

$$\begin{aligned} Z_{C^\perp,f}(x,y) &= (-1)^2 \frac{2^{24}}{|C|} Z_{C,f}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) \\ &= a'(x+y)^{30}(x-y)^{14} + b'(x+y)^{22}(x-y)^{22} + a'(x+y)^{14}(x-y)^{30} \end{aligned}$$

$C^\perp$ は minimum weight 4 より，$Z_{C^\perp,f}$ の中の x^{44} の係数は 0 である。よって，$b' = -2a'$ を得る。ゆえに，

$$\begin{aligned} &W_{C^\perp,f}(x,y) \\ &= (xy)^2 \left(a'(x+y)^{30}(x-y)^{14} - 2a'(x+y)^{22}(x-y)^{22} + a'(x+y)^{14}(x-y)^{30}\right) \end{aligned}$$

すると，直接的な計算により $W_{C^\perp,f}$ の中の $x^{42}y^6$ の係数は 0 であることを得る。Theorem 4.2 より，$D_6^\perp$ は 2-design である。

参考文献

[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory Ser. A* **6** (1969), 122-151.

[2] C. Bachoc, On harmonic weight enumerators of binary codes, *Des. Codes Cryptogr.* **18** (1999), no. 1-3, 11-28.

[3] K. Betsumiya, DATABASE: Triply even codes of length 48, `http://www.st.hirosaki-u.ac.jp/~betsumi/triply-even/`

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

[5] P. Delsarte, Hahn polynomials, discrete harmonics, and t-designs, *SIAM J. Appl. Math.* **34** (1978), no. 1, 157-166.

[6] J. F. Dillon, J. R. Schatz, "Block designs with the symmetric difference property", in: Proc. of the NSA Mathematical Sciences Meetings, (Ward R. L. Ed.), pp. 159-164, 1987.

[7] N. Horiguchi, T. Miezaki and H. Nakasora, On the support designs of extremal binary doubly even self-dual codes, *Des. Codes Cryptogr.*, **72** (2014), 529-537.

[8] D. H. Lehmer, The vanishing of Ramanujan's $\tau(n)$, *Duke Math. J.* **14** (1947), 429–433.

[9] T. Miezaki and H. Nakasora, An upper bound of the value of t of the support t-designs of extremal binary doubly even self-dual codes, *Des. Codes Cryptogr.*, **79** (2016), 37-46.

[10] T. Miezaki and H. Nakasora, The support designs of the triply even codes of length 48, *J. Combin. Designs*, to appear.

[11] T. Miezaki, Tsuyoshi Miezaki's website:
https://sites.google.com/site/tmiezaki/data

[12] M. Miyamoto, A new construction of the Moonshine vertex operator algebras over the real number field, *Ann. of Math.*, **159** (2004), 535–596.

[13] B. B. Venkov, Even unimodular extremal lattices (Russian), *Algebraic geometry and its applications. Trudy Mat. Inst. Steklov.* **165** (1984), 43–48; translation in *Proc. Steklov Inst. Math.* **165** (1985) 47–52.

[14] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999), 277-286.

Bordered complex Hadamard matrices and strongly regular graphs

Takuya Ikuta (Kobe Gakuin University) and
Akihiro Munemasa (Tohoku University)

1 Introduction

We classify bordered complex Hadamard matrices whose core is contained in the Bose-Mesner algebra of a strongly regular graph. We denote by r, s the nontrivial eigenvalues of a strongly regular graph with parameter (k, λ, μ), where $r > 0$, $s \leq -1$. As a consequence of our classification, we have the following: (i) If the core is a conference graph, then there are two kinds of complex Hadamard matrices. One is of Butson-type whose entries are 4-th roots of unity, and the other is a complex Hadamard matrix whose entries contain a complex number which is not a root of unity. (ii) If the core is a strongly regular graph with parameters $(2r^2, r^2, r^2)$, where r is an integer with $r \geq 2$, then we have a (real) Hadamard matrix. (iii) If neither (i) nor (ii) occurs, then we have $k = \frac{-2rs \pm 1 + h}{2}$, where $h = \sqrt{4r(r+1)s(s+1)+1} \in \mathbb{Z}$. No example is known for this case. In this report, we mainly consider the essential case (iii).

A complex Hadamard matrix is a square matrix W of order n which satisfies $W\overline{W}^\top = nI$ and all of whose entries are complex numbers of absolute value 1. In this paper, we consider a complex Hadamard matrix of the form:

$$W = \begin{pmatrix} 1 & \boldsymbol{e} \\ \boldsymbol{e}^\top & W_1 \end{pmatrix}, \tag{1}$$

where $\boldsymbol{e}$ is the all 1's row vector of size n. The submatrix W_1 is said to be a core of W. In [5] J. Seberry constructed a complex Hadamard matrix W whose entries are 4-th roots of unity, and the core W_1 is contained in the Bose–Mesner algebra of a conference graph. And, in [4] S. N. Singh and Om Prakash Dubey constructed a Hadamard matrix W whore core W_1 is contained in the Bose–Mesner algebra of strongly regular graph with parameters $(2r^2, r^2, r^2)$. As a natural problem, assuming W_1 is contained in the Bose–Mesner algebra of a strongly regular graph, we are interested in whether other complex Hadamard matrices arise or not.

Let X be a finite set with n elements, and let $\mathfrak{X} = (X, \{R_i\}_{i=0}^2)$ be a symmetric

2-class association scheme with the first eigenmatrix $P = (P_{i,j})_{\substack{0\le i\le 2\\ 0\le j\le 2}}$:

$$\begin{pmatrix} 1 & k_1 & k_2 \\ 1 & r & -(r+1) \\ 1 & s & -(s+1) \end{pmatrix}, \tag{2}$$

where $r, s \in \mathbb{R}$, $r \ge 0$, and $s \le -1$. We let $\mathfrak{A}$ denote the Bose–Mesner algebra spanned by the adjacency matrices A_0, A_1, A_2 of $\mathfrak{X}$. A strongly regular graph Γ with parameters (k, λ, μ) is equivalent to $\mathfrak{X}$, via the correspondence R_1 equal to the set of edges and R_2 equal to the set of non-edges. In this paper, by exchanging R_1 and R_2, we may assume that $r + s \ge -1$ without loss of generality.

Let

$$W_1 = w_0 A_0 + w_1 A_1 + w_2 A_2 \in \mathfrak{A}. \tag{3}$$

and w_0, w_1, w_2 ($w_1 \ne w_2$) are complex numbers of absolute value 1. Then we have the following.

Theorem 1. *Suppose that $r, s \in \mathbb{R}$, $r \ge 0$, $s \le -1$, and $r + s \ge -1$. Let W_1 be the matrix defined in* (3)*. If the matrix W defined by* (1) *is a complex Hadamard matrix, then one of the following holds.*

(i) *Γ is a conference graph on $(2r+1)^2$ vertices, and*

  (a) $(w_0, w_1, w_2) = (-1, \pm i, \mp i)$, *or*

  (b) $(w_0, w_1, w_2) = (1, \frac{-1 \pm i\sqrt{4r^4+8r^3+4r^2-1}}{2r(r+1)}, \frac{-1 \mp i\sqrt{4r^4+8r^3+4r^2-1}}{2r(r+1)})$.

(ii) $(k_1, s) = (2r^2, -r)$, *and* $(w_0, w_1, w_2) = (1, -1, 1)$.

(iii) $r + s > 0$, $h = \sqrt{4r(r+1)s(s+1)+1} \in \mathbb{Z}$, *and* $k_1 = (-2rs \pm 1 + h)/2$.

Conversely, if (i) *or* (ii) *hold, then the matrix* (1) *is a complex Hadamard matrix.*

Remark 1. Strongly regular graphs having parameter (ii) in Theorem 1 are given by $(k, \lambda, \mu) = (2r^2, r^2, r^2)$. These strongly regular graphs were already considered in [4]. The list of strongly regular graphs up to $1,300$ vertices are given in Brouwer's database [2]. According to that, strongly regular graphs with parameters $(2r^2, r^2, r^2)$ exist for $r = 2, \ldots, 10, 12, \ldots, 16, 18$, are unknown for $r = 11, 17$. No example is known for strongly regular graph with parameter (iii) in Theorem 1.

2 Preliminaries

Let $(X, \{R_i\}_{i=0}^d)$ be a symmetric d-class association scheme with the first eigenmatrix $P = (P_{i,j})_{\substack{0\le i\le d\\ 0\le j\le d}}$. (For more general and detailed theory of association schemes, see [1].) We let $\mathfrak{A}$ denote the Bose–Mesner algebra spanned by the adjacency matrices $A_0, A_1, \ldots, A_d$ of $\mathfrak{X}$. Then the adjacency matrices are expressed as

$$A_j = \sum_{i=0}^{d} P_{i,j} E_i \quad (j = 0, 1, \ldots, d), \tag{4}$$

where $E_0 = \frac{1}{n}J, E_1, \ldots, E_d$ are the primitive idempotents of $\mathfrak{A}$.

In (1), let

$$W_1 = \sum_{j=0}^{d} w_j A_j \in \mathfrak{A} \tag{5}$$

and $w_0, \ldots, w_d$ are complex numbers of absolute value 1.

Define

$$\beta_k = \sum_{j=0}^{d} w_j P_{k,j} \quad (k = 0, 1, \ldots, d). \tag{6}$$

By (4), (5) and (6) we have

$$W_1 = \sum_{k=0}^{d} \beta_k E_k. \tag{7}$$

Let X_j $(0 \le j \le d)$ be indeterminates. For $k = 1, 2, \ldots, d$, let e_k be the polynomial defined by

$$e_k = \prod_{h=0}^{d} X_h \left(\sum_{j=0}^{d} P_{k,j}^2 + \sum_{0 \le j_1 < j_2 \le d} P_{k,j_1} P_{k,j_2} \left(\frac{X_{j_1}}{X_{j_2}} + \frac{X_{j_2}}{X_{j_1}} \right) - (n+1) \right), \tag{8}$$

and e_0 be the polynomial defined by

$$e_0 = 1 + \sum_{j=0}^{d} k_j X_j. \tag{9}$$

Then we have the following.

Lemma 1. *The following statements are equivalent:*

(i) *the matrix W defined by* (1) *is a complex Hadamard matrix,*

(ii) $\beta_k \overline{\beta_k} = n + 1$ *for* $k = 1, \ldots, d$, *and* $1 + \sum_{j=0}^{d} k_j w_j = 0$,

(iii) $(w_j)_{0 \le j \le d}$ *is a common zero of* e_k $(k = 0, \ldots, d)$.

Let W_1 be the matrix defined by (3), and let W be the matrix defined by (1). Consider the polynomial ring

$$\mathscr{R} = \mathbb{C}[X_0, X_1, X_2].$$

Then by (8) and (9) we have

$$\begin{aligned}
e_0 =& 1 + X_0 + k_1 X_1 + k_2 X_2, && (10)\\
e_1 =& -\left((r+1)X_1 - rX_2\right) X_0^2 - \left(r(r+1)(X_1 - X_2)^2 + (k_1 + k_2) X_1 X_2\right) X_0 \\
&+ (rX_1 - (r+1)X_2) X_1 X_2, && (11)\\
e_2 =& -\left((s+1)X_1 - sX_2\right) X_0^2 - \left(s(s+1)(X_1 - X_2)^2 + (k_1 + k_2) X_1 X_2\right) X_0 \\
&+ (sX_1 - (s+1)X_2) X_1 X_2. && (12)
\end{aligned}$$

Let $\mathcal{I}$ be the ideal of $\mathscr{R}$ generated by (10), (11), and (12). We write

$$\boldsymbol{w} = (w_0, w_1, w_2) \tag{13}$$

for brevity. Let

$$w_j = a_j + b_j i \tag{14}$$

for $j = 0, 1, 2$, where $a_j, b_j \in \mathbb{R}$, $a_j^2 + b_j^2 = 1$, and $i^2 = -1$. We write

$$\boldsymbol{w'} = (a_0 + b_0 i, a_1 + b_1 i, a_2 + b_2 i) \tag{15}$$

for brevity.

Lemma 2. *Let W_1 be the matrix defined by* (3)*, and let W be the matrix defined by* (1)*. Then the matrix W is a complex Hadamard matrix if and only if $\boldsymbol{w}$ is a common zero of the polynomials e_k $(k = 0, 1, 2)$.*

3 Strongly regular graphs

In this section, we consider a symmetric 2-class association scheme and a strongly regular graph. Let $\mathfrak{X} = (X, \{R_i\}_{i=0}^2)$ be a symmetric 2-class association scheme with the first eigenmatrix (2). We have the following three cases in (2): (a) $r + s \geq 0$, (b) $r + s = -1$, (c) $r + s \leq -2$. Suppose that (c) holds. Then the eigenvalues of R_2 satisfy $-(r + 1) - (s + 1) \geq 0$. By exchanging R_1 and R_2, we may assume that $r + s \geq -1$ without loss of generality. Therefore we only consider the two cases (a) and (b). Under this assumption, we have

$$k_2 \geq 2. \tag{16}$$

Indeed, if $k_2 = 1$, then R_2 is a matching, and hence the eigenvalues satisfy $-r-1 = -1$ and $-s - 1 = 1$. This implies $r + s = -2$, contrary to our assumption.

A strongly regular graph Γ with parameters (k, λ, μ) is equivalent to $\mathfrak{X}$, via the correspondence R_1 equal to the set of edges and R_2 equal to the set of non-edges. The complement of a strongly regular graph is also a strongly regular graph. The three parameters of Γ are $k(= k_1) = p_{1,1}^0$, $\lambda = p_{1,1}^1$, and $\mu = p_{1,1}^2$. Then we have

$$\mu = k_1 + rs, \tag{17}$$

$$\lambda = r + s + \mu, \tag{18}$$

$$k_2\mu = k_1(k_1 - \lambda - 1), \tag{19}$$

$$n = 1 + k + k(k - \lambda - 1)/\mu. \tag{20}$$

A conference graph is a strongly regular graph Γ satisfying one of the following two equivalence conditions:

(i) $k_1 = 2r(r + 1)$, $r + s = -1$,

(ii) $m_1 = m_2$.

We remark that the eigenvalues r, s of a strongly regular graph Γ are integers unless Γ is a conference graph. If Γ is a conference graph, then $r = \frac{-1+\sqrt{2k_1+1}}{2}$ and $s = \frac{-1-\sqrt{2k_1+1}}{2}$. In any case,

$$rs \in \mathbb{Z}. \tag{21}$$

By (17), (18) and (19), we have

$$\frac{k_2\mu}{k_1} = -(r+1)(s+1). \tag{22}$$

This shows that $s = -1$ is equivalent to $\mu = 0$. In fact this occurs precisely when Γ is a disjoint union of complete graphs.

4 Properties of the polynomials $L(X)$, $M(X)$, and $S(X)$

Throughout this section, suppose that $r, s \in \mathbb{R}$, $r \geq 0$, $s < -1$, and $r + s \geq -1$. Define the polynomials $L(X)$, $M(X)$, and $S(X)$ as follows:

$$\begin{aligned} L(X) &= X^3 + \frac{4rs - r - s + 3}{2}X^2 + \frac{-4rs(r+s-1)+1}{2}X \\ &\quad + \frac{rs(r^2 + 2(3s+1)r + s^2 + 2s + 2)}{2}, \end{aligned} \tag{23}$$

$$M(X) = L(X) - 4(X + rs)^2, \tag{24}$$

$$S(X) = s_4X^4 + s_3X^3 + s_2X^2 + s_1X + s_0, \tag{25}$$

where

$$\begin{aligned} s_4 &= (r+s+1)^2, \\ s_3 &= 4sr^3 + 8s(s+1)r^2 + (4s^3 + 8s^2 + 8s + 2)r + 2s + 2, \\ s_2 &= 2s(2s-1)r^4 + 2s(s+1)(4s-3)r^3 + 2s(2s^3 + s^2 + 6s + 4)r^2 \\ &\quad - 2s(s+1)(s^2 + 2s - 6)r + 1, \\ s_1 &= -2rs(2sr^4 + 6s(s+1)r^3 + (6s^3 - 4s^2 - 8s - 1)r^2 \\ &\quad + 2(s+1)(s^3 + 2s^2 - 6s - 1)r - s^2 - 2s - 2), \\ s_0 &= r^2s^2(r^4 + 4(s+1)r^3 + (22s^2 + 28s + 8)r^2 \\ &\quad + 4(s+1)(s^2 + 6s + 2)r + (s^2 + 2s + 2)^2). \end{aligned}$$

We put

$$\alpha_\pm = \frac{r+s-1}{2} \pm \frac{\sqrt{(s-1)^2 - 6rs + r(r-2)}}{2}, \tag{26}$$

$$\beta_\pm = -rs - \frac{1}{2} \pm \frac{\sqrt{4r(r+1)s(s+1)+1}}{2}, \tag{27}$$

$$\gamma_\pm = \frac{r+s+3}{2} \pm \frac{\sqrt{r^2 + 2(5s+3)r + (s+3)^2}}{2}, \tag{28}$$

$$\delta = -rs + \sqrt{r(r+1)s(s+1)}. \tag{29}$$

Then $\alpha_\pm$, $\beta_\pm$, $\delta \in \mathbb{R}$. By (23), (24), and (25) we have

$$L(X)^2 - \frac{S(X)}{4} = (X-\alpha_-)(X-\alpha_+)(X-\beta_-)^2(X-\beta_+)^2, \tag{30}$$

$$M(X)^2 - \frac{S(X)}{4} = (X-\gamma_-)(X-\gamma_+)(X-(\beta_-+1))^2(X-(\beta_++1))^2. \tag{31}$$

Lemma 3. *We have the following:*

(i) $\alpha_\pm, \beta_- + 1 < -rs$.

(ii) $-rs < \beta_+ < \delta < \beta_+ + 1$.

(iii) *If* $\gamma_\pm \in \mathbb{R}$ *then* $\gamma_\pm < -rs$.

Lemma 4. *We have*

(i) $L(-rs) = M(-rs) = \frac{r(r+1)s(s+1)((2s+1)r+s+1)}{2} < 0$,

(ii) $\sqrt{S(-rs)} = r(r+1)s(s+1)(r+s+1)$.

5 The case $r + s \geq 0$

In this section, we suppose that $r, s \in \mathbb{Z}$, $r \geq 2$, $s \leq -2$, and $r + s \geq 0$. We consider properties of the polynomials (23), (24), and (25).

Lemma 5. *We have the following:*

(i) $L(X)$ *has exactly one real root* ζ *in* $(-rs, \infty)$, *and* $\beta_+ \leq \zeta < \delta$,

(ii) $L(x) < 0$ *for* $-rs < x < \zeta$, *and* $L(x) \geq 0$ *for* $\zeta \leq x$.

Lemma 6. *We have the following:*

(i) $M(X)$ *has exactly one real root* η *in* $(-rs, \infty)$, *and* $\delta < \eta \leq \beta_+ + 1$,

(ii) $M(x) \leq 0$ *for* $-rs < x \leq \eta$, *and* $M(x) > 0$ *for* $\eta < x$.

5.1 The case $r + s > 0$

Throughout this subsection, we suppose that $r \geq 3$, $s \leq -2$, and $r + s > 0$. Let $u = r + s$. Then $u \in \mathbb{Z}$ and

$$1 \leq u \leq r - 2. \tag{32}$$

Let $h = \sqrt{4r(r+1)(r-u)(r-u-1)+1}$.

Lemma 7. *The polynomial $S''(X)$ has two distinct real roots:*

$$\tau_\pm = \frac{c_1 \pm \sqrt{c_2}}{6(u+1)^2}, \tag{33}$$

where

$$c_1 = 3(u+1)^2(2r(r-u)-1) + 3(r(r+1)+(r-u)(r-u-1)), \tag{34}$$
$$c_2 = 12r(r+1)u(u+2)(u^2+2u-2)(r-u)(r-u-1) + 3(u+1)^2. \tag{35}$$

Lemma 8. *Let $\tau_\pm$ be the real number defined by* (33)*. Then $\tau_\pm < \beta_+$.*

Define

$$\begin{aligned} g_1 &= 4u(u+2)(u(u+2)-2)r(r+1)(r-u)(r-u-1) + (u+1)^2, \\ g_2 &= 2r(r+1)(r-u)(r-u-1) \\ &\quad \times (8u(u+2)r(r+1)(r-u)(r-u-1) + 7u(u+2) - 1) - 1, \\ g_3 &= 16u(u+2)r(r+1)(r-u)(r-u-1) - 1. \end{aligned}$$

Lemma 9. *We have $g_1 > 0$, $g_2 > 0$, and $g_3 > 0$.*

Lemma 10. *The polynomial $S(X)$ has exactly two real roots, say, ξ_1, ξ_2, and $\beta_+ < \xi_1 < \delta < \xi_2 < \beta_+ + 1$. Moreover, both ξ_1 and ξ_2 are simple.*

Lemma 11. *We have $L(\beta_+) \le 0$ and $M(\beta_+ + 1) \ge 0$.*

Lemma 12. *We have $\xi_1 < \zeta < \eta < \xi_2$.*

Lemma 13. *Let $A = (-rs, \xi_1]$ and $B = [\xi_2, \infty)$. Then we have the following:*

(i) *$S(x) \ge 0$ for $x \in \mathbb{R}$ holds if and only if $x \in A \cup B$.*

(ii) *For $x \in A \cup B$,*

(a) *$M(x) \le \frac{\sqrt{S(x)}}{2} \le L(x)$ holds if and only if $x = \beta_+ + 1$,*

(b) *$M(x) \le \frac{-\sqrt{S(x)}}{2} \le L(x)$ holds if and only if $x = \beta_+$.*

6 Proof of Theorem 1

In this section, we prove (iii) in Theorem 1. We assume that $r, s \in \mathbb{R}$, $r \ge 1$, $s \le -1$, and $r + s \ge 0$. Let W_1 be the matrix defined by (3), and W be the matrix defined by (1). We suppose that the matrix W defined by (1) is a complex Hadamard matrix.

Recall that $\mathcal{I}$ is the ideal of $\mathscr{R}$ generated by (10), (11), and (12).

Lemma 14. *We have $s < -1$ and $k_1 + rs > 0$.*

Lemma 15. *Let a_j be the real numbers defined by* (14) *for $j = 0, 1, 2$. Then a_0, a_1, and a_2 satisfy the following:*

$$(L(k_1) - M(k_1))^2 a_1^2 + 2(L(k_1)^2 - M(k_1)^2)a_1 + (L(k_1) + M(k_1))^2 - S(k_1) = 0, \quad (36)$$

$$2(k_1 + rs)^2 rsa_0 - 2k_1^2(k_1 + rs)^2 a_1 + h_0 = 0, \quad (37)$$

$$2(k_1 + rs)^3 a_1 - 2(k_1 + rs)r(r + 1)s(s + 1)a_2 + \ell_0 = 0, \quad (38)$$

where

$$\begin{aligned} h_0 &= -k_1^5 + (r + s - 2rs + 1)k_1^4 + 3rs(r + s + 1)k_1^3 \\ &\quad - rs((r + s)^2 + 2(r + s) - 1)k_1^2 + 4r^2s^2k_1 + 2r^3s^3, \\ \ell_0 &= k_1(k_1 - r - s - 1)(k_1^2 + 2rsk_1 - rs(r + s + 1)). \end{aligned}$$

Lemma 16. *We have the following:*

(i) $S(k_1) \geq 0$,

(ii) $M(k_1) \leq \frac{\sqrt{S(k_1)}}{2} \leq L(k_1)$ *or* $M(k_1) \leq \frac{-\sqrt{S(k_1)}}{2} \leq L(k_1)$.

Lemma 17. *Suppose that $r + s > 0$. Then we have* (iii) *in* Theorem 1.

Proof. By (i) in Lemma 14 and Lemma 17 we have $k_1 \in A \cup B$. By (ii) (a) and (b) in Lemma 14 and (ii) in Lemma 17 we have $k_1 \in \{\beta_+, \beta_+ + 1\}$. Then by (27) we have

$$\sqrt{4r(r + 1)s(s + 1) + 1} \in \mathbb{Z}.$$

Therefore we have (iii) in Theorem 1. □

References

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

[2] A. E. Brouwer, *Parameters of Strongly Regular Graphs*, `https://www.win.tue.nl/~aeb/graphs/srg/srgtab.html`

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

[4] S. N. Singh and Om Prakash Dubey, *On the parameters of* 2*-class Hadamard association schemes*, International Journal of Mathematics and Technology 11 (2), (2014), 112–116.

[5] J. Wallis, *Complex Hadamard matrices*, Linear and Multilinear Algebra 1 (3), (1973), 257–272.

Vertex operator algebras and modular linear differential equations

有家 雄介 *
鹿児島大学教育学部

1 はじめに

C_2-cofinite かつ有理的な頂点作用素代数 (VOA) の既約加群の指標の生成する空間が $SL_2(\mathbb{Z})$ の作用で不変になることはよく知られている ([12]). この定理の証明の過程で, Zhu は, 頂点作用素代数の既約加群の指標はある種の微分方程式を満たすことを証明している. この微分方程式が本稿で扱うモジュラー微分方程式 (modular linear differential equation, MLDE) である. モジュラー微分方程式とは, セール微分

$$\vartheta_k(f(\tau)) = q\frac{d}{dq}f(\tau) - \frac{k}{12}E_2(\tau)f(\tau), \qquad \vartheta_0^i = \vartheta_{2(i-1)} \circ \vartheta_0^{i-1}$$

とウエイト $2(d-i)$ のモジュラー形式 $P_i(\tau)$ を用いて

$$\vartheta_0^d(f(\tau)) + \sum_{i=0}^{d-1} P_i(\tau)\vartheta_0^i(f(\tau)) = 0$$

と表せる微分方程式である. ここで, $\mathbb{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}$, $q = e^{2\pi i\tau}$ で, $E_{2k}(\tau)$ は定数項が 1 になるように正規化したウエイト $2k$ のアイゼンシュタイン級数である.

以下では, 頂点作用素代数 V は CFT 型のもののみ考える. つまり, $V = \bigoplus_{n=0}^{\infty} V_n$ かつ $\dim V_0 = 1$ を仮定する. 正整数 d に対して, その指標が d 階のモジュラー微分方程式の解となるような頂点作用素代数はどのくらい存在するか, という問題を考える. $d = 1$ のときは, 解は定数しかないので, 対応する頂点作用素代数は自明なものに限る. $d = 2$ の場合には, 対応する頂点作用素代数は, 中心電荷 $-22/5$ の単純 Virasoro VOA

* arike@edu.kagoshima-u.ac.jp

$L(-22/5,0)$ と単純リー代数 $A_1, A_2, G_2, D_4, F_4, E_6, E_7, E_8$ に付随するレベル 1 のアフィン頂点作用素代数であることが [8, 9] において示されている．

$d = 3$ の場合には対応する頂点作用素代数は無限個現れることが知られている ([1])．そこで，ウエイト 1 の空間が自明であるようなものだけを考えると，中心電荷の候補は表 1 のように有限個であることがわかる ([6, 10, 11, 3, 5])．さらに，中心電荷が 164/5 と 236/7 の場合を除いて対応する頂点作用素代数の候補も見つかっている ([6, 10, 11])．

No.	中心電荷	VOA
1	$-68/7$	$L(-68/7,0)$
2	$1/2$	$L(1/2,0)$
3	$-44/5$	$L(-22/5,0)\otimes L(-22/5,0)$
4	8	$V^+_{\sqrt{2}E_8}$
5	16	$V^+_{BW_{16}}$
6	47/2	$VB^\natural_{\mathbb{Z}}$
7	24	$V^\natural$
8	32	$V_L^+ \oplus (V_L)_T^+$ (L: extremal)
9	164/5	?
10	236/7	?
11	40	$V_L^+ \oplus (V_L)_T^+$ (L: extremal)

表 1　中心電荷と対応する VOA

本稿では，永友清和氏との共同研究により得られた以下の定理について報告する．

Theorem 1 ([2])**.** No.9 と No. 10 に対応する C_2-cofinite かつ有理的な頂点作用素代数は存在しない．

2　階数 3 の MLDE と中心電荷

まず，表 1 の中心電荷を得る方法を説明する．詳しい計算や証明などは [3] を参照されたい．

階数 3 の MLDE は，ウエイト 4 のモジュラー形式は $E_4(\tau)$ の定数倍，ウエイト 6 のモジュラー形式は $E_6(\tau)$ の定数倍であることを用いると $\vartheta_0^3(f) + xE_4(\tau)\vartheta_0(f) + yE_6(\tau)f = 0$ となる．頂点作用素代数 V の指標 $Z_V(\tau) = q^{-c/24}(1 + 0\cdot q + mq^2 + \cdots)$ がこの MLDE

の解になることを仮定する．ここで，V の中心電荷 c は有理数であると仮定する．また，$m = \dim V_2$ である．このとき，$Z_V(\tau)$ を MLDE に代入して最初の 3 つの項の係数を比べると，

$$576cx - 13824y + c^3 + 12c^2 = 0, \tag{1}$$
$$480cx + 24192y - c^2 - 24c = 0 \tag{2}$$

および，

$$c^3m - 132c^2m - 864c^2 + 576cmx + 5760cm + 1244160cx - 41472c - 27648y - c^2 - 24c = 0 \tag{3}$$

となる．(1) と (2) から

$$x = \frac{-7c^2 - 80c + 96}{5952}, \qquad y = \frac{5c^3 + 66c^2 + 144c}{214272} \tag{4}$$

となる．これを (3) に代入して整理すると，有理数 c と正整数 m の関係式

$$70c^3 - 1496m - c^2(2m - 955) + 2c(55m + 1195) = 0 \tag{5}$$

が得られる．この方程式を満たす組 $(c, m) \in \mathbb{Q} \times \mathbb{Z}_{>0}$ は 41 個あることがわかる ([3, §4])．それぞれの c に対して (4) を用いて対応する MLDE を決定し，その Z_V に対応する解の係数を求め，高い次数の係数として分数や負の数が現れるものを除外すると表 1 の c のリストが得られる．

3　解の表示

中心電荷が 164/5 と 236/7 の場合に現れる MLDE はそれぞれ

$$\vartheta_0^3(f) - \frac{169}{100}E_4(\tau)\vartheta_0(f) + \frac{1271}{1080}E_6(\tau)f = 0, \tag{6}$$
$$\vartheta_0^3(f) - \frac{149}{64}E_4(\tau)\vartheta_0(f) + \frac{93869}{74088}E_6(\tau)f = 0 \tag{7}$$

である．フロベニウスの方法を用いて，例えば (6) の解の係数を求めると，

$$\begin{aligned} f_1(\tau) &= q^{-41/30}(1 + 90118q^2 + 53459408q^3 + \cdots), \\ f_2(\tau) &= q^{5/6}(10168 + 3704965q + 338289360q^2 + \cdots), \\ f_3(\tau) &= q^{31/30}(615164 + 152560672q + 11717226984q^2 + \cdots) \end{aligned} \tag{8}$$

となる．

Proposition 2 ([3])**.** 82 次の斉次多項式 $k_1(x,y)$ と $k_2(x,y)$ が存在して，

$$f_1(\tau) = k_1(\phi,\psi), \quad f_2(\tau) = k_2(\phi,\psi), \quad f_3(\tau) = k_1(\psi,-\phi)$$

となる．ここで，

$$\phi(\tau) = q^{-1/60}\prod_{n=0}^{\infty}\frac{1}{(1-q^{5n+1})(1-q^{5n+4})}, \quad \psi(\tau) = q^{11/60}\prod_{n=0}^{\infty}\frac{1}{(1-q^{5n+2})(1-q^{5n+3})}.$$

この命題に現れる関数 ψ は，中心電荷 $-22/5$ の単純 Virasoro VOA $L(-22/5,0)$ の指標であり，ϕ は $L(-22/5,0)$ の最低ウエイト $-1/5$ の既約加群の指標である．この関数の S 変換はよく知られているように，

$$\begin{pmatrix}\psi(-1/\tau)\\ \phi(-1/\tau)\end{pmatrix} = \begin{pmatrix} -2\sqrt{\frac{1}{5}\left(\frac{\sqrt{5}}{8}+\frac{5}{8}\right)} & 2\sqrt{\frac{1}{5}\left(\frac{5}{8}-\frac{\sqrt{5}}{8}\right)} \\ 2\sqrt{\frac{1}{5}\left(\frac{5}{8}-\frac{\sqrt{5}}{8}\right)} & 2\sqrt{\frac{1}{5}\left(\frac{\sqrt{5}}{8}+\frac{5}{8}\right)} \end{pmatrix}\begin{pmatrix}\psi(\tau)\\ \phi(\tau)\end{pmatrix}. \tag{9}$$

である (例えば [7] 等を参照)．そこで，$k_1(x,y)$ と $k_2(x,y)$ の具体形と (9) を組み合わせることにより，

$$\begin{pmatrix}f_1(-1/\tau)\\ f_2(-1/\tau)\\ f_3(-1/\tau)\end{pmatrix} = \begin{pmatrix} \left(\sqrt{5}+5\right)/10 & 10\sqrt{5} & \left(5-\sqrt{5}\right)/10 \\ 1/25\sqrt{5} & -1/\sqrt{5} & -1/25\sqrt{5} \\ \left(5-\sqrt{5}\right)/10 & -10\sqrt{5} & \left(\sqrt{5}+5\right)/10 \end{pmatrix}\begin{pmatrix}f_1(\tau)\\ f_2(\tau)\\ f_3(\tau)\end{pmatrix} \tag{10}$$

となることがわかる．

中心電荷が 236/7 の場合，すなわち MLDE が (7) の場合も，解を中心電荷 $-68/7$ の単純 Virasoro VOA の既約加群の指標の多項式として表すことができる．この多項式による表示を用いて S 変換を求めることができる ([3])．

4 Theomre 1 の証明

ここでは，中心電荷が 164/5 の場合の証明を解説する．中心電荷が 236/7 の場合も同様である．

まず，証明に用いる quantum dimension と global dimension について述べる．V を頂点作用素代数とし，M をその既約加群とする．V の指標 $Z_V(\tau)$ と M の指標 $Z_M(\tau)$ がともに $\mathbb{H}$ 上の正則関数であると仮定する．このとき，

$$\mathrm{qdim}_V M = \lim_{y\to 0}\frac{Z_M(\sqrt{-1}y)}{Z_V(\sqrt{-1}y)}$$

を M の **quantum dimension** という．さらに，V の既約加群が有限個であるとし，$M^0, \dots, M^d$ を既約加群の完全代表系であるとする．このとき，

$$\mathrm{glob}(V) = \sum_{i=0}^{d} (\mathrm{qdim}_V M^i)^2$$

を V の **global dimension** という．

Proposition 3 ([4])**.** V を CFT 型の単純，C_2-cofinite で有理的な頂点作用素代数とし，$M^0 = V$, M^1, ..., M^d を既約加群の完全代表系とする．$M^1, \dots, M^d$ の最低ウエイトがすべて正であるとすると，以下が成り立つ．
(a) $\mathrm{qdim}_V M^i \geq 1$.
(b) $\mathrm{glob}(V) = 1/(S_{00})^2$. ここで，$S_{00}$ は $Z_V(-1/\tau)$ を $Z_{M^i}(\tau)$ の線形結合で表したときの $Z_V(\tau)$ の係数である．

Theorem 1 は，C_2-cofinite かつ有理的で，指標が f_1 であるような V が存在することを仮定して，(10) と Proposition 3 を用いて $\mathrm{glob}(V)$ を 2 通りに計算することで矛盾を導き出すことにより示される．実際，そのような V が存在すれば，V は Proposition 3 の仮定を満たすことが簡単に証明できる (詳しくは [2] を参照してください)．このとき (10) と Proposition 3 (b) より

$$\mathrm{glob}(V) = \left(\frac{10}{\sqrt{5}+5}\right)^2 = 1.90983...$$

となることがわかる．一方，やはり (10) より V は 3 つ以上既約加群を持つことがわかるので，Proposition 3 (a) より

$$\mathrm{glob}(V) \geq 3$$

となって矛盾を得る．

参考文献

1. Arike, Y., Kaneko, M., Nagatomo, K. and Sakai, Y.: Affine vertex operator algebras and modular linear differential equations, Lett. Math. Phys. **106** 693–718 (2016)
2. Arike, Y., Nagatomo, K.: Central charges 164/5 and 236/7, preprint.

3. Arike, Y., Nagatomo, K. and Sakai, Y.: Characterization of the simple Virasoro vertex operator algebras with 2 and 3-dimensional space of characters, Contemp. Math. **695** 175–204 (2017)
4. Dong, C., Jiao, X. and Xu, F.: Quantum dimensions and quantum Galois theory, Trans. Amer. Math. Soc. **365** No. 12 6441–6469 (2013)
5. Hampapura, H. R. and Mukhi, S.: Two-dimensional RCFT's without Kac-Moody symmetry, JHEP **07** 138 (2016)
6. Höhn, G.: Conformal designs based on vertex operator algebras, Adv. Math. **217** 2301–2335 (2008)
7. Iohara, K. and Koga, Y.: Representation theory of the Virasoro algebra, Springer-Verlag, London, (2011)
8. Mathur, S. D., Mukhi, S. and Sen, A.: On the classification of rational conformal field theories, Phys. Letter B. **213** 303–308 (1988)
9. Mathur, S. D., Mukhi, S. and Sen, A.: Reconstruction of conformal field theories from modular geometry on the torus Nucl. Phys. B. **318** 483–540 (1988)
10. Tuite, M. P.: Exceptional vertex operator algebras and the Virasoro algebra, Contemp. Math. **497** 213–225 (2009)
11. Tuite, M. P. and Van, H. D.: On exceptional vertex operator (super) algebras, In: Mason G., Penkov I., Wolf J. A. (eds), Developments and Retrospectives in Lie Theory: Algebraic Methods, Dev. Math. **38** 351–384. Springer, Cham (2014) arXiv:1401.5229v1.
12. Zhu, Y.: Modular invariance of characters of vertex operator algebras, J. Amer. Math. Soc. **9** 237–302 (1996)

On automorphism groups of the holomorphic VOAs associated with Niemeier lattices and the -1-isometries

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@tohoku.ac.jp

本稿では Niemeier 格子 VOA と -1-自己同型の持ち上げに $\mathbb{Z}_2$-軌道体構成法を適用して得られる中心電荷 24 の正則頂点作用素代数 (VOA) の自己同型群に関する最近の結果 [Sh19+] について述べる. 講演で述べた中心電荷 24 の正則 VOA の分類に関する解説は [LS19] や [Sh18] にあるため, 本稿では省略する.

1 背景

概ね完成した中心電荷 24 の正則 VOA の分類[注 1]を用いて次の問題に取り組んでいる.

- (共形重み 1 の空間が 0 でない) 中心電荷 24 の正則 VOA [注 2]の自己同型群を決定せよ.

中心電荷 24 の正則 VOA V が $V_1 \neq 0$ を満たすとする. このとき, V_1 は 0-積でリー代数構造を持ち, V_1 の内部自己同型群 $\mathrm{Inn}(V_1)$ は VOA の内部自己同型群 $\mathrm{Inn}(V)$ に自然に拡張される. 一方で, V_1 のリー代数構造は分かっているため, $\mathrm{Inn}(V_1)$ も分かっている. したがって, $\mathrm{Aut}(V)$ における $\mathrm{Inn}(V_1)$ 以外の構造を決定したい. そこで, 次の群構造を決定することを目標とする:

- $K(V) := \{g \in \mathrm{Aut}(V) \mid g = id \text{ on } V_1\}$;
- $\mathrm{Out}(V) := \mathrm{Aut}(V)/(K(V)\mathrm{Inn}(V))$.

ここで $\mathrm{Inn}(V)/(K(V) \cap \mathrm{Inn}(V)) \cong \mathrm{Inn}(V_1)$ を満たし, $\varphi : \mathrm{Aut}(V) \to \mathrm{Aut}(V_1)$ を制限写像とすると, $K(V) = \mathrm{Ker}\ \varphi$, $\mathrm{Out}(V) \cong \mathrm{Im}\ \varphi/\mathrm{Inn}(V_1)$ であることを注意しておく.

[注 1] 共形重み 1 の空間 V_1 が 0 である中心電荷 24 の正則 VOA はムーンシャイン VOA と同型, という予想 ([FLM88]) だけが未解決である.

[注 2] 本稿で扱う正則 VOA は有理的 (表現が完全可約), C_2-有限 ($V/\langle u_{(-2)}v \mid u, v \in V\rangle$ が有限次元), CFT 型 (V_0 が一次元), 自己双対 (V の contragredient 加群が V と同型) を仮定している.

2 Niemeier 格子 VOA

N をルートを持つ Niemeier 格子とし, V_N を付随する正則格子 VOA とする. Q を N のルート格子とする. $(V_N)_1 = (V_Q)_1$ であり, $(V_N)_1$ が生成する部分 VOA は V_Q となる. さらに, V_N は V_Q の N/Q で次数付けされた単純カレント拡大である. $g \in K(V_N)$ とすると, V_Q 上 $g = 1$ となる. よって, g は V_N の既約 V_Q-部分加群上にスカラーで作用し, N/Q 上の既約指標と見なせる. したがって, $K(V_N) \subset (N/Q)^*$ となる. ここで $(N/Q)^*$ は既約指標のなすアーベル群であり, $(N/Q)^* \cong N/Q$ である. 明らかに $(N/Q)^* \subset K(V_N)$ であるため,

$$K(V_N) \cong (N/Q)^* \cong N/Q$$

となる. 特に, $K(V_N) \subset \mathrm{Inn}(V_N)$ である.[注 3]

V_N の自己同型群は [DN99] において計算されている.

命題 2.1. $\mathrm{Aut}(V_N) = \mathrm{Inn}(V_N)O(\hat{N})$. ただし $O(\hat{N}) \cong \mathbb{Z}_2^{24}.O(N)$.

$O(\hat{N})$ の正規部分群 $\mathbb{Z}_2^{24}$ は $\mathrm{Inn}(V_N)$ の部分群である. さらに Q の Weyl 群 $W(Q)$ の元の持ち上げは $\mathrm{Inn}(V_N)$ の元で実現できる. したがって,

$$\mathrm{Out}(V_N) \cong \mathrm{Aut}(V_N)/\mathrm{Inn}(V_N) \cong O(N)/W(Q) \cong \mathrm{Aut}(N/Q).$$

ここで $\mathrm{Aut}(N/Q)$ は glue code N/Q の自己同型群である.

N がリーチ格子 Λ の場合は, $(V_\Lambda)_1$ は 24 次元の abelian Lie algebra であり, $\mathrm{Inn}(V_\Lambda) \subset K(V_\Lambda)$ である. さらに $\mathrm{Aut}(V_\Lambda) \cong (\mathbb{C}^\times)^{24}.O(\Lambda)$ であり, $K(V_\Lambda) = \mathrm{Inn}(V_\Lambda) \cong (\mathbb{C}^\times)^{24}$ かつ $\mathrm{Out}(V_\Lambda) \cong O(\Lambda)$ である.

3 V_N の $\mathbb{Z}_2$-軌道体構成法と主結果

V_N を Niemeier 格子 N に付随する格子 VOA とする. $\theta \in \mathrm{Aut}(V_N)$ を $-1 \in O(N)$ の持ち上げとする. $V_N^+ = \{v \in V_N \mid \theta(v) = v\}$ は V_N の部分 VOA となる. $V_N(\theta)$ を既約 θ-twisted V_N-加群とし, $V_N(\theta)_\mathbb{Z}$ で $V_N(\theta)$ の整数重みの部分空間とする. すると $V_N(\theta)_\mathbb{Z}$ は既約 V_N^+-加群となる.

定理 3.1 ([FLM88, DGM96, EMS19+])**.** *V_N^+-加群 $V = V_N^+ \oplus V_N(\theta)_\mathbb{Z}$ は $\mathbb{Z}_2$-次数付けを持つ V_N^+ の単純カレント拡大としての正則 VOA 構造を持つ.*

N が長さ 24 の自己双対重偶二元符号から構成法 A で得られている場合は V は Niemeier 格子 VOA と同型になる.[注 4] このような N が 9 通りある. また, $N = \Lambda$ の時は V はムー

[注 3] V が中心電荷 24 の正則 VOA の時は $K(V) \subset \mathrm{Inn}(V)$ と予想している.

[注 4] V はその自己双対重偶二元符号からリーチ格子を作る方法で作った Niemeier 格子に付随する VOA と同型. 対応の詳細は [DGM96] にある.

ンシャイン VOA である. したがって, このように構成される正則 VOA の中で, 自己同型群が調べられていないものが $14(=24-9-1)$ 個ある.

