第 39 回代数的組合せ論シンポジウム報告集

2023 年 6 月 19 日 − 21 日
於　新小倉会議室　６号会議室

まえがき

この報告集は 2023 年 6 月 19 日から 21 日にわたり、新小倉会議室およびオンラインのハイブリッド形式で行われた「第 39 回代数的組合せ論シンポジウム」の講演記録です。研究集会には約 70 名（内現地参加約 40 名）の参加がありました。講演者の皆様をはじめ、ご参加いただいた皆様、この集会の開催にご協力いただいた皆様に深く感謝いたします。

本研究集会は次の援助を受けて開催されました。

基盤研究（C）研究代表者：栗原大武（課題番号：JP20K03623）
基盤研究（C）研究代表者：田上真　（課題番号：JP19K03425）

世話人（50 音順）：　栗原 大武　（山口大学）
島倉 裕樹　（福岡大学）
田上 真　（九州工業大学）
中空 大幸　（岡山県立大学）
宗政 昭弘　（東北大学）

第 39 回代数的組合せ論シンポジウム

標記の研究集会を下記の要領で開催しますので，ご案内申し上げます。

世話人： 栗原 大武 （山口大学）
島倉 裕樹 （福岡大学）
田上 真 （九州工業大学）
中空 大幸 （岡山県立大学）
宗政 昭弘 （東北大学）

日程：2023 年 6 月 19 日 (月) ～21 日 (水)
会場：新小倉会議室 6 号会議室（福岡県北九州市小倉北区米町 2 丁目 2 番 1 号 新小倉ビル）

プログラム

6 月 19 日 (月)

12:45–13:25 飯寄 信保（山口大学），澤辺 正人（国士舘大学）
有限群の部分群束の被覆について

13:40–14:20 山内 博（東京女子大学）
松尾代数から生成される頂点代数

14:35–15:15 井上 浩一（群馬パース大学）
An alternative construction of the Hermitian unital 2-$(28, 4, 1)$ design

15:45–16:25 石川 麗菜（早稲田大学）
符号の Jacobi 多項式とその組み合わせデザインへの応用

16:40–17:20 宗政 昭弘（東北大学）
Jacobi polynomials and harmonic weight enumerators of the first-order Reed-Muller codes and the extended Hamming codes

6 月 20 日 (火)

9:30–10:10 石塚 慶太（東北大学）
Construction and Characterization of LCD Codes

10:25–11:05 中田 彬文（広島大学）
The Delsarte theory for probability measures on compact homogeneous spaces

11:20–12:00 奥田 隆幸（広島大学）
等質空間上の固有な群作用と符号理論の関係について

13:30–14:10 藪奥 哲史（北九州工業高等専門学校）
The number of connected bipartite graphs with given Betti numbers: its asymptotic behavior and generating functions

14:25–15:05 吉野 聖人（広島工業大学）
Equiangular lines with common angle $\arccos\frac{1}{3}$

15:35–16:15 城本 啓介（熊本大学）
Rank-Metric Codes and Matroids

16:30–17:10 田邊 顕一朗（東京都市大学）
頂点代数上の加群のシュアー・ワイル型双対性

6 月 21 日 (水)

9:30–10:10 佐竹 翔平（熊本大学）
Explicit constructions of regular expander graphs of general degree and their applications

10:25–11:05 三枝崎 剛（早稲田大学）
拡大平方剰余符号から得られる 3-デザインについて

11:20–12:00 大浦 学（金沢大学）
符号の重み多項式に関する話題

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 (C) 20K03623 「グラフ構造を通じて見る対称空間の研究」（代表者：栗原 大武）
- 科研費基盤研究 (C) 19K03425 「代数的組合せ論的デザイン理論の総合的研究」（代表者：田上 真）

本研究集会に関する情報のページ：
会期前に生じた予定の変更・情報の更新などの連絡は下記ページに掲載いたします。
`https://sites.google.com/view/2023-symposium-algcombin`

目　次

有限群の部分群束と群の構造

飯寄信保（山口大学），澤辺正人（国士舘大学）

1　準備

以下，G を有限群，$\pi(G)$ を群 G の位数を割り切る素数の全体とする。$\pi(G)$ の部分集合 π に対し，
$\mathrm{Sgp}_\pi(G)$ を G の π-部分群全体，
$\mathcal{N}_\pi(G)$ を G の冪零 π-部分群全体，
$e||G|$ に対し，$\mathcal{N}_e(G) = \{H \in \mathcal{N}_{\pi(G)}(G) | \exp(H)|e\}$,
$Ab_\pi(G)$ を G の可換 π-部分群全体，
$\mathcal{A}_\pi$ を G の π-可換部分群でその exponent が $\Pi_{p\in\pi}p$ を割り切るもの全体,
$\mathcal{L}_\pi(G) = \{L \in \mathcal{N}_\pi | O_\pi Z N_G(L) \leq L\}$
とする。これらの部分群の族は含有関係によりポセットとみなし，また，それに付随する単体的複体と考え, それらも同じ記号を用いて表すものとする。このとき，$\mathcal{N}_\pi(G), Ab_\pi(G)$ 及び $\mathcal{L}_\pi(G)$ はホモトピー同値である [3]。また，これらのホモロジー群の基本的な扱いは [3] に記載されている。本稿の目的は，これらの単体的複体の構造から群 G の構造について何が言えるかということを明らかにすることである。

2　指標環と $\mathrm{Sgp}_\pi(G)$ 等の関係

筆者は群の構造と指標との関係について考察してきた。その考察において，特に次の prime graph というものは, 強力な道具であった [6]。

定義（prime graph) prime graph $\Gamma(G)$ とは，頂点集合を $\pi(G)$ とし，辺集合を $\{(p,q) | p \neq q, \exists g \in G\ s.t.\ pq|o(g)\}$ でる無向グラフである。

偶数位数の群 G の prime graph が非連結な場合，2 を含まない連結成分を π とすると，G は Hall 冪零 π-部分群をもつことが知られており，また，G においては π に含まれる素数たちは同一のような振る舞いをすることが観察されている。この Hall 冪零 π-部分群は例外指標と密接に関係している。群指標と prime graph の関係は，prime graph が非連結な場合に特殊な sharp 指標が存在することが知られている。この視点から考察すると G の指標環 $\mathbf{Z}[\mathrm{Irr}(G)]$ をイデアル $\mathbf{Z}\cdot 1^G$ で割ってできる $\mathbf{Z}$-加群は，π と π' に対応する部分加群の直和になることが得られる。ブラウアーの通常指標に関する定理を踏まえると，これらの議論において $\mathcal{N}_{\pi(G)}(G)$ が重要であることは容易に理解できると思う。ブラウアーの理論を踏まえ，部分群の束 $\mathcal{N}_{\pi(G)}(G)$ と指標環を結び付ける道具として我々は，クイバの表現を用いている。$\mathrm{Sgp}_\pi(G)$ を点集合,（異なる）2 元 $H, K \in \mathrm{Sgp}_\pi(G)$ が $H < K$ のときこれを矢（$K \to H$) と考えることにより，$\mathrm{Sgp}_\pi(G)$ をクイバとみなすことができる。更に，各 $H \in \mathrm{Sgp}_\pi(G)$ に指標環 $\mathbf{Z}[\mathrm{Irr}(H)]$ を，$K \to H$ に制限写像 $\mathrm{res}^K_H : \mathbf{Z}[\mathrm{Irr}(K)] \to \mathbf{Z}[\mathrm{Irr}(H)]$ を対応させることで $\mathrm{Sgp}_\pi(G)$ の表現を得ることができる。（その他の部分群束については，このクイバの部分構造と考え，表現もその部分構造へ制限したものを考える。）指標環の代わりに p-ブラウアー指標の為す環（これは $\mathbf{Z}[\mathrm{Irr}(H)]$ の各要素の定義域を $G_{p'}$ へ制限し

たもの全体 $\mathbf{Z}[\mathrm{Irr}(H)]|_{G_{p'}}$ と一致する）を対応させることにより新たな表現ができる。このような表現を用いることで，部分群の指標の G への誘導指標を立体的に観察することができるであろうし，各表現の間の morphism を考えれば，Cartan 行列およびその一般化を得ることができる。この一般化された Cartan 行列は，異なる 2 つの素数に関するブラウアー指標間の関係を記述するものである [5]。本稿においては，$\mathcal{N}_{\pi(G)}(G)$ の幾何的構造と G の構造について考えることにする。

3 $\mathcal{N}_\pi(G)$ の被覆

$\mathcal{N}_\pi(G)$ の構造を調べる際に，都合の良い部分構造を考えそれらのデータを基に考察することは極普通なことだと思う。ここでは次のような部分構造への分解を考えたい。

$$\mathcal{N}_\pi(G) = \cup_{\lambda\in\Lambda}\mathcal{N}_\pi(A_\lambda) \quad (\text{ここで，} A_\lambda \text{ は } G \text{ の部分群})$$

本稿において，上の和集合においてどの一つの $\mathcal{N}_\pi(A_\lambda)$ が欠けても等号が成立しない場合，既約であると呼ぶことにする。

ここで，A_λ 達をどのように選ぶかが問題となる。単純に考えると極大部分群の中から選ぶという方法が思いつくのであるが，多くの場合で極大部分群を決定することは困難であることが多い。また個々の $\mathcal{N}_\pi(A_\lambda)$ の構造も一般に計算するのが難しいと考えられる。それゆえ形式的・抽象的な議論する場合以外には適切でないと考えられる。

我々の目的を踏まえ，指標環との関係から次のような $\mathcal{N}_\pi(G)$ の分解を考えている。

$$\mathcal{N}_\pi(G) = \cup_{\lambda\in\Lambda}\mathcal{N}_\pi(C_G(x_\lambda)) \quad (\text{ここで，} x_\lambda \in G_\pi)$$

この $\{\mathcal{N}_\pi(C_G(x_\lambda))\}_{\lambda\in\Lambda}$ を $\mathcal{N}_\pi(G)$ の被覆と呼ぶことにし，$\mathcal{N}_\pi(G)$ の被覆 $\{\mathcal{N}_\pi(C_G(x_\lambda))\}_{\lambda\in\Lambda}$ 達の中の $|\Lambda|$ の最小値を $l(\mathcal{N}_\pi(G))$ で表すこととする。この被覆において各 $\mathcal{N}_\pi(C_G(x_\lambda))$ は可縮であるから，その意味で単純な構造を持っていることがわかる。冒頭に記載されている部分群の束についても同様に被覆が定義される。$\mathcal{N}_\pi(G)$ の被覆 $\{\mathcal{N}_\pi(C_G(x_\lambda))\}_{\lambda\in\Lambda}$ の各ピースを $\langle x_\lambda|\lambda\in\Lambda\rangle$ に制限してできる $\langle x_\lambda|\lambda\in\Lambda\rangle$ の被覆 $\{\mathcal{N}_\pi(C_{\langle x_\lambda|\lambda\in\Lambda\rangle}(x_\mu))\}_{\mu\in\Lambda}$ の各ピースも可縮になっていることから次の問いが浮かんでくる。

Quiz　$\mathcal{N}_\pi(G)$ と $\mathcal{N}_\pi(\langle x_\lambda|\lambda\in\Lambda\rangle)$ の幾何的構造に関してどのような関係があるか。

上の問に対して，次がわかっている。

定理　$\langle x_\lambda|\lambda\in\Lambda\rangle$ が冪零であれば，$\mathcal{N}_\pi(G)$ と $\mathcal{N}_\pi(\langle x_\lambda|\lambda\in\Lambda\rangle)$ はホモトピー同値である。よって，この場合 $\mathcal{N}_\pi(G)$ は可縮である。

恐らく G が単純群の場合，上の定理と同様なことが成り立つと予想される。

4 $l(\mathcal{N}_e(G))$ と G の関係

$l(\mathcal{N}_e(G))$ と G の関係を考えることは，極普通なことであろう。しかし，$\mathcal{N}_e(G)$ の力の及ばない範囲を考えるのは，ほぼ無意味と思われるので $l(\mathcal{N}_e(G))$ と $O^{\pi(e)'}(G)$（$O^{\pi(e)'}(G)$ は $[G:N]$ と e が互いに外なるような正規部分群 N で位数が最小のもの）或いは，

$$Y_e(G) := \langle x\in G|\ o(x)|e\rangle$$

との関係を調べる方が適当だと思われる。例えば，次の事実は，明らかに成立つ。

$$l(\mathcal{N}_e(G)) = 1 \iff (|Z(O^{\pi(e)'}(G))|,\ e) \neq 1$$

$l(\mathcal{N}_e(G)) = 1$ 以外の場合では次の Quiz が考えられる。

Quiz　$2 \leq l(\mathcal{N}_e(G)) \leq 4$ ならば，$O^{\pi(e)'}(G)$ は可解であるか。

5　$l(\mathcal{N}_e(G)) = 2$ の場合

この節では，$l(\mathcal{N}_e(G)) = 2$ の場合を考察する。即ち，次の既約な被覆がある場合を考える。

$$\mathcal{N}_e(G) = \mathcal{N}_e(C_G(s)) \cup \mathcal{N}_e(C_G(t))$$

但し，$s, t \in G$ であり $o(s) = p, o(t) = q \in \pi(e)$ とする。この条件は、かなり強い条件なので伝統的な群論の手法を用いれば解決できると思うが，ここでは「束」,「poset]，或は「単体的複体」の中でできるだけ考えたい。

補題　**A**　$[s, t] \neq 1$ とする。このとき，次が成り立つ。
$[s^g, s^h] = 1\ (\forall g, h \in C_G(t))$ 及び，$[t^k, t^l] = 1\ (\forall k, l \in C_G(s))$

証明は次のとおりである。ある $g, h \in C_G(t)$ に対して，$[\langle s^g \rangle, \langle s^h \rangle] \neq 1$ とすれば $[\langle s \rangle, \langle s^{hg^{-1}} \rangle] \neq 1$ となるので，$\langle s^{hg^{-1}} \rangle \notin \mathcal{N}_e(C_G(s))$。故に，$\langle s^{hg^{-1}} \rangle \in \mathcal{N}_e(C_G(t))$ を得るが, これは $[s, t] = 1$ を意味するので矛盾である。

この補題から群論色の議論を多少行うと次が直ちに得られる。

命題　**B**　素数 p について $\mathcal{N}_p(G) = \mathcal{N}_p(C_G(s)) \cup \mathcal{N}_p(C_G(t))$ かつ $[s, t] \neq 1$ であれば，$p = 2$ であり $\langle s, t \rangle \simeq D_8$ である。

前章の定理を用いると次を得る。

系　　$l(\mathcal{N}_p(G)) = 2$ ならば，$\mathcal{N}_p(G)$ は可縮である。

補題 A の証明でも明らかなように次にあげる集合は重要である。

$$\mathcal{S} = \{x \in G | [s, s^x] \neq 1\} \text{ 及び，} \quad \mathcal{T} = \{y \in G | [t, t^y] \neq 1\}$$

なぜならば，補題 A の証明方法を用いると $x \in \mathcal{S}$ ならば

$$x^* : \mathcal{N}_e(C_G(s)) \to \mathcal{N}_e(C_G(t))\ (X \in \mathcal{N}_e(C_G(s)) \mapsto X^x)$$

なる単射 poset map を得ることができるからである。実際，$X \in \mathcal{N}_e(C_G(s))$ ならば $\langle s, X \rangle \in \mathcal{N}_e(C_G(s))$ であり，$\langle s^x, X \rangle^x \notin \mathcal{N}_e(C_G(s))$ となるから $\langle s^x, X \rangle^x \in \mathcal{N}_e(C_G(t))$。よって $X^x \in \mathcal{N}_e(C_G(t))$ となる。

これと似たような議論をすると「もし $[s, t] = 1$ であるならば，$\mathcal{S} \cap \mathcal{T} = \emptyset$」も得られる。

また, $\mathcal{S}=\emptyset$ であるならば，$O_p(G)\neq 1$, 及び，$\mathcal{T}=\emptyset$ であるならば，$O_q(G)\neq 1$ が成り立つことも容易にわかる。

補題　C　$\mathcal{S}\neq\emptyset$ かつ $\mathcal{T}\neq\emptyset$ とする。このとき

$$H=\mathcal{ST}\cup\mathcal{STST}\cup\mathcal{STSTST}\cup\cdots$$

は明らかに G の部分群であり，$H=C_G(s)HC_G(t)$ を満たす。特に $\mathcal{N}_e(G)=\mathcal{N}_e(H)$。

補題 C を用いてほのかに Qillen 予想の香りのする次の主張を得る。

定理

$$F(G)\cap O_{\{p,q\}}(G)\neq 1.$$

（文責　飯寄）

参考文献

[1] D. Gorenstein, “Finite Groups”, Chelsea 1980, 2nd edition.

[2] B. Huppert, “Character theory of finite groups”, De Gruyter Expositions in Mathematics, **25**, Walter de Gruyter & Co., Berlin, (1998)

[3] N. Iiyori and M. Sawabe, Quiver representations of extended subgroup posets of finite groups, Hokkaido Mathematical Journal, **51** (2022), 407-443

[4] N. Iiyori and M. Sawabe, d-Covers of posets of nilpotent subgroups, preprint

[5] N. Iiyori and M. Sawabe, Partially ordered sets of non-trivial nilpotent π-subgroups II, *Topology Appl.*, **231** (2017), 197-218.

[6] N. Iiyori and H. Yamaki, On a conjecture of Frobenius, *Bull. Amer. Math. Soc.* (N.S.) **25** (1991), 413–416.

[7] J.R. Munkres, “Elements of algebraic topology”, Addison-Wesley Publishing Company, Menlo Park, CA, 1984.

[8] D. Quillen, Homotopy properties of the poset of nontrivial p-subgroups of a group, *Adv. Math.* **28** (1978), 101–128.

[9] S.D. Smith, “Subgroup complexes”, Mathematical Surveys and Monographs, **179**, American Mathematical Society, Providence, RI, 2011.

松尾代数から生成される頂点代数

東京女子大学 現代教養学部 数理科学科 山内 博

概 要

本研究は Cuipo Jiang, Ching Hung Lam 両氏との共同研究に基づくものである。そのあらましを報告する。

1 松尾代数

まず，3 互換群の定義を復習する。

定義 1.1. G を群，I を位数が 2 の元からなる G の部分集合とする。G は I で生成され，任意の $a, b \in I$ について $a^b = bab \in I$ であり，また $|ab| \leq 3$ が満たされるとき，組 (G, I) を **3 互換群**と呼ぶ。

3 互換群の概念は Fischer により導入され, 適当な仮定の下でその分類が研究された (cf. [Fi71])。対称群 $G = \mathfrak{S}_n$ とその互換のなす類 $I = \{(i\ j) \in \mathfrak{S}_n \mid 1 \leq i < j \leq n\}$ が典型的な例であり，その名もこの例から来ていると思われる。他にも以下の例が 3 互換群となることが知られている。(互換の類が明らかなものについては省略している。)

- ADE 型のワイル群，ここで 3 互換類は鏡映
- $G = \mathrm{Sp}_{2n}(2)$ で I は移換全体
- $G = \mathrm{O}^{\pm}_{2n}(2)$ で I は移換全体
- $G = \mathrm{O}^{\pm}_{2n}(3)$ で I は鏡映全体
- $G = \mathrm{U}_n(2)$ で I は移換全体
- $G = \mathrm{Fi}_{22,23,24}$，この場合 I は一意的な共役類

3 互換群 (G, I) が与えられたとき，$a, b \in I$ について，$|ab| = 3$ のとき二項関係 $a \sim b$ が成り立つものと定め，この二項関係により隣接関係を定めることにより I にはグラフの構造が入る。ここで $a \sim b$ ならば $a^b = b^a$ すなわち $bab = aba$ が成り立つ。簡便のため，$a \sim b$ のとき $a \circ b = aba$ と定める。このとき 3 互換群に付随した松尾代数は以下のように定義される。

定義 1.2 ([Ma05])**.** (G, I) を 3 互換群とする。$\alpha, \beta \in \mathbb{C}$ として，$B_{\alpha,\beta}(G) = \bigoplus_{i \in I} \mathbb{C}x^i$ に積および内積を以下のように定める。

$$x^i x^j = \begin{cases} 2x^i & (i = j) \\ \dfrac{\alpha}{2}(x^i + x^j - x^{i \circ j} & (i \sim j) \\ 0 & (\text{その他}) \end{cases} \qquad (x^i \,|\, x^j) = \begin{cases} \dfrac{\beta}{2} & (i = j) \\ \dfrac{\alpha\beta}{8} & (i \sim j) \\ 0 & (\text{その他}) \end{cases} \tag{1.1}$$

このとき $B_{\alpha,\beta}(G)$ は不変内積を持つ可換代数となる。これを (G, I) に付随した**松尾代数**と呼ぶ。

頂点代数との対応を考慮して，各生成元 x^i は $x^i x^i = 2x^i$ を満たすように積を定義しているが，このとき $x^i/2$ が冪等元となるので，松尾代数は冪等元で張られ，生成される代数である。一般には松尾代数は非結合的である。

3 互換群の定義において I は共役類とは限らなかった。I が一つの共役類となるための条件は，先述したグラフ構造を考えたとき，これが連結となることであり，それゆえ I が一つの共役類でないことと，$I = I_1 \sqcup I_2$ で $I_i \neq \varnothing$ $(i = 1, 2)$ なる非連結な部分集合に分割されることは同値である。この場合，$G_i = \langle I_i \rangle$ $(i = 1, 2)$ とおけば (G_i, I_i) は G の 3 互換部分群であり，G はこれらの中心積 $G = G_1 * G_2$ となっている。対応して，松尾代数も両側イデアルへの直和分解

$$B_{\alpha,\beta}(G) = B_{\alpha,\beta}(G_1) \oplus B_{\alpha,\beta}(G_2)$$

を持ち，さらにこの分解は内積に関する直交分解にもなっている。そのため，松尾代数の構造を考える際は，I は一つの共役類と仮定して差し支えない[1]。I が連結，すなわち一つの共役類であるとき，G を連結もしくは直既約という。また，$|I| = 1$ のとき，G および I を自明といい，そうでないとき非自明という。以下では主に非自明かつ直既約な例を考える。

G が直既約のとき，$i \in I$ に対して $k := |\{j \in I \mid j \sim i\}|$ は i に依らず一定値をとる。(これは I をグラフとみたときの次数と一致する。) もし $k\alpha + 4 \neq 0$ ならば，次の元

$$\omega = \frac{4}{k\alpha + 2} \sum_{i \in I} x^i \tag{1.2}$$

を考えると，直接計算により $\omega/2$ は $B_{\alpha,\beta}(G)$ の単位元を与えることが確認できる。また，このとき $2(\omega\,|\,\omega) = 4\beta|I|/(k\alpha + 4)$ であることも確認できる[2]。

さて，G は共役により I に作用していた。その作用は自然に $B_{\alpha,\beta}(G)$ の自己同型へと拡張される。すなわち，次の準同型が一意に定まる。

$$\begin{array}{rccc} \sigma: & G & \longrightarrow & \operatorname{Aut} B_{\alpha,\beta}(G) \\ & a & \longmapsto & \sigma_a : x^i \mapsto x^{aia^{-1}} \end{array} \tag{1.3}$$

定義から $\operatorname{Ker}\sigma = Z(G)$ であり，それゆえ G の中心が自明であれば，σ は単射となる。ここで $\alpha \neq 2$ を仮定する。すると，各 $i \in I$ について，x^i の随伴作用 $\operatorname{ad} x^i$ は 3 つの固有値 $0, 2, \alpha$ を持ち，松尾代数は次ように分解する。

$$\begin{array}{rccccc} B_{\alpha,\beta}(G) & = & \mathbb{C}x^i & \oplus & \operatorname{Ker}\operatorname{ad} x^i & \oplus & \operatorname{Ker}(\operatorname{ad} x^i - \alpha) \\ \operatorname{ad}\, x^i & : & 2 & & 0 & & \alpha \\ \sigma_i & : & 1 & & 1 & & -1 \end{array} \tag{1.4}$$

このとき，$\operatorname{ad} x^i$ による固有空間分解から，$i \in I$ の作用が復元されることが見てとれる。これは，松尾代数の場合には，3 互換群を忘れても，生成元 (冪等元) x^i の作用から，群が復元できることを意味している。次節でみるように，他の代数の部分構造として松尾代数が含まれている場合，その代数構造から自己同型群として 3 互換群の作用が自然と現れることがある。実際には，松尾代数はこのような考察を経て，導入されたものである (cf. [Mi96, Ma05])。

[1] 初めから 3 互換群の定義において I は共役類としてしまってもよいのだが，3 互換部分群を考えた場合，例えば $\mathfrak{S}_k \times \mathfrak{S}_{n-k} < \mathfrak{S}_n$ のような，必ずしも 3 互換類が共役類とは限らないものが現れるため，そうしていない。

[2] 頂点代数において ω は共形ベクトルに対応し，$2(\omega\,|\,\omega)$ の値は中心電荷に対応する。

2 グライス代数

V を OZ 型の頂点代数，すなわち $V = \oplus_{n\geq 0} V_n$, $V_0 = \mathbb{C}\mathbb{1}$, $V_1 = 0$ なる次数分解を持つ頂点代数とする。このとき次数 2 の部分空間 V_2 には以下の積[3]および内積により不変内積を持つ可換代数構造が導入される。

$$ab = a_{(1)}b, \qquad (a\,|\,b)\mathbb{1} = a_{(3)}b \qquad (a, b \in V_2) \tag{2.1}$$

これを V の**グライス代数**とよぶ[4]。以下では，主に OZ 型の頂点代数を考える。$e \in V_2$ は $L^e(n) = e_{(n+1)}$ とおくときに以下の交換関係式

$$[L^e(m), L^e(n)] = (m-n)L^e(m+n) + \delta_{m+n,0}\frac{m^3-m}{12}c_e, \qquad c_e = 2(e\,|\,e) \in \mathbb{C} \tag{2.2}$$

を満たすとき，中心電荷 c_e の**ヴィラソロ元**と呼ばれる。

補題 2.1 ([Mi96]). $e \in V_2$ がヴィラソロ元であることと，$e/2$ がグライス代数における冪等元であることは同値であり，このとき中心電荷は $c_e = 2(e\,|\,e)$ で与えられる。

この補題より，グライス代数における冪等元を考察することは頂点代数におけるヴィラソロ元を調べることと同義となり，重要となる。

定義 2.2. 中心電荷 $1/2$ のヴィラソロ元 $e \in V_2$ はそれが生成するヴィラソロ頂点部分代数が単純すなわち $\langle e\rangle \cong L(1/2, 0)$ となるとき，**イジング元**と呼ばれる。また，イジング元 $e \in V$ が V において $L(1/2, 1/16)$ と同型な部分加群を持たないとき，σ **型**と呼ばれる。

$e \in V$ が σ 型のイジング元であるならば，V を $\langle e\rangle \cong L(1/2, 0)$-加群とみたとき，$L(1/2, 0)$ および $L(1/2, 1/2)$ の直和と同型となる。それゆえゼロモード $2e_{(1)} = 2L^e(0)$ は V 上半単純であり，整数固有値を持つ。よって $(-1)^{2e_{(1)}}$ は V 上 well-defined となる。

命題 2.3 ([Mi96]). V を OZ 型の頂点代数とする。

(1) $e \in V$ を σ 型イジング元とするとき，$\sigma_e := (-1)^{2e_{(1)}} \in \operatorname{Aut} V$ である。

(2) e, f を相異なる σ 型イジング元とするとき，$(e\,|\,f) = 0$ もしくは 2^{-5} である。$(e\,|\,f) = 2^{-5}$ ならば $|\sigma_e\sigma_f| = 3$, $\sigma_e f = \sigma_f e$ であり，グライス代数において $ef = \dfrac{1}{4}(e + f - \sigma_e f)$ を満たす。また，$(e\,|\,f) = 0$ ならば $\sigma_e\sigma_f = \sigma_f\sigma_e$ で，グライス代数において $ef = 0$ となる。

(3) E_V を V における σ 型イジング元の集合とするとき，$G_V = \langle \sigma_e \mid e \in E_V\rangle$ は 3 互換群をなす。

命題 2.3 (2) より，線形包 $\mathbb{C}E_V \subset V_2$ はグライス代数において部分代数をなし，3 互換群 G_V に付随した松尾代数 $B_{1/2,1/2}(G_V)$ の準同型像となることが分かる。さらに，G_V はグライス代数のみならず，頂点代数全体の構造を保つ自己同型群を与えている。このように σ 型イジング元で生成される頂点代数には 3 互換群が自然と対応する。

[3] ここで $Y(a, z) = \sum_{n\in\mathbb{Z}} a_{(n)}z^{-n-1} \in (\operatorname{End} V)[\![z^{\pm 1}]\!]$ である。

[4] その理由は V としてムーンシャイン頂点代数 $V^\natural$ を考えた場合，最初グライスによって構成され，その後コンウェイにより再構成されたモンスター群のグライス代数が得られるからである。

3　σ 型イジング元で生成される頂点代数

次の条件を満たす頂点代数を考えよう。

条件 1. 頂点代数 V は以下を満たす。

(1) V は OZ 型である。

(2) E_V を V における σ 型イジング元の集合として，V は E_V により生成されている。

以下，V は上記の条件を満たすものとする。このとき $I_V = \{\sigma_e \mid e \in E_V\}$ として $G_V = \langle I_V \rangle$ とすれば (G_V, I_V) は 3 互換群となるのであった。もし E_V が $E_V = A \sqcup B$, $A \perp B = 0$ なる直交分割を持てば，$V = \langle A \rangle \otimes \langle B \rangle$ となり，さらに $\langle A \rangle$, $\langle B \rangle$ それぞれも条件 1 をみたす。よって以下では E_V は直既約，すなわち非自明な直交分割を持たないものとする。

命題 3.1 ([JLY19])**.** V は $\{a_{1(-n_1)} \cdots a_{k(-n_k)}\mathbb{1} \mid k \geq 0,\ a_i \in E_V,\ n_i \geq 0\}$ の線形包と一致する。

この命題から特に，V のグライス代数は $\mathbb{C}E_V$ と一致することが分かる。これと命題 2.3 を合わせることで次が従う。

命題 3.2 ([Mi96, Ma05])**.** 全射 $B_{1/2,1/2}(G_V) \twoheadrightarrow V_2 = \mathbb{C}E_V$ が存在する。特に，V が単純であれば，そのグライス代数 V_2 は $B = B_{1/2,1/2}(G_V)$ としてその非退化商 $B/\mathrm{rad}\, B$ と同型である。

条件 1 を満たす頂点代数については多くの先行研究がなされており，正定値性の仮定の下では (V ではなく) G_V の分類が完成している。

定理 3.3 ([KM01, Ma05])**.** V を条件 1 を満たす $\mathbb{R}$ 上の頂点代数とし，さらに V の不変内積は正定値とする。3 互換群 $G_V = \langle \sigma_e \mid e \in E_V \rangle$ で直既約なものは，次の群

$$\mathfrak{S}_n,\quad \mathrm{O}_6^-(2),\quad \mathrm{O}_8^-(2),\quad \mathrm{Sp}_6(2),\quad \mathrm{Sp}_8(2),\quad \mathrm{O}_8^+(2),\quad \mathrm{O}_{10}^+(2)$$

もしくはこれらの自然加群による次の拡大のいずれかに同型である。

$$F{:}\mathfrak{S}_n,\quad F^2{:}\mathfrak{S}_n,\quad \mathbb{F}_2^6{:}\mathrm{O}_6^-(2),\quad \mathbb{F}_2^6{:}\mathrm{Sp}_6(2),\quad \mathbb{F}_2^8{:}\mathrm{O}_8^+(2)$$

ここで埋め込み $\mathfrak{S}_{2n+1} < \mathrm{Sp}_{2n}(2)$ および $\mathfrak{S}_{2n+2} < \mathrm{Sp}_{2n}(2)$ により $\mathfrak{S}_n$ の自然加群 F は $\mathbb{F}_2^{2\lfloor (n-1)/2 \rfloor}$ としている。

この定理に現れる 3 互換群はカイパースとホールの分類 [CH95] において斜交型と呼ばれるものに限られている。また，上記の群を実現する頂点代数の例も知られており，R を ADE 型のルート格子として，$V_{\sqrt{2}R}^+$ の部分代数として得られている (cf. [Ma05])。

定理 3.3 は頂点代数 V ではなく，それに付随する 3 互換群 G_V の分類に関する結果であったが，V 自身については次の定理が成り立つ。

定理 3.4 ([JLY19])**.** 条件 1 を満たす頂点代数は唯一つの単純商を持つ。特に，単純であれば，頂点代数構造はそのグライス代数から一意的に定まる。

この定理の系として，定理 3.3 に現れる群 G_V を実現する V は一意であり，[Ma05] で与えられた例のみであることが分かる。さて，定理 3.4 において，我々は単純性の仮定の下で一意性を得たが，単純性自体についてもさらに考察を行い，次の結果を得た。

命題 3.5 (Jiang-Lam-Y.). V を条件 1 を満たす頂点代数とする。$G_V = \langle \sigma_e \mid e \in E_V \rangle$ が定理 3.3 に現れる以下の群と同型ならば，V は単純頂点代数となる。

$F^{\leq 2}$:$\mathfrak{S}_n$, $\mathrm{O}_6^-(2)$, $\mathbb{F}_2^6$:$\mathrm{O}_6^-(2)$, $\mathrm{O}_8^-(2)$, $\mathrm{Sp}_6(2)$, $\mathbb{F}_2^6$:$\mathrm{Sp}_6(2)$, $\mathrm{Sp}_8(2)$, $\mathrm{O}_8^+(2)$, $\mathbb{F}_2$:$\mathrm{O}_8^+(2)$, $\mathrm{O}_{10}^+(2)$

さらに，上記の結果に基づいて，F^3:$\mathfrak{S}_4$, $\mathbb{F}_2^8$:$\mathrm{Sp}_8(2)$ および $\mathrm{O}_{10}^-(2)$ は条件 1 を満たす頂点代数 V に付随する群 G_V の部分群には成りえないことが証明できる。この考察とカイパースとホールによる 3 互換群の分類結果 [CH95] を合わせることで，次の分類定理を得た。

定理 3.6 (Jiang-Lam-Y.). V を条件 1 を満たす頂点代数とし，$G_V = \langle \sigma_e \mid e \in E_V \rangle$ は直既約とする。このとき G_V は定理 3.3 に現れるものに限る。すなわち，定理 3.3 は $\mathbb{C}$ 上で考え，正定値性を課さなくてもそのまま成り立つ。

これで条件 1 を満たす頂点代数の完全な分類が得られたと考えられる。分類が完成した事自体は嬉しいのであるが，出来上がった結果だけを見てみると，元となった定理 3.3 を補強したのみで，それを超えた何か新しい例はないという結果でもあるため，この点においては少々残念なところでもあるというのが正直な印象である。

講演では，代数的組合せ論を関する集会であることから，分類結果をまとめた，下の表を最後に示して締めくくりとした。(頂点代数の記法については説明は省略している。)

V	$K(A_{n-1},2)$	$V^+_{\sqrt{2}A_{n-1}}$	$V^+_{\sqrt{2}D_n}$	$K(E_6,2)$	$V^+_{\sqrt{2}E_6}$	$K(E_7,2)$
G_V	$\mathfrak{S}_n$	F:$\mathfrak{S}_n$	F^2:$\mathfrak{S}_n$	$\mathrm{O}_6^-(2)$	2^6:$\mathrm{O}_6^-(2)$	$\mathrm{Sp}_6(2)$
$\dim V_2$	$n(n-1)/2$	$n(n-1)$	$n(3n-1)/2$	36	57	63
$\lvert I_V\rvert$	$n(n-1)/2$	$n(n-1)$	$2n(n-1)$	36	72	63
c.c.	$n(n-1)/(n+2)$	$n-1$	n	$36/7$	6	$63/10$
density	$n/2+1$	n	$2(n-1)$	7	12	10

V	$V^+_{\sqrt{2}E_7}$	$\mathrm{Com}(K(A_2,2),V^+_{\sqrt{2}E_8})$	$K(E_8,2)$	$K(E_8,2)$	$V^+_{\sqrt{2}E_8}$	$V^+_{\sqrt{2}E_8}$
G_V	2^6:$\mathrm{Sp}_6(2)$	$\mathrm{O}_8^-(2)$	$\mathrm{O}_8^+(2)$	$\mathrm{Sp}_8(2)$	2^8:$\mathrm{O}_8^+(2)$	$\mathrm{O}_{10}^+(2)$
$\dim V_2$	91	85	120	120	156	156
$\lvert I_V\rvert$	126	136	120	255	240	496
c.c.	7	$34/5$	$15/2$	$15/2$	8	8
density	18	20	16	34	30	62

この表において density なる値は $|I_V|$ を中心電荷の値で割ったものであり，ここだけの意味で設けた私の創作であって，広く受け入れられているものではない。格子に付随した頂点代数に

おいては，中心電荷は格子の階数すなわち次元と一致し，また，$|I_V|$ は無限系列においてはほぼ格子の階数の 2 乗に比例することから，この比は対称性の大きさを測る一つの尺度と思い，勝手ながら紹介させて頂いた。分類結果において例外的に対称性が大きくなっている例をよく表現していると個人的には考えている。

参考文献

[CH95] H. Cuypers and J.I. Hall, The 3-transposition groups with trivial center. *J. Algebra* **178** (1995), 149–193.

[Fi71] B. Fischer, Finite groups generated by 3-transpositions. I. *Invent. Math.* **13**, 232–246.

[JLY19] C. Jiang, C.H. Lam and H. Yamauchi, Vertex operator algebras generated by Ising vectors of σ-type. *Math. Z.* **293** (2019), 425–442.

[KM01] M. Kitazume and M. Miyamoto, 3-transposition automorphism groups of VOA. Groups and combinatorics–in memory of Michio Suzuki, 315–324, Adv. Stud. Pure Math., 32, Mathematical Society of Japan, Tokyo 2001.

[Ma05] A. Matsuo, 3-transposition groups of symplectic type and vertex operator algebras. *J. Math. Soc. Japan* **57**(3) (2005), 639–649. `arXiv:math/0311400`.

[Mi96] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras. *J. Algebra* **179** (1996), 528–548.

An alternative construction of the Hermitian unital 2-$(28, 4, 1)$ design

井上　浩一

群馬パース大学 (k-inoue@teac.paz.ac.jp)

1　まえがき

非退化な Hermite 形式をもつ $\mathbb{F}_4 := \mathbb{F}_2[\omega]$ $(\omega^2 + \omega + 1 = 0)$ 上の 3 次元ベクトル空間 V は，任意の基底 (e_1, e_2, e_3) に対して $(e_1, e_2, e_3, \omega e_1, \omega e_2, \omega e_3)$ を基底とする $\mathbb{F}_2$ 上の 6 次元ベクトル空間 V' とみなすことができるが，さらに

$$Q(x) := h(x, x), \qquad s(x, y) := h(x, y) + h(y, x) \quad (\forall x, y \in V)$$

によって定義される V' 上の 2 次形式 Q は，非退化かつ Witt 指数 2 (いわゆるマイナス型) であり，その極形式が s になる。これはユニタリ群 $U(3, 2)$ から直交群 $O^-(6, 2)$ がつくられることを意味しており，実際に $U(3, 2)$ は $O^-(6, 2)$ の極大部分群である。一方，Aut$\mathbb{F}_4$ の位数 2 の元 θ が引き起こす半線形変換 $\hat{\theta}$ と，$U(3, 2)$ が生成する群 $\Gamma U(3, 2)$ の指数 3 の部分群 $\Sigma U(3, 2)$ は，Chevalley 群 $G_2(2)$ の極大部分群である。また，2 つの群 $O^-(6, 2) : 2$ と $G_2(2)$ はともにシンプレクティック群 $Sp(6, 2)$ の極大部分群である。これらの相関図は図 1 の通りであり，—は極大部分群を，数字は指数を，$S_6(2)$ は $Sp(6, 2)$ を表す。今回，我々 [5] は $\Sigma U(3, 2)$ からつくられる $O^-(6, 2)$ を変形させて，$G_2(2)$ を構成することができた。

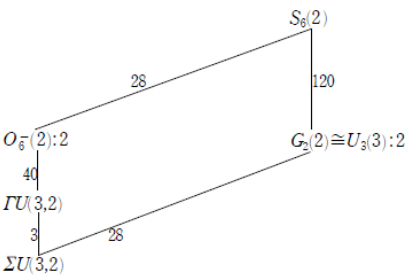


図 1　$Sp(6, 2)$ の部分群

以下，話を簡単にするために数ベクトル空間で記述するが，抽象ベクトル空間で記述することもできる (例えば，Taylor [8, Chapter 10])。また，(組合せ) デザインの定義は省くが，多くの参考

書があるので (例えば，Cameron & van Lint [2])，そちらを参照されたい。

2 Hermitian unital design

有限体 $K := \mathbb{F}_{q^2}$ (q : 素数べき) 上の 3 次元ベクトル空間 $V := K^3$ に (非退化な)Hermite 形式

$$h(x,y) := \sum_{i=1}^{3} x_i \overline{y_i} \qquad (\forall x, y \in V)$$

を定義する。ここで，$x := (x_1, x_2, x_3)$，$y := (y_1, y_2, y_3)$ であり，$\mathrm{Aut}\left(\mathbb{F}_{q^2}/\mathbb{F}_q\right)$ の (ただ 1 つの) 位数 2 の元 θ に対して $\bar{\lambda} = \lambda^\theta$ $(\forall \lambda \in \mathbb{F}_{q^2})$ とかく。$\lambda^\theta = \lambda^q$ が成り立つ。

V の 1 次元部分空間 $\langle x \rangle$，2 次元部分空間 $\langle x, y \rangle$ をそれぞれ射影平面 $PG(V)$ の点，直線とみなし，

$$[x] := \{\lambda x \mid \lambda \in K^\times\}, \qquad [x,y] := \{[y]\} \cup \{[x + \lambda y] \mid \lambda \in K\}$$

と同一視する。$[x]$ と (h に関して) 直交する点全体を $[x]^\perp$ で表す:

$$[x]^\perp := \{[z] \mid h(x,z) = 0\}$$

$PG(V)$ の isotropic point 全体を Ω，nonisotropic point 全体を $\bar{\Omega}$ で表す:

$$\Omega := \{[a] \mid h(a,a) = 0\}, \qquad \bar{\Omega} := \{[u] \mid h(u,u) \neq 0\}.$$

$|\Omega| = q^3 + 1$，$|\bar{\Omega}| = q^4 - q^3 + q^2$ が成り立つ。さらに，次の定理はよく知られている (例えば，Taylor [8, Chapter 10, p.123])。

定理 1. 結合構造 $\boldsymbol{H(q)} := \left(\Omega, \left\{\Omega \cap [u]^\perp \mid [u] \in \bar{\Omega}\right\}\right)$ は 2-$(q^3+1, q+1, 1)$ design であり，$\mathrm{Aut}\boldsymbol{H(q)} = P\Gamma U(3,q)$ である。

注意 2. この $\boldsymbol{H(q)}$ は **Hermitian unital design** と呼ばれる。特に，$\boldsymbol{H(2)}$ は 2-(9,3,1) design, すなわち位数 3 の Affine 平面である。$\boldsymbol{H(3)}$ は表題に現れる 2-(28,4,1) design であり，$P\Gamma U(3,3)$ $\left(= U_3(3) : 2 \text{ とかく}\right)$ は $G_2(2)$ と同型であることが知られている。

G. Hölz [4] は $\boldsymbol{H(3)}$ に 252 個の 4-arc (i.e., どの 3 個も collinear でない Ω の 4-subset) を加えて，2-(28,4,5) design を構成した。この design の自己同型群は $\left(U_3(3) : 2 \text{ ではなく}\right) Sp(6,2)$ になる。この design の 1 点に関する derived design 1-(27,3,5) は，J. A. Thas [9] によって (一意的に存在する) 位数 (2,4) の generalized quadrangle であることが認識された。さらに，Cameron *et al.* [1] は，この quadrangle の (デザインとしての) 拡大が一意的であることを示した。この quadrangle は，$O_6^-(2)$-geometry における 27 個の singular vector と 45 個の totally singular line によって記述されるが，まえがきで述べたように $U_3(2)$-geometry から $O_6^-(2)$-geometry を構成することができるから，我々は $U_3(2)$-geometry に着目した。

以下，$q = 2$ とし $\mathbb{F}_4 = \mathbb{F}_2[\omega]$ $(\omega^2 + \omega + 1 = 0)$ とする。

補題 3. $PG(V)$ の line は次の 2 種類に分かれる:

- hyperbolic line ····· 3 個の Ω の元と，直交する 2 個の $\bar{\Omega}$ の元を含む。$[u]^\perp$ ($[u] \in \bar{\Omega}$) の形をしている。
- parabolic line ····· 1 個の Ω の元と，互いに非直交な 4 個の $\bar{\Omega}$ の元を含む。$[a]^\perp$ ($[a] \in \Omega$) の形をしている。

したがって

$$\bar{\Omega} \overset{1:1}{\longleftrightarrow} \text{hyperbolic line 全体}, \qquad \Omega \overset{1:1}{\longleftrightarrow} \text{parabolic line 全体}$$

が成り立つ。

3 $H(3)$ の別構成

この章では $U_3(2)$-geometry から $\boldsymbol{H(3)}$ の cross characteristic construction を与える。$\boldsymbol{H(2)}$ のすべての parallel class は 4 個あるが，それらを F_1, F_2, F_3, F_4 とする。ただし，$\boldsymbol{H(2)}$ のブロック $\Omega \cap [u]^\perp$ と $[u] \in \bar{\Omega}$ は同一視する。各 F_i のどの 2 元も直交している。逆に，直交している 2 個の $\bar{\Omega}$ の元はただ 1 つの F_i に含まれる。

$$H_0 := F_1 \cup F_2, \qquad \tilde{H_0} := F_3 \cup F_4$$

とおくと，両方とも $PG(V)$ の hyperoval になる。$PG(V)$ の hyperoval とは，どの 3 個も collinear でない 6 点集合のことであり，$PG(V)$ の任意の line と 0 または 2 点で交わるという性質をもつ。

$V_0 := \{a \in V \mid [a] \in \Omega\}$ (isotropic vector 全体) とし，$\Omega \ni [a] = \{a, \omega a, \omega^2 a\}$ を V_0 の 3-subset とみれば，結合構造

$$\boldsymbol{D} := (V_0, \Omega)$$

は 1-(27,3,1) design になる。さらに，$a \in V_0$ に対して

$$B(a) := \left\{x \in V_0 \mid h(a,x) = 1 \text{ and } [a,x]^\perp \in H_0\right\}$$

と

$$\tilde{B}(a) := \left\{x \in V_0 \mid h(a,x) = 1 \text{ and } [a,x]^\perp \in \tilde{H_0}\right\}$$

を定義し，$\boldsymbol{D}$ に新しい点 ∞ と新しいブロックたち

$$\mathcal{B} := \bigcup_{a \in V_0} \left\{B(a), \tilde{B}(a)\right\}$$

を付け加えた結合構造を $\boldsymbol{D^*}$ とする。

命題 4. $\boldsymbol{D^*}$ は 2-$(28, 4, 1)$ design である。

略証明. V_0 の異なるベクトル a, b を取る。

i) $[a]=[b]$ のとき，$\{a,b\}$ を含む $\boldsymbol{D}^*$ のブロックは $[a]\cup\{\infty\}$ のみ。

ii) $h(a,b)=1$ のとき，$c:=a+b\in V_0$ である。

(i) $[a,b]^\perp\in H_0$ のとき，$\{a,b\}\subset B(c)$ である。

(ii) $[a,b]^\perp\in \tilde{H}_0$ のとき，$\{a,b\}\subset \tilde{B}(c)$ である。

iii) $h(a,b)\in\{\omega,\bar{\omega}\}$ のとき，$\alpha:=h(a,b)$, $\langle u\rangle:=\langle a,b\rangle^\perp$ とおく。

(i) $[a,b]^\perp\in H_0$ のとき，$[u]\in H_0$ であり，ある $\lambda\in\mathbb{F}_4^\times$ に対して $c:=\bar{\alpha}a+\alpha b+\lambda u\in V_0$ とおくと，$\{a,b\}\subset\tilde{B}(c)$ である。

(ii) $[a,b]^\perp\in \tilde{H}_0$ のとき，$[u]\in \tilde{H}_0$ であり，ある $\lambda\in\mathbb{F}_4^\times$ に対して $c:=\bar{\alpha}a+\alpha b+\lambda u\in V_0$ とおくと，$\{a,b\}\subset B(c)$ である。

以上により，2 点を含むブロックが少なくとも 1 個あることが示されるが，ちょうど 1 個あることもわかる。 □

$|\mathrm{Aut}\boldsymbol{D}^*|$ を求めるために，群論的考察を必要とする。

$$\hat{\theta}(x):=(\bar{x}_1,\bar{x}_2,\bar{x}_3)\quad(\forall x:=(x_1,x_2,x_3)\in V)$$

によって定義される V 上の半線形変換 $\hat{\theta}$ と，ユニタリ群 $U(3,2)$ が生成する群を $\Gamma U(3,2)$ とかき，$\hat{\theta}$ と特殊ユニタリ群 $SU(3,2)$ が生成する群を $\Sigma U(3,2)$ とかくことにすれば，各々の群の位数は表 1 の通りである。

群	位数
$\Gamma U(3,2)$	1296
$U(3,2)$	648
$\Sigma U(3,2)$	432
$SU(3,2)$	216

表 1

補題 5. (上記の)$\mathcal{B}$ は $\Sigma U(3,2)$-不変である。

定理 6. $\boldsymbol{D}^*$ は $\boldsymbol{H(3)}$ と同型である。

略証明. $\Sigma U(3,2)$ は $\boldsymbol{D}^*$ に作用しているから，$|\mathrm{Aut}\boldsymbol{D}^*|$ は 432 の倍数である。Krčadinac [6] が非自明な自己同型写像をもつ 2-(28,4,1) design を分類している。その分類によれば，432 の倍数であるものはただ 1 つしかなく，$|U_3(3):2|$ になる。したがって，$\mathrm{Aut}\boldsymbol{D}^*\simeq U_3(3):2$ であり，$\boldsymbol{D}^*$ は $\boldsymbol{H(3)}$ と同型である。 □

注意 7. $\{F_1,F_2,F_3,F_4\}$ を交わっていない 2 つの 2-subset に分ける方法は $\frac{1}{2}\binom{4}{2}=3$ 通りあるから，H_0 と $\tilde{H}_0$ の組の定義の仕方も 3 通りあって，それぞれに対して上記の $\mathcal{B}$ を定義することができる。それらを $\mathcal{B}_1,\mathcal{B}_2,\mathcal{B}_3$ とすれば，$|\mathcal{B}_i\cap\mathcal{B}_j|=0$ $(i\neq j)$ であり，$\Gamma U(3,2)$ の位数 3 の元によっ

て移り合うから，$\boldsymbol{D}$ に $\mathcal{B}_i$ $(i=1,2,3)$ を付け加えて得られる 2-(28,4,1) design は互いに同型になる。

$\boldsymbol{D}^*$ を射影化して，$\boldsymbol{H(2)}$ のブロックを付け加えると，(一意的に存在する)3-(10,4,1) design (すなわち，Witt design $\boldsymbol{W_{10}}$) が得られる。
$[a]\in\Omega$ に対して

$$B[a]:=\{[x]\mid x\in B(a)\}\quad\text{と}\quad \tilde{B}[a]:=\left\{[x]\mid x\in\tilde{B}(a)\right\}$$

を定義する。

系 8. 結合構造

$$\left(\Omega\cup\{\infty\},\ \{B\cup\{\infty\}\mid B:\text{block of }\boldsymbol{H(2)}\}\cup\bigcup_{[a]\in\Omega}\left\{B[a],\tilde{B}[a]\right\}\right)$$

は 3-(10,4,1) design である。

$U_3(2)$-geometry における H_0 と $\tilde{H}_0$ の組は，$O_6^-(2)$ を $G_2(2)$ に変形させるためのカギであるように思われる。以下，$G_2(2)$ を自己同型群にもつ代表的な組合せ構造物 srg(36,14,4,6) と GH(2,2) の別構成を与える。

4　srg(36,14,4,6) の別構成

この節では，$G_2(2)$ を自己同型群にもつ強正則グラフ $\mathrm{srg}(36,14,4,6)$ の別構成を与える。強正則グラフ (strongly regular graph, 略して srg) の定義は省くが，Cameron & van Lint [2] などを参照されたい。

$V_1:=\{u\in V\mid h(u,u)=1\}$ (nonisotropic vector 全体) とし

$$W:=\{u\in V_1\mid [u]\in H_0\}\ \text{と}\ \tilde{W}:=\{u\in V_1\mid [u]\in\tilde{H}_0\}$$

を定義する。$V_1=W\cup\tilde{W}$ (非交和), $|W|=|\tilde{W}|=18$ である。

命題 9. $W\cup\tilde{W}$ を頂点集合にもつグラフ Δ の辺集合を次のように定める:

(i) $u,v\in W$ または $u,v\in\tilde{W}$ は $h(u,v)\in\{0,1\}$ のときに限り隣接する。
(ii) $u\in W$ と $v\in\tilde{W}$ は $h(u,v)\in\{\omega,\bar{\omega}\}$ のときに限り隣接する。

このとき，Δ は $\mathrm{srg}(36,21,12,12)$ であり，$\mathrm{Aut}\Delta\simeq G_2(2)$ である。

略証明. グラフ

$$\left(V_1,\left\{\{u,v\}\in\binom{V_1}{2}\mid s(u,v)=0\right\}\right)$$

は自己同型群が $O_6^-(2):2$ となる $\mathrm{srg}(36,15,6,6)$ であることが知られている。ここで，s は最初のページで定義した交代形式である。$s(u,v)=0 \Leftrightarrow h(u,v)\in\{0,1\}$ に注意すれば，このグラフの W に関する switching graph は命題 9 の Δ になり，Δ は $\mathrm{srg}(36,21,12,12)$ になることがわかる。また，Spence [7] は 36 点上の srg を分類している。その分類によれば，上記の 2 つのグラフはリストに記載されている同じ switching class (No.1) に属すから，$\mathrm{Aut}\Delta \simeq G_2(2)$ となる。 □

系 10. Δ の補グラフ $\bar{\Delta}$ は srg(36,14,4,6) であり，自己同型群は $G_2(2)$ である。さらに，辺集合は次のようになる:

(i) $u,v\in W$ または $u,v\in\tilde{W}$ は $h(u,v)\in\{\omega,\bar{\omega}\}$ のときに限り隣接する。
(ii) $u\in W$ と $v\in\tilde{W}$ は $h(u,v)=1$ (0 はない) のときに限り隣接する。

5 GH(2,2) の別構成

この節では，$G_2(2)$ を自己同型群にもつ generalized hexagon GH(2,2) の別構成を与える。partial linear space $\boldsymbol{S}:=(\mathcal{P},\mathcal{L},\mathrm{I})$ の incidence graph Γ が連結，直径 (diameter)6 および内周 (girth)12 をみたし，かつ各点を通るライン数が 3 で，各ラインのサイズが 3 であるとき，$\boldsymbol{S}$ は**位数 (2,2) の generalized hexagon** と呼ばれ, GH(2,2) と表される。これの一般的な定義については Van Maldeghem [10] などを参照されたい。例えば，Fano 平面の点集合とライン集合の和集合を「点集合」とし，結合している点とラインの組全体を「ライン集合」と定義すれば，この「点集合」と「ライン集合」は GH(1,2) をなす。GH(2,2) は同型と双対 (i.e., $\boldsymbol{S}$ の点とラインを入れ換え，結合を逆にしたもの) を除いて一意に存在することが知られている (Cohen & Tits [3])。

$a\in V_0$ に対して

$$L(a):=\{x\in W\mid h(a,x)=0 \text{ and } a+x\in W\}\cup\{a\}$$

と

$$\tilde{L}(a):=\left\{x\in\tilde{W}\mid h(a,x)=0 \text{ and } a+x\in\tilde{W}\right\}\cup\{a\}$$

を定義する。

命題 11. 結合構造

$$\left(V\setminus\{0\},\ \bigcup_{a\in V_0}\left\{[a],L(a),\tilde{L}(a)\right\}\right)$$

は GH(2,2) である。

6 あとがき

Chevalley 群 $G_2(2)$ を自己同型群にもつ 3 つの代表的な組み合わせ構造物 2-(28,4,1) design, srg(36,14,4,6) および GH(2,2) の別構成をベクトル空間 $\mathbb{F}_4^3$ のベクトルたちで記述できるように

なった。さらに，Hermitian unital design $\boldsymbol{H(3)}$ の射影化で Witt design $\boldsymbol{W_{10}}$ が得られたことも (少なくとも我々にとっては) 意外であった。$\boldsymbol{H(3)}$ と同じパラメータをもつが非同型な design として，**Ree unital design** と呼ばれるものがある。これの構成は，ベクトル空間 $\mathbb{F}_3^6$ のベクトルたちで記述されることが定説になっているが，これの自己同型群 $L_2(8):3$ がシンプレクティック群 $S_6(2)$ の極大部分群であることから，本文の 1-(27,3,1) design $\boldsymbol{D}$ の拡大により得られると思う。その際，$\Sigma U(3,2)$ の位数 18 の部分群 ($\simeq$ 二面体群 D_{18}) に着目することになるが，この関係性は次のようにしても得られる: 直交群 $O^-(2,8)$ は位数 18 の二面体群と同型であり，$O^-(2,8)$-geometry (V,q) (q : マイナス型の 2 次形式) から, q の極形式を b として

$$Q(x) := q(x) + q(x)^2 + q(x)^4, \quad s(x,y) := b(x,y) + b(y,x)^2 + b(x,y)^4 \quad (\forall x, y \in V)$$

によって定義される 2 次形式 Q は，非退化かつ Witt 指数 2 (いわゆるマイナス型) であり，その極形式が s になるので，$O^-(6,2)$-geometry が構成される。ベクトル空間 $\mathbb{F}_8^2$ (または $\mathbb{F}_2^6$) のベクトルたちで記述できたら，cross characteristic construction になるから面白いように思える。ただし，射影平面 $PG(2,8)$ の典型的な hyperoval と交わっていない 28 本の射影直線と，63 個の nonisotoropic point から構成することができるので，cross characteristic construction がないわけではない。

参考文献

[1] P. J. Cameron, D. R. Hughes and A. Pasini, Extended generalized quadrangles, Geom. Dedica. **35** (1990), 193-228.

[2] P. J. Cameron and J. H. van Lint, *Designs, Graphs, Codes and their links*, London Mathematical Society Student Text **22**, Cambridge Univ. Press, 1991.

[3] A. M. Cohen and J. Tits, On generalized hexagons and a near octagon whose lines have three points, Europ. J. Combin. **6** (1985), 13-27.

[4] G. Hölz, Constructions of designs which contain a unital, Arch. Math. **37** (1981), 179-183.

[5] K. Inoue, An alternative construction of the Hermitian unital 2-(28,4,1) design, J. Combin. Designs **30** (2022), 752-759.

[6] V. Krčadinac, Steiner 2-designs $S(2,4,28)$ with nontrivial automorphisms, Glasnik Matematički **37** (2002), 259-268.

[7] E. Spence, Regular two-graphs on 36 vertices, Linear Algebra and its Applications 226-228 (1995), 459-497.

[8] D. E. Taylor, *The Geometry of the Classical Groups*, Sigma Series in Pure Mathematics **9**, Heldermann Verlag, Berlin, 1992.

[9] J. A. Thas, Extensions of finite generalized quadrangles, *Symp. Math.* **28** (1986), 127-143, Academic Press, London, 1986.

[10] H. Van Maldeghem, *Generalized polygons*, Birkhäuser Verlag, Basel, 1998.

符号の Jacobi 多項式とその組合せデザインへの応用

石川麗菜 *

1 はじめに

1997 年に小関道夫氏により導入された，符号の Jacobi 多項式という概念がある [8]．これまで多くの研究者が Jacobi 多項式を符合理論に応用すべく研究を行なってきた．中でも最も成功を収めたのは A. Bonnecaze 氏らによる符号から得られる組合せデザインの存在性の判定である．A. Bonnecaze 氏らは，Molien 級数や Jacobi 多項式の係数，Type II 符号の重さ分布多項式に着目し，符号がいつ組合せデザインを持つかどうかの判定法を与え，実際に組合せデザインを構成した．さらに，A. Bonnecaze 氏らは colored t-design という概念を導入し，$\mathbb{Z}_4$ 符号と $\mathbb{F}_3$ 符号に対応させ，Jacobi 多項式を用いて colored t-design を構成した [1, 2, 3]．また，2022 年には，Chakraborty 氏らが複数の符号語を用いる Jacobi 多項式の概念を導入し，Cameron 氏が定義した一般化 t-design への応用を示した [6].

本稿では，$\mathbb{F}_q$ 上の符号に対して一般化 Jacobi 多項式の概念を導入し，符号から得られる colored t-design の存在性を判定する条件を与える．これは小関道夫氏による符号の Jacobi 多項式を拡張した新しい概念である．第 2 章では組合せデザインと符号の定義を導入する．第 3 章では実際に具体的な符号を用いて，colored design を構成する方法を紹介する．

2 組合せデザイン

組合せデザインは試験の効率化を図る実験計画法の一つとして 19 世紀に誕生し，20 世紀以降も多くの数学者たちが理論を発展させてきた．第 1 章では，組合せデザインの概念を説明する．次に線形符号を説明した後，線形符号から組合せデザインを構成できることを示す．また，組合せデザインが Jacobi 多項式によって判定できることを紹介する．

2.1 組合せデザインの定義と例

はじめに，組合せデザインの定義を例を交えながら説明する．

定義 2.1 (t-(n,k,λ) design)**.** $X=\{1,2,\ldots,n\}$, $\mathcal{B}\subset\binom{X}{k}$ とする．$(X,\mathcal{B})$ が t-(n,k,λ) design であるとは，任意の $T\in\binom{X}{t}$ に対して，

$$\lambda=|\{B\in\mathcal{B}\mid T\subseteq B\}|$$

が一定に定まることである．

*早稲田大学大学院基幹理工学研究科，reina.i@suou.waseda.jp

例 2.2.

$$\begin{cases} X = \{1,2,3,4,5,6,7\}, \\ \mathcal{B} = \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}, \end{cases}$$

とおくと，任意の $T \in \binom{X}{2}$ に対して

$$|\{B \in \mathcal{B} \mid T \subseteq B\}| = 1.$$

よって，$(X, \mathcal{B})$ は 2-$(7,3,1)$ design である．これは，任意の二つの数字の組 $(\in \binom{X}{2})$ が図 1 のただ一つの辺上に現れることに対応する．

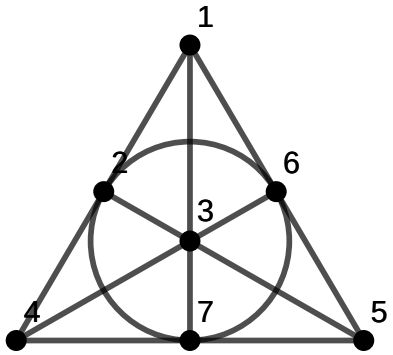


図 1

2.2　符号から得られる組合せデザイン

t-design は符号を用いて構成することができる. 符号を定義するにあたり，ハミング距離を次で定義する．

定義 2.3 (ハミング距離)**.** $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ に対し，ハミング距離 $d_H(x,y)$ を以下で定義する．

$$d_H(x,y) := \sum_{i=1}^{n} d(x_i, y_i)$$

ただし，

$$d(x_i, y_i) := \begin{cases} 0 \ (x_i = y_i) \\ 1 \ (x_i \neq y_i) \end{cases} .$$

例 2.4.

$$d_H((0,0),(0,1)) = 1.$$

定義 2.5 (線形符号)**.** $C(\neq \{0\})$ が $\mathbb{F}_q^n$ の部分空間で，$\dim(C) = k$ かつ最小ハミング距離 $d_{\min}(C) = d(\neq 0)$ が成り立つとき，$[n,k,d]_q$ 線形符号であるという．ここで，最小ハミング距離 $d_{\min}(C)$ とは，符号 C の相異なるベクトルの最小ハミング距離のことである．n を C の length という．

例 2.6.

$$C = \{(0,0,0),(1,1,0),(0,1,1),(1,0,1)\}$$

は $[3,2,2]_2$ 線形符号である．
なぜならば，基底として $\{(1,1,0),(0,1,1)\}$ がとれるので $\dim(C) = 2$ である．また，

$$\begin{aligned} d_H((0,0,0),(1,1,0)) &= d_H((0,0,0),(0,1,1)) = d_H((0,0,0),(1,0,1)) \\ &= d_H((1,1,0),(0,1,1)) = d_H((1,1,0),(1,0,1)) \\ &= d_H((0,1,1),(1,0,1)) = 2 \end{aligned}$$

より，$d = d_{\min} = 2$ となる．

なお，線形符号 C の元 $c = (c_1,\ldots,c_n)$ を C の符号語という．

定義 2.7 (線形符号の内積)**.** $[n,k,d]_q$ 線形符号の符号語 $x = (x_1,\ldots,x_n),\ y = (y_1,\ldots,y_n)$ の内積を次で定義する．

$$x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$$

なお，$x \cdot y = 0$ のとき，$x,\ y$ は直交するという．

定義 2.8 (双対符号)**.** 線形符号 $C^\perp$ の任意の符号語が C の任意の符号語と直交するとき，$C^\perp$ は $[n,k,d]_q$ 線形符号 C の双対符号であるという．すなわち，双対符号は以下で定義される．

$$C^\perp := \{x \in \mathbb{F}_q^n \mid x \cdot y = 0, \forall y \in C\}.$$

定義 2.9. C を $[n,k,d]_q$ 線形符号とし $(k = \dim(c))$，符号語 $c \in C$ を $c = (c_1,c_2,\ldots,c_n)$ としたとき，以下を定義する．

- $\mathrm{supp}(c) := \{i \mid c_i \neq 0\}$,
- $\mathrm{wt}(c) := |\mathrm{supp}(c)|$,
- $C_\ell := \{c \in C \mid \mathrm{wt}(c) = \ell\}$.