[Sh19+] の主結果は, これら 14 個の正則 VOA について $K(V)$ と $\mathrm{Out}(V)$ を決定したことである. 実際には $(V_N)_1=\bigoplus_{i=1}^s \mathfrak{g}_i$ を既約分解とし, $\mathrm{Out}(V)$ の代わりに

$$\mathrm{Out}(V)_1=\{g\in\mathrm{Out}(V)\mid g(\mathfrak{g}_i)=\mathfrak{g}_i\ 1\le\forall i\le s\},\quad \mathrm{Out}_2(V)=\mathrm{Out}(V)/\mathrm{Out}(V)_1$$

を決定している. 詳細は表 1 にある. 以後, どのように決定したかについて解説していく.

表 1: $K(V)$, $\mathrm{Out}_1(V)$ and $\mathrm{Out}_2(V)$

No.	Q	V_1	$K(V)$	$\mathrm{Out}_1(V)$	$\mathrm{Out}_2(V)$
2	A_2^{12}	$A_{1,4}^{12}$	$\mathbb{Z}_2$	1	M_{12}
5	A_3^8	$A_{1,2}^{16}$	$\mathbb{Z}_2^5$	1	$\mathbb{Z}_2^4:L_4(2)$
12	A_4^6	$B_{2,2}^6$	$\mathbb{Z}_2$	1	Sym_5
16	$A_5^4D_4$	$A_{3,2}^4A_{1,1}^4$	$\mathbb{Z}_4\times\mathbb{Z}_2^3$	$\mathbb{Z}_2$	$\mathbb{Z}_2^4:\mathrm{Sym}_3$
23	A_6^4	$B_{3,2}^4$	$\mathbb{Z}_2$	1	Alt_4
25	$A_7^2D_5^2$	$D_{4,2}^2B_{2,1}^4$	$\mathbb{Z}_2^3$	1	$\mathrm{Sym}_2\times\mathrm{Sym}_4$
29	A_8^3	$B_{4,2}^3$	$\mathbb{Z}_2$	1	Sym_3
31	$A_9^2D_6$	$D_{5,2}^2A_{3,1}^2$	$\mathbb{Z}_4^2$	$\mathbb{Z}_2$	$\mathrm{Sym}_2\times\mathrm{Sym}_2$
38	E_6^4	$C_{4,1}^4$	$\mathbb{Z}_2$	1	Sym_4
39	$A_{11}D_7E_6$	$D_{6,2}B_{3,1}^2C_{4,1}$	$\mathbb{Z}_2^2$	1	Sym_2
41	A_{12}^2	$B_{6,2}^2$	$\mathbb{Z}_2$	1	Sym_2
47	$A_{15}D_9$	$D_{8,2}B_{4,1}^2$	$\mathbb{Z}_2^2$	1	Sym_2
50	$A_{17}E_7$	$D_{9,2}A_{7,1}$	$\mathbb{Z}_8$	$\mathbb{Z}_2$	1
57	A_{24}	$B_{12,2}$	$\mathbb{Z}_2$	1	1

4 既約ルート格子 R に付随する V_R^+

次の定理は既知の可能性があるが, [Sh19+] では証明をつけた.

定理 4.1. R を既約ルート格子とし, $R\ncong A_1$ とする. このとき, V_R^+ はある半単純リー代数 $(V_R^+)_1$ に付随する正整数レベルの *simple affine VOA* と同型である.

[DM06] によって, $(V_R^+)_1$ の生成する部分 VOA は正整数レベルの simple affine VOA と同型となる. そこで, [FLM88] の V_Λ^+ の生成系を求める方法を用いて, $(V_R^+)_1$ が V_R^+ を生成することを確認した.

具体的な対応とレベルは表 2 にある.

表 2: $(V_R^+)_1$ のリー代数構造と V_R^+ のレベル k_R

R	$(V_R^+)_1$	level
A_2	A_1	4
A_{2n} $(n \geq 2)$	B_n	2
A_{2n-1} $(n \geq 2)$	D_n	2
D_{2n} $(n \geq 2)$	$D_n \oplus D_n$	1
D_{2n+1} $(n \geq 2)$	$B_n \oplus B_n$	1
E_6	C_4	1
E_7	A_7	1
E_8	D_8	1

注意 4.2. $(V_{A_1}^+)_1$ は 1 次元の *abelian* リー代数である．そして, $\langle (V_{A_1}^+)_1 \rangle$ は *Heisenberg VOA* となり, $V_{A_1}^+$ を生成しない.

5 主定理の概略

N を 3 章で考えた 14 個の Niemeier 格子のいずれかとする．Q を N のルート格子とし, $N = \bigoplus_{i=1}^t Q_i$ を既約ルート格子の直和への分解とする．$V = V_N^+ \oplus V_N(\theta)_{\mathbb{Z}}$ とし, $V_1 = \mathfrak{g} = \bigoplus_{i=1}^s \mathfrak{g}_i$ を単純イデアルの直和とする．U を $V_1 (= (V_N^+)_1)$ で生成された部分 VOA とする.

5.1 $K(V)$

$\mathfrak{g}$ の Cartan subalgebra をとり, $P^\vee$ を coweight 格子とする．$x \in P^\vee$ に対して, $\sigma_x = \exp(2\pi\sqrt{-1}x_{(0)})$ とおく．明らかに, $\sigma_x \in K(V)$ である.

$g \in K(V)$ とする．$U \cong \bigotimes_{i=1}^t (V_{Q_i}^+)$ となり, V_N^+ は既約 U-加群の有限個の直和となる．U 上 $g = id$ なので, 既約 U-加群 M に対して, g-共役 $M \circ g$ は M と同型である．また, V_N^+ と $V_N(\theta)_{\mathbb{Z}}$ にはそれぞれ unwisted 型と twisted 型の既約 $V_{Q_i}^+$-加群しか現れないので, $g(V_N^+) = V_N^+$, $g(V_N(\theta)_{\mathbb{Z}}) = V_N(\theta)_{\mathbb{Z}}$ となる．conformal weight を見ることで, 他の二つの既約 V_N^+-加群も g-共役で保たれる．$g_0 = g_{|V_N^+}$ とすると, $V_N^- \circ g_0 \cong V_N^-$ より, g_0 は V_N の自己同型に持ち上がる．さらに, V_N の自己同型群の構造 ([DN99]) を見ることで, $g_0 \in O(\hat{N})/\langle\theta\rangle$ がわかる．さらに, $O(\hat{N})/\langle\theta\rangle$ の部分群として $K(V)/\langle z\rangle$ の構造を具体的に調べることで, $K(V)$ の元は $\{\sigma_x \mid x \in P^\vee\}$ で生成されることがわかる．結論として次を得る.

命題 5.1. $K(V) = \{\sigma_x \mid x \in P^\vee\}$.

さらに, $K(V)$ の群構造を調べることで, 表 1 を得る．この計算では, N/Q を用いた V の U-加群構造の記述を用いる.

5.2 $\mathrm{Out}(V)$

- $\mathrm{Out}_1(V) := \{g \in \mathrm{Out}(V) \mid g(\mathfrak{g}_i) = \mathfrak{g}_i \ 1 \leq \forall i \leq s\}$.
- $\mathrm{Out}_2(V) := \mathrm{Out}(V)/\mathrm{Out}_1(V) \subset \mathrm{Sym}_s$.
- $G_1(N) := \{g \in \mathrm{Aut}(N/Q) \mid g(Q_i) = Q_i \ 1 \leq \forall i \leq t\}$.
- $G_2(N) := \mathrm{Aut}(N/Q)/G_1(N)$.

と定義する. $\mathrm{Out}_1(V)$ が $\mathfrak{g}_i$ の diagram automorphism で生成されており, $G_1(N)$ と $G_2(N)$ は [CS99] で $\mathrm{Aut}(N/Q)$ の記述に用いられている. $\mathrm{Out}_1(V)$ と $\mathrm{Out}_2(V)$ を記述することで, $\mathrm{Out}(V)$ が大まかに分かる.

まず, 表 2 から, 全ての $1 \leq i \leq t$ に対して, $Q_i \notin \{A_{2n-1}, D_{2n}, E_7, E_8 \mid n \geq 3\}$ ならば, $\mathfrak{g}_i$ の diagram automorphism は自明なので, $\mathrm{Out}_1(V) = 1$. また, $O(N)$ が $\mathrm{Aut}(V)$ に持ち上がるので, $G_2(N) \subset \mathrm{Out}_2(V)$ である. さらに, 全ての i に対して, $Q_i \notin \{A_3, D_n \mid n \geq 4\}$ ならば, 各 $(V_{Q_i}^+)_1$ が単純イデアルとなり, $s = t$ と $\mathrm{Out}_2(V) \cong G_2(N)$ を得る. 以上から, 次を得る.

命題 5.2. *$Q \cong A_2^{12}$, A_4^6, A_6^4, A_8^3, E_6^4, A_{12}^2 または A_{24} ならば, $\mathrm{Out}_1(V) = 1$ かつ $\mathrm{Out}_2(V) \cong G_2(N)$.*

残りの 7 個の関しては別の方法を用いる. $N_0 = N \cap (Q/2)$ とすると, $V_{N_0}^+$ は V_N^+ の単純カレント U-部分加群の直和である. ここに現れる単純カレント U-加群の集合を C_N とする. すると, フュージョン積によって, C_N はアーベル群をなす. さらに, $\mathrm{Irr}(\mathfrak{g}_i)_{sc}$ を単純カレント $\langle \mathfrak{g}_i \rangle$-加群の集合とすると, C_N はアーベル群 $\prod_{i=1}^s \mathrm{Irr}(\mathfrak{g}_i)_{sc}$ の部分群となる. $\mathrm{Aut}(\prod_{i=1}^s \mathrm{Irr}(\mathfrak{g}_i)_{sc})$ を置換と, $\mathfrak{g}_i$ の diagram automorphism で生成される群とする. そこで, C_N を環上の符号と見なし, $\mathrm{Aut}(C_N)$ を C_N を保つ $\mathrm{Aut}(\prod_{i=1}^s \mathrm{Irr}(\mathfrak{g}_i)_{sc})$ の部分群とする. 明らかに $\mathrm{Out}(V) \subset \mathrm{Aut}(C_N)$ である. また, $\mathrm{Aut}(C_N)$ は具体的に計算でき, その生成元を $\mathrm{Out}(V)$ から見つけることができる. 実際には $\mathrm{Aut}(V_N^+)$ の持ち上げ ([Sh06]) と, [FLM88] で記述された例外的な自己同型で $\mathrm{Aut}(C_N)$ が生成されることを証明する. したがって, 次を得る.

命題 5.3. *Q が A_3^8, $A_5^4 D_4$, $A_7^2 D_5^2$, $A_9^2 D_6$, $A_{11} D_7 E_6$, $A_{15} D_9$ または $A_{17} E_7$ ならば $\mathrm{Out}(V) = \mathrm{Aut}(C_N)$.*

具体的に $\mathrm{Aut}(C_N)$ を計算することで, 表 1 を得る.

注意 5.4. 一般には $\mathrm{Out}(V)$ と $\mathrm{Aut}(C_N)$ は異なる. 例えば, $Q = A_2^{12}$ のときは, $\mathrm{Out}(V) \cong M_{12}$ だが, $\mathrm{Aut}(C_N) \cong \mathrm{Sym}_{12}$ となる.

これら結果から, $Q \ncong A_3^8$, $A_7^2 D_5^2$ のときは, $\mathrm{Aut}(V)/\langle z \rangle \cong \mathrm{Aut}(V_N^+)$ となり, $Q \cong A_3^8$, $A_7^2 D_5^2$ のときは, $\mathrm{Aut}(V)$ は $\mathrm{Aut}(V_N^+)$ の持ち上げと [FLM88] の例外型の自己同型で生成される.

注意 5.5. *$Q \cong A_3^8$, $A_7^2 D_5^2$ の時, N は自己双対重偶符号 d_6^4, $d_{10} e_7^2$ からリーチ格子の構成と同様な方法で構成される. この場合に [FLM88] の例外的な自己同型の構成が適用できる.*

6　今後の課題

現時点で自己同型群が調べられていない中心電荷 24 の正則 VOA は $32(=70-24-14)$ 個ある. 本稿で述べた [Sh19+] の手法を使うことで計算可能な場合もあるが, 全てを決定することは難しい. 別宮氏と Lam 氏と共同で, [Hö] を用いた (ある程度) 統一的な手法での計算を試みている.

参考文献

[CS99] J.H. Conway and N.J.A. Sloane, Sphere packings, lattices and groups, 3rd Edition, Springer, 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.

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

[DN99] C. Dong and K. Nagatomo, Automorphism groups and twisted modules for lattice vertex operator algebras, *in* Recent developments in quantum affine algebras and related topics (Raleigh, NC, 1998), 117–133, *Contemp. Math.*, **248**, Amer. Math. Soc., Providence, RI, 1999.

[EMS19+] J. van Ekeren, S. Möller and N. Scheithauer, Construction and classification of holomorphic vertex operator algebras, *J. Reine Angew. Math.* (Published Online).

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

[Hö] G. Höhn, On the Genus of the Moonshine Module; arXiv:1708.05990.

[LS19] C.H. Lam and H. Shimakura, 71 holomorphic vertex operator algebras of central charge 24, *Bull. Inst. Math. Acad. Sin. (N.S.)* **14**, (2019), 87–118.

[Sh06] H. Shimakura, The automorphism groups of the vertex operator algebras V_L^+: general case, *Math. Z.* **252** (2006), 849–862.

[Sh18] 島倉裕樹, 中心電荷２４の正則頂点作用素代数の分類について, 第 63 回代数学シンポジウム報告集, (2018) 18–26.

[Sh19+] H. Shimakura, Automorphism groups of the holomorphic vertex operator algebras associated with Niemeier lattices and the $-$ 1-isometries, *J. Math. Soc. Japan.* (to appear).

非退化偶格子に付随する頂点代数の不変部分代数の既約弱加群
(Irreducible weak modules for some fixed point subalgebra of the vertex algebra associated with a non-degenerate even lattice)

田辺顕一朗 (北海道大学大学院理学研究院数学部門)

e-mail : ktanabe@math.sci.hokudai.ac.jp

1 はじめに

V_L を非退化偶格子 $(L, \langle\ ,\ \rangle)$ に付随する頂点代数とする．格子の自己同型 $L \ni \alpha \mapsto -\alpha \in L$ から誘導される V_L の位数 2 の自己同型 θ に対して，θ で固定される元全体からなる部分代数 $V_L^+ = V_L^\theta = \{a \in V_L \mid \theta a = a\}$ を考える．頂点代数の研究において V_L や V_L^+ は重要な役割を担ってきた．例えば，Leech 格子 Λ に対して，V_Λ^+ とその既約加群を用いてムーンシャイン頂点代数 $V^\natural$ が構成されている [10]．あるいは，$\langle\alpha_1, \alpha_1\rangle = \langle\alpha_2, \alpha_2\rangle = 0$, $\langle\alpha_1, \alpha_2\rangle = -1$ で定められる 2 次元ローレンツ格子 $\Lambda_{1,1} = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2$ を考えたとき，$V^\natural$ と $V_{\Lambda_{1,1}}$ とのテンソル積 $V^\natural \otimes_{\mathbb{C}} V_{\Lambda_{1,1}}$ から構成された一般 Kac–Moody Lie 環は，Borcherds によるムーンシャイン予想の解決に決定的な役割を果たした．

頂点代数 V_L と V_L^+ の表現についてみていく．ここで考える頂点代数 V の表現は 2 種類であり，一つは V 加群，もう一つは弱 V 加群である．正確な定義は後で述べるが，大雑把にいって頂点代数 V が作用している $\mathbb{C}$ ベクトル空間 M で，$\mathbb{N}$ 次数付きを課しているものを V 加群 $(M = \oplus_{i=0}^\infty M(i))$，課していないものを弱 V 加群という．V 加群は弱 V 加群になる．V が $\mathbb{Z}$ 次数付きである場合，特に V が頂点作用素代数である場合には，V に付随する Zhu 代数 $A(V)$ の既約加群と，既約 $\mathbb{N}$ 次数付き弱 V 加群とは 1 対 1 に対

応することが Zhu によって示されている [21, Theorem 2.2.1]．既約 V 加群は既約 $\mathbb{N}$ 次数付き弱 V 加群で各斉次空間が有限次元のものであるから，Zhu 代数は既約 V 加群を分類する際の強力な道具となっている．しかし，弱 V 加群についてはそのようなものは知られていない．V_L や V_L^+ は $\mathbb{Z}$ 次数付きの頂点代数であり，特に L が正定値の場合には頂点作用素代数になる．

Dong [4] によって任意の弱 V_L 加群は完全可約であること，既約弱 V_L 加群の完全代表系は $\{V_{\lambda+L} \mid \lambda + L \in L^\perp/L\}$ で与えられることが示されている．ここで $L^\perp$ は L の双対格子である．V_L^+ 加群については以下のことが知られている．まず，既約 V_L^+ 加群は分類されている [3, 8, 12, 19]．さらに，任意の V_L^+ 加群は完全可約であること [1, 6, 20]，および V_L^+ は C_2 余有限であること [2, 18, 11] が示されている．V_L^+ 加群の研究には，V_L^+ の部分代数であるハイゼンベルグ頂点作用素代数 $M(1)^+$ の加群の研究が有用であるため，既約 $M(1)^+$ 加群の分類が [7, 9] においてなされている．

次に弱 V_L^+ 加群について考える．L が正定値の場合，V_L^+ は頂点作用素代数となることから，C_2 余有限性と合わせて [2, Theorem 4.5] により，任意の弱 V_L^+ 加群は完全可約であること，および任意の既約弱加群は既約加群になることが分かる．したがって，L が正定値でない場合が問題となる．この場合，V_L と V_L^+ は頂点作用素代数にならないことはすぐに分かる．V_L^+ 自身が加群ではない既約弱 V_L^+ 加群となることから，弱加群を研究することは自然である．しかし，Zhu 代数のような強力な道具がないため，V_L 以外の頂点代数について，その弱加群のことはこれまでほとんど何も分かっていなかった．V_L^+ については既約弱加群が分類できたということが今回の結果である：

定理 1.1. [17, Theorem 1.1] L を階数が有限の非退化偶格子とする．V_L^+ の既約弱加群は次のいずれかと同型である．

(1) $V_{\lambda+L}^{\pm}$, $\lambda + L \in L^\perp/L$ で $2\lambda \in L$.
(2) $V_{\lambda+L} \cong V_{-\lambda+L}$, $\lambda + L \in L^\perp/L$ で $2\lambda \notin L$.
(3) $\{$(既約 θ-twisted V_L 加群)$^{\pm}\}$.

θ-twisted 加群については説明を省略する．定理にある各弱加群が既約であることは，以前から知られていたことであり，また簡単に証明できる．(3) は V_L^+ 加群になっているが，L が正定値でない場合は (1),(2) はそうではない．L が正定値の場合には，当然のことであるが，この結果は [3, 8] の結果に一致する．

証明は非常に長いため，この文章内で述べることは出来ないが，4 節で一番重要な補題とその証明を述べる．計算機の援用なしには無理だと思われるほど膨大な計算を必要とす

るが，核心のアイディアは単純であり強力である．この手法は他の頂点 (作用素) 代数の (弱) 加群の研究にも有用であると思う．

2　頂点 (作用素) 代数とその加群

頂点代数や弱加群の定義を書いておく．

定義 2.1. 次の条件を満たす $(V, Y, \mathbf{1})$ を頂点代数という:

(1) V は $\mathbb{C}$ 上のベクトル空間.

(2) x を形式的変数として，Y は線形写像

$$\begin{array}{rccc} Y(\ ,x): & V\otimes_{\mathbb{C}} V & \longrightarrow & V((x)) \\ & \cup & & \cup \\ & a\otimes b & \longmapsto & Y(a,x)b \end{array}$$

である．$Y(a,x)b = \sum_{i\in\mathbb{Z}} a_i b x^{-i-1}$ と展開を書く．

(3) $\mathbf{1}\in V$ で $Y(\mathbf{1},x) = \mathrm{id}_V$ (V 上の恒等写像). つまり，$\mathbf{1}_{-1} = \mathrm{id}_V$ と $\mathbf{1}_i = 0\ (i\neq -1)$.
また，$a\in V$ に対して，$Y(a,x)\mathbf{1} = a + \sum_{i\leq -2} a_i \mathbf{1} x^{-i-1} \in V[[x]]$.

(4) $a,b,c\in V$ に対して，$Y(a,b,c|x,y)\in V[[x,y]][x^{-1},y^{-1},(x-y)^{-1}]$ が存在して

$$\begin{aligned} \iota_{x,y} Y(a,b,c|x,y) &= Y(a,x)Y(b,y)c \in V((x))((y)), \\ \iota_{y,x} Y(a,b,c|x,y) &= Y(b,y)Y(a,x)c \in V((y))((x)), \\ \iota_{y,x-y} Y(a,b,c|x,y) &= Y(Y(a,x-y)b,y)c \in V((y))((x-y)). \end{aligned}$$

ここで

$$\begin{aligned} V[[x]] &= \{\sum_{i=0}^{\infty} v_{(i)}x^i \mid v_i\in V\ (i=0,1,\ldots)\}, \\ V[[x,y]] &= \sum_{i,j=0}^{\infty} v_{(i,j)}x^i y^j \mid v_{(i,j)}\in V\ (i,j=0,1,\ldots)\}, \\ V((x)) &= \{\sum_{i\in\mathbb{Z}} v_{(i)}x^i \mid v_{(i)}\in V\ (i\in\mathbb{Z}) \text{ で } v_{(i)}=0 (i\ll 0)\}, \\ V((x))((y)) &= (V((x)))((y)) \end{aligned}$$

等である．$\iota_{x,y} f$ は，f を $|x|>|y|$ と思って形式的に展開したものである．$\iota_{y,x}, \iota_{x,y-x}$ も同様に定める．つまり，$a\in V$ に対して $\iota_{x,y}(a) = \iota_{y,x}(a) = \iota_{y,x-y}(a) = a$ で，$j,k,l\in\mathbb{Z}$

に対して二項展開を用いて

$$\iota_{x,y}\big(x^j y^k (x-y)^l\big) = \sum_{i=0}^{\infty} \binom{l}{i} (-1)^i x^{j+l-i} y^{k+i} \in \mathbb{C}((x))((y)),$$
$$\iota_{y,x}\big(x^j y^k (x-y)^l\big) = \sum_{i=0}^{\infty} \binom{l}{i} (-1)^{l-i} y^{k+l-i} x^{j+i} \in \mathbb{C}((y))((x)),$$
$$\iota_{x,y-x}\big(x^j y^k (x-y)^l\big) = \sum_{i=0}^{\infty} \binom{k}{i} y^{j+k-i} (-1)^l (y-x)^{l+i} \in \mathbb{C}((y))((x-y)) \tag{2.1}$$

と定める．頂点代数 V に対して共形元 (Virasoro 元) ω の存在を課し，いくつかの条件を追加したものを頂点作用素代数 (cf. [10],[13]) という:

定義 2.2. $(V, Y, \mathbf{1})$ を頂点代数で，$\omega \in V$ とする．次の条件を満たすとき，$(V, Y, \mathbf{1}, \omega)$ を**頂点作用素代数**という．

(1) $c_V \in \mathbb{C}$ が存在して，$i, j \in \mathbb{Z}$ に対して

$$[\omega_i, \omega_j] = (i-j)\omega_{i+j-1} + \delta_{i+j-2,0} \frac{i(i-1)(i-2))}{12} c_V \tag{2.2}$$

を満たす．さらに $a \in V$ に対して $\omega_0 a = a_{-2}\mathbf{1}$ となる．

(2) $i \in \mathbb{Z}$ に対して，$V_i = \{a \in V \mid \omega_1 a = ia\}$ とおくと，$V = \oplus_{i\in\mathbb{Z}} V_i$ と直和分解する．さらに各 i に対して $\dim_{\mathbb{C}} V_i < \infty$ で $V_i = 0$ $(i \ll 0)$.

以下 V は頂点代数とし，定義 2.2 の (1) の条件を満たす ω を持つことを仮定する (以下で扱う格子頂点代数 V_L やその部分代数 V_L^+ は，(2) の最後の条件「各 i に対して $\dim_{\mathbb{C}} V_i < \infty$ で $V_i = 0$ $(i \ll 0)$」を除いて定義 2.2 の条件を全て満たしている)．その条件の下で V の弱加群を次のように定める[*1]．

定義 2.3. 次の条件を全て満たす組 (M, Y_M) を**弱 V 加群**という．

(1) M は $\mathbb{C}$ 上のベクトル空間.

(2) $Y_M(\ ,x)$: $\begin{array}{ccc} V \otimes_{\mathbb{C}} M & \longrightarrow & M((x)) \\ \cup & & \cup \\ a \otimes u & \longmapsto & Y_M(a,x)u \end{array}$ は $\mathbb{C}$ 線形写像．$Y_M(a,x)u = \sum_{i\in\mathbb{Z}} a_i u x^{-i-1}$ と展開を書く．

[*1] ω の存在を仮定せずに弱加群の定義を述べることは出来るが，自然な定義を与えるためには少し準備が必要であるため省略する．

(3) $Y_M(\mathbf{1}, x) = \mathrm{id}_M$.

(4) $a, b \in V, u \in M$ に対して，$Y_M(a, b, u|x, y) \in M[[x, y]][x^{-1}, y^{-1}, (x-y)^{-1}]$ が存在して

$$\begin{aligned} \iota_{x,y} Y_M(a, b, u|x, y) &= Y_M(a, x) Y_M(b, y) u \in M((x))((y)), \\ \iota_{y,x} Y_M(a, b, u|x, y) &= Y_M(b, y) Y_M(a, x) u \in M((y))((x)), \\ \iota_{y,x-y} Y_M(a, b, u|x, y) &= Y_M(Y(a, x-y)b, y) u \in M((y))((x-y)) \end{aligned}$$

となる．

次に V 加群の定義を紹介する．

定義 2.4. M を弱 V 加群とする．M が $M = \bigoplus_{i \in \mathbb{C}} M_i, M_i = \{u \in M \mid \omega_1 u = iu\}$ と ω_1 の固有空間に分解し

(1) 任意の $i \in \mathbb{C}$ に対して $\dim_{\mathbb{C}} M_i < \infty$ である．

(2) 任意の $\lambda \in \mathbb{C}$ に対して，$M_{\lambda+n} = 0, \mathbb{Z} \ni n \ll 0$ となっている．

とき，M を V **加群**という．

3 ハイゼンベルグ頂点作用素代数と格子頂点代数

ここでは, 格子頂点代数とその部分代数であるハイゼンベルグ頂点作用素代数, およびそれらの不変部分代数を紹介する．$\mathfrak{h}$ を非退化双線形形式 $\langle -, - \rangle : \mathfrak{h} \times \mathfrak{h} \to \mathbb{C}$ を持つ有限次元 $\mathbb{C}$ ベクトル空間とする．K を記号として $\mathbb{C}$ 上のベクトル空間 $\hat{\mathfrak{h}} = \mathfrak{h} \otimes_{\mathbb{C}} \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}K$ に，リー環の構造を

$$[\alpha(i), \beta(j)] = \delta_{i+j,0} \langle \alpha, \beta \rangle K, \qquad [\hat{\mathfrak{h}}, K] = 0 \tag{3.1}$$

で定める．ここで $\alpha(i) = \alpha \otimes t^i$ $(\alpha \in \mathfrak{h}, i \in \mathbb{Z})$ とおいている．$\hat{\mathfrak{h}}$ の 2 つの部分リー環 $\hat{\mathfrak{h}}^{\geq 0} = \oplus_{i=0}^{\infty} \mathfrak{h} \otimes t^i \oplus \mathbb{C}K$ と $\hat{\mathfrak{h}}^{<0} = \oplus_{i<0} \mathfrak{h} \otimes t^i$ をとる．$\alpha \in \mathfrak{h}$ に対して，一次元 $\hat{\mathfrak{h}}^{\geq 0}$ 加群 $\mathbb{C}e^{\alpha}$ を

$$\beta(i) e^{\alpha} = \begin{cases} \langle \beta, \alpha \rangle e^{\alpha}, & i = 0, \\ 0, & i \geq 1, \end{cases} \ (\beta \in \mathfrak{h}), \qquad K e^{\alpha} = e^{\alpha} \tag{3.2}$$

で定め，$\hat{\mathfrak{h}}$ への誘導加群

$$M(1, \alpha) = \mathscr{U}(\hat{\mathfrak{h}}) \otimes_{\mathscr{U}(\hat{\mathfrak{h}}^{\geq 0})} \mathbb{C}e^{\alpha} \cong \mathscr{U}(\hat{\mathfrak{h}}^{<0}) \otimes_{\mathbb{C}} e^{\alpha}$$

を取る．ここで $\mathscr{U}(\hat{\mathfrak{h}})$ は，$\hat{\mathfrak{h}}$ の包絡環を表している．$\alpha = 0$ のとき，$1 \otimes e^0 \in M(1,0)$ を $\mathbf{1}$ と書いて，$M(1,0)$ の元 $\alpha_1(-j_1)\cdots\alpha_k(-j_k) \otimes e^0$ $(\alpha_1, \ldots, \alpha_k \in \mathfrak{h}, j_1, \ldots, j_k \in \mathbb{Z}_{>0})$ を，$\alpha_1(-j_1)\cdots\alpha_k(-j_k)\mathbf{1}$ と表すことにする．

$\alpha_1, \ldots, \alpha_k \in \mathfrak{h}$ とする．$i_1, \ldots, i_k \in \mathbb{Z}$ に対して写像

$$:\alpha_1(i_1)\cdots\alpha_1(i_k):\, : M(1,\alpha) \to M(1,\alpha)$$

を帰納的に

$$\begin{aligned} :\alpha_1(i_1):&= \alpha_1(i_1), \\ :\alpha_1(i_1)\cdots\alpha_1(i_k):&= \begin{cases} \alpha_1(i_1):\alpha_2(i_2)\cdots\alpha_1(i_k):, & i_1 < 0, \\ :\alpha_2(i_2)\cdots\alpha_1(i_k):\alpha_1(i_1), & i_1 \geq 0 \end{cases} \quad (k \geq 2) \end{aligned}$$

で定め，$\alpha_1(-j_1)\ldots\alpha_k(-j_k)\mathbf{1} \in M(1, \mathbb{C}e^0)$, $(j_1, \ldots, j_k \in \mathbb{Z}_{>0})$ に対して

$$\begin{aligned} &Y_{M(1,\alpha)}(\alpha_1(-j_1)\ldots\alpha_k(-j_k)\mathbf{1}, x) \\ &= :\Big(\frac{1}{(j_1-1)!}\frac{d^{j_1-1}}{dx^{j_1-1}}\sum_{m_1\in\mathbb{Z}}\alpha_1(m_1)x^{-m_1-1}\Big)\cdots\Big(\frac{1}{(j_k-1)!}\frac{d^{j_k-1}}{dx^{j_k-1}}\sum_{m_k\in\mathbb{Z}}\alpha_k(m_k)x^{-m_k-1}\Big): \end{aligned}$$

とおく．例えば

$$\begin{aligned} &Y_{M(1,\alpha)}(\alpha_1(-1)\mathbf{1}, x) = \sum_{m\in\mathbb{Z}}\alpha_1(m)x^{-m-1}, \\ &Y_{M(1,\alpha)}(\alpha_1(-1)\alpha_2(-1)\mathbf{1}, x) = \sum_{m_1,m_2\in\mathbb{Z}} :\alpha_1(m_1)\alpha_1(m_2):x^{-m_1-m_2-2} \\ &= \sum_{m_2\in\mathbb{Z}}\sum_{m_1<0}\alpha_1(m_1)\alpha_2(m_2)x^{-m_1-m_2-2} + \sum_{m_2\in\mathbb{Z}}\sum_{m_1\geq 0}\alpha_2(m_2)\alpha_1(m_1)x^{-m_1-m_2-2} \end{aligned} \tag{3.3}$$

となる．$h^{[1]}, \ldots, h^{[d]}$ を $\mathfrak{h}$ の正規直交基底として

$$\omega = \frac{1}{2}\sum_{i=1}^{d} h^{[i]}(-1)^2\mathbf{1} \in M(1,0) \tag{3.4}$$

とおく．(3.1), (3.2), (3.3) から

$$\begin{aligned} &\omega_1(\alpha_1(-j_1)\ldots\alpha_k(-j_k)e^\alpha) \\ &= (j_1 + \cdots + j_k + \frac{\langle\alpha,\alpha\rangle}{2})\alpha_1(-j_1)\ldots\alpha_k(-j_k)e^\alpha \end{aligned} \tag{3.5}$$

となる．次のことはよく知られている:

定理 3.1. (1) $(M(1,0), Y_{M(1,0)}, \mathbf{1}, \omega)$ は頂点作用素代数となる．頂点作用素代数 $M(1,0)$ を (ランク d の) **ハイゼンベルグ頂点作用素代数**といい，$M(1)$ で表す．

(2) 任意の $\alpha \in \mathfrak{h}$ に対して，$(M(1,\alpha), Y_{M(1,\alpha)})$ は既約 $M(1)$ 加群となる．また $\{M(1,\alpha) \mid \alpha \in \mathfrak{h}\}$ は既約 $M(1)$ 加群の同型類の完全代表系となっている．

$(L, \langle\ ,\ \rangle)$ を階数 d の非退化偶格子とする．$\mathfrak{h} = \mathbb{C} \otimes_{\mathbb{Z}} L$ に対して，ハイゼンベルグ頂点作用素代数 $M(1)$ を考える．$\lambda \in \mathfrak{h}$ に対して，$V_{\lambda+L} = \oplus_{\beta \in \lambda+L} M(1,\beta)$ とおく．

定理 3.2. (1) V_L には，ω を共形元として $M(1)$ 加群構造と両立する頂点作用素代数の構造が一意的に入る．V_L を L に付随する頂点代数 (**格子頂点代数**) という．

(2) 任意の弱 V_L 加群は完全可約であり，$\{V_{\lambda+L} \mid \lambda + L \in L^\perp/L\}$ は既約弱 V_L 加群の同型類の完全代表系となっている [4, Theorem 3.1].

$n \in \mathbb{Z}$ に対して $(V_L)_n = \{a \in V_L \mid \omega_1 a = na\}$ であったから 3.5 より

- L が正定値ならば，任意の $n \in \mathbb{Z}$ に対して $\dim_{\mathbb{C}}(V_L)_n < +\infty$ で，$n < 0$ ならば $\dim_{\mathbb{C}}(V_L)_n = 0$.
- L が正定値でないならば，任意の $n \in \mathbb{Z}$ に対して $\dim_{\mathbb{C}}(V_L)_n = +\infty$.

となる．これより V_L が頂点作用素代数となるためには，L が正定値であることが必要十分であることが分かる．

$\theta : V_L \to V_L$ を，格子の自己同型 $L \ni \alpha \mapsto -\alpha \in L$ から誘導される V_L の位数 2 の自己同型とする．$\alpha_1, \ldots, \alpha_k \in \mathfrak{h}, \alpha \in L$ に対して

$$\theta(\alpha_1(-j_1)\ldots\alpha_k(-j_k)\mathbf{1}) = (-1)^k \alpha_1(-j_1)\ldots\alpha_k(-j_k)\mathbf{1},$$
$$\theta(e^\alpha) \in \mathbb{C}e^{-\alpha}$$

が成り立っている．$\operatorname{rank} L = 1$ の場合は，θ を $\theta(e^\alpha) = e^{-\alpha}$ $(\alpha \in L)$ と取ることが出来る．

$$M(1)^\pm = \{a \in M(1) \mid \theta a = \pm a\},$$
$$V_L^\pm = \{a \in V_L \mid \theta a = \pm a\} \tag{3.6}$$

とおく．$M(1)^+$ は頂点作用素代数，V_L^+ は頂点代数となる．

4　定理の証明について

定理 1.1 の証明は $\operatorname{rank} L = 1$ の場合に限っても長いため，ここで紹介することは出来ない．定理の証明で一番重要な補題 4.2 を紹介することを目標とする．V を頂点代数，M を弱 V 加群，$a \in V \setminus \{0\}, u \in M \setminus \{0\}$ として整数 $\epsilon(a,u)$ を

$$a_{\epsilon(a,u)}u \neq 0, \quad a_i u = 0 \ ({}^{\forall} i > \epsilon(a,u)) \tag{4.1}$$

で定める．定理 1.1 および補題 4.2 の証明のアイデアは，$M(1)^+$ または V_L^+ の生成元に対して計算機を用いて関係式 $R = 0$ を十分にたくさん見つけ，適当な $n \in \mathbb{Z}$ と $u \in M \setminus \{0\}$ に関して作用 $R_n u = 0$ をとることにより，各生成元 a に対して $\epsilon(a,u)$ の条件を得ることである．この方法は，とにかく関係式をたくさん見つけさえすればよいので，他の頂点 (作用素) 代数の (弱) 加群の研究にも有効であると思う．

以降，$\operatorname{rank} L = 1$，さらに $L = \mathbb{Z}\alpha$ と表したとき，$p = \langle \alpha, \alpha \rangle \in 2\mathbb{Z} \setminus \{0, 2\}$ を仮定する．$\langle \alpha, \alpha \rangle = 2$ の場合は V_L^+ の生成元が違ってくるだけで，結果は同じである．$h = \alpha / \sqrt{\langle \alpha, \alpha \rangle}$ とおくと，$\langle h, h \rangle = 1$ となる．頂点作用素代数 $M(1)^+$ は共形元 $\omega = h(-1)^2\mathbf{1}/2$ と

$$\begin{aligned} H &= \frac{1}{3}h(-3)h(-1)\mathbf{1} - \frac{1}{3}h(-2)^2\mathbf{1}, \\ &\quad \text{または} \\ J &= h(-1)^4\mathbf{1} - 2h(-3)h(-1)\mathbf{1} + \frac{3}{2}h(-2)^2\mathbf{1} \\ &= -9H + 4\omega_{-1}^2\mathbf{1} - 3\omega_{-3}\mathbf{1} \end{aligned} \tag{4.2}$$

で生成されており [5, Theorem 2.7 (2)]，さらに ω, H, J は次の関係式

$$\begin{aligned} [\omega_i, J_j] &= (3i - j)J_{i+j-1}, \\ [\omega_i, H_j] &= (3i - j)H_{i+j-1} + \frac{i(i-1)(3i+j-6)}{6}\omega_{i+j-3} \\ &\quad + \frac{-1}{3}\binom{i}{5}\delta_{i+j-4,0}, \\ [J_i, J_j] &= (-\frac{1392}{5}\omega_{-6}\mathbf{1} - \frac{2784}{5}\omega_{-4}\omega_{-1}\mathbf{1} + 120\omega_{-3}\omega_{-2}\mathbf{1} + \frac{1632}{5}\omega_{-2}\omega_{-1}^2\mathbf{1} \\ &\quad - \frac{56}{5}\omega_{-2}J_{-1}\mathbf{1} - \frac{56}{5}\omega_{-1}J_{-2}\mathbf{1} + \frac{6}{5}J_{-4}\mathbf{1})_{i+j} + \cdots \end{aligned} \tag{4.3}$$

を満たしている．V_L^+ は $M(1)^+$ と $E = e^{\alpha} + e^{-\alpha}$ から生成されており，

$$[\omega_i, E_j] = ((-1 + \frac{p}{2})i - j)E_{i+j-1} \tag{4.4}$$

が成り立っている．Risa/Asir[16] を用いて次の V_L^+ の元は全て 0 となることが分かる．

$$\begin{aligned}
P^{(8),H} &= -2376\omega_{-2}\omega_{-2}\omega_{-1}\mathbf{1} + 3168\omega_{-3}\omega_{-1}\omega_{-1}\mathbf{1} - 6256\omega_{-3}\omega_{-3}\mathbf{1} - 11799\omega_{-4}\omega_{-2}\mathbf{1} \\
&\quad + 30456\omega_{-5}\omega_{-1}\mathbf{1} + 2310\omega_{-7}\mathbf{1} - 9504\omega_{-1}\omega_{-1}H_{-1}\mathbf{1} - 6024\omega_{-3}H_{-1}\mathbf{1} \\
&\quad - 13419\omega_{-2}H_{-2}\mathbf{1} - 6516\omega_{-1}H_{-3}\mathbf{1} + 11868H_{-5}\mathbf{1} + 5040H_{-1}^2\mathbf{1}, \qquad (4.5) \\
P^{(8),J} &= -29056\omega_{-1}^4\mathbf{1} - 118960\omega_{-2}^2\omega_{-1}\mathbf{1} + 39040\omega_{-3}\omega_{-1}^2\mathbf{1} - 39480\omega_{-3}^2\mathbf{1} \\
&\quad - 32120\omega_{-4}\omega_{-2}\mathbf{1} + 497760\omega_{-5}\omega_{-1}\mathbf{1} + 230360\omega_{-7}\mathbf{1} \\
&\quad + 5024\omega_{-1}^2J_{-1}\mathbf{1} - 8536\omega_{-3}J_{-1}\mathbf{1} + 8939\omega_{-2}J_{-2}\mathbf{1} \\
&\quad - 2444\omega_{-1}J_{-3}\mathbf{1} + 1572J_{-5} + 560J_{-1}^2\mathbf{1}, \qquad (4.6) \\
P^{(9)} &= 30J_{-6}\mathbf{1} - 30\omega_{-1}J_{-4}\mathbf{1} + 27\omega_{-2}J_{-3}\mathbf{1} - 39\omega_{-3}J_{-2}\mathbf{1} \\
&\quad + 16\omega_{-1}^2J_{-2}\mathbf{1} + 52\omega_{-4}J_{-1}\mathbf{1} - 32\omega_{-2}\omega_{-1}J_{-1}\mathbf{1}, \qquad (4.7)
\end{aligned}$$

$$\begin{aligned}
P^{(10),H} &= 919328\omega_{-9}\mathbf{1} - 545856\omega_{-5}\omega_{-1}\omega_{-1}\mathbf{1} \\
&\quad - 529536\omega_{-4}\omega_{-4}\mathbf{1} + 545352\omega_{-4}\omega_{-2}\omega_{-1}\mathbf{1} \\
&\quad + 520160\omega_{-3}\omega_{-3}\omega_{-1}\mathbf{1} - 524968\omega_{-3}\omega_{-2}\omega_{-2}\mathbf{1} \\
&\quad - 10240\omega_{-3}\omega_{-1}\omega_{-1}\omega_{-1}\mathbf{1} + 7680\omega_{-2}\omega_{-2}\omega_{-1}\omega_{-1}\mathbf{1} \\
&\quad + 1937712\omega_{-5}H_{-1}\mathbf{1} - 845376\omega_{-3}\omega_{-1}H_{-1}\mathbf{1} \\
&\quad - 381048\omega_{-2}\omega_{-2}H_{-1}\mathbf{1} + 30720\omega_{-1}\omega_{-1}\omega_{-1}H_{-1}\mathbf{1} \\
&\quad - 720081\omega_{-4}H_{-2}\mathbf{1} - 128280\omega_{-2}\omega_{-1}H_{-2}\mathbf{1} \\
&\quad - 435576\omega_{-3}H_{-3}\mathbf{1} + 234528\omega_{-1}\omega_{-1}H_{-3}\mathbf{1} \\
&\quad + 345849\omega_{-2}H_{-4}\mathbf{1} - 1211160\omega_{-1}H_{-5}\mathbf{1} \\
&\quad + 2360970H_{-7}\mathbf{1} + 70875H_{-2}H_{-2}\mathbf{1} \\
&\quad + 734184\omega_{-7}\omega_{-1}\mathbf{1} + 898766\omega_{-6}\omega_{-2}\mathbf{1}, \qquad (4.8)
\end{aligned}$$

$$
\begin{aligned}
P^{(10),J} = {} & 8192\omega_{-1}^5\mathbf{1} - 2048\omega_{-1}^3 J_{-1}\mathbf{1} \\
& + 758496\omega_{-9}\mathbf{1} - 1728\omega_{-5}\omega_{-3}\mathbf{1} \\
& - 15232\omega_{-5}\omega_{-1}\omega_{-1}\mathbf{1} - 60848\omega_{-4}\omega_{-4}\mathbf{1} \\
& - 134224\omega_{-4}\omega_{-2}\omega_{-1}\mathbf{1} - 6912\omega_{-3}\omega_{-3}\omega_{-1}\mathbf{1} \\
& - 136872\omega_{-3}\omega_{-2}\omega_{-2}\mathbf{1} - 112640\omega_{-3}\omega_{-1}\omega_{-1}\omega_{-1}\mathbf{1} \\
& - 69280\omega_{-2}\omega_{-2}\omega_{-1}\omega_{-1}\mathbf{1} - 6092\omega_{-4}J_{-2}\mathbf{1} \\
& + 6272\omega_{-3}\omega_{-1}J_{-1}\mathbf{1} + 360\omega_{-2}\omega_{-2}J_{-1}\mathbf{1} \\
& + 152\omega_{-2}\omega_{-1}J_{-2}\mathbf{1} + 1856\omega_{-3}J_{-3}\mathbf{1} \\
& + 9408\omega_{-1}\omega_{-1}J_{-3}\mathbf{1} + 12656\omega_{-2}J_{-4}\mathbf{1} \\
& - 29968\omega_{-1}J_{-5}\mathbf{1} + 43320J_{-7}\mathbf{1} \\
& + 525J_{-2}J_{-2}\mathbf{1} + 1309248\omega_{-7}\omega_{-1}\mathbf{1} \\
& + 352992\omega_{-6}\omega_{-2}\mathbf{1}, \qquad (4.9)
\end{aligned}
$$

$$
\begin{aligned}
Q^{(4)} = {} & 2(p-2)(-27+54p-44p^2+40p^3)\omega_{-3}E \\
& - 12p(p-2)(-3+4p)\omega_{-1}^2 E \\
& - 6p(p-2)(-9+2p)(-1+2p)H_{-1}E \\
& + (-72p^3-96p^2+210p-90)\omega_0\omega_{-2}E \\
& + (120p^2-48p+36)\omega_0^2\omega_{-1}E \\
& + (-48p-9)\omega_0^4 E. \qquad (4.10)
\end{aligned}
$$