すなわち，$\mathrm{supp}(c)$ は符号語 c の 0 以外の要素をもつ座標の集合，$\mathrm{wt}(c)$ は符号語 c の 0 以外の要素の数，C_ℓ は 0 以外の要素を ℓ 個持つような符号語の集合である．

例 2.10. $C = \{(0,0,0),(1,1,0),(0,1,1),(1,0,1)\}$ について，

$$\begin{cases} \mathrm{supp}((0,1,1)) = \{2,3\}, \\ \mathrm{wt}((0,1,1)) = 2, \\ C_2 = \{(1,1,0),(0,1,1),(1,0,1)\}. \end{cases}$$

定義 2.11 (Type II 符号)**.** C を $[n,k,d]_2$ 線形符号とする．C が Type II 符号とは，$C = C^\perp$ かつ 任意の $c \in C$ に対して $\mathrm{wt}(c) \equiv 0 \pmod 4$ を満たすことである．

例 2.12 (length 8 の Type II 符号)**.** $\widetilde{H}$ (拡大 Hamming $[8,4,4]_2$ 符号) は Type II 符号である．実際，$\widetilde{H}$ の生成行列

$$\widetilde{G} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}$$

は $\widetilde{G}\widetilde{G}^t = \mathbb{O}$ を満たすので $\widetilde{H} = \widetilde{H}^\perp$ (自己双対) である．

また，$\widetilde{H}$ は $(0,0,0,0,0,0,0,0)$，$(1,1,1,1,1,1,1,1)$ と以下の符号語から成る．

$$\begin{array}{ll} (1,1,0,1,0,0,0,1) & (0,0,1,0,1,1,1,0) \\ (0,1,1,0,1,0,0,1) & (1,0,0,1,0,1,1,0) \\ (0,0,1,1,0,1,0,1) & (1,1,0,0,1,0,1,0) \\ (0,0,0,1,1,0,1,1) & (1,1,1,0,0,1,0,0) \\ (1,0,0,0,1,1,0,1) & (0,1,1,1,0,0,1,0) \\ (0,1,0,0,0,1,1,1) & (1,0,1,1,1,0,0,0) \\ (1,0,1,0,0,0,1,1) & (0,1,0,1,1,1,0,0) \end{array}$$

たしかに任意の $c \in \widetilde{H}$ に対して，$\mathrm{wt}(c)$ $(= 0 \text{ or } 4 \text{ or } 8) \equiv 0 \pmod 4$ である．

定義 2.13 (Type III 符号)**.** C を $[n,k,d]_3$ 線形符号とする．C が Type III 符号とは，$C = C^\perp$ かつ任意の $c \in C$ に対して $\mathrm{wt}(c) \equiv 0 \pmod 3$ を満たすことである．

例 2.14 (length 4 の Type III 符号)**.**

$$\begin{aligned} C = \{&(0,0,0,0),(2,0,2,2),(2,1,0,1),(2,2,1,0),(1,0,1,1), \\ &(0,1,1,2),(1,2,0,2),(1,1,2,0),(0,2,2,1)\} \end{aligned}$$

は Type III 符号である．実際，C の生成行列

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$$

は $GG^t = \mathbb{O}$ を満たし，$\forall c \in C$ は $\mathrm{wt}(c) \equiv 0 \pmod 3$ である．

定義 2.15 (Type IV 符号)**.** C を $[n,k,d]_4$ 線形符号とする．C が Type IV 符号とは，$C = C^\perp$ かつ任意の $c \in C$ に対して $\mathrm{wt}(c) \equiv 0 \pmod 2$ を満たすことである．

例 2.16 (length 4 の Type IV 符号)**.**

$$\begin{aligned} t_4 = \{&(1,1,0,0),(\alpha,\alpha,\alpha^2,\alpha^2),(\alpha,\alpha,\alpha,\alpha),(\alpha,\alpha,1,1),(\alpha,\alpha,0,0), \\ &(\alpha^2,\alpha^2,\alpha^2,\alpha^2),(\alpha^2,\alpha^2,\alpha,\alpha),(\alpha^2,\alpha^2,1,1),(\alpha^2,\alpha^2,0,0), \\ &(0,0,\alpha^2,\alpha^2),(0,0,\alpha,\alpha),(0,0,1,1),(0,0,0,0),(1,1,\alpha^2,\alpha^2), \\ &(1,1,\alpha,\alpha),(1,1,1,1)\} \end{aligned}$$

は Type IV 符号である．実際，t_4 の生成行列

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

は $GG^t = \mathbb{O}$ を満たすので $C = C^\perp$．$\forall c \in t_4$ は $\mathrm{wt}(c) \equiv 0 \pmod 2$ である．

定義 2.17 (符号から作る t-design)**.** $X = \{1, 2, \ldots, n\}$, $\mathcal{B}(C_\ell) := \{\mathrm{supp}(c) \mid c \in C, \mathrm{wt}(c) = \ell\}$ とおく．このとき C を上手く選ぶと、$(X, \mathcal{B})$ は t-design になる．

例 2.18.

$$\begin{cases} C = \{(0,0,0),(1,1,0),(0,1,1),(1,0,1)\} \subset \mathbb{F}_2^3, \\ C_2 = \{(1,1,0),(0,1,1),(1,0,1)\}, \\ X = \{1,2,3\}, \\ \mathcal{B}(C_2) = \{\{1,2\},\{1,3\},\{2,3\}\}, \end{cases}$$

とすると，任意の $T \in \binom{X}{2} = \{\{1,2\},\{1,3\},\{2,3\}\}$ に対して

$$|\{B \in \mathcal{B}(C_2) \mid T \subseteq B\}| = 1.$$

従って，$(X, \mathcal{B}(C_2))$ は 2-$(3,2,1)$ design である．

例 2.19.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

を生成行列とする符号 H(Hamming $[7,3,4]$ 符号) を考える．H は，$(0,0,0,0,0,0,0)$，$(1,1,1,1,1,1,1)$ と以下の H_3 と H_4 から成る．

$$\begin{array}{cc} (1,1,0,1,0,0,0) & (0,0,1,0,1,1,1) \\ (0,1,1,0,1,0,0) & (1,0,0,1,0,1,1) \\ (0,0,1,1,0,1,0) & (1,1,0,0,1,0,1) \\ (0,0,0,1,1,0,1) & (1,1,1,0,0,1,0) \\ (1,0,0,0,1,1,0) & (0,1,1,1,0,0,1) \\ (0,1,0,0,0,1,1) & (1,0,1,1,1,0,0) \\ (1,0,1,0,0,0,1) & (0,1,0,1,1,1,0) \\ H_3 = \{c \mid \mathrm{wt}(c) = 3\} & H_4 = \{c \mid \mathrm{wt}(c) = 4\} \end{array}$$

$$\begin{cases} X = \{1,2,3,4,5,6,7\}, \\ \mathcal{B}(H_3) = \{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}, \end{cases}$$

とすると，任意の $T \in \binom{X}{2}$ に対して $|\{B \in \mathcal{B} \mid T \subseteq B\}| = 1$. $(X, \mathcal{B}(H_3))$ は 2-$(7,3,1)$ design である．

2.3 Jacobi 多項式と組合せデザイン

Jacobi 多項式を用いると C からどのような t-design が得られるのかを判断できる．Jacobi 多項式を以下のように定義する．

定義 2.20 (Jacobi 多項式)**.** C を $[n,k,d]_q$ 線形符号, $T \subset \{1,\dots,n\} = [n]$ とする.

$$\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) := \sum_{c\in C} x_0^{m_0(c)} x_1^{m_1(c)} y_0^{n_0(c)} y_1^{n_1(c)}.$$

ここで,

$$\begin{aligned} m_0(c) &:= |\{i \mid c_i = 0, i \in T\}|, \\ m_1(c) &:= |\{i \mid c_i \neq 0, i \in T\}|, \\ n_0(c) &:= |\{i \mid c_i = 0, i \in [n]\setminus T\}|, \\ n_1(c) &:= |\{i \mid c_i \neq 0, i \in [n]\setminus T\}|. \end{aligned}$$

例 2.21. $[4,2,2]_2$ 線形符号

$$C = \{(0,0,0,0),(0,1,0,1),(1,0,1,0),(1,1,1,1)\}$$

の $T=\{1\}$ の Jacobi 多項式は以下である.

$$\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) = x_0^1x_1^0y_0^3y_1^0 + x_0^1x_1^0y_0^1y_1^2 + x_0^0x_1^1y_0^2y_1^1 + x_0^0x_1^1y_0^0y_1^3.$$

定理 2.22. 任意の $T \subset \{1,\dots,n\}$ $(|T|=t)$ に対し, $\mathrm{J}_{C,T}$ が一意的に定まるとする. このとき, 任意の ℓ に対し C_ℓ $(\neq \emptyset)$ は t-design である.

例 2.23. $C = \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}$, $T \subset \{1,2,3\}$, $|T|=2$ とする.

- $T=\{1,2\}$
  $\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) = x_0^2y_0 + x_1^2y_0 + x_0x_1y_1 + x_0x_1y_1.$

- $T=\{1,3\}$
  $\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) = x_0^2y_0 + x_0x_1y_0 + x_1^2y_0 + x_0x_1y_1.$

- $T=\{2,3\}$
  $\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) = x_0^2y_0 + x_0x_1y_0 + x_0x_1y_1 + x_1^2y_0.$

従って任意の ℓ について, $C_\ell(\neq\emptyset)$ は 2-design である.

たしかに $\begin{cases} X=\{1,2,3\} \\ \mathcal{B}(C_2) = \{\{1,2\},\{1,3\},\{2,3\}\} \end{cases}$ と見れば $(X,\mathcal{B}(C_2))$ は 2-design である.

例 1.12. において, $x_0^2y_0$ の項は all 0 の符号語に対応する. どのように T を定めても $x_0^2y_0$ の係数は 1 であり, 線形符号が必ず all 0 の符号語を含むことを示している.

2.4 Jacobi 多項式の MacWilliams 恒等式

次に, Jacobi 多項式が一意的であることを理論的に示す方法を紹介する.

補題 2.24. C が $[n,k,d]_q$ 自己双対符号 ($C=C^{\perp}$) ならば $\dim(C)=\dfrac{n}{2}$ である.
(なぜなら次元定理 $\dim(C^{\perp})=n-k=\dim(C)=k$ より，$k=\dfrac{n}{2}$ である．)

定理 2.25 (Jacobi 多項式の MacWilliams 恒等式)**.** C が $[n,k,d]_2$ 線形符号のとき，以下が成り立つ.

$$\mathrm{J}_{C^{\perp},T}(x_0,x_1,y_0,y_1)=\frac{1}{|C|}\mathrm{J}_{C,T}(x_0+x_1,x_0-x_1,y_0+y_1,y_0-y_1).$$

特に，C が Type II 符号のとき,

$$\begin{cases}\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) &= \mathrm{J}_{C,T}\left(\dfrac{x_0+x_1}{\sqrt{2}},\dfrac{x_0-x_1}{\sqrt{2}},\dfrac{y_0+y_1}{\sqrt{2}},\dfrac{y_0-y_1}{\sqrt{2}}\right)\\ \mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) &= \mathrm{J}_{C,T}(x_0,\sqrt{-1}x_1,y_0,\sqrt{-1}y_1)\end{cases}$$

が成り立つ.

例 2.26. Type II 符号として $\widetilde{H}$ (拡大Hamming $[8,4,4]_2$ 符号) を考える．$\widetilde{H}$ は，$(0,0,0,0,0,0,0,0),(1,1,1,1,1,1,1,1)$ と以下の符号語から成る.

$$\begin{array}{ll}(1,1,0,1,0,0,0,1) & (0,0,1,0,1,1,1,0)\\ (0,1,1,0,1,0,0,1) & (1,0,0,1,0,1,1,0)\\ (0,0,1,1,0,1,0,1) & (1,1,0,0,1,0,1,0)\\ (0,0,0,1,1,0,1,1) & (1,1,1,0,0,1,0,0)\\ (1,0,0,0,1,1,0,1) & (0,1,1,1,0,0,1,0)\\ (0,1,0,0,0,1,1,1) & (1,0,1,1,1,0,0,0)\\ (1,0,1,0,0,0,1,1) & (0,1,0,1,1,1,0,0)\end{array}$$

$T=\{1\}$ とする．このとき

$$\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1)=x_0y_0^7+7x_0y_0^3y_1^4+7y_0^4y_1^3x_1+y_1^7x_1,$$

$$\begin{aligned}\mathrm{J}_{C,T}\left(\frac{x_0+x_1}{\sqrt{2}},\frac{x_0-x_1}{\sqrt{2}},\frac{y_0+y_1}{\sqrt{2}},\frac{y_0-y_1}{\sqrt{2}}\right) &= \frac{1}{16}(x_0-x_1)(y_1-y_0)^7\\ &\quad+\frac{7}{16}(x_0+x_1)(y_0+y_1)^3(y_1-y_0)^4\\ &\quad+\frac{7}{16}(x_0-x_1)(y_0+y_1)^4(y_1-y_0)^3\\ &\quad+\frac{1}{16}(x_0+x_1)(y_0+y_1)^7\\ &= x_0y_0^7+7x_0y_0^3y_1^4+7y_0^4y_1^3x_1+y_1^7x_1,\end{aligned}$$

$$\mathrm{J}_{C,T}(x_0,\sqrt{-1}x_1,y_0,\sqrt{-1}y_1)=x_0y_0^7+7x_0y_0^3y_1^4+7y_0^4y_1^3x_1+y_1^7x_1$$

より，たしかに

$$\begin{aligned}\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) &= \mathrm{J}_{C,T}\left(\frac{x_0+x_1}{\sqrt{2}},\frac{x_0-x_1}{\sqrt{2}},\frac{y_0+y_1}{\sqrt{2}},\frac{y_0-y_1}{\sqrt{2}}\right)\\ &= \mathrm{J}_{C,T}(x_0,\sqrt{-1}x_1,y_0,\sqrt{-1}y_1)\\ &= x_0y_0^7+7x_0y_0^3y_1^4+7y_0^4y_1^3x_1+y_1^7x_1,\end{aligned}$$

が成り立つ.

系 2.27. C が Type II 符号のとき，C の Jacobi 多項式は次の群 G に関する不変式である．

$$G = \left\langle \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \sqrt{-1} \end{bmatrix} \right\rangle.$$

定義 2.28 (Molien 級数)**.**

$$M_G(u,v) = \sum_{n=0}^{\infty} \sum_{i=0}^{n} \dim(\mathbb{C}[x_0,x_1,y_0,y_1]^G)_{i,n-i} u^i v^{n-i}$$

を Molien 級数という．ここで，

$$\begin{aligned} M_{i,n-i} :&= (\mathbb{C}[x_0,x_1,y_0,y_1]^G)_{i,n-i} \\ &= \{f \in \mathbb{C}[x_0,x_1,y_0,y_1] \mid \forall g \in G,\ gf = f, \\ &\qquad\qquad f \text{ の } x_0,x_1 \text{ の次数が } i, \\ &\qquad\qquad f \text{ の } y_0,y_1 \text{ の次数が } n-i\}. \end{aligned}$$

定理 2.29 (Molien)**.** 次が成立する．

$$M_G(u,v) = \frac{1}{|\widetilde{G}|} \sum_{g \in \widetilde{G}} \frac{1}{\det(I-ug)\det(I-vg)}.$$

$$\left(\widetilde{G} = \left\langle \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{bmatrix} \right\rangle. \right)$$

例 2.30. $M_G(u,v)$ を用いると，以下のように理論的に t-design の存在がわかる．

$$\begin{aligned} M_G(u,v) &= \frac{1}{|\widetilde{G}|} \sum_{g \in \widetilde{G}} \frac{1}{\det(I-vg)\det(I-ug)} \\ &= 1 + v^8 + v^{16} + 2v^{24} + 2v^{32} + 2v^{40} + \cdots \\ &\quad + (1v^7 + v^{15} + 2v^{23} + 3v^{31} + 3v^{39} + \cdots)u \\ &\quad + (1v^6 + 2v^{14} + 3v^{22} + 4v^{30} + 5v^{38} + \cdots)u^2 \\ &\quad + (1v^5 + \cdots)u^3 + \cdots \end{aligned}$$

uv^7 に対応する不変式の空間 $M_{1,7}$ の次元は 1 である．よって，$|T| = 1$ のとき

$$\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1) \in M_{1,7}$$

であり，ある多項式の定数倍で表せる．すなわち，任意の T ($|T| = 1$) について

$$\mathrm{J}_{C,T}(x_0,x_1,y_0,y_1)$$

は 1 本に定まる．従って，任意の ℓ に対し，$\widetilde{H_\ell}$ は 1-design であるといえる．

同様に $u^2v^6 \in M_{2,6}$，$u^3v^5 \in M_{3,5}$ の係数が 1 であることから 2-design と 3-design がわかる．

3　色付き組合せデザイン

本章では第 1 章で紹介した組合せデザインを色付き design に拡張する．色付き組合せデザインの定義を例を交えて説明した後，符号からこれを作る方法を述べる．また，一般化 Jacobi 多項式の概念を導入し，色付き組合せデザインを判定する方法を説明する．最後に，Type IV 符号に MacWilliams 恒等式・Molien の定理を導入し，得られた色付き design を紹介する．

3.1　色付き組合せデザインの定義と例

定義 3.1 (q-colored t-design)**.**

$$\begin{cases} X = \{1, \dots, n\}, \\ Col = \mathbb{F}_q = \{x_1, \dots, x_q\}, \\ \mathcal{B} = \binom{X}{k}, \\ \rho : X \times \mathcal{B} \to Col (\text{ただし，} \mathcal{B} \text{ は多重集合}), \end{cases}$$

とする．$\mathcal{D} = (X, \mathcal{B}, \rho)$ が q-colored t-design であるとは，任意の $P \in \binom{Col}{t}$（多重集合）に対して，次の λ_P が定まることである．

$$\forall T \in \binom{X}{t}, |\{B \in \mathcal{B} \mid P = \rho(T, B)\}| = \lambda_P$$

すなわち，任意の $T \in \binom{X}{t}$ を含む $B \in \mathcal{B}$ の数 λ_P が一定になる．

例 3.2. $X = \{1, 2, 3\}$,
$\mathcal{B} = \{\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},$
$\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},$
$\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\}\},$
$Col = \{\bullet, \bullet, \bullet\}$,
$\rho(T, B) =$
$\{\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},$
$\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},$
$\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\},\{1,2\},\{1,3\},\{2,3\}\},$
$P \in \binom{Col}{2} = \{\{\bullet,\bullet\},\{\bullet,\bullet\},\{\bullet,\bullet\},\{\bullet,\bullet\},\{\bullet,\bullet\},\{\bullet,\bullet\}\}$, とする．このとき，任意の P に対してどんな $T \in \binom{X}{2}$ を選んでも λ_P が一定である．よって，$\mathcal{D} = (X, \mathcal{B}, \rho)$ は 3-colored 2-design である．

T と P の関係は以下になる．

T \ P	$\{\bullet,\bullet\}$	$\{\bullet,\bullet\}$	$\{\bullet,\bullet\}$	$\{\bullet,\bullet\}$	$\{\bullet,\bullet\}$	$\{\bullet,\bullet\}$
$\{1,2\}$	1	2	2	1	2	1
$\{1,3\}$	1	2	2	1	2	1
$\{2,3\}$	1	2	2	1	2	1

3.2 符号から得られる色付き組合せデザイン

colored t-design は符号から作ることができる．符号から得る q-colored t-design を次のように定義する．

定義 3.3 (符号から得る q-colored t-design)**.**

$$\begin{cases} C : [n,k,d]_q\text{線形符号}, \\ Co\ell = \mathbb{F}_q = \{x_1,\dots,x_q\}, \\ n_{x_i} = |\{j \mid c = (c_1,\dots,c_n) \in C, c_j = x_i\}|, \\ C_{(n_{x_1},\dots,n_{x_q})} = \{c \in C \mid c \text{ に含まれる } x_i \text{ の数が } n_{x_i}\}, \\ X = \{1,\dots,n\}, \\ \mathcal{B} = \{X_c \mid X_c = X, c \in C_{(n_{x_1},\dots,n_{x_q})}\}, \\ \rho : X \times \mathcal{B} \to Co\ell\ ; (i, X_c) \mapsto c_i, \end{cases}$$

とおく．$\mathcal{D} = (X, \mathcal{B}, \rho)$ が q-colored t-design であるとは，任意の $P \in \binom{Co\ell}{t}$ に対して，次の λ_P が定まることである．

$$\forall T \in \binom{X}{t}, |\{B \in \mathcal{B} \mid P = \rho(T,B)\}| = \lambda_P.$$

これは先の colored t-design と本質的に一致する．

例 3.4. $X = \{1,2,3\}$, C を以下の $\mathbb{F}_3$ 符号とする．

$$C = \{(0,0,0),(1,0,2),(2,0,1),(2,1,0),(0,1,2),\\ (1,1,1),(1,2,0),(2,2,2),(0,2,1)\}.$$

さらに，$C_{(1,1,1)} \subset C$ を次で定める．

$$C_{(1,1,1)} := \{(1,0,2),(2,0,1),(0,1,2),(2,1,0),(1,2,0),(0,2,1)\}.$$

ここで，

$$\mathcal{B} = \{\{1,2,3\},\{1,2,3\},\{1,2,3\},\{1,2,3\},\{1,2,3\},\{1,2,3\}\}$$

である．このとき，任意の 1 つの色 $P \in \binom{\{0,1,2\}}{1}$ に対して，どのような座標 $T \in \binom{\{1,2,3\}}{1}$ を選んでも $\lambda_P = 2$ で一定なので，3-colored 1-design である．

T \ P	0	1	2
$\{1\}$	2	2	2
$\{2\}$	2	2	2
$\{3\}$	2	2	2

$C_{(1,1,1)} := \{(1,0,2),(2,0,1),(0,1,2),(2,1,0),(1,2,0),(0,2,1)\}$ は 3-colored 2-design でもある．なぜなら，任意の 2 つの色 $P \in \binom{\{0,1,2\}}{2}$ に対し，どのような座標 $T \in \binom{\{1,2,3\}}{2}$ を選んでも $\lambda_P = 0, 2$ で一定である．

T \ P	$\{0,0\}$	$\{0,1\}$	$\{0,2\}$	$\{1,1\}$	$\{1,2\}$	$\{2,2\}$
$\{1,2\}$	0	2	2	0	2	0
$\{1,3\}$	0	2	2	0	2	0
$\{2,3\}$	0	2	2	0	2	0

3.3 一般化 Jacobi 多項式と組合せデザイン

一般化 Jacobi 多項式を用いると，符号から colored t-design が得られるかどうかを判断できる．一般化 Jacobi 多項式を次のように定義する．

定義 3.5 ([7, 一般化 Jacobi 多項式]). C を長さ n の $\mathbb{F}_q$ 線形符号，$T \subset [n]$, $u \in C$, $u = (u_1, \ldots, u_n)$ とする．

$$\mathrm{CJ}_{C,T}(\{x_a, y_a\}_{a\in\mathbb{F}_q}) := \sum_{\boldsymbol{u}\in C} \prod_{a\in\mathbb{F}_q} x_a^{n_{a,T}(u)} y_a^{n_{a,[n]\setminus T}(u)},$$

ここで，

$$n_{a,T}(u) := |\{i \mid u_i = a, i \in T\}|,$$
$$n_{a,[n]\setminus T}(u) := |\{i \mid u_i = a, i \in [n]\setminus T\}|.$$

例 3.6. C を長さ 4 の $\mathbb{F}_3$ 線形符号，

$$\begin{aligned} C = \{&(0,0,0,0),(0,1,1,2),(0,2,2,1),\\ &(1,0,1,1),(1,1,2,0),(1,2,0,2),\\ &(2,0,2,2),(2,1,0,1),(2,2,1,0)\} \end{aligned}$$

とする．
$T = \{1,3\}$ のとき，

$$\begin{aligned} \mathrm{CJ}_{C_4,T}(x_0,x_1,x_2,y_0,y_1,y_2) = {}& x_0^2y_0^2 + x_1^2y_0^1y_1^1 + x_2^2y_0^1y_2^1 + x_0^1x_1^1y_1^1y_2^1\\ &+ x_1^1x_2^1y_0^1y_1^1 + x_0^1x_2^1y_1^2 + x_0^1x_2^1y_1^1y_2^1\\ &+ x_0^1x_1^1y_2^2 + x_1^1x_2^1y_0^1y_2^1. \end{aligned}$$

例 3.7. length 4 の Type IV 符号

$$\begin{aligned} t_4 = \{&(1,1,0,0),(\alpha,\alpha,\alpha^2,\alpha^2),(\alpha,\alpha,\alpha,\alpha),(\alpha,\alpha,1,1),(\alpha,\alpha,0,0),\\ &(\alpha^2,\alpha^2,\alpha^2,\alpha^2),(\alpha^2,\alpha^2,\alpha,\alpha),(\alpha^2,\alpha^2,1,1),(\alpha^2,\alpha^2,0,0),\\ &(0,0,\alpha^2,\alpha^2),(0,0,\alpha,\alpha),(0,0,1,1),(0,0,0,0),(1,1,\alpha^2,\alpha^2),\\ &(1,1,\alpha,\alpha),(1,1,1,1)\} \end{aligned}$$

を考える．$T=\{1,2\}$ のとき，

$$\begin{aligned}\mathrm{CJ}_{t_4,T}(x_0,x_1,x_\alpha,x_{\alpha^2},y_0,y_1,y_\alpha,y_{\alpha^2}) &= x_1^2y_0^2+x_\alpha^2y_{\alpha^2}^2+x_\alpha^2y_\alpha^2+x_\alpha^2y_1^2\\ &\quad+x_\alpha^2y_0^2+x_{\alpha^2}^2y_{\alpha^2}^2+x_{\alpha^2}^2y_\alpha^2+x_{\alpha^2}^2y_1^2\\ &\quad+x_{\alpha^2}^2y_0^2+x_0^2y_{\alpha^2}^2+x_0^2y_\alpha^2+x_0^2y_1^2\\ &\quad+x_0^2y_0^2+x_1^2y_{\alpha^2}^2+x_1^2y_\alpha^2+x_1^2y_1^2.\end{aligned}$$

定理 3.8. 任意の T ($|T|=t$) について $\mathrm{CJ}_{C,T}$ が一意的に定まるならば，任意の $\mathcal{B}(C_{(n_{x_1},\ldots,n_{x_q})})$ ($\neq\emptyset$) は q-colored t-design である．

例 3.9. 前の例の 3-colored 2-design の符号
$C=\{(0,0,0),(1,0,2),(2,0,1),(2,1,0),(0,1,2),(1,1,1),(1,2,0),$
$(2,2,2),(0,2,1)\}$, $C_{(1,1,1)}:=\{(1,0,2),(2,0,1),(0,1,2),(2,1,0),(1,2,0),(0,2,1)\}$
を用いる．

$|T|=1$ について，

- $T=\{1\}$ のとき

$$\begin{aligned}\mathrm{CJ}_{\mathrm{C}_{(1,1,1)},\mathrm{T}}(\mathrm{x}_0,\mathrm{x}_1,\mathrm{x}_2,\mathrm{y}_0,\mathrm{y}_1,\mathrm{y}_2) &= x_1^1y_0^1y_2^1+x_2^1y_0^1y_1^1+x_2^1y_0^1y_1^1+x_0^1y_1^1y_2^1\\ &\quad+x_1^1y_0^1y_2^1+x_0^1y_1^1y_2^1\\ &=2x_0^1y_1^1y_2^1+2x_1^1y_0^1y_2^1+2x_2^1y_0^1y_1^1.\end{aligned}$$

- $T=\{2\}$ のとき

$$\begin{aligned}\mathrm{CJ}_{\mathrm{C}_{(1,1,1)},\mathrm{T}}(\mathrm{x}_0,\mathrm{x}_1,\mathrm{x}_2,\mathrm{y}_0,\mathrm{y}_1,\mathrm{y}_2) &= x_0^1y_1^1y_2^1+x_0^1y_1^1y_2^1+x_1^1y_0^1y_2^1+x_1^1y_0^1y_2^1\\ &\quad+x_2^1y_0^1y_1^1+x_2^1y_0^1y_1^1\\ &=2x_0^1y_1^1y_2^1+2x_1^1y_0^1y_2^1+2x_2^1y_0^1y_1^1.\end{aligned}$$

- $T=\{3\}$ のとき

$$\begin{aligned}\mathrm{CJ}_{\mathrm{C}_{(1,1,1)},\mathrm{T}}(\mathrm{x}_0,\mathrm{x}_1,\mathrm{x}_2,\mathrm{y}_0,\mathrm{y}_1,\mathrm{y}_2) &= x_2^1y_0^1y_1^1+x_1^1y_0^1y_2^1+x_0^1y_1^1y_2^1+x_2^1y_0^1y_1^1\\ &\quad+x_0^1y_1^1y_2^1+x_1^1y_0^1y_2^1\\ &=2x_0^1y_1^1y_2^1+2x_1^1y_0^1y_2^1+2x_2^1y_0^1y_1^1.\end{aligned}$$

よって，$|T|=1$ なる任意の T で $\mathrm{CJ}_{C,T}$ が一致するので，3-colored 1-design の符号である．

また，$|T|=2$ について，

- $T=\{1,2\}$ のとき

$$\begin{aligned}\mathrm{CJ}_{C_{(1,1,1)},T}(x_0,x_1,x_2,y_0,y_1,y_2) &= x_1^1x_0^1y_2^1+x_2^1x_0^1y_1^1+x_0^1x_1^1y_2^1+x_2^1x_1^1y_0^1\\ &\quad+x_1^1x_2^1y_0^1+x_0^1x_2^1y_1^1\\ &=2x_0^1x_1^1y_2^1+2x_1^1x_0^1y_2^1+2x_2^1x_0^1y_1^1.\end{aligned}$$

- $T=\{1,3\}$ のとき

$$\begin{aligned}\mathrm{CJ}_{C_{(1,1,1)},T}(x_0,x_1,x_2,y_0,y_1,y_2) &= x_1^1x_2^1y_0^1+x_2^1x_1^1y_0^1+x_0^1x_2^1y_1^1+x_2^1x_1^1y_0^1\\ &\quad +x_1^1x_0^1y_2^1+x_0^1x_1^1y_2^1\\ &= 2x_0^1x_1^1y_2^1+2x_1^1x_0^1y_2^1+2x_2^1x_0^1y_1^1.\end{aligned}$$

- $T=\{2,3\}$ のとき

$$\begin{aligned}\mathrm{CJ}_{C_{(1,1,1)},T}(x_0,x_1,x_2,y_0,y_1,y_2) &= x_0^1x_2^1y_1^1+x_0^1x_1^1y_2^1+x_1^1x_2^1y_0^1+x_1^1x_0^1y_2^1\\ &\quad +x_2^1x_0^1y_1^1+x_2^1x_1^1y_0^1\\ &= 2x_0^1x_1^1y_2^1+2x_1^1x_0^1y_2^1+2x_2^1x_0^1y_1^1.\end{aligned}$$

よって，$|T|=2$ なる任意の T で $\mathrm{CJ}_{C,T}$ が一致するので，3-colored 2-design の符号である．

3.4 Type IV 符号の MacWilliams 恒等式

定理 3.10 (Type IV 符号の MacWilliams 恒等式)**.** C が Type IV 符号のとき，次が成り立つ．

$$\mathrm{CJ}_{C,T}(x_0,x_1,x_\alpha,x_{\alpha^2},y_0,y_1,y_\alpha,y_{\alpha^2})=\mathrm{CJ}_{C,T}\left(X_0,X_1,X_2,X_3,Y_0,Y_1,Y_2,Y_3.\right)$$

ここで，

$$\begin{aligned}X_0&=\frac{x_0+x_1+x_\alpha+x_{\alpha^2}}{2},\ Y_0=\frac{y_0+y_1+y_\alpha+y_{\alpha^2}}{2},\\ X_1&=\frac{x_0+x_1-x_\alpha-x_{\alpha^2}}{2},\ Y_1=\frac{y_0+y_1-y_\alpha-y_{\alpha^2}}{2},\\ X_2&=\frac{x_0-x_1+x_\alpha-x_{\alpha^2}}{2},\ Y_2=\frac{y_0-y_1+y_\alpha-y_{\alpha^2}}{2},\\ X_3&=\frac{x_0-x_1-x_\alpha+x_{\alpha^2}}{2},\ Y_3=\frac{y_0-y_1-y_\alpha+y_{\alpha^2}}{2}.\end{aligned}$$

系 3.11. Type IV 符号の一般化 Jacobi 多項式 $\mathrm{CJ}_{C,T}(x_0,x_1,x_\alpha,x_{\alpha^2},y_0,y_1,y_\alpha,y_{\alpha^2})$ は以下の群 G に関して不変である．

$$G=\langle A_1\oplus A_1,A_2\oplus A_2,A_3\oplus A_3,A_4\oplus A_4\rangle.$$

ただし，

$$A_1=\frac{1}{2}\begin{bmatrix}1&1&1&1\\1&1&-1&-1\\1&-1&1&-1\\1&-1&-1&1\end{bmatrix},A_2=\begin{bmatrix}1&0&0&0\\0&-1&0&0\\0&0&-1&0\\0&0&0&-1\end{bmatrix},$$

$$A_3=\begin{bmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix},A_4=\begin{bmatrix}1&0&0&0\\0&0&1&0\\0&0&0&1\\0&1&0&0\end{bmatrix}.$$

ここで，A_1 は MacWilliams 恒等式，A_2 は Type IV 符号の任意の符号語 c の $\mathrm{wt}(c)$ が偶数であること，A_3 は任意の符号語に all 1 ベクトルを加えた符号語，そして A_4 は任意の符号語に α をかけた符号語にそれぞれ対応する．

定理 3.12. C_6^{IV} は 2-design である.

Proof. $|T|=2$ で Jacobi 多項式が一意的に定まることを示す. 前の $\widetilde{G}$ についての Molien 級数は以下のようになる.

$$\begin{aligned} M_G(u,v) = 1 &+ v^2 + v^4 + 2v^6 + \cdots \\ &+ (v + v^3 + 2v^5 + 6v^9 + \cdots)u \\ &+ (1 + 2v^2 + 3v^4 + \cdots)u^2 \\ &+ \cdots \end{aligned}$$

u^2v^4 の係数に注目すると, 3 である. すなわち $|T|=2$ の Jacobi 多項式には 3 つの基底 f_1, f_2, f_3 が存在する.

$$\begin{cases} f_1 = R(x_0^2 y_0^4) \\ f_2 = R(x_0^2 y_1^2 y_\alpha^2) \\ f_3 = R(x_0 x_\alpha y_0 y_1 y_\alpha^2) \end{cases}$$

ここで,

$$R(*) = \frac{1}{|G|}\sum_{g\in G} g(*) \text{ (Reynolds operator)}.$$

いま, $|T|=2$ の C_6^{IV} に対する一般化 Jacobi 多項式は 3 つの基底を用いて次のように表せる.

$$\mathrm{CJ}_{C_6^{\mathrm{IV}},T}(x_0, x_1, x_\alpha, x_{\alpha^2}, y_0, y_1, y_\alpha, y_{\alpha^2}) = a_1 f_1 + a_2 f_2 + a_3 f_3.$$

ここで, $S: \begin{cases} x_0 \mapsto x_0 \\ \{x_1, x_\alpha, x_{\alpha^2}\} \mapsto x_1 \\ y_0 \mapsto y_0 \\ \{y_1, y_\alpha, y_{\alpha^2}\} \mapsto y_1 \end{cases}$
とする. このとき

$$S(\mathrm{CJ}_{C_6^{\mathrm{IV}},T})(x_0, x_1, x_\alpha, x_{\alpha^2}, y_0, y_1, y_\alpha, y_{\alpha^2}) = \mathrm{J}_{C_6^{\mathrm{IV}},T}(x_0, x_1, y_0, y_1)$$

が成り立つ.

$\mathrm{CJ}_{C_6^{\mathrm{IV}},T} = a_1 f_1 + a_2 f_2 + a_3 f_3$ に S を作用させたものは

$$\begin{aligned} S(\mathrm{CJ}_{C_6^{\mathrm{IV}},T}) &= a_1\widetilde{f_1} + a_2\widetilde{f_2} + a_3\widetilde{f_3} \\ &= 30x_\alpha^4 y_0^2 + 90x_{\alpha^2}^4 y_0^2 + 720 x_\alpha x_{\alpha^2}^3 y_0 y_1 + 540 x_\alpha^2 x_{\alpha^2}^2 y_1^2 \\ &+ 540 x_{\alpha^2}^4 y_1^2. \end{aligned} \tag{1}$$

また,

$$\begin{aligned}
S(\mathrm{CJ}_{C_6^{\mathrm{IV}},T}) &= A_4^2(\mathrm{J}_{C,\varnothing}) \\
&= 54a_1y_0^2x_\alpha^4 + 108a_1y_0^2x_\alpha^2x_{\alpha^2}^2 + 126a_1y_0^2x_{\alpha^2}^4 + 6a_2y_0^2x_\alpha^4 \\
&+ 12a_2y_0^2x_\alpha^2x_{\alpha^2}^2 + 78a_2y_0^2x_{\alpha^2}^4 + 6a_3y_0^2x_\alpha^4 - 12a_3y_0^2x_\alpha^2x_{\alpha^2}^2 \\
&+ 6a_3y_0^2x_{\alpha^2}^4 + 144a_1y_0y_1x_\alpha^3x_{\alpha^2} + 1008a_1y_0y_1x_\alpha x_{\alpha^2}^3 \\
&- 48a_2y_0y_1x_\alpha^3x_{\alpha^2} + 48a_2y_0y_1x_\alpha x_{\alpha^2}^3 + 192a_3y_0y_1x_\alpha x_{\alpha^2}^3 \\
&+ 18a_1y_1^2x_\alpha^4 + 756a_1y_1^2x_\alpha^2x_{\alpha^2}^2 + 1242a_1y_1^2x_{\alpha^2}^4 + 18a_2y_1^2x_\alpha^4 \\
&+ 180a_2y_1^2x_\alpha^2x_{\alpha^2}^2 + 90a_2y_1^2x_{\alpha^2}^4 - 6a_3y_1^2x_\alpha^4 + 108a_3y_1^2x_\alpha^2x_{\alpha^2}^2 \\
&+ 90a_3y_1^2x_{\alpha^2}^4. \quad (\because (C_6^{\mathrm{IV}})_\ell \text{は 2-design}) \qquad (2)
\end{aligned}$$

ここで,

$$A_4(P) := \frac{1}{n}\left(y_0\frac{\partial P}{\partial x_0} + y_1\frac{\partial P}{\partial x_1}\right).$$

従って式 (1), (2) の係数を比較して次の連立方程式を解けばよい.

実際に $y_0^2x_\alpha^4, y_0^2x_\alpha^2x_{\alpha^2}^2, y_0y_1x_\alpha^3x_{\alpha^2}$ の係数を比較すると,

$$\begin{cases} 54a_1 + 6a_2 + 6a_3 = 30 \\ 18a_1 + 18a_2 + -6a_3 = 0 \\ 144a_1 - 48a_2 = 0 \end{cases}$$

$$\therefore a_1 = \frac{5}{24}, a_2 = \frac{5}{8}, a_3 = \frac{5}{2}$$

が一意的に得られ，$\mathrm{CJ}_{C_6^{\mathrm{IV}},T}$ は一本に定まることがわかる.

主結果 3.1 ([7]). 同様の手法で Type IV 符号による 4-colored t-design が以下のように得られた.

length	t	$(n_0, n_1, n_\alpha, n_{\alpha^2})$(要素の入れ替え可)	$\lvert\mathcal{B}\rvert$
4	1	$(2,2,0,0)$	2
6	1	$(2,2,2,0)$	15
8	1	$(4,4,0,0)$	14
6	2	$(2,2,2,0)$	15
8	2	$(4,4,0,0)$	14
8	3	$(4,4,0,0)$	14

終わりに

本稿では，$\mathbb{F}_q$ 上の符号に対して一般化 Jacobi 多項式の概念を導入し，符号から色付き design の存在性を判定する条件を与えた．結果，Type IV 符号の colored t-design について MacWilliams 恒等式を導入し，Molien の定理を応用することで colored design の存在性を導くことができた.

今後の課題として,

1. 他の $\mathbb{F}_q$ 符号からどのような colored design が得られるかを考察すること,

2. 一般化 design および 一般化 colored design を符号から構成すること，
3. Jacobi 多項式と Jacobi 形式の関係を一般化 Jacobi 多項式において拡張すること，
4. 論文 [5] にて調和 Tutte 多項式を導入したが，これを一般化して Jacobi–Tutte 多項式，Jacobi–chromatic 多項式を導入すること，

などが挙げられる．

最後になりますが，講演の機会をいただいた世話人の栗原大武先生，島倉裕樹先生，田上真先生，中空大幸先生，宗政昭弘先生に感謝申し上げます．

参考文献

[1] A. Bonnecaze, B. Mourrain, and P. Solé, Jacobi polynomials, type II codes, and designs. *Des. Codes Cryptogr.* **16** (1999), no. 3, 215–234.

[2] A. Bonnecaze, E. Rains, and P. Solé, 3-colored 5-designs and $\mathbb{Z}_4$-codes. *J. Statist. Plann. Inference* **86** (2000), no. 2, 349–368.

[3] A. Bonnecaze, P. Solé, and P. Udaya, Tricolore 3-designs in type III codes. *Discrete Math.* **241** (2001), no. 1-3, 129–138.

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

[5] T. Britz, H.S. Chakraborty, R.Ishikawa, and T. Miezaki, Harmonic Tutte polynomials of matroids II, submitted to *Des. Codes Cryptogr.*

[6] H.S. Chakraborty, T. Miezaki, M. Oura, and Y. Tanaka, Jacobi polynomials and design theory I, to appear in *Discrete Math.*

[7] H.S. Chakraborty, R. Ishikawa, and Y. Tanaka, Jacobi polynomials and design theory II, submitted to *Discrete Math.*

[8] M. Ozeki, On the notion of Jacobi polynomials for codes, *Math. Proc. Cambridge Philos. Soc.* **121** (1) (1997) 15–30.

[9] Wolfram Research, Inc., Mathematica, Version 11.2, Champaign, IL (2017).

Jacobi polynomials and harmonic weight enumerators of the first-order Reed–Muller codes and the extended Hamming codes

宗政　昭弘
(三枝崎剛氏との共同研究)

第 39 回代数的組合せ論シンポジウム

1　序

まず，講演タイトルにある用語について説明する。m を正の整数とし，$V = \mathbb{F}_2^m$ を 2 元体 $\mathbb{F}_2$ 上の m 次元ベクトル空間とする。**First-order Reed–Muller code** $RM(1,m)$ は，次で定義される長さ 2^m，次元 $m+1$ の線形符号である。

$$RM(1,m) = \{(\lambda(x)+b)_{x\in V} \mid \lambda \in V^*,\ b \in \mathbb{F}_2\} \subseteq \mathbb{F}_2^V$$

ただし，$V^* = \mathrm{Hom}(V, \mathbb{F}_2)$ は V の双対空間である。容易にわかるように，$RM(1,m)$ の符号語のうち重みが長さのちょうど半分，つまり 2^{m-1} となるようなもののサポートは V のアフィン超平面である。それ以外の符号語は 0 と all-one ベクトルしかないことから，$RM(1,m)$ の重み枚挙多項式は

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

である。

より一般に，単に**符号**とは $\mathbb{F}_2^n$ の線形部分空間を指すこととする。また，整数 $0 \le \ell \le n$ に対して

$$C_\ell = \{c \in C \mid \mathrm{wt}(c) = \ell\},$$
$$\mathcal{B}(C_\ell) = \{\mathrm{supp}(c) \mid c \in C_\ell\}.$$

と定義する。したがって特に $C = RM(1,m)$ (長さは $n = 2^m$) に対しては

$\mathcal{B}(C_{2^{m-1}})$ は $V = \mathbb{F}_2^m$ のアフィン超平面全体の集合

となる。よく知られているように，この集合は 3-**デザイン** の **ブロック** の集合になっている。

ここで，Ω を有限集合，$\binom{\Omega}{k}$ を Ω の k 点部分集合全体の族とするとき，部分集合 $\mathcal{B} \subseteq \binom{\Omega}{k}$ が t-**デザイン**の **ブロック**の集合であるとは，Ω の任意の t 点がある一定数個の $\mathcal{B}$ のメンバーに含まれているときをいう。もし $\mathcal{B}(C_\ell)$ が t-デザインのブロックの集合であるとき，単に C_ℓ は t-デザインを**サポート**する，ということにする。

一般に，長さ n の符号 C の**双対符号**とは

$$C^\perp = \{y \in \mathbb{F}_2^n \mid (x, y) = 0 \text{ for all } x \in C\}$$

で定義される。First order Reed–Muller code $RM(1, m)$ の双対符号 $RM(1, m)^\perp$ は**拡張ハミング符号** として知られている。この事実を利用して，拡張ハミング符号の重み枚挙多項式が計算できることはよく知られている。それは次の MacWilliams 恒等式を利用できることによる。

$$\sum_{c \in C^\perp} x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} = \frac{1}{|C|} \sum_{c \in C} (x+y)^{n-\mathrm{wt}(c)} (x-y)^{\mathrm{wt}(c)}.$$

符号とデザインの関係については，次の定理が有名である。

定理 1 (Assmus–Mattson [1])**.** C を長さ n の符号とし，

$$d^\perp = C^\perp \text{ の最小重み}$$

とする。もし $\{1, 2, \ldots, n-t\}$ の中に C の符号語の重みが高々 $d^\perp - t$ 個しかないとすると，$C_\ell = \emptyset$ でない限りは C_ℓ は t-デザインをサポートする。

上記の定理 1 を $n = 2^m, C = RM(1, m), t = 3$ として適用する。$d^\perp$ は拡張ハミング符号の最小重みで，それは 4 であることはよく知られているので $d^\perp - t = 1$ である。実際，$\{1, 2, \ldots, n-t\} = \{1, 2, \ldots, 2^m - 3\}$ の中に C の符号語の重みは 2^{m-1} のみである ((1) より) から，定理 1 の仮定がみたされ，$C_\ell = \emptyset$ でない限りは C_ℓ は 3-デザインをサポートする。

ここで，定理の結論は $C_\ell = \emptyset$ でない限りは ℓ には依存しないが，Miezaki–Nakasora [6] によって，符号 $C, t < t', \ell \neq \ell'$ で C_ℓ は t-デザインしかサポートしないのに $C_{\ell'}$ は t'-デザインをサポートする，という例が見出されている。このことは，定理 1 がデザインの強さとして最も強いものをいつも結論として出しているわけではないことを意味している。

この講演では，$C = RM(1, m), RM(1, m)^\perp$ に対して，$C_\ell \neq \emptyset$ である限りは 3-デザインをサポートするものの，いかなる場合も 4-デザインをサポートしないことを Jacobi 多項式を利用した方法と調和重み枚挙多項式を利用した方法の 2 週類の方法で示すことができたことを報告する。

2　符号の Jacobi 多項式

C を長さ n の符号とし，$T \subseteq [n] = \{1, \ldots, n\}$ とする。C の T に関する **Jacobi 多項式**とは

$$J_{C,T}(w,z,x,y) = \sum_{c \in C} w^{m_0(c)} z^{m_1(c)} x^{n_0(c)} y^{n_1(c)}, \text{ ただし}$$

$$\begin{aligned} m_0(c) &= |\{j \in T \mid c_j = 0\}|, \\ m_1(c) &= |\{j \in T \mid c_j = 1\}|, \\ n_0(c) &= |\{j \in [n] \setminus T \mid c_j = 0\}|, \\ n_1(c) &= |\{j \in [n] \setminus T \mid c_j = 1\}|. \end{aligned}$$

で定義される。m_0, m_1, n_0, n_1 の意味は以下の通り。

$$\begin{array}{cc|cc} [n] & & T & [n] \setminus T \\ c & & \underbrace{0\cdots0}_{m_0(c)}\ \underbrace{1\cdots1}_{m_1(c)} & \underbrace{0\cdots0}_{n_0(c)}\ \underbrace{1\cdots1}_{n_1(c)} \end{array}$$

$|T| = t$ であるとき，$J_{C,T}$ における $z^t x^{n-\ell} y^{\ell-t}$ の係数は，T をサポートに含むような重み ℓ の符号語の個数であるので，これが $T \in \binom{[n]}{t}$ について一定であることが，C_ℓ が t-デザインをサポートすることと必要十分である。

次の定理では，$C = RM(1,m)$ の 2^n 個の座標の集合が $V = \mathbb{F}_2^m$ であったことを思い出す必要がある。C はベクトル空間 V の平行移動で不変であるから，次の定理において座標の部分集合 T は，$0 \in T$ となるもののみを考えれば十分であることに注意しておく。

定理 2. m を正の整数とし，$C = RM(1,m), T = \{0, u_1, u_2, u_3\} \in \binom{V}{4}$ とすると

(i) $u_1 + u_2 \neq u_3$ ならば

$$\begin{aligned} J_{C,T}(w,z,x,y) = {} & (2^{m-3}-1)(z^4 x^{2^{m-1}} y^{2^{m-1}-4} + w^4 x^{2^{m-1}-4} y^{2^{m-1}}) \\ & + 2^{m-1}(w^3 z x^{2^{m-1}-3} y^{2^{m-1}-1} + w z^3 x^{2^{m-1}-1} y^{2^{m-1}-3}) \\ & + 3 \cdot 2^{m-2} w^2 z^2 x^{2^{m-1}-2} y^{2^{m-1}-2} \\ & + w^4 x^{2^m-4} + z^4 y^{2^m-4}. \end{aligned}$$

(ii) $u_1 + u_2 = u_3$ ならば

$$\begin{aligned} J_{C,T}(w,z,x,y) = {} & (2^{m-2}-1)(z^4 x^{2^{m-1}} y^{2^{m-1}-4} + w^4 x^{2^{m-1}-4} y^{2^{m-1}}) \\ & + 3 \cdot 2^{m-1} w^2 z^2 x^{2^{m-1}-2} y^{2^{m-1}-2} \\ & + w^4 x^{2^m-4} + z^4 y^{2^m-4}. \end{aligned}$$

さて，$C = RM(1,m)$ に対して，$C_{2^{m-1}}$ が 4-デザインをサポートするかについては，$J_{C,T}$ における $z^4 x^{2^{m-1}} y^{2^{m-1}-4}$ の係数を見る必要がある。

$$\begin{array}{cc|cc} & & T & [n]\setminus T \\ \hline [n] & & \underbrace{1\cdots1}_{} & \underbrace{0\cdots0}_{}\ \underbrace{1\cdots1}_{} \\ c & & 4 & 2^{m-1}\ \ 2^{m-1}-4 \\ & & z & x\ \ y \end{array}$$

つまり，それが $T \in \binom{[n]}{4}$ をサポートに含むような重み 2^{m-1} の符号語の個数である。定理 2 によれば $T = \{0, u_1, u_2, u_3\}$ に対して

$$J_{C,T} = \begin{cases} (2^{m-3}-1)z^4 x^{2^{m-1}} y^{2^{m-1}-4} + \cdots & \text{if } u_1+u_2 \neq u_3, \\ (2^{m-2}-1)z^4 x^{2^{m-1}} y^{2^{m-1}-4} + \cdots & \text{if } u_1+u_2 = u_3 \end{cases} \tag{2}$$

となっているので，これは T の取り方に依存する。したがって $C_{2^{m-1}}$ は決して 4-デザインをサポートしない。

次に，この根拠になっている定理 2 の部分 (2) についてのみ，証明を与える。定理 2 の完全な証明は [5] を参照されたい。まず，$C = RM(1,m)$ を記述し直すと

$$\begin{aligned} C &= \{(\lambda(x)+b)_{x\in V} \mid \lambda \in V^*,\ b \in \mathbb{F}_2\} \\ &= V^* \cup (V^* + \mathbf{1}) \\ &= \{0\} \cup \{\mathbf{1}\} \cup \underbrace{(V^* \setminus \{0\}) \cup ((V^*+\mathbf{1}) \setminus \{\mathbf{1}\})}_{\text{重み } 2^{m-1}}. \end{aligned}$$

となるので，$J_{C,T}$ における $z^4 x^{2^{m-1}} y^{2^{m-1}-4}$ の係数は

$$\begin{aligned} &\#\{c \in C_{2^{m-1}} \mid \mathrm{supp}(c) \supseteq T\} \\ &= \#\{c \in (V^* \setminus \{0\}) \cup ((V^*+\mathbf{1}) \setminus \{\mathbf{1}\}) \mid \mathrm{supp}(c) \supseteq T\} \\ &= \#\{c \in (V^*+\mathbf{1}) \setminus \{\mathbf{1}\} \mid \mathrm{supp}(c) \supseteq T\} \\ &= \#\{c' \in V^* \setminus \{0\} \mid \mathrm{supp}(c') \cap T = \emptyset\} \\ &= \#\{c' \in V^* \setminus \{0\} \mid \mathrm{Ker}(c') \supseteq T\} \\ &= \#\{W \in \begin{bmatrix} V \\ m-1 \end{bmatrix} \mid W \supseteq T\} \\ &= 2^{m-\dim\langle T\rangle} - 1. \end{aligned}$$

よって (2) が示せた。

次に，拡張ハミング符号 $C^\perp = RM(1,m)^\perp$ のサポートするデザインを調べるために，Ozeki による MacWilliams 恒等式の類似に言及する。

定理 3 (Ozeki [7]). C を長さ n の符号とし，$T \subseteq [n]$ とすると，

$$J_{C^\perp,T}(w,z,x,y) = \frac{1}{|C|} J_{C,T}(w+z, w-z, x+y, x-y).$$

$C = RM(1,m), T \in \binom{V}{4}$ に対して定理 2 で $J_{C,T}$ がすでにわかっているので，定理 3 によって $J_{C^\perp,T}$ が計算できる。その 2 つの多項式において $z^4 x^{2^{m-1}} y^{2^{m-1}-4}$ の係数が定理 2 にある 2 通りの T に対して異なっていることが確認できれば，$C_\ell^\perp$ が 4-デザインをサポートしないことがわかるのである。

3 調和重み枚挙多項式

整数 $0 \le k \le n$ に対して，関数 $f\colon \binom{[n]}{k} \to \mathbb{R}$ が**調和**関数であるとは，

$$\forall y \in \binom{[n]}{k-1}, \sum_{\substack{x \in \binom{[n]}{k} \\ x \supseteq y}} f(x) = 0$$

が成り立つときをいう。調和関数全体の集合を次で表す。

$$\mathrm{Harm}_k = \{ f\colon \binom{[n]}{k} \to \mathbb{R} \mid f \text{ は調和関数} \}.$$

調和関数 $f\colon \binom{[n]}{k} \to \mathbb{R}$ の定義域を拡張して次の $\tilde{f}$ を定義する。

$$\begin{array}{rcl} \tilde{f}\colon 2^{[n]} & \to & \mathbb{R} \\ u & \mapsto & \sum_{\substack{x \in \binom{[n]}{k} \\ x \subseteq u}} f(x) \end{array}$$

ここで $2^{[n]}$ は $[n]$ のべき集合を表す。

長さ n の符号 C と，調和関数 $f\colon \binom{[n]}{k} \to \mathbb{R}$ に対して，f に関する C の**調和重み枚挙多項式** $w_{C,f}$ は次で定義される。

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

定理 4 (Delsarte [4]). 上記の記号の下，$0 \le \ell \le n$ とすると，C_ℓ が t-デザインをサポートする必要十分条件は任意の $f \in \mathrm{Harm}_k, 1 \le k \le t$ に対して $w_{C,f}(x,y)$ における $x^{n-\ell} y^\ell$ の係数

$$\sum_{c \in C_\ell} \tilde{f}(\mathrm{supp}(c))$$

が 0 となることである。

さて，定理 4 を $C = RM(1,m)$ に適用するために，$U \subseteq V = \mathbb{F}_2^m$ を 3 次元部分空間とする。すると， $C = RM(1,m)$ を座標の集合 U に制限して得られる符号は $RM(1,3)$ に同型であり，これはその双対符号でもある長さ 8 の拡張ハミング符号とも同型である。

定理 5. $f \in \mathrm{Harm}_k$ を，$\binom{V}{k} \setminus \binom{U}{k}$ の上で $f = 0$ をみたす調和関数とする。このとき，$C = RM(1,m)$ に対して

$$w_{C,f}(x,y) = 2^{m-3} x^{2^{m-1}} y^{2^{m-1}} \sum_{\substack{a \in H_8 \\ \mathrm{wt}(a)=4}} \tilde{f}(a)$$

が成り立つ。

我々の目標は，$C_{2^{m-1}}$ が 4-デザインをサポートしないことを示すことである。そのためには $f \in \mathrm{Harm}_4$ をとる必要があるが，その構成のために

$$\mathcal{B} = \{\mathrm{supp}(z) \mid z \in H_8,\ \mathrm{wt}(z) = 4\}$$

を考える。拡張ハミング符号 H_8 において，$(H_8)_4 = RM(1,3)_4$ は 3-デザインをサポートするので，$\mathcal{B}$ は 3-デザインのブロックの集合である。実際，任意の $y \in \binom{U}{3}$ に対して

$$\sum_{\substack{x \in \binom{U}{4} \\ x \supseteq y}} 1_{\mathcal{B}}(x) = |\{x \in \mathcal{B} \mid x \supseteq y\}| = 1$$

が成り立つ。同じことが $\mathcal{B}$ を $\mathcal{B}^\tau$ で置き換えても成り立つ。ただし τ は U の 2 つの座標を入れ替える互換である。これらのことから

$$f = 1_{\mathcal{B}} - 1_{\mathcal{B}^\tau} \tag{3}$$

は調和多項式であることがわかる，すなわち $f \in \mathrm{Harm}_4$ であり，さらに定理 5 の仮定をみたす。$|\mathcal{B} \cap \mathcal{B}^\tau| = 6$ より，この f に対して

$$w_{C,f}(x,y) = 2^{m-3} x^{2m-1} y^{2m-1} |\mathcal{B} \setminus \mathcal{B}^\tau| = 2^m x^{2m-1} y^{2m-1}$$

となるので，定理 4 より $C_{2^{m-1}}$ は 4-デザインをサポートしない。

最後に，$C^\perp = RM(1,m)^\perp$ についても，すべての重みで 4-デザインをサポートしないことを調和重み枚挙多項式を使って示す。Jacobi 多項式の場合と同様に，MacWilliams 恒等式の類似が必要になる。

定理 6 (Bachoc [2])**.** C を長さ n の符号とし，$f \in \mathrm{Harm}_k$ とする。このとき

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

と書けて，$Z_{C,f}$ は $n-2k$ 次斉次多項式で

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

をみたす。

$C = RM(1,m)$ とすると，(3) で定義された f に対して定理 5 で $w_{C,f}$ がすでにわかっているので，定理 6 によって $w_{C^\perp,f}$ が計算できる。$w_{C^\perp,f}$ の係数が $C_\ell^\perp \neq \emptyset$ なる $0 < \ell < n$ すべてについて 0 でないことを確かめることにより，拡張ハミング符号 $C^\perp$ に対して $C_\ell^\perp$ が 4-デザインをサポートしないことがわかるのである。

参考文献

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

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

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

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

[5] T. Miezaki and A. Munemasa, Jacobi polynomials and harmonic weight enumerators of the first-order Reed–Muller codes and the extended Hamming codes, arXiv:2303.16349, to appear in *Des. Codes Cryptogr.*

[6] T. Miezaki and H. Nakasora, The support designs of the triply even binary codes of length 48, *J. Combin. Designs*, **27** (2019), 673–681.

[7] M. Ozeki, On the notion of Jacobi polynomials for codes. *Math. Proc. Cambridge Philos. Soc.* **121** (1997), no. 1, 15–30.

Construction and Characterization of LCD Codes

石塚 慶太 *

概 要

LCD 符号は，2010 年代の後半から脚光を浴び始めた比較的新しい符号のクラスであり，暗号理論や量子符号理論への応用が知られている．本稿では，LCD 符号の基本的性質や先行研究を，自身の研究とともに紹介する．

1 線形符号の構成と分類

この節では，LCD 符号の導入に必要な，符号理論の基本的な事実を説明する．

1.1 線形符号

q を素数べきとして，$\mathbb{F}_q$ で位数 q の有限体を表す．$[n,k]_q$ 符号とは，$\mathbb{F}_q^n$ の k 次元部分空間である．$[n,k]_q$ 符号は $\mathbb{F}_q$ 上の $[n,k]$ 符号とも呼ばれる．パラメータ n,k はそれぞれ，符号の長さ，符号の次元と呼ばれる．ベクトル $x=(x_1,x_2,\ldots,x_n)\in\mathbb{F}_q^n$ のハミング重みは，$\mathrm{wt}(x)=|\{i\mid x_i\neq 0\}|$ である．符号 C の最小重みは $d(C)=\min\{\mathrm{wt}(x)\mid x\in C,\ x\neq \mathbf{0}_n\}$ である．最小重みが d である $[n,k]_q$ 符号を，$[n,k,d]_q$ 符号と書く．

1.2 基本的問題 1：構成

パラメータ n,k,q に対して，$[n,k]_q$ 符号は複数存在する．最も大きな最小重みをもつ $[n,k]_q$ 符号を optimal な符号という．optimal な符号は，最小重みが最大であることから数学的に興味深い上に，情報通信への応用上も有用であることが知られている．そのために，optimal な符号を具体的に求めることが符号理論の基本的な問題の一つとなっている．

1.3 基本的問題 2：分類

非同値な符号の個数を求める研究を分類という．ここで，符号 C,C' が同値であるとは，ある単項行列 M が存在して $C'=CM=\{cM\mid c\in C\}$ であることをいう．分類の研究は，optimal な符号のみを対象に行う場合が多い．この理由は，optimal な符号が特に興味深いことと，optimal の制約を課さない場合は列挙が不可能なほどに符号の個数が多いことの 2 つが考えられる．

*東北大学大学院情報科学研究科（〒 980-8579 宮城県仙台市青葉区荒巻字青葉 6 番 3 号 09，E-mail: keita.ishizuka.p5@dc.tohoku.ac.jp）

2 LCD 符号とは

2.1 定義

定義 2.1. $[n,k]_q$ 符号 C の双対符号は $C^\perp = \{x \in \mathbb{F}_q^n \mid (x,y) = \sum_{i=1}^n x_i y_i = 0 \text{ for all } y \in C\}$ で定義される．

双対符号とは C の直交空間である．実数上のベクトル空間の直交空間は補空間である．一方，有限体は正標数を持つために，双対符号は必ずしも補空間にならない．双対符号が補空間であるような符号が LCD 符号である．

例 2.2. $C^\perp$ が補空間でない符号 C の例を挙げる．$C = \{(0,0),(1,1)\}$ は $[2,1]_2$ 符号である．$C^\perp = \{(0,0),(1,1)\}$ なので，$C = C^\perp$ である．

定義 2.3. $[n,k]_q$ 符号 C が $C \cap C^\perp = \{\mathbf{0}_n\}$ を満たす時，C を LCD 符号（linear complementary dual code）と呼ぶ．

$\mathbb{F}_{q^2}^n$ に属するベクトル x, y のエルミート内積は $(x,y)_h = \sum_{i=1}^n x_i y_i^q$ である．標準内積の代わりにエルミート内積を用いて，エルミート双対符号およびエルミート LCD 符号が定義される．

定義 2.4. $[n,k]_{q^2}$ 符号 C のエルミート双対符号は $C^{\perp h} = \{x \in \mathbb{F}_{q^2}^n \mid (x,y)_h = \sum_{i=1}^n x_i y_i^q = 0 \text{ for all } y \in C\}$ で定義される．

定義 2.5. $[n,k]_{q^2}$ 符号 C が $C \cap C^{\perp h} = \{\mathbf{0}_n\}$ を満たす時，C をエルミート LCD 符号と呼ぶ．

2.2 歴史

LCD 符号は 1992 年に導入された [12] が，盛んに研究がなされるようになったのは 2010 年代後半である．以下，LCD 符号の重要な先行研究を述べる．LCD 符号は，Massey [12] によって定義された．Carlet, Guilley [2] によって，$\mathbb{F}_2$ 上の LCD 符号は暗号理論に応用できることが示された．Lu, Li, Guo, Fu [11] によって，$\mathbb{F}_4$ 上のエルミート LCD 符号はある種の量子符号の構成に役立つことが示された．Carlet, Mesnager, Tang, Qi, Pellikaan [3] による以下の定理は特に重要である．

定理 2.6. (i) $q > 3$ について，$\mathbb{F}_q$ 上の任意の符号は LCD 符号に同値である．

(ii) $q > 2$ について，$\mathbb{F}_{q^2}$ 上の任意の符号はエルミート LCD 符号に同値である．

2.3 基本的性質

符号の基底を行ベクトルに並べた行列を，符号の生成行列という．LCD 符号については，Massey [12] による以下の特徴づけが基本的である．この定理に基づいて，LCD 符号の研究は生成行列に帰着させて行うことが多い．

定理 2.7. C を $[n,k]_q$ 符号とする．以下は同値である：

(i) C は LCD 符号である．

(ii) $C \oplus C^\perp = \mathbb{F}_q^n$.

(iii) $\det GG^T \neq 0$．ただし G は C の生成行列．

$\mathbb{F}_{q^2}$ 上の行列 G の転置行列及び共役行列をそれぞれ G^T 及び $\overline{G}$ で表す．エルミート LCD 符号について 定理 2.7 と同様の結果が成立する [4].

定理 2.8. C を $[n,k]_{q^2}$ 符号とする．以下は同値である：

(i) C はエルミート LCD 符号である．

(ii) $C \oplus C^{\perp h} = \mathbb{F}_{q^2}^n$.

(iii) $\det G\overline{G}^T \neq 0$. ただし G は C の生成行列.

2.4 self-dual 符号との関係

$C = C^{\perp}$ なる符号 C を self-dual 符号という．self-dual 符号は，組合せ論の他の分野との関連が多数示されている重要な符号である．LCD 符号，self-dual 符号はそれぞれ，$C \cap C^{\perp}$ の次元が最小，最大の符号である．$C \cap C^{\perp}$ は符号の Hull と呼ばれ，Hull(C) で表記される．Hull に着目して LCD 符号と self-dual 符号を関連付ける研究として， [6] がある．

3 LCD 符号の punctured 符号と shortened 符号について

この節では，LCD 符号についての研究内容を紹介する．LCD 符号の punctured 符号及び shortened 符号についての先行研究に基づく研究であるので，punctured 符号及び shortened 符号の説明，先行研究の説明を行ってから自身の結果を述べる．

3.1 punctured 符号及び shortened 符号

C を $\mathbb{F}_q$ 上の $[n,k]$ 符号，$T \subseteq \{1,2,\ldots,n\}$ とする．全ての $i \in T$ について C の第 i 成分を削除する操作を C の T についての puncture という．その結果得られる符号は C の T についての punctured 符号と呼ばれ，C^T で表される．$C(T) = \{(c_1,c_2,\ldots,c_n) \in C \mid c_i = 0 \text{ for all } i \in T\}$ は C の部分空間である．$C(T)$ を T について puncture した結果得られる符号は，C の T についての shortened 符号と呼ばれ，C_T で表される．$T = \{i\}$ の場合は，$C^{\{i\}}$ 及び $C_{\{i\}}$ をそれぞれ C^i 及び C_i と略記する．puncture 及び shorten は，符号に対する基本的かつ重要な操作である．例えば，Assmus–Mattson の定理の証明に，punctured 符号が用いられている．

3.2 Bouyuklieva による先行研究

Bouyuklieva [1] は $\mathbb{F}_2$ 上の LCD 符号の punctured 符号及び shortened 符号について，以下のような特徴づけを行った.

定理 3.1. C は $\mathbb{F}_2$ 上の $[n,k]$ LCD 符号で，$d(C), d(C^{\perp}) \geq 2$ を満たすとする．任意の $1 \leq i \leq n$ について，C^i または C_i のどちらか一方のみが LCD 符号である.

定理 3.2. C は $\mathbb{F}_2$ 上の $[n,k]$ LCD 符号で，$d(C), d(C^{\perp}) \geq 2$ を満たすとする．C が even 符号であるとき，かつその時に限り，任意の $1 \leq i \leq n$ について C^i が LCD 符号である.

定理 3.3. C は $\mathbb{F}_2$ 上の $[n,k]$ LCD 符号で，$d(C), d(C^{\perp}) \geq 2$ を満たすとする．C が odd 符号かつ $\mathbf{1}_n \in C$ であるとき，かつその時に限り，任意の $1 \leq i \leq n$ について C_i が LCD 符号である.

定理の主張において，$d(C), d(C^{\perp}) \geq 2$ という仮定が不自然に思われるかもしれない．しかし，以下の理由から，この仮定は自然なものである：$d(C^{\perp}) = 1$ であるような符号 C は，任意のベクトル $(c_1, \ldots, c_n) \in C$ について $c_i = 0$ であるような座標 i を含むことが知られている．そのような符号は，常に 0 であるような座標を含まない符号に座標を添加して得られるために，$d(C^{\perp}) = 1$ なる符号 C を考察の対象から除外しても問題はない．C は $C^{\perp}$ の双対符号なので，同様の議論から $d(C) = 1$ なる符号 C を考察の対象から除外しても問題ない．

3.3 研究内容

以下のような問いをモチベーションとして研究を行い，次の結果を得た [8].

(i) $\mathbb{F}_2$ 以外の有限体上の LCD 符号で [1] と同様の結果は成り立つのか.

(ii) エルミート LCD 符号で [1] と同様の結果が成り立つのか.

定理 3.4. C は $\mathbb{F}_4$ 上の $[n, k]$ エルミート LCD 符号で，$d(C), d(C^{\perp_h}) \geq 2$ を満たすとする．任意の $1 \leq i \leq n$ について，C^i または C_i のどちらか一方のみがエルミート LCD 符号である.

補題 3.5 (Ken Saito)**.** C を $\mathbb{F}_4$ 上の $[n, k]$ エルミート LCD 符号とする．C の生成行列 G で，$G\overline{G}^T = I_k$ を満たすものが存在する.

定理 3.6. C は $\mathbb{F}_4$ 上の $[n, k]$ エルミート LCD 符号で，$d(C), d(C^{\perp_h}) \geq 2$ を満たすとする．G を C の生成行列で $G\overline{G}^T = I_k$ を満たすようにとり，l_i で G の第 i 列を表す．C^i がエルミート LCD 符号である時，かつその時に限り，$\mathrm{wt}(l_i)$ は偶数である.

系 3.7. C は $\mathbb{F}_4$ 上の $[n, k]$ エルミート LCD 符号で，$d(C), d(C^{\perp_h}) \geq 2$ を満たすとする．G を C の生成行列で $G\overline{G}^T = I_k$ を満たすようにとり，l_i で G の第 i 列を表す．C_i がエルミート LCD 符号である時，かつその時に限り，$\mathrm{wt}(l_i)$ は奇数である.

補題 3.5 は Saito (private communication, Dec. 31, 2021) による．補題 3.5 を用いて，定理 3.6 が示される．系 3.7 は，定理 3.4 と 定理 3.6 から直ちに従う.

4 今後の研究の方向

この節では，LCD 符号についての予想や研究課題等を述べる.

4.1 構成と分類の研究

定理 2.6 により，$\mathbb{F}_2, \mathbb{F}_3$ 上の LCD 符号及び $\mathbb{F}_4$ 上のエルミート LCD 符号のみが一般の線形符号と異なる同値類を持つことがわかっている．また，$\mathbb{F}_2$ 上の LCD 符号及び $\mathbb{F}_4$ 上のエルミート LCD 符号はそれぞれ，暗号理論及び量子符号理論への応用が示されている [3, 11]. よって，特に $\mathbb{F}_2$ 上の LCD 符号及び $\mathbb{F}_4$ 上のエルミート LCD 符号の構成及び分類が盛んに行われている．自身の構成と分類の研究として，[7, 9, 10] を挙げる.

4.2 LCD 符号の最小重みに関する予想

$d(n,k) = \max\{d(C) \mid C : [n,k] \text{ LCD code over } \mathbb{F}_2\}$ と定義する．Bouyuklieva [1] は，以下の予想を立てた．

予想 4.1. 任意の $1 \leq k \leq n$ について，$d(n+1,k) = d(n,k)+1$ または $d(n+1,k) = d(n,k)$ が成立する．

[5] によれば，一般の線形符号においても上記の予想の反例は見つかっていない．そのため，一般の線形符号についても成立する命題かもしれない．しかし，一般の線形符号において成立することが，LCD 符号のみに限っても成り立つというのは興味深いと考えている．

参考文献

[1] S. Bouyuklieva, *Optimal binary LCD codes*, Des. Codes Cryptogr. **89** (2021), no. 11, 2445–2461. MR4321779

[2] C. Carlet and S. Guilley, *Complementary dual codes for counter-measures to side-channel attacks*, Adv. Math. Commun. **10** (2016), no. 1, 131–150. MR3471065

[3] C. Carlet, S. Mesnager, C. Tang, Y. Qi, and R. Pellikaan, *Linear codes over $\mathbb{F}_q$ are equivalent to LCD codes for $q > 3$*, IEEE Trans. Inform. Theory **64** (2018), no. 4, part 2, 3010–3017. MR3784604

[4] C. Güneri, B. Özkaya, and P. Solé, *Quasi-cyclic complementary dual codes*, Finite Fields Appl. **42** (2016), 67–80. MR3550383

[5] M. Grassl, *Bounds on the minimum distance of linear codes and quantum codes*. Available online at `http://codetables.de/`, Accessed on 2022-05-14.