補題 4.1. M を零でない弱 $M(1)^+$ 加群で，任意の $u \in M \setminus \{0\}$ に対して $\epsilon(\omega,u) \geq 2$ となっているものとする．u を M の零でない元で $\epsilon(\omega,u)$ が最小となるものとする．このとき

$$
\epsilon(J,u) = 2\epsilon(\omega,u)+1, \quad J_{\epsilon(J,u)}u = 4\omega^2_{\epsilon(\omega,u)}u, \text{ かつ } \epsilon(H,u) \leq 2\epsilon(\omega,u) \qquad (4.11)
$$

が成り立つ．

Proof. 簡単に

$$
r = \epsilon(\omega,u), \quad s = \epsilon(J,u) \qquad (4.12)
$$

と書くことにする．等式 $P^{(9)}_{s+2r+3}u = 0$ を考える．例えば $\omega_1 J = 4J$, $\omega_i J = 0$ $(i \geq 2)$

から

$$
\begin{aligned}
&(\omega_{-1}J_{-4}\mathbf{1})_{s+2r+3}\\
&=\sum_{i<0}\omega_i\binom{-s-2r+i}{3}J_{s+2r-i-1}+\sum_{0\le i}\binom{-s-2r+i}{3}J_{s+2r-i-1}\omega_i\\
&=\sum_{i\le r}\omega_i\binom{-s-2r+i}{3}J_{s+2r-i-1}+\sum_{r<i}\binom{-s-2r+i}{3}J_{s+2r-i-1}\omega_i\\
&\quad-\sum_{0\le i\le r}\binom{-s-2r+i}{3}[\omega_i,J_{s+2r-i-1}]\\
&=\sum_{i\le r}\omega_i\binom{-s-2r+i}{3}J_{s+2r-i-1}+\sum_{r<i}\binom{-s-2r+i}{3}J_{s+2r-i-1}\omega_i\\
&\quad-\sum_{0\le i\le r}\binom{-s-2r+i}{3}\sum_{j=0}^{1}\binom{i}{j}(\omega_jJ)_{s+2r-1-j}\\
&=\sum_{i\le r}\omega_i\binom{-s-2r+i}{3}J_{s+2r-i-1}+\sum_{r<i}\binom{-s-2r+i}{3}J_{s+2r-i-1}\omega_i\\
&\quad-\sum_{0\le i\le r}\binom{-s-2r+i}{3}(-(s+2r-1)+4i)J_{s+2r-2}
\end{aligned}
\tag{4.13}
$$

と計算できる．したがって $r\ge 2$ と，r と s の定義から $(\omega_{-1}J_{-4}\mathbf{1})_{s+2r+3}u=0$ となる．同様の計算で

$$
\begin{aligned}
0&=(J_{-6}\mathbf{1})_{s+2r+3}u=(\omega_{-2}J_{-3}\mathbf{1})_{s+2r+3}u\\
&=(\omega_{-3}J_{-2}\mathbf{1})_{s+2r+3}u=(\omega_{-4}J_{-1}\mathbf{1})_{s+2r+3}u
\end{aligned}
\tag{4.14}
$$

および

$$
\begin{aligned}
(\omega_{-1}^2J_{-2}\mathbf{1})_{s+2r+3}u&=(-s-1)J_s\omega_r^2u,\\
(\omega_{-2}\omega_{-1}J_{-1}\mathbf{1})_{s+2r+3}u&=(-r-1)J_s\omega_r^2u
\end{aligned}
\tag{4.15}
$$

となる．したがって

$$
\begin{aligned}
0&=P^{(9)}_{s+2r+3}u=(16(-s-1)-32(-r-1))J_s\omega_r^2u\\
&=16(-s+2r+1)J_s\omega_r^2u\\
&=16(-s+2r+1)\omega_r^2J_su
\end{aligned}
\tag{4.16}
$$

となる．ここで $[\omega_r,J_s]u=(3r-s)J_{s+r-1}u=0$ を用いた．したがって $s=2r+1$ または $\omega_r^2J_su=\omega_r(\omega_rJ_su)=0$ となる．$\omega_r^2J_su=0$ とすると (2.2) と (4.3) から

$\omega_i(\omega_r J_s u) = \omega_i J_s u = 0$ $(i > r)$ となっているので，r の最少性に矛盾する．故に $s = 2r+1$ となる．上の計算と同様にして

$$\begin{aligned} 0 = P^{(10),J}_{5r+4} u &= (8192\omega_{-1}^5 \mathbf{1} - 2048\omega_{-1}^3 J_{-1}\mathbf{1})_{5r+4} u \\ &= 2048(4\omega_r^5 - J_{2r+1}\omega_r^3)u \\ &= 2048\omega_r^3(4\omega_r^2 - J_{2r+1})u \end{aligned} \tag{4.17}$$

となる．これより $\omega_r(\omega_r^2(4\omega_r^2 - J_{2r+1})u) = 0$ であり，また任意の $i > r$ に対して，(2.2) より $\omega_i\omega_r^2(4\omega_r^2 - J_{2r+1})u = 0$ であるから，r の最小性により $\omega_r^2(4\omega_r^2 - J_{2r+1})u = 0$ である．同様のことを繰り返して $(4\omega_r^2 - J_{2r+1})u = 0$ が分かる．(4.2) より $\epsilon(H,u) \leq 2\epsilon(\omega,u)$ が分かる． □

弱 V_L^+ 加群 M に対して

$$\Omega_{V_L^+}(M) = \left\{ u \in M \;\middle|\; \begin{array}{l} \text{斉次な } a \in V_L^+ \\ \text{と } i > \mathrm{wt}\, a - 1 \text{ に対して } a_i u = 0 \end{array} \right\} \tag{4.18}$$

とおく．次が定理 1.1 を証明するうえで一番重要な補題である．

補題 4.2. M を零でない弱 V_L^+ 加群とする．このとき，零でない $u \in \Omega_{V_L^+}(M)$ で次のいずれかを満たすものが存在する．

(1) $\epsilon(\omega,u) = -1$.
(2) $H_3 u = 0$.
(3) $\omega_1 u = u, H_3 u = u$.
(4) $\omega_1 u = (1/16)u, H_3 u = (-1/128)u$.
(5) $\omega_1 u = (9/16)u, H_3 u = (15/128)u$.

Proof. $\epsilon(\omega,u) < 0$ となる $u \in M \setminus \{0\}$ が存在する場合は，[14, Proposition 3.3 (a)] と [15, Proposition 4.1.1] より u から生成される V_L^+ 加群は V_L^+ と同型になる．これは (1) の場合である．したがって，全ての零でない $u \in M$ に対して $\epsilon(\omega,u) \geq 0$ を仮定し，u として $\epsilon(\omega,u)$ が最小のものを取る．簡単に

$$r = \epsilon(\omega,u), \quad s = \epsilon(J,u), \quad t = \epsilon(E,u) \tag{4.19}$$

と書くことにする．$r \geq 2$ を仮定する．補題 4.1 から $s = 2r+1, J_{2r+1}u = 4\omega_r^2 u, H_i u = 0$ $(i \geq 2r)$ となる． 展開 $Q^{(4)}_{t+2r+2}$ において，各項の右端の部分が ω_i $(r+1 \leq i), H$ $(2r+1 \leq i)$，または E_k $(k \in \mathbb{Z})$ となるようにし ((4.13) の計算を参照)，$Q^{(4)}_{t+2r+2}u$ を取ると

$$0 = Q^{(4)}_{t+2r+2}u = -12p(p-2)(-3+4p)\omega_r^2 E_t u, \tag{4.20}$$

を得る．$p \in 2\mathbb{Z} \setminus \{0,2\}$ であったから $\omega_r^2 E_t u = 0$ となる．$i > r$ のときに (2.2) と (4.4) から $\omega_i(\omega_r E_t u) = 0$ となるため，r の最小性より $\omega_r E_t u = 0$ となる．同様にして $E_t u = 0$ が分かるので矛盾する．したがって $r \leq 1$ が分かる．次に $s \geq 4$ を仮定する．上と同様の計算から

$$0 = P_{2s+1}^{(8),J} u = J_s^2 u = J_s(J_s u), \tag{4.21}$$

となる．(4.3) から $i > r$ と $j > s$ に対して $\omega_i J_s u = J_j J_s u = 0$ が分かるため，$\epsilon(\omega, J_s u) \leq r, \epsilon(J, J_s u) < s$ が分かる．$J_s u$ を u に取り替えていけば，$r \leq 1$, $s \leq 3$ となる u を得ることが出来る． 特に $\epsilon(H, u) \leq 3$ となる．ここで関係式

$$0 = P_7^{(8),H} u = -72(132\omega_1^2 - 65\omega_1 + 3 - 70H_3)H_3 u \tag{4.22}$$

$$0 = P_9^{(10),H} u = 240H_3(-207 + 4725H_3 + 4472\omega_1 - 9118\omega_1^2 + 128\omega_1^3)u, \tag{4.23}$$

から $0 = (\omega_1 - 1)(16\omega_1 - 1)(16\omega_1 - 9)H_3 u$ を得るので，証明が終わる． □

Remark 4.3. 補題 4.2 において，u は，(1) のとき $\mathbf{1} \in M(1)^+$， (2) のとき $e^\beta \in M(1,\beta), \beta + L \in L^\perp/L$, (3) のとき $h(-1)\mathbf{1} \in M(1)^-$, (4),(5) は θ-twisted V_L 加群の元にあたる．

参考文献

[1] T. Abe, *Rationality of the vertex operator algebra V_L^+ for a positive definite even lattice L*, Math. Z. **249** (2005), 455–484.

[2] T. Abe, G. Buhl and C. Dong, *Rationality, regularity, and C_2-cofiniteness*, Trans. Amer. Math. Soc. **356** (2004), 3391–3402.

[3] T. Abe and C. Dong, *Classification of irreducible modules for the vertex operator algebra V_L^+ : general case*, J. Algebra **273** (2004), 657–685.

[4] C. Dong, *Vertex algebras associated with even lattices*, J. Algebra **160** (1993), 245–265.

[5] C. Dong and R. L. Griess Jr, *Rank one lattice type vertex operator algebras and their automorphism groups*, J. Algebra **208** (1998), 262–275.

[6] C. Dong, C. Jiang and X. Lin, *Rationality of vertex operator algebra V_L^+: higher rank*, Proc. Lond. Math. Soc. **104** (2012), 799–826.

[7] C. Dong and K. Nagatomo, *Classification of irreducible modules for the vertex operator algebra* $M(1)^+$, J. Algebra **216** (1999), 384–404.

[8] C. Dong and K. Nagatomo, *Representations of vertex operator algebra* V_L^+ *for rank one lattice* L, Comm. Math. Phys. **202** (1999), 169–195.

[9] C. Dong and K. Nagatomo, *Classification of irreducible modules for the vertex operator algebra* $M(1)^+$*:II. higher rank*, J. Algebra **240** (2001), 289–325.

[10] I. B. Frenkel, J. Lepowsky and A. Meurman, *Vertex operator algebras and the monster*, Pure and Applied Math. **134**, Academic Press, 1988.

[11] P. Jitjankarn and G. Yamskulna, *C_2-cofiniteness of the vertex algebra V_L^+ when L is a nondegenerate even lattice*, Comm. Algebra **38** (2010), 4404–4415.

[12] L. Jordan, *Classification of irreducible V_L^+-modules for a negative definite rank one even lattice L*, Ph.D. thesis, University of California at Santa Cruz, 2006.

[13] J. Lepowsky and H. S. Li, *Introduction to vertex operator algebras and their representations*, Progress in Mathematics **227**, Birkhauser Boston, Inc., Boston, MA, 2004.

[14] H. S. Li, *Symmetric invariant bilinear forms on vertex operator algebras*, J. Pure Appl. Algebra **96** (1994), 279–297.

[15] H. S. Li, *Local systems of vertex operators, vertex superalgebras and modules*, J. Pure Appl. Algebra **109** (1996), 143–195.

[16] Risa/Asir, `http://www.math.kobe-u.ac.jp/Asir/asir.html`.

[17] K. Tanabe, *The irreducible weak modules for the fixed point subalgebra of the vertex algebra associated to a non-degenerate even lattice by an automorphism of order* 2, `https://arxiv.org/abs/1910.07126`.

[18] G. Yamskulna, *C_2-cofiniteness of the vertex operator algebra V_L^+ when L is a rank one lattice*, Comm. Algebra **32** (2004), 927–954.

[19] G. Yamskulna, *Classification of irreducible modules of the vertex algebra V_L^+ when L is a nondegenerate even lattice of an arbitrary rank*, J. Algebra **320** (2008), 2455–2480.

[20] G. Yamskulna, *Rationality of the vertex algebra V_L^+ when L is a non-degenerate even lattice of arbitrary rank*, J. Algebra **321** (2009), 1005–1015.

[21] Y. Zhu, *Modular invariance of characters of vertex operator algebras*, J. Amer. Math. Soc. **9** (1996), 237–302.

A large family of strongly regular Cayley graphs

–強正則ケーリーグラフの大きな族について–

熊本大学大学院　先端科学研究部　　籾原　幸二*
Koji Momihara
Faculty of Advanced Science and Technology,
Kumamoto University

概 要

論文 [7] では, 3 値のガウス周期に基づいて, 有限体の加法群上の強正則ケーリーグラフの構成法を与えた. 特に, [1] の結果と共に, 以下の場合に, パラメータ $(q^6, r(q^3+1), -q^3+r^2+3r, r^2+r)$, $r=M(q^2-1)/2$ を持つ強正則ケーリーグラフの存在性を示した: (i) $M=1$ かつ $q\equiv 3 \pmod 4$; (ii) $M=3$ かつ $q\equiv 7 \pmod{24}$; (iii) $M=7$ かつ $q\equiv 11, 51 \pmod{56}$. 一方, $M>7$ の場合については, これまで特に議論されることはなかった. この論文では, 奇数 M を割る任意の正整数 M' に対し, $-1\notin\langle 2\rangle \pmod{M'}$ が満たされるとき, 上記のパラメータをもつ強正則グラフが存在する素数 q が無限個存在することを示す. この論文は, [8] の抜粋および要約である.

1　導入

Γ を v 頂点上の単純グラフとする. Γ が, k-正則で, 隣接 (非隣接)2 頂点に同時に隣接する頂点数がちょうど $\lambda(\mu)$ 個のとき, パラメータ (v,k,λ,μ) をもつ強正則グラフと呼ばれる. 特に, 完全グラフや空グラフでない k-正則グラフが強正則であることと, その隣接行列が固有値として k 以外の固有値をちょうど 2 種類持つことが同値であることが知られている.

G を加法的に記述した可換群とし, D を G の逆元で閉じた単位元を含まない部分集合とする. このとき, 頂点集合を G とし, $x-y\in D$ のとき (x,y) を辺とすることで得られるグラフをケーリーグラフと呼び, $\mathrm{Cay}(G,D)$ と記す. D はこのグラフの連結集合と呼ばれる. また, $\mathrm{Cay}(G,D)$ の固有値は, D の指標値で決まることが知られている. G の指標 ψ に対し,

$$\psi(D)=\sum_{x\in D}\psi(x)$$

とする. このとき, $\mathrm{Cay}(G,D)$ の固有値は, $\psi(D)$, $\psi\in G^{\perp}$ で与えられる. ここで, $G^{\perp}$ は G の指標群とする.

[1] では, $q\equiv 3 \pmod 4$ なる素数ベキ q に対し, パラメータ $(q^6, r(q^3+1), -q^3+r^2+3r, r^2+r)$, $r=(q^2-1)/2$ を持つ強正則グラフの構成法が与えられた. この強正則グラフから, 有限射影空

[1]Email: momihara@educ.kumamoto-u.ac.jp
この研究は, 科学研究費補助金 (若手研究 (B) 17K14236, 基盤研究 (B) 15H03636) の補助を受けています.

間 $\mathsf{PG}(5,q)$ における非退化な楕円型二次曲面上の $\frac{q+1}{2}$-ovoid を構成でき, 有限幾何学上重要なものである. また, 著者は, この論文の構成法が 3 値ガウス周期の枠組みで一般化できることを示し, 以下の定理を証明した.

定理 1.1. ([7]) q を素数ベキとする. 以下の場合に, パラメータ $(q^6, r(q^3+1), -q^3+r^2+3r, r^2+r)$, $r=(q^2-1)M/2$ を持つ強正則ケーリーグラフが存在する:

(1) $M=3$ かつ $q\equiv 7\,(\mathrm{mod}\ 24)$;

(2) $M=7$ かつ $q\equiv 11, 51\,(\mathrm{mod}\ 56)$.

この論文では, $M>7$ の場合に上述のパラメータの強正則グラフが存在するかどうかに興味がある. M,h を, M を奇数, $1\le h\le M-1$, $M\,|\,h^2+h+1$ なる正整数とする. $\Psi_{M,h}$ を, パラメータ $(p^6, r(p^3+1), -p^3+r^2+3r, r^2+r)$, $r=(p^2-1)M/2$ をもつ $(\mathbb{F}_{p^6},+)$ 上の強正則ケーリーグラフが存在するような $p\equiv h\,(\mathrm{mod}\ M)$ かつ $p\equiv 3\,(\mathrm{mod}\ 4)$ なる素数の集合とする. 以下が主定理である.

定理 1.2. M を割る任意の $M'>1$ に対し, $-1\notin\langle 2\rangle\,(\mathrm{mod}\ M')$ が満たされるとき, $\Psi_{M,h}$ は無限集合である.

上記の定理の条件を満たす $M<200$ は, $7, 31, 49, 73, 79, 103, 127, 151, 199$ である.

特に, M が奇素数ベキで, かつ, $\mathbb{Q}(\zeta_M+\zeta_M^{-})$ の類数が奇数の場合には, $\Psi_{M,h}$ の密度を計算できる. この内容の詳細については, [8] を参照していただきたい.

2 準備

2.1 ガウス周期

p を素数とし, $\zeta_p=\exp(2\pi i/p)\in\mathbb{C}$ を 1 の原始 p 乗根とする. 正整数 f,n に対し, $q=p^f$ とし, $\mathbb{F}_{q^n}$ を位数 q^n の有限体を記すこととする. 写像 $\psi_{\mathbb{F}_{q^n}}:\mathbb{F}_{q^n}\to\mathbb{C}^*$ を

$$\psi_{\mathbb{F}_{q^n}}(x)=\zeta_p^{\mathrm{Tr}_{q^n/p}(x)}$$

で定める. ここで, $\mathrm{Tr}_{q^n/p}$ は $\mathbb{F}_{q^n}$ から $\mathbb{F}_p$ へのトレース写像とする. このとき, $\psi_{\mathbb{F}_{q^n}}$ は, $\mathbb{F}_{q^n}$ の加法群の指標で, 標準加法的指標と呼ばれる.

ω を $\mathbb{F}_{q^n}$ の原始根とし, N を q^n-1 を割る正整数とする. このとき, 指数 N の円分類を以下のように定める:

$$C_i^{(N,q^n)}=\omega^i\langle\omega^N\rangle,\ 0\le i\le N-1.$$

このとき, 位数 N のガウス周期を以下で定める:

$$\psi_{\mathbb{F}_{q^n}}(C_i^{(N,q^n)})=\sum_{x\in C_i^{(N,q^n)}}\psi_{\mathbb{F}_{q^n}}(x),\ 0\le i\le N-1.$$

[5] では, ガウス周期 $\psi_{\mathbb{F}_{q^n}}(C_i^{(N,q^n)})$, $i=0,1,\ldots,N-1$, がいつ 3 種類の等差的な値を取るかという問題を, ある 3-クラスのアソシエーションスキームの問題と関連して調べた. この論文では, $n=3$ の場合のみを考える.

以下の定理がこの章の主結果である. 証明は, [8] を参照されたい.

定理 2.1. M,h を $0<h<M-1$ かつ $M\,|\,h^2+h+1$ を満たす正整数とする. q をある素数 p の冪で, $q\equiv h\,(\mathrm{mod}\ M)$ を満たすものとする. さらに, $N=\frac{q^3-1}{M(q-1)}$ とおき, ω を $\mathbb{F}_{q^3}$ の原始根として一つ固定する. このとき,

$$p>\Big(\frac{12M}{\phi(M)}\Big)^{\phi(M)/2\mathrm{ord}_M(p)}$$

が成立すれば, $\psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)})$, $i=0,1,\ldots,N-1$ は, ちょうど 3 つの値 $-M+2q,-M+q,-M$ をとる.

丸田 [6] は, p に対する限界式を与えることなくこの定理の証明を符号理論の言葉で与えたが, [8] では, [3] の結果を用いてより単純明快に証明し, かつ, 限界式も明示できる.

3　3 値のガウス周期に基づくケーリーグラフの構成について

3.1　構成法の枠組み

$q^n\equiv 3\,(\mathrm{mod}\ 4)$ を素数ベキとし, ω を $\mathbb{F}_{q^n}$ の原始根とする. N を $(q^n-1)/(q-1)$ を割る奇数とし, $C_i^{(N,q^n)}=\omega^i\langle\omega^N\rangle$, $i=0,1,\ldots,N-1$ とする. この章では, ガウス周期 $\psi_{\mathbb{F}_{q^n}}(C_i^{(N,q^n)})$, $i=0,1,\ldots,N-1$ の値は常に 3 つの等差的な値 $\alpha_1,\alpha_2,\alpha_3$ を取ると仮定し, $\alpha_1-\alpha_2=\alpha_2-\alpha_3>0$ とする.

$$I_j=\{i\,(\mathrm{mod}\ N)\,|\,\psi_{\mathbb{F}_{q^n}}(C_i^{(N,q^n)})=\alpha_j\},\ \ j=1,2,3,$$

とし, T_1,T_2 を I_2 のある分割とする. $T_i'\equiv 4^{-1}T_i\,(\mathrm{mod}\ N)$, $i=1,2$ とし,

$$X=2T_1'\cup(2T_2'+N)\,(\mathrm{mod}\ 2N) \tag{3.1}$$

と定める. また,

$$\begin{aligned}Y_X:=&\{Ni+4j\,(\mathrm{mod}\ 4N):(i,j)\in(\{0,3\}\times T_1')\cup(\{1,2\}\times T_2')\}\\&\cup\{Ni+4j\,(\mathrm{mod}\ 4N):i=0,1,2,3,\ j\in 4^{-1}I_1\,(\mathrm{mod}\ N)\}\end{aligned} \tag{3.2}$$

とする. このとき, $X\equiv 2^{-1}I_2\,(\mathrm{mod}\ N)$ かつ $Y_X\equiv I_1\cup I_1\cup I_1\cup I_1\cup I_2\cup I_2\,(\mathrm{mod}\ N)$ が成立している.

今, γ を $\mathbb{F}_{q^{2n}}$ の原始根で, $\gamma^{q^n+1}=\omega$ なるものとする. また, $\mathbb{F}_{q^n}$ の部分集合として,

$$D_X=\bigcup_{i\in Y_X}C_i^{(4N,q^{2n})} \tag{3.3}$$

と定義する. ここで, $C_i^{(4N,q^{2n})}=\gamma^i\langle\gamma^{4N}\rangle$, $i=0,1,\ldots,4N-1$ である. このとき, $|D_X|=(q^{2n}-1)(2|I_1|+|I_2|)/2N$ が成立する. この D_X は, 我々の所望する強正則ケーリーグラフの連結集合になりうるかどうかを調べる. D_X の指標値は, 以下のように決まる.

命題 3.1. ([7, Proposition 4.2]) 任意の $a \in \mathbb{Z}_{4N}$ に対し, $b \equiv 4^{-1}a \pmod N$ と $c \equiv 2b \pmod{2N}$ を定める. このとき, D_X の指標値は,

$$\psi_{\mathbb{F}_{q^{2n}}}(\gamma^a D_X) = \frac{\rho_{q^n}\delta_a q^n}{2G_{q^n}(\eta)} \left(2\psi_{\mathbb{F}_{q^n}}(\omega^c \bigcup_{\ell \in X} C_\ell^{(2N,q^n)}) - \psi_{\mathbb{F}_{q^n}}(\omega^c \bigcup_{\ell \in 2^{-1}I_2} C_\ell^{(N,q^n)}) \right) + \frac{(q^n-1)(2|I_1|+|I_2|)}{2N} + \begin{cases} -q^n, & a \in I_1 \pmod N \text{ のとき}, \\ -\frac{q^n}{2}, & a \in I_2 \pmod N \text{ のとき}, \\ 0, & a \in I_3 \pmod N \text{ のとき}, \end{cases} \tag{3.4}$$

で与えられる. ここで, $q^n \equiv 7$ か $3 \pmod 8$ で, $\rho_{q^n} = 1$ または -1 と定める. また, $a \equiv 0, N \pmod 4$ か $a \equiv 2, 3N \pmod 4$ で, $\delta_a = 1$ または -1 と定める. さらに, η は $\mathbb{F}_{q^n}$ の位数 2 の乗法的指標とする.

注意 3.2. X を (3.1) で定義される集合で,

$$2\psi_{\mathbb{F}_{q^n}}(\omega^c \bigcup_{\ell \in X} C_\ell^{(2N,q^n)}) - \psi_{\mathbb{F}_{q^n}}(\omega^c \bigcup_{\ell \in 2^{-1}I_2} C_\ell^{(N,q^n)}) = \begin{cases} \pm G_{q^n}(\eta), & c \in 2^{-1}I_2 \pmod N \text{ のとき}, \\ 0, & \text{その他}, \end{cases} \tag{3.5}$$

を満たすとする. ここで, (3.5) を (3.4) に代入して, D_X はちょうど 2 つの値 $(q^n-1)(2|I_1|+|I_2|)/2N$ と $-q^n+(q^n-1)(2|I_1|+|I_2|)/2N$ を取ることになる. このとき, $\mathrm{Cay}(\mathbb{F}_{q^{2n}}, D_X)$ は強正則グラフとなる. 特に, パラメータ $(q^{2n}, r(q^n+1), -q^n+r^2+3r, r^2+r)$, $r = (|I_2|+2|I_1|)(q^n-1)/2N$ を持つことがわかる.

3.2 PG$(2,q)$ における conic の分解とその商について

この章では, [2, 4] で発見された PG$(2,q)$ の conic の良い分解について説明する.

q を素数ベキとし, ω を $\mathbb{F}_{q^3}$ の原始根とする. $\mathbb{F}_{q^3}$ を $\mathbb{F}_q$ 上の 3 次元ベクトル空間だと解釈する. PG$(2,q)$ の点を $\langle\omega^i\rangle := \omega^i\mathbb{F}_q^*$, $0 \le i \le q^2+q$ と同一視する. $Q : \mathbb{F}_{q^3} \to \mathbb{F}_q$ の非退化な二次形式を $Q(x) := \mathrm{Tr}_{q^3/q}(x^2)$ で定義する. このとき, Q は PG$(2,q)$ の conic $\mathcal{Q}$ を定義し, $q+1$ 点含んでいる. $\mathbb{Z}_{q^2+q+1}$ の部分集合を以下で定まる:

$$W_{\mathcal{Q}} = \{i \pmod{q^2+q+1} : Q(\omega^i) = 0\} = \{d_0, d_1, \ldots, d_q\}. \tag{3.6}$$

ここで, 各元は適当な順序でラベルを付けている. このとき, $\mathcal{Q} = \{\langle\omega^{d_i}\rangle : 0 \le i \le q\}$ が成立する.

以下に, $W_{\mathcal{Q}}$ の分解を定める. $d_0 \in W_{\mathcal{Q}}$ に対し,

$$\mathcal{X}_{\mathcal{Q}} := \{\omega^{d_i}\mathrm{Tr}_{q^3/q}(\omega^{d_0+d_i}) : 1 \le i \le q\} \cup \{2\omega^{d_0}\} \tag{3.7}$$

と

$$X_{\mathcal{Q}} := \{\log_\omega(x) \pmod{2(q^2+q+1)} : x \in \mathcal{X}_{\mathcal{Q}}\} \tag{3.8}$$

を定める. このとき, $X_{\mathcal{Q}} \equiv W_{\mathcal{Q}} \pmod{q^2+q+1}$ である. 集合 $X_{\mathcal{Q}} \subseteq \mathbb{Z}_{2(q^2+q+1)}$ は, $|E_1|+|E_2| = q+1$ なる部分集合 $E_1, E_2 \subseteq \mathbb{Z}_{q^2+q+1}$ が存在し,

$$X_{\mathcal{Q}} = 2E_1 \cup (2E_2 + (q^2+q+1)) \pmod{2(q^2+q+1)} \tag{3.9}$$

が成立する. よって, $X_{\mathcal{Q}}$ は偶部分と奇部分に分解される. このとき, $2(E_1 \cup E_2) \equiv W_{\mathcal{Q}} \pmod{q^2+q+1}$ が成り立ち, $X_{\mathcal{Q}}$ が $W_{\mathcal{Q}}$ の分解を誘導する.

補題 3.3. ([4, Lemma 3.4]) $\mathcal{X}_{\mathcal{Q}}$ の定義で, d_0 の代わりに d_i を用いると, 得られる $X'_{\mathcal{Q}}$ について, $X'_{\mathcal{Q}} \equiv X_{\mathcal{Q}}$ または $X_{\mathcal{Q}} + (q^2+q+1) \pmod{2(q^2+q+1)}$ が成立する.

次に, $X_{\mathcal{Q}}$ の商について考える. この章では, N が q^2+q+1 を割るとし, ガウス周期 $\psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)})$, $i = 0, 1, \ldots, N-1$ がちょうど 3 つの値 $-M+2q, -M+q, -M$ をとるとする. ここで, $M = \frac{q^2+q+1}{N}$ と定める. このとき, $X_{\mathcal{Q}} \equiv 2^{-1}(I_1 \cup I_1 \cup I_2) \pmod{N}$ となることが示せる. ここで, 多重集合

$$X_i := \{x \pmod{2N} : x \in X_{\mathcal{Q}}, x \pmod{N} \in 2^{-1}I_i\},\ i = 1, 2, \tag{3.10}$$

を定める. このとき, $X_1 \equiv 2^{-1}(I_1 \cup I_1) \pmod{N}$ かつ $X_2 \equiv 2^{-1}I_2 \pmod{N}$ が成立する. ここで, 群 G の上で定義された多重集合が, G の多重でない通常の部分集合であるとき, 純部分集合と呼ぶことにする. このとき, X_2 が $\mathbb{Z}_{2N}$ の純部分集合であるが, X_1 はそうでないかもしれない.

命題 3.4. ([7, Proposition 5.5]) X_1 が $\mathbb{Z}_{2N}$ の純部分集合であるとき,

$$2\psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell \in X_2} C_\ell^{(2N,q^3)}) - \psi_{\mathbb{F}_{q^3}}(\omega^c \bigcup_{\ell \in 2^{-1}I_2} C_\ell^{(N,q^3)}) = \begin{cases} \pm G_{q^3}(\eta), & c \in 2^{-1}I_2 \pmod{N} \text{ のとき,} \\ 0, & \text{その他,} \end{cases}$$

が成立する.

定理 3.5. $q \equiv 3 \pmod{4}$ を素数ベキとし, M を q^2+q+1 を割る正整数とする. また, $N = \frac{q^2+q+1}{M}$ とする. ガウス周期 $\psi_{\mathbb{F}_{q^3}}(C_i^{(N,q^3)})$, $i = 0, 1, \ldots, N-1$ がちょうど 3 つの値 $-M, -M+q, -M+2q$ を取り, X_1 が $\mathbb{Z}_{2N}$ の純部分集合であると仮定する. このとき, $\mathrm{Cay}(\mathbb{F}_{q^6}, D_{X_2})$ はパラメータ $(q^6, r(q^3+1), -q^3+r^2+3r, r^2+r)$, $r = (q^2-1)M/2$ をもつ強正則グラフとなる. ここで, X_i, $i = 1, 2$ は (3.10) で定義され, D_X は (3.3) で定義されている.

証明: 命題 3.1, 命題 3.4, 注意 3.2 を $n = 3$ と $X = X_2$ として適用すればよい. □

3.3 X_1 が $\mathbb{Z}_{2N}$ 上純部分集合となるための条件

$u \in W_{\mathcal{Q}}$ が $u \pmod{N} \in 2^{-1}I_1$ を満たすとき, $W_{\mathcal{Q}} \equiv 2^{-1}(I_1 \cup I_1 \cup I_2) \pmod{N}$ であるので, $u + \ell_u N \in W_{\mathcal{Q}}$ を満たす $\ell_u \in \{1, 2, \ldots, M-1\}$ が存在する. ここで,

$$g_M(\omega^u) = \mathrm{Tr}_{q^3/q}(\omega^{2u+\ell_u N})\omega^{\ell_u N}$$

と定義する.

補題 3.6. η を $\mathbb{F}_{q^3}$ の位数 2 の乗法的指標とする. このとき, X_1 が $\mathbb{Z}_{2N}$ 上純部分集合であるための必要十分条件は, $u \pmod N \in 2^{-1}I_1$ なる全ての $u \in W_{\mathcal{Q}}$ に対し, $\eta(2) \neq \eta(g_M(\omega^u))$ が成立することである.

証明: (3.7) より, d_0 として u をとると, 補題 3.3 より $2\omega^u$, $g_M(\omega^u)\omega^u \in \mathcal{X}_{\mathcal{Q}}$ または $2\omega^{u+q^2+q+1}$, $g_M(\omega^u)\omega^{u+q^2+q+1} \in \mathcal{X}_{\mathcal{Q}}$ を得る. どちらの場合についても, X_1 が $\mathbb{Z}_{2N}$ 上純部分集合であるための必要十分条件は, $\eta(2) \neq \eta(g_M(\omega^u))$ が満たされることである. □

補題 3.7. ([7, Lemma 5.8]) $u \pmod N \in 2^{-1}I_1$ なる $u \in W_{\mathcal{Q}}$ に対し,

$$\eta(g_M(\omega^u)) = \eta(-1)\eta(1-\omega^{\frac{\ell u(q+1)(q^3-1)}{M}})\eta(1-\omega^{\frac{2\ell u q(q^3-1)}{M}}) \tag{3.11}$$

が成立する.

[7] では, 上の補題を用いて, X_1 が $\mathbb{Z}_{2N}$ 上で純部分集合であるための条件を, $M = 3$ または 7 の場合に, q に対する特徴付けとして与えた. 以下の命題によって, $M > 7$ の場合も扱えるようになる. 証明は [8] を参照していただきたい.

命題 3.8. η を $\mathbb{F}_{q^3}$ の位数 2 の乗法的指標とする. このとき, X_1 が $\mathbb{Z}_{2N}$ で純部分集合であるための必要十分条件は, $\eta(2) \neq \eta(1+\omega^{\frac{\ell(q^3-1)}{M}})$ がすべての $\ell \in \{1, 2, \ldots, M-1\}$ で成立することである.

よって, この章の残りでは, まず $\eta(1+\omega^{\frac{\ell(q^3-1)}{M}})$, $1 \leq \ell \leq M-1$ がすべて等しくなるための M 及び q への必要条件を求めることにする. それをするために, $1+\omega^{\frac{\ell(q^3-1)}{M}}$, $1 \leq \ell \leq M-1$ らの間の乗法的な関係式について考える. ϵ_M で $\omega^{\frac{q^3-1}{M}}$ および $\zeta_M = \exp(2\pi i/M)$ どちらも表記することとする.

補題 3.9. 任意の整数 ℓ に対し,

$$1 + \epsilon_M^{\ell} = \epsilon_M^{\ell}(1 + \epsilon_M^{-\ell})$$

が成立する.

補題 3.10. $\gcd(\ell, M) = 1$ なる任意の整数 ℓ に対し, 以下が成立する:

$$\prod_{i=0}^{\mathrm{ord}_M(2)-1} (1 + \epsilon_M^{2^i\ell}) = 1$$

証明: $2^{\mathrm{ord}_M(2)} \equiv 1 \pmod M$ に注意して,

$$\prod_{i=0}^{\mathrm{ord}_M(2)-1} (1 + \epsilon_M^{2^i\ell}) = \prod_{i=0}^{\mathrm{ord}_M(2)-1} \frac{1-\epsilon_M^{2^{i+1}\ell}}{1-\epsilon_M^{2^i\ell}} = \frac{1-\epsilon_M^{2^{\mathrm{ord}_M(2)}\ell}}{1-\epsilon_M^{\ell}} = 1$$

を得る. □

補題 3.11. $-1 \in \langle 2 \rangle \pmod M$ を満たすとき, $\gcd(\ell, M) = 1$ なる任意の整数 ℓ に対し, 以下が成立する:

$$\prod_{i=0}^{\mathrm{ord}_M(2)/2-1} 1 + \epsilon_M^{2^i \ell} = -\epsilon_M^{-\ell}.$$

証明: $2^{\mathrm{ord}_M(2)/2} \equiv -1 \pmod M$ に注意して,

$$\begin{aligned}\prod_{i=0}^{\mathrm{ord}_M(2)/2-1} (1 + \epsilon_M^{2^i \ell}) &= \prod_{i=0}^{\mathrm{ord}_M(2)/2-1} \frac{1 - \epsilon_M^{2^{i+1}\ell}}{1 - \epsilon_M^{2^i \ell}} = \frac{1 - \epsilon_M^{2^{\mathrm{ord}_M(2)/2}\ell}}{1 - \epsilon_M^{\ell}} \\ &= \frac{1 - \epsilon_M^{-\ell}}{1 - \epsilon_M^{\ell}} = -\epsilon_M^{-\ell}\end{aligned}$$

を得る. □

補題 3.12. $t \nmid s$ なる整数 $s, t > 1$ に対し, $M = st$ とする. このとき, $\gcd(\ell, M) = 1$ なる整数 ℓ に対し, 以下が成立する:

$$1 + \epsilon_t^{s\ell} = \prod_{i=0}^{s-1} (1 + \epsilon_s^i \epsilon_t^{\ell}). \tag{3.12}$$

特に, $M = p^e$, $e \geq 2$ なる素数ベキのとき, 任意の $1 \leq j \leq e-1$ に対し, 以下が成立する:

$$1 + \epsilon_M^{p^j \ell} = \prod_{i=0}^{p^j - 1} (1 + \epsilon_{p^j}^i \epsilon_M^{\ell}). \tag{3.13}$$

証明: $-\epsilon_t^{-\ell}$ を $x^s - 1 = \prod_{i=0}^{s-1}(x - \epsilon_s^i)$ へ代入して, $-\epsilon_t^{-s\ell} - 1 = -\epsilon_t^{-s\ell} \prod_{i=0}^{s-1}(1 + \epsilon_s^i \epsilon_t^{\ell})$ を得る. また, $-\epsilon_t^{s\ell}$ を両辺に掛けて, 前者の結果 $1 + \epsilon_t^{s\ell} = \prod_{i=0}^{s-1}(1 + \epsilon_s^i \epsilon_t^{\ell})$ を得る. また, (3.12) を $M = t = p^e$, $s = p^j$ として適用することで, 後者の結果を得る. □

系 3.13. η を $\mathbb{F}_{q^3}$ の位数 2 の乗法的指標とする. また, ℓ を $\gcd(\ell, M) = 1$ なる整数とする. このとき, 以下が成立する:

(1) $\eta(1 + \epsilon_M^{\ell}) = \eta(1 + \epsilon_M^{-\ell})$.

(2) $\prod_{i=0}^{\mathrm{ord}_M(2)-1} \eta(1 + \epsilon_M^{2^i \ell}) = 1$.

(3) $-1 \in \langle 2 \rangle \pmod M$ のとき, $\prod_{i=0}^{\mathrm{ord}_M(2)/2-1} \eta(1 + \epsilon_M^{2^i \ell}) = \eta(-1)$.

(4) $t \nmid s$ なる整数 $s, t > 1$ に対し, $M = st$ とする. このとき, $\eta(1 + \epsilon_t^{s\ell}) = \prod_{i=0}^{s-1} \eta(1 + \epsilon_s^i \epsilon_t^{\ell})$ が成立する. 特に, $M = p^e$, $e \geq 2$ が素数ベキのとき, 任意の $1 \leq j \leq e-1$ に対し, $\prod_{i=0}^{p^j - 1} \eta(1 + \epsilon_{p^j}^i \epsilon_M^{\ell}) = \eta(1 + \epsilon_M^{p^j \ell})$ が成り立つ.

証明: $\eta(\epsilon_M^{\ell}) = 1$ に注意して, 補題 3.9, 3.10, 3.11, 3.12 らから従う. □

注意 3.14. $M = p^e$, $e \geq 2$ なる素数ベキの場合, 補題 3.12 の (3.13) より, $\gcd(M, i) \neq 1$ なる $1 + \epsilon_M^i$ らは全て, $\gcd(M, i) = 1$ なる $1 + \epsilon_M^i$ らから決定できることが分かる. 特に, $\gcd(i, M) = 1$ なる全ての i に対し, $\eta(1 + \epsilon_M^i) = \alpha$, $\alpha \in \{1, -1\}$ が成り立つとき, $\gcd(i, M) \neq 1$ なるすべての i に対し, $\eta(1 + \epsilon_M^i) = \alpha$ が成立する.

また, M が合成数の場合については, 以下の命題を得ることができる. 証明は [8] を参照してほしい.

命題 3.15. M を素数ベキでない正整数 *(*合成数*)* とする. $-1 \notin \langle 2\rangle \pmod M$ であり, かつ, $|\langle 2\rangle \pmod M|$ が偶数であると仮定する. $U_M = \{x : 1 \le x \le M-1, \gcd(x, M) = 1\}$ の任意の $\phi(M)/4$-元部分集合 X で,

$$X \cup -X \cup 2X \cup -2X = U_M \tag{3.14}$$

を満たすものをとる. このとき, $\gcd(\ell, M) = 1$ なる任意の正整数 ℓ に対し,

$$\prod_{x\in X} \eta(1+\epsilon_M^{2x\ell}) = \eta(-1)^{\frac{\phi(M)}{4}+c}, \tag{3.15}$$

が成立する. ここで, $c = |\{x \in X \cup 2X \pmod M : (M+1)/2 \le x < M\}|$ と定める.

これらの結果を用いて, すべての $1 \le \ell < M$ に対し $\eta(2) \neq \eta(1+\epsilon_M^\ell)$ を満たす素数ベキ q を, $M = 3, 7, 21$ の場合に決定できる. 特に, $M = 21$ の場合が新たな結果である.

命題 3.16. ([7, Proposition 5.9]) $q \equiv 1 \pmod 3$ とする. このとき, $\mathbb{F}_{q^3}$ において, 全ての $i = 1, 2$ で $\eta(2) \neq \eta(1+\epsilon_3^i)$ が成立するための必要十分条件は, $q \equiv 7, 13 \pmod{24}$ である.

証明: $1+\epsilon_3^2 = -\epsilon_3$ かつ $1+\epsilon_3 = -\epsilon_3^2$ より, $\eta(1+\epsilon_3) = \eta(1+\epsilon_3^2) = \eta(-1) = (-1)^{\frac{q-1}{2}}$ を得る. 一方, 平方剰余の相互法則の補助法則より, $\eta(2) = (-1)^{\frac{p^2-1}{8}}$ を得る. よって, $\eta(2) \neq \eta(1+\epsilon_3^i)$, $i = 1, 2$ は, $q \equiv 5, 7 \pmod 8$ の場合に限る. 最後に, $q \equiv 1 \pmod 3$ という条件より, 結果を得る. □

命題 3.17. ([7, Proposition 5.10]) $q \equiv 2$ または $4 \pmod 7$ とする. このとき, $\mathbb{F}_{q^3}$ において, 全ての $i = 1, 2, \ldots, 6$ で $\eta(2) \neq \eta(1+\epsilon_7^i)$ が成立するための必要十分条件は, $q \equiv 11, 37, 51, 53 \pmod{54}$ である.