[6] K. Guenda, S. Jitman, and T. A. Gulliver, *Constructions of good entanglement-assisted quantum error correcting codes*, Des. Codes Cryptogr. **86** (2018), no. 1, 121–136. MR3742836

[7] K. Ishizuka, *Classification of optimal quaternary Hermitian LCD codes of dimension 2*, J. Algebra Comb. Discrete Struct. Appl. **7** (2020), no. 3, 229–236. MR4221779

[8] K. Ishizuka, *Construction of quaternary hermitian lcd codes*, Cryptography and Communications **15** (2023), no. 2, 455–467.

[9] K. Ishizuka and K. Saito, *Construction for both self-dual codes and LCD codes*, Adv. Math. Commun. (2022). (to appear).

[10] K. Ishizuka and K. Saito, *On the existence of quaternary Hermitian LCD codes with H ermitian dual distance 1*, Discrete Math. **345** (2022), no. 2, Paper No. 112702, 3. MR4338405

[11] L. Lu, R. Li, L. Guo, and Q. Fu, *Maximal entanglement entanglement-assisted quantum codes constructed from linear codes*, Quantum Inf. Process. **14** (2015), no. 1, 165–182. MR3296312

[12] J. L. Massey, *Linear codes with complementary duals*, Discrete Math. **106/107** (1992), 337–342. MR1181930

The Delsarte theory for probability measures on compact homogeneous spaces

Akifumi Nakada*
D1, Mathematics Program,
Graduate School of Advanced Science and Engineering,
Hiroshima University

Abstract

Delsarte theory links coding theory and design theory as dual concepts through Fourier analysis. This theory provides a fundamental tool for studying codes and designs. This paper presents a formulation of Delsarte theory for probability measures. This paper is based on joint work with Takayuki Okuda (Hiroshima University).

1 Introduction to Delsarte theory for finite subsets

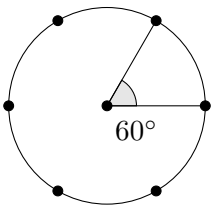
We present some well-known facts about the Delsarte theory for finite subsets on homogeneous spaces corresponding to the Gelfand pairs. The Delsarte theory links coding theory and design theory by spherical Fourier transforms. So, We also introduce coding theory and design theory.

1.1 Coding theory

In this paper, let M be the homogeneous space corresponding to a compact Gelfand pair (G, H), $\mathcal{I}$ be the orbit space of the diagonal action $G \curvearrowright M \times M$, $R\colon M \times M \to \mathcal{I}$ be the quotient map in topology and $i_0 \in \mathcal{I}$ be the diagonal set of $M \times M$.

For a non-empty finite subset $X \subset M$ and a subset $\mathcal{A} \subset \mathcal{I}$, if $R(X \times X) \subset \mathcal{A}$, then we call X an *$\mathcal{A}$-code*.

Example 1.1 (Regular hexagon)**.** Let G be the orthogonal group $O(2)$ in dimension 2 and H be $O(1)$. Then $M \cong S^1 \subset \mathbb{R}^2$, $\mathcal{I} = [-1, 1]$ and R is the inner product. And let $\mathcal{A} \coloneqq [-1, 1/2] \cup \{ 1 \}$ and X be the vertex set of the regular hexagon. Then X is an $\mathcal{A}$-code with the maximum cardinality.



* nakada-aki@hiroshima-u.ac.jp

1.2 Design theory

We denote by $C(M)$ the set of all continuous complex functions on M, and μ_M the pushforward of the probability Haar measure on G by the quotient map $G \to M$. We note that μ_M is a G-invariant probability Radon measure on M. The L^2-space on M with respect to μ_M is denoted by $L^2(M)$. It is well known that $C(M)$ can be realized as a dense subspace of $L^2(M)$ with respect to the L^2-norm.

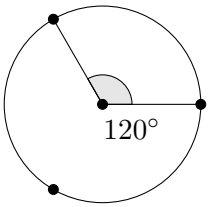
Throughout this paper, we define $\mathcal{J}$ as the set of all irreducible subrepresentations of the unitary regular G-representation $G \to U(L^2(M))$, and V_0 as the space of all constant complex functions on M. Then $V_0 \in \mathcal{J}$. The set $\mathcal{J}$ will be regarded as a discrete space. According to the Peter–Weyl theorem, for each $V \in \mathcal{J}$, the dimension of V is finite, and $V \subset C(M)$.

For a non-empty finite subset $X \subset M$ and a subset $\mathcal{T} \subset \mathcal{J}$ with $V_0 \in \mathcal{T}$, if

$$\int f \, d\mu_M = \frac{1}{\#X} \sum_{p \in X} f(p)$$

for all $V \in \mathcal{T}$ and $f \in V$, then we call X a *$\mathcal{T}$-design*.

Example 1.2 (Regular triangle)**.** Let $(G, H) \coloneqq (O(2), O(1))$. Then $M \cong S^1 \subset \mathbb{C}$, μ_M is the canonical probability measure and $\mathcal{J} = \{ V_n \coloneqq \langle z^n, \overline{z^n} \rangle_{\mathrm{lin}} \mid n \in \mathbb{Z}_{\geq 0} \}$. And let $\mathcal{T} \coloneqq \{ V_n \mid n = 0, 1, 2 \}$ and X be the vertex set of the regular triangle. Then X is a $\mathcal{T}$-design with the minimum cardinality.



1.3 Delsarte theory

Fix a non-empty finite subset $X \subset M$. First, we define the *$\mathcal{I}$-distribution* $a^X \in \mathbb{C}_{\mathcal{I}}$ of X as follows:

$$a_i^X \coloneqq \frac{\#R^{-1}(i) \cap X \times X}{\#X \times X} \quad (i \in \mathcal{I}),$$
$$a^X \coloneqq (a_i^X)_{i \in \mathcal{I}} \in \mathbb{C}_{\mathcal{I}}.$$

Where $\mathbb{C}_{\mathcal{I}}$ is the vector space generated by the set $\mathcal{I}$. Therefore, $(a_i^X)_i = 0$ for all but finitely many $i \in \mathcal{I}$.

Then, for a subset $\mathcal{A} \subset \mathcal{I}$, the following two conditions are equivalent:

(1) X is an $\mathcal{A}$-code,

(2) $a_i^X = 0$ for all $i \notin \mathcal{A}$.

This equivalence links coding theory and $\mathcal{I}$-distributions.

Second, we define the linear map μ_X as follows:

$$\mu_X \colon C(M) \to \mathbb{C}$$
$$f \mapsto \frac{1}{\#X} \sum_{p \in X} f(p).$$

And we define the $\mathcal{J}$-*distribution* $b^X \in C(\mathcal{J})$ of X as follows:

$$\begin{aligned} b^X \colon \mathcal{J} &\to \mathbb{C} \\ V &\mapsto b_V^X \coloneqq \|\mu_X \colon (V, \|-\|_2) \to \mathbb{C}\|_{\mathrm{op}}^2. \end{aligned}$$

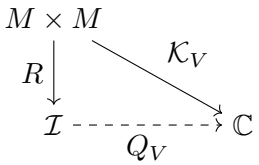
Then, for a subset $\mathcal{T} \subset \mathcal{J}$ with $V_0 \in \mathcal{T}$, the following two conditions are equivalent:

(1) X is a $\mathcal{T}$-design,

(2) $b_V^X = 0$ for all $V \in \mathcal{T} - \{ V_0 \}$.

This equivalence also links design theory and $\mathcal{J}$-distributions.

Third, We introduce the spherical Fourier transforms that link the $\mathcal{I}$ and $\mathcal{J}$-distributions. For each $V \in \mathcal{J}$, there exists a unique continuous map $Q_V \colon \mathcal{I} \to \mathbb{C}$ that makes the following diagram commutative, since the universality of quotient maps in topology.



We call this Q_V the *spherical function* for V. Using this, we define the *spherical Fourier transform* $\mathcal{F} \colon \mathbb{C}_{\mathcal{I}} \to C(\mathcal{J})$ as follows:

$$\begin{aligned} \mathcal{F}(a) \coloneqq \widehat{a} \colon \mathcal{J} &\to \mathbb{C} \\ V &\mapsto \sum_{i \in \mathcal{I}} a_i \cdot Q_V(i). \end{aligned}$$

Then $\mathcal{F}$ is a linear injection and the *MacWilliams identity* $\widehat{a^X} = b^X$ holds. To summarize the above, we link coding theory and design theory by the spherical Fourier transform.

And finally, We introduce the bound on the cardinality of X, called Delsarte's bound. If X is an $\mathcal{A}$-code and a $\mathcal{T}$-design, then for every feasible solution of the dual problem of the following linear programming problem, the bound on $a_{i_0}^X \in \mathbb{R}$ is obtained.

$$\begin{array}{cl} \text{Find a vector} & a \in \mathbb{C}_{\mathcal{I}}, \\ \text{that minimize or maximize} & a_{i_0}, \\ \text{subject to} & a \geq 0, \\ & a = 0 \text{ on } \mathcal{A}^c, \\ & \widehat{a} \geq 0, \\ & \widehat{a} = 0 \text{ on } \mathcal{T} - \{ V_0 \}, \\ & \widehat{a}(V_0) = 1. \end{array}$$

As a corollary, we obtain the bound on the cardinality of X since $a_{i_0}^X = 1/\#X$. The optimal bound obtained in this way is called *Delsarte's bound*.

2 Delsarte theory for probability measures

We generalize the Delsarte theory introduced above to probability measures. In this paper, the set of all positive unital bounded linear functionals on $C(M)$ with respect to the uniform norm is denoted by $\mathcal{P}(M)$, and we call an element in $\mathcal{P}(M)$ *probability measure* on M. It should be remarked that by Riesz–Markov–Kakutani representation theorem (see [16] for the details), $\mathcal{P}(M)$ can be identified with the set of all probability Radon measures on M.

2.1 Coding theory

Using the fact that the support $\operatorname{supp}\mu_X \subset M$ of measure μ_X coincides with X, we generalize the coding theory to probability measures in a natural way. Specifically, for a probability measure $\mu \in \mathcal{P}(M)$ and a subset $\mathcal{A} \subset \mathcal{I}$, if $R(\operatorname{supp}\mu \times \operatorname{supp}\mu) \subset \mathcal{A}$, then we call μ an *$\mathcal{A}$-code*.

2.2 Design theory

We also generalize the design theory to probability measures in a natural way. Specifically, for a probability measure $\mu \in \mathcal{P}(M)$ and a subset $\mathcal{T} \subset \mathcal{J}$ with $V_0 \in \mathcal{T}$, if $\mu_M(f) = \mu(f)$ for all $V \in \mathcal{T}$ and $f \in V$, then we call μ a *$\mathcal{T}$-design*.

2.3 Delsarte theory

Fix a probability measure $\mu \in \mathcal{P}(M)$. First, we define the *$\mathcal{I}$-distribution* $a^\mu \in \mathcal{P}(\mathcal{I})$ of μ by $a^\mu := R_*(\mu \otimes \mu)$ using product and pushforward of measures. Note that we have not defined an equivalent for a_i^X. This is because if a_i^X is generalized to a_i^μ in a natural way, $a_i^\mu = 0$ in most cases.

However, coding theory for probability measures and $\mathcal{I}$-distributions are linked by the following proposition:

Proposition 2.1. *For a subset $\mathcal{A} \subset \mathcal{I}$, the following two conditions are equivalent:*
(1) μ is an $\mathcal{A}$-code,
(2) $\operatorname{supp} a^\mu \subset \mathcal{A}$.

Second, we generalize the $\mathcal{J}$-distribution to the probability measure μ as follows:

$$\begin{aligned} b^\mu \colon \mathcal{J} &\to \mathbb{C} \\ V &\mapsto b_V^\mu := \|\mu \colon (V, \|-\|_2) \to \mathbb{C}\|_{\mathrm{op}}^2. \end{aligned}$$

Then design theory for probability measures and $\mathcal{J}$-distributions are also linked by the following proposition:

Proposition 2.2. *For a subset $\mathcal{T} \subset \mathcal{J}$ with $V_0 \in \mathcal{T}$, the following two conditions are equivalent:*
(1) μ is a $\mathcal{T}$-design,
(2) $\operatorname{supp} b^\mu \subset \mathcal{T}^c \cup \{ V_0 \}$.

Third, we also generalize the spherical Fourier transform to probability measures as follows:

$$\begin{aligned} \mathcal{F}(a) := \widehat{a} \colon \mathcal{J} &\to \mathbb{C} \\ V &\mapsto a(Q_V). \end{aligned}$$

Then $\mathcal{F} \colon \mathcal{P}(\mathcal{I}) \to C(\mathcal{J})$ is a linearly injection and the following main results are obtained:

Theorem 2.3 (MacWilliams identity)**.** $\widehat{a^\mu} = b^\mu$.

To summarize the above, we link coding theory and design theory for probability measures by the spherical Fourier transform.

And finally, we will consider the generalization of Delsarte's bound to probability measures. It is necessary to consider the "cardinality" of a measure. Thus, we will consider a real-valued

continuous function $\varphi \in C(\mathcal{I})$ and, if $a^\mu(\varphi) \neq 0$, we call $1/a^\mu(\varphi)$ the φ-cardinality of μ. Then the following proposition holds:

Proposition 2.4. *Let $X \subset M$ be a non-empty finite subset and $\varphi \in C(\mathcal{I})$ satisfy $\varphi(i_0) = 1$ and $\varphi^{-1}(0)^c \cap R(X \times X) = \{ i_0 \}$. Then the φ-cardinality of μ_X and the cardinality of X coincide.*

To describe Delsarte's bound, we fix our notations as below: the *spherical Fourier transform* $\widehat{\psi} \in C(\mathcal{J})$ of $\psi \in C(\mathcal{I})$ denotes $\widehat{\psi}(V) \coloneqq a^{\mu_M}(\psi \cdot \overline{Q_V})/\dim V$, the *transpose* $\psi^\top \in C(\mathcal{I})$ denotes $\psi^\top([p,q]) \coloneqq \psi([q,p])$ and $C^\top_{\mathbb{R}}(\mathcal{I})$ denotes $\left\{ \psi \in C(\mathcal{I}) \,\middle|\, \overline{\psi} = \psi = \psi^\top \right\}$. Then the other of the main results are obtained:

Theorem 2.5 (Delsarte's bound)**.** *Let $\varphi \in C^\top_{\mathbb{R}}(\mathcal{I})$. And we put*

$$
\begin{aligned}
S^c &\coloneqq \left\{ \psi \in C^\top_{\mathbb{R}}(\mathcal{I}) \cap \bigoplus_{V \in \mathcal{J}} \mathbb{C}Q_V \;\middle|\; \widehat{\psi} \geq 0 \text{ on } \mathcal{T}^c,\ \varphi - \psi \geq 0 \text{ on } \mathcal{A} \right\}, \\
S^d &\coloneqq \left\{ \psi \in C^\top_{\mathbb{R}}(\mathcal{I}) \cap \bigoplus_{V \in \mathcal{J}} \mathbb{C}Q_V \;\middle|\; \widehat{\psi} \leq 0 \text{ on } \mathcal{T}^c,\ \varphi - \psi \leq 0 \text{ on } \mathcal{A} \right\}, \\
c &\coloneqq \sup a^{\mu_M}(S^c), \\
d &\coloneqq \inf a^{\mu_M}(S^d).
\end{aligned}
$$

Then we have bounds $c \leq a^\mu(\varphi) \leq d$ for $\mu \in \mathcal{P}(M)$ that is an $\mathcal{A}$-code and a $\mathcal{T}$-design.

As a corollary, we obtain the bound on the φ-cardinality of μ. The optimal bound on $a^\mu(\varphi)$ obtained in this way is called *Delsarte's bound*.

3 Examples of 1-designs on the 2-dimensional sphere

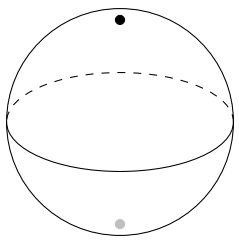
In this section, let $(G, H) \coloneqq (O(3), O(2))$. Then $M \cong S^2 \subset \mathbb{R}^3$, $\mathcal{I} = [-1, 1]$, R is the inner product,

$$
\begin{aligned}
\mathcal{J} &= \left\{ \mathrm{Harm}_n(S^2) \coloneqq \left\{ \begin{array}{l} \text{homogeneous harmonic polynomial} \\ \text{functions of degree } n \end{array} \right\} \,\middle|\, n \in \mathbb{Z}_{\geq 0} \right\} \\
&\cong \mathbb{Z}_{\geq 0}
\end{aligned}
$$

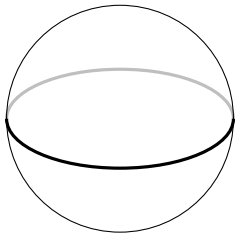
and Q_n is constant multiple of Legendre polynomials of degree n. In particular $Q_0(t) = 1$, $Q_1(t) = 3t$ ($t \in [-1, 1]$). And let $\mathcal{A} \coloneqq \mathcal{I}$, $\mathcal{T} \coloneqq \{ 0, 1 \} \subset \mathcal{J}$ and $\varphi(t) \coloneqq t/2 + 1/2$ ($t \in [-1, 1]$) $\in C(\mathcal{I})$.

According to Delsarte's bound, for any $\mu \in \mathcal{P}(M)$ that is an $\mathcal{A}$-code and a $\mathcal{T}$-design, φ-cardinality of μ is 2.

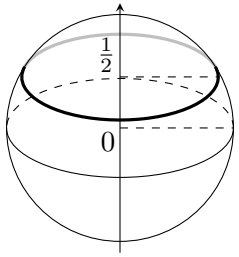
Example 3.1 (Antipodes)**.** Let $X \coloneqq \{ (1, 0, 0), (-1, 0, 0) \} \subset M$. Then $\mu_X \in \mathcal{P}(M)$ is an $\mathcal{A}$-code and a $\mathcal{T}$-design. In fact, φ-cardinality of μ_X is 2.



Example 3.2 (Great circle)**.** Let $\mu_0 \in \mathcal{P}(M)$ be the canonical probability measure on $\{ (0, \cos\theta, \sin\theta) \mid \theta \in \mathbb{R} \} \subset M$. Then μ_0 is an $\mathcal{A}$-code and a $\mathcal{T}$-design. In fact, φ-cardinality of μ_0 is 2.



Example 3.3 (Small circle)**.** Let $\mu_{1/2} \in \mathcal{P}(M)$ be the canonical probability measure on $\left\{ (1/2, \sqrt{3}/2\cos\theta, \sqrt{3}/2\sin\theta) \,\middle|\, \theta \in \mathbb{R} \right\} \subset M$. Then φ-cardinality of $\mu_{1/2}$ is $8/5 < 2$. In fact, $\mu_{1/2}$ is not a $\mathcal{T}$-design.



4 Summary

By replacing finite subsets with probability measures, we generalized coding theory, design theory and Delsarte theory to probability measures on homogeneous spaces corresponding to compact Gelfand pairs. Table 1 lists the corresponding terms that appear in Delsarte theory, both for finite subsets and probability measures.

Table 1 Correspondence of terms appearing in Delsarte theory

	Finite subset	Probability measure
Object	Finite subset X of M	Prob. measure μ on M
$\mathcal{A}$-code	$R(X \times X) \subset \mathcal{A}$	$R(\operatorname{supp}\mu \times \operatorname{supp}\mu) \subset \mathcal{A}$
$\mathcal{T}$-design	$\mu_M(f) = \mu_X(f)$	$\mu_M(f) = \mu(f)$
a_i^-	$\#R^{-1}(i) \cap X^2 / \#X^2$	$\times$
$\mathcal{I}$-distribution a^-	$(a_i^X)_{i\in\mathcal{I}} \in \mathbb{C}_{\mathcal{I}}$	$R_*(\mu \otimes \mu) \in \mathcal{P}(\mathcal{I})$
b_V^-	$\lVert \mu_X \colon V \to \mathbb{C} \rVert_{\mathrm{op}}^2$	$\lVert \mu \colon V \to \mathbb{C} \rVert_{\mathrm{op}}^2$
$\mathcal{J}$-distribution b^-	$V \mapsto b_V^X$	$V \mapsto b_V^\mu$
$\widehat{a}$	$V \mapsto \sum_{i\in\mathcal{I}} a_i \cdot Q_V(i)$	$V \mapsto a(Q_V)$
SFT $\mathcal{F}$	$\mathbb{C}_{\mathcal{I}} \to C(\mathcal{J})$	$\mathcal{P}(\mathcal{I}) \to C(\mathcal{J})$

Three problems remain. First, there is no $\varphi \in C(\mathcal{I})$ such that Delsarte's bound on the φ-cardinality are consistent with that on the normal cardinality. Second, φ is assumed to be a continuous function that takes values in the unit closed interval $[0, 1]$. We do not know what such a function means in terms of applications. Third, we do not know the good presentation of the image of the spherical Fourier transform $\mathcal{F} \colon \mathcal{P}(\mathcal{I}) \to C(\mathcal{J})$.

References

[1] C. Bachoc, E. Bannai and R. Coulangeon, *Codes and designs in Grassmannian spaces*, Discrete Math. **277**(2004), 15–28.

[2] C. Bachoc, R. Coulangeon and G. Nebe, *Designs in Grassmannian spaces and lattices*, J. Algebraic Combin. **16**(2002), 5–19.

[3] E. Bannai and E. Bannai, *A survey on spherical designs and algebraic combinatorics on spheres*, European J. Combin. **30**(2009), 1392–1425.

[4] E. Bannai and S. G. Hoggar, *On tight t-designs in compact symmetric spaces of rank one*, Proc. Japan Acad. Ser. A Math. Sci. **61**(1985), 78–82.

[5] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko and M. Viazovska, *The sphere packing problem in dimension 24*, Ann. of Math. (2) **185**(2017), 1017–1033.

[6] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. 1973.

[7] P. Delsarte, J. M. Goethals and J. J. Seidel, *Spherical codes and designs*, Geometriae Dedicata **6**(1977), 363–388.

[8] H. Kurihara and T. Okuda, *Great antipodal sets on complex Grassmannian manifolds as designs with the smallest cardinalities*, J. Algebra **559**(2020), 432–466.

[9] V. I. Levenshtein, *On bounds for packings in n-dimensional euclidean space*, Dokl. Akad. Nauk SSSR **245**(1979), 1299–1303.

[10] O. R. Musin, *The kissing number in four dimensions*, Ann. of Math. (2) **168**(2008), 1–32.

[11] L. Nachbin, *The Haar integral*, D. Van Nostrand Co., Inc., Princeton, N.J.-Toronto-London, 1965.

[12] Y. Nakata et al., *Quantum Circuits for Exact Unitary t-Designs and Applications to Higher-Order Randomized Benchmarking*, PRX Quantum **2**(2021), 030339.

[13] A. M. Odlyzko and N. J. A. Sloane, *New bounds on the number of unit spheres that can touch a unit sphere in n dimensions*, J. Combin. Theory Ser. A **26**(1979), 210–214.

[14] A. Roy, *Bounds for codes and designs in complex subspaces*, J. Algebraic Combin. **31**(2010), 1–32.

[15] A. Roy and A. J. Scott, *Unitary designs and codes*, Des. Codes Cryptogr. **53**(2009), 13–31.

[16] W. Rudin, *Real and complex analysis*, McGraw-Hill Book Co., New York, 1987.

[17] M. S. Viazovska, *The sphere packing problem in dimension 8*, Ann. of Math. (2) **185**(2017), 991–1015.

等質空間上の固有な群作用と符号理論の関係について

奥田 隆幸 (広島大学大学院先進理工系科学研究科)

Abstract. 本稿では等質集合上の符号理論に粗幾何学の視点を持ち込み, 等質空間上の群作用の固有性を符号理論の枠組みで言い換える試みを紹介する. 本稿は小川健翔氏 (広島大), 長屋拓暁氏 (広島大) との共同研究の内容に基づく.

1. 序

G を局所コンパクト群とし, 等質 G 空間 X を考える. G の離散部分群 Γ が等質 G 空間 X の不連続群 (discontinuous group) であるとは, Γ の X の作用が真性不連続 (properly discontinuous), つまり, 任意の $x \in X$ について, x のある近傍 C が存在して,

$$\{\gamma \in \Gamma \mid \gamma \cdot C \cap C \neq \emptyset\} = \{e\}$$

となることとする. ただし e は G の単位元を表す.

Γ が X の不連続群であるとき, 商写像 $\pi : X \to \Gamma\backslash X$ は Γ 主束, 特に正則被覆写像となる. このようにして得られる空間 $\Gamma\backslash X$ を等質 G 空間 X の Clifford–Klein 形とよぶ. 特に G がリー群である場合には, $\Gamma\backslash X$ は (G, X) 多様体と呼ばれる構造を持ち, X に定まる G 不変な局所幾何構造 (例えば正定値計量, 不定値計量, 複素構造, シンプレクティック構造など) を引き継ぐ. このような意味で Clifford–Klein 形は「X と同様な局所構造を持つ空間」であり, 不連続群論および Clifford–Klein 形の研究は幾何学における重要な研究テーマとなっている.

L を G の閉部分群 (離散とは限らない) であって, X への作用が固有 (proper) である, すなわち, 任意の X のコンパクト集合 C について, L の部分集合

$$L_C := \{l \in L \mid l \cdot C \cap C \neq \emptyset\}$$

がコンパクトになるものとする. このとき L の捩れのない離散部分群は必ず X の不連続群となる. したがって, このような L を探す研究は, X の不連続群を構成する有効な手法を提供する.

等質空間 X の各点の固定化部分群がコンパクトである場合には, X に自然な G 不変距離が定まることが多く, また G の任意の閉部分群 L が X に固有に作用するということもあり, X 上の不連続群論は古くから多くの研究がなされてきた. 代表的なものとしては, A. Borel による非コンパクトリーマン対称空間における余コンパクト不連続群の構

The author is supported by JSPS Grants-in-Aid for Scientific Research JP20K14310 an JP22H01124.

成や, 種数が 2 以上の閉リーマン面 (双曲平面のコンパクト Clifford–Klein 形とみなせる) の幾何構造の変形を司るタイヒミュラー空間の理論の華々しい成果などが挙げられる.

しかし等質空間 X の各点の固定化部分群が非コンパクトである場合には, 通常 X は G 不変な距離を持たない. また, G の非コンパクト閉部分群 L について, X への L の作用は固有であるとは限らないという難点がある. このような非コンパクトな固定化部分群を持つ等質空間上の不連続群論, Clifford–Klein 形および固有な群作用の系統的な研究は, 小林俊行氏による 1980 年代後半からの一連の仕事 ([7, 8, 9]) に端を発する. 詳細については小林氏による解説 [11, 12] を参照されたい.

一方で, 誤り訂正符号, 接吻数問題, 球充填問題などに代表される等質集合上の符号理論は, 組合せ論の重要な分野として発展を遂げてきた. 本稿の目的は, これまで別々の研究領域として発展してきた等質空間上の不連続群論と等質集合上の符号理論を, 粗幾何学の言葉を用いて結びつけることである. その第一歩として, 本稿では等質集合上の符号理論に粗幾何学の視点を持ち込み, 等質空間上の群作用の固有性を符号理論の枠組みで言い換える試みを紹介する.

2. 等質集合上の符号理論, 等質空間上の固有作用

本節では等質集合上の符号理論および等質空間上の固有な群作用の各種用語を定める.

2.1. 等質集合, 等質空間.

まず本稿で用いる “等質集合” および “等質空間” についての用語を定めよう.

以下, 群 G を固定する. M を集合とし, G の M への推移的な作用 $\rho : G \times M \to M$ を固定したとき, 本稿では組 (M, ρ) を等質 G 集合とよぶ. また各 $(g, p) \in G \times M$ について,

$$g \cdot_\rho p := \rho(g, p) \in M$$

と書く. M の各点 p について, G の部分群

$$G^p := \{g \in G \mid g \cdot_\rho p = p\}$$

を p における G の固定化部分群 (isotropy) とよぶ. 各 $p, q \in M$ について, それらの固定化部分群 G^p, G^q は G の内部自己同型により互いに共役であることに注意しておく.

また群 G の部分群 H を固定したとき, 剰余類集合 G/H は自然な意味で等質 G 集合とみなせ, この等質集合の各点における固定化部分群は, G の内部自己同型について H と共役な部分群となる. これより等質 G 集合を考えることと, G の部分群の共役類を考えることは (しかるべき意味で) 等価である.

以下 G が局所コンパクトなハウスドルフ位相群である場合を考える. 本稿では, M が局所コンパクトなハウスドルフ位相空間であり, 推移的な群作用 $\rho : G \times M \to M$ が連続であり, さらに各 $p \in M$ について

$$\pi_p : G \to M,\ g \mapsto g \cdot_\rho p$$

が開写像になるとき, 組 (M,ρ) を等質 G 空間とよぶことにする. 等質 G 空間 (M,ρ) について, 各点における固定化部分群は G の閉部分群となる. 逆に G の閉部分群 H を固定するとき, 剰余類空間 G/H (位相は商位相) は自然な意味で等質 G 空間となる. これより等質 G 空間を考えることと, G の閉部分群の共役類を考えることは (しかるべき意味で) 等価である.

2.2. **等質集合上の符号理論.** 以下, G を群とし, (M,ρ) を等質 G 集合とする. 本小節では M 上の "F 禁止符号 '' の用語を定めておく.

直積集合 $M\times M$ に ρ の誘導する対角な G 作用を定め, その軌道集合を $\mathcal{I}$ と書くことにする. また

$$\mathcal{R}: M\times M\to\mathcal{I}$$

を商写像とする. ここで $M\times M$ の部分集合

$$i_0:=\{(p,p)\in M\times M\mid p\in M\}$$

は単一の対角 G 軌道をなすため, $i_0\in\mathcal{I}$ となることに注意しておく.

本稿では M の部分集合 Y について,

$$\mathcal{R}_Y:=\mathcal{R}(Y\times Y)\subset\mathcal{I}$$

とおく. Y が空でないなら $i_0\in\mathcal{R}_Y$ となることに注意. また, $\mathcal{I}$ の各部分集合 F with $i_0\in F$ について, "F 禁止符号" という用語を以下の意味で用いる:

Definition 2.1 (F 禁止符号[1])**.** F を $\mathcal{I}$ の部分集合 *with* $i_0\in F$ とする. M の部分集合 Y が F 禁止符号 *(F-free code)* であるとは,

$$\mathcal{R}_Y\cap F\subset\{i_0\}$$

が成り立つこととする. これは「$y_1,y_2\in Y$ が $y_1\neq y_2$ であるなら $\mathcal{R}(y_1,y_2)\notin F$」となることに他ならない.

以下で紹介するように,「等質集合上の F 禁止符号」という概念は誤り訂正符号, 接吻数問題, 球充填問題などに統一的な枠組みを与える.

Example 2.2. 半直積群 $G=\mathfrak{S}_n\ltimes(\mathfrak{S}_2)^n$ の等質集合 $M=\{0,1\}^n$ について考える. ただし, G の部分群 $\mathfrak{S}_n$ は $M=\{0,1\}^n$ に成分の入れ替えとして作用しているものとし, また各部分群 $\mathfrak{S}_2$ (n 個ある) は $M=\{0,1\}^n$ に *"bit-flip"* として各成分に作用しているものとする. このとき対角 G 軌道集合 $\mathcal{I}$ は $n+1$ 点集合 $\{0,\dots,n\}$ と同一視され, また商写像 $\mathcal{R}$ は *Hamming* 距離関数*:*

$$\mathcal{R}:\{0,1\}^n\times\{0,1\}^n\to\{0,\dots,n\},\ (x,x')\mapsto\#\{i\mid x_i\neq x'_i\}$$

とみなすことができる. また上記同一視において $i_0=0$ である. ここで $\mathcal{I}$ の部分集合 F を $\{0,1,\dots,2e\}$ として固定する. このとき F 禁止符号とは, 長さ n の e 誤り訂正二進符号に他ならない.

誤り訂正符号の詳細については例えば [13] などを参照されたい.

[1]講演のときと "F 禁止符号" の用語の用法を微修正しています.

Example 2.3. n 次直交群 $G = O(n)$ の等質集合である $n-1$ 次元球面 $M = S^{n-1}$ (ここでは $\mathbb{R}^n$ の原点中心の単位球面として実現されているものとする) について考える. このとき対角 G 軌道集合 $\mathcal{I}$ は閉区間 $[-1, 1]$ と同一視され, 商写像 $\mathcal{R}$ は $\mathbb{R}^n$ における内積

$$\mathcal{R} : S^{n-1} \times S^{n-1} \to [0, 1],\ (x, x') \mapsto \langle x, x' \rangle_{\mathbb{R}^n} = \sum_i x_i x'_i$$

とみなせる. この同一視において $i_0 = 1$ であることに注意. ここで $\mathcal{I}$ の部分集合 F を区間 $(1/2, 1]$ として定めると, F 禁止符号とは, S^{n-1} における接吻配置に他ならない.

接吻数問題の解説としては [3] を, また球面上の一般的な符号理論については [18] または [1, 19, Chapter 5] を参照されたい.

Example 2.4. n 次運動群 $G = O(n) \ltimes \mathbb{R}^n$ の等質集合である n 次元ユークリッド空間 $M = \mathbb{R}^n$ を考える. このとき対角 G 軌道集合 $\mathcal{I}$ は区間 $\mathbb{R}_{\geq 0} = [0, \infty)$ と同一視され, 商写像 $\mathcal{R}$ は $\mathbb{R}^n$ におけるユークリッド距離関数

$$\mathcal{R} : \mathbb{R}^n \times \mathbb{R}^n \to [0, \infty),\ (x, x') \mapsto \sqrt{\|x - x'\|_{\mathbb{R}^n}} = \sqrt{\sum_i (x_i - x'_i)^2}.$$

とみなせる. この同一視において $i_0 = 0$ であることに注意. ここで $\mathcal{I}$ の部分集合 F を区間 $[0, 2)$ として定めると, F 禁止符号とは, $\mathbb{R}^n$ における単位球充填の中心点集合に他ならない.

球充填問題の一般的な解説としては *H. Cohn* による [5] を参照されたい. また *M. Viazovska* を中心とした研究グループによる球充填問題についての近年の驚くべき進展 ([6, 17]) については, 同じく *H. Cohn* による記事 [4] も参考になると思われる.

もう一つ F 禁止符号の例を挙げておく:

Example 2.5. G を不定値直交群 $O(2, 2m)$ とし, G の等質集合 として不定値グラスマン $M = \mathrm{Gr}_{(2,0)}(\mathbb{R}^{2,2m})$ (*the set of all* $(2, 0)$*-subspaces in* $\mathbb{R}^{2,2m}$) を考える. このとき対角 G 軌道空間 $\mathcal{I}$ は閉凸錐

$$\{\alpha \in \mathbb{R}^2 \mid \alpha_1 \geq \alpha_2 \geq 0\} \subset \mathbb{R}^2$$

と同一視され, 商写像 $\mathcal{R}$ は

$$\mathcal{R} : M \times M \to \mathcal{I},\ (V_1, V_2) \mapsto (-\log \lambda_1, -\log \lambda_2)$$

で与えられる. ただし, ここで $V_1, V_2 \in \mathrm{Gr}_{(2,0)}(\mathbb{R}^{2,2m})$ に対して,

$$p_{V_s} : \mathbb{R}^{2,2m} \to \mathbb{R}^{2,2m}$$

を V_s への直交射影 $(s = 1, 2)$ とし, また $\lambda_1 \leq \lambda_2 \leq 1$ を線形変換

$$(p_{V_1} \circ p_{V_2})|_{V_1} : V_1 \to V_1$$

の固有値とする. この同一視において $i_0 = (0, 0)$ である.

$\mathcal{I}$ の部分集合 F を $\{\alpha_2 = 0\}$ とする. このとき $M = \mathrm{Gr}_{(2,0)}(\mathbb{R}^{2,2m})$ の部分集合 Y が F 禁止符号であるとは, Y の任意の異なる二元 V_1, V_2 について, $V_1 \cap V_2 = 0$ が成り立つことと同値である. このような F

禁止符号の例としては不定値複素グラスマン $Y := \mathrm{Gr}_{(1,0)}(\mathbb{C}^{1,m})$ ($\mathbb{R}^{2,2m}$ に定まる標準的な複素構造 J について, *the set of all J-stable $(2,0)$-subspaces of* $\mathbb{R}^{2,2m} = \mathbb{C}^{1,m}$ としたもの) などがある. 実際, この Y について

$$\mathcal{R}_Y = \{\alpha_1 = \alpha_2\} \subset \mathcal{I}$$

となり, $Y = \mathrm{Gr}_{(1,0)}(\mathbb{C}^{1,m})$ は F 禁止符号であることが分かる.

Remark 2.6. G が有限群である場合には, $(M, \mathcal{R})$ は *schurian association scheme* を定める. 一般のアソシエーションスキームにおける符号理論については [1, 19] に詳しい.

2.3. **等質空間上の固有な群作用.** 本小節では G を局所コンパクトなハウスドルフ位相群とし, (X, σ) を節 2.1 で定めた意味の等質 G 空間とする. この X についての各点の固定化部分群は非コンパクトである場合もありうることとする.

G の閉部分群 L を固定したとき, L は X に σ によって作用する. この作用も σ の記号で表すこととする. 局所コンパクト群 L の局所コンパクト空間 X への連続作用 σ が固有 (proper) であるとは, X の任意のコンパクト部分集合 C に対して, L の部分集合

$$L_C := \{l \in L \mid (l \cdot_\sigma C) \cap C \neq \emptyset\}$$

がコンパクトとなることをいう.

等質 G 空間 X の各点の固定化部分群がコンパクトであるとき, または G の閉部分群 L がコンパクトであるときには, L の X への作用は固有である. しかし X の各点の固定化部分群が非コンパクトであり, L も非コンパクトである場合には, L の X への作用が固有である場合も, そうでない場合もある.

Example 2.7. アファイン群 $G = GL(n, \mathbb{R}) \ltimes \mathbb{R}^n$ の等質空間としてアファイン空間 $X = \mathbb{R}^n$ を考える. $X = \mathbb{R}^n$ の点 $x = 0$ を固定すると, その固定化部分群は $H := GL(n, \mathbb{R}) \ltimes \{0\}$ となる. このとき G の閉部分群 $L := \{(I_n, v) \mid v \in \mathbb{R}^n\}$ は X へ固有に作用する. また別の閉部分群として $L' := H = GL(n, \mathbb{R}) \ltimes \{0\}$ を考えると, L' の X の作用は固有ではない.

Example 2.8. $G = SL(2, \mathbb{R})$ の等質空間 $X = \mathbb{R}^2 \setminus \{(0,0)\}$ について考える. X の点 $x = (1, 0)$ を固定すると, その固定化部分群は

$$H := \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$$

となる. このとき, G の非コンパクト閉部分群

$$L := \left\{ \begin{pmatrix} e^a & 0 \\ 0 & e^{-a} \end{pmatrix} \middle| \ a \in \mathbb{R} \right\}$$

は X への作用は固有ではない. この例は, すべての L 軌道は X における閉集合であるにも関わらず, L 作用が固有ではないというものになっている.

次の問題を考える:

Problem 2.9 (固有性判定問題)**.** 局所コンパクト群 G の等質空間 X および G の閉部分群 L を固定する. このとき L の X への作用が固有であるか否か判定せよ.

等質 G 空間 X の点を一つ固定し, その固定化部分群を H と書くことにすると, (X, L) についての以下の四条件は同値であることが知られている:

(i) 等質空間 $X = G/H$ における L の作用が固有.
(ii) 等質空間 G/L における H の作用が固有.
(iii) 直積空間 $G/H \times G/L$ における G の対角作用が固有.
(iv) G の任意のコンパクト部分集合 C_1, C_2 について, G の部分集合 $L \cap C_1 \cdot H \cdot C_2^{-1}$ がコンパクトになる.

したがって, 上記の固有性判定問題は以下のような問題と等価である:

Problem 2.10. 局所コンパクト群 G の閉部分群の組 (H, L) を固定する. このとき, 以下の条件 $(\star)$ を満たすか否か判定せよ:

条件 $(\star)$: G の任意のコンパクト部分集合 C_1, C_2 について, G の部分集合 $L \cap C_1 \cdot H \cdot C_2^{-1}$ がコンパクトになる.

この問題は H, L がどちらも非コンパクトである場合には一般には簡単ではない. しかし G が線形簡約リー群である場合には, 小林俊行氏, Y. Benoist 氏による簡明な判定定理が知られている:

以下, G を線形簡約リー群とする. G の極大コンパクト群 K を固定し, $M = G/K$ と書き, $p_0 := eK \in M$ とおいておく. また M の G 不変リーマン計量を固定し, 誘導される M 上の距離関数を d とする (このとき M はリーマン対称空間と呼ばれる空間となる). $M \times M$ の対角 G 軌道空間 $\mathcal{I}$ において, 距離 $d^{\mathcal{I}}$ を

$$d^{\mathcal{I}} : \mathcal{I} \times \mathcal{I} \to \mathbb{R}_{\geq 0},$$
$$(i_1, i_2) \mapsto \inf\{d(i_1, i_2) \mid p \in i_1, q \in i_2\}$$

と定める. このようにして得られる距離空間 $(\mathcal{I}, d^K)$ は "up to finite cover (詳細略)" でユークリッド空間における閉凸錐と等長であることが知られている. また,

$$\mu : G \to \mathcal{I},\ g \mapsto \mathcal{R}(p_0, g \cdot p_0)$$

をカルタン射影とよぶ. ただし $\mathcal{R} : M \times M \to \mathcal{I}$ は商写像とする.

Theorem 2.11 (固有性判定定理: T. Kobayashi [7, 10], Y. Benoist [2], また [15] も参照されたい)**.** 上記設定において, G の閉部分群 (H, L) の組について, 以下の二条件は同値である:

(i) (H, L) は条件 $(\star)$ を満たす (これは L の G/H への作用が固有であることと同値).
(ii) このとき任意の非負整数 $r \geq 0$ について, $\mathcal{I}$ の部分集合 $\mu(L) \cap \overline{N}_r(\mu(H))$ は有界, ただし $\mathcal{I}$ の各部分集合 S および非負実数

r について,

$$\overline{N}_r(S) := \{\alpha \in \mathfrak{a}_+ \mid d^K(\alpha, s) \leq r \text{ for some } s \in S\}$$

と定める.

Example 2.12. G を不定値直交群 $O(2, 2m)$ とする. G の極大コンパクト群として $K = O(2) \times O(2m)$ を固定する. このとき $M = G/K$ は不定値グラスマン $M = \mathrm{Gr}_{(2,0)}(\mathbb{R}^{2,2m})$ (*the set of all* $(2,0)$*-subspaces in* $\mathbb{R}^{2,2m}$) とみなせる. また対角 G 軌道空間 $\mathcal{I}$ は閉凸錐

$$\{\alpha \in \mathbb{R}^2 \mid \alpha_1 \geq \alpha_2 \geq 0\} \subset \mathbb{R}^2$$

と等長に同一視され, 商写像 $\mathcal{R}$ は *Example 2.5* で紹介した形で与えられる.

以下, 不定値直交群 $G = O(2, 2m)$ の等質空間

$$X = \{x \in \mathbb{R}^{2,2m} \mid (x, x)_{2,2m} = 1\}$$

について考える. この空間 X は符号 $(1, 2m)$ の G 不変擬リーマン計量を定めることにより, 擬リーマン空間形 (断面曲率が一定) の構造を持つ. また X の点 $x_0 = (1, 0, \ldots, 0)$ として固定すると, その固定化部分群は $H := O(1, 2m)$ となる.

G の閉部分群として不定値ユニタリ群 $L := U(1, m)$ を考える. このとき,

$$\mu(L) = \{\alpha_1 = \alpha_2\},$$
$$\mu(H) = \{\alpha_2 = 0\}$$

となる. 特に任意の $r \in \mathbb{R}$ について

$$\mu(L) \cap \overline{N}_r(\mu(H)) = \{\alpha_1 = \alpha_2 \leq r\}$$

は有界である. 固有性判定定理より (H, L) は条件 $(\star)$ を満たし, 特に $L = U(1, m)$ の X への作用は固有である. また, この L の作用は余コンパクト, つまり $L\backslash X$ がコンパクトになることが知られており, 特に L の捩れのない余コンパクト離散部分群 Γ を選ぶごとに Γ は X の余コンパクトな不連続群となる. 特に *Clifford–Klein* 形 $\Gamma\backslash X$ としてコンパクトな符号 $(1, 2m)$ の擬リーマン空間形が手に入る.

3. 粗幾何学に関する用語の準備

集合上に大規模かつ一様な近傍構造を定めたものを粗空間といい, 粗空間を取り扱う分野を粗幾何学という. 本節では粗幾何学に関する各種用語を定めておく.

3.1. 粗構造, 粗空間.

本小節では粗構造および粗空間についての用語を定める.

以下, Ω を集合とし, Ω のべき集合を $\mathcal{P}(\Omega)$ と書くことにする. ここで

$$\mathrm{End}_U(\mathcal{P}(\Omega)) := \{E : \mathcal{P}(\Omega) \to \mathcal{P}(\Omega) \mid E \text{ preserves any unions}\}.$$

とおく. ただし "$E : \mathcal{P}(\Omega) \to \mathcal{P}(\Omega)$ preserves any union" とは任意の $\mathcal{U} \subset \mathcal{P}(\Omega)$ について,

$$E(\bigcup_{U \in \mathcal{U}} U) = \bigcup_{U \in \mathcal{U}} E(U)$$

が成り立つこととする.

Remark 3.1. 直積集合 $\Omega \times \Omega$ のべき集合を $\mathcal{P}(\Omega \times \Omega)$ と書くことにすると, $\mathrm{End}_U(\mathcal{P}(\Omega))$ は以下の対応 $E \mapsto \Phi_E$ により, 自然に $\mathcal{P}(\Omega \times \Omega)$ と一対一に対応する: 各 $E \in \mathrm{End}_U(\mathcal{P}(\Omega))$ について, $\Phi_E \subset \Omega \times \Omega$ を,

$$\Phi_E = \{(x, y) \in \Omega \times \Omega \mid y \in E(\{x\})\}$$

と定める.

J. Roe [16] の教科書では $\mathcal{P}(\Omega \times \Omega)$ の言葉で粗幾何学の各用語が定義されている. 本稿で紹介する粗幾何学の用語は, 上記対応により各用語を $\mathrm{End}_U(\mathcal{P}(\Omega))$ の言葉で置き換えたものである.

$\mathrm{End}_U(\mathcal{P}(\Omega))$ は写像の合成についてモノイドをなしている. 単位元は恒等写像 $\mathrm{id}_{\mathcal{P}(\Omega)}$ である. また, 以下のような $\mathrm{End}_U(\mathcal{P}(\Omega))$ 上の対合および上半束構造を定めておく.

- 各 $E \in \mathrm{End}_U(\mathcal{P}(\Omega))$ について, その "転置" $E^T \in \mathrm{End}_U(\mathcal{P}(\Omega))$ を

  $$E^T : \mathcal{P}(\Omega) \to \mathcal{P}(\Omega),\ S \mapsto \{x \in \Omega \mid E(\{x\}) \cap S \neq \emptyset\}.$$

  として定める. 転置はモノイド $\mathrm{End}_U(\mathcal{P}(\Omega))$ における対合を定める. すなわち $(E \circ F)^T = F^T \circ E^T$ が任意の $E, F \in \mathrm{End}_U(\mathcal{P}(\Omega))$ について成り立つ.
- $E, F \in \mathrm{End}_U(\mathcal{P}(\Omega))$ について, "$E \subset F$" であるとは, $E(S) \subset F(S)$ が任意の $S \in \mathcal{P}(\Omega)$ について成り立つこととする. この二項関係 "$\subset$" は $\mathrm{End}_U(\mathcal{P}(\Omega))$ 上の半順序を定め, さらに上半束 (join semi-lattice) になっている. 各 $E, F \in \mathrm{End}_U(\mathcal{P}(\Omega))$ についての join は

  $$E \cup F : \mathcal{P}(\Omega) \to \mathcal{P}(\Omega),\ S \mapsto E(S) \cup F(S)$$

  で与えられる.

集合 Ω 上の粗構造 (coarse structure) を以下で定める:

Definition 3.2 (粗構造, 粗空間)**.** $\mathrm{End}_U(\mathcal{P}(\Omega))$ の部分集合 $\mathcal{E}$ が 集合 Ω 上の粗構造であるとは, 以下の五条件が成り立つこととする:

(*i*) 恒等写像 $\mathrm{id}_{\mathcal{P}(\Omega)}$ *on* $\mathcal{P}(\Omega)$ は $\mathcal{E}$ の元.
(*ii*) $\mathcal{E}$ は合成について閉じる, つまり $E_1 \circ E_2 \in \mathcal{E}$ が任意の $E_1, E_2 \in \mathcal{E}$ について成り立つ.
(*iii*) $\mathcal{E}$ は転置について閉じる, つまり $E^T \in \mathcal{E}$ が任意の $E \in \mathcal{E}$ について成り立つ.
(*iv*) $\mathcal{E}$ は *join* について閉じる, つまり, $E_1 \cup E_2 \in \mathcal{E}$ が任意の $E_1, E_2 \in \mathcal{E}$ について成り立つ.

(*v*) $\mathcal{E}$ は半順序集合 $\mathrm{End}_U(\mathcal{P}(\Omega))$ の *lower set* である, つまり, 任意の $E \in \mathcal{E}$ および任意の $F \in \mathrm{End}_U(\mathcal{P}(\Omega))$ について, $F \subset E$ であるなら $F \in \mathcal{E}$ が成り立つ.

このとき, 組 $(\Omega, \mathcal{E})$ を粗空間 (*coarse space*) という. また本稿では, $\mathcal{E}$ の各元を制御作用素 (*controlled operator*)[2] とよぶことにする.

粗空間における「有界集合」の概念を以下で定義する:

Definition 3.3 (有界集合)**.** $(\Omega, \mathcal{E})$ を粗空間とする. Ω の部分集合 B が有界であるとは, $B = \emptyset$ であるか, またはある元 $x \in \Omega$ およびある制御作用素 $E \in \mathcal{E}$ が存在して $B \subset E(\{x\})$ となることとする.

Example 3.4. (Ω, d) を距離空間とする. Ω 上の粗構造

$$\mathcal{E}_d := \{E \in \mathrm{End}_U(\mathcal{P}(\Omega)) \mid E \subset \overline{N}_r \text{ for some } r \geq 0\}$$

を距離関数 d の定める有界粗構造 *(bounded coarse structure)* とよぶ. ただし, 各 $r \geq 0$ について, $\overline{N}_r \in \mathrm{End}_U(\mathcal{P}(\Omega))$ を

$$\overline{N}_r : \mathcal{P}(\Omega) \to \mathcal{P}(\Omega),\ S \mapsto \{x \in \Omega \mid d(x, s) \leq r \text{ for some } s \in S\}$$

として定める. 粗空間 (Ω, E_d) についての有界集合とは, 距離 d についての有界集合のことに他ならない.

また, 粗空間の部分集合の組に対して "BI-pair" という概念を以下で定めておく.

Definition 3.5 ([14] in preparation)**.** $(\Omega, \mathcal{E})$ を粗空間とする. Ω の部分集合の組 (S, S') が *BI (bounded intersection)* であるとは, 任意の制御作用素 $E \in \mathcal{E}$ について, 共通部分 $S \cap E(S')$ が有界であることとする.

BI-pair の概念は $\mathcal{P}(\Omega)$ における対称な二項関係を定める, つまり, (S, S') が BI であることと, (S', S) が BI であることは同値である.

3.2. **粗写像, 粗同値写像.** 二つの粗空間の間の写像についての各種用語を以下で定めておく: 以下, $(\Omega_i, \mathcal{E}_i)$ $(i = 1, 2)$ を粗空間とし, $\varphi : \Omega_1 \to \Omega_2$ を写像とする.

まず, 以下の記号を導入する:

$$\varphi_* : \mathcal{P}(\Omega_1) \to \mathcal{P}(\Omega_2),\ S \mapsto \varphi(S),$$
$$\varphi^* : \mathcal{P}(\Omega_2) \to \mathcal{P}(\Omega_1),\ S' \mapsto \varphi^{-1}(S').$$

つまり φ_* は順像を表し, φ^* は逆像を表すものとする.

Definition 3.6 (粗一様写像)**.** 写像 $\varphi : \Omega_1 \to \Omega_2$ が粗一様 (*coarsely uniform* または *bornologous*) であるとは, 任意の制御作用素 $E \in \mathcal{E}_1$ について, $\varphi_* \circ E \circ \varphi^* \in \mathrm{End}_U(\mathcal{P}(\Omega_2))$ が制御作用素, つまり $\varphi_* \circ E \circ \varphi^* \in \mathcal{E}_2$ となることとする.

[2]教科書 [16] では制御集合 (controlled set) と呼ばれている概念に対応する.

Definition 3.7 (粗固有写像)**.** 写像 $\varphi : \Omega_1 \to \Omega_2$ が粗固有 (*coarsely proper*) であるとは, 任意の有界集合 B *in* $(\Omega_2, \mathcal{E}_2)$ について, 逆像 $\varphi^{-1}(B)$ が有界 *in* $(\Omega_1, \mathcal{E}_1)$ であることとする.

Definition 3.8 (粗写像)**.** 写像 $\varphi : \Omega_1 \to \Omega_2$ が粗 (*coarse*) であるとは, 粗一様かつ粗固有であることとする.

Definition 3.9 (粗同値写像)**.** 写像 $\varphi : \Omega_1 \to \Omega_2$ が粗同値 (*coarsely equivalent*) であるとは, 以下の条件をみたすこととする:

- φ は粗写像.
- 粗写像 $\psi : \Omega_2 \to \Omega_1$ であって, $\varphi^* \circ \psi^* \in \mathcal{E}_1$ かつ $\psi^* \circ \varphi^* \in \mathcal{E}_2$ となるものが存在する.

Example 3.10. $\mathbb{R}$ および $\mathbb{Z}$ にそれぞれ通常の距離から定まる有界粗構造を考え, 粗空間とみなす. このとき

$$\varphi : \mathbb{R} \to \mathbb{Z},\ r \mapsto \lfloor r \rfloor$$

は粗同値写像となる.

粗空間における BI-pair に関して次の定理が成り立つ:

Theorem 3.11 ([14] in preparation)**.** 粗同値写像は *BI-pair* を保つ. すなわち, $\varphi : \Omega_1 \to \Omega_2$ が粗同値写像であり, $S, S' \subset \Omega_1$ とするとき, 以下の二条件は同値である:

(*i*) (S, S') は *BI in* $(\Omega_1, \mathcal{E}_1)$.
(*ii*) $(\varphi(S), \varphi(S'))$ は *BI in* $(\Omega_2, \mathcal{E}_2)$.

4. 等質集合上の粗符号理論

節 2.2 の設定で考える. 本節では "F 禁止符号" の一般化として, "粗 F 禁止符号" の概念を導入する.

以下, 対角 G 軌道集合 $\mathcal{I}$ に粗構造 $\mathcal{E}$ を定めておく. $\mathcal{I}$ の各部分集合 F with $i_0 \in F$ について, "粗 F 禁止符号" を以下で定義しよう:

Definition 4.1 (粗 F 禁止符号)**.** F を $\mathcal{I}$ の部分集合 *with* $i_0 \in F$ とする. M の部分集合 Y が粗 F 禁止符号であるとは, $\mathcal{I}$ の部分集合の組 $(\mathcal{R}_Y, F)$ が *BI*, すなわち, 任意の制御作用素 $E \in \mathcal{E}$ について, 共通部分 $\mathcal{R}_Y \cap E(F)$ が $(\mathcal{I}, \mathcal{E})$ において有界であることとする.

Remark 4.2. F 自身が $(\mathcal{I}, \mathcal{E})$ において有界である場合には, すべての M の部分集合は粗 F 禁止符号となる.

Remark 4.3. $\mathcal{E}_{\mathrm{disc}}$ が $\mathcal{I}$ 上の離散粗構造, つまり

$$\mathcal{E}_{\mathrm{disc}} = \{E \in \mathrm{End}_U(\mathcal{P}(\Omega)) \mid E \subset \mathrm{id}_{\mathcal{P}(\Omega)}\}$$

の場合には, 粗 F 禁止符号とは, 節 *2.2* における F 禁止符号のことに他ならない (この場合, $(\mathcal{I}, \mathcal{E}_{\mathrm{disc}})$ における有界集合とは, 一点集合または空集合を意味することに注意).

Example 4.4. *Example 2.5* の設定として, 不定値直交群 $G = O(2, 2m)$ の等質集合として不定値グラスマン $M = \mathrm{Gr}_{(2,0)}(\mathbb{R}^{2,2m})$ (*the set of all* $(2, 0)$*-subspaces in* $\mathbb{R}^{2,2m}$) を考える. また対角 G 軌道集合 $\mathcal{I}$ は閉凸錐

$$\{\alpha \in \mathbb{R}^2 \mid \alpha_1 \geq \alpha_2 \geq 0\} \subset \mathbb{R}^2,$$

と同一視し, 自然に定まる距離関数を $d^{\mathcal{I}}$ と書くことにする. この $d^{\mathcal{I}}$ についての $\mathcal{I}$ 上の有界粗構造を $\mathcal{E}_{d^{\mathcal{I}}}$ と書くことにする. また *Example 2.5* と同様に $\mathcal{I}$ の部分集合 F を

$$F = \{\alpha_2 = 0\} \subset \mathcal{I}.$$

として固定する.

ここで *Example 2.5* でも紹介した $M = \mathrm{Gr}_{(2,0)}(\mathbb{R}^{2,2m})$ の部分集合として不定値複素グラスマン $Y = \mathrm{Gr}_{(1,0)}(\mathbb{C}^{1,m})$ を考える. この Y について

$$\mathcal{R}_Y = \{\alpha_1 = \alpha_2\} \subset \mathcal{I}$$

となるため, *Example 2.12* の後半の議論により, $Y = \mathrm{Gr}_{(1,0)}(\mathbb{C}^{1,m})$ は粗 F 禁止符号であることが分かる.

5. 等質空間上の群作用の固有性と粗符号理論

本節では G を局所コンパクトなハウスドルフ位相群とする.

5.1. 粗幾何学を用いた固有性判定定理.

G 上の “両側コンパクト粗構造” を以下で定めておく:

Definition 5.1 (両側コンパクト粗構造 on G)**.** 局所コンパクト位相群 G 上の粗構造 $\mathcal{E}^{LR}_{\mathrm{cpt}}(G)$ を以下で定め, 本稿では G 上の両側コンパクト粗構造とよぶことにする*:*

$$\mathcal{E}^{LR}_{\mathrm{cpt}}(G) := \{E \in \mathrm{End}_U(\mathcal{P}(G)) \mid \\ E \subset E^G_{C_1,C_2} \textit{ for some compact subsets } C_1 \textit{ and } C_2 \textit{ of } G\}$$

ただし, G の部分集合 C_1, C_2 について, $E^G_{C_1,C_2} \in \mathrm{End}_U(\mathcal{P}(G))$ を

$$E^G_{C_1,C_2} : \mathcal{P}(G) \to \mathcal{P}(G),\ S \mapsto C_1 \cdot S \cdot C_2^{-1}$$

により定める.

Section 2.3 で紹介した事実と簡単な考察により以下が成り立つことが分かる:

Proposition 5.2. (H, L) を G の閉部分群の組とする. このとき以下の五条件は同値である*:*

- 等質空間 $X = G/H$ における L の作用が固有.
- 等質空間 G/L における H の作用が固有.
- 直積空間 $G/H \times G/L$ における G の対角作用が固有.
- (H, L) は条件 $(\star)$ *stated in Section 2.3* を満たす.
- (H, L) は *BI in* $(G, \mathcal{E}^{LR}_{\mathrm{cpt}}(G))$.

また Theorem 3.11 の帰結として以下の定理が成り立つ:

Theorem 5.3 ([14] in preparation)**.** $(\Omega, \mathcal{E})$ を粗空間とし, $\varphi : (G, \mathcal{E}^{LR}_{\mathrm{cpt}}(G)) \to (\Omega, \mathcal{E})$ を粗同値写像とする. G の部分集合の組 (H, L) について, 以下の三条件は同値:

(i) (H, L) は条件 $(\star)$ *stated in Section 2.3* を満たす.
(ii) (H, L) は *BI in* $(G, \mathcal{E}^{LR}_{\mathrm{cpt}}(G))$.
(iii) $(\varphi(H), \varphi(L))$ は *BI in* $(\Omega, \mathcal{E})$.

この定理は以下の意味で固有性判定定理 2.11 の一般化になっている:

Theorem 5.4 ([14] in preparation)**.** G を線形簡約リー群とし, *Section 2.3* で紹介した意味でのカルタン射影 $\mu : G \to \mathcal{I}$ を考える. このとき μ は粗空間 $(G, \mathcal{E}^{LR}_{\mathrm{cpt}}(G))$ と $(\mathcal{I}, \mathcal{E}_{d^{\mathcal{I}}})$ の間の粗同値写像を与える. ただし $\mathcal{E}_{d^{\mathcal{I}}}$ は距離 $d^{\mathcal{I}}$ の定める $\mathcal{I}$ 上の有界粗構造を表す.

5.2. **粗符号理論の枠組みでの言い換え.** 本稿の主定理は Theorem 5.3 を粗符号理論の枠組みに載せたものである. 以下で詳しく紹介する.

$M = (M, \rho)$ を等質 G 空間であって, 各点の固定化部分群がコンパクトであるものとする. 節 2.2 と同様に, $M \times M$ の対角 G 軌道集合を $\mathcal{I}$, 商写像を $\mathcal{R} : M \times M \to \mathcal{I}$ と書く.

このとき以下が成り立つ:

Proposition 5.5. $\mathcal{I}$ 上の粗構造 $\mathcal{E}^{LR}_{\mathrm{cpt}}(\mathcal{I})$ であって, 以下の条件を満たすものがただ一つ存在する:

条件: M の任意の点 p について,

$$\varphi_p : G \to \mathcal{I},\ g \mapsto \mathcal{R}(p, g \cdot_\rho p)$$

とおくと, φ_p は $(G, \mathcal{E}^{LR}_{\mathrm{cpt}}(G))$ から $(\mathcal{I}, \mathcal{E}^{LR}_{\mathrm{cpt}}(\mathcal{I}))$ への粗同値写像となる.

以下, M の点 p_0 を一つ固定しておき,

$$\pi : G \to M,\ g \mapsto g \cdot_\rho p_0$$

とおく. G の各部分集合 S について, $\mathcal{I}$ の部分集合 F_S を

$$F_S := \mathcal{R}_{\pi(S)} = \mathcal{R}(\pi(S), \pi(S))$$

として定める.

(H, L) が G の閉部分群の組であるという設定下で Theorem 5.3 を $(\Omega, \mathcal{E}) = (\mathcal{I}, \mathcal{E}^{LR}_{\mathrm{cpt}}(\mathcal{I}))$ に適用することにより, 本稿の主結果である以下の定理を得る:

Theorem 5.6. (H, L) を G の閉部分群の組とする. このとき以下の五条件は同値である:

(i) 等質空間 G/H における L の作用は固有.
(ii) 等質空間 G/L における H の作用は固有.
(iii) (H, L) は *BI in* $(G, \mathcal{E}^{LR}_{\mathrm{cpt}}(G))$.
(iv) M の部分集合 $\pi(L)$ は粗 F_H 禁止符号 *with respect to* $(\mathcal{I}, \mathcal{E}^{LR}_{\mathrm{cpt}}(\mathcal{I}))$.
(v) M の部分集合 $\pi(H)$ は粗 F_L 禁止符号 *with respect to* $(\mathcal{I}, \mathcal{E}^{LR}_{\mathrm{cpt}}(\mathcal{I}))$.

Example 5.7. *Example 4.4* の設定として, 不定値直交群 $G = O(2, 2m)$ の等質集合として不定値グラスマン $M = \mathrm{Gr}_{(2,0)}(\mathbb{R}^{2,2m})$ を考え,

$$\mathcal{I} = \{\alpha \in \mathbb{R}^2 \mid \alpha_1 \geq \alpha_2 \geq 0\} \subset \mathbb{R}^2,$$

に有界粗構造を入れておく. $\mathcal{I}$ の部分集合 F を

$$F = \{\alpha_2 = 0\} \subset \mathcal{I}.$$

とする. このとき $M = \mathrm{Gr}_{(2,0)}(\mathbb{R}^{2,2m})$ の部分集合 $Y = \mathrm{Gr}_{(1,0)}(\mathbb{C}^{1,m})$ は粗 F 禁止符号になるのであった.

このとき $\mathcal{I}$ の有界粗構造は上で定めた粗構造 $\mathcal{E}^{LR}_{\mathrm{cpt}}(\mathcal{I})$ と一致している (*by Theorem 5.4*). また M の基点として

$$x = \mathrm{Span}\{(1, 0, \ldots, 0), (0, 1, \ldots, 0)\} \in M$$

を定めておくと, $G = O(2, 2m)$ の閉部分群の組

$$(H, L) := (O(1, 2m), U(1, m))$$

に対して, $F_H = F$ かつ $\pi(L) = Y$ となる. これより *Example 2.12* で紹介した $X = G/H$ における L 作用の固有性を, 本稿の主定理 *Theorem 5.6* の帰結とみなすこともできる.

Concluding Remarks: 本稿の目的は等質空間上の不連続群論と等質集合上の符号理論を粗幾何学の言葉を用いて結びつけることであった. とりあえず等質空間上の群作用の固有性を粗符号理論の枠組みで説明することには成功したと言えるが, 今後は以下のような課題に取り組みたい:

- **課題 1: 線形簡約リー群以外の具体例:** 粗符号の概念や本稿の主定理 5.6 はさまざまな局所コンパクト群 G および等質 G 集合 M (固定化部分群がコンパクト) について意味のあるものになっていると信じているが, 著者は現時点では G が線形簡約リー群である場合および G が運動群の場合でしか意味のある例を持っていない. 特に G がアフィン群である場合などを中心に, いろいろな例を探したい.
- **課題 2: 粗符号の定式化の精査:** 本稿の設定では M は単なる等質集合であるが, $\mathcal{I}$ には粗構造を入れるという歪な形で粗符号の定式化が行われている. M にも粗構造を定めるのが自然であると思われるが, そのような定式化についても考えたい.
- **課題 3: 粗符号理論における Delsarte 理論の整備:** 有限等質集合およびアソシエーションスキーム上の符号理論においては Delsarte 理論という強力な道具がある (例えば [1, 19] を参照). 粗符号理論における Delsarte 理論についても整備を行いたい.
- **課題 4: 余コンパクトな不連続群の研究についての応用:** 不連続群論において最も重要な研究テーマの一つとして, 「与えられた等質 G 空間 X について, 余コンパクトな不連続群が存在するか否か判定せよ」という問題がある. この問

題について, 粗符号理論を応用する形で何等かの貢献ができればと考えている.

References

1. Eiichi Bannai, Etsuko Bannai, Tatsuro Ito, and Rie Tanaka, *Algebraic combinatorics*, vol. 5, Walter de Gruyter GmbH & Co KG, 2021.
2. Yves Benoist, *Actions propres sur les espaces homogènes réductifs*, Ann. of Math. (2) **144** (1996), no. 2, 315–347. MR 1418901
3. Peter Boyvalenkov, Stefan Dodunekov, and Oleg Musin, *A survey on the kissing numbers*, Serdica Math. J. **38** (2012), no. 4, 507–522. MR 3060792
4. Henry Cohn, *A conceptual breakthrough in sphere packing*, Notices Amer. Math. Soc. **64** (2017), no. 2, 102–115. MR 3587715
5. ———, *Packing, coding, and ground states*, Mathematics and materials, IAS/Park City Math. Ser., vol. 23, Amer. Math. Soc., Providence, RI, 2017, pp. 45–102. MR 3700014
6. Henry Cohn, Abhinav Kumar, Stephen D. Miller, Danylo Radchenko, and Maryna Viazovska, *The sphere packing problem in dimension 24*, Ann. of Math. (2) **185** (2017), no. 3, 1017–1033. MR 3664817
7. Toshiyuki Kobayashi, *Proper action on a homogeneous space of reductive type*, Math. Ann. **285** (1989), no. 2, 249–263. MR 1016093
8. ———, *Discontinuous groups acting on homogeneous spaces of reductive type*, Representation theory of Lie groups and Lie algebras (Fuji-Kawaguchiko, 1990), World Sci. Publ., River Edge, NJ, 1992, pp. 59–75. MR 1190750
9. ———, *A necessary condition for the existence of compact Clifford-Klein forms of homogeneous spaces of reductive type*, Duke Math. J. **67** (1992), no. 3, 653–664. MR 1181319
10. ———, *Criterion for proper actions on homogeneous spaces of reductive groups*, J. Lie Theory **6** (1996), no. 2, 147–163. MR 1424629
11. ———, *Discontinuous groups for non-Riemannian homogeneous spaces*, Mathematics unlimited—2001 and beyond, Springer, Berlin, 2001, pp. 723–747. MR 1852186
12. Toshiyuki Kobayashi, *Conjectures on reductive homogeneous spaces*, arXiv:2204.08854v1, 2022.
13. Florence Jessie MacWilliams and Neil James Alexander Sloane, *The theory of error-correcting codes*, vol. 16, Elsevier, 1977.
14. Hiroki Nagaya, Kento Ogawa, and Takayuki Okuda, *A generalization of Kobayashi's properness criterion from a viewpoint of coarse geometry*, in preparation.
15. Kento Ogawa and Takayuki Okuda, *A proof of Kobayashi's properness criterion from a viewpoint of metric geometry*, arXiv e-prints (2023), arXiv:2304.14101.
16. John Roe, *Lectures on coarse geometry*, University Lecture Series, vol. 31, American Mathematical Society, Providence, RI, 2003. MR 2007488
17. Maryna S. Viazovska, *The sphere packing problem in dimension 8*, Ann. of Math. (2) **185** (2017), no. 3, 991–1015. MR 3664816
18. 坂内英一 and 坂内悦子, **球面上の代数的組合せ理論** *(***シュプリンガー現代数学シリーズ***)*, 丸善出版, 2014.
19. 坂内英一, 坂内悦子, and 伊藤達郎, **代数的組合せ論入門** *(***共立叢書現代数学の潮流***)*, 共立出版, 2016.