証明: $1+\epsilon_7^\ell = 1+\epsilon_7^{q\ell} = 1+\epsilon_7^{q^2\ell}$ かつ $\prod_{i=0}^2 \eta(1+\epsilon_7^{2^i\ell}) = 1$ より, $\eta(1+\epsilon_7^i) = 1$, $i = 1, 2, \ldots, 6$ を得る. よって, 平方剰余の相互法則の補助法則より, 全ての $i = 1, 2, \ldots, 6$ で $\eta(2) \neq \eta(1+\epsilon_7^i)$ となる必要十分条件は, $q \equiv 3, 5 \pmod 8$ である. 最後に, $q \equiv 2, 4 \pmod 7$ という条件より, 結果を得る. □

命題 3.18. $q \equiv 4$ または $16 \pmod{21}$ とする. このとき, $\mathbb{F}_{q^3}$ において, 全ての $i = 1, 2, \ldots, 20$ で $\eta(2) \neq \eta(1+\epsilon_{21}^i)$ が成立するための必要十分条件は, $q \equiv 37, 109 \pmod{168}$ である.

証明: $X = \{1, 4, 16\}$ とする. 命題 3.15 より, $\prod_{i\in X} \eta(1+\epsilon_{21}^{i\ell}) = \eta(-1)$ を得る. 一方, フロベニウス自己同型を作用させて, $\eta(1+\epsilon_{21}^\ell) = \eta(1+\epsilon_{21}^{4\ell}) = \eta(1+\epsilon_{21}^{16\ell})$ を得る. よって, $\eta(1+\epsilon_{21}^\ell) = \eta(-1)$ が $\gcd(\ell, 21) = 1$ なるすべての ℓ で成り立つ. さらに, 命題 3.17 の証明より, $\eta(1+\epsilon_7^i) = 1$, $i = 1, 2, \ldots, 6$ が成り立つ. また, 命題 3.16 の証明より, $\eta(1+\epsilon_3^i) = \eta(-1)$, $i = 1, 2$ を得る. よって, 平方剰余の相互法則の補助法則より, 全ての $i = 1, 2, \ldots, 21$ で $\eta(2) \neq \eta(1+\epsilon_{21}^i)$ となるための必要十分条件は, $q \equiv 5 \pmod 8$ である. 最後に, $q \equiv 4, 16 \pmod{21}$ という条件より, 結果を得る. □

注意 3.19. $M=21$ の場合について, 系 3.13 (1)–(4) より, $\eta(1+\epsilon_{21}^{i})$ らの間の以下の等式を得る: $\prod_{i\in\{1,2,4,8,16,11\}}\eta(1+\epsilon_{21}^{i\ell})=1$, $\prod_{i\in\{1,8\}}\eta(1+\epsilon_{21}^{i\ell})=1$, $\prod_{i\in\{1,4,10,13,16,19\}}\eta(1+\epsilon_{21}^{i\ell})=1$, $\eta(1+\epsilon_{21}^{\ell})=\eta(1+\epsilon_{21}^{-\ell})$. ここで, ℓ は $\gcd(\ell,M)=1$ なる任意の正整数とする. このとき, $\prod_{i\in\{1,4,16\}}\eta(1+\epsilon_{21}^{i})=\eta(-1)$ はこれらの関係式からは得られないことは明らかであるので, 命題 3.15 は系 3.13 (1)–(4) に含まれないことが分かる.

$\mathcal{P}_M$ を $M\,|\,q^2+q+1$ を満たす素数ベキの集合とする. また, $\alpha,\beta\in\{1,-1\}$ に対し,

$$\Psi_{M,\alpha,\beta}=\{q\in\mathcal{P}_M:\eta(1+\epsilon_M^{i})=\alpha, 1\le i<M, \eta(-1)=\beta\}$$

と定める. このとき, 命題 3.8 の観点から, $\Psi_{M,\alpha,\beta}$ がいつ空になるのかについて調べる.

命題 3.20. *(1)* $-1\in\langle 2\rangle\pmod M$ であるとき, $\Psi_{M,1,-1}=\emptyset$ である.

(2) $-1\in\langle 2\rangle\pmod M$, かつ, $\mathrm{ord}_M(2)/2$ が偶数であるとき, $\Psi_{M,-1,-1}=\emptyset$ である.

(3) $-1\in\langle 2\rangle\pmod M$, かつ, $\mathrm{ord}_M(2)/2$ が奇数のとき, $\Psi_{M,-1,1}=\emptyset$ である.

(4) $\mathrm{ord}_M(2)$ が奇数のとき, $\beta=1,-1$ 双方の場合について, $\Psi_{M,-1,\beta}=\emptyset$ である.

証明: (1) $q\equiv 3\pmod 4$ かつ $-1\in\langle 2\rangle\pmod M$ のとき, 系 3.13 (3) より, $\prod_{i=0}^{\mathrm{ord}_M(2)/2-1}\eta(1+\epsilon_M^{2^i})=-1$ が成り立つ. このとき, すべての $i=1,2,\dots,M-1$ で $\eta(1+\epsilon_M^{i})=1$ が成り立つことは不可能である.

(2) $q\equiv 3\pmod 4$ かつ $-1\in\langle 2\rangle\pmod M$ のとき, 系 3.13 (3) より, $\prod_{i=0}^{\mathrm{ord}_M(2)/2-1}\eta(1+\epsilon_M^{2^i})=-1$ が成り立つ. 一方, $\mathrm{ord}_M(2)/2$ が偶数で, すべての $i=1,2,\dots,M-1$ で $\eta(1+\epsilon_M^{i})=-1$ と仮定すると, $\prod_{i=0}^{\mathrm{ord}_M(2)/2-1}\eta(1+\epsilon_M^{2^i})=1$ を得る. これは矛盾である.

(3) $q\equiv 1\pmod 4$ かつ $-1\in\langle 2\rangle\pmod M$ のとき, 系 3.13 (3) より, $\prod_{i=0}^{\mathrm{ord}_M(2)/2-1}\eta(1+\epsilon_M^{2^i})=1$ が成り立つ. 一方, $\mathrm{ord}_M(2)/2$ が奇数で, すべての $i=1,2,\dots,M-1$ で $\eta(1+\epsilon_M^{i})=-1$ と仮定すると, $\prod_{i=0}^{\mathrm{ord}_M(2)/2-1}\eta(1+\epsilon_M^{2^i})=-1$ を得る. これは矛盾である.

(4) 系 3.13 (2) より, $\prod_{i=0}^{\mathrm{ord}_M(2)-1}\eta(1+\epsilon_M^{2^i})=1$ を得る. 一方, すべての $i=1,2,\dots,M-1$ で $\eta(1+\epsilon_M^{i})=-1$ と仮定すると, $\prod_{i=0}^{\mathrm{ord}_M(2)-1}\eta(1+\epsilon_M^{2^i})=-1$ を得る. これは矛盾である. □

4 $\Psi_{M,h,\alpha,\beta}$ 内の素数の無限存在性について

h を $M\,|\,h^2+h+1$ を満たす正整数とし, $\mathcal{P}_{h,M}$ を $p\equiv h\pmod M$ なる素数の集合とする. 各 $\alpha,\beta\in\{1,-1\}$ に対し,

$$\Psi_{M,h,\alpha,\beta}=\{p\in\mathcal{P}_{h,M}:\mathbb{F}_{p^3}\text{において}\eta(1+\epsilon_M^{i})=\alpha, 1\le i\le M-1, \eta(2)=-\alpha, \eta(-1)=\beta\}$$

と定める. この章では, $\Psi_{M,h,\alpha,\beta}$ 内の素数の無限存在性に興味がある. これを調べるために, よく知られた Dirichlet の素数定理の一般化である, Chebotarëv の密度定理について述べる.

F を代数体 E のガロア拡大とする. $\mathcal{O}_F$ と $\mathcal{O}_E$ で, F と E の整数環を表す. $\mathfrak{p}$ を F で不分岐な E の素イデアルとし, $\mathfrak{P}$ を F の $\mathfrak{p}$ 上の素イデアルとする. このとき, $\mathrm{Gal}((\mathcal{O}_F/\mathfrak{P})/(\mathcal{O}_E/\mathfrak{p}))$

から $\mathrm{Gal}(F/E)$ への, 唯一の単射準同型写像 h で以下の条件を満たすものがある. 任意の $\sigma \in \mathrm{Gal}((\mathcal{O}_F/\mathfrak{P})/(\mathcal{O}_E/\mathfrak{p}))$ に対し, $h(\sigma)(\mathfrak{P}) = \mathfrak{P}$, かつ, $h(\sigma) : \mathcal{O}_F \to \mathcal{O}_F$ によって誘導される $\mathcal{O}_F/\mathfrak{P}$ からそれ自身への写像が σ そのものに一致する. 特に, フロベニウス自己同型 $x \to x^{|\mathcal{O}_E/\mathfrak{p}|}$ の像 $\sigma_{\mathfrak{P}}$ を, $\mathfrak{P}$ に関するフロベニウス写像と呼ぶ. フロベニウス写像は, $\mathfrak{P}$ に対するガロア群の作用 $\tau \in \mathrm{Gal}(F/E)$ について, $\sigma_{\tau\mathfrak{P}} = \tau\sigma_{\mathfrak{P}}\tau^{-1}$ が成立しているため, $\mathfrak{p}$ の上の素イデアル $\mathfrak{P}$ の選び方と, $\sigma_{\mathfrak{P}}$ の共役類が対応することになる.

$P(E)$ を F で不分岐な E の素イデアルの集合とする. C_σ で $\sigma \in \mathrm{Gal}(F/E)$ を含む共役類とする. 固定した $\sigma \in \mathrm{Gal}(F/E)$ に対し, $P(E)$ の素イデアルの集合 S_σ を以下で定める:

$$S_\sigma = \{\mathfrak{P} \cap E \in P(E) : \mathfrak{P} \text{ は } F \text{ の素イデアルで, } \sigma_{\mathfrak{P}} \in C_\sigma \text{ を満たす }\}.$$

S_σ の Dirichlet 密度を

$$\lim_{s\to 1+0} \Big(\sum_{\mathfrak{p}\in S_\sigma} \frac{1}{N(\mathfrak{p})^s} \Big) \Big/ \Big(\sum_{\mathfrak{p}\in P(E)} \frac{1}{N(\mathfrak{p})^s} \Big)$$

で定義し, また, S_σ の自然密度を

$$\lim_{x\to\infty} \frac{|\{\mathfrak{p} \in S_\sigma : N(\mathfrak{p}) \le x\}|}{|\{\mathfrak{p} \in P(E) : N(\mathfrak{p}) \le x\}|}$$

で定める. 以下の定理が Chebotarëv の密度定理である.

定理 4.1. *S_σ の Dirichlet 密度 (および自然密度) は $\frac{|C_\sigma|}{|G|}$ に等しい. 特に, 非零の場合, S_σ は無限集合である.*

S_σ の Dirichlet 密度と自然密度を $\delta(S_\sigma)$ と記すことにする.

この章の残りで, 定理 1.2 の証明を与えることに徹する. $i = 0, 1, \ldots, M-1$ と $j = 0, 1$ に対し, $x_{i,j} = (-1)^j\sqrt{1+\zeta_M^i}$ とし, $Z_M = \{x_{i,j} : i = 0, 1, \ldots, M-1, j = 0, 1\}$ と定める. E_M を $\mathbb{Q}$ に Z_M の元と ζ_4 を全て添加して得られる体とする. 定理 4.1 を我々の場合に適用するため, E_M の構造について調べる必要がある. E_M について, ガロア理論から以下のことが分かる.

事実 4.2. (i) $\mathbb{Q}(\zeta_M)$ は $\mathbb{Q}$ の正規拡大であるので, $\mathrm{Gal}(E_M/\mathbb{Q}(\zeta_M))$ は $\mathrm{Gal}(E_M/\mathbb{Q})$ の正規部分群である.

(ii) $\mathbb{Q}(\zeta_M, x_{i,0})/\mathbb{Q}(\zeta_M)$, $i = 0, 1, \ldots, M-1$ と $\mathbb{Q}(\zeta_M, \zeta_4)/\mathbb{Q}(\zeta_M)$ は高々2 次の拡大であり, $\mathrm{Gal}(E_M/\mathbb{Q}(\zeta_M))$ は, $\prod_{i=0}^{M-1} \mathrm{Gal}(\mathbb{Q}(\zeta_M, x_{i,0})/\mathbb{Q}(\zeta_M)) \times \mathrm{Gal}(\mathbb{Q}(\zeta_M, \zeta_4)/\mathbb{Q}(\zeta_M))$ の部分群と同型であるので, $\mathrm{Gal}(E_M/\mathbb{Q}(\zeta_M))$ は基本可換 2-群である.

次にクンマーの理論における以下の定理を応用する.

定理 4.3. *K を ζ_n を含む標数 0 の体とし, $(K^\times)^n = \{a^n : a \in K^\times\}$ と定める. R を $(K^\times)^n$ を含む $K^\times$ の部分群とし, $K(\sqrt[n]{R})$ で $\{\sqrt[n]{a} : a \in R\}$ の元を K へ添加して得られる拡大とし, abel 拡大と仮定する. もし, $R/(K^\times)^n$ が有限であれば, $\mathrm{Gal}(K(\sqrt[n]{R})/K)$ は, $R/(K^\times)^n$ に同型である.*

補題 4.4. $\mathrm{Gal}(E_M/\mathbb{Q}(\zeta_M))$ は, $(\mathbb{Q}(\zeta_M)^\times)^2$ を法とした 2 と -1 と $1+\zeta_M^i$, $i = 1, 2, \ldots, M-1$ によって生成される群に同型である.

証明: 定理を 4.3 を, $K=\mathbb{Q}(\zeta_M)$, $n=2$, $R=\langle 2,-1,1+\zeta_M^i, y : i=1,2,\ldots,M-1, y\in(K^\times)^2\rangle$ として適用すれば良い. □

補題 4.5. $2\notin\langle -1,1+\zeta_M^i, y : i=1,2,\ldots,M-1, y\in(\mathbb{Q}(\zeta_M)^\times)^2\rangle$ が成立する.

証明: ある $x\in\mathbb{Q}(\zeta_M)$ が存在し, $2=-1^{i_0}\prod_{i=1}^{M-1}(1+\zeta_M^i)^{c_i}\cdot x^2$ と仮定する. $-1^{i_0}\prod_{i=1}^{M-1}(1+\zeta_M^i)^{c_i}$ は単数であるので, x は $\mathbb{Q}(\zeta_M)$ の単数ではない. このとき, (2) は $\mathbb{Q}(\zeta_M)$ で分岐するが, M は奇数なのであり得ない. □

補題 4.6. $-1\in\langle 1+\zeta_M^i, y : i=1,2,\ldots,M-1, y\in(\mathbb{Q}(\zeta_M)^\times)^2\rangle$ であるための必要十分条件は, M を割るある整数 $M'>1$ が存在し, $-1\in\langle 2\rangle \pmod{M'}$ となることである.

証明: M を割る任意の整数 $M'>1$ に対し, $-1\notin\langle 2\rangle \pmod{M'}$ とし, ある c_i らと $x\in\mathbb{Q}(\zeta_M)$ が存在し, $-1=\prod_{i=1}^{M-1}(1+\zeta_M^i)^{c_i}\cdot x^2$ と書けると仮定する. $\sigma\in\mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ を $\sigma:\zeta_M\to\zeta_M^2$ なる自己同型とする. $\mathrm{ord}_M(2)$ は奇数であるので,

$$\prod_{i=0}^{\mathrm{ord}_M(2)-1}\sigma^i(-1)=-1$$

を得る. 一方, 補題 3.10 より,

$$\prod_{i=0}^{\mathrm{ord}_M(2)-1}\Big(\prod_{j=1}^{M-1}\sigma^i(1+\zeta_M^j)^{c_j}\Big)\sigma^i(x)^2=\prod_{i=0}^{\mathrm{ord}_M(2)-1}\sigma^i(x)^2$$

を得る. よって, -1 が $\mathbb{Q}(\zeta_M)$ で平方数になる. しかし, それは M が奇数であることに矛盾する.

逆に, M を割るある整数 $M'>1$ が存在し, $-1\in\langle 2\rangle \pmod{M'}$ となると仮定すると, 補題 3.11 より, $-1=\prod_{i=0}^{\mathrm{ord}_{M'}(2)/2-1}\sigma^i(1+\zeta_{M'})$ を得る. □

D_M を $x_{i,0}$, $1\le i\le M-1$ の元をすべて $\mathbb{Q}$ へ添加して得られる体とする. これまでの結果をまとめて以下の命題を得る.

命題 4.7. *(1)* M を割る任意の整数 $M'>1$ に対し, $-1\notin\langle 2\rangle \pmod{M'}$ であるとき, $\mathrm{Gal}(E_M/\mathbb{Q}(\zeta_M))$ は $\mathrm{Gal}(\mathbb{Q}(\zeta_M,\sqrt{2})/\mathbb{Q}(\zeta_M))\times\mathrm{Gal}(\mathbb{Q}(\zeta_M,\zeta_4)/\mathbb{Q}(\zeta_M))\times\mathrm{Gal}(D_M/\mathbb{Q}(\zeta_M))$ に同型である.

(2) M を割るある整数 $M'>1$ に対し, $-1\in\langle 2\rangle \pmod{M'}$ であるとき, $\mathrm{Gal}(E_M/\mathbb{Q}(\zeta_M))$ は $\mathrm{Gal}(\mathbb{Q}(\zeta_M,\sqrt{2})/\mathbb{Q}(\zeta_M))\times\mathrm{Gal}(D_M/\mathbb{Q}(\zeta_M))$ に同型である.

特に, $\mathrm{Gal}(D_M/\mathbb{Q}(\zeta_M))$ は $(\mathbb{Q}(\zeta_M)^\times)^2$ を法とする $1+\zeta_M^i$, $i=1,2,\ldots,M-1$ によって生成される群に同型である.

さらに以下のことも導かれる.

系 4.8. *(1)* M を割る任意の整数 $M'>1$ に対し, $-1\notin\langle 2\rangle \pmod{M'}$ であるとき, $\mathrm{Gal}(E_M/\mathbb{Q})$ は $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})\times\mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q})\times\mathrm{Gal}(D_M/\mathbb{Q})$ に同型である. 特に, その同型対応は, 群の埋め込みを与える.

(2) M を割るある整数 $M'>1$ に対し, $-1\in\langle 2\rangle \pmod{M'}$ であるとき, $\mathrm{Gal}(E_M/\mathbb{Q})$ は $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})\times\mathrm{Gal}(D_M/\mathbb{Q})$ に同型である. 特に, その同型対応は, 群の埋め込みを与える.

定理 4.1 を適用する準備ができたので, そのセッティングを行う. $\mathcal{O}_{E_M}$ を E_M の整数環とする. $M \mid h^2+h+1$ を満たす整数 $1 \leq h \leq M-1$ を任意に固定し, p を $p \equiv h \pmod{M}$ を満たす E_M で不分岐な素数とする. さらに, $\mathfrak{P}$ を E_M の (p) の上の素イデアルとする. π_p を $\mathcal{O}_{E_M}/\mathfrak{P}$ のフロベニウス自己同型とする, すなわち, $\pi_p : x \to x^p$ である. また, $\sigma_{\mathfrak{P}}$ を $E_M/\mathbb{Q}$ の $\mathfrak{P}$ に関するフロベニウス写像とする. ここで, $\mathcal{O}_{E_M}/\mathfrak{P}$ は位数 p^3 の $\mathcal{O}_{\mathbb{Q}(\zeta_M)}/\mathfrak{p}$ に同型な部分体を含んでいることに注意する. ここで, $\mathfrak{p} = \mathfrak{P} \cap \mathbb{Q}(\zeta_M)$ である. η を $\mathcal{O}_{\mathbb{Q}(\zeta_M)}/\mathfrak{p}$ の位数 2 の乗法的指標とするとき, π_p と $\sigma_{\mathfrak{P}}$ の関係から以下を得る:

$$
\begin{aligned}
& p \equiv h \pmod{M},\ \eta(1+\zeta_M^i) = \alpha,\ 1 \leq i \leq M-1, \\
& \qquad\qquad \eta(2) = -\alpha \text{ かつ } \eta(-1) = \beta \text{ in } \mathcal{O}_{\mathbb{Q}(\zeta_M)}/\mathfrak{p} \\
\Leftrightarrow\ & \pi_p(\zeta_M + \mathfrak{P}) = \zeta_M^h + \mathfrak{P},\ \pi_p^3(x_{i,0} + \mathfrak{P}) = \alpha x_{i,0} + \mathfrak{P},\ 1 \leq i \leq M-1, \\
& \qquad\qquad \pi_p^3(\sqrt{2} + \mathfrak{P}) = -\alpha\sqrt{2} + \mathfrak{P} \text{ かつ } \pi_p^3(\zeta_4 + \mathfrak{P}) = \beta\zeta_4 + \mathfrak{P} \\
\Leftrightarrow\ & \sigma_{\mathfrak{P}}(\zeta_M) = \zeta_M^h,\ \sigma_{\mathfrak{P}}^3(x_{i,0}) = \alpha x_{i,0},\ 1 \leq i \leq M-1, \\
& \qquad\qquad \sigma_{\mathfrak{P}}^3(\sqrt{2}) = -\alpha\sqrt{2} \text{ かつ } \sigma_{\mathfrak{P}}^3(\zeta_4) = \beta\zeta_4. \qquad (4.1)
\end{aligned}
$$

D'_M を, D_M に ζ_4 を添加して得られる体とする. 今, 定理 4.1 を $F = E_M$, $E = \mathbb{Q}$, $G = \mathrm{Gal}(E_M/\mathbb{Q})$ として適用する.

定理 4.9. *h を $M \mid h^2+h+1$ かつ $1 \leq h \leq M-1$ を満たす整数とする. このとき,*

(1) $\Psi_{M,h,1,1} \cup \Psi_{M,h,1,-1}$ *は無限集合.*

(2) M *を割る任意の整数 $M' > 1$ に対し, $-1 \notin \langle 2 \rangle \pmod{M'}$ であれば, $\Psi_{M,h,1,1}$ と $\Psi_{M,h,1,-1}$ の双方が無限集合である.*

証明: $\sigma(\zeta_M) = \zeta_M^h$, $\sigma^3(x_{i,0}) = x_{i,0}$, $1 \leq i \leq M-1$, $\sigma^3(\sqrt{2}) = -\sqrt{2}$ を満たす ((2) については, 各 $\beta \in \{1,-1\}$ に対し, $\sigma^3(\zeta_4) = \beta\zeta_4$ も満たす)$\sigma \in \mathrm{Gal}(E_M/\mathbb{Q})$ が存在することを示す. このとき, 定理 4.1 より, $\delta(S_\sigma) > 0$ を得る. また, 同値性 (4.1) より, $\mathbb{F}_{p^3}$. において $p \equiv h \pmod{M}$, $\eta(1+\epsilon^i) = 1$, $1 \leq i \leq M-1$, $\eta(2) = -1$ を満たす ((2) については, 各 $\beta \in \{1,-1\}$ に対し, $\eta(-1) = \beta$ も満たす) 素数 p が無限個存在することになる.

(1) $\sigma_1(\sqrt{2}) = -\sqrt{2}$ であるような $\sigma_1 \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ を取る. $\mathrm{Gal}(D'_M/\mathbb{Q})/\mathrm{Gal}(D'_M/\mathbb{Q}(\zeta_M)) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ であり, $\mathrm{Gal}(D'_M/\mathbb{Q}(\zeta_M))$ の任意の元の位数は高々2 より, $\sigma_2(\zeta_M) = \zeta_M^h$ かつ $\sigma_2^3 = \mathrm{id}$ を満たす $\sigma_2 \in \mathrm{Gal}(D'_M/\mathbb{Q})$ が存在する. ここで, $\sigma = (\sigma_1, \sigma_2) \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(D'_M/\mathbb{Q}) \simeq \mathrm{Gal}(E_M/\mathbb{Q})$ とすればよい.

(2) (1) と同様の σ_1 を考える. さらに, $\beta \in \{1,-1\}$ を一つ固定し, $\sigma_2(\zeta_4) = \beta\zeta_4$ なる $\sigma_2 \in \mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q})$ を取る. また, $\mathrm{Gal}(D_M/\mathbb{Q})/\mathrm{Gal}(D_M/\mathbb{Q}(\zeta_M)) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_M)/\mathbb{Q})$ かつ $\mathrm{Gal}(D_M/\mathbb{Q}(\zeta_M))$ の任意の元の位数は高々2 より, $\sigma_3(\zeta_M) = \zeta_M^h$ かつ $\sigma_3^3 = \mathrm{id}$ を満たす $\sigma_3 \in \mathrm{Gal}(D_M/\mathbb{Q})$ が存在する. ここで, $\sigma = (\sigma_1, \sigma_2, \sigma_3) \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_4)/\mathbb{Q}) \times \mathrm{Gal}(D_M/\mathbb{Q}) \simeq \mathrm{Gal}(E_M/\mathbb{Q})$ とすればよい. □

定理 1.2 の証明: M を割る任意の整数 $M' > 1$ に対し, $-1 \notin \langle 2 \rangle \pmod{M'}$ であるとき, 定理 4.9 (2) より, $\Psi_{M,h,1,-1}$ は無限集合である. よって, 定理 3.5 を定理 2.1 と命題 3.8 とともに適用することで結果を得る. □

参考文献

[1] J. Bamberg, M. Lee, K. Momihara, Q. Xiang, A new family of hemisystems of the Hermitian surface, *Combinatorica*, **38**, 43–66, (2018).

[2] J. De Beule, J. Demeyer, K. Metsch, M. Rodgers, A new family of tight sets in $\mathcal{Q}^+(5,q)$, *Des. Codes Cryptogr.* **78**, 655–678, (2016).

[3] T. D. Duc, K. H. Leung, B. Schmidt, Upper bounds for cyclotomic numbers, `arXiv:1903.07321`.

[4] T. Feng, K. Momihara, Q. Xiang, Cameron-Liebler line classes with parameter $x = \frac{q^2-1}{2}$, *J. Combin. Theory Ser. A* **133**, 307–338, (2015).

[5] T. Feng, K. Momihara, Q. Xiang, Three-valued Gauss periods, circulant weighing matrices and association schemes, *J. Algebraic Combin.* **43**, 851–875, (2016).

[6] T. Maruta, Cyclic and pseudo-cyclic MDS codes of dimension three, *Atti Sem. Mat. Fis. Univ. Modena* **43**, 529–533, (1995).

[7] K. Momihara, Constructions of strongly regular Cayley graphs based on three-valued Gauss periods, *Europ. J. Combin.* **70**, 232–250, (2018).

[8] K. Momihara, Q. Xiang, A large family of strongly regular Cayley graphs from three-valued Gauss periods, in **preparation**.

On QMC designs and related topics

平尾 将剛（愛知県立大学 情報科学部）*

1 はじめに

$\mathbb{R}^{d+1}$ を $d+1$ 次元 Euclid 空間とする．$\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^{d+1}$ に対して，その内積を $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ とし，ノルムを $\|\boldsymbol{x}\| = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}$ とする．$\mathbb{S}^d = \{\boldsymbol{x} \in \mathbb{R}^{d+1} \mid \|\boldsymbol{x}\| = 1\}$ を d 次元単位球面とし，σ_d を $\mathbb{S}^d$ 上の正規化された表面測度とする．我々は $\mathbb{S}^d$ の「良い」性質を持つ N 点部分集合 $X_N = \{\boldsymbol{x}_1, \ldots, \boldsymbol{x}_N\}$ に関心があり，特に球面積分に対してよい数値近似精度を与えることができる集合を構成したい．代数的組合せ論においては Delsarte et al. [9] により，多項式に対する球面積分を正確に与える点集合として，**球面上の t-デザイン (spherical t-design)** が導入された[*1]．

Definition 1.1. 任意の $f \in \mathcal{P}_t(\mathbb{R}^{d+1})$ に対して，

$$\frac{1}{N} \sum_{i=1}^{N} f(\boldsymbol{x}_i) = \int_{\mathbb{S}^d} f(\boldsymbol{x}) \, d\sigma_d(\boldsymbol{x})$$

が成り立つとき，X_N を球面上の t-デザインであると言う．ここで $\mathcal{P}_t(\mathbb{R}^{d+1})$ は高々 t 次の $d+1$ 変数多項式からなるベクトル空間とする．

球面デザインは代数的組合せ論をはじめ，数値積分法，統計的実験計画法，情報理論など多岐に渡る応用を持つことが知られている．しかしながら，これまでに例えば，Seymour-Zaslavsky [17], Hardin-Sloane [11] や Bondarenko et al. [5] においてその存在問題は詳細に調べてこられてものの，実際に要求を満たす点集合をどうやって構成すれば良いかに対しては数値解析の実応用に応えるレベルでは解決していないのが現状である[*2]．

球面デザインを一般化・拡張する研究は数多くあるが，その中でも特に数値積分法に特化したひとつの拡張として Brauchart et al. [7] が導入した **QMC (Quasi-Monte Carlo, 準モンテカルロ) デザイン系列**とそれらに関連した話題について本講演では近年の自身の結果を踏まえて紹介する．

* 〒480-1198 愛知県長久手市茨ケ廻間 1522 番 3　愛知県立大学 情報科学部　(e-mail: hirao@ist.aichi-pu.ac.jp)
本研究は JSPS 科研費 16K17645 の助成を受けたものである．

*1 数値積分法においては，特に Chebyshev 型 quadrature (cubature) 公式として知られたものである．

*2 少なくとも統計的実験計画法においては要求される t が小さいことから，応用上の要求を応えることができるレベルでその構成法は与えられていると信じている．例えば，Sawa et al. [16] を参照して欲しい．

QMC デザイン系列とは，多項式に対する球面積分から一歩飛び出し，ある関数クラス (実際には後述するように球面上のソボレフ空間) に対する球面上の積分に対して良い近似を与え，より高速な誤差の収束性を実現する球面上の点列のことをである．

球面積分の近似精度をよくするためには，近似点の個数 N を大きくすると同時にそれらが互いに離れていることが必要になるだろうと想像できる．これは球面上のデザインに対してはいつでも正しいとは限らないが，Brauchart et al. [7] の主結果から，関数クラスを制限してしまえば，このことは正しいことが保証される．

次に問題となるのはどのように QMC デザイン系列を構成・生成するかである．球面上のデザインのように「正確な積分値」ではなく「近似値」を採用したことで，点集合に対する要求も若干軽減されることは想像に難くないと思われるが，やはり具体的な構成法を与えることは容易ではない．そのため，Brauchart et al. [7] では，ランダム・サンプリングのひとつである**球面上のジッタード・サンプリング**が QMC デザイン系列を生成することを再発見している．球面上のジッタード・サンプリングとはラフに言えば，球面を面積が等しくなる，かつ，それらの分割した領域の最大半径が「小さくなるよう」に分割したのち，ひとつひとつの分割した領域上で一様分布により点をサンプリングする方法である．この方法で得られる球面上の点配置は予め互いに離れていることが期待され，実際に十分な効果があることを教えてくれる．しかしながら，当然ながら上記のように球面分割するのは容易ではない (球面分割については，Leopardi [15] を参照)．

本講演ではジッタード・サンプリングのよう球面上の確率点過程に焦点を絞る．特にここでは**行列式点過程（Determinantal point process, DPP）**の中のいくつか代表的なものに焦点を絞り，QMC デザイン系列の生成を含む幾つかの話題について扱っていく．DPP は，1970 年代中頃に Macchi によって量子力学的粒子のひとつである**フェルミ粒子**をモデル化するために提案されたランダム点配置からであり，各点間に反発力が働くことからジッタード・サンプリングのように我々が強制的に点通しを離さなくても，自動的にジッタード・サンプリングに近い状況を生成してくれるからである．また，解析的な扱いが比較的容易であるからでもある．さらには，幾つかのシミュレーションアルゴリズムも提案されているからである (例えば，DPP に関する詳細なサーベイとして Hough et al. [14] を挙げることができる)．

本講演では先に述べたように球面上の DPP の中でも代表的な**球面アンサンブル (spherical ensemble)**, **調和アンサンブル (harmonic ensemble)** を中心に扱う．次章の最初に球面上の Sobolev 空間における QMC デザイン系列の定義を紹介し，特に上記の 2 つの DPP を用いることにより，(多少空間は異なるが) QMC デザイン系列が確率的に生成できることを紹介する．さらに代数的組合せ論の研究者にも馴染みにある**フレーム・ポテンシャル**を調べることにより，これらの DPP から得られる点配置が球面デザインにどれだけ近い構造なのかを考察していく．

2 QMC デザイン

2.1 球面上の Sobolev 空間と QMC デザイン

本節では球面上の Sobolev 空間と QMC デザインを扱う．そのために先ずは球面 $\mathbb{S}^d$ 上の Sobolev 空間の定義から行う．特に本講演で扱う Sobolev 空間は再生核 Hilbert 空間であることが種々の解析を行う上で非常に有効に働くことを注意しておく．

l 次の球面上の斉次調和多項式の作るベクトル空間を $\mathrm{Harm}_l(\mathbb{S}^d)$ とし，その次元を $Z(d,t) = \dim(\mathrm{Harm}_l(\mathbb{S}^d)))$ で表すことにする．$Y_{l,k}(\boldsymbol{x}), k = 1, \ldots, Z(d,t)$ を次の条件を満たす $\mathrm{Harm}_l(\mathbb{S}^d)$ の正規直交基底とする．

$$\int_{\mathbb{S}^d} Y_{l_1,k_1}(\boldsymbol{x}) Y_{l_2,k_2}(\boldsymbol{x})\, d\sigma_d(\boldsymbol{x}) = \delta_{l_1,l_2}\delta_{k_2,k_2}$$

を満たす．ここでやや乱暴だが，パラメータ $s \geq 0$ の Sobolev 空間 $\mathbb{H}^s(\mathbb{S}^d)$ を次の性質を満たす関数 $f \in \mathbb{L}_2(\mathbb{S}^d)$ の作るベクトル空間として定義する．$f \in \mathbb{L}_2(\mathbb{S}^d)$ のフーリエ係数

$$\hat{f}_{l,k} := \langle f, Y_{l,k} \rangle_{\mathbb{L}_2(\mathbb{S}^d)} = \int_{\mathbb{S}^d} f(\boldsymbol{x}) Y_{l,k}(\boldsymbol{x})\, d\sigma_d(\boldsymbol{x})$$

について，$\lambda_l := l(l+d-1)$ として，

$$\sum_{l=0}^{\infty} \sum_{k=1}^{Z(d,l)} (1+\lambda_l)^s |\hat{f}_{l,k}|^2 < \infty$$

を満たすものとして話を進める (より詳細については，Brauchart et al. [7] を参照)．このとき，$\mathbb{H}^0(\mathbb{S}^d) = \mathbb{L}_2(\mathbb{S}^d)$ であり，また $s > s'$ に対して，$\mathbb{H}^s(\mathbb{S}^d) \subset \mathbb{H}^{s'}(\mathbb{S}^d)$ が成り立つことに注意する．また，$\mathbb{H}^s(\mathbb{S}^d)$ の内積は，$a_l^{(s)} \asymp (1+\lambda_l)^{-s} \asymp (1+l)^{-2s}$ を満たす実正数列 $\{a_l^{(s)}\}_{l\geq 0}$ に対し，

$$\langle f, g \rangle_{\mathbb{H}^s} := \sum_{l=0}^{\infty} \sum_{k=1}^{Z(d,l)} \frac{1}{a_l^{(s)}} \hat{f}_{l,k} \hat{g}_{l,k}$$

とし，ノルムは

$$\|f\|_{\mathbb{H}^s} := \left[\sum_{l=0}^{\infty} \sum_{k=1}^{Z(d,l)} \frac{1}{a_l^{(s)}} |\hat{f}_{l,k}|^2 \right]^{1/2}$$

とする．

球面上の Sobolev 空間 $\mathbb{H}^s(\mathbb{S}^d)$ の解析において重要となるのが，先述したようにこれが再生核 Hilbert 空間になることである．例えば，Brauchart et al. [7] におけるジッタード・サンプリングの近似性能の評価は，内積をデリケートに選ぶことにより，再生核が以下のようにコンパクトな表示を持つことを利用している (Cui-Freeden [8] で提示された distance kernel の一般化であることから，Brauchart らは，**generalized distance kernel** と呼んでいる)．

- $d/2 < s < d/2+1$ に対して，

$$K_{\mathrm{gd}}^{(s)}(\boldsymbol{x},\boldsymbol{y}) := 2V_{d-2s}(\mathbb{S}^2) - |\boldsymbol{x}-\boldsymbol{y}|^{2s-d}, \quad \forall \boldsymbol{x},\boldsymbol{y} \in \mathbb{S}^d. \tag{1}$$

- $d/2+L < s < d/2+L+1$ (L は正整数) に対して，

$$K_{\mathrm{gd}}^{(s)}(\boldsymbol{x},\boldsymbol{y}) := \left(1-(-1)^{L+1}\right) V_{d-2s}(\mathbb{S}^d) + \mathcal{Q}_L(\langle \boldsymbol{x},\boldsymbol{y}\rangle) + (-1)^{L+1}|\boldsymbol{x}-\boldsymbol{y}|^{2s-d}, \quad \boldsymbol{x},\boldsymbol{y} \in \mathbb{S}^d. \tag{2}$$

ここで

$$\mathcal{Q}_L(\langle \boldsymbol{x},\boldsymbol{y}\rangle) := \sum_{l=1}^{L} \left((-1)^{L+1-l}-1\right) \alpha_l^{(s)} Z(d,l) P_l^{(d)}(\langle \boldsymbol{x},\boldsymbol{y}\rangle).$$

であり，$P_l^{(d)}$ は正規化された Gegenbaur (もしくは Legendre) 多項式である．

Sobolev 空間 $\mathbb{H}^s(\mathbb{S}^d)$ において，積分 $I(f) = \int_{\mathbb{S}^d} f(\boldsymbol{x})\, d\sigma_d(\boldsymbol{x})$ に対する N 点集合 $X_N \subset \mathbb{S}^d$ での近似 $Q[X_N](f) := \frac{1}{N}\sum_{\boldsymbol{x}\in X_N} f(\boldsymbol{x})$ における最悪誤差 (worst-case error) を

$$\mathrm{wce}(Q[X_N]; \mathbb{H}^s(\mathbb{S}^d)) := \sup_{\substack{f\in\mathbb{H}^s(\mathbb{S}^d) \\ \|f\|_{\mathbb{H}^s}\le 1}} |Q[X_N](f) - I(f)|$$

で定義する．このとき，$\mathbb{H}^s(\mathbb{S}^d)$ 上の QMC デザイン系列は次で定義される．

Definition 2.1 ($\mathbb{H}^s(\mathbb{S}^d)$ 上の QMC デザイン系列, [7])**.** $s > d/2$ とし，$\{X_N\}$ を $\mathbb{S}^d$ 上の点集合の増大列とする．このとき，N に依存しない定数 $c(s,d) > 0$ が存在し，

$$\mathrm{wce}(Q[X_N]; \mathbb{H}^s(\mathbb{S}^d)) \le \frac{c(s,d)}{N^{s/d}}. \tag{3}$$

が成り立つとき，増大列 $\{X_N\}$ を $\mathbb{H}^s(\mathbb{S}^d)$ 上の *QMC* デザイン系列であると言う．

また最近では，Brauchart et al. [7] により，一般の Sobolev 空間 $W_p^s(\mathbb{S}^d)$ 上の QMC デザインや，球面以外の多様体上の Sobolev 空間における QMC デザインが定義されている．また，近年では Brauchart らにより，有限点集合に対する hyperuniformity の観点からの研究も進められていることを注意しておく．

2.2 DPP と QMC デザイン

本節では行列式点過程 (DPP) の非常に大まかなレビューを最初に与える．非常に良くまとまったサーベイが数多くあり，詳細については例えば，Hough et al. [14] を参照して欲しい．ここで $\mathbb{K}(\boldsymbol{x},\boldsymbol{y}) : \mathbb{S}^d \times \mathbb{S}^d \to \mathbb{R}$ を可測関数とする．

Definition 2.2 ($\mathbb{S}^d$ 上の行列式点過程)**.** $\mathbb{S}^d$ 上のランダム点過程がカーネル $\mathbb{K}$ に関する行列式点過程であるとは，σ_d に関する k 点相関関数 $\rho_k : (\mathbb{S}^d)^k \to \mathbb{R}_{\ge 0}$ が

$$\rho_k(\boldsymbol{x}_1,\ldots,\boldsymbol{x}_k) = \det(\mathbb{K}(\boldsymbol{x}_i,\boldsymbol{x}_j))_{1\le i,j\le k}, \quad \forall k \ge 1$$

で与えられることである．すなわち，関数 $h : (\mathbb{S}^d)^k \to [0,\infty)$ に対して，

$$\mathbb{E}\left(\sum_{\boldsymbol{x}_1,\dots,\boldsymbol{x}_k\in\mathcal{X}}^{\neq} h(\boldsymbol{x}_1,\dots,\boldsymbol{x}_k)\right)$$
$$=\int_{\mathbb{S}^d}\cdots\int_{\mathbb{S}^d}\rho_k(\boldsymbol{x}_1,\dots,\boldsymbol{x}_k)h(\boldsymbol{x}_1,\dots,\boldsymbol{x}_k)\,d\sigma_d(\boldsymbol{x}_1)\cdots d\sigma_d(\boldsymbol{x}_k).$$

が成り立つことである．

最初に代表的な行列式点過程のひとつである**球面アンサンブル (spherical ensemble)** を紹介する．A_N, B_N を各成分が独立で標準複素ガウス分布に従う $N\times N$ とし，$A_N^{-1}B_N$ の固有値を $\{\lambda_1,\lambda_2,\dots,\lambda_N\}$ とする．このとき，このランダム固有値の集合は，カーネル

$$\mathbb{K}(\boldsymbol{x},\boldsymbol{y})=(1+\boldsymbol{x}\bar{\boldsymbol{y}})^{N-1}$$

に関する行列式点過程である．ここで g を平面 $\{(t_1,t_2,0)\mid t_1,t_2\in\mathbb{R}\}$ から 2 次元球面 $\mathbb{S}^2$ へのステレオ写像とすると，集合 $\mathcal{X}_N:=\{\boldsymbol{x}_i=g^{-1}(\lambda_i)\mid 1\le i\le N\}$ はまた，$\mathbb{S}^2$ 上の行列式点過程となる．例えば，$\mathbb{S}^2$ 上の 2 点間相関関数は次で与えられる ([1])．

$$\rho_2(\boldsymbol{x},\boldsymbol{y})=\left(\frac{N}{4\pi}\right)^2\left\{1-\left(\frac{|\boldsymbol{x}-\boldsymbol{y}|^2}{4}\right)^{N-1}\right\},\quad \boldsymbol{x},\boldsymbol{y}\in\mathbb{S}^2.$$

次に自然数 L を固定し，$\mathbb{K}_L(\boldsymbol{x},\boldsymbol{y})$ を多項式空間 $\mathcal{P}_L(\mathbb{S}^d)$ の再生核とする．このとき，再生核 $\mathbb{K}_L(\boldsymbol{x},\boldsymbol{y})$ をもとに $N=\dim(\mathcal{P}_L(\mathbb{S}^d))\asymp L^d$ 点での d 次元球面 $\mathbb{S}^d$ 上の行列式点過程 $\mathcal{X}_N$ が存在することが知られている ([14])．この行列式点過程は**調和アンサンブル (harmonic ensemble)** とも呼ばれる．例えば，この行列式点過程の 2 点相関関数は次で与えられる．

$$\rho_2(\boldsymbol{x},\boldsymbol{y})=\det\begin{bmatrix}R_L(1) & R_L(\boldsymbol{x}\cdot\boldsymbol{y})\\ R_L(\boldsymbol{x}\cdot\boldsymbol{y}) & R_L(1)\end{bmatrix}=R_L(1)^2-R_L(\boldsymbol{x}\cdot\boldsymbol{y})^2. \tag{4}$$

ここで $R_L(x)$ は区間 $[-1,1]$, 重み関数 $(1-x)^{d/2}(1+x)^{d/2-1}$ の積分に対するある直交多項式である．詳細については更なる詳細については，例えば，Hough et al. [14] を参照して欲しい．