(T. Okuda) Graduate School of Advanced Science and Engineering, Hiroshima University, 1-3-1 Kagamiyama, Higashi-Hiroshima City, Hiroshima, 739-8526, Japan.

Email address: okudatak@hiroshima-u.ac.jp

The number of connected bipartite graphs with given Betti numbers: its asymptotic behavior and generating functions

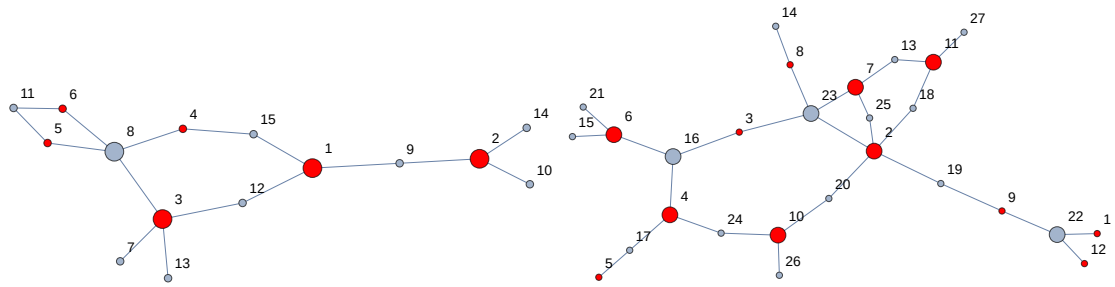
Satoshi Yabuoku (National Institute of Technology, Kitakyushu College)*

Abstract

We consider the number of connected bipartite graphs whose Betti number is k and its bivariate exponential generating functions (e.g.f. for short). By solving recurrence partial differential equations which e.g.f.s satisfy, we obtain the explicit form of e.g.f.s and derive the asymptotic behavior of their coefficients. We also introduce a family of basic graphs to classify connected bipartite graphs and give another expression of the e.g.f.s as the sum over basic graphs of rational functions of those for the number of labeled bipartite rooted spanning trees. This is a joint work with Taro Hasui (IMI, Kyushu University) and Tomoyuki Shirai (IMI, Kyushu University).

1 Introduction

Let $G = (V, E)$ be a simple (i.e., no self-loops and multiple edges) bipartite graph with bipartition $V = V_1 \sqcup V_2$, and we call it a bipartite (r, s, k)-graph if $|V_1| = r$, $|V_2| = s$ and $|E| = r + s - 1 + k$, which is also considered as a spanning subgraph with k-cycles in the complete bipartite graph $K_{r,s}$, see Figure 1.



(a) $(6, 9, 2)$-graph. (b) $(12, 15, 3)$-graph.

Figure 1: Example of bipartite (r, s, k)-graphs.

Let $N_{\mathrm{bi}}(r, s, k)$ be the number of connected bipartite (r, s, k)-graphs whose Betti number is k, the number of independent cycles. We focus on the values $N_{\mathrm{bi}}(r, s, k)$ for given Betti number k and the asymptotic behavior of sum of $N_{\mathrm{bi}}(r, s, k)$ with $r + s = n$. For $k = 0$, connected bipartite $(r, s, 0)$-graphs are spanning trees in $K_{r,s}$, and it is well known [3] that

$$N_{\mathrm{bi}}(r, s, 0) = r^{s-1} s^{r-1}, \tag{1}$$

which is the bipartite version of Cayley's formula.

* e-mail: yabuoku@kct.ac.jp

This work was supported by JSPS KAKENHI Grant Numbers JP18H01124 and JP20K20884, JSPS Grant-in-Aid for Transformative Research Areas (A) JP22H05105, and JST CREST Mathematics (15656429). TS was also supported in part by JSPS KAKENHI Grant Numbers, JP20H00119 and JP21H04432.

Note that when $k = 1$, connected bipartite $(r, s, 1)$-graphs are *unicycles* in $K_{r,s}$ and discussed in the context of cuckoo hushing by [2].

To analyze $N_{\mathrm{bi}}(r, s, k)$, we consider the bivariate exponential generating function for $N_{\mathrm{bi}}(r, s, k)$ defined as follows: for $k = 0, 1, \ldots,$

$$F_k(x, y) := \sum_{r,s=0}^{\infty} \frac{N_{\mathrm{bi}}(r, s, k)}{r!s!} x^r y^s.$$

For simplicity, we write the exponential generating function for spanning trees in (1) by

$$T(x, y) := F_0(x, y) = x + y + \sum_{r,s=1}^{\infty} \frac{r^{s-1}s^{r-1}}{r!s!} x^r y^s.$$

We introduce the following functions of x and y:

$$T_x = D_x T, \quad T_y = D_y T, \quad Z = T_x + T_y, \quad W = T_x T_y,$$

where $D_x = x\partial_x$ and $D_y = y\partial_y$ are the Euler differential operators.

By a combinatorial argument, we have recurrence equations for $N_{\mathrm{bi}}(r, s, k)$, and we obtain the recurrence linear partial differential equations for $\{F_k\}_{k=0,1,\ldots}$ as following.

Proposition 1.1. *For $k = -1, 0, 1, 2, \ldots,$*

$$\begin{aligned}&(D_x + D_y + k)F_{k+1}\\ &= (D_x D_y - D_x - D_y + 1 - k)F_k + \sum_{l=0}^{k+1} D_x F_l \cdot D_y F_{k+1-l},\end{aligned} \tag{2}$$

where $D_x = x\partial_x$ and $D_y = y\partial_y$.

Now we can solve the equation (2) inductively and obtain $F_k, k = 1, 2, \ldots$ in terms of the known function T.

2 Derivation of F_k

From Proposition 1.1, we have the explicit forms of F_1 and F_2 as functions of Z and W.

Proposition 2.1. *The function $F_1(x, y)$ is expressed as $F_1 = f_1(W)$ with $f_1(w) = -\frac{1}{2}\big(\log(1 - w) + w\big)$, i.e.,*

$$F_1(x, y) = -\frac{1}{2}\Big(\log(1 - T_x T_y) + T_x T_y\Big).$$

Theorem 2.2. *The function $F_2(x, y)$ is expressed as $F_2 = f_2(Z, W)$ with*

$$f_2(z, w) = \frac{w^2}{24(1 - w)^3}\big\{(2 + 3w)z + 2w(6 - w)\big\}.$$

From Proposition 1.1, we also have the explicit forms of $F_3, F_4, \ldots$ and so on. For $k \geq 2$, by using another expression for F_k discussed in Section 4, we have the following expression for F_k.

Theorem 2.3. *For $k \geq 2$, the function $F_k(x, y)$ is expressed as $F_k = f_k(Z, W)$ with*

$$f_k(z, w) = \frac{w^2}{(1-w)^{3(k-1)}} \sum_{j=0}^{k-1} q_{k,j}(w) z^j,$$

where $q_{k,j}(w)$ is a polynomial in w.

We remark that $F_k(x, y)$ has no logarithmic term for $k \geq 2$.

3 Asymptotic behavior of the coefficients of $F_k(x, x)$

From Section 2, we obtain the asymptotic behavior of the coefficients of the diagonals $F_k(x, x)$. Let $\langle x^n \rangle A(x)$ denote the operation of extracting the coefficient a_n of $x^n/n!$ in an exponential formal power series $A(x) = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$, i.e.

$$\langle x^n \rangle A(x) = a_n.$$

The coefficients of $\langle x^n \rangle F_k(x, x)$ counts the number of connected bipartite graphs with Betti number k over n vertices, or equivalently, the total number of connected bipartite (r, s, k)-graphs with $r + s = n$. We denote it by

$$\begin{aligned} N_{\mathrm{bi}}(n, k) := \langle x^n \rangle F_k(x, x) &= \sum_{r+s=n} \binom{n}{r} N_{\mathrm{bi}}(r, s, k) \\ &= \#\{\text{bipartite } (r, s, k)\text{-graphs with } r + s = n\}. \end{aligned}$$

Let $N(n, k)$ be the number of connected graphs whose Betti number is k on the complete graph K_n. For $k \geq 1$, the asymptotic behavior of $N(n, k)$ was shown in [4], and we obtain the following results.

Theorem 3.1. *For $n = 4, 5, \ldots,$*

$$\begin{aligned} N_{\mathrm{bi}}(n, 1) &= n^{n-1} \sum_{2 \leq k \leq n/2} \frac{n!}{(n-2k)! n^{2k}} \\ &\sim \sqrt{\frac{\pi}{8}} n^{n-1/2} \sim N(n, 1) \quad (n \to \infty). \end{aligned}$$

Hence, the asymptotic behavior of the number of *unicycles* in $K_{r,s}$ with $r + s = n$ coincides with that in K_n.

n	3	4	5	6	7	8	9	10	11
$N(n, 1)$	1	15	222	3660	68295	1436568	33779340	880107840	25201854045
$N_{\mathrm{bi}}(n, 1)$	0	6	120	2280	46200	1026840	25102224	673706880	19745850960

Figure 2: $N(n, 1)$ and $N_{\mathrm{bi}}(n, 1)$ for $n = 3, 4, \ldots, 11$

Theorem 3.2. *As $n \to \infty$,*

$$N_{\mathrm{bi}}(n, 2) \sim \frac{5}{48} n^{n+1} \sim \frac{1}{2} N(n, 2).$$

n	4	5	6	7	8	9	10	11
$N(n,2)$	6	205	5700	156555	4483360	136368414	4432075200	154060613850
$N_{\mathrm{bi}}(n,2)$	0	20	960	33600	1111040	37202760	1295884800	47478243120

Figure 3: $N(n,2)$ and $N_{\mathrm{bi}}(n,2)$ for $n = 4, 5, \ldots, 11$

Hence, the asymptotic behavior of the number of *bicycles* in $K_{r,s}$ with $r+s=n$ coincides with one half of that in K_n.

For general k, we have the following asymptotic equality.

Theorem 3.3. *For $k \geq 0$, as $n \to \infty$,*

$$N_{\mathrm{bi}}(n,k) \sim \frac{1}{2^{k-1}} N(n,k). \tag{3}$$

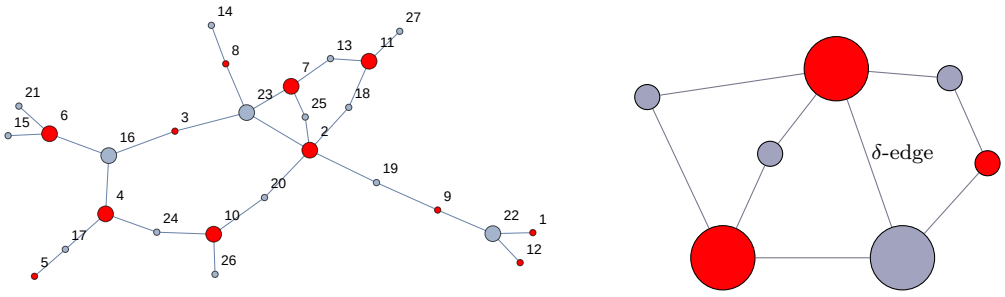
Remark 3.4. We can show that the spanning trees in $K_{r,s}$ for some (r,s) with $r+s=n$ are in two-to-one correspondence with those in K_n. Therefore, we obtain the following equation:

$$N_{\mathrm{bi}}(n,0) = 2N(n,0),$$

which gives (3) for $k=0$.

4 Another expression for F_k

Roughly speaking, for each connected bipartite graph $G=(V,E)$, we can obtain a simplified graph $\mathcal{B}(G)$, which is called *basic graph*, by deleting leafs and its adjacent edges of G and contracting their paths. We give an example of obtained basic graph $\mathcal{B}(G)$ in Figure 4.



(a) $(12,15,29)$-graph G. (b) $(3,4,9)$-basic graph $\mathcal{B}(G)$.

Figure 4: Example of G and obtained basic graph $\mathcal{B}(G)$.

Note that the Betti number of $\mathcal{B}(G)$ is equal to that of G. By the combinatorial argument developed in [4], for given $\mathcal{B}$, we reconstruct connected bipartite graphs, and we have the another expression of F_k.

Theorem 4.1. *For $k \geq 2$, $F_k(x,y)$ is decomposed into the sum of rational functions of T_x and T_y over basic graphs as*

$$F_k(x,y) = \sum_{\mathcal{B} \in BG_k} J_{\mathcal{B}}(x,y)$$

with

$$J_{\mathcal{B}}(x,y) = \frac{T_x^{|V_1|}T_y^{|V_2|}}{g_{\mathcal{B}}(1-T_xT_y)^{N_{\mathrm{sp}}+k-1-d}},$$

where $V_1 \sqcup V_2$ *is the vertex set of* $\mathcal{B}$*,* $g_{\mathcal{B}}$ *is the number of automorphisms of* $\mathcal{B}$*,* N_{sp} *and* d *are the numbers of vertices with degree* ≥ 3 *and* δ*-edges in* $\mathcal{B}$*, respectively.*

For example, if we take $\mathcal{B}$ as the above $\mathcal{B}(G)$ in Figure 4, we have

$$J_{\mathcal{B}}(x,y) = \frac{T_x^{|V_1|}T_y^{|V_2|}}{g_{\mathcal{B}}(1-T_xT_y)^{N_{\mathrm{sp}}+k-1-d}} = \frac{T_x^3T_y^4}{2(1-T_xT_y)^4}.$$

For definition of *δ-edge* and more details, see [1].

References

[1] T. Hasui, T. Shirai, and S. Yabuoku, Enumeration of connected bipartite graphs with given Betti number. ArXiv:2208.03996

[2] R. Kutzelnigg. Random graphs and Cuckoo Hashing. A precise average case analysis of Cuckoo Hashing and some parameters of sparse random graphs. Sudwestdeutscher Verlag für Hochschuleschriften, 2009.

[3] H. I. Scoins. The number of trees with nodes of alternate parity. Proc. Cambridge Philos. Soc. **58** (1962), 12–16.

[4] E. M. Wright. The number of connected sparsely edged graphs. J. Graph Theory **1** (1977), 317–330.

Equiangular lines with common angle $\arccos(1/3)$

吉野 聖人
広島工業大学情報学部情報工学科

1 はじめに

本稿では共通角度 $\arccos(1/3)$ の等角直線族の個数に関する結果を紹介する．

まず、**等角直線族**とは互いに成す角が一定であるような原点を通る直線の集合である．例えば、図 1 は角度 $\pi/3$ の等角直線族の例である．正整数 d に対して，d 次元ユークリッド空間内

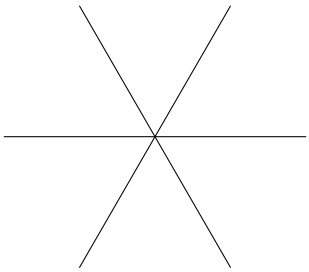


図 1: 2 次元ユークリッド空間内の角度 $\pi/3$ の等角直線族のひとつ

の角度 $\arccos(\alpha)$ の等角直線族の最大濃度 $N_\alpha(d)$ は盛んに研究されてきた．その歴史は 1940 年代 [3] にまで遡る．Lemmens 氏と Seidel 氏は d 次元空間内において共通角度 $\arccos(\alpha)$ の等角直線族の本数が $n > 2d$ を満たすならば $1/\alpha$ は奇数であることを証明した [4]．そのため、α が奇数の逆数の場合が主な研究対象となる．特に一番簡単な $\alpha = 1/3$ の場合は，Lemmens 氏と Seidel 氏 [4] がピラー法を導入して $N_{1/3}$ の全ての値を決定した. その後しばらくして、より詳

表 1: d 次元空間内の共通角度 $\arccos(1/3)$ の等角直線族の最大本数 [4]

d	3–4	5	6	7–14	15–
$N_{1/3}(d)$	$2(d-1)$	10	16	28	$2(d-1)$

細に共通角度 $\arccos(1/3)$ の等角直線族の研究が始まった．まず、等角直線族を含む最小の空間の次元をその**階数**と呼ぶ．そして，階数 d かつ共通角度 $\arccos(\alpha)$ の等角直線族の最大濃度を $N^*_\alpha(d)$ とするとき，$d \in \{8, \dots, 11\}$ に対して $N^*_{1/3}(d) < 28 = N^*_{1/3}(7)$ が示されている [2]．さらに Lin 氏と Yu 氏は $N^*_{1/3}(8) = 14$ [5] を示し，階数 8 で共通角度 $\arccos(1/3)$ かつ濃度 14 の等角直線族は一意であることも示している [5]. 本稿で報告する主結果ではないが，Meng-Yue Cao 氏，Jack H. Koolen 氏，宗政昭弘氏との共同研究により $d \geq 8$ ならば $N^*_{1/3}(d) = 2(d-1)$、かつそうでないとき $N^*_{1/3}(d) = N_{1/3}(d)$ を示している [1]．実際には極大な共有角度 $\arccos(1/3)$ の等角直線族の決定というより詳細な結果を与えている．ここまでで紹介したような本数が多

い等角直線族の研究がある一方で、等角直線族の個数自体を観察した研究もある．それを紹介するためにまず次の定義で記号を導入する．

定義 1. 非負整数 n に対して，$\omega(n)$ を 7 次元空間内かつ共通角度 $\arccos(1/3)$ の n 本の等角直線族の個数とする．また $s(n)$ を単に共通角度 $\arccos(1/3)$ の n 本の等角直線族の個数とする．なお、ここでの個数は等長変換をのぞいて数えている．

Szöllősi 氏と Östergård 氏は $\omega(n)$ に関する表 2 を与えた [7]．それをグラフにすると図 2 となり対称になっていることに気づく．ただし，不思議と $\omega(6)$ と $\omega(22)$ は 1 だけ異なる． 本稿

表 2: $\omega(n)$ の値

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	13
$\omega(n)$	0	1	1	2	3	5	**9**	16	23	37	54	70	90	101	103
n	28	27	26	25	24	23	22	21	20	19	18	17	16	15	
$\omega(n)$	1	1	1	2	3	5	**10**	16	23	37	54	70	90	101	

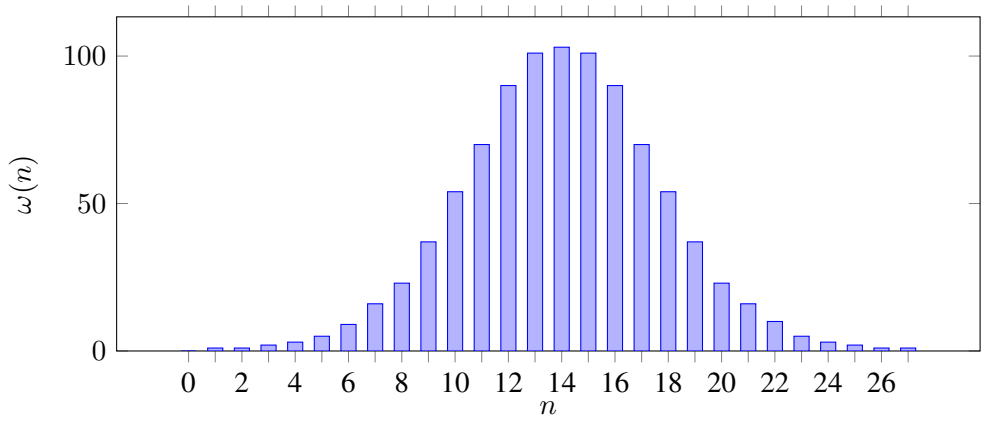


図 2: $\omega(n)$ の棒グラフ

で紹介する結果の 1 つである次の定理 2 はこの対称性を説明したものである

定理 2. $n \in \{0, \ldots, 28\} \setminus \{6, 22\}$ に対して $\omega(n) = \omega(28 - n)$．また $\omega(6) + 1 = \omega(22)$.

また，彼らは $s(n)$ も小さい n の範囲では PC で列挙し表 3 を与えている．本稿で紹介する 2

表 3: $s(n)$ の値

n	3	4	5	6	7	8	9	10	11	12	13
$s(n)$	2	3	5	9	16	25	40	58	75	96	108

つめの結果である定理 3 はすべての $s(n)$ を与える．

定理 3. 非負整数 n に対して

$$s(n) = \begin{cases} \omega(n) & \text{if } n \leq 7, \\ \omega(n) + n - 6 & \text{if } 8 \leq n \leq 12, \\ \omega(n) + \left\lfloor \frac{n}{2} \right\rfloor + 1 & \text{if } 13 \leq n. \end{cases}$$

2 つの結果はいずれも [1] で導入されたスイッチングルートを用いて作られるルート格子によって得られる．そのため、まず準備として基本的な用語を導入する．

2 準備

対角成分が 0 で非対角成分が ± 1 である対称行列は**サイデル行列**と呼ばれる．2 つのサイデル行列 S と S' が**スイッチング同値**であるとは，ある ± 1 対角行列 D と置換行列 P が存在して $S = (PD)S'(PD)^\top$ が成り立つことである．またそのとき $S \sim_{\mathrm{sw}} S'$ と書き，$[S] := \{S' : \text{サイデル行列} \mid S \sim_{\mathrm{sw}} S'\}$ と定める．

グラフ Γ に対してサイデル行列 $S(\Gamma)$ を $S(\Gamma) := J - I - 2A(\Gamma)$ によって定める．ただし，$A(\Gamma)$ はグラフ Γ の隣接行列を表し，J は成分が全て 1 の行列を表す．さらに，$S(G)$ の固有値のを**サイデル固有値**と呼ぶ．また，2 つのグラフ Γ と Δ に対して，$S(\Gamma)$ と $S(\Delta)$ がスイッチング同値であるとき，2 つのグラフは**スイッチング同値**であるという．グラフ Γ とスイッチング同値なグラフ全体を $[\Gamma]$ で表す．

最大固有値 λ である位数 n のサイデル行列 S に対して，$r := \mathrm{rank}(\lambda I - S)$ とおく．このとき，$I - S/\lambda$ は半正値であるからある単位ベクトル $\mathsf{u}_1, \dots, \mathsf{u}_n \in \mathbb{R}^r$ が存在して

$$(I - S/\lambda)_{i,j} = (\mathsf{u}_i, \mathsf{u}_j)$$

を満たす．そのため，$\{\mathbb{R}\mathsf{u}_1, \dots, \mathbb{R}\mathsf{u}_n\}$ は階数 r かつ角度 $\arccos(1/\lambda)$ の等角直線族である．逆にこの等角直線族からスイッチング同値を除いて元のサイデル行列は復元される．よって以降は等角直線族の代わりにサイデル行列，或いはそのスイッチングクラスを主に扱う．

3 ルート格子

本稿で扱う格子は全て整格子であるとする．長さ $\sqrt{2}$ のベクトルをルートといい、ルートで生成される格子をルート格子という．既約ルート格子は次のように分類される．

$$\begin{aligned}
\mathsf{A}_n &:= \{\mathsf{v} \in \mathbb{Z}^{n+1} \mid (\mathsf{v}, \mathsf{j}) = 0\} \quad (n \in \mathbb{Z}_{\geq 1}),\\
\mathsf{D}_n &:= \{\mathsf{v} \in \mathbb{Z}^{n} \mid (\mathsf{v}, \mathsf{j}) \in 2\mathbb{Z}\} \quad (n \in \mathbb{Z}_{\geq 4}),\\
\mathsf{E}_8 &:= \mathsf{D}_8 \sqcup (\mathsf{j}/2 + \mathsf{D}_8)\,,\\
\mathsf{E}_7 &:= \{\mathsf{v} \in \mathsf{E}_8 \mid (\mathsf{v}, \mathsf{e}_1 - \mathsf{e}_2) = 0\},\\
\mathsf{E}_6 &:= \{\mathsf{v} \in \mathsf{E}_8 \mid (\mathsf{v}, \mathsf{e}_1 - \mathsf{e}_2) = (\mathsf{v}, \mathsf{e}_2 - \mathsf{e}_3) = 0\}.
\end{aligned}$$

ただし，e_i は第 i 成分が 1 で他の成分は 0 であるベクトルとし，j は成分が全て 1 のベクトルである．

ルート格子 L のワイル群を $W(\mathsf{L})$ と書く．そして，2 つのルート格子 L, M の間の等長変換全体の集合を $\mathrm{Hom}(\mathsf{L}, \mathsf{M})$ とかく．さらに，各 $\mathsf{u} \in \mathsf{L}$ と $\mathsf{v} \in \mathsf{M}$ に対して，$\mathrm{Hom}((\mathsf{L}, \mathsf{u}), (\mathsf{M}, \mathsf{v})) := \{f \in \mathrm{Hom}(\mathsf{L}, \mathsf{M}) \mid f(\mathsf{u}) = \mathsf{v}\}$ とする．等長写像については次の定理を後ほど用いる．

定理 4 ([6])**.** 階数 8 以下の既約ルート L を取る．$|W(\mathsf{E}_8) \backslash \mathrm{Hom}(\mathsf{L}, \mathsf{E}_8)|$ の濃度は L が A_7 または D_8 と同型のときちょうど 2 であり，そうでないとき 1 である．

4　スイッチングルート

グラフ G に対して，その**錐**は $\tilde{G}$ で表され，G に新しい点を追加してその点と G の全ての点を結んでできるグラフとして定義される．この定義のもとで次が成り立つ．

定理 5. 任意のグラフ G に対して以下は同値である．

(1) サイデル行列 $S(G)$ の最大固有値は 3 以下である．

(2) 錐 $\tilde{G}$ の隣接行列 $A(\tilde{G})$ の最小固有値は -2 以上である．

いずれかが成り立つ場合，$\mathrm{rank}(3I - S(G)) + 1 = \mathrm{rank}(A(\tilde{G}) + 2I)$ が成り立つ．

この定理によって次の定義内でうまくベクトルが取れることが分かる．

定義 6. サイデル最大固有値 3 以下の位数 n のグラフ G をとる．ベクトル $\mathsf{u}_0, \ldots, \mathsf{u}_n$ を $A(\tilde{G}+2I)$ をグラム行列に持つものとする．このとき，既約ルート格子 $\Lambda(G) := \langle \mathsf{u}_0, \ldots, \mathsf{u}_n \rangle$ が定まる．このように格子を作るときの u_0 を**スイッチングルート**と呼ぶ．

なおこの定義において $\Lambda(G) = \Lambda(H)$ $(H \in [G])$ が成り立つ．詳細は [1] を参照されたい．

5　定理 2 の証明の概略

本章では定理 2 の証明の概略を与える．

定義 7. 非負整数 n を取る．最大固有値が 3 以下のサイズ n のサイデル行列全体の集合を $\mathcal{S}^{(n)}$ と書く．また既約ルート格子 L に対して $\mathcal{S}^{(n)}(\mathsf{L}) := \{S(G) \in S^{(n)} \mid \Lambda(G) = \mathsf{L}\}$ と定める．また，

$$\Omega^{(n)} := \bigsqcup_{\mathsf{L}:\ 8\text{ 次元以下の既約ルート格子}} S^{(n)}(\mathsf{L})$$

とおく．

定義と定理 5 から $s(n) = |S^{(n)}|$ と $\omega(n) = |\Omega^{(n)}|$ である．そして $\Lambda(\cdot)$ の定義から次が得られる．

補題 8.

$$S^{(n)}/\sim_{\mathrm{sw}} = \bigsqcup_{\mathsf{L}:\ \text{既約ルート格子}} \mathcal{S}^{(n)}(\mathsf{L})/\sim_{\mathrm{sw}}$$

これより，$s(n)$ を決定するには $S^{(n)}(\mathsf{A}_m)$ と $S^{(n)}(\mathsf{D}_m)$ を決定すれば良い．しかしこれは A_m や D_m のルートは簡単に記述できるので次の結果が得られ，直ちに定理 2 が従う．

補題 9. 整数 $n \geq 3$ に対して $\mathcal{S}^{(n)}(\mathsf{A}_m)/\sim_{\mathrm{sw}}$ は $m = n+1$ のとき $\{[S(K_n)]\}$，そうでないとき空である．整数 $n \geq 4$ に対して $\mathcal{S}^{(n)}(\mathsf{D}_m)/\sim_{\mathrm{sw}}$ は $2(m-2) \geq n \geq m-1$ のとき $\{[S(D_{m-2,n-m+2})]\}$，そうでないとき空である．

6　定理 3 の証明の概略

まず，$\Omega^{(n)}$ は最大固有値が 3 以下かつ $\mathrm{rank}(3I-S)\leq 7$ のサイデル行列 S 全体の成す集合と一致するのであった．故に，$\Omega^{(n)}$ と $\Omega^{(28-n)}$ の間に写像を作ることで定理 3 の主張である対称性を説明する．

ルート格子 E_8 のルート全体を R と書き，ルートを 1 つ固定し $\mathsf{r}\in R$ とする．このとき，$N(\mathsf{E}_8):=\{\mathsf{u}\in R\mid(\mathsf{r},\mathsf{u})=1\}$ とおく．さらに R 上の同値関係 $\sim$ を

$$\mathsf{u}\sim\mathsf{v}:\Longleftrightarrow\ \mathsf{u}=\mathsf{v}\ \text{または}\ \mathsf{u}=\mathsf{r}-\mathsf{v}$$

で定める．このとき写像

$$\begin{array}{rccc}\bar{\phi}_n: & W(\mathsf{E}_8)_{\mathsf{r}}\backslash\binom{N(\mathsf{E}_8)/\sim}{n} & \to & \Omega^{(n)}/\sim_{\mathrm{sw}}\\ & W(\mathsf{E}_8)_{\mathsf{r}}\{[\mathsf{u}_1],\dots,[\mathsf{u}_n]\} & \mapsto & [S(G)].\end{array}$$

を $A(G)+2I$ が $\mathsf{u}_1,\dots,\mathsf{u}_n$ のグラム行列になる G で定義する．これが well-defined になることは明らかではないが，自然に確かめることができる．この写像に関して次が成り立つことを証明すれば、補集合を取る全単写

$$\begin{array}{rcl}W(\mathsf{E}_8)_{\mathsf{r}}\backslash\binom{N(\mathsf{E}_8)/\sim}{n} & \to & W(\mathsf{E}_8)_{\mathsf{r}}\backslash\binom{N(\mathsf{E}_8)/\sim}{28-n}\\ W(\mathsf{E}_8)_{\mathsf{r}}\{[\mathsf{u}_1],\dots,[\mathsf{u}_n]\} & \mapsto & W(\mathsf{E}_8)_{\mathsf{r}}\left((N(\mathsf{E}_8)/\sim)\backslash\{[\mathsf{u}_1],\dots,[\mathsf{u}_n]\}\right).\end{array}$$

があるので定理 3 が直ちに従う．

定理 10. 非負整数 $n\neq 6$ に対して $\bar{\phi}_n$ は全単射である．また写像 $\bar{\phi}_6$ による $[S(K_6)]$ は濃度 2 の逆像をもち，そのほかの逆像はすべて濃度 1 である．

Proof. まず逆像を考え全射性を示し，その後その濃度を考える．任意に $\Omega^{(n)}/\sim_{\mathrm{sw}}$ の元 $[S(G)]$ を取る．このとき，$A(\tilde{G})+2I$ をグラム行列に持つベクトル $\mathsf{v}_0,\dots,\mathsf{v}_n$ が取れる．なお，$\Lambda(G)$ はこれらのベクトルで生成されるルート格子であった．そして $[S(G)]$ の逆像が

$$\{W(\mathsf{E}_8)_{\mathsf{r}}f(\{[\mathsf{v}_1],\dots,[\mathsf{v}_n]\})\mid f\in\mathrm{Hom}((\mathsf{L},\mathsf{v}_0),(\mathsf{E}_8,\mathsf{r}))\},\tag{6.1}$$

と書ける．ワイル群 $W(\mathsf{E}_8)$ はルート全体 R に推移的に作用するので $\mathrm{Hom}((\mathsf{L},\mathsf{v}_0),(\mathsf{E}_8,\mathsf{r}))$ と $\mathrm{Hom}(\mathsf{L},\mathsf{E}_8)$ の間に自然な同型が存在する．したがって定理 4 より $\Lambda(\Gamma)$ が A_7 と D_8 のどちらとも同型でないとき，逆像 (6.1) の濃度は 1 となる．次に $\Lambda(G)$ が D_8 と同型なときも $\mathrm{Hom}((\mathsf{L},\mathsf{v}_0),(\mathsf{E}_8,\mathsf{r}))$ の元となる具体的な 2 つの写像が分かり，逆像 (6.1) を計算すると結局は濃度が 1 だと分かる．最後に $\Lambda(G)$ が A_7 と同型なときは，まず $[G]=[K_6]$ となることが分かる．そして，E_8 の中に A_7 と同型な格子がちょうど 2 つあることは知られており，逆像 (6.1) の濃度がちょうど 2 つであることが従う．□

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] M.-Y. Cao, J. H. Koolen, A. Munemasa, and K. Yoshino. Maximality of Seidel matrices and switching roots of graphs. *Graphs Combin.*, 37(5):1491–1507, 2021.

[2] A. Glazyrin and W.-H. Yu. Upper bounds for s-distance sets and equiangular lines. *Adv. Math.*, 330:810–833, 2018.

[3] J. Haantjes. Equilateral point-sets in elliptic two- and three-dimensional spaces. *Nieuw Arch. Wiskunde (2)*, 22:355–362, 1948.

[4] P. W. H. Lemmens and J. J. Seidel. Equiangular lines. *J. Algebra*, 24:494–512, 1973.

[5] Y.-C. R. Lin and W.-H. Yu. Equiangular lines and the Lemmens-Seidel conjecture. *Discrete Math.*, 343(2):111667, 18, 2020.

[6] T. Oshima. A classification of subsystems of a root system. *arXiv:0611904v4*, 2007.

[7] F. Szöllősi and P. Östergård. Enumeration of Seidel matrices. *European J. Combin.*, 69:169–184, 2018.

Rank-Metric Codes and Matroids

城本　啓介
熊本大学大学院先端科学研究部（工学系）
keisuke@kumamoto-u.ac.jp

1　Codes and Matroids

S を有限集合とし，$\rho : 2^S \to \mathbb{Z}$ を関数とする．次の 3 つの条件を満たす順序対 $M = (S, \rho)$ を**マトロイド** (cf. [21]) という．

(1) $X \subseteq S$ ならば，$0 \leq \rho(X) \leq |X|$ である．

(2) $X, Y \subseteq S$ かつ $X \subseteq Y$ ならば，$\rho(X) \leq \rho(Y)$ である．

(3) $X, Y \subseteq S$ ならば，$\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y)$ である．

$\mathbb{F}_q$ を q-元体とする．$\mathbb{F}_q$ 上の $[n, k]$-符号 C と任意の部分集合 $X \subseteq S := \{1, 2, \ldots, n\}$ に対して，

$$\rho(X) := \dim C \setminus (S - X) (= \dim C - \dim C(S - X))$$

と定義する．ここで，任意の $Y \subseteq S$ に対して，$C \setminus Y$ は Y による punctured 符号を表し，

$$C(Y) := \{\boldsymbol{x} \in C \ : \ \mathrm{supp}(\boldsymbol{x}) \subseteq Y\}$$

とする．このとき，$M_C := (S, \rho)$ は上記の 3 条件を満たすので， M_C はマトロイドとなる．

マトロイド $M = (S, \rho)$ の階数母関数を次のように定義する．

$$R(M; x, y) := \sum_{X \subseteq S} x^{\rho(S) - \rho(X)} y^{|X| - \rho(X)}$$

1976 年に Greene ([18]) は，$\mathbb{F}_q$ 上の $[n, k]$-符号 C のハミング重み多項式 $W_C(x, y)$ と対応するマトロイド M_C の階数母関数の関係を示す次のよく知られた恒等式（Greene's identity と言われている）を証明した．

$$W_C(x, y) = y^{n - \dim C} (x - y)^{\dim C} R(M_C; \frac{qy}{x - y}, \frac{x - y}{y})$$

上記の結果の応用として，符号のハミング重み多項式に関するマックウィリアムズ恒等式の組合せ論的証明を与えている (cf. [28])．この論文以降，符号とマトロイドの関係に関する多くの論文が出版されている ([2, 3, 4, 25, 5, 8, 26, 27])．

2 (q,r)-ポリマトロイドと階数母関数

以後，$\mathrm{Mat}(n\times m,\mathbb{F}_q)$ により $\mathbb{F}_q$ 上の $n\times m$ 行列空間を表す．$\mathbb{F}_q$ 上のサイズ $n\times m$ の **(Delsarte) 階数距離符号** $\mathcal{C}$ ([10, 11]) とは，$\mathrm{Mat}(n\times m,\mathbb{F}_q)$ の $\mathbb{F}_q$-線形部分空間である．$E:=\mathbb{F}_q^n$ とし，$D\le E$ で D は E の部分空間であることを表すこととする．任意の部分空間 $J\le E$ に対して，次を定義する．

$$\begin{aligned}\mathcal{C}(J) &:= \{M\in\mathcal{C}\mid \mathrm{col}(M)\subseteq J\}\\ J^{\perp} &:= \{\boldsymbol{y}\in\mathbb{F}_q^n\mid \boldsymbol{x}\cdot\boldsymbol{y}=0,\ {}^{\forall}\boldsymbol{x}\in J\}\end{aligned}$$

ここで，$\mathrm{col}(M)$ は M の $\mathbb{F}_q$ 上の列空間を表す．

Lemma 1 $\mathcal{C}(J)$ は，$\mathrm{Mat}(n\times m,\mathbb{F}_q)$ の $\mathbb{F}_q$-線形部分空間である．

$\Sigma(J)$ により，E の任意の部分空間 J の全ての部分空間族を表す．

ここで，(q,r)-ポリマトロイドをマトロイド（正確には r-ポリマトロイド）の q-類似として，次のように定義する (cf. [22])．

Definition 2 (q,r)-**ポリマトロイド** は次の 3 つの条件を満たすベクトル空間 $E:=\mathbb{F}_q^n$ と関数 $\rho:\Sigma(E)\to\mathbb{Z}^+\cup\{0\}$ の順序対 $P=(E,\rho)$ である：

(R1) $A\le E$ ならば，$0\le\rho(A)\le r\dim A$ である．

(R2) $A,B\le E$ かつ $A\subseteq B$ ならば，$\rho(A)\le\rho(B)$ である．

(R3) $A,B\le E$ ならば，$\rho(A+B)+\rho(A\cap B)\le\rho(A)+\rho(B)$ である．

ここで，(R1) から $\rho(\{\mathbf{0}\})=0$ であり，$(q,1)$-ポリマトロイドは単に q-**マトロイド**と言われている．

Proposition 3 $\mathcal{C}$ を $\mathrm{Mat}(n\times m,\mathbb{F}_q)$ 内の階数距離符号とし，$\rho:\Sigma(E)\to\mathbb{Z}^+\cup\{0\}$ を任意の E の部分空間 J に対して，次のように定義する．

$$\rho(J):=\dim_{\mathbb{F}_q}\mathcal{C}-\dim_{\mathbb{F}_q}\mathcal{C}(J^{\perp})$$

このとき，$P_{\mathcal{C}}:=(E,\rho)$ は，(q,m)-ポリマトロイドである．

なお，マトロイドの q-類似と階数距離符号の関係については，近年活発的に研究が展開されている．興味がある方は，[19, 24, 14, 6, 17, 20, 15, 1, 7, 16] 等を参照されたい．

(q,r)-ポリマトロイド $P=(E,\rho)$ の**階数母関数**を次のように定義する．

$$R_P(X_1,X_2,X_3,X_4):=\sum_{D\in\Sigma(E)}f_P^D(X_1,X_2)g^{\dim D}(X_3,X_4)$$

ここで，任意の E の部分空間 J に対して，

$$f_P^J(X,Y) := X^{\rho(E)-\rho(J)}Y^{r\dim J-\rho(J)}$$

とし，任意の非負整数 $l \in \mathbb{Z}^+ \cup \{0\}$ に対して，

$$g^l(X,Y) := \prod_{i=0}^{l-1}(X - q^iY)$$

とする．

Proposition 4 任意の (q,r)-ポリマトロイド $P=(E,\rho)$ と任意の E の部分空間 J に対して，次のように関数を定める．

$$\rho^*(J) := \rho(J^\perp) + r\dim J - \rho(E)$$

このとき，順序対 $P^*=(E,\rho^*)$ は，(q,r)-ポリマトロイドである．

さらに，(q,r)-ポリマトロイド $P=(E,\rho)$ の階数母関数 $R_P(X_1,X_2,X_3,X_4)$ に対して，次の多項式を新たに定義する

$$\widehat{R}_P(X_1,X_2,X_3,X_4) := \sum_{D\in\Sigma(E)} f_P^D(X_1,X_2)g^{\dim D^\perp}(X_3,X_4)$$

このとき，(q,r)-ポリマトロイドの階数母関数について，次の双対性が得られる．

Theorem 5 $P=(E,\rho)$ を (q,r)-ポリマトロイドとする．このとき，

$$R_{P^*}(X_1,X_2,X_3,X_4) = \widehat{R}_P(X_2,X_1,X_3,X_4)$$

が成立する．

２つの行列 $M,N \in \mathrm{Mat}(n\times m,\mathbb{F}_q)$ の**トレース積**を次のように定める．

$$\langle M,N\rangle := \mathrm{Tr}(MN^{\mathrm{T}})$$

ここで，Tr は行列の対角和とする．

$\mathcal{C}$ を $\mathrm{Mat}(n\times m,\mathbb{F}_q)$ 内の階数距離符号とする．$\mathcal{C}$ の**双対符号**を次のように定義する．

$$\mathcal{C}^\perp := \{N \in \mathrm{Mat}(n\times m,\mathbb{F}_q) \,:\, \langle M,N\rangle = 0 \text{ for all } M\in\mathcal{C}\}$$

このとき，次の結果が知られている (Lemma 5 in [23]).

Lemma 6 ([23]) 階数距離符号 $\mathcal{C},\mathcal{D} \in \mathrm{Mat}(n\times m,\mathbb{F}_q)$ に対して，次のことが成立する．

(1) $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$

(2) $\dim_{\mathbb{F}_q}(\mathcal{C}^{\perp}) = nm - \dim_{\mathbb{F}_q}(\mathcal{C})$

(3) $(\mathcal{C} \cap \mathcal{D})^{\perp} = \mathcal{C}^{\perp} + \mathcal{D}^{\perp}$, *and* $(\mathcal{C} + \mathcal{D})^{\perp} = \mathcal{C}^{\perp} \cap \mathcal{D}^{\perp}$

Proposition 7 $\mathcal{C}$ を $\mathrm{Mat}(n \times m, \mathbb{F}_q)$ 内の任意の階数距離符号とし，$P_{\mathcal{C}} = (E, \rho)$ を Proposition 3 で記載したような手法で $\mathcal{C}$ から得られた (q, m)-ポリマトロイドとする．このとき，$P_{\mathcal{C}}^{*} = P_{\mathcal{C}^{\perp}}$ である．

Definition 8 (cf. [13, 23, 9]) $\mathcal{C}$ を $\mathrm{Mat}(n \times m, \mathbb{F}_q)$ 内の階数距離符号とする．$\mathcal{C}$ の**階数重み分布**を $\{A_i(\mathcal{C})\}_{i \in \mathbb{Z}_{\geq 0}}$ とする．ここで，

$$A_i(\mathcal{C}) := |\{M \in \mathcal{C} \,:\, \mathrm{rank}(M) = i\}|$$

である．$\mathcal{C}$ の**階数重み多項式**を次のように定義する．

$$W_{\mathcal{C}}^{\mathrm{R}}(x, y) := \sum_{i=0}^{\min\{n,m\}} A_i(\mathcal{C}) x^{\min\{n,m\}-i} y^i$$

以下が，本報告書の主結果である．(q, r)-ポリマトロイドと階数距離符号に対する Greene 型恒等式の一種であると言える．

Theorem 9 $\mathcal{C}$ を $\mathrm{Mat}(n \times m, \mathbb{F}_q)$ 内の任意の階数距離符号とし，$P_{\mathcal{C}} = (E, \rho)$ を Proposition 3 で記載したような手法で $\mathcal{C}$ から得られた (q, m)-ポリマトロイドとする．ここで，$n \leq m$ とする．このとき，次の等式が成立する．

$$W_{\mathcal{C}}^{\mathrm{R}}(x, y) = y^{n - \dim \mathcal{C}/m} R_{P_{\mathcal{C}}}(qy^{1/m}, \frac{1}{y^{1/m}}, x, y)$$

3　マックウィリアムズ恒等式への応用

本章では，Theorem 9 の応用の 1 つとして階数距離符号のマックウィリアムズ型恒等式を紹介する．Theorem 9，Proposition 7 と Theorem 5 を組み合わせることで次の等式が証明できる．

Proposition 10 $\mathcal{C}$ を $\mathrm{Mat}(n \times m, \mathbb{F}_q)$ 内の任意の階数距離符号とする．このとき，

$$W_{\mathcal{C}^{\perp}}^{\mathrm{R}}(x, y) = \frac{1}{|\mathcal{C}|} \sum_{S \in \Sigma(E)} A_{\mathcal{C}}(S) \sum_{j=0}^{n} \sum_{l=0}^{j} \begin{bmatrix} n - \dim S \\ j - l \end{bmatrix}_q \begin{bmatrix} n - j + l \\ l \end{bmatrix}_q (-1)^l q^{\binom{l}{2}} q^{m(j-l)} y^j x^{n-j},$$

が成立する．ここで，$\begin{bmatrix} a \\ b \end{bmatrix}_q$ は非負整数 a, b の q-２項係数を表す．

Proposition 10 はある種の階数距離符号のマックウィリアムズ型恒等式と見ることができるが，従来の線形符号の場合に近い形で表現するために，参考として [12, 13] で用いられている多項式の q-積や q-除算の概念を導入する．

Definition 11 ([12, 13]) $a(x,y;m) = \sum_{i=0}^{r} a_i(m)x^{r-i}y^i$ と $b(x,y;m) = \sum_{j=0}^{s} b_j(m)x^{s-j}y^j$ を非斉次多項式とする．$a(x,y;m)$ と $b(x,y;m)$ の q-**積** $c(x,y;m)$ を次の次数 $(r+s)$ の非斉次多項式で定義する．

$$c(x,y;m) := a(x,y;m) * b(x,y;m) = \sum_{u=0}^{r+s} c_u(m)x^{r+s-u}y^u$$

ここで,

$$c_u(m) := \sum_{i=0}^{u} q^{is} a_i(m) b_{u-i}(m-i)$$

である．$n \geq 0$ に対して，$a(x,y;m)$ の q-n **乗**を帰納的に次のように定義する．

$$\begin{aligned} a(x,y;m)^{[0]} &:= 1 \\ a(x,y;m)^{[n]} &:= a(x,y;m)^{[n-1]} * a(x,y;m),\ n = 1,2,\ldots \end{aligned}$$

Definition 12 ([12, 13]) $a(x,y;m) = \sum_{i=0}^{r} a_i(m)x^{r-i}y^i$ の q-**変換** を次の非斉次多項式で定義する．

$$\overline{a}(x,y;m) := \sum_{i=0}^{r} a_i(m)y^{[i]} * x^{[r-i]}$$

このとき，次の等式が成立することが分かる．

Lemma 13 (1) $\begin{bmatrix} a \\ b \end{bmatrix}_q = \begin{bmatrix} a-1 \\ b \end{bmatrix}_q + q^{a-b}\begin{bmatrix} a-1 \\ b-1 \end{bmatrix}_q = q^b\begin{bmatrix} a-1 \\ b \end{bmatrix}_q + \begin{bmatrix} a-1 \\ b-1 \end{bmatrix}_q$

(2) $\begin{bmatrix} a \\ b \end{bmatrix}_q \begin{bmatrix} b \\ c \end{bmatrix}_q = \begin{bmatrix} a \\ b-c \end{bmatrix}_q \begin{bmatrix} a-b+c \\ c \end{bmatrix}_q$

(3) $\begin{bmatrix} a \\ b \end{bmatrix}_q = \sum_{i=0}^{n} q^{i(a-b-n+i)} \begin{bmatrix} n \\ i \end{bmatrix}_q \begin{bmatrix} a-n \\ b-i \end{bmatrix}_q, \quad n = 0,1,\ldots,a$

(4) $\binom{a+b}{2} = \binom{a}{2} + ab + \binom{b}{2}$

これまでの議論を組み合わせることで，階数距離符号の別の表記でのマックウィリアムズ型恒等式が得られる．

Theorem 14 $\mathcal{C}$ を $\mathrm{Mat}(n \times m, \mathbb{F}_q)$ 内の任意の階数距離符号とする．ここで，$n \leq m$ とする．このとき，次の等式が成立する．

$$W_{\mathcal{C}^\perp}^{\mathrm{R}}(x,y) = \frac{1}{|\mathcal{C}|}\overline{W_{\mathcal{C}}^{\mathrm{R}}}(x + (q^m-1)y, x-y)$$

参考文献

[1] G. Alfarano, E. Byrne, The cyclic flats of a q-matroids, Preprint arXiv: 2204.02353 (2022).

[2] A. Barg, The matroid of supports of a linear code, *Appl. Algebra Engrg. Commun. Comput.* **8** (1997), pp. 165–172.

[3] T. Britz, Code enumerators and Tutte polynomials, *IEEE Trans. Inform. Theory* **56** (2010), 4350–4358.

[4] T. Britz and K. Shiromoto, On the covering dimension of a linear code, *IEEE Trans. Inform. Theory* **62** (2016), 2694–2701.

[5] T. Britz, K. Shiromoto, and T. Westerbäck, Demi-matroids from codes over finite Frobenius rings, *Des. Codes Cryptogr.* **75** (2015), pp. 97–107.

[6] T. Britz, A. Mammoliti, K. Shiromoto, Wei-type duality theorems for rank metric codes, *Des. Codes Cryptogr.* **88** (8), 1503–1519 (2020).

[7] E. Byrne, M. Ceria, R. Jurrius, Constructions of new q-cryptomorphisms, *J. Combin. Theory. Ser. B*, **153**, 149–194 (2022).

[8] T.H. Chan, A. Grant, and T. Britz, Quasi-uniform codes and their applications, *IEEE Trans. Inform. Theory* **59** (2013), 7915–7926.

[9] J. Cruz, E. Gorla, H.H. López and A. Ravagnani, Weight distribution of rank-metric codes, *Des. Codes Cryptogr.* **86** (2018), pp. 1–16.

[10] P. Delsarte, Bilinear forms over a finire field, with applications to coding theory, *Journal of Combinatorial Theory, Series A* **25** (1978), pp. 226–241.

[11] E.M. Gabidulin, Theory of codes with maximum rank distance (Russian), *Problemy Peredachi Informatsii* **21**, 3–16 (1985).

[12] M. Gadouleau and Z. Yan, MacWilliams identity for the rank metric, *ISIT2007*, Nice, France, June 24 - June 29, 2007, pp. 36–40.

[13] M. Gadouleau and Z. Yan, MacWilliams identity for the rank metric, *EURASIP Journal on Wireless Communications and Networking*, vol. **2008**, Article ID 754021, 13 pages.

[14] S. R. Ghorpade, T. Johnsen, A polymatroid approach to generalized weights of rank metric codes, *Des. Codes Cryptogr.*, **88**, 2531–2546 (2020).

[15] H. Gluesing-Luerssen, B. Jany, q-Polymatroids and their relation to rank-metric codes, *J. Algebraic Combin.*, **56**, 725–753 (2022).

[16] H. Gluesing-Luerssen, B. Jany, Coproducts in categories of q-matroids, *Eur. J. Comb.* **112**, 103733 (2023).

[17] E. Gorla, R. Jurrius, H.H. López, A. Ravagnani, Rank-metric codes and q-polymatroids, *J. Algebr. Comb.* **52**, 1–19 (2020).

[18] C. Greene, Weight enumeration and the geometry of linear codes, *Stud. Appl. Math.* **55** (1976), pp. 119–128.

[19] R. Jurrius, R. Pellikaan, Defining the q-analogue of a matroid, *Electron. J. Comb.* **25**(3), P3.2 (2018).

[20] C. Michela, J. Relinde, The direct sum of q-matroids, Preprint arXiv:2109.13637 (2021).

[21] J. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.

[22] J. Oxley and G. Whittle, A characterization of Tutte invariants of 2-polymatroids, *Journal of Combinatorial Theory, Series B* **59** (1993), pp. 210–244.

[23] A. Ravagnani, Rank-metric codes and their duality theory, *Designs, Codes, and Cryptography* **80** (2016), pp. 197–216.

[24] K. Shiromoto, Codes with the rank metric and matroids, *Des. Codes Cryptogr.* **87** (8), 1765–1776 (2019).

[25] J. Simonis, The effective length of subcodes, *Appl. Algebra Engrg. Commun. Comput.* **5** (1994), pp. 371–377.

[26] J. Simonis and A. Ashikhmin, Almost affine codes, *Des. Codes Cryptogr.*, **14** (1998), pp. 179–197.

[27] D. Vertigan, Latroids and their representation by codes over modules, *Trans. Amer. Math. Soc.* **356** (2004), pp. 3841–3868.

[28] D.J.A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

頂点代数上の加群のシュアー・ワイル型双対性

田邊顕一朗 (東京都市大学)

1 はじめに

頂点 (作用素) 代数は，ムーンシャイン予想の解決や 2 次元共形場理論の数学的定式化等を目的として 1986 年に Borcherds[4] によって導入された新しい代数系である．V を頂点代数，G を V の自己同型群としたとき，G によって固定される V の元の全体 $V^G = \{a \in V \mid \text{任意の } g \in G \text{ に対して } ga = a\}$ は V の部分代数となる．固定部分代数 V^G 加群は，よい性質をもつ頂点代数の構成への応用があるため，この分野の重要な研究対象となっている．例えば，Borcherds[5] によるムーンシャイン予想の解決で決定的な役割を果たしたムーンシャイン頂点作用素代数 [4, 14] は，格子に付随する頂点代数の固定部分代数とその加群を用いて構成されている．V^G 加群の研究において基本的な問題は，V 加群や群 G との関係である．V 加群は自然に V^G 加群となるが，V 加群と V^G 加群との対応を記述するためには，V 加群の拡張である twisted V 加群が必要となる．物理学者達による予想の一部を次に挙げる：

予想 [7]. V は単純な頂点作用素代数，G はその位数有限の自己同型群とする．

(i) 任意の既約 V^G 加群は，ある既約な g-twisted V 加群 ($g \in G$) の部分加群である．
(ii) 任意の V 加群が完全可約ならば，任意の V^G 加群もそうである．

ここで 1-twisted V 加群が通常の V 加群である．正確には，この予想は物理の論文である [7] の内容の一部を，頂点作用素代数の言葉で述べたものであり，頂点作用素代数にどのような条件を付けるかに関しては不確定さがある．ここでは反例が見つかっていないと理由から，「単純」という条件のみを仮定している．条件をより強くして，「V は単純かつ正則な頂点作用素代数」とする場合もある．この予想の現状については，[6, 11] 等を参照されたい．ここでは，この予想の前段階である次の問題を考える：予想 (i) に関して，そもそも既約 twisted V 加群の中に既約 V^G 加群がはいっているのか，あるいはもっと強く

問題 1. V が単純な頂点作用素代数のとき，既約な twisted V 加群 M は完全可約 V^G 加

群か？ つまり，M は既約 V^G 加群の直和になっているか？

この問題に対する系統的研究は，Dong–Mason[10] によって始められ，そこでは G が可解群で $M = V$ の場合が肯定的に解決された．その後，G が一般の有限群で $M = V$ のとき [9], M が V 加群のとき [13]，最終的には [17] で問題 1 は肯定的に解決された．この結果の $M = V$ の場合の応用として，単純頂点作用素代数上のガロア対応が示されている [9, 10, 15].

近年，Heisenberg 頂点代数の固定部分代数上のホイッタカー型既約弱加群の分類 [20] を一つの契機として，固定部分代数上の加群の系統的研究が開始されつつある (cf. [1, 2, 12])．そこでは問題 1 において「頂点作用素代数」を「可算次元[*1]の頂点代数」に変更したもの, つまり

問題 2. V が単純な可算次元の頂点代数のとき，既約な twisted V 加群 M は完全可約 V^G 加群か?

が考えられている．特に [12] ではその部分的解決である「g が G の中心に入っている場合には既約 g-twisted V 加群 M は完全可約 V^G 加群である」ことが示され，応用として単純頂点代数上のガロア対応が得られている．「頂点作用素代数」を「頂点代数」に変更しても，もとの予想や問題 1 が意味をなすことは明らかではあったが，頂点代数上の加群に対しては，頂点作用素代数上の加群に対して用いられてきた Zhu 代数などの強力な方法が使えなくなるため，以前は研究は非常に難しいと思われていたのである．最近，[20, 21, 22] の登場により以前よりは頂点代数上の加群 (頂点作用素代数上の弱加群) が扱えるようになってきた．今回はこの流れに沿って，問題 2 が完全に解決出来たことを報告する．

2 頂点 (作用素) 代数とその加群

頂点代数とその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.

[*1] 可算次元という条件は証明に Shur の補題 (既約 twisted V 加群 M に対して $\mathrm{End}_V M = \mathbb{C}$) が必要であるために仮定されている.

(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

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

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

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

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. [14, 16]) 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，次の条件を満たす $\omega \in V$ が存在することを仮定する．

(条件)　任意の $a \in V$ に対して $\omega_0 a = a_{-2}\mathbf{1}$.

この条件の下で V の加群を次のように定める[*2]．

定義 2.3. (頂点代数上の加群) 次の条件を全て満たす組 (M, Y_M) を V **加群**という．

(1) M は $\mathbb{C}$ 上のベクトル空間.

(2) $Y_M(\ ,x): \quad \begin{array}{ccc} V \otimes_{\mathbb{C}} M & \longrightarrow & M((x)) \\ \cup & & \cup \\ a \otimes u & \longmapsto & Y_M(a,x)u \end{array}$ 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．

(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．

有限位数の自己同型 $g \in \mathrm{Aut}\, V$ に対して，$V^r = \{a \in V \mid ga = e^{-2\pi\sqrt{-1}r/|g|}a\}$ $(r = 0, 1, \ldots, |g|-1)$ とおく．$V = \bigoplus_{r=0}^{|g|-1} V^r$ に注意する．

[*2] ω の存在を仮定せずに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．

定義 2.4. (頂点代数上の g-twisted 加群) $g \in \operatorname{Aut} V$ を有限位数の自己同型とする．次の条件を全て満たす組 (M, Y_M) を 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．さらに $a \in V^r$ のとき，$Y_M(a,x)u \in M((x))x^{-r/|g|}$ となっている．つまり，$i \notin r/T + \mathbb{Z}$ ならば $a_i u = 0$ となっている．

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

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

$$\begin{aligned} \iota_{x,y} Y_M(a,b,u|x,y) &= Y_M(a,x)Y_M(b,y)u \in M((x^{1/|g|}))((y^{1/|g|})), \\ \iota_{y,x} Y_M(a,b,u|x,y) &= Y_M(b,y)Y_M(a,x)u \in M((y^{1/|g|}))((x^{1/|g|})), \\ \iota_{y,x-y} Y_M(a,b,u|x,y) &= Y_M(Y(a,x-y)b,y)u \in M((y^{1/|g|}))((x-y)) \end{aligned}$$

となる．上の左辺の展開は (2.1) と同様に定める．

Remark 2.5. 2 つの異なる有限位数の自己同型 $g, h \in \operatorname{Aut} V$ が与えられたとき，g-twisted V 加群 M と h-twisted V 加群 N の直和 $M \oplus N$ は，twisted 加群の定義 2.4 (2) より，一般には twisted 加群にならないことに注意する．つまり，自己同型が異なる twisted 加群は直和で閉じていない．これは加群論においては致命的な欠点であり，実際先行研究 [12, 13] では今回の主結果 (定理 3.4) を，V 加群に制限した形でしか示すことが出来なかった．twisted 加群を直和で閉じるように拡張することを目的として，筆者が以前 (2015 年) 導入したものが次の (V,T) 加群 [19] である．もちろん今回の結果を見越して導入したわけではないが，定理 3.4 は (V,T) 加群の基本性質である補題 3.6 を用いて，既存の枠組みで直ちに証明出来る．これは (V,T) 加群の概念の有用性を示している．

定義 2.6. ((V,T) 加群) T を正の整数とする．次の条件を全て満たす組 (M, Y_M) を (V,T) **加群**という．

(1) M は $\mathbb{C}$ 上のベクトル空間.

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

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

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

$$\begin{aligned}\iota_{x,y} Y_M(a, b, u|x, y) &= Y_M(a, x) Y_M(b, y) u \in M(\!(x^{1/T})\!)(\!(y^{1/T})\!),\\ \iota_{y,x} Y_M(a, b, u|x, y) &= Y_M(b, y) Y_M(a, x) u \in M(\!(y^{1/T})\!)(\!(x^{1/T})\!),\\ \iota_{y,x-y} Y_M(a, b, u|x, y) &= Y_M(Y(a, x-y)b, y) u \in M(\!(y^{1/T})\!)(\!(x-y)\!)\end{aligned}$$

となる．

Remark 2.7. (1) T, T' を二つの正の整数，T'' を T, T' の公倍数とする．(V, T) 加群 M と (V, T') 加群 N はともに (V, T'') 加群となり，さらに直和 $M \oplus N$ は (V, T'') 加群となる．この意味で (V, T) 加群は直和で閉じている．

(2) $(V, 1)$ 加群の定義は V 加群の定義と一致する．

(3) 有限位数の自己同型 $g \in \mathrm{Aut}\, V$ と，$|g||T$ となる正の整数 T に対して g-twisted V 加群は (V, T) 加群となる．

(4) twisted 加群と (V, T) 加群との違いは，定義 2.4 (2) 中の条件である「$a \in V^r$ のとき，$Y_M(a, x)u \in M(\!(x)\!)x^{-r/|g|}$」があるかないかだけである．一見してあまり違いはないように思えるが，twisted 加群と比較して (V, T) 加群を調べることは遙かに難しくなる．twisted 加群は $a \in V^r$ と調整した上で，掛け算 $x^{r/|g|} Y_M(a, x)u \in M(\!(x)\!)$ をとることにより整数べき $M(\!(x)\!)$ の中で扱うことが出来るが，(V, T) 加群はそう出来ないことが大雑把な理由である．

次の結果は，(V, T) 加群が twisted 加群の拡張になっていることを示している：

補題 2.8. [23, Lemma 2.4] V を単純な頂点代数，$g, h \in \mathrm{Aut}\, V$ を有限位数の自己同型，T を $|g|, |h|$ の公倍数，M を g-twisted V 加群，N を h-twisted V 加群とする．このとき，(V, T) 加群として $M \cong N$ であるためには，$g = h$ かつ g-twisted V 加群として $M \cong N$ であることが必要十分である．

Remark 2.9. 上の補題で頂点代数が単純という仮定は必要である．V を頂点代数，M をその加群とし，$\tilde{V} = V \oplus M$ に次で頂点代数構造を入れる．

$$Y_{\tilde{V}}(a, x)b = \begin{cases} Y_V(a, x)b & a, b \in V,\\ Y_M(a, x)b & a \in V, b \in M,\\ e^{\omega_0 x} Y_M(b, -x)a & a \in M, b \in V,\\ 0 & a, b \in M.\end{cases}$$

$\tilde{V}$ はイデアル M を持つため，単純ではない．$g \in \operatorname{Aut}\tilde{V}$ を，$g|_V = \mathrm{id}_V, g|_M = -\mathrm{id}_M$ で定める．定義から直接分かることだが，$Y_{\tilde{V}}(a,x)$ $(a \in \tilde{V})$ を M 上に制限することにより，M は $\tilde{V}$ 加群にも g-twisted $\tilde{V}$ 加群にもなってしまう．この例から分かるように，twisted 加群よりも (V,T) 加群の方が概念として自然であることが分かる．

次に V が頂点作用素代数であるとき，V 加群の定義を紹介する．V が頂点作用素代数の場合には，頂点作用素代数としての V 加群と，頂点代数としての V 加群は定義が異なることに注意する．

定義 2.10. (頂点作用素代数上の加群) V を頂点作用素代数とする．定義 2.3 の条件 (1)–(4) を全て満たす (M, Y_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，さらに

(5) 任意の $i \in \mathbb{C}$ に対して $\dim_{\mathbb{C}} M_i < \infty$ である．
(6) 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．

V が頂点作用素代数であるとき，頂点作用素代数としての g-twisted V 加群は，上の定義中の「定義 2.3」を「定義 2.4」に，「$\mathbb{Z} \ni n \ll 0$」を「$(1/|g|)\mathbb{Z} \ni n \ll 0$」に変更して定義する．頂点作用素代数としての (V,T) 加群も同様に定義する．

3 半単純 $\mathbb{C}$ 多元環 $A_\alpha(G,S)$ と双対性

以下，T は固定された正の整数とする．(V,T) 加群と (V^G,T) 加群とを，定義 3.3 で定める半単純 $\mathbb{C}$ 多元環 $A_\alpha(G,S)$ を通して結びつける．$\mathbb{C}$ 多元環 $A_\alpha(G,S)$ はホップ代数で研究されていたもの [3, 8, 18] を頂点作用素代数上の加群の言葉で書き直したものである [13]．ここではより一般的な (V,T) 加群の場合に拡張して述べる．拡張は自明である．

定義 3.1. $G \leq \operatorname{Aut} V$, S を (V,T) 加群からなる集合とする．

(1) (V,T) 加群 (M,Y_M) と $\sigma \in \operatorname{Aut} V$ に対して，(V,T) 加群 $(M \circ \sigma, Y_{M\circ\sigma})$ を，

$$M \circ \sigma = M, \quad Y_{M\circ\sigma}(a,x) = Y_M(\sigma a, x)$$

で定める．

(2) 任意の $\sigma \in G, M \in S$ に対して $N \in S$ が存在して $M \circ \sigma^{-1} \cong N$ となるとき，つ

まりベクトル空間としての同型 $\phi(\sigma, M) : M \to N$ が存在して

$$\phi(\sigma, M)Y_M(a, x) = Y_N(\sigma a, x)\phi(\sigma, M), a \in V \tag{3.1}$$

となるとき，S は G **安定**であるという．このとき，$N \in S$ を $M \cdot \sigma^{-1}$ で表すことにする．

Remark 3.2. M が g-twisted V 加群のとき，$M \circ \sigma$ は $\sigma g \sigma^{-1}$-twisted V 加群となる．

$M \in S$ が既約 (V, T) 加群のとき，$\sigma, \tau \in G$ に対して，$\alpha_M(\sigma, \tau) \in \mathbb{C}$ が存在して

$$\phi(\sigma, M \cdot \tau^{-1})\phi(\tau, M) = \alpha_M(\sigma, \tau)\phi(\sigma\tau, M). \tag{3.2}$$

となる．さらに $\sigma, \tau, \rho \in G$ に対して

$$\alpha_{M\cdot\rho^{-1}}(\sigma, \tau)\alpha_M(\sigma\tau, \rho) = \alpha_M(\sigma, \tau\rho)\alpha_M(\tau, \rho). \tag{3.3}$$

が成り立つ．

以降，G は $\mathrm{Aut}\, V$ の有限位数の部分群，S は非同型な既約 (V, T) 加群からなる G 安定な有限集合とする．

定義 3.3. $\mathbb{C}$ ベクトル空間 $A_\alpha(G, S) = \mathbb{C}[G] \otimes (\bigoplus_{M\in S} \mathbb{C}e(M))$ 上に積

$$(\sigma \otimes e(M)) \cdot (\tau \otimes e(N)) = \delta_{M\cdot\tau,N}\alpha_N(\sigma, \tau)\sigma\tau \otimes e(N). \tag{3.4}$$

を定義して $A_\alpha(G, S)$ は半単純 $\mathbb{C}$ 多元環となる．ここで $\mathbb{C}[G]$ は群環であり，$\bigoplus_{M\in S} \mathbb{C}e(M)$ は $e(M), M \in S$, を基底とするベクトル空間である．

$S = \bigcup_{j\in J} O_j$ を G の作用による S の分解とする．$j \in J$ に対して，O_j の代表元 $M^j \in O_j (\subset S)$ を一つずつ固定しておく．(V, T) 加群 M に対して，$G_M = \{\sigma \in G \mid M \circ \sigma \cong M\}$ とおく．$M \in S$ に対して $\alpha_M = \alpha|_{G_M\times G_M}$ は G_M の 2 コサイクルとなる．2 コサイクル α_M に付随する G_M の twisted 群環を $\mathbb{C}^{\alpha_M}[G_M]$ で表しておく．$\mathbb{C}^{\alpha_{M^j}}[G_{M^j}]$ の既約加群の同型類全体を Λ_j で表しておく．半単純 $\mathbb{C}$ 多元環 $A_\alpha(G, S)$ の既約加群の同型類の完全代表系は，$\Lambda := \{(j, \lambda) \mid j \in J, \lambda \in \Lambda_j\}$ として $\{W^j_\lambda \mid (j, \