2.3 QMC デザインに関する主結果

本節では球面上の行列式点過程から準モンテカルロ系列デザインが確率的に生成できることを紹介する．主張の証明は省略し，Hirao [12] にそれらは譲ることにする．ただし，本質的には $d/2<s<d/2+1$ における最悪誤差 $\mathrm{wce}(Q[X_N];\mathbb{H}^s(\mathbb{S}^d))$ は generalized distance kernel を用い，次のように **(離散) リース・ポテンシャル**の計算に帰着できること，

$$\mathrm{wce}(Q[X_N];\mathbb{H}^s(\mathbb{S}^d))=\left(V_{d-2s}(\mathbb{S}^d)-\frac{1}{N^2}\sum_{i\neq j}|\boldsymbol{x}_j-\boldsymbol{x}_i|^{2s-d}\right)^{1/2}, \tag{5}$$

および，リース・ポテンシャルの計算は 2 点相関関数 ρ_2 を用いた計算に帰着することができることに依っている．最初に 2 次元球面 $\mathbb{S}^2$ の場合における結果を述べる．

Theorem 2.3 ([12])**.** $1 < s < 2$ とする．このとき，上で紹介した球面アンサンブルから定義されるランダム N 点集合 $\mathcal{X}_N$ に対して，

$$E\left[\mathrm{wce}(Q[\mathcal{X}_N];\mathbb{H}^s(\mathbb{S}^2))^2\right] = 2^{2s-2}B(s,N) \tag{6}$$

が成り立つ．ここで $B(s,N)$ はベータ関数である．

ここでスターリングの公式を用いると，固定した s に対して，$B(s,N) \sim \Gamma(s)N^{-s}$ $(N \to \infty)$ であることが分かる．したがって，十分大きな N に対して (6) は平均的に (3) を満たしていることが分かる．したがって，spherical ensemble から定義されるランダム点配置は $\mathbb{H}^s(\mathbb{S}^2)$ に対する QMC デザイン系列を確率的に生成することが分かる．

さらに一般次元の球面 $\mathbb{S}^d$ に関しては，前節で紹介した多項式空間 $\mathcal{P}_L(\mathbb{S}^d)$ から構成される行列式点過程を用いると，次の評価式を得ることができる．

Proposition 2.4 ([12])**.** $\mathcal{X}_N$ を多項式空間 $\mathcal{P}_L(\mathbb{S}^d)$ の再生核 $\mathbb{K}_L(\boldsymbol{x},\boldsymbol{y})$ から構成される $N = \dim(\mathcal{P}_L(\mathbb{S}^d))$ 点の調和アンサンブルであるとする．このとき，$d/2 + 1/2 < s < d/2 + 1$ に対して，N とは独立な定数 $C(s,d) > 0$ が存在し，

$$\mathbb{E}[\{\mathrm{wce}(Q[\mathcal{X}_N];\mathbb{H}^s(\mathbb{S}^d))\}^2] \le \frac{C(s,d)}{N^{1+1/(2d)}}$$

を満たす．

上記の命題は単純なモンテカルロ法を用いるより，調和アンサンブルが Hirao [12] では，任意の $d/2 < s < d/2 + 1$ の滑らかさを持つ Sobolev 空間に対して，QMC デザイン系列を生成するかどうか決定することができなかったが，何度かのディスカッションの後に Marzo により次のように肯定的に解決された．

Theorem 2.5 (Marzo)**.** $\mathcal{X}_N$ を多項式空間 $\mathcal{P}_L(\mathbb{S}^d)$ の再生核 $\mathbb{K}_L(\boldsymbol{x},\boldsymbol{y})$ から構成される $N = \dim(\mathcal{P}_L(\mathbb{S}^d))$ 点の調和アンサンブルであるとする．このとき，$d/2 < s < d/2 + 1/2$ に対して，N とは独立な定数 $C'(s,d) > 0$ が存在し，

$$\mathbb{E}[\{\mathrm{wce}(Q[\mathcal{X}_N];\mathbb{H}^s(\mathbb{S}^d))\}^2] \le \frac{C'(s,d)}{N^{s/d)}}$$

を満たす．

この行列式点過程はパラメータ $d/2 < s < d/2 + 1/2$ の Sobolev 空間 $\mathbb{H}^s(\mathbb{S}^d)$ に対する QMC デザイン系列を確率的に生成するが，$s > d/2 + 1$ の Sobolev 空間 $\mathbb{H}^s(\mathbb{S}^d)$ に対しては通常のモンテカルロ法より速い収束性を示すが，QMC デザイン系列を構成できないことを示している．そこで次が重要な問題であると考えている．

Problem 2.6. $d/2 < s < d/2+1$ とする．このとき，Sobolev 空間 $\mathbb{H}^s(\mathbb{S}^d)$ に対する QMC デザイン系列を生成する行列式点過程のクラスを特定せよ．

また，上記の主張でカバーできなかった $s = \frac{d}{2} + \frac{1}{2}$ に対して，調和アンサンブルは QMC デザイン系列を与えることができるか精査する必要があると考えている．

3 フレーム・ポテンシャル

3.1 p-フレームポテンシャルと DPP

近年，球面点配置の研究は球面が持つポテンシャル・エネルギーを介して調査される傾向がある (例えば，Brauchart-Grabner [6] のサーベイはそれらを俯瞰するのに大いに役立つと思われる)．本節では前章から引き続き，DPP，および，ジッタード・サンプリングで得られる点配置が，球面デザインとどれだけ近い (遠い) 構造なのかを **p-フレーム・ポテンシャル (p-frame potential)** を介して議論していきたい．主結果に関する証明は前節と同様に省略する．それらは Hirao [13] を参照していただきたい．

Definition 3.1 (p-フレーム・ポテンシャル)**.** p を正の実数とする．$\mathbb{S}^d$ 上の N 点部分集合 X_N に対する p-フレーム・ポテンシャルは次で定義される．

$$\mathrm{FP}_p(X_N) = \sum_{i=1}^{N}\sum_{j=1}^{N} |\langle \boldsymbol{x}_i, \boldsymbol{x}_j\rangle|^p.$$

Benedetto-Fickus [4] によって，2-フレーム・ポテンシャルの最小値，および最小値を達成する場合の X_N の分類が与えられている

Theorem 3.2 ([4])**.** n を一つ固定する．このとき，$\mathbb{S}^d$ 上の N 点部分集合に対する 2-フレーム・ポテンシャルついて，次の (i), (ii) が成り立つ．

(i) $N \leq d+1$ のとき， 2-フレーム・ポテンシャルの最小値は N である．さらに最小値を達成するのは，$\mathbb{R}^{d+1}$ の N 個の直交基底である．
(ii) $N \geq d+1$ のとき, 2-フレーム・ポテンシャルの最小値は $N^2/(d+1)$ である．さらに最小値を達成するのは，$\mathbb{R}^{d+1}$ 上の FUNTF をなす n 点部分集合である．

p が偶数の場合は，例えば，次に紹介する Seidelnikov の不等式のように球面デザインとの関連が研究されている (例えば，坂内・坂内 [2], Seidel [18] を参照).

Proposition 3.3 (Seidelnikov の不等式 (cf. [2]))**.** X_N を $\mathbb{S}^d$ 上の N 点部分集合とする．このとき，各 $p \in \mathbb{N}$ に対して次が成り立つ．

$$\sum_{i=1}^{N}\sum_{j=1}^{N}\langle \boldsymbol{x}_i, \boldsymbol{x}_j\rangle^p \geq \begin{cases} N^2\mathrm{PFP}(p), & p\text{が偶数}, \\ 0, & p\text{が奇数}. \end{cases}$$

ここで $\mathrm{PFP}(p) := \int_{\mathbb{S}^d}\int_{\mathbb{S}^d} |\langle \boldsymbol{x}, \boldsymbol{y}\rangle|^p \, d\sigma_d(\boldsymbol{x}) d\sigma_d(\boldsymbol{y})$ である．また，X_N が $\mathbb{S}^d$ 上の t-デザインであることと $1 \le p \le t$ を満たす正整数 p に対して，上式が等式を満たすことは同値である．

また，p が一般の場合は，Bilyk らの研究グループが p-フレーム・ポテンシャルの最小値を達成する場合の X_N の分類等を精力的に行なっており，非常に興味深い．例えば，Bilyk et al.(arXiv:1908.10354, arXiv:1908.00885) を参照して欲しい．

さて，本講演の主題のひとつでえある代表的な行列式点過程のひとつである球面アンサンブル，および，調和アンサンブルに対する p-フレーム・ポテンシャルの計算・評価は次のように与えられる．QMC デザインに関する主結果と同様に本質的には，フレーム・ポテンシャルの計算も 2 点相関関数 ρ_2 を用いた計算に帰着できることに依っている．

Theorem 3.4 ([13])**.** (i) $\mathcal{X}_N$ を $\mathbb{S}^2$ 上の spherical ensemble とする．このとき，

$$\mathbb{E}(\mathrm{FP}_p(\mathcal{X}_N)) = N^2\mathrm{PFP}(p) + N - \frac{N^2 B(N, p+1)}{2^N} - \frac{N^2}{2(p+1)}{}_2F_1(1, 1-N; p+2; \frac{1}{2}).$$

(ii) $\mathcal{X}_N$ を多項式空間 $\mathcal{P}_L(\mathbb{S}^d)$ の再生核 $\mathbb{K}_L(\boldsymbol{x}, \boldsymbol{y})$ から構成される $N = \dim(\mathcal{P}_L(\mathbb{S}^d))$ 点の行列式点過程とする．このとき，

$$\begin{aligned}\mathbb{E}(\mathrm{FP}_p(\mathcal{X}_N)) &= N^2\mathrm{PFP}(p) + N - \frac{|\mathbb{S}^{d-1}|}{|\mathbb{S}^d|}\int_{-1}^{1} |t|^p R_L(t)^2 (1-t^2)^{d/2-1}\, dt \\ &= N^2\mathrm{PFP}(p) + \mathcal{O}(N^{(d-1)/d}) \quad (N \to \infty)\end{aligned}$$

さらに Brauchart et al. [7] で扱われている手法を精査することにより，ジッタード・サンプリングに対しても p-フレーム・ポテンシャルの期待値の上からの評価を与えることができている．

Theorem 3.5 ([13])**.** $\mathbb{S}^d$ 上の等面積に分割された互いに素な部分集合 $D_{1,N}, \ldots, D_{N,N}$ は，i, N に依存しない正定数 c が存在し，$\mathrm{diam} D_{i,N} \le c/N^{1/d}$ を満たすとする．ここで各部分集合 $D_{i,N}$ 上の一様分布から得られるランダム N 点集合を X_N とする．このとき，

$$\mathbb{E}(\mathrm{FP}_p(X_N)) \le N^2\mathrm{PFP}(p)N - N(1 - \frac{c^2}{2N^{2/d}})^{p/2}$$

特に $d = 2$ のとき，上式から次を確かめることができる．

$$\mathbb{E}(\mathrm{FP}_p(X_N)) - N^2\mathrm{PFP}(p) \le N - N(1 - \frac{c^2}{2N^2})^{p/2} \to \frac{pc^2}{4} \quad (N \to \infty)$$

3.2 タイト・フレームと DPP

前節の評価をもとに DPP のもうひとつの応用として，DPP が finite unit norm tight frame の良い近似を与えることを紹介する．

最初に $\mathbb{S}^d$ 上の N 点部分集合 $\{\boldsymbol{x}_i\}_{i=1}^N$ が，$\mathbb{R}^{d+1}$ 上の *finite unit norm frame* であるとは，ある正数 A, B $(0 < A \leq B < \infty)$ が存在し，次の不等式を満たすときにいう:

$$A\|\boldsymbol{x}\|^2 \leq \sum_{i=1}^{N} |\langle \boldsymbol{x}, \boldsymbol{x}_i \rangle|^2 \leq B\|\boldsymbol{x}\|^2, \quad \text{for all } \boldsymbol{x} \in \mathbb{R}^{d+1}.$$

特に $A = B$ のときを **tight frame** とよぶ．また，**finite unit norm tight frame** を今後，**FUNTF** と省略することにする．

次に tight frame の特徴付けに重要な $\mathbb{R}^{d+1}$ 上の N 点部分集合 $\{\boldsymbol{x}_i\}_{i=1}^N$ に対する解析作用素とその共役作用素をそれぞれ次で定義する:

$$F : \mathbb{R}^{d+1} \to \mathbb{R}^N, \quad \boldsymbol{x} \mapsto (\langle \boldsymbol{x}, \boldsymbol{x}_i \rangle)_{i=1}^N \quad \text{(解析作用素)},$$
$$F^* : \mathbb{R}^N \to \mathbb{R}^{d+1}, \quad (c_i)_{i=1}^N \mapsto \sum_{i=1}^{N} c_i \boldsymbol{x}_i \quad \text{(共役作用素)}.$$

次はよく知られた事実である．

Lemma 3.6 (well-known)**.** $\mathbb{S}^d$ 上の N 点部分集合 $\{\boldsymbol{x}_i\}_{i=1}^n$ に対して，次の (i), (ii) は同値である:

(i) $\{\boldsymbol{x}_i\}_{i=1}^N$ が $\mathbb{R}^{d+1}$ 上の FUNTF をなす．　(ii) $F^*F = \frac{1}{d+1}\mathcal{I}_{d+1}$.

代表的な行列式点過程である球面アンサンブル，調和アンサンブル，および，ジッタード・サンプリングにより得られるランダム点配置に着目すると，Ehler [10] が扱っている球面上の一様分布を用いて得られる点集合より，それらのランダム点配置の方が漸近的に FUNTF に近い構造であることを示唆している．

Theorem 3.7 ([13])**.** (i) $\{\boldsymbol{x}_i\}_{i=1}^N$ を $\mathbb{S}^2$ 上の spherical ensemble とする．このとき，

$$\mathbb{E}(\|\frac{1}{n}F^*F - \frac{1}{3}\mathcal{I}_3\|_{\mathcal{F}}^2) = \frac{4}{(N+1)(N+2)}.$$

(ii) L を自然数とし，$N = \dim(\mathcal{P}_L(\mathbb{S}^d)) = \binom{d+L}{d} + \binom{d+L-1}{d}$ とする．$\{\boldsymbol{x}_i\}_{i=1}^N$ を $\mathbb{S}^d$ 上の harmonic ensemble とする．このとき，

$$\mathbb{E}(\|\frac{1}{N}F^*F - \frac{1}{d+1}\mathcal{I}_{d+1}\|_{\mathcal{F}}^2) = \frac{1}{N^2}\frac{d(-d+d^2+4dL+4L^2)}{(d+L)(d+2L+1)(d+2L-1)}\binom{d+L}{d}$$
$$= O(N^{-\frac{d+1}{d}}) \quad (N \to \infty).$$

(iii) $\{\boldsymbol{x}_i\}_{i=1}^N$ を $\mathbb{S}^d$ 上のジッタード・サンプリングとする．このとき，

$$\mathbb{E}(\|\frac{1}{N}F^*F - \frac{1}{d+1}\mathcal{I}_{d+1}\|_{\mathcal{F}}^2) \leq \frac{c^2}{2N^{1+2/d}}.$$

ここで $\|\cdot\|_{\mathcal{F}}$ は Frobenius ノルムである．

4 最後に

最後に QMC デザイン系列，DPP の他の発展，今後の課題について箇条書きして終わりとする．

- Brauchart et al. [7] では，さらに点数のオーダーが $\mathcal{O}(t^d)$ の球面 t-デザインは “infinite strength”を持つことを示している．これは全ての $s > d/2$ に対して，最悪誤差 $\mathrm{wce}(Q(X_N); \mathbb{H}^s(\mathbb{S}^d))$ が N に関して最適な収束レートを持つことを意味している．したがって，この点数のオーダーでの球面 t-デザイン列が構成できれば良いのだが...
- QMC デザイン系列を与える deterministic な点集合として，球面デザインや Fekete 点集合等が知られているが，本質的に新しい集合列は知られていない．準モンテカルロ法で用いられる digital nets 等の構成手法の球面類似はできないだろうか？また，少し話題が変わるかもしれないが，組込み構造を持った球面デザイン (またはその類似物) を構成することはできないだろうか？
- 本講演では代表的な行列式点過程として球面アンサンブルと調和アンサンブルしか扱わなかった．例えば，球面アンサンブルは近年，Beltrán と Etayo によりひとつの一般次元化が与えられている ([3]) が，これこそが球面アンサンブルの一般化だと呼ばれるものが何かは (少なくとも私は) 分かっていない．今後，この方面の研究の進展が望まれる[*3]．
- 近年，Brauchart らの研究グループは “hyperuniformity” と呼ばれる物理の概念を球面上の有限点配置の研究に持ち込み，QMC デザインとの関連を調べている．(離散) リース・ポテンシャルや p-フレーム・ポテンシャルとそれとの関連は明確になっていない．今後，調べる価値がないだろうか？

参考文献

[1] Alishahi, K., Zamani, M.S.: The spherical ensemble and uniform distribution of points on the sphere. Electron. J. Probab. **20**(23), 1–27 (2015)

[2] Bannai, E., Bannai, E.: Algebraic Combinatorics on Spheres. Springer, Tokyo (1999). Japanese

[3] Beltrán, C., Etayo, U.: A generalization of the spherical ensemble to even-dimensional spheres. J. Math. Anal. Appl. **475**(2), 1073–1092 (2019)

[4] Benedetto, J.J., Fickus, M.: Finite normalized tight frames. Adv. Comput. Math **18**(2-4), 357–385 (2003)

[5] Bondarenko, A., Radchenko, D., Viazovska, M.: Optimal asymptotic bounds for spherical designs. Ann. Math. **178**, 443–452 (2013)

[*3] 香取-白井 (arXiv:1903.04945) がおおいな助けのひとつになると考えている．

[6] Brauchart, J.S., Grabner, P.J.: Distributing many points on spheres: minimal energy and designs. J. Complexity **31**(3), 293–326 (2015)

[7] Brauchart, J.S., Saff, E.B., Sloan, I.H., Womersley, R.S.: QMC designs: optimal order quasi-Monte Carlo integration schemes on the sphere. Math. Comput. **83**(290), 2821–2851 (2014)

[8] Cui, J., Freeden, W.: Equidistribution on the sphere. SIAM J. Sci. Comput. **18**(2), 595,609 (1997)

[9] Delsarte, P., Goethals, J.M., Seidel, J.J.: Spherical codes and designs. Geom. Dedicata **6**(3), 363–388 (1977)

[10] Ehler., M.: Random tight frames,. J. Fourier Anal. Appl. **18**(1), 1–20 (2012)

[11] Hardin, R.H., Sloane, N.J.A.: Mclaren's improved snub cube and other new spherical designs in three dimensions. Discrete Comput. Geom. **15**(4), 433–440 (1996)

[12] Hirao, M.: QMC designs and determinantal point processes. In: Monte carlo and quasi-monte carlo methods 2016, pp. 331–343. Springer (2018)

[13] Hirao, M.: On p-frame potentials of determinantal point processes and its application to approximate fintie unit norm tight frames (in preparation)

[14] Hough, J.B., Krishnapur, M., Peres, Y., Virág, B.: Zeros of Gaussian Analytic Functions and Determinantal Point Processes. American Mathematical Society, Providence, RI (2009)

[15] Leopardi, P.: A partition of the unit sphere into regions of equal area and small diameter. Electron. Trans. Numer. Anal. **25**, 309–327 (2006)

[16] Sawa, M., Hirao, M., Kageyama, S.: Euclidean design theory. Springer (2019)

[17] Seymour, P.D., Zaslavsky, T.: Averaging sets: a generalization of mean values and spherical designs. Adv. Math. **52**(3), 213–240 (1984)

[18] Shatalov, O.: Isometric embeddings $l_2^m \to l_p^n$ and cubature formulas over classical fields. Ph.D. thesis, Technion-Israel Institute of Technology, Haifa, Israel (2001)

Reflexive polytopes arising from finite graphs and the unimodality of h^*-vectors

東谷　章弘 *

本研究は、Katharina Jochemko 氏と Mateusz Michałek 氏との共同研究 [4] に基づく。

有限グラフ G から symmetric edge polytope と呼ばれる反射的凸多面体 P_G が構成できる。本稿の主結果は、G が完全二部グラフであるときの P_G の h^* 列を具体的に計算したというものである。本稿では、主結果そのものよりも、結果が得られる過程で用いられる様々なテクニックが非常に興味深いので、紹介したい。

1　格子凸多面体の h^* 列

格子凸多面体とは、有限個の格子点（整数点）の集合 $\{\mathbf{v}_1,\dots,\mathbf{v}_m\} \subset \mathbb{Z}^d$ が存在して $\mathrm{conv}(\{\mathbf{v}_1,\dots,\mathbf{v}_m\}) \subset \mathbb{R}^d$ と表されるときに言う。（ただし $\mathrm{conv}(X)$ は X の凸閉包を表す。）格子凸多面体 $P \subset \mathbb{R}^d$ に対し、$1+\sum_{n=1}^{\infty} |nP \cap \mathbb{Z}^d| t^n$ という母函数を考えると以下のような有理関数になることが知られている：

$$1+\sum_{n=1}^{\infty} |nP \cap \mathbb{Z}^d| t^n = \frac{h_0^* + h_1^* t + \cdots + h_d^* t^d}{(1-t)^{d+1}}$$

（ただし分子の各係数は非負整数である）。母函数の分子に現れる非負整数係数多項式 $h_0^* + h_1^* t + \cdots + h_d^* t^d$ を P の h^* **多項式**といい、係数の列 $(h_0^*, h_1^*, \dots, h_d^*)$ を P の h^* **列**という。P の h^* 多項式を $h_P^*(t)$ で表し、h^* 列を $h^*(P)$ で表す。

2　反射的凸多面体

格子凸多面体 $P \subset \mathbb{R}^d$ が**反射的**であるとは、$\mathbb{R}^d$ の原点が P の内部に含まれる、かつ、

$$P^\vee = \{\mathbf{x} \in \mathbb{R}^d : \langle \mathbf{x}, \mathbf{y} \rangle \leq 1 \ \ \forall \mathbf{y} \in P\}$$

が再び格子凸多面体になるときにいう。（ただし $\langle \cdot, \cdot \rangle$ は $\mathbb{R}^d$ の標準内積を表す。）反射的凸多面体とその h^* 列に関して、以下の特徴付けが知られている：

命題 1 ([2, 3])**.** P を格子凸多面体とし、$h^*(P) = (h_0^*, h_1^*, \dots, h_d^*)$ とする。このとき、P が反射的であることと、$h_i^* = h_{d-i}^*$ $(i = 0, 1, \dots, d)$ が成り立つことが同値である。

*大阪大学大学院情報科学研究科（E-mail:higashitani@ist.osaka-u.ac.jp）　本研究は、科学研究費補助金（若手研究 (B)♯17K14177）の助成を受けている。

3 Symmetric edge polytope

以下、“グラフ” といえば、有限連結単純グラフを指す。グラフ G の頂点集合を $\{1, 2, \ldots, d\}$ とし辺集合を $E(G)$ とする。$\mathbf{e}_1, \ldots, \mathbf{e}_d$ は $\mathbb{R}^d$ の標準基底を表す。このとき、

$$P_G = \mathrm{conv}(\{\mathbf{e}_i - \mathbf{e}_j, \mathbf{e}_j - \mathbf{e}_i : \{i, j\} \in E(G)\}) \subset \mathbb{R}^d$$

とおく。格子凸多面体 P_G を G の **symmetric edge polytope** と呼ぶ ([6, Section 4])。P_G は $(d-1)$ 次元反射的凸多面体になることが知られている。

Symmetric edge polytope の h^* 列に関して、以下が知られている：

(a) v を G の葉とすると、$h^*_{P_G}(t) = (1+t)h^*_{P_{G\setminus v}}(t)$ となる。つまり、G が木ならば、$h^*_{P_G}(t) = (1+t)^{d-1}$ (つまり $h^*_i = \binom{d-1}{i}$ $(i = 0, 1, \ldots, d-1)$) となる。

(b) $G = K_d$ ならば、$h^*_i = \binom{d-1}{i}^2$ $(i = 0, 1, \ldots, d-1)$ となる ([1])。

(c) 他にも、G がサイクルの場合 ([7]) や $G = K_{a,b}$ で $a \leq 3$ の場合 ([5]) の h^* 列が計算されている。

4 主結果

反射的凸多面体は、最も重要な格子凸多面体のクラスの 1 つとして様々な研究が展開されている。特に、反射的凸多面体の h^* 列は、命題 1 から対称になり、その **unimodal 性**（非負整数列 $(a_1, \ldots, a_d)$ が unimodal であるとは、$a_1 \leq \cdots \leq a_k \geq \cdots \geq a_d$ となるときにいう）は盛んに研究されている。より具体的に、symmetric edge polytope の h^* 列は常に unimodal であると予想されており、例えば上述のグラフに関しては unimodal 性も示されている。

本講演の主結果は、以下の定理である。

定理 2. 任意の非負整数 a, b に対し、

$$h^*_{P_{K_{a+1,b+1}}}(t) = \sum_{i=0}^{\min(a,b)} \binom{2i}{i}\binom{a}{i}\binom{b}{i} t^i (1+t)^{a+b+1-2i}$$

が成立する。

この定理の系として、$P_{K_{a+1,b+1}}$ の h^* 列の unimodal 性がしたがう。

5 証明の流れ

定理 2 の証明には様々な道具が用いられている。

以下、頂点集合 $\{v_0, v_1, \ldots, v_a\} \sqcup \{w_0, w_1, \ldots, w_b\}$ 上の完全二部グラフを考える。P_G の頂点 $\mathbf{e}_i - \mathbf{e}_j$ を、$i \to j$ という有向矢とみなし、無向グラフ G の各辺を互いに逆向きの 2 本の有向矢で置き換えた有向グラフと見なして考える。

(i) まず、$P_{K_{a+1,b+1}}$ に付随するトーリックイデアルの**グレブナー基底**を計算することにより、$P_{K_{a+1,b+1}}$ の単模三角形分割を得ることが出来る。このようにして得られた単模三角形分割における各単体は、完全二部グラフ $K_{a+1,b+1}$ における “平面的” 全域木でさらにいくつかの部分構造を禁止したものに対応することがわかる。具体的には、以下の 7 つの構造を禁止した全域木である。

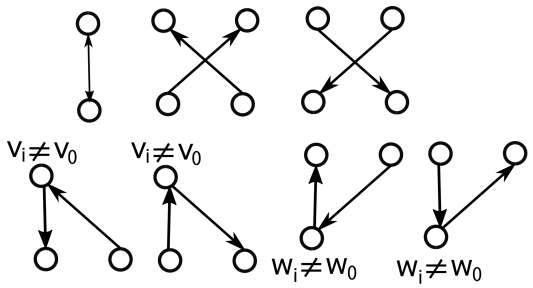

図 1: 7 つの禁止構造

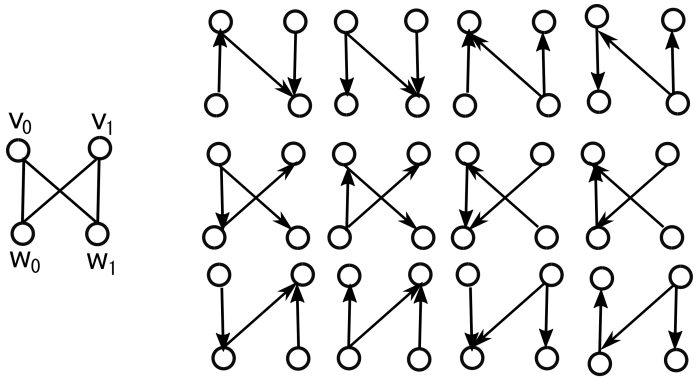

図 2: $K_{2,2}$ の場合：7 つの構造を禁止したものは上記の 12 個になる。

(ii) ここで、以下が成立することがわかる：

$$\sharp\{K_{a+1,b+1}\text{における “平面的” 全域木 }\} = \binom{a+b}{a}$$

証明は、全域木の平面性からただちにしたがう。

(iii) “一般の位置にある点” を用いて **half-open 三角形分割**を以下のようにして得ることが出来る。

- (i) で与えられた単模三角形分割の各 facet F と、一般の位置にある点 x に対し、F の各面の “ON” と “OFF” を決めることで F を half-open facet にする。
- 具体的には、x が F の面の**内側にある**ならば、その facet は “ON” にし、**外側にある**ならば、“OFF” にする。
- Half-open 三角形分割から h^* 列を読み取ることが出来る。具体的には、

$$h_i^* = \#\{\text{“OFF” の面が } i \text{ 個の facet}\}$$

となる。

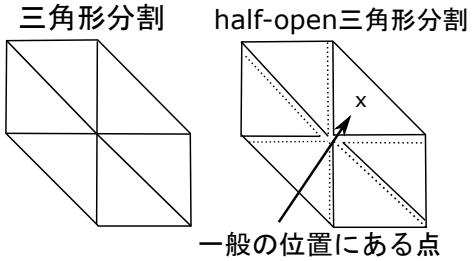

図 3: P_{K_3} の三角形分割と half-open 三角形分割

さらに、各 facet に対応する全域木の言葉で以下のように解釈することが出来る。

- T を上の 7 つの部分構造を禁止した全域木とし、$\vec{e}$ を T の矢とする。
- このとき、$T \setminus \vec{e}$ は 2 つの連結成分 U_1, U_2 に分かれる。w_0 を含む方を U_1 とし、含まない方を U_2 とする。
- ここで、$\vec{e}$ が **ingoing** であるとは、$\vec{e}$ の終点が U_1 で始点が U_2 となっているときにいう。
- 三角形分割の facet に対応する全域木 T に対し、

$$\#\{\text{“OFF” の面}\} = \#\{T \text{ の ingoing 矢}\}.$$

となる。

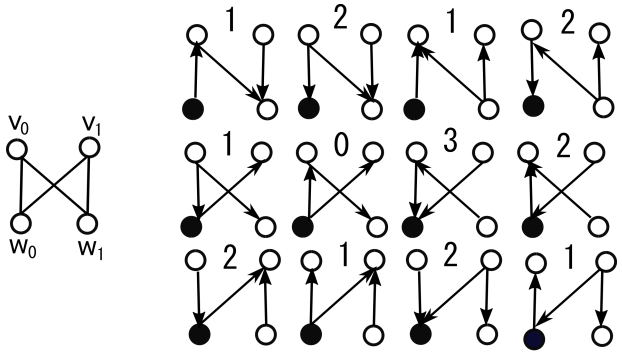

図 4: $K_{2,2}$ の場合：図 2 の各全域木の ingoing 矢の本数

(iv) (iii) で構成した half-open 三角形分割と (ii) の公式を用いて、ingoing 矢の数え上げを注意深く行うと、$P_{K_{a+1,b+1}}$ の h^* 多項式が以下のようになることが分かる：

$$\begin{aligned}
h^*_{P_{K_{a+1,b+1}}}(t) &= \sum_{i=0}^{a}\sum_{j=0}^{b}\binom{a}{i}\binom{b}{j}\binom{i+j}{j}\binom{a-i+b-j-1}{b-j-1}t^{j+a-i} \\
&+ \sum_{i=0}^{a}\sum_{j=0}^{b}\binom{a}{i}\binom{b}{j}\binom{i+j-1}{j-1}\binom{a-i+b-j}{b-j}t^{j+a-i+1} \\
&+ \sum_{i=1}^{a+1}\sum_{j=0}^{b}\binom{a+1}{i}\binom{b}{j}\binom{i+j-1}{i-1}\binom{a-i+b-j}{a-i}t^{j+a-i+1} \\
&= (1+t)\sum_{i=0}^{a}\sum_{j=0}^{b}\binom{a}{i}\binom{b}{j}\binom{a-i+j}{j}\binom{b+i-j}{i}t^{i+j}
\end{aligned}$$

(v) 最後に、以下の等式が証明できる：

$$\sum_{i=0}^{\min(a,b)}\binom{2i}{i}\binom{a}{i}\binom{b}{i}t^i(1+t)^{a+b-2i} = \sum_{i=0}^{a}\sum_{j=0}^{b}\binom{a}{i}\binom{b}{j}\binom{a-i+j}{j}\binom{b+i-j}{i}t^{i+j}$$

この等式は、$K_{a+1,b+1}$ における特殊な 4-彩色の数え上げに注目して、2 通りの数え上げを行うことで証明できる。

まとめると、以下の通りである。

- まず、$P_{K_{a+1,b+1}}$ に付随するグレブナー基底を計算することで、$P_{K_{a+1,b+1}}$ の単模三角形分割を求める。
- 次に、その三角形分割の facet を有向グラフの言葉で（７つの構造を禁止した全域木として）理解する。
- 次に、ある一般の位置にある点を用いて、**half-open 三角形分割**を求め、有向グラフの言葉で解釈する。
- そのようにして求めた half-open 三角形分割から、h^* 多項式を求めることが出来る。
- 最後に、二項係数に関する等式をグラフの 4-彩色の数え上げを用いて計算する。

参考文献

[1] F. Ardila, M. Beck, S. Hoşten, J. Pfeifle and K. Seashore, Root polytopes and growth series of root lattices, *SIAM J. Discrete Math.* **25** 360–378, (2011).

[2] V. Batyrev, Dual polyhedra and mirror symmetry for Calabi–Yau hypersurfaces in toric varieties, *J. Algebraic Geom.* **3** 493–535, (1994).

[3] T. Hibi, Dual polytopes of rational convex polytopes, *Combinatorica* **12** 237–240, (1992).

[4] A. Higashitani, K. Jochemko and M. Michałek, Arithmetic aspects of symmetric edge polytopes, *Mathematika*, **65** 763–784 (2019).

[5] A. Higashitani, M. Kummer and M. Michałek, Interlacing Ehrhart Polynomials of Reflexive Polytopes, *Selecta Math.*, **23** 2977–2998, (2017).

[6] T. Matsui, A. Higashitani, Y. Nagazawa, H. Ohsugi and T. Hibi, Roots of Ehrhart polynomials arising from graphs, *J. Algebr. Comb.* **34** 721–749, (2011).

[7] H. Ohsugi and K. Shibata, Smooth Fano polytopes whose Ehrhart polynomial has a root with large real part, *Discrete Comp. Geom.* **47** 624–628, (2012).

93

The Rudvalis group and the Hoffman-Singleton graph

Masaaki Kitazume (北詰 正顕)

Chiba University (千葉大学)

June 18, 2019

Joint work with Naoki Chigira (Kumamoto Univ.)

The Rudvalis group *Ru*

(0.1) *Ru* : sporadic simple group of order $2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$.

- rank 3 group — the Rudvalis graph [Rudvalis (1984)]
- Point stabilizer $\cong {}^2F_4(2)$ (${}^2F_4(2)'$: Tits' simple group.)
- $4060 = 1 + 1755 + 2304$.

(0.2) L : $\mathbb{Z}[i]$-lattice of rank 28 [Conway (1977)]

- $\mathrm{Aut}(L) = 4 \cdot Ru$

(0.3) $\mathcal{S}$: a set of 4060×4 vectors of $L_4 := \{\ x \in L \mid |x|^2 = (x,x) = 4\ \}$.

- $L = \langle \mathcal{S} \rangle_{\mathbb{Z}[i]}$ [ATLAS, Wilson's book "*Finite Simple Groups*"]

(0.4) $\overline{\mathcal{S}} = \{\ \overline{v} = \{\pm v, \pm iv\} \mid v \in \mathcal{S}\ \}$ $(|\overline{\mathcal{S}}| = 4060)$
$\mathcal{E} = \{\ \{\overline{v}, \overline{u}\} \mid (v,u) = 0\ \}$

- $(\overline{\mathcal{S}}, \mathcal{E}) \cong$ the Rudvalis graph.

The Hoffman-Singleton graph *HoS*

[ATLAS] There are also maximal heptads of 7 minimal vectors with all inner product 1. Each of these is one of a set of 50, whose sum are all congruent modulo 5, and which form a copy of the Hoffman-Singleton graph when intersecting heptads are joined.

- The Hoffman-Singleton graph (*HoS*-graph) :
  strongly regular graph with parameters $(50, 7, 0, 1)$, i.e.
  - diameter $= 2$
  - valency $= 7$
  - no triangles
  - no quadrangles
    $\Longrightarrow \#(\mathit{points}) = 50 (= 1 + 7 + 7 \times 6)$.

The lattice $L = \langle \mathcal{S} \rangle_{\mathbb{Z}[i]}$

(1) $\forall x, y \in \mathcal{S}\ (\overline{x} \neq \overline{y}) : (x, y) = \begin{cases} 0 & (1755 \times 4) \\ \pm 1, \pm i & (2304 \times 4). \end{cases}$

(2) L : even unimodular lattice as a $\mathbb{Z}$-lattice of rank 56.

- $|L_2| = 0$, $|L_4| = 4060 \times 4$ (i.e. $L_4 = \mathcal{S}$)

(2.1) $|L_6| = 18708480$ ($\longleftarrow$ theta series)
$$= \frac{(4060 \times 4) \times 2304}{2}$$

(2.2) $L_6 = \{\ x + y \mid x, y \in L_4, (x, y) = -1\ \}$

Pentads

97

(2.3) (1) $x, y, z \in L_4$ with $(x, y) = (y, z) = (z, x) = -1$
$\Longrightarrow |x + y + z|^2 = 4 + 4 + 4 + 6 \times (-1) = 6$ (i.e. $x + y + z \in L_6$)
$\Longrightarrow \exists u, v \in L_4$ such that $x + y + z + u + v = 0$
(2) $x, y, z, u \in L_4$ with $(x, y) = \cdots = -1$
$\Longrightarrow |x + y + z + u|^2 = 4 \times 4 + 12 \times (-1) = 4$ (i.e. $x + y + z + u \in L_4$)
$\Longrightarrow \exists v \in L_4$ such that $x + y + z + u + v = 0$

Definition 1 (Pentads)

A set $\{x_1, x_2, x_3, x_4, x_5\}$ $(\subset L_4)$ with $x_1 + x_2 + x_3 + x_4 + x_5 = 0$ is called a *pentad*.
Note that all inner products $(x_i, x_j) = -1$ for $i \neq j$.

Heptads (1)

Lemma 1 (Characterization of heptads (by MAGMA))

Let $x, y, z \in L_4$ with $(x, y) = (y, z) = (z, x) = 1$.
Then the set $\{\ w \in L_4 \mid (w, -x) = (w, y) = (w, z) = 1\ \}$ consists of 6 vectors $(w_1, w_2, \ldots, w_6)$. Moreover all inner products $(a, b) = 1$ for $a \neq b \in H := \{-x\} \cup \{w_1, \ldots, w_6\}$.

Definition 2 (Heptads)

The set H in Lemma 1 is called a *heptad*. We set $m(H) = \sum_{v \in H} v$.

(3.1) $H = \{\ w \in L_4 \mid (w, m(H)) = 10\ \}$.

(Proof.) Suppose $(w, m(H)) = (w, a_1 + \cdots + a_7) = 10$. Since $(w, a_j) \in \{0, \pm 1, \pm i, \pm 4, \pm 4i\}$, there exists some j such that $(w, a_j) = 4$ and $(w, a_k) = 1$ for $k \neq j$ (i.e. $w = a_j \in H$). □

Heptads (2)

99

Lemma 2 ("Modulo 5" property (by MAGMA))

Another heptad
$H' = \{x, y, z, \ldots\} = \{\ w \in L_4 \mid (w, x) = (w, w_1) = (w, w_2) = 1\ \}$ is obtained from $-x, w_1, w_2$ by Lemma 1. Then $m(H') = m(H) + 5x$.

(4.1) $H'' = \{\ w \in L_4 \mid (w, x) = (w, w_j) = (w, w_k) = 1\ \} \Longrightarrow H' = H''$.

(Proof.) $m(H'') = m(H) + 5x = m(H')$. By (3.1), $H'' = H'$. □

(4.2) $\forall a \in H \setminus \{-x\}$, $\forall b \in H' \setminus \{x\}$, $(a, b) = 1$.

Definition 3 (Edges of *HoS*-graph)

We call that "*H and H′ are joined*" for the above heptads H, H' with $m(H') = m(H) + 5x$, and $-x \in H$.

Remark 1 ("Intersecting" haptads)

$H \cap (-H') = \{-x\}$.

Constructing *HoS*-graph (1)

100

(5) $H_0 = \{x_0, \ldots\}$: heptad
$H_1 = \{-x_0, x_1, \ldots\}$ with $m(H_1) = m(H_0) - 5x_0$
$H_2 = \{-x_1, x_2, \ldots\}$ with $m(H_2) = m(H_1) - 5x_1$

- $\mathcal{H}_1 := \{\ H : \textit{heptad} \mid m(H) = m(H_0) - 5x\ (x \in H_0)\ \}$,
$\mathcal{H}_2 := \{\ H' : \textit{heptad} \mid m(H') = m(H) - 5y\ (y \in H \in \mathcal{H}_1)\ \}$,
$\mathcal{H} := \{H_0\} \cup \mathcal{H}_1 \cup \mathcal{H}_2$,
$\mathcal{E} := \{\{H, H'\} \mid H, H' \in \mathcal{H}, m(H') = m(H) - 5z\ (z \in H)\ \}$.

We will prove that $(\mathcal{H}, \mathcal{E}) \cong$ *HoS*-graph. But we can easily verify the properties "*valency*$= 7$", "*no triangles*", "*no quadrangles*". So it suffices to show that $H_2 (\in \mathcal{H}_2)$ is joined with some $H_3 \in \mathcal{H}_2$ (i.e. "*diameter*$= 2$").

(5.1) $(m(H_0), y) = 10\ (\forall y \in H_0)$ (by (3.1))
$(m(H_0), z) = 5\ \ (\forall z \in H_1 \setminus \{-x_0\})$ (by (4.2))
$(m(H_0), w) = (m(H_1) + 5x_0, w) = 5 + 5 \times (-1) = 0$
$(\forall w \in H_2 \setminus \{-x_1\})$

Constructing *HoS*-graph (2)

(5.2) $\exists u \in H_0 \setminus \{x_0\}$ such that $(u, x_2) = 1$.

(Proof.) By (5.1) and $(x_0, x_2) = -1$,
$0 = (x_0 + y_1 + \cdots + y_6, x_2) = -1 + (y_1, x_2) + \cdots + (y_6, x_2)$.
Since $(x_0, y_j) = 1$ and $(x_0, x_2) = -1$, we have $x_2 \neq y_j$.
Hence $(y_j, x_2) \in \{0, \pm 1, \pm i, -4, \pm 4i\}$ and thus there exists some j such that $(y_j, x_2) = 1$. □

- We set $u = -x_4$ in (5.2).

(5.3) $(x_0, x_4) = -1$ by $x_0, -x_4 (= u) \in H_0$,
$(x_2, x_4) = -1$ by definition,
$(x_1, x_4) = -1$ by (4.2) ($x_1 \in H_1$, $-x_4 \in H_0$),
$(x_0, x_1) = -1$ by $-x_0, x_1 \in H_1$,
$(x_1, x_2) = -1$ by $-x_1, x_2 \in H_2$, and
$(x_0, x_2) = -1$ by (4.2).

- By (2.3)(2), $\exists x_3' \in L_4$ such that $\{x_0, x_1, x_2, x_3', x_4\}$ is a pentad (i.e. $x_0 + x_1 + x_2 + x_3' + x_4 = 0$).

Constructing *HoS*-graph (3)

(6) $H_0 = \{-x_4, x_0, \ldots\}$,
$H_1 = \{-x_0, x_1, \ldots\}$ $(\in \mathcal{H}_1)$,
$H_2 = \{-x_1, x_2, \ldots\}$ $(\in \mathcal{H}_2)$,
$H_4 = \{x_4, \ldots\}$ $(\in \mathcal{H}_1)$, with $m(H_4) = m(H_0) + 5x_4$.

(6.1) $(m(H_4), -x_3') = (m(H_0) + 5x_4, x_0 + x_1 + x_2 + x_4)$
$= 10 + 5 + 0 + (-10) + 5(-1 - 1 - 1 + 4) = 10$.
Hence we have $-x_3' \in H_4$.

(6.2) We apply the arguments for H_0, H_1, H_2 to H_4, H_0, H_1. Then by (5.2),
$\exists x_3$ such that $-x_3 \in H_4 \setminus \{x_4\}$, $(-x_3, x_1) = 1$,
and moreover by (5.3),
$\exists x_2' \in L_4$ such that $\{x_0, x_1, x_2', x_3, x_4\}$ is a pentad
(i.e. $x_0 + x_1 + x_2' + x_3 + x_4 = 0$).

Constructing *HoS*-graph (4)

(6.3) Hence we have $x_2' + x_3 = x_0 + x_1 + x_4 = x_2 + x_3'$, and thus $\{x_2', x_3\} = \{x_2, x_3'\}$.
Since $-x_3, -x_3' \in H_4$, we have $(x_3, x_3') = 1$. On the other hand, $(x_2, x_3') = -1$ (pentad). Hence $x_2 \neq x_3$, that is, $x_2 = x_2'$ and $x_3 = x_3'$.
i.e. $x_0 + x_1 + x_2 + x_3 + x_4 = 0$.

(6.4) $H_3 = \{x_3, \ldots\}$ $(\in \mathcal{H}_2)$ with $m(H_3) = m(H_4) + 5x_3$,
$H_3' = \{-x_2, \ldots\}$ with $m(H_3') = m(H_2) - 5x_2$.
Then
$m(H_3) = m(H_0) + 5x_4 + 5x_3$, and
$m(H_3') = m(H_0) - 5x_0 - 5x_1 - 5x_2$.
Hence $m(H_3) = m(H_3')$, i.e. $H_3 = H_3'$.
This means that H_2 is joined with H_3 $(\in \mathcal{H}_2)$.
Hence we have proved that $(\mathcal{H}, \mathcal{E}) \cong$ *HoS*-graph.

単項式型対称式の主特殊化と巡回群の群行列式

山口尚哉 * , 山口由佳 † , 渋川元樹 ‡

令和元年 9 月 30 日

1 はじめに

対称多項式の一つの型に, 分割に対して定義される単項式型対称式がある. 一方で, 有限群に対して定義される概念に群行列式というものがある. これは, 群の元に対する不定元からなる同次多項式であり, その群の正則表現を用いて定義される. 私たちは, 巡回群の群行列式の冪乗の各項の係数が, 単項式型対称式の主特殊化に等しいことに気づき, 巡回群の群行列式の性質を用いて, 単項式型対称式の主特殊化の性質を与えた. また逆にこの主特殊化の性質から, 素数位数の群の群行列式の項数を得た. これは, 素数位数の群の群行列式の項全体が, その群の正則表現の作用で不変な同次多項式の成す線型空間の基底を成すことを示している.

複素数 ω_n を 1 の原始 n 乗根の 1 つとし, $\zeta_{(n,k)} := (\omega_n, \omega_n^2, \ldots, \omega_n^{kn})$ とする. 単項式型対称式の主特殊化とは, 長さ kn の分割 λ に対して定義される単項式型対称式 $m_\lambda(x)$ の変数 x に, $x = \zeta_{(n,k)}$ を代入した $m_\lambda(\zeta_{(n,k)})$ をいう. 主特殊化 $m_\lambda(\zeta_{(n,k)})$ の性質を述べるために, 記号をいくつか導入する. 長さ kn の分割 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_{kn})$ $(n \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{kn} \geq 1)$ に対して, $|\lambda| := \lambda_1 + \lambda_2 + \cdots + \lambda_{kn}$ とし, 長さ kn の分割全体の成す集合の部分集合 Λ_n^k を

$$\Lambda_n^k := \{\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_{kn}) \mid n \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{kn} \geq 1,\ n \mid |\lambda|\}$$

で与える. また, 整数 l に対して, $l \cdot \lambda \in \Lambda_n^k$ を, $(\overline{l\lambda_1}, \overline{l\lambda_2}, \ldots, \overline{l\lambda_{kn}}) \in (\mathbb{Z}/n\mathbb{Z})^{kn}$ を適当な並び換えによって Λ_n^k の元とみなしたものとし, $\nu \subset \lambda$ を満たす分割 $\nu \in \Lambda_n^1$ に対して, $\lambda \setminus \nu \in \Lambda_n^{k-1}$ を, λ から ν を削ってできる分割とする. ただし, $\mathbb{Z}/n\mathbb{Z}$ は, 位数 n の巡回群を表すとする. このとき, 主特殊化 $m_\lambda(\zeta_{(n,k)})$ は以下の性質をもつ.

Theorem 1.1 (see Theorem **6.1** for proof)**.** 単項式型対称式の主特殊化 $m_\lambda(\zeta_{(n,k)})$ に関して, 以下が成り立つ.

(1) 長さ kn の任意の分割 λ に対して, $m_\lambda(\zeta_{(n,k)}) \in \mathbb{Z}$.

(2) 長さ kn の任意の分割 λ に対して, $n \nmid |\lambda|$ ならば, $m_\lambda(\zeta_{(n,k)}) = 0$.

*山口尚哉, 長崎大学 情報系新学部創設準備室, Email: yamaguchi@nagasaki-u.ac.jp
†山口由佳, 長崎大学 情報系新学部創設準備室, Email: yamaguchiyuka@nagasaki-u.ac.jp
‡渋川元樹, 神戸大学大学院理学研究科数学専攻, Email: g-shibukawa@math.kobe-u.ac.jp

(3) p を素数とする. 長さ p の任意の分割 λ に対して, $p \mid |\lambda| \iff m_\lambda(\zeta_{(p,1)}) \neq 0$.

(4) l を n と互いに素な正の整数, $\lambda \in \Lambda_n^k$ とする. このとき, $m_{l\cdot\lambda}(\zeta_{(n,k)}) = m_\lambda(\zeta_{(n,k)})$.

(5) l を自然数, $\lambda \in \Lambda_n^{k+l}$ とする. このとき, $m_\lambda(\zeta_{(n,k+l)}) = \sum_{\substack{\nu \in \Lambda_n^k \\ \nu \subset \lambda}} m_\nu(\zeta_{(n,k)}) m_{\lambda\setminus\nu}(\zeta_{(n,l)})$.

(6) $\lambda = (2^{2k-2a}, 1^{2a}) \in \Lambda_2^k$ とする. このとき, $m_\lambda(\zeta_{(2,k)}) = (-1)^a \binom{k}{a} \neq 0$.

(7) $\lambda = (n^{kn-a}, \lambda_1^a) \in \Lambda_n^k$ $(n > \lambda_1)$ とする. このとき,

$$m_\lambda(\zeta_{(n,k)}) = (-1)^{a+\frac{a}{n}\gcd(\lambda_1,n)} \binom{k\gcd(\lambda_1,n)}{\frac{a}{n}\gcd(\lambda_1,n)} \neq 0.$$

(8) k を偶数, もしくは n を奇数とし, $\lambda = (\lambda_1^a, \lambda_2^{kn-a}) \in \Lambda_n^k$ $(\lambda_1 > \lambda_2)$ とする. このとき,

$$m_\lambda(\zeta_{(n,k)}) = (-1)^{a+\frac{a}{n}\gcd(\lambda_1-\lambda_2,n)} \binom{k\gcd(\lambda_1-\lambda_2,n)}{\frac{a}{n}\gcd(\lambda_1-\lambda_2,n)} \neq 0.$$

実は, 主特殊化 $m_\lambda(\zeta_{(n,1)})$ は, $\mathbb{Z}/n\mathbb{Z}$ の群行列式の項の係数に等しいことが, Dedekind の定理を用いると容易にわかる. 有限群 G の群行列式 $\Theta(G)$ とは, $g \in G$ に対する不定元 x_g からなる同次多項式であり, その群 G の正則表現を用いて定義されるものである. また, Dedekind の定理とは, 有限可換群の群行列式を複素数体 $\mathbb{C}$ 上で 1 次の因子の積に分解するものである. この定理を $\mathbb{Z}/n\mathbb{Z}$ に適用し, 1 次の因子の積を展開すれば, $\Theta(\mathbb{Z}/n\mathbb{Z})$ の項の係数が, $m_\lambda(\zeta_{(n,1)})$ に等しいことが自然に得られるのである. もっと一般に, $m_\lambda(\zeta_{(n,k)})$ は $\Theta(\mathbb{Z}/n\mathbb{Z})$ の k 乗の項の係数に等しいことが, 同様にして示せる. つまりは, 長さ N の分割 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ に対して, $x_\lambda := x_{\lambda_1} x_{\lambda_2} \cdots x_{\lambda_N}$ とすれば, 次が成り立つことがわかる.

Lemma 1.2 (see Lemma **5.2** for proof)**.** 任意の正の整数 k と n に対して, 次が成り立つ.

$$\Theta(\mathbb{Z}/n\mathbb{Z})^k = \sum_{\lambda \in \Lambda_n^k} m_\lambda(\zeta_{(n,k)}) x_\lambda.$$

この表示より, $\Theta(G)^k$ の項数を $\mathrm{N}(\Theta(G)^k)$ とすれば, $\mathrm{N}(\Theta(G)^k)$ に関する次の不等式が直ちに得られる.

Corollary 1.3 (Corollary **4.3**)**.** 任意の正の整数 k と n に対して, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/n\mathbb{Z})^k\right) \leq \left|\Lambda_n^k\right|.$$

また, $m_\lambda(\zeta_{(n,k)})$ が $\Theta(\mathbb{Z}/n\mathbb{Z})^k$ の項 x_λ の係数に等しいことより, $\Theta(G)$ の性質を用いて, $m_\lambda(\zeta_{(n,k)})$ の性質を得ることができる. 群行列式 $\Theta(G)$ は, 以下の性質をもつ.

1. $\Theta(G)$ の項の係数は整数.

2. G が可換のとき, $\Theta(G)$ の項として $x_{a_1} x_{a_2} \cdots x_{a_n}$ があれば, a_i たちの積は G の単位元.

3. ψ を G の自己同型写像としたとき, 不定元 x_g を $x_{\psi(g)}$ としても $\Theta(G)$ は不変.

私たちは, $\Theta(G)$ のこれらの性質を用いて, $m_\lambda(\zeta_{(n,k)})$ の性質を得る. そして, $m_\lambda(\zeta_{(n,k)})$ の性質を得た上で, 改めて $\Theta(G)$ について見直すことにする.

主特殊化 $m_\lambda(\zeta_{(n,k)})$ は $\Theta(\mathbb{Z}/n\mathbb{Z})^k$ の項 x_λ の係数に等しいので, 分割 λ が $m_\lambda(\zeta_{(n,k)})$ の零点か否かを判別することができれば, $\Theta(\mathbb{Z}/n\mathbb{Z})^k$ の項数を知ることができる. したがって, Theorem **1.1** の (3) より, 次が成り立つことがわかる.

Corollary 1.4 (Corollary **4.5**)**.** 整数 p を素数とする. このとき, 次が成り立つ.

$$\mathrm{N}\left(\Theta\left(\mathbb{Z}/p\mathbb{Z}\right)\right) = \left|\Lambda_p^1\right|.$$

ここで, 集合 Λ_n^k の濃度 $|\Lambda_n^k|$ は, $\mathbb{Z}/n\mathbb{Z}$ の正則表現の作用で不変な n 変数 kn 次同次多項式の成す線型空間 $\mathbb{C}[x_1, x_2, \ldots, x_n]_{kn}^{\mathbb{Z}/n\mathbb{Z}}$ の次元に等しいことがわかるので, Corollary **1.4** より, 次が成り立つ.

Corollary 1.5 (Corollary **4.6**)**.** 整数 p を素数とする. このとき, 次が成り立つ.

$$\mathrm{N}\left(\Theta\left(\mathbb{Z}/p\mathbb{Z}\right)\right) = \dim \mathbb{C}[x_1, x_2, \ldots, x_p]_p^{\mathbb{Z}/p\mathbb{Z}}.$$

したがって, 位数が素数 p である群の群行列式 $\Theta(\mathbb{Z}/p\mathbb{Z})$ の項数は, その群 $\mathbb{Z}/p\mathbb{Z}$ の正則表現の作用で不変な p 変数 p 次同次多項式の成す線型空間 $\mathbb{C}[x_1, x_2, \ldots, x_p]_p^{\mathbb{Z}/p\mathbb{Z}}$ の次元に等しいことがわかる. これは, $\Theta(\mathbb{Z}/p\mathbb{Z})$ の項全体が, $\mathbb{C}[x_1, x_2, \ldots, x_p]_p^{\mathbb{Z}/p\mathbb{Z}}$ の基底を成すことを示している.

さて, $a(n,m)$ を有限巡回群 $\mathbb{Z}/n\mathbb{Z}$ の正則表現の作用で不変な n 変数 m 次同次多項式の成す線型空間 $\mathbb{C}[x_1, x_2, \ldots, x_n]_m^{\mathbb{Z}/n\mathbb{Z}}$ の次元とすれば, $a(n,m)$ は二項係数と Euler のトーシェント関数 φ を用いて, 次のように明示的に表示できることが知られている ([2] と [3]).

Theorem 1.6 (Hermite の相互律)**.** 任意の正の整数 m と n に対して, 次が成り立つ.

$$a(n,m) = \frac{1}{m+n} \sum_{d \mid \gcd(m,n)} \binom{\frac{m}{d} + \frac{n}{d}}{\frac{n}{d}} \varphi(d).$$

この Thoerem **1.6** を用いれば, Corollary **1.3** は次のように書き換えられる.

Lemma 1.7 (see Lemma **7.3** for proof)**.** 任意の正の整数 k と n に対して, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/n\mathbb{Z})^k\right) \leq \left|\Lambda_n^k\right| = a(n,kn) = \frac{1}{n} \sum_{d \mid n} \binom{dk+d-1}{d-1} \varphi\left(\frac{n}{d}\right).$$

Lemma **1.7** の右辺は, 巡回群の巡回指数の特殊化になっている. 巡回指数とは Redfield [12] と Pólya [11] によって, それぞれ独立に定義された概念である. Lemma **1.7** において n を素数とすれば, Corollary **1.4** より, 次の Corollary が直ちに得られる.

Corollary 1.8 (Corollary **7.4**)**.** 任意の素数 p に対して, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/p\mathbb{Z})\right) = \left|\Lambda_p^1\right| = a(p,p) = \frac{1}{p} \sum_{d \mid p} \binom{2d-1}{d-1} \varphi\left(\frac{p}{d}\right).$$

また, 直積群の群行列式の項数に関して, 次の等式が成り立つことを示した.

Lemma 1.9 (see Lemma **8.1** for proof)**.** 集合 G を有限群 H と K の直積群とする. このとき, 次が成り立つ.

$$\Theta(G)|_{x_{(h,k)}=x_hx_k} = \Theta(H)^{|K|}\Theta(K)^{|H|} \in \mathbb{C}[x_h, x_k; h \in H, k \in K].$$

ただし, $\Theta(G)|_{x_{(h,k)}=x_hx_k}$ は, $\Theta(G)$ の不定元 $x_{(h,k)}$ に x_hx_k を代入したものを表す.

明らかに, 不定元を特殊化した群行列式の項数は, 特殊化する前の群行列式の項数以下である. したがって, 直積群の群行列式の項数を下から評価する次の不等式が得られる.

Corollary 1.10 (Corollary **8.2**)**.** 有限直積群 $G = H \times K$ に対して, 次の不等式が成り立つ.

$$\mathrm{N}(\Theta(G)) \geq \mathrm{N}\left(\Theta(H)^{|K|}\Theta(K)^{|H|}\right) = \mathrm{N}(\Theta(H)^{|K|})\,\mathrm{N}(\Theta(K)^{|H|}).$$

特に m_i を素冪で, $G = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_l\mathbb{Z}$ とすれば, 群行列式に関する次の不等式が得られる.

$$\prod_{i=1}^{l} \mathrm{N}\left(\Theta(\mathbb{Z}/m_i\mathbb{Z})^{\frac{n}{m_i}}\right) \leq \mathrm{N}\left(\Theta(G)\right) \leq \frac{1}{n}\sum_{d|n}\binom{dk+d-1}{d-1}\varphi\left(\frac{n}{d}\right).$$

2 単項式型対称式

本章では, 単項式型対称式について説明し, この単項式型対称式に関する等式を一つ与える. この等式は, 長さが素数のある分割が, 単項式型対称式の主特殊化の非零点であることを証明するのに用いられる.

単項式型対称式を与えるには, 自然数全体の集合の直積集合への対称群の作用を定める必要がある. また, 多重指数の記法を用いると, 単項式型対称式の表記が簡潔になる. そのために, まずは, 自然数全体の集合の直積集合への対称群の作用を定め, 次に, 多重指数の記法について説明する. 自然数全体の集合 $\mathbb{N}$ は 0 を含むとし, N 次対称群 $\mathfrak{S}_N$ の $\mathbb{N}^N$ への作用を次で与える.

$$\begin{array}{ccccc} \mathfrak{S}_N & \curvearrowright & \mathbb{N}^N & \xrightarrow{\simeq} & \mathbb{N}^N \\ \cup & & \cup & & \cup \\ \sigma & \curvearrowright & \nu := (\nu_1, \nu_2, \ldots, \nu_N) & \mapsto & \sigma\cdot\nu := (\nu_{\sigma(1)}, \nu_{\sigma(2)}, \ldots, \nu_{\sigma(N)}). \end{array}$$

そして, N 個の変数の組 $x := (x_1, x_2, \ldots, x_N)$ と多重指数 $\mu := (\mu_1, \mu_2, \ldots, \mu_N) \in \mathbb{N}^N$ に対して,

$$x^\mu := x_1^{\mu_1}x_2^{\mu_2}\cdots x_N^{\mu_N} \in \mathbb{C}[x_1, x_2, \ldots, x_N] =: \mathbb{C}[x]$$

とする. この記法を, 多重指数の記法という. 多重指数の記法を用いれば, 長さ N の分割 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ $(n \geq \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N \geq 1)$ に対して, 単項式型対称式

$$m_\lambda(x) := \sum_{\mu \in \mathfrak{S}_N\cdot\lambda} x^\mu$$

が定まる. ただし, $\mathfrak{S}_N \cdot \lambda := \{\sigma \cdot \lambda \mid \sigma \in \mathfrak{S}_N\}$ とする.

対称群 $\mathfrak{S}_N$ の長さ N の分割 λ における固定部分群を $\mathfrak{S}_N^\lambda := \{\sigma \in \mathfrak{S}_N \mid \sigma \cdot \lambda = \lambda\}$ とし, $\lambda[i] := |\{j \mid \lambda_j = i\}|$ とおく. このとき, 次が成り立つ.

Lemma 2.1. 長さ N の任意の分割 λ に対して, 次が成り立つ.

$$m_\lambda(x) \prod_{i \geq 1} (\lambda[i]!) = \sum_{\sigma \in \mathfrak{S}_N} x^{\sigma \cdot \lambda}.$$

Proof. まず, 次の等式

$$|\mathfrak{S}_N^\lambda| = \prod_{i \geq 1} (\lambda[i]!)$$

が成り立つので,

$$\begin{aligned}
\sum_{\sigma \in \mathfrak{S}_N} x^{\sigma \cdot \lambda} &= \sum_{[g] \in \mathfrak{S}_N / \mathfrak{S}_N^\lambda} \sum_{h \in \mathfrak{S}_N^\lambda} x^{gh \cdot \lambda} \\
&= |\mathfrak{S}_N^\lambda| \sum_{[g] \in \mathfrak{S}_N / \mathfrak{S}_N^\lambda} x^{g \cdot \lambda} \\
&= |\mathfrak{S}_N^\lambda| \sum_{\mu \in \mathfrak{S}_N \cdot \lambda} x^\mu \\
&= \left(\prod_{i \geq 1} (\lambda[i]!) \right) m_\lambda(x)
\end{aligned}$$

が成り立つ. □

分割 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ に対して, $|\lambda| := \lambda_1 + \lambda_2 + \cdots + \lambda_N$ とする. Lemma **2.1** は, 長さが素数 p の分割 λ が $p \mid |\lambda|$ を満たせば, λ が単項式型対称式の主特殊化の非零点であることを証明するのに用いられる.

3 単項式型対称式の主特殊化

本章では, 単項式型対称式の主特殊化について説明し, それから, 分割が主特殊化の非零点であることを Lemma **2.1** を用いて言い換え, そして, 長さが素数の分割が単項式型対称式の主特殊化の非零点であるための十分条件を与える. また, Theorem **1.1** の (7) と (8) が成り立つことを示す. 第 1 章では, 群行列式の性質を用いて, 単項式型対称式の主特殊化の性質を得ることができると述べたが, この十分条件と (7), (8) については, 群行列式の性質を用いずに与える.

複素数 ω_n を 1 の原始 n 乗根の 1 つとし, $\zeta_{(n,k)} := \left(\omega_n, \omega_n^2, \ldots, \omega_n^{kn}\right)$ とする. 長さ kn の分割 λ によって定義される単項式型対称式 $m_\lambda(x)$ の x に, $x = \zeta_{(n,k)}$ を代入した $m_\lambda(\zeta_{(n,k)})$ を単項式型対称式の主特殊化という.

Lemma **2.1** より, $m_\lambda(\zeta_{(n,k)}) \neq 0$ を満たす λ である必要十分条件は,

$$\sum_{\sigma \in \mathfrak{S}_{kn}} (\zeta_{(n,k)})^{\sigma \cdot \lambda} = \sum_{\sigma \in \mathfrak{S}_{kn}} \omega_n^{\lambda_1 \sigma(1) + \lambda_2 \sigma(2) + \cdots + \lambda_{kn} \sigma(kn)} \neq 0$$

を満たす λ である. したがって, 分割 λ が単項式型対称式の主特殊化の零点か否かを判別するには, 分割 λ が $\sum_{\sigma\in\mathfrak{S}_{kn}}(\zeta_{(n,k)})^{\sigma\cdot\lambda}$ の零点か否かを判別できればよい[1].

正の整数 k が 1 で, n が素数のとき, 分割 λ が $\sum_{\sigma\in\mathfrak{S}_{kn}}(\zeta_{(n,k)})^{\sigma\cdot\lambda}$ の非零点であるための十分条件は次で与えられる.

Lemma 3.1. 整数 p を素数とし, $i_1, i_2, \ldots, i_p \in \mathbb{N}$ とする. このとき, $p \mid i_1 + i_2 + \cdots + i_p$ ならば, 次が成り立つ.

$$\sum_{\sigma\in\mathfrak{S}_p} \omega_p^{i_1\sigma(1)+i_2\sigma(2)+\cdots+i_p\sigma(p)} \neq 0.$$

Lemma **3.1** を示すために, 次の補題を与える.

Lemma 3.2. 自然数 n を正の整数, N を n の倍数, $i_1, i_2, \ldots, i_N \in \mathbb{N}$, そして, f を周期 n の関数とする. このとき, $n \mid i_1 + i_2 + \cdots + i_N$ ならば, 次が成り立つ.

$$\sum_{\sigma\in\mathfrak{S}_N} f(i_1\sigma(1)+i_2\sigma(2)+\cdots+i_N\sigma(N)) = N \sum_{\tau\in\mathfrak{S}_{N-1}} f(i_1\tau(1)+i_2\tau(2)+\cdots+i_{N-1}\tau(N-1)).$$

Proof. まず, 次の等式が成り立つ.

$$\sum_{\sigma\in\mathfrak{S}_N} f(i_1\sigma(1)+i_2\sigma(2)+\cdots+i_N\sigma(N)) = \sum_{k=1}^{N} \sum_{\substack{\sigma\in\mathfrak{S}_N \\ \sigma(k)=N}} f(i_1\sigma(1)+i_2\sigma(2)+\cdots+i_N\sigma(N)).$$

写像 $\mathfrak{S}_N \ni \sigma \mapsto \sigma\circ(k\ N) \in \mathfrak{S}_N$ は全単射なので, 上式の右辺は

$$\begin{aligned}
&\sum_{k=1}^{N} \sum_{\substack{\sigma\in\mathfrak{S}_N \\ \sigma(N)=N}} f(i_1\sigma(1)+\cdots+i_{N-1}\sigma(N-1)-i_k\sigma(k)+i_k\sigma(N)+i_N\sigma(k)) \\
&\quad= \sum_{k=1}^{N} \sum_{\substack{\sigma\in\mathfrak{S}_N \\ \sigma(N)=N}} f(i_1\sigma(1)+\cdots+i_{N-1}\sigma(N-1)-i_k\sigma(k)-(i_1+\cdots+i_{N-1})\sigma(k)) \\
&\quad= \sum_{k=1}^{N} \sum_{\substack{\sigma\in\mathfrak{S}_N \\ \sigma(N)=N}} f(i_1(\sigma(1)-\sigma(k))+\cdots+i_{N-1}(\sigma(N-1)-\sigma(k))-i_k\sigma(k))
\end{aligned}$$

となる. ここで, $\sigma(N) = N$ のとき,

$$\begin{aligned}
&f(i_1(\sigma(1)-\sigma(N))+\cdots+i_{N-1}(\sigma(N-1)-\sigma(N))-i_N\sigma(N)) \\
&\quad= f(i_1\sigma(1)+\cdots+i_{N-1}\sigma(N-1))
\end{aligned}$$

であり, $k \neq N$ かつ $\sigma(N) = N$ のとき,

$$\begin{aligned}
&\{\sigma(1)-\sigma(k),\ldots,\sigma(k-1)-\sigma(k),-\sigma(k),\sigma(k+1)-\sigma(k),\ldots,\sigma(N-1)-\sigma(k)\} \\
&\quad\equiv \{1,2,\ldots,N-1\} \mod N
\end{aligned}$$

[1] この指数和は, Waring の公式の一般化の係数である [9].

となるので,

$$\begin{aligned}
&\sum_{k=1}^{N} \sum_{\substack{\sigma\in\mathfrak{S}_N \\ \sigma(N)=N}} f(i_1(\sigma(1)-\sigma(k))+\cdots+i_{N-1}(\sigma(N-1)-\sigma(k))-i_k\sigma(k)) \\
&\quad = \sum_{k=1}^{N} \sum_{\tau\in\mathfrak{S}_{N-1}} f(i_1\tau(1)+\cdots+i_{N-1}\tau(N-1)) \\
&\quad = N \sum_{\tau\in\mathfrak{S}_{N-1}} f(i_1\tau(1)+\cdots+i_{N-1}\tau(N-1))
\end{aligned}$$

がわかる. □

Lemma **3.1** を示す.

Proof of Lemma **3.1**. まず, $2 \mid i_1+i_2$ の場合は, 直接計算により, $\sum_{\sigma\in\mathfrak{S}_2} \omega_2^{i_1\sigma(1)+i_2\sigma(2)} \neq 0$ を示せる. 整数 p を奇素数とし, $p \mid i_1+i_2+\cdots+i_p$ とすると, Lemma **3.2** より, 次が成り立つ.

$$\sum_{\sigma\in\mathfrak{S}_p} \omega_p^{i_1\sigma(1)+i_2\sigma(2)+\cdots+i_p\sigma(p)} = p \sum_{\sigma\in\mathfrak{S}_{p-1}} \omega_p^{i_1\sigma(1)+i_2\sigma(2)+\cdots+i_{p-1}\sigma(p-1)}.$$

このとき, $\sum_{k=1}^{p} C_k = (p-1)!$ を満たす $C_k \in \mathbb{N}$ が存在して,

$$\sum_{\sigma\in\mathfrak{S}_{p-1}} \omega_p^{i_1\sigma(1)+i_2\sigma(2)+\cdots+i_{p-1}\sigma(p-1)} = \sum_{k=1}^{p} C_k\omega_p^k$$

と表示することができる. ここで, $\sum_{k=1}^{p} C_k\omega_p^k \neq 0$ を背理法で示す. もし, $\sum_{k=1}^{p} C_k\omega_p^k = 0$ とすれば, $\{\omega_p, \omega_p^2, \ldots, \omega_p^{p-1}\}$ は線型独立なので, $C_1 = C_2 = \cdots = C_p$ となる. つまり, $p \mid \sum_{k=1}^{p} C_k$ となる. ところが, $\sum_{k=1}^{p} C_k = (p-1)!$ なので, $p \nmid \sum_{k=1}^{p} C_k$ である. したがって, $\sum_{k=1}^{p} C_k\omega_p^k \neq 0$ となる. □

Lemma **3.1** より, 長さが素数 p の分割 λ が, $p \mid |\lambda|$ を満たせば, $m_\lambda(\zeta_{(p,1)}) \neq 0$ となることがわかった. つまり, 次が成り立つことがわかった.

Corollary 3.3. 整数 p を素数とする. このとき, 長さ p の任意の分割 λ に対して, 次が成り立つ.

$$p \mid |\lambda| \Longrightarrow m_\lambda(\zeta_{(p,1)}) \neq 0.$$

実は, $p \nmid |\lambda|$ を満たせば, $m_\lambda(\zeta_{(p,1)}) = 0$ となることがわかる (この事実は第 5 章で示される). よって, 次の補題が成り立つことがわかる.

Lemma 3.4 ((3) of Theorem **1.1**)**.** 整数 p を素数とする. このとき, 長さ p の任意の分割 λ に対して, 次が成り立つ.

$$p \mid |\lambda| \iff m_\lambda(\zeta_{(p,1)}) \neq 0.$$

正の整数 r と s に対して, r と s の最大公約数を $\gcd(r,s)$ と表す. このとき, 次が成り立つことがわかる.

Lemma 3.5 ((7) of Theorem **1.1**)**.** 長さ kn の分割 $\lambda=(n^{kn-a},\lambda_1^a)$ $(n>\lambda_1)$ に対して, 次が成り立つ.

$$m_\lambda(\zeta_{(n,k)})=\begin{cases}(-1)^{a+\frac{a}{n}\gcd(\lambda_1,n)}\dbinom{k\gcd(\lambda_1,n)}{\frac{a}{n}\gcd(\lambda_1,n)}\neq 0, & n\mid a\lambda_1\\ 0, & n\nmid a\lambda_1\end{cases}.$$

Proof. 分割 $\lambda=(n^{kn-a},\lambda_1^a)$ $(n>\lambda_1)$ に対して,

$$m_\lambda(\zeta_{(n,k)})=\sum_{1\le i_1<\cdots<i_a\le kn}\omega_n^{\lambda_1(i_1+\cdots+i_a)}$$

なので,

$$\begin{aligned}\sum_{a=0}^{kn}(-1)^a m_\lambda(\zeta_{(n,k)})u^{kn-a}&=\sum_{a=0}^{kn}\sum_{1\le i_1<\cdots<i_a\le kn}(-1)^a\omega_n^{\lambda_1(i_1+\cdots+i_a)}u^{kn-a}\\&=\prod_{j=1}^{kn}(u-\omega_n^{j\lambda_1})\end{aligned}$$

となる. ここで, $d:=\gcd(\lambda_1,n)$, $l:=\frac{n}{d}$, $m:=\frac{\lambda_1}{d}$ とすれば, $\gcd(l,m)=1$ なので, 1 のある原始 l 乗根 ω_l が存在して, $\omega_n^{\lambda_1}=\omega_l$ となるので,

$$\begin{aligned}u^l-1&=(u-\omega_l)(u-\omega_l^2)\cdots(u-\omega_l^l)\\&=(u-\omega_n^{\lambda_1})(u-\omega_n^{2\lambda_1})\cdots(u-\omega_n^{l\lambda_1})\end{aligned}$$

が成り立つ. したがって,

$$\begin{aligned}\prod_{j=1}^{kn}(u-\omega_n^{j\lambda_1})&=\left(\prod_{j=1}^{l}(u-\omega_n^{j\lambda_1})\right)\left(\prod_{j=l+1}^{2l}(u-\omega_n^{j\lambda_1})\right)\cdots\left(\prod_{j=(kd-1)l+1}^{kdl}(u-\omega_n^{j\lambda_1})\right)\\&=\prod_{j=1}^{l}(u-\omega_l^j)^{kd}\\&=(u^l-1)^{kd}\\&=\sum_{j=0}^{kd}\binom{kd}{j}(-1)^j u^{l(kd-j)}\\&=\sum_{j=0}^{kd}\binom{kd}{j}(-1)^j u^{kn-\frac{n}{d}j}\end{aligned}$$

となる. ここで, u^{kn-a} の係数を比較することにより

$$(-1)^a m_\lambda(\zeta_{(n,k)})=\begin{cases}\dbinom{kd}{\frac{ad}{n}}(-1)^{\frac{ad}{n}}, & \frac{n}{d}\mid a,\\ 0, & \frac{n}{d}\nmid a\end{cases}$$

が得られる. また, $n\mid ad \iff n\mid a\lambda_1$ より, Lemma が示された. □

Lemma 3.6 ((8) of Theorem **1.1**)**.** 正の整数 k を偶数, もしくは n を奇数とする. このとき, 長さ kn の分割 $\lambda = (\lambda_1^a, \lambda_2^{kn-a})$ $(\lambda_1 > \lambda_2)$ に対して, 次が成り立つ.

$$m_\lambda(\zeta_{(n,k)}) = \begin{cases} (-1)^{a+\frac{a}{n}\gcd(\lambda_1-\lambda_2,n)} \binom{k\gcd(\lambda_1-\lambda_2,n)}{\frac{a}{n}\gcd(\lambda_1-\lambda_2,n)} \neq 0, & n \mid a(\lambda_1-\lambda_2) \\ 0, & n \nmid a(\lambda_1-\lambda_2) \end{cases}.$$

Proof. 分割 $\lambda = (\lambda_1^a, \lambda_2^{kn-a})$ $(\lambda_1 > \lambda_2)$ に対して, 定義より

$$m_\lambda(\zeta_{(n,k)}) = \sum_{\substack{I\subset[kn] \\ |I|=a}} \left(\prod_{i\in I} \omega_n^{\lambda_1 i}\right)\left(\prod_{j\in I^c} \omega_n^{\lambda_2 j}\right)$$

となる. ただし, $[kn] := \{1, 2, \ldots, kn\}$, $I^c := [kn] \setminus I$ である. ここで

$$\begin{aligned} m_\lambda(\zeta_{(n,k)}) &= \sum_{\substack{I\subset[kn] \\ |I|=a}} \left(\prod_{i\in I} \omega_n^{\lambda_1 i}\right)\left(\prod_{i\in I} \omega_n^{-\lambda_2 i}\right)\left(\prod_{i\in I} \omega_n^{\lambda_2 i}\right)\left(\prod_{j\in I^c} \omega_n^{\lambda_2 j}\right) \\ &= \sum_{\substack{I\subset[kn] \\ |I|=a}} \left(\prod_{i\in I} \omega_n^{(\lambda_1-\lambda_2) i}\right)\left(\prod_{j\in [kn]} \omega_n^{\lambda_2 j}\right) \\ &= \omega_n^{\lambda_2 \frac{kn(kn+1)}{2}} \sum_{\substack{I\subset[kn] \\ |I|=a}} \left(\prod_{i\in I} \omega_n^{(\lambda_1-\lambda_2) i}\right) \end{aligned}$$

と変形する. さらに k が偶数, もしくは n が奇数であることから $\frac{k(kn+1)}{2} \in \mathbb{Z}$ であることに注意すると,

$$m_\lambda(\zeta_{(n,k)}) = m_{\left(n^{kn-a},(\lambda_1-\lambda_2)^a\right)}(\zeta_{(n,k)})$$

を得るので, Lemma **3.5** より結論を得る. □

4 群行列式と分割

本章では, 群行列式とその性質を述べ, 巡回群の群行列式の冪乗の各項が分割に対応することを説明する. この対応を用いると, 巡回群の群行列式の冪乗を簡潔に表示することができる.

まず, 群行列式の歴史的なことについて少しだけ触れておく. 群行列式は Dedekind によって定義された概念であり (例えば [6, p. 150], [13, p. 224]), Frobenius はこの群行列式の $\mathbb{C}$ 上の既約分解を求める過程において有限群の表現論を構築した (例えば [4], [5]). これらの歴史的な経緯に関しては, [6], [7], [8], [13] などが詳しい. では, 群行列式の定義を述べる. 有限集合 $G = \{g_1, g_2, \ldots, g_n\}$ を位数 n の群, x_g を $g \in G$ に対する不定元とし, $\mathbb{C}[x_g] = \mathbb{C}[x_g; g \in G] := \mathbb{C}[x_{g_1}, x_{g_2}, \ldots, x_{g_n}]$ を不定元 x_g から成る n 変数多項式環とする. このとき, G の群行列式 $\Theta(G)$ は次で与えられる:

Definition 4.1 (群行列式)**.** 有限群 G の群行列式を次で定義する.

$$\Theta(G) := \sum_{\sigma\in\mathfrak{S}_n} \mathrm{sgn}(\sigma) x_{g_1^{-1}g_{\sigma(1)}} x_{g_2^{-1}g_{\sigma(2)}} \cdots x_{g_n^{-1}g_{\sigma(n)}} \in \mathbb{C}[x_g].$$

この定義より, 群行列式は n 変数 n 次同次多項式であることがわかる. また, G が可換であるとき, $\Theta(G)$ の項として $x_{a_1}x_{a_2}\cdots x_{a_n}$ が現れれば, a_i たちの積は G の単位元になることがわかる (実は, 非可換のときも適当な順序で積をとれば単位元になることが知られている. 詳細は [10, Lemma 1] と [15] を参照).

したがって, G が巡回群 $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{1}, \overline{2}, \ldots, \overline{n}\right\}$ であるときは, 群行列式の項が n 次同次であることより, 任意の $i \in \{1, 2, \ldots, n\}$ に対して, $x_{\overline{i}} = x_i$ として, $\Theta(\mathbb{Z}/n\mathbb{Z})$ の項 $x_{i_1}x_{i_2}\cdots x_{i_n}$ の変数を添え字の数の大きい順に並び換えることにより, $\Theta(\mathbb{Z}/n\mathbb{Z})$ の項を, 各因子が 1 以上 n 以下の長さ n の分割に対応させることができる. また, $\Theta(\mathbb{Z}/n\mathbb{Z})$ の項の添え字の積は単位元になることより, $\Theta(\mathbb{Z}/n\mathbb{Z})$ の任意の項の添え字の和は n の倍数となる. よって, 長さ N の分割 $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_N)$ に対して, $x_\lambda := x_{\lambda_1}x_{\lambda_2}\cdots x_{\lambda_N} \in \mathbb{C}[x] = \mathbb{C}[x_g]$,

$$\Lambda_n := \{\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n) \mid 1 \le \lambda_j \le \lambda_i \le n\,(j > i), n \mid |\lambda|\}$$

とすれば, 整数 c_λ が存在して,

$$\Theta(\mathbb{Z}/n\mathbb{Z}) = \sum_{\lambda\in\Lambda_n} c_\lambda x_\lambda \in \mathbb{C}[x]$$

とかける. この表示は, 同類項をまとめた簡潔な表示といえる.

Example 4.2. 位数 3 の巡回群の群行列式は, $\Theta(\mathbb{Z}/3\mathbb{Z}) = x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3$ である. 項 $x_1^3, x_2^3, x_3^3, x_1x_2x_3$ をそれぞれ, 長さ 3 の分割 $(1,1,1), (2,2,2), (3,3,3), (3,2,1)$ と見なすことができる.

もっと一般に,

$$\Lambda_n^k := \{\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_{kn}) \mid 1 \le \lambda_j \le \lambda_i \le n\,(j > i), n \mid |\lambda|\}$$

とすれば, 整数 c_λ が存在して,

$$\Theta\left(\mathbb{Z}/n\mathbb{Z}\right)^k = \sum_{\lambda\in\Lambda_n^k} c_\lambda x_\lambda \in \mathbb{C}[x]$$

とかける. 実は, この係数 c_λ は $m_\lambda(\zeta_{(n,k)})$ に等しいことがわかる (この事実は第 5 章で示される).

さて, この表示より, $\Theta(G)^k$ の項数を $\mathrm{N}(\Theta\left(G\right)^k)$ とすれば, $\mathrm{N}(\Theta\left(G\right)^k)$ に関する以下の不等式が直ちに得られる.

Corollary 4.3 (Corollary **1.3**)**.** 任意の正の整数 k と n に対して, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/n\mathbb{Z})^k\right) \le \left|\Lambda_n^k\right|.$$

この不等式は, 次の疑問を引き起こす.

Question 4.4. 任意の正の整数 k と n に対して, 次の等式は成り立つであろうか.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/n\mathbb{Z})^k\right) = \left|\Lambda_n^k\right|.$$

つまり, 任意の正の整数 k と n に対して, もし, $n \mid i_1 + i_2 + \cdots + i_{kn}$ ならば, 単項式 $x_{i_1}x_{i_2}\cdots x_{i_{kn}}$ は $\Theta(G)^k$ の項であるか. さらに言い換えれば, 任意の正の整数 k と n, 任意の $\lambda \in \Lambda_n^k$ に対して, $m_\lambda(\zeta_{(n,k)}) \neq 0$ は成り立つか.

この疑問は否定的に解決される. つまり, 一般に, $n \mid i_1 + i_2 + \cdots + i_{kn}$ だからといって, 単項式 $x_{i_1}x_{i_2}\cdots x_{i_{kn}}$ は $\Theta(G)^k$ の項とは限らない. 例えば, $k = 1$ で $n = 6$ のときが反例である. 単項式 $x_1x_3^2x_5x_6^2$ は $\Theta(\mathbb{Z}/6\mathbb{Z})$ の項ではないが, $6 \mid 1+3+3+5+6+6$ である.

しかしながら, Lemma **3.4** より, $k = 1$ で n が素数の場合は, 等式となることがわかる (この事実は第 6 章で示される). つまり, 次の Corollary が成り立つ.

Corollary 4.5 (Corollary **1.4**)**.** 整数 p を素数とする. このとき, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/p\mathbb{Z})\right) = \left|\Lambda_p^1\right|.$$

ここで, 集合の濃度 $|\Lambda_n^1|$ は, $\mathbb{Z}/n\mathbb{Z}$ の正則表現の作用で不変な n 変数 n 次同次多項式の成す線型空間 $\mathbb{C}[x_1, x_2, \ldots, x_n]_n^{\mathbb{Z}/n\mathbb{Z}}$ の次元に等しいことがわかる (この事実は第 7 章で示される). つまり, 次が成り立つ.

Corollary 4.6 (Corollary **1.5**)**.** 整数 p を素数とする. このとき, 次が成り立つ.

$$\mathrm{N}\left(\Theta\left(\mathbb{Z}/p\mathbb{Z}\right)\right) = \dim \mathbb{C}[x_1, x_2, \ldots, x_p]_p^{\mathbb{Z}/p\mathbb{Z}}.$$

したがって, 位数が素数 p である群の群行列式 $\Theta(\mathbb{Z}/p\mathbb{Z})$ の項数は, その群 $\mathbb{Z}/p\mathbb{Z}$ の正則表現の作用で不変な p 変数 p 次同次多項式の成す線型空間 $\mathbb{C}[x_1, x_2, \ldots, x_p]_p^{\mathbb{Z}/p\mathbb{Z}}$ の次元に等しいことがわかる. これは, $\Theta(Z/p\mathbb{Z})$ の項全体が, $\mathbb{C}[x_1, x_2, \ldots, x_p]_p^{\mathbb{Z}/p\mathbb{Z}}$ の基底を成すことを示している. これらについては, 第 7 章で詳しく述べる.

5 Dedekind の定理と単項式型対称式の主特殊化

本章では, Dedekind の定理について説明し, この定理を用いて, 巡回群の群行列式の冪乗の各項の係数が, 単項式型対称式の主特殊化に等しいことを示す. この事実を用いると, Lemma **3.4** を示すことができる.

以下では G を可換とし, $\widehat{G}$ を G の $\mathbb{C}$ 上の既約表現全体の集合とする (つまりは, 指標群とする). Dedekind は $\Theta(G)$ の $\mathbb{C}$ 上の既約分解を次のように与えた (例えば [1], [13], [14]). これを Dedekind の定理という.

Theorem 5.1 (Dedekind の定理)**.** 有限可換群 G の群行列式 $\Theta(G)$ は, $\mathbb{C}$ 上で 1 次因子の積として次のように分解される.

$$\Theta(G) = \prod_{\chi \in \widehat{G}} \sum_{g \in G} \chi(g) x_g.$$

この Dedekind の定理を用いると, $\Theta(\mathbb{Z}/n\mathbb{Z})^k$ の項 x_λ の係数が, 主特殊化 $m_\lambda(\zeta_{(n,k)})$ に等しいことがわかる.

Lemma 5.2 (Lemma **1.2**)**.** 任意の k に対して, 次が成り立つ.

$$\begin{aligned}\Theta(\mathbb{Z}/n\mathbb{Z})^k &= \sum_{\lambda:\text{長さ } kn \text{ の分割で, 各因子は } 1 \text{ 以上 } n \text{ 以下}} m_\lambda(\zeta_{(n,k)})x_\lambda \\ &= \sum_{\lambda\in\Lambda_n^k} m_\lambda(\zeta_{(n,k)})x_\lambda.\end{aligned}$$

Proof. Theorem **5.1** と Lemma **2.1** より, 次が成り立つ.

$$\begin{aligned}\Theta\left(\mathbb{Z}/n\mathbb{Z}\right)^k &= \left(\prod_{i=1}^{n}\sum_{j=1}^{n}\omega_n^{ij}x_j\right)^k \\ &= \left(\prod_{i_1=1}^{n}\sum_{j=1}^{n}\omega_n^{i_1 j}x_j\right)\left(\prod_{i_2=n+1}^{2n}\sum_{j=1}^{n}\omega_n^{i_2 j}x_j\right)\cdots\left(\prod_{i_k=(k-1)n+1}^{kn}\sum_{j=1}^{n}\omega_n^{i_k j}x_j\right) \\ &= \sum_{\lambda:\text{長さ } kn \text{ の分割で, 各因子は } 1 \text{ 以上 } n \text{ 以下}}\left\{\sum_{\sigma\in\mathfrak{S}_{kn}}(\zeta_{(n,k)})^{\sigma\cdot\lambda}\prod_{i\geq 1}(\lambda[i]!)^{-1}\right\}x_\lambda \\ &= \sum_{\lambda:\text{長さ } kn \text{ の分割で, 各因子は } 1 \text{ 以上 } n \text{ 以下}} m_\lambda(\zeta_{(n,k)})x_\lambda.\end{aligned}$$

また, 群行列式の定義より, $n \nmid |\lambda|$ となる λ に関する項 x_λ は $\Theta(\mathbb{Z}/n\mathbb{Z})^k$ に現れない. よって, $n \nmid |\lambda|$ となる λ に対する $m_\lambda(\zeta_{(n,k)})$ は 0 に等しいことがわかる. □

Lemma **5.2** より, Theorem **1.1** の (2) が成り立つことがわかる. つまり, $n \nmid |\lambda|$ となる λ に対する $m_\lambda(\zeta_{(n,k)})$ は 0 に等しいことがわかる. したがって, この事実と Corollary **3.3** より, Lemma **3.4** が成り立つことがわかった.

6 巡回群の群行列式の性質から得られる単項式型対称式の主特殊化の性質

本章では, 巡回群の群行列式の性質を用いて, 単項式型対称式の主特殊化の性質を導く.

整数 l と分割 $\lambda \in \Lambda_n^k$ に対して, $l\cdot\lambda \in \Lambda_n^k$ を, $(\overline{l\lambda_1}, \overline{l\lambda_2}, \ldots, \overline{l\lambda_{kn}}) \in (\mathbb{Z}/n\mathbb{Z})^{kn}$ を適当な並び換えによって Λ_n^k の元とみなしたものとし, $\nu \subset \lambda$ を満たす分割 $\nu \in \Lambda_n^1$ に対して, $\lambda \setminus \nu \in \Lambda_n^{k-1}$ を, λ から ν を削ってできる分割とする. このとき, 単項式型対称式の主特殊化に関して, 次の定理が成り立つ.

Theorem 6.1 (Theorem **1.1**)**.** 単項式型対称式の主特殊化 $m_\lambda(\zeta_{(n,k)})$ に関して, 以下が成り立つ.

(1) 長さ kn の任意の分割 λ に対して, $m_\lambda(\zeta_{(n,k)}) \in \mathbb{Z}$.

(2) 長さ kn の任意の分割 λ に対して, $n \nmid |\lambda|$ ならば, $m_\lambda(\zeta_{(n,k)}) = 0$.

(3) p を素数とする. 長さ p の任意の分割 λ に対して, $p \mid |\lambda| \iff m_\lambda(\zeta_{(p,1)}) \neq 0$.

(4) l を n と互いに素な正の整数, $\lambda \in \Lambda_n^k$ とする. このとき, $m_{l\cdot\lambda}(\zeta_{(n,k)}) = m_\lambda(\zeta_{(n,k)})$.

(5) l を自然数, $\lambda \in \Lambda_n^{k+l}$ とする. このとき, $m_\lambda(\zeta_{(n,k+l)}) = \sum_{\substack{\nu \in \Lambda_n^k \\ \nu \subset \lambda}} m_\nu(\zeta_{(n,k)}) m_{\lambda\setminus\nu}(\zeta_{(n,l)})$.

(6) $\lambda = (2^{2k-2a}, 1^{2a}) \in \Lambda_2^k$ とする. このとき, $m_\lambda(\zeta_{(2,k)}) = (-1)^a \binom{k}{a} \neq 0$.

(7) $\lambda = (n^{kn-a}, \lambda_1^a) \in \Lambda_n^k$ $(n > \lambda_1)$ とする. このとき,

$$m_\lambda(\zeta_{(n,k)}) = (-1)^{a+\frac{a}{n}\gcd(\lambda_1,n)} \binom{k\gcd(\lambda_1,n)}{\frac{a}{n}\gcd(\lambda_1,n)} \neq 0.$$

(8) k を偶数, もしくは n を奇数とし, $\lambda = (\lambda_1^a, \lambda_2^{kn-a}) \in \Lambda_n^k$ $(\lambda_1 > \lambda_2)$ とする. このとき,

$$m_\lambda(\zeta_{(n,k)}) = (-1)^{a+\frac{a}{n}\gcd(\lambda_1-\lambda_2,n)} \binom{k\gcd(\lambda_1-\lambda_2,n)}{\frac{a}{n}\gcd(\lambda_1-\lambda_2,n)} \neq 0.$$

Theorem **6.1** の (1) と (2) は, 群行列式の定義と Lemma **5.2** より明らかである. また, (3) は Lemma **3.4**, (7) は Lemma **3.5**, (8) は Lemma **3.6** より従う. 性質 (4) を示すために, 群行列式に関する次の補題を用意する.

Lemma 6.2. 集合 G を有限群, 写像 ψ を G の自己同型とする. このとき, $\Theta(G)$ の不定元 x_g を $x_{\psi(g)}$ と置き換える変換で, $\Theta(G)$ は不変である.

Lemma **6.2** を用いて, 性質 (4) を示す.

Proof of Theorem **6.1** (4). 正の整数 n と互いに素な正の整数 l と任意の元 $\bar{i} \in \mathbb{Z}/n\mathbb{Z}$ に対して, $\psi_l(\bar{i}) = \overline{li}$ とすれば, ψ_l は $\mathbb{Z}/n\mathbb{Z}$ の自己同型写像となる. したがって, $\mathbb{C}$ 代数写像 $\tilde{\psi}_l$ を $\tilde{\psi}_l \colon \mathbb{C}[x_g] \ni x_{\bar{i}} \mapsto x_{\overline{li}} \in \mathbb{C}[x_g]$ によって定義すれば, Lemma **6.2** より, $\tilde{\psi}_l(\Theta(\mathbb{Z}/n\mathbb{Z})^k) = \Theta(\mathbb{Z}/n\mathbb{Z})^k$ となるので, Lemma **5.2** より, $m_\lambda(\zeta_{(n,k)}) = m_{l\cdot\lambda}(\zeta_{(n,k)})$ が得られる. □

性質 (5) を示す.

Proof of Theorem **6.1** (5). Lemma **5.2** と恒等式 $\Theta(\mathbb{Z}/n\mathbb{Z})^{k+l} = \Theta(\mathbb{Z}/n\mathbb{Z})^k \Theta(\mathbb{Z}/n\mathbb{Z})^l$ より, 直ちに導かれる. □

性質 (6) を示す.

Proof of Theorem **6.1** (6). 任意の $\lambda \in \Lambda_2^k$ に対して, $a \in \mathbb{N}$ が存在して $\lambda = (2^{2k-2a}, 1^{2a})$ が成り立つことに注意しておく. 定義より, $\Theta(\mathbb{Z}/2\mathbb{Z}) = x_2^2 - x_1^2$ となるので,

$$\begin{aligned}\Theta(\mathbb{Z}/2\mathbb{Z})^k &= (x_2^2 - x_1^2)^k \\ &= \sum_{a=0}^{k} \binom{k}{a} (x_2^2)^{k-a} (-x_1^2)^a \\ &= \sum_{a=0}^{k} (-1)^a \binom{k}{a} x_1^{2a} x_2^{2(k-a)}\end{aligned}$$

となる. よって, Lemma **5.2** より, $m_\lambda(\zeta_{(2,k)}) = (-1)^a \binom{k}{a} \neq 0$ が成り立つ. □

7 可換群の群行列式の項数と正則表現の作用で不変なある線型空間の次元に関する不等式

本章では, 可換群の群行列式の冪乗の項数と, その群の正則表現の作用で不変なある多変数同次多項式の成す線型空間の次元に関する不等式について説明する. 有限可換群が巡回群である場合は, この不等式は Corollary **4.3** と等しいことがわかる. この事実と Lemma **3.4** より, Corollary **4.6** が導かれる. つまり, 素数位数の群の群行列式の項全体は, その群の正則表現の作用で不変な同次多項式の成す線型空間の基底を成すことがわかる. また, 正則表現の作用で不変な同次多項式の成す線型空間の次元は, 二項係数と Euler のトーシェント関数を用いて明示的に表示できることが知られているので, これを用いると, 素数位数の群の群行列式の項数を, 二項係数と Euler のトーシェント関数を用いて明示的に表示できることがわかる.

既約表現全体 $\widehat{G}$ は群を成すので, Dedekind の定理より, 任意の $\chi \in \widehat{G}$ に対して, $\Theta(G)$ の不定元 x_g を $\chi(g)x_g$ と変換しても $\Theta(G)$ は不変である. したがって, $\chi \in \widehat{G}$ に対して, $\mathbb{C}$ 代数写像 ψ_χ を $\psi_\chi \colon \mathbb{C}[x_g] \ni x_g \mapsto \chi(g)x_g \in \mathbb{C}[x_g]$ によって定義すれば, $\Theta(G)^k$ の項 $x_{a_1}x_{a_2}\cdots x_{a_{kn}}$ に対して,

$$\psi_\chi\left(x_{a_1}x_{a_2}\cdots x_{a_{kn}}\right) = x_{a_1}x_{a_2}\cdots x_{a_{kn}}$$

となることがわかる. よって, $\Theta(G)^k$ の項は, kn 次同次多項式全体の集合 $\mathbb{C}[x]_{kn}$ の部分集合 $\mathbb{C}[x]_{kn}^{\psi_\chi} := \{f \in \mathbb{C}[x]_{kn} \mid \psi_\chi(f) = f\}$ に属する. ゆえに,

$$\mathrm{N}\left(\Theta(G)^k\right) \leq \dim \bigcap_{\chi \in \widehat{G}} \mathbb{C}[x]_{kn}^{\psi_\chi} \tag{1}$$

が成り立つ. 特に $G = \mathbb{Z}/n\mathbb{Z}$ の場合は, $\widehat{\mathbb{Z}/n\mathbb{Z}} (\cong \mathbb{Z}/n\mathbb{Z})$ はある既約指標 χ によって生成されるので, 次の系が得られる.

Corollary 7.1. 任意の正の整数 k と n に対して, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/n\mathbb{Z})^k\right) \leq \dim \mathbb{C}[x]_{kn}^{\psi_\chi}.$$

ここで,

$$S := \{(i_1, i_2, \dots, i_n) \in \mathbb{N}^n \mid i_1 + i_2 + \cdots + i_n = kn,\ n \mid i_1 + 2i_2 + \cdots + ni_n\}$$

とすれば,

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \in \mathbb{C}[x]_{kn}^{\psi_\chi} \iff (i_1, i_2, \dots, i_n) \in S$$

であり, 写像 ϕ: $S \ni (i_1, i_2, \dots, i_n) \mapsto (n^{i_n}, (n-1)^{i_{n-1}}, \dots, 1^{i_1}) \in \Lambda_n^k$ は全単射なので, 不等式 (1) は, Corollary **4.3** が成り立つことを示していることに他ならない.

また, $G = \mathbb{Z}/n\mathbb{Z}$ の場合, $\mathbb{C}[x]_{kn}^{\psi_\chi}$ は $\mathbb{Z}/n\mathbb{Z}$ の正則表現の作用で不変な線型空間なので, $\mathbb{C}[x]_{kn}^{\psi_\chi} = \mathbb{C}[x]_{kn}^{\mathbb{Z}/n\mathbb{Z}}$ と書ける. 実際, V を $\mathbb{C}$ 上の n 次元線型空間とし, V の基底を $(e_1, e_2, \dots, e_n)$ とする. このとき, 表現 ρ: $\mathbb{Z}/n\mathbb{Z} \to \mathrm{GL}(V)$ を $\rho(\overline{1})e_i = \omega_n^i e_i$ で定めれば, ρ は $\mathbb{Z}/n\mathbb{Z}$ の正則表現と同値である. この表現 ρ を V 上の多項式環 $P[V] = \mathbb{C}[x]$ へ拡張したものを $\tilde{\rho}$ とする. そして, $\mathbb{Z}/n\mathbb{Z}$ の $\mathbb{C}[x]$ への作用を

$$\begin{array}{ccccc} \mathbb{Z}/n\mathbb{Z} & \curvearrowright & \mathbb{C}[x] & \xrightarrow{\simeq} & \mathbb{C}[x] \\ \cup & & \cup & & \cup \\ \overline{i} & \curvearrowright & x_j & \mapsto & \tilde{\rho}(\overline{i})x_j = \omega_n^{ij} x_j \end{array}$$

で与えれば, $\mathbb{C}[x]_{kn}^{\psi_\chi} = \mathbb{C}[x]_{kn}^{\mathbb{Z}/n\mathbb{Z}}$ と書ける. したがって, n が素数 p の場合, $\dim \mathbb{C}[x]_p^{\mathbb{Z}/p\mathbb{Z}} = |\Lambda_p^1|$ となることと, x_λ が $\Theta(G)$ の項ならば, $x_\lambda \in \mathbb{C}[x]_p^{\psi_\chi} = \mathbb{C}[x]_p^{\mathbb{Z}/p\mathbb{Z}}$ となることより, $\Theta(\mathbb{Z}/p\mathbb{Z})$ の項全体が, $\mathbb{C}[x]_p^{\mathbb{Z}/p\mathbb{Z}}$ の基底となることがわかる. これは, Corollary **4.6** が導かれたことを意味する.

ここで, $a(n, m)$ を $\mathbb{Z}/n\mathbb{Z}$ の正則表現の作用で不変な n 変数 m 次同次多項式の成す線型空間 $\mathbb{C}[x_1, x_2, \dots, x_n]_m^{\mathbb{Z}/n\mathbb{Z}}$ の次元とすれば, $a(n, m)$ は, 二項係数と Euler のトーシェント関数 φ を用いて以下のように明示的に表示できることが知られている ([2] と [3]).

Theorem 7.2 (Hermite の相互律, Theorem **1.6**)**.** 任意の正の整数 m と n に対して, 次が成り立つ.

$$a(n, m) = \frac{1}{m+n} \sum_{d \mid \gcd(m,n)} \binom{\frac{m}{d} + \frac{n}{d}}{\frac{n}{d}} \varphi(d).$$

よって, この表示を用いれば, 次の Lemma を得る.

Lemma 7.3 (Lemma **1.7**)**.** 任意の正の整数 k と n に対して, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/n\mathbb{Z})^k\right) \leq \left|\Lambda_n^k\right| = a(n, kn) = \frac{1}{n} \sum_{d \mid n} \binom{dk + d - 1}{d - 1} \varphi\left(\frac{n}{d}\right).$$

Proof. Theorem **7.2** より,

$$\begin{aligned} a(n, kn) &= \frac{1}{kn+n} \sum_{d \mid \gcd(kn,n)} \binom{\frac{kn}{d} + \frac{n}{d}}{\frac{n}{d}} \varphi(d) \\ &= \frac{1}{n(k+1)} \sum_{d \mid n} \binom{\frac{kn}{d} + \frac{n}{d}}{\frac{n}{d}} \varphi(d) \\ &= \frac{1}{n(k+1)} \sum_{d \mid n} \binom{dk + d}{d} \varphi\left(\frac{n}{d}\right) \end{aligned}$$

となる. ここで,

$$\frac{1}{n(k+1)}\binom{dk+d}{d} = \frac{1}{n(k+1)}\frac{dk+d}{d}\frac{(dk+d-1)!}{(dk)!(d-1)!} = \frac{1}{n}\binom{dk+d-1}{d-1}$$

より, Lemma は示された. □

Lemma **7.3** の右辺は, 巡回群の巡回指数の特殊化になっている. 巡回指数とは Redfield [12] と Pólya [11] によって, それぞれ独立に定義された概念である. Lemma **7.3** において n を素数とすれば, Corollary **4.5** より, 次の Corollary が直ちに得られる.

Corollary 7.4 (Corollary **1.8**)**.** 任意の素数 p に対して, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/p\mathbb{Z})\right) = \left|\Lambda_p^1\right| = a(p,p) = \frac{1}{p}\sum_{d|p}\binom{2d-1}{d-1}\varphi\left(\frac{p}{d}\right).$$

8 直積群の群行列式の項数に関する不等式

本章では, 直積群の群行列式の項数に関する等式を得る. この等式は, 直積群の群行列式の項数を下から評価する不等式を導く.

直積群の群行列式の項数に関する等式は次である.

Lemma 8.1 (Lemma **1.9**)**.** 集合 G を有限群 H と K の直積群とする. このとき, 次が成り立つ.

$$\Theta(G)\big|_{x_{(h,k)}=x_hx_k} = \Theta(H)^{|K|}\Theta(K)^{|H|} \in \mathbb{C}[x_h, x_k; h \in H, k \in K].$$

ただし, $\Theta(G)\big|_{x_{(h,k)}=x_hx_k}$ は, $\Theta(G)$ の不定元 $x_{(h,k)}$ に x_hx_k を代入したものを表す.

Proof. 群 H と K をそれぞれ $H = \{h_1, h_2, \ldots, h_{|H|}\}$, $K = \{k_1, k_2, \ldots, k_{|K|}\}$ とし, G の元 g_i を $g_i = (h_p, k_q)$ と表す. ただし, $i = |H|(q-1)+p$, $1 \le p \le |H|$, $1 \le q \le |K|$ とする. このとき, 次が成り立つ.

$$\begin{aligned}\left(x_{g_ig_j^{-1}}\right)_{1\le i,j\le|G|}\Big|_{x_{(h,k)}=x_hx_k} &= \left(\left(x_{h_ih_j^{-1}}\right)_{1\le i,j\le|H|} x_{k_sk_t^{-1}}\right)_{1\le s,t\le|K|} \\ &= \left(x_{h_ih_j^{-1}}\right)_{1\le i,j\le|H|} \otimes \left(x_{k_ik_j^{-1}}\right)_{1\le i,j\le|K|}.\end{aligned}$$

ただし, $\otimes$ は, Kronecker 積を表す. したがって,

$$\Theta(G)\big|_{x_{(h,k)}=x_hx_k} = \Theta(H)^{|K|}\Theta(K)^{|H|}$$

が成り立つ. □

明らかに, 不定元を特殊化した群行列式の項数は, 特殊化する前の群行列式の項数以下となる. したがって, 次が成り立つことがわかる.

Corollary 8.2 (Corollary **1.10**)**.** 有限直積群 $G = H \times K$ に対して, 次の不等式が成り立つ.

$$\mathrm{N}(\Theta(G)) \geq \mathrm{N}\left(\Theta(H)^{|K|}\Theta(K)^{|H|}\right) = \mathrm{N}(\Theta(H)^{|K|})\,\mathrm{N}(\Theta(K)^{|H|}).$$

特に, m_i を素冪で, $G = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_l\mathbb{Z}$ とすれば, 群行列式に関する次の不等式が得られる.

$$\prod_{i=1}^{l} \mathrm{N}\left(\Theta(\mathbb{Z}/m_i\mathbb{Z})^{\frac{n}{m_i}}\right) \leq \mathrm{N}\left(\Theta(G)\right) \leq \frac{1}{n}\sum_{d|n}\binom{dk+d-1}{d-1}\varphi\left(\frac{n}{d}\right).$$

9 素数に関する単項式型対称式の主特殊化の零点予想

本章では, 素数に関する単項式型対称式の主特殊化の零点予想について述べる. 私たちは, 以下が成り立つことを予想する.

Conjecture 9.1. 正の整数 k, 素数 p, 長さ kp の分割 λ に対して, 次が成り立つ.

$$p \mid |\lambda| \iff m_\lambda(\zeta_{(p,k)}) \neq 0.$$

すなわち, $p \nmid |\lambda|$ ならば, 分割 λ が主特殊化の零点となることを予想している. この予想は, 次の予想と同値である.

Conjecture 9.2. 正の整数 k と素数 p に対して, 次が成り立つ.

$$\mathrm{N}\left(\Theta(\mathbb{Z}/p\mathbb{Z})^k\right) = |\Lambda_p^k| = \frac{1}{p}\sum_{d|p}\binom{dk+d-1}{d-1}\varphi\left(\frac{p}{d}\right).$$

謝辞

関係者の皆様に御礼申し上げます。このような場での発表の機会を設けて頂きありがとうございます。特に篠原雅史先生には格別の感謝を申し上げます。また、山口、山口、渋川が共同研究に至るきっかけを作って下さった落合啓之先生に感謝いたします。

参考文献

[1] Keith Conrad. The origin of representation theory. *Enseignement Mathematique*, 44:361–392, 1998.

[2] A. Elashvili and M. Jibladze. Hermite reciprocity for the regular representations of cyclic groups. *Indagationes Mathematicae*, 9(2):233 – 238, 1998.

[3] A. Elashvili, M. Jibladze, and D. Pataraia. Combinatorics of necklaces and "hermite reciprocity". *Journal of Algebraic Combinatorics*, 10(2):173–188, Sep 1999.

[4] Ferdinand Georg Frobenius. Über die primfactoren der gruppendeterminante. *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin*, pages 1343–1382, 1896. Reprinted in *Gesammelte Abhandlungen, Band III*. Springer-Verlag Berlin Heidelberg, New York, 1968, pages 38–77.

[5] Ferdinand Georg Frobenius. Über gruppencharaktere. *Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin*, pages 985–1021, 1896. Reprinted in *Gesammelte Abhandlungen, Band III*. Springer-Verlag Berlin Heidelberg, New York, 1968, pages 1–37.

[6] Thomas Hawkins. The origins of the theory of group characters. *Archive for History of Exact Sciences*, 7(2):142–170, Jan 1971.

[7] Thomas Hawkins. Hypercomplex numbers, Lie groups, and the creation of group representation theory. *Archive for History of Exact Sciences*, 8(4):243–287, Jan 1972.

[8] Thomas Hawkins. New light on Frobenius' creation of the theory of group characters. *Archive for History of Exact Sciences*, 12(3):217–243, Sep 1974.

[9] John Konvalina. A generalization of Waring's formula. *journal of combinatorial theory, Series A*, 75(2):281–294, 1996.

[10] Richard Mansfield. A group determinant determines its group. *Proceedings of the American Mathematical Society*, 116(4):939–941, 1992.

[11] George Pólya. Kombinatorische anzahlbestimmungen für gruppen, graphen und chemische verbindungen. *Acta Mathematica*, 68:145–254, 1937.

[12] J. Howard Redfield. The theory of group-reduced distributions. *American Journal of Mathematics*, 49(3):433–455, 1927.

[13] Bartel Leenert van der Waerden. *A history of algebra*. Springer-Verlag Berlin Heidelberg, 1985.

[14] Naoya Yamaguchi. An extension and a generalization of Dedekind's theorem. *International Journal of Group Theory*, 6(3):5–11, 2017.

[15] Naoya Yamaguchi and Yuka Yamaguchi. Generalized group determinant gives a necessary and sufficient condition for a subset of a finite group to be a subgroup. *arXiv preprint arXiv:1902.04908*, 2019.

Frame numbers, splitting fields, and integral adjacency algebras of commutative association schemes

花木 章秀 (信州大学理学部 hanaki@shinshu-u.ac.jp)

(X, S) を可換なアソシエーションスキームとする。牛山裕暁は修士論文 (2019 信州大学) [6] で次の式を与えた。

$$\mathcal{F}(S) = (-1)^e \left| \bigoplus_i \mathcal{O}_{K_i} : \varphi(\mathbb{Z}S) \right|^2 \prod_i d(K_i)$$

ここで $\mathcal{F}(S)$ は Frame 数、K_i は同型 $\varphi : \mathbb{Q}S \xrightarrow{\sim} \bigoplus_i K_i$ で定まる代数体、$d(K_i)$ は K_i の判別式、$\mathcal{O}_{K_i}$ は K_i の整数環、$e = \sharp\{s \in S \mid s \neq s^*\}/2$ である。あとで説明するように、有理整数環 $\mathbb{Z}$ 上の隣接代数 $\mathbb{Z}S$ は自然に $\bigoplus_i \mathcal{O}_{K_i}$ に埋め込まれる。牛山は多くの例を計算することによってこの式を予想し $|S| = 3$ の場合にそれを証明した。本講演ではこの式を一般に証明し、またその意味なども解説する。証明は本質的には古い結果などを組み合わせるだけでき、式の意味をよく理解すれば難しくはない。この式は可換アソシエーションスキームの指標表の可能性を制限するなどの応用が期待できるが、現在の所、有用な応用は見つかってはいない。

1 アソシエーションスキームと隣接代数、指標

X を有限集合とする。S を $X \times X$ の分割、すなわち $X \times X = \bigcup_{s \in S} s$, $s \in S$ は空でない、また $s \neq t$ ならば $s \cap t = \emptyset$、であるとする。このとき組 (X, S) が**アソシエーションスキーム** (association scheme) であるとは

(1) $1 := \{(x, x) \mid x \in X\} \in S$,

(2) $s \in S$ ならば $s^* := \{(y, x) \mid (x, y) \in s\} \in S$,

(3) $s, t, u \in S$ に対して非負整数 p^u_{st} が存在して、$(x, y) \in u$ ならば $\sharp\{z \in X \mid (x, z) \in s, (z, y) \in t\} = p^u_{st}$

をみたすこととする。条件 (3) は隣接行列を使えば理解しやすい。$s \in S$ に対して、その**隣接行列** (adjacency matrix) σ_s とは、行、列、ともに集合 X で添字付けられた行列で、その (x, y)-成分は $(x, y) \in s$ のとき 1、そうでないとき 0 として定まるものである。これらを用いると、条件は

(1)' ある $1 \in S$ があって s_1 は単位行列、

(2)' $s \in S$ に対して、ある $s^* \in S$ があって $\sigma_{s^*} = \sigma_s^T$ (転置行列)、

(3)' $s, t, u \in S$ に対して非負整数 p^u_{st} が存在して、行列の積に関して $\sigma_s \sigma_t = \sum_{u \in S} p^u_{st} \sigma_u$

と書き直すことができる。$s \in S$ に対して $n_s := p^1_{ss^*}$ とおいて、これを**分岐指数** (valency) という。行列 σ_s は各行、各列にそれぞれ n_s 個の 1 をもつことが分かる。任意の $s, t, u \in S$ に対して $p^u_{st} = p^u_{ts}$ が成り立つとき (X, S) は**可換** (commutative) であるという。これは $\sigma_s \sigma_t = \sigma_t \sigma_s$

第 36 回代数的組合せ論シンポジウム 2019.6.19 長崎大学

であることと同値である。また任意の $s \in S$ に対して $s^* = s$ であるとき (X, S) は**対称** (symmetric) であるという。対称ならば可換であることがすぐに分かる。

条件 (3)' から $\mathbb{Z}S := \bigoplus_{s\in S} \mathbb{Z}\sigma_s$ は環になる。また単位元をもつ可換環 R に対して $RS := R \otimes_{\mathbb{Z}} \mathbb{Z}S$ は R-代数となる。これを (X, S) の R 上の**隣接代数** (adjacency algebra) という。σ_s を R 上の行列と見て $\{\sigma_s \mid s \in S\}$ の生成する R-代数と思ってもよい。(X, S) が可換ならば、任意の係数環上の隣接代数は可換である。

命題 1.1. [5, Theorem 4.1.3 (ii)]. アソシエーションスキーム (X, S) の標数 0 の体 K 上の隣接代数 KS は分離的、したがって半単純である。

Wedderburn の定理 [3, Theorem 2.4.3] から、複素数体 $\mathbb{C}$ 上の隣接代数 $\mathbb{C}S$ について、ある正の整数 $d_1, \ldots, d_\ell$ が存在して

$$\mathbb{C}S \cong \bigoplus_{i=1}^{\ell} M_{d_i}(\mathbb{C})$$

となる。各直和因子への射影が $\mathbb{C}S$ の既約表現の同値類の完全代表系となる。表現の対角和 (トレース) を**指標** (character) という。特に既約表現の指標を**既約指標**という。表現の同値類は行列の相似を許すが、その対角和は一定であり、指標は一意に決まる。また複素数体上の半単純代数に対しては表現が同値であることと指標が一致することは同値である。既約指標全体の集合を $\mathrm{Irr}(S)$ と表す。$\mathrm{Irr}(S)$ は複素既約表現の同値類の集合と思ってもよい。$\mathrm{Irr}(S) \times S$ 行列 $(\chi(\sigma_s))_{\chi,s}$ を (X, S) の**指標表** (characer table) という。$\chi(\sigma_s)$ は代数的整数となるので、指標表は代数的整数を成分とする行列である。(X, S) が可換ならば $|\mathrm{Irr}(S)| = |S|$ であり、指標表は正方行列となる。これを **第一固有行列** (first eigenmatrix) ともいう。

隣接代数は行列環として定義されているため、初めから表現が一つ与えられている。これを**標準表現** (standard representation) といい、その指標 γ を**標準指標** (standard character) という。定義から $\gamma(\sigma_s) = \delta_{1s}|X|$ である。標準指標を既約指標の和に分解し

$$\gamma = \sum_{\chi\in\mathrm{Irr}(S)} m_\chi \chi$$

と表すとき、この重複度 m_χ を χ の**重複度** (multiplicity) という。

2 Frame 数

アソシエーションスキーム (X, S) に対して、その *Frame* **数** (Frame number) $\mathcal{F}(S)$ は、分岐指数、既約指標の次数と重複度を用いて次のように定義される。

$$\mathcal{F}(S) := |X|^{|S|} \frac{\prod_{s\in S} n_s}{\prod_{\chi\in\mathrm{Irr}(S)} m_\chi^{\chi(1)^2}}$$

Frame 数について次のようなことが知られている。

命題 2.1. [2, Chap. 2, Theorem 4.2 (i)]. $\mathcal{F}(S) \in \mathbb{Z}$ である[1]。

次の定理は可換の場合に Arad-Fisman-Muzychuk [1] で示された後に、一般の場合は Hanaki [4] で示された。実は今回の結果も本質的には [4] で既に示されている。

定理 2.2 (Arad-Fisman-Muzychuk [1, Theorem 1.1]; Hanaki [4, Theorem 4.2])**.** F を正標数 p の体とする。このとき隣接代数 FS が分離的 (半単純) であるための必要十分条件は $p \nmid \mathcal{F}(S)$ となることである。

アソシエーションスキームが可換であるときには更にいくつかのことが知られている。

[1] 更に強く $|X|^{-2}\mathcal{F}(S) \in \mathbb{Z}$ である。この数を *Frame* **商** (Frame quotient) という。

命題 2.3. [2, Chap. 2, Theorem 4.2 (ii) and its proof]. (X, S) が可換であるならば、指標表 T を用いて $\mathcal{F}(S) = (\det T)\overline{(\det T)}$ と表すことができる。特に指標の値がすべて有理数 (有理整数) ならば $\mathcal{F}(S)$ は平方数である。

(X, S) を可換とし、指標の値がすべて有理数であると仮定する。このとき同型 $\varphi : \mathbb{C}S \cong \mathbb{C} \oplus \cdots \oplus \mathbb{C}$ は単射

$$\varphi : \mathbb{Z}S \to \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$$

を引き起こす。σ_s $(s \in S)$ の像が指標表の列となることから $|\det T| = |\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} : \varphi(\mathbb{Z}S)|$ であり、したがって

$$\mathcal{F}(S) = |\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} : \varphi(\mathbb{Z}S)|^2$$

が成り立っている。

ここで簡単な例を見ておく。

例 2.4. (X, S) を conference グラフ ($\left(n, \frac{n-1}{2}; \frac{n-5}{4}, \frac{n-1}{4}\right)$-強正則グラフ) で定まる $|S| = 3$ のアソシエーションスキームとする。このとき指標表と Frame 数は以下の通り。

	σ_0	σ_1	σ_2	m_i
χ_0	1	$(n-1)/2$	$(n-1)/2$	1
χ_1	1	$(-1+\sqrt{n})/2$	$(-1-\sqrt{n})/2$	$(n-1)/2$
χ_2	1	$(-1-\sqrt{n})/2$	$(-1+\sqrt{n})/2$	$(n-1)/2$

$$\mathcal{F}(S) = n^2 \cdot n$$

例 2.5. A を 2-(v, k, λ) 対称デザインの結合行列とする。またデザインの位数を $n := k - \lambda$ とする。

$$\sigma_0 = \begin{pmatrix} I_v & O_v \\ O_v & I_v \end{pmatrix}, \quad \sigma_1 = \begin{pmatrix} J_v - I_v & O_v \\ O_v & J_v - I_v \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} O_v & A \\ A^T & O_v \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} O_v & J_v - A \\ J_v - A^T & O_v \end{pmatrix}.$$

とおけば、これらを隣接行列として対称アソシエーションスキームが定義される。このとき指標表と Frame 数は以下の通り。

	σ_0	σ_1	σ_2	σ_3	m_i
χ_0	1	$v-1$	k	$v-k$	1
χ_1	1	$v-1$	$-k$	$-v+k$	1
χ_2	1	-1	$\sqrt{n}$	$-\sqrt{n}$	$v-1$
χ_3	1	-1	$-\sqrt{n}$	$\sqrt{n}$	$v-1$

$$\mathcal{F}(S) = (2v)^4 \cdot \frac{(v-1)k(v-k)}{(v-1)^2} = 2^4 v^4 n$$

上記の二つの例では、(一般には n に依存するが) Frame 数は平方数ではなく、平方因子以外に n が現れている。またその n が指標の値に $\sqrt{n}$ として現れているように見える ($\mathcal{F}(S) = (\det T)\overline{(\det T)}$ によって当たり前のことではあるが)。

3 整数環上の隣接代数

指標の値が有理数とは限らない場合について $|\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} : \varphi(\mathbb{Z}S)|$ に相当するものを考える。(X, S) を可換アソシエーションスキームとする。Wedderburn の定理 [3, Theorem 2.4.3] から、有理数体 $\mathbb{Q}$ 上の隣接代数 $\mathbb{Q}S$ はいくつかの斜体上の全行列環の直和に同型となるが、可換性を仮定しているので、斜体は体で、行列環のサイズはすべて 1 となる。すなわち

$$\mathbb{Q}S \cong K_1 \oplus \cdots \oplus K_\ell$$

となる代数体 $K_1,\dots,K_\ell$ が存在する。実際に K_i と同型は次のように与えられる。$\mathrm{Irr}(S)$ を代数共役によって類別し、その完全代表系を $\chi_1,\dots,\chi_\ell$ とする。K_i を $\mathbb{Q}$ に $\{\chi_i(\sigma_s)\mid s\in S\}$ を添加した体とする。このとき $\varphi:\mathbb{Q}S\to K_1\oplus\cdots\oplus K_\ell$, $\varphi(\sigma_s)=(\chi_1(\sigma_s),\dots,\chi_\ell(\sigma_s))$ が $\mathbb{Q}$-同型となる。K_i の整数環を $\mathcal{O}_{K_i}$ で表す。指標の値 $\chi_i(\sigma_s)$ が代数的整数であることから、この同型 φ は単射

$$\varphi:\mathbb{Z}S\to\mathcal{O}_{K_1}\oplus\cdots\oplus\mathcal{O}_{K_\ell}$$

を引き起こす。$|\mathcal{O}_{K_1}\oplus\cdots\oplus\mathcal{O}_{K_\ell}:\varphi(\mathbb{Z}S)|$ を考えるのが自然であろう。[2]

4 判別式

この節で述べる結果は、本質的には [4] で既に示されている。

有限次代数体にはよく知られているように判別式が定義されるが、これを一般化して有限次代数とその表現 (加群) に対しても判別式が定義される (例えば [3, §6.3] を参照)。

K を体とし、A を n 次元 K-代数、$a_1\dots,a_n\in A$ とする。また A の有限次元行列表現 Φ を考える。このとき

$$d_{\{a_i\},\Phi}:=\det(\mathrm{trace}\ \Phi(a_ia_j))$$

とおいて、これを A の $\{a_1,\dots,a_n\}$ と Φ に関する**判別式** (discriminant) という。A を有限次代数体 ($\mathbb{Q}$ の有限次拡大体)、$\{a_1,\dots,a_n\}$ を A の整数基、Φ を A の正則表現とすれば、この定義は代数体の判別式の定義と同じになる。$b_1,\dots,b_n\in A$ を正方行列 P を用いて $(b_1,\dots,b_n)=(a_1,\dots,a_n)P$ と表せたとすると $d_{\{b_i\},\Phi}=(\det P)^2d_{\{a_i\},\Phi}$ である。このことから $a_1\dots,a_n$ が基底でなければ $d_{\{a_i\},\Phi}=0$ であることが分かる。

L を K の拡大体とするとき、K-代数 A の係数を拡大して L-代数 $A^L:=L\otimes_K A$ が得られる。A の表現も自然に A^L の表現に拡張される。判別式は A^L の表現と見ても変わらないので、適当に係数を拡大して考えても構わない。

(X,S) をアソシエーションスキームとし、次の表現を考える。

- 標準表現 Γ : 指標は $\sum_{\chi\in\mathrm{Irr}(S)}m_\chi\chi$
- 正則表現 Λ' : 指標は $\sum_{\chi\in\mathrm{Irr}(S)}\chi(1)\chi$
- Λ : 指標 $\sum_{\chi\in\mathrm{Irr}(S)}\chi$ をもつ表現

後で (X,S) を可換と仮定するが、その際には $\Lambda=\Lambda'$ となる。隣接代数 $\mathbb{C}S$ の基底としては次を考える。

- $\{\sigma_s\mid s\in S\}$: 隣接行列の集合
- $\{e_{jk}^{(i)}\mid 1\le i\le\ell,\ 1\le j,k\le d_i\}$: 同型 $\mathbb{C}S\cong\bigoplus_{i=1}^{\ell}M_{d_i}(\mathbb{C})$ による各直和因子の行列単位の逆像

補題 4.1. $d_{\{\sigma_s\},\Gamma}=(-1)^e|X|^{|S|}\prod_{s\in S}n_s$ が成り立つ。ただし $e=\sharp\{s\in S\mid s\neq s^*\}/2$ である。

Proof. $d_{\{\sigma_s\},\Gamma}=\det(\mathrm{trace}\ \Gamma(\sigma_s\sigma_t))$ であって、$\mathrm{trace}\ \Gamma(\sigma_s\sigma_t)=\delta_{s^*t}n_s|X|$ である。符号のズレは $s^*\neq s$ となる回数だけ生じる。 □

補題 4.2. $d_{\{e_{jk}^{(i)}\},\Gamma}=(-1)^f\prod_{\chi\in\mathrm{Irr}(S)}m_\chi^{\chi(1)^2}$ が成り立つ。ただし $f=\sum_{\chi\in\mathrm{Irr}(S)}\chi(1)(\chi(1)-1)/2$ である。

Proof. $\mathrm{trace}\,\Gamma(e_{jk}^{(i)}e_{j'k'}^{(i')})=\delta_{jk'}\delta_{j'k}\delta_{ii'}m_{\chi_i}$ である。よって $\mathrm{trace}\,\Gamma(e_{jk}^{(i)}e_{j'k'}^{(i')})=(-1)^f\prod_{\chi\in\mathrm{Irr}(S)}m_\chi^{\chi(1)^2}$ である。符号のズレは $e_{jk}^{(i)}\neq e_{kj}^{(i)}$ となる回数、すなわち非対称な行列単位の数だけ生じる。 □

[2] もちろん、この部分加群の単因子を調べれば、より深い情報が得られるが、今回は単因子については考えない。

補題 4.3. $d_{\{e_{jk}^{(i)}\},\Lambda} = (-1)^f$ が成り立つ。ただし $f = \sum_{\chi\in\mathrm{Irr}(S)} \chi(1)(\chi(1)-1)/2$ である。

Proof. 前の補題で表現の既約因子の重複度を 1 とすればよい。 □

命題 4.4. $\mathcal{F}(S) = (-1)^e d_{\{\sigma_s\},\Lambda}$ が成り立つ。ただし $e = \sharp\{s \in S \mid s \neq s^*\}/2$ である。

Proof. 基底 $\{\sigma_s\}$ と $\{e_{jk}^{(i)}\}$ の変換行列を P とすれば

$$\frac{d_{\{\sigma_s\},\Gamma}}{d_{\{e_{ij}^{(\chi)}\},\Gamma}} = (\det P)^2 = \frac{d_{\{\sigma_s\},\Lambda}}{d_{\{e_{ij}^{(\chi)}\},\Lambda}}$$

である。上の補題から結果を得る。 □

可換アソシエーション・スキームに対しては $\Lambda = \Lambda'$ であったから、次が成り立つ。

系 4.5. (X, S) が可換ならば正則表現 Λ' について $\mathcal{F}(S) = (-1)^e d_{\{\sigma_s\},\Lambda'}$ が成り立つ。ただし $e = \sharp\{s \in S \mid s \neq s^*\}/2$ である。

5 結果とその証明

次の定理がこの講演の主結果である。

定理 5.1. (X, S) を可換アソシエーションスキームとする。ある代数体 K_i $(i = 1, \ldots, \ell)$ と同型 $\varphi : \mathbb{Q}S \to \bigoplus_{i=1}^{\ell} K_i$ が存在する。この同型によって $\mathbb{Z}S$ は $\bigoplus_{i=1}^{\ell} \mathcal{O}_{K_i}$ に埋め込まれる。このとき

$$\mathcal{F}(S) = (-1)^e \left| \bigoplus_{i=1}^{\ell} \mathcal{O}_{K_i} : \varphi(\mathbb{Z}S) \right|^2 \prod_{i=1}^{\ell} d(K_i)$$

が成り立つ。ここで $\mathcal{O}_{K_i}$ は K_i の整数環、$d(K_i)$ は K_i の判別式、また $e = \sharp\{s \in S \mid s^* \neq s\}$ である。

Proof. 系 4.5 によって $\mathcal{F}(S) = (-1)^e d_{\{\sigma_s\},\Lambda'}$ である。ここでは Λ' は $\mathbb{C}$ 上の表現と見て $\mathbb{C}S$ の判別式を考えている。しかし、正則表現は $\mathbb{Q}$ 上でも実現されているので、この式を $\mathbb{Q}$ 上で考えても値は変わらないので、これを $\mathbb{Q}$-代数 $\mathbb{Q}S$ の正則表現の判別式と見ることができる。

各 K_i の整数基を集めて $\{\omega_j^{(i)} \mid 1 \leq i \leq \ell,\ 1 \leq j \leq \dim_{\mathbb{Q}} K_i\}$ を考えれば、これは $\bigoplus_{i=1}^{\ell} \mathcal{O}_{K_i}$ の基底となり $d_{\{\omega_j^{(i)}\},\Lambda'} = \prod_{i=1}^{\ell} d(K_i)$ である。$\bigoplus_{i=1}^{\ell} \mathcal{O}_{K_i}$ における $\varphi(\mathbb{Z}S)$ の指数を考えれば結果の式が成り立つ。 □

6 残された問題

主定理 (定理 5.1) は可換とは限らないアソシエーションスキームにも拡張されるであろうが、その際にはいくつかの問題を解決しなくてはならない。一般には斜体 D_i を用いて

$$\mathbb{Q}S \cong \bigoplus_{i=1}^{\ell} M_{d_i}(D_i)$$

と表される。この代数の “maximal order” における $\mathbb{Z}S$ の指数を見るのが自然と思われるが、同型が一意的でないことや斜体の判別式を考えなくてはならない。現状ではまだ眺めているだけである。

主定理の式を用いることによって、ある種のアソシエーションスキームの非存在が言える可能性があると思う。そのような例を探してみたい。

References

[1] Z. Arad, E. Fisman, and M. Muzychuk, *Generalized table algebras*, Israel J. Math. **114** (1999), 29–60.

[2] E. Bannai and T. Ito, *Algebraic combinatorics. I*, The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, 1984.

[3] Yu. A. Drozd and V. V. Kirichenko, *Finite-dimensional algebras*, Springer-Verlag, Berlin, 1994.

[4] A. Hanaki, *Semisimplicity of adjacency algebras of association schemes*, J. Algebra **225** (2000), no. 1, 124–129.

[5] P.-H. Zieschang, *An algebraic approach to association schemes*, Lecture Notes in Mathematics, vol. 1628, Springer-Verlag, Berlin, 1996.

[6] 牛山裕暁, アソシエーションスキームの整数環上の隣接代数, 修士論文, 信州大学, 2019.

Hamming スキーム上の調和指数 t-design

堀　亮太
九州工業大学大学院情報工学府
田上　真
九州工業大学大学院情報工学研究院

1　序論

球面上の調和指数デザインの Hamming スキーム版を行ったので、ここではその報告を行いたい。まず調和指数デザインの復習をする。

$\mathfrak{X} = (X, \{R_i\}_{i=0}^n)$ を対称アソシエーションスキームとし、$A_i \in M_X(\mathbb{C})$ $(i = 0, 1, \cdots, n)$ 達を関係 R_i 達に対する隣接行列とする (アソシエーションスキームの基礎理論については Bannai-Ito [5], Delsarte [9] を参照のこと)。一般に、$\mathbb{C}$ を複素数体、$M_X(\mathbb{C})$ を行と列が X で添え字付けられた行列全体、$\langle v_i : 1 \leq i \leq m \rangle$ をベクトル $v_1, \cdots, v_m$ で張られる $\mathbb{C}$ 上の部分空間を表すとする。

$\mathcal{A} = \langle A_i : 0 \leq i \leq n \rangle$ を $\mathfrak{X}$ の **Bose-Mesner 代数**とする。$\mathcal{A}$ のもう一つの特別な基底 $\{E_j : j = 0, 1, \cdots, n\}$ が次のように構成される ($\{E_j\}$ 達は半単純可換代数 $\mathcal{A}$ の原始冪等元全体である。以下の一般論については Delsarte[9] を参照のこと)。一般に、集合 X に対して、$\mathbb{C}^X$ を X で添え字付けられた $\mathbb{C}$ 成分縦ベクトル全体のなすエルミート内積空間を表すとする。$M_X(\mathbb{C})$、したがって $\mathcal{A}$ は $\mathbb{C}^X$ に左からの積で自然に作用する。今、$\mathfrak{X}$ は対称アソシエーションスキームであるので、A_i 達は互いに可換な実対称行列になり、$\mathbb{C}^X$ は $\mathbb{C}^X = W_0 \oplus W_1 \oplus \cdots \oplus W_n$ と A_i 達の極大な共通固有空間に直交分解される。ここで、極大の共通固有空間の数は $n + 1$ 個であり、さらにその一つは全ての成分が 1 のベクトル $\mathbf{1} \in \mathbb{C}^X$ で生成される 1 次元部分空間になることが知られている。一般性を失うことなく、$W_0 = \langle \mathbf{1} \rangle$ とする。$E_j \in M_X(\mathbb{C})$ を、$\mathbb{C}^X$ から W_j への直交射影子を $\mathbb{C}^X$ の標準基底で行列表示したものとすると、E_j 達は $\mathcal{A}$ の新しい基底となることが知られている。今、$W_0 = \langle \mathbf{1} \rangle$ であるので、$E_0 = \dfrac{1}{|X|} J$ である。$\dim W_j = m_j$ とし、$\{f_1, \cdots, f_{m_j}\}$ を W_j の正規直交基底の一つとする。縦ベクトル $\{f_1, \cdots, f_{m_j}\}$ を順に列に並べた $X \times m_j$ 行列を $P_j = (f_1, \cdots, f_{m_j})$ とすると、$E_j = P_j ({}^*P_j) \in M_X(\mathbb{C})$ となる。特に、E_j 達は半正定値である。ここで、一般に行列 A に対して、${}^tA, {}^*A$ で、それぞれ A の転置行列、エルミート転置行列を表すとする。

$\mathcal{A}$ の二つの基底 $\{A_i : 0 \leq i \leq n\}$、$\{E_i : 0 \leq i \leq n\}$ の間の変換を表す行列が**第 1 固有行列** P、**第 2 固有行列** Q である。すなわち、$P_j(i)$, $Q_j(i)$ でそれぞれ、P, Q の (i, j) 成分を表すとすると、

$$A_j = \sum_{j=0}^{n} P_j(i)E_i, \quad |X|E_j = \sum_{j=0}^{n} Q_j(i)A_i \quad (0 \leq i, j \leq n)$$

となっている。上記の様に、E_j 達は A_i 達の極大な共通固有空間への直交射影子になっており、さらに A_i 達は実対称行列なので、$P_j(i)$ 達は実数である。したがって、P, Q は $\{0, 1, \cdots, n\}$ で添え字づけられた実数成分を持つ $(n+1)$ 次正方行列である。よって、さらに E_j 達も実数成分の実対称行列になっている。

X の空でない部分集合 C に対して、$\phi_C \in \mathbb{C}^X$ を C の**特性ベクトル**、${}^t a = {}^t(a_0, a_1, \cdots, a_n) \in \mathbb{C}^{\{0,1,\cdots,n\}}$ を C の**内分布**とする。すなわち、

$$(\phi_C)(x) = \begin{cases} 1: & \text{if } x \in C, \\ 0: & \text{otherwise.} \end{cases}$$

$$a_i = \frac{1}{|C|}\left|R_i \cap C^2\right| = \frac{1}{|C|}{}^t\phi_C A_i \phi_C$$

と定義される。一般に $v \in \mathbb{C}^X$, $x \in X$ に対して、$v(x)$ で v の x 成分を表す。また内分布 $a = (a_0, a_1, \cdots, a_n)$ の **Q-変換**を $a' = (a'_0, a'_1, \cdots, a'_n) = aQ$ とする。以上の表記の下、対称アソシエーションスキーム $(X, \{R_i\}_{i=0}^n)$ 上の T-design は次のように定義される。

定義 1.1 (Delsarte[9]). $\{1, \cdots, n\}$ の部分集合 T に対して、X の空でない部分集合 C が **T-design** であるとは、任意の $t \in T$ に対して、$a'_t = 0$ が成り立つ時を言う。

T を $T = \{1, 2, \cdots, t\}$ と取り、対称アソシエーションスキームをそれぞれ Hamming スキーム、Johnson スキームと取ると、$\{1, \cdots, t\}$-design はそれぞれ強さ t の直交配列、組合せ t-design という、よく知られた組合せ構造と一致する事が知られている (Delsarte[9])。また、いくつかのアソシエーションスキーム上で、$\{1, \cdots, t\}$-design の ranked poset の言葉による特徴付けが与えられている ([10, 18])。この報告では、T が一つの元 $\{t\}$ からなる時、T-design を特に調和指数 t-design と呼び、一般の Hamming スキーム上で、調和指数 t-design を考察する。Binary Hamming スキーム上の調和指数 t-design ついては、Zhu et al.[20] による先行研究がある。

対称アソシエーションスキーム上の design は様々な空間上へ、良い有限点配置として数多くの拡張がなされている。特に、その拡張の初期のものとして、Delsarte-Goethals-Seidel[11] による球面全体をよく近似する有限点配置としての球面デザインがあり、代数的組合せ論の主な研究対象の一つとなっている。(これらの拡張の歴史については、Bannai-Bannai-Ito[2, 5 章] とその中の参考文献を参照のこと)。上記のように、調和指数 t-design は Delsarte[9] によって、T-design としてすでに定義されていたが、同様の概念は球面上でも

考えられ、調和指数 t-design の実質的な研究は球面上の場合に、Bannai-Okuda-Tagami[6] によって始められた。調和指数 t-design についてのこれまでの他の研究については、代数的組合せ論の観点からのデザイン理論の survey である Bannai et al. [3, 第 6 節] とその参考文献を参照のこと。

次に Hamming スキーム及びその上の調和解析を解説していく（[9, 5, 19, 12] 等を参照）。

q を 2 以上の自然数、F を q 個の元からなる加法群とし、F の単位元を 0 とする。また、n を自然数とし、$X = F^n$ とする。$x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n) \in X$ に対して、**Hamming 距離** $\partial(x, y) = \partial_H(x, y)$ を

$$\partial(x, y) = \partial_H(x, y) = |\{i : x_i \neq y_i \ (1 \leq i \leq n)\}|$$

とし、**Hamming 重み** $\mathrm{w}t(x)$ を

$$\mathrm{w}t(x) = d(x, 0) = |\{i : x_i \neq 0 \ (1 \leq i \leq n)\}|$$

とする。また、$0 \leq t \leq n$ に対して、

$$X_t := \{x \in X : \mathrm{w}t(x) = t\}$$

とする。X 上の関係達 R_i $(0 \leq i \leq n)$ を

$$R_i = \{(x, y) \in X \times X : \partial(x, y) = i\}$$

で定義すると、$(X, \{R_i\}_{i=0}^n)$ は 対称アソシエーションスキーム、さらには $P-$ and $Q-$ 多項式アソシエーションスキームになることが知られており、**Hamming アソシエーションスキーム（または単に Hamming スキーム）**と呼ばれる。$P-$ and $Q-$ 多項式アソシエーションスキーム、及び Hamming スキームについての詳しい解説については [5, 9, 12, 4] 等を参照のこと。

以下、F の代数構造として、(I) 素数冪でない q に対しては、$F = \mathbb{Z}_q$ を考え、 (II) q が素数冪 $q = p^r$ (p は素数) の場合には、$F = \mathrm{GF}(q)$ を考えるとするとする。ここで、$\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z} = \{0, 1, \ldots, q-1\}$ は有理整数環 $\mathbb{Z}$ のイデアル $q\mathbb{Z}$ による剰余環を表し、$\mathrm{GF}(q)$ は位数 q の有限体を表すとする。

$X = F^n$ の指標群を $Y = X^*$ とする。この時、X と Y は同型で、Y の元は X の元を用いて、次のように表されることが知られている。(I), (II) の場合で、指標 χ_y $(y \in X)$ の表記を使い分ける。

(I) の場合： $F = \mathbb{Z}_q$ とする。$\zeta = \zeta_q = \exp\left(\dfrac{2\pi i}{q}\right)$ とし、$y = (y_1, \cdots, y_n) \in X$ に対して、指標 $\chi_y \in Y$ を、$x = (x_1, \cdots, x_n) \in X$ での値が

$$\chi_y(x) = \zeta^{x \cdot y} = \zeta^{x_1 y_1 + \cdots + x_n y_n}$$

であるとして定める。

(II) の場合： $q = p^r$ (p は素数) とし、$F = \mathrm{GF}(q)$ とする。また、$\mathrm{GF}(p) = \mathbb{Z}_p$ とみなし、拡大 $\mathrm{GF}(q)/\mathrm{GF}(p)$ のトレース T を準備する。すなわち、$T = T_{\mathrm{GF}(q)/\mathrm{GF}(p)} : \mathrm{GF}(q) \to \mathrm{GF}(p)$ で、$T(x) = x + x^p + x^{p^2} + \cdots + x^{p^{r-1}}$ と計算される。$\zeta = \zeta_p = \exp\left(\dfrac{2\pi i}{p}\right)$ とし、$y = (y_1, \cdots, y_n) \in X$ に対して、指標 $\chi_y \in Y$ を、$x = (x_1, \cdots, x_n) \in X$ での値が

$$\chi_y(x) = \zeta^{T(x \cdot y)} = \zeta^{T(x_1 y_1 + \cdots + x_n y_n)}$$

であるとして定める。この場合にも、$x \cdot y = x_1 y_1 + \cdots + x_n y_n$ は標準内積とする。

(I), (II) のどちらの場合においても、y が X 全体を動く時、χ_y は指標群 Y 全体を動く。χ_y は $\chi_y(x)$ を x 成分として持つ $\mathbb{C}^X$ の元と見ることができ、以下その様にみなす。$\mathbb{C}^X$ はエルミート標準内積を持っており、その内積で, $x \neq y \in X$ に対して、χ_x, χ_y は直交している（指標の直交関係）。この時、$0 \leq j \leq n$ に対して、$W_j = \langle \chi_y : y \in X_j \rangle \subset \mathbb{C}^X$ とすると、$\{W_j\}$ 達は $\{A_i\}$ 達の極大な共通固有空間になることが知られている。χ_y 達は直交しているので、$\left\{ \dfrac{1}{\sqrt{|X|}} \chi_y : y \in X_j \right\}$ は W_j の正規直交基底になる (Banai-Ito[5, 3.2 節], Terras[19, 3 章 Theorem 2 及び page 89] を参照のこと)。

Hamming スキームの第 1 固有行列、第 2 固有行列は Krawtchouk 多項式の言葉で次のように書けることが知られている。すなわち、Krawtchouk 多項式

$$K_k(u) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{u}{j} \binom{n-u}{k-j}$$

に対して、$P_j(i) = Q_j(i) = K_j(i)$ となる。ここで、$\{A_i\}$, $\{E_j\}$ は上記の様に Hamming 距離及び χ_y ($\mathrm{wt}(y) = j$) で、順序付けられている。勿論、固有行列が上記の様に書けることは、(I)、(II) どちらの場合にも成り立つ。

注意 1. F にどのような加法群の構造を入れても、隣接行列 A_i ($i = 0, 1, \cdots, n$) (隣接行列の定義は群構造とは無関係であることに注意せよ) の極大共通固有空間 W_j ($j = 0, 1, \cdots, n$) は、有限加法群の双対性によって、加法群の単位元 0 と異なる座標の数で添え字付けられて与えられる。そのように添え字付けられた順序に対して、定義 1.1 による T-design であるという構造は加法群の構造の入れ方に依存しない。

$m \in \mathbb{N}$ に対して、$\Phi_m(s) = \prod_\eta (s - \eta)$ を円の m 分多項式とする。ここで、積 $\prod_\eta$ は 1 の原始 m 乗根 η 全体を動くものとする。次の定理は Hamming スキーム上における調和指数 t-design の構造の特徴付けを与えている。

次は本研究の一つ目の主定理である。

定理 1. 次が成り立つ。
(i) (I) の場合を考える。すなわち、$F = \mathbb{Z}_q$、$X = \mathbb{Z}_q^n$ とする。C を X の空でない部分集合とする。$y \in X$、$0 \leq i \leq q-1$ に対して、

$$c_i(y) = |\{x \in C : x \cdot y \equiv i \pmod{q}\}|$$

とし、$f_y(s) = \sum_{i=0}^{q-1} c_i(y)s^i$ と置く。この時、C が調和指数 t-*design* である必要十分条件は、任意の $y \in X_t$ に対して、$f_y(s)$ が $\Phi_q(s)$ で割り切れる事である。
(ii) (II) の場合を考える。すなわち、$q = p^r$ (p は素数)、$F = \mathrm{GF}(q)$、$X = F^n$ とする。C を X の空でない部分集合とする。$y \in X$、$i \in \mathrm{GF}(p) = \mathbb{Z}_p$ に対して、

$$c_i(y) = |\{x \in C : T(x \cdot y) = i\}|$$

とする。この時、C が調和指数 t-*design* である必要十分条件は、任意の $y \in X_t$ に対して、

$$c_0(y) = c_1(y) = \cdots = c_{p-1}(y) = \frac{|C|}{p} \tag{1}$$

が成り立つことである。

定理 1 は Hamming スキームの部分集合が調和指数 t-design である為の同値条件を指標群の言葉で与えている次の補題を適用することによって示される。

補題 1.1. X の空でない部分集合 C が調和指数 t-*design* である為の必要十分条件は、任意の $y \in X_t$ に対して、

$$\sum_{x \in C} \chi_y(x) = 0 \tag{2}$$

が成り立つことである。

定理 1 より、次の系を得る。直交配列でも同様の条件が成り立っていたことに注意する。

系 1.1. $q = p^r$ (p は素数）とし、$F = \mathrm{GF}(q)$、$X = F^n$ とする。この時、$C \subset X$ が調和指数 t-*design* であるならば、$|C|$ は p で割り切れる。

[6] の Theorem 1.1 で、1 次元低い球面上の球面 t-design を用いた、調和指数 t-design の構成法が与えられている。次に与えられる二つ目の主定理はその構成法の Hamming スキーム上における類似になっており、調和指数 t-design の一般的構成法を与える。

定理 2. i を自然数とし、$C \subset F^n$ を $\{t, t-1, t-2, \cdots, t-i\} - design$ とする。$C' \subset F^{n+i}$ を

$$C' = \{(0, \cdots, 0, x) : x \in C\}$$

と定める。この時、C' は調和指数 t-*design* である。

次の三つ目の主定理は調和指数 t-design に対する Fisher 型下界を与える。$m_t = Q_t(0) = K_t(0) = \dim W_t = \mathrm{rank} E_t = \binom{n}{t}(q-1)^t$ とする。

定理 3. C を *Hamming* スキーム $X = F^n$ 上の調和指数 t-*design* とする。$C_{n,t} := -\min\{K_t(1), K_t(2), \ldots, K_t(n)\}$ とする。この時、次の不等式が成り立つ。

$$|C| \geq \frac{1}{C_{n,t}}(C_{n,t} + m_t) =: B_{n,t} \tag{3}$$

また、(3) において等号成立する為の必要十分条件は、任意の $(x, y) \in C^2$ $(x \neq y)$ に対して、$C_{n,t} = -K_t(\partial(x, y))$ が成り立つことである。

注意 2. F^n の部分集合 C が逆に、任意の $(x,y) \in C^2$ $(x \neq y)$ に対して、$C_{n,t} = -K_t(\partial(x,y))$ であり、かつ定理 3 の等号成立条件を満たすならば、C は 調和指数 t-design になることが示せる。定理 3 において、等号が成立するとき、C を **tight 調和指数 t-design** と呼ぶ。

調和指数 t-design に対する Fisher 型下界は Zhu et al.[20] により、すでに与えられているが、定理 3 は [20] で与えられているものと少し異なっている。[20] では、上記の $C_{n,t}$ に対応するものは多項式 $K_t(s)$ の定義域 $\mathbb{R}$ における最小値のマイナス倍として定義されているが、上の定理 3 では $C_{n,t}$ は $K_t(s)$ の有限点集合 $\{1,\ldots,n\}$ 上での最小値のマイナス倍として定義されており、[20] のものよりもいつも小さい。従って、我々の与えた不等式は [20] のものを改善している。さらに、[20] では、$K_t(s)$ の定義域 $\mathbb{R}$ における最小値を考えた為、t が偶数の時にしか、議論できなかったが、定理 3 では有限集合上での最小値を考えているので、t が奇数の場合でも議論することができる。Zhu et al.[20] はいくつかの調和指数に対して、binary Hamming スキーム上 の tight 調和指数 t-design の存在問題を議論している。本報告では上記の改善された Fisher 型下界を用いた tight 調和指数の定義を用いて、その存在問題を再考する。

2 Delsarte の線形計画限界式と定理 3 の関係

Delsarte[9] は対称アソシエーションスキーム上の T-design に対して、線形計画法による下界 (線形限界式) を与えている。オリジナルの論文 [9] では、この線形限界式は第一固有行列を使った形で与えられているが、その下界は次の線形計画問題の最適値によって与えられることがすぐに解る ([7])。

$$
\begin{aligned}
\min \quad & \sum_{i=0}^{n} a_i, \\
\text{subject to} \quad & a_0 = 1, \\
& a_i \geq 0 \quad i \in \{1,\ldots,n\}, \\
& \sum_{i=0}^{n} a_i Q_j(i) \geq 0 \quad j \in \{1,\ldots n\} \setminus T, \\
& \sum_{i=0}^{n} a_i Q_j(i) = 0 \quad j \in T.
\end{aligned}
\qquad
\begin{aligned}
\max \quad & \sum_{j=0}^{n} b_j Q_j(0), \\
\text{subject to} \quad & b_0 = 1, \\
& b_j \leq 0 \quad j \in \{1,\ldots,n\} \setminus T, \\
& \sum_{j=0}^{n} b_j Q_j(i) \geq 0 \quad i \in \{1,\ldots,n\}.
\end{aligned}
$$

左右の問題は互いに双対の問題となっている。特に 調和指数 t-design の場合は $T = \{t\}$

であるので、右の問題は

$$\begin{aligned} \max \quad & \sum_{j=0}^{n} b_j Q_j(0), \\ \text{subject to} \quad & b_0 = 1, \\ & b_j \le 0 \quad j \in \{1,\dots,n\} \setminus \{t\}, \\ & \sum_{j=0}^{n} b_j Q_j(i) \ge 0 \quad i \in \{1,\dots,n\}. \end{aligned}$$

となる。Hamming スキームの場合、$Q_j(i) = K_j(i)$ であるので、$L(x) = 1 + b_t K_t(x)$ とすると、全ての $i \in \{1,\dots,n\}$ に対して、$L(i) = 1 + b_t K_t(i) \ge 0$ を満たし、$L(0) = 1 + b_t K_t(0)$ を最大にするものを探す問題（すなわち、この最大値が $B_{n,t}$ である）は、上記の線形計画問題の適解で、 $j = t$ 以外で $b_j = 0$ であるものの中での $L(0) = 1 + b_t K_t(0)$ を最大にするものを探す問題と同値である。従って、もし dual degree が $n-1$ なる X の部分集合 C（即ち 調和指数 t-design であるが、$i \neq t$ なる i に対しては 調和指数 i-design でないもの。dual degree の正確な定義は [12] を参照のこと。) で Delsarte の線形計画限界式において等号を満たすものが存在すれば、、Fisher 型不等式の定理 3 と Delsarte による線形計画限界式は一致する。また 定理 3 より Delsarte の線形計画限界式の方がいつもよい下界を与えることがわかる。

3 いくつかの計算結果と tight 調和指数 t-design の存在問題

次に、Hamming スキームにおいて、定理 3 で与えられた Fisher 型下界 $B_{n,t}$ をパラメータを動かしながら実際に計算した結果を述べ、いくつかの場合には tight design の存在性を議論する。

3.1 調和指数 1-design

$t = 1$ の場合、調和指数 1-design は勿論 1-design と一致するので、それは strength 1 の orthogonal array と同値である。定理 3 で与えられた $B_{n,1}$ は、$K_1(u) = (q-1)n - qu$ であるので、$C_{n,1} = n$ であり、$B_{n,t} = q$ となる。従って、F^n 上の tight 調和指数 1-design は列に F の q 個の元達の順列を並べたものを、n 列並べた $q \times n$ 行列の行ベクトル達となる。

3.2 調和指数 2-design

(I) $q = 2$ の場合

この時、$F = \mathbb{Z}_2 = \{0, 1\}$、$K_2(u) = 2\left(u - \frac{n}{2}\right)^2 - \frac{n}{2} = 2u^2 - 2nu + \frac{n^2}{2} - \frac{n}{2}$ である。この場合、tight 調和指数 design は次の様に特徴づけられる。n が偶数の場合はすでに Zhu[20] によって示されている。

命題 3.1. $\mathbb{Z}_2^n$ 上の *tight* 調和指数 2-*design* は次の様に特徴付けられる。

(i) n が偶数の時、位数 n の *Hadamard* 行列と同値である。

(ii) $n \equiv 3 \pmod 4$ の時、位数 $n+1$ の *Hadamard* 行列と同値である。

(iii) $n \equiv 1 \pmod 4$ の時、存在しない。

(II) $q = 3$ の場合

このとき、F=$\mathbb{Z}_3$、$2K_2(u) = 9\left(u - \frac{4n-1}{6}\right)^2 - \frac{8n+1}{4}$ であり、次の命題が成り立つ。

命題 3.2. $\mathbb{Z}_3^n$ 上の *tight* 調和指数 2-*design* が存在するならば、$n \equiv 1,\ 2 \pmod 3$ でなければならない。さらに、$n \equiv 1 \pmod 3$ の場合、$B_{n,2} = 2n + 1$、$n \equiv 2 \pmod 3$ の場合、$B_{n,2} = 2n - 1$ である。

(III) $q = 4$ の場合

このとき、$F = \mathrm{GF}(4)$、$2K_2(u) = 4\left(u - \frac{3n-1}{4}\right)^2 - 3n - 1$ であり、次の命題が成り立つ。

命題 3.3. $F = GF(4)$、$X = F^n$ とする時、X 上に *tight* 調和指数 *2-design* は存在しない。

(IV) $q = 5$ の場合

このとき、$F = \mathrm{GF}(5)$、$2K_2(u) = 25\left(u - \frac{8n-3}{10}\right)^2 - \frac{16n+9}{4}$ であり、次の命題が成り立つ。

命題 3.4. $\mathbb{Z}_5^n$ 上の *tight* 調和指数 2-*design* が存在するならば、$n \equiv 1,\ 2 \pmod 5$ でなければならない。さらに、$n \equiv 1 \pmod 5$ の場合、$B_{n,2} = 4n + 1$、$n \equiv 2 \pmod 5$ の場合、$B_{n,2} = 4n - 3$ である。

(V) $q = 6$ の場合

このとき、$F = \mathrm{GF}(6)$、$2K_2(u) = 36\left(u - \frac{5n-2}{6}\right)^2 - 5n - 4$ であり、次の命題が成り立つ。

命題 3.5. $\mathbb{Z}_6^n$ 上の *tight* 調和指数 2-*design* が存在するならば、$n \equiv 0,\ 1,\ 2 \pmod 6$ でなければならない。さらに、$n \equiv 0 \pmod 6$ の場合、$B_{n,2} = 5n - 4$、$n \equiv 1 \pmod 6$ の場合、$B_{n,2} = 5n + 1$、$n \equiv 2 \pmod 6$ の場合、$B_{n,2} = 5n - 4$ である。

一般には次の様に、n を固定し、q を大きくしていった時の tight 調和指数 2-design の非存在が言える。

定理 4. $|F| = q$ とする。q が n に比べて十分大きいとき、*Hamming* スキーム $X = F^n$ 上に *tight* 調和指数 *2-design* は存在しない。

証明は q が n に比べて十分大きいとき、$B_{n,t}$ が整数にならないことを示すことによりなされる。

3.3 調和指数 3-design

$t = 3$ の場合、調和指数 2-design の場合と同様にして、次の定理が示せる。

定理 5. $|F| = q$ とする。q が n に比べて十分大きいとき、*Hamming* スキーム $X = F^n$ 上に *tight* 調和指数 *3-design* は存在しない。

3.4 調和指数 n-design

通常の n-design はすべての点を取らないといけないが、調和指数 n-design の場合は次のようになる。

定理 6.

$$C = \{(0, \cdots, 0, c) \in F^n : c \in F\}$$

は *tight* 調和指数 *n-design* である。

4 付録

最後に、$3 \leq t \leq 5$、$2 \leq q \leq 6$、$t + 1 \leq n \leq 10$ の範囲で、$B_{n,t}$ が整数値になり、かつ q が素数冪の時は、系 1.1 の条件を満たす場合と、その $B_{n,t}$ の値を示した表を報告しておく。

t	3	3	3	3	3	3	3	4	4	4	4	4
q	2	3	4	4	4	5	6	2	2	2	2	3
n	4 ∼ 10	4 ∼ 10	4	5	7∼ 10	9∼ 10	10	6	7∼ 8	9	10	5
$B_{n,t}$	2	9	10	16	28	65	126	4	8	10	16	6

t	4	4	4	5	5	5	5	5	5	5	5
q	3	4	5	2	3	3	4	4	5	6	6
n	7	5∼ 6	6	6∼ 10	7∼ 8	10	6	10	6∼7	6	7
$B_{n,t}$	15	16	25	2	15	33	10	82	25	26	36

参考文献

[1] Ei. Bannai, Et. Bannai and T. Ito, *Introduction to Algebraic Combinatorics*, (in Japanese) Kyoritsu, 2016.

[2] E. Bannai and T. Ito, *Algebraic Combinatorics I, Association Schemes*, Benjamin/Cummings, Menlo Park, CA, 1984.

[3] E. Bannai, T. Okuda and M. Tagami, Spherical designs of harmonic index t, *J. Approx. Theory*, **195** (2015), 1–18.

[4] A.E. Brouwer and W.H. Haemers, Assocation Schemes, In *Handbook of Combinatorics*, volume 1, Elsevier, Amsterdam, 1995.

[5] J. H. Comway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, third edition, Springer-Verlag, NewYork, 1999.

[6] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Thesis, Universite Catholique de Louvain* (1973), *Philips Res. Rep. Suppl.* **10** (1973).

[7] P. Delsarte, Association schemes and t-design in regular semilattices, *J. Comb. Theory (A)* **20** (1976), 230–243.

[8] P. Delsarte, J.M. Goethals, and J.J. Seidel, Spherical codes and designs, *Geom. Dedicata* **6** (1977), 363–388.

[9] P. Delsarte and V. I. Levenshtein, Association schemes and coding theory, *IEEE Trans. Inform. Theory* **44** (1998) (6), 2477–2504.

[10] R. Hori, On HI t-designs in Hamming scheme, (in Japanese) *Master's thesis, Kyushu Institute of Technology*, 2016.

[11] D. Stanton, t-designs in classical association schemes, *Graphs Combin.* **2** (1986)(3), 283–286.

[12] A. Terras, *Fourier Analysis on Finite Groups and Applications*, London Math. Soc., 1999.

[13] Y. Zhu, Ei. Bannai, Et. Bannai, T. Ikuta and K. Kim, Harmonic index designs in binary hamming schemes, *Graphs and Combin.*, **33** (2017)(3), 1–14.

On tight 4-designs in Hamming association schemes

須田　庄 (愛知教育大)

1 Tight 4-designs in Hamming association schemes

デザイン理論において、位数が最小である tight デザインの分類は最も基本的な問題である。デザイン理論は一般に Q-多項式アソシエーションスキームや実球面において Delsarte 等により統一的な定式化の下で研究されてきた [3, 4]。Q-多項式アソシエーションスキームの重要な例であるハミングアソシエーションスキーム $H(n,q)$ のデザインは、古くから知られている直交配列と等価であることが Delsarte により示されている。野田 [8] は 1979 年に Delsarte 理論を用いて、$H(n,q)$ の tight 4-デザインについて以下の結果を得た。

定理 1. C をハミングアソシエーションスキーム $H(n,q)$ の *tight* 4-デザインとしたとき、次のいずれかが成り立つ。

1. $(|C|,n,q)=(16,5,2)$ かつ C は長さが 5 の二元体上の反復符号の双対符号、
2. $(|C|,n,q)=(243,11,3)$ かつ C は長さが 11 の三元体上のゴレイ符号の双対符号、
3. $(|C|,n,q)=(9a^2(9a^2-1)/2,(9a^2+1)/5,6)$、ただし a は次の合同式を満たす整数である：$a\equiv 21,69 \pmod{240}$.

3 のパラメータの場合については、存在性･非存在性について未解決であった。この報告集ではこの場合の非存在性の結果を紹介する。本研究は Alexander Gavrilyuk と Janoš Vidali との共同研究に基づくものであり、以下で述べる定理の証明は論文 [5] を参照されたい。

2 Association schemes

X を有限集合、$R_0,R_1,\ldots,R_D$ を $X\times X$ の空でない部分集合とし、A_i $(0\le i\le D)$ をグラフ (X,R_i) の隣接行列とする。このとき、$(X,\{R_i\}_{i=0}^D)$ が

クラスが D の（対称）アソシエーションスキームであるとは、次の条件を満たすときとする：

1. $A_0 = I_{|X|}$ (I_n はサイズが n の単位行列),
2. $\sum_{i=0}^{D} A_i = J_{|X|}$ (J_n は $n \times n$ の成分がすべて 1 の行列),
3. $A_i^\top = A_i$ $(1 \le i \le D)$,
4. 任意の i, j, k に対しある非負整数 p_{ij}^k が存在して、$A_i A_j = \sum_{k=0}^{D} p_{ij}^k A_k$ が成り立つ。

隣接行列で生成される実数体上のベクトル空間 $\mathcal{A} := \langle A_0, A_1, \ldots, A_D \rangle_{\mathbb{R}}$ は上記の条件 4 より代数となる (Bose-Mesner 代数と呼ばれる)。このとき、$\mathcal{A}$ は半単純な可換代数であるので、原始べき等元 $E_0 = \frac{1}{|X|} J_{|X|}, E_1, \ldots, E_D$ からなる $\mathcal{A}$ の基底が存在する。代数 $\mathcal{A}$ は成分ごとの積（$\circ$ と記す）についても閉じているので、クライン数 (Krein parameters) q_{ij}^k $(0 \le i, j, k \le D)$ を次で定める：$E_i \circ E_j = \frac{1}{|X|} \sum_{k=0}^{D} q_{ij}^k E_k$. ここで、クライン数は非負実数であることが知られている。集合 $\{A_0, A_1, \ldots, A_D\}$, $\{E_0, E_1, \ldots, E_D\}$ はベクトル空間 $\mathcal{A}$ の基底であるので、基底変換行列 $Q = (Q_{ij})_{i,j=0}^{D}$ を $E_i = \frac{1}{|X|} \sum_{j=0}^{D} Q_{ji} A_j$ で定める。この行列 Q を第二固有行列という。

アソシエーションスキーム $(X, \{R_i\}_{i=0}^{D})$ が Q-多項式 (Q-polynomial) であるとは、原始べき等元のある順序付け $E_1, \ldots, E_D$ が存在して、クライン数がなす行列 $L_1^* := (q_{1j}^k)_{k,j=0}^{D}$ が三重対角行列となり、対角成分の一つ上と一つ下の成分がすべて正となるときとする。$a_i^* = q_{1,i}^i$, $b_i^* = q_{1,i+1}^i$, $c_i^* = q_{1,i-1}^i$ とおいて、$\{b_0^*, b_1^*, \ldots, b_{D-1}^*; c_1^*, c_2^*, \ldots, c_D^*\}$ を Krein array という。Q-多項式アソシエーションスキームにおいて、Krein array からアソシエーションスキームのパラメータ $(p_{ij}^k, q_{ij}^k, Q = (Q_{ji})$ やここでは未定義な第一固有行列 $P = (P_{ji}))$ がすべて計算される。

例 1. $V = \{1, 2, \ldots, q\}$ $(q \ge 2)$ とし、$X = V^n$ とする。$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in X$ に対して、x, y のハミング距離 $d(x, y)$ を $x_j \ne y_j$ となる j の個数とする。$i = 0, 1, \ldots, n$ に対して $R_i = \{(x, y) \mid x, y \in X, d(x, y) = i\}$ としたとき、$(X, \{R_i\}_{i=0}^{n})$ は、第二固有行列が $Q = (K_{n,q,j}(i))_{i,j=0}^{n}$ となる Q-多項式アソシエーションスキームとなる。ここで $K_{n,q,i}(x) = \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{x}{j} \binom{n-x}{i-j}$ は *Krawtchouk polynomial* である。これをハミングアソシエーションスキームといい、$H(n, q)$ と記す。

3 Designs in Q-polynomial association schemes and orthogonal arrays

Q-多項式アソシエーションスキーム $(X, \{R_i\}_{i=0}^{D})$ の頂点集合 X の部分集合 C が t-デザイン (t-design) であるとは、C の特性ベクトル $\chi = \chi_C$ が

$\chi^\top E_i \chi = 0$ $(1 \le i \le t)$ を満たすこととする。

Q-多項式アソシエーションスキームがハミングアソシエーションスキームのとき、デザインの概念は組合せ論的に定義される直交配列と等価である。直交配列 $\mathrm{OA}(N, n, q, t)$ (orthogonal array) とは成分を $1, 2, \ldots, q$ とする $N \times n$ 行列 M であって次の性質をみたすものである：M の任意の $N \times t$ 部分行列の行ベクトルは $\{1, 2, \ldots, q\}^t$ の各要素を $\lambda := N/q^t$ 回含む。(ハミングアソシエーションスキーム $H(n, q)$ の部分集合 C に対して、C の各要素を行ベクトルとする行列を M としたとき、C が t-デザインであることとが M が直交配列 $\mathrm{OA}(|C|, n, q, t)$ であることが同値である。)

$t = 2e$ に対して、$|C|$ の下界は Rao [9] により次の通り与えられた:

$$|C| \ge \sum_{k=0}^{e} \binom{n}{k} (q-1)^k.$$

この不等式において等号が成立する直交配列（もしくはデザイン）を tight という。

“Tight デザインが存在するならば、Krawtchouk polynomial の和の多項式の零点は整数に限る”ことを示す次の定理は基本的かつ重要である。ここで、部分集合 $C \subset X$ に対して、$S(C) = \{d(x, y) \mid x, y \in X, x \ne y\}$ と定める。また、$|S(C)|$ を C の次数 (degree) という。

定理 2 ([3])**.** *C を $H(n, q)$ の tight $2e$-デザインとする。*

1. *$|S(C)| = e$ が成り立つ。*
2. *$S(C) = \{\alpha_1, \ldots, \alpha_e\}$ とする。このとき、$|C| \prod_{i=1}^{e} (1 - x/\alpha_i) = \sum_{j=0}^{e} K_{n,q,j}(x)$ が成り立つ。特に e 次の多項式 $\sum_{j=0}^{e} K_{n,q,j}(x)$ は、区間 $[1, n]$ において相異なる e 個の整数からなる零点を持つ。*

定理 2 により、以下のパラメーターの $H(n, q)$ の tight $2e$-デザインは非存在が示された。(n が明記されていない場合は、任意の n に対して非存在が示された。)

- $e = 2, q \ne 6$ [8],
- $e \ge 3, q \ge 3$ [6],
- $e = 3, q = 2$ and $e = 4, 5, 6, q = 2, n \le 10^9$ [7].

注意 1. [8] では $H(n, 6)$ の tight 4-デザインが存在するならば、合同式 $a \equiv 21, 69 \pmod{240}$ を満たす整数 a を用いて $n = (9a^2+1)/5$ となることが示されている。このとき、$\sum_{j=0}^{2} K_{(9a^2+1)/5,6,j}(x) = 9\left(4x^2 - 12a^2x + 9a^4 - a^2\right)/2$ の零点は $x = a(3a \pm 1)/2$ であり、整数 a に関する合同式からこれらは整数になる。従って、定理 2 からは $q = 6, n = (9a^2+1)/5$ の場合の tight 4-デザインの非存在は示されない。

次数が s の C に対して、$S(C)=\{\alpha_1,\dots,\alpha_s\}$, $\alpha_0=0$ とし、$S_i=\{(x,y)\in C\times C \mid d(x,y)=\alpha_i\}$ $(0\le i\le s)$ と定める。

定理 3 ([3]). C を $H(n,q)$ の t-デザインとし、次数を s とする。このとき $t\ge 2s-2$ であれば、$(C,\{S_i\}_{i=0}^s)$ はクラスが s の Q-多項式アソシエーションスキームである。

よって、tight 4-デザインからはクラスが 2 の Q-多項式アソシエーションスキーム（強正則グラフ）が得られる。

4 Main theorem

主結果は次の二つの内容

(1) $H(n,q)$ の tight 4-デザインに付随するクラスが 2 の Q-多項式アソシエーションスキームから、クラスが 4 の Q-多項式アソシエーションスキームの構成

(2) (1) で得られたクラスが 4 の Q-多項式アソシエーションスキームと同じパラメータを持つアソシエーションスキームの非存在性の結果

から従う。(1) の内容は、任意の tight 4-デザインに対して成り立つ結果である。一方、(2) の結果は、(1) の $q=6$ の場合に得られるクラスが 4 の Q-多項式アソシエーションスキームに対して得られる結果である。

4.1 Q-polynomial association schemes of class 4

C を $H(n,q)$ の tight 4-デザインとする。このとき、ある正の整数 α_1,α_2 に対して、$S(C)=\{\alpha_1,\alpha_2\}$ となる (α_i は 2 次方程式 $\sum_{i=0}^2 K_{n,q,i}(x)=0$ の解である)。

$i\in\{1,2,\dots,q\}$ に対して、C_i を次で定める：

$$C_i=\{(x_2,\dots,x_n)\mid (i,x_2,\dots,x_n)\in C\}.$$

このとき、$\tilde{C}:=\bigcup_{i=1}^q C_i$ は $H(n-1,q)$ の部分集合であり、$S(\tilde{C})=\{\alpha_1,\alpha_2,\alpha_1-1,\alpha_2-1\}$ となる。$\tilde{C}\times\tilde{C}$ の部分集合 $\tilde{S}_0,\tilde{S}_1,\dots,\tilde{S}_4$ を次で定める:$\tilde{S}_0=\{(x,y)\in\tilde{C}\times\tilde{C}\mid d(x,y)=0\}$ とし、$i\in\{1,2\}$ に対して

$$\tilde{S}_{2i-1}=\{(x,y)\in\tilde{C}\times\tilde{C}\mid d(x,y)=\alpha_i-1\},$$
$$\tilde{S}_{2i}=\{(x,y)\in\tilde{C}\times\tilde{C}\mid d(x,y)=\alpha_i\}.$$

このとき次の定理が成り立つ。

定理 4. C を $H(n,q)$ の *tight* 4-デザインとする。このとき $(\tilde{C}, \{\tilde{S}_i\}_{i=0}^4)$ はクラスが 4 の Q-多項式アソシエーションスキームであり、その *Krein array* は

$$\{(n-1)(q-1),(n-2)(q-1),2(q-1),1;1,2,(n-2)(q-1),(n-1)(q-1)\}.$$

である。

注意 2. $\tilde{C}$ は $H(n-1,q)$ の部分集合として、$t := 3$-デザインかつ次数 $s := 4$ である。$t = 2s-5$ となるので、定理 3 の仮定 "$t \geq 2s-2$" を満たさない。よって定理 4 は、従来の Delsarte 理論では導かれない結果である。

定理 4 は、各 C_i が $H(n-1,q)$ の 3-デザインであり次数が 2 であることと、さらに相異なる i,j に対して

$$|\{d(x,y) \mid x \in C_i, y \in C_j\}| = 2$$

であることを用いて、(一つの部分集合に関する) 従来の Delsarte 理論の "$t \geq 2s-2$ 型の定理 (定理 3)" を複数の部分集合に拡張することで得られる。該当する球面上の結果については [10] を参照されたい。

4.2 Non-existence for some Q-polynomial association schemes

定理 4 において、$n = (9a^2+1)/5, q = 6$ ($a \equiv 21, 69 \pmod{240}$) のときのアソシエーションスキームの非存在性について考える。$r = 3a$ とおいて、対応するパラメータを持つアソシエーションスキームに関して一般に次が成り立つ。

定理 5. $(X, \{R_i\}_{i=0}^4)$ を Q-多項式アソシエーションスキームとし、その *Krein array* を $\{r^2-4, r^2-9, 10, 1; 1, 2, r^2-9, r^2-4\}$ とする。このとき、$r = 9$ が成り立つ。

定理 5 の証明には以下の三重交差数 (triple intersection number) とその性質を用いる [2]。頂点 $u,v,w \in X$ と整数 i, j, k ($0 \leq i,j,k \leq D$) に対して、

$$\begin{bmatrix} u & v & w \\ i & j & k \end{bmatrix} := |\{x \in X \mid (u,x) \in R_i, (v,x) \in R_j, (w,x) \in R_k\}|$$

を三重交差数と呼ぶ。三重交差数とクライン数、第二固有行列の間には次の重要な関係が成り立つ。

定理 6. ([2, Theorem 3], cf. [1, Theorem 2.3.2]) $(X, \{R_i\}_{i=0}^D)$ をクラスが D の対称なアソシエーションスキームとし、その第二固有行列を Q、クライン数を q_{ij}^k ($0 \leq i,j,k \leq D$) とする。このとき、

$$q_{ij}^k = 0 \quad \Longleftrightarrow \quad \sum_{r,s,t=0}^{D} Q_{ri}Q_{sj}Q_{tk} \begin{bmatrix} u & v & w \\ r & s & t \end{bmatrix} = 0 \quad \textit{for all } u,v,w \in X.$$

が成り立つ。

定理 5 の証明の概略は以下の通りである。与えられたアソシエーションスキームは Q-多項式であるので、多数の i, j, k に対して $q_{ij}^k = 0$ となる。そのような i, j, k に対して、定理 6 から適当な三頂点に対する三重交差数に関する一次関係式が得られる。三重交差数を未知数とする連立一次方程式の解は、$r \neq 9$ の場合に非整数となる。しかしこれは三重交差数の整数性に反する。

定理 4, 5 から、定理 1 の $q = 6$ の場合の tight 4-デザインの非存在が従う。

参考文献

[1] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1989.

[2] K. Coolsaet and A. Jurišić. Using equality in the Krein conditions to prove nonexistence of certain distance-regular graphs. *J. Combin. Theory Ser. A*, 115(6):1086–1095, 2008.

[3] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.

[4] P. Delsarte, J.-M. Goethals, and J. J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, 6(3):363–388, 1977.

[5] A. Gavrilyuk, S. Suda and J. Vidali, On tight 4-designs in Hamming association schemes, to appear in *Combinatorica*.

[6] Y. Hong. On the nonexistence of nontrivial perfect e-codes and tight $2e$-designs in Hamming schemes $H(n, q)$ with $e \geq 3$ and $q \geq 3$. *Graphs Combin.*, 2(2):145–164, 1986.

[7] R. Mukerjee and S. Kageyama. On existence of two symbol complete orthogonal arrays. *J. Combin. Theory Ser. A*, 66(1):176–181, 1994.

[8] R. Noda. On orthogonal arrays of strength 4 achieving Rao's bound. *J. London Math. Soc. (2)*, 19(3):385–390, 1979.

[9] R. C. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *Suppl. J. Roy. Statist. Soc.*, 9:128–139, 1947.

[10] S. Suda. Coherent configurations and triply regular association schemes obtained from spherical designs. *J. Combin. Theory Ser. A*, 117(8):1178–1194, 2010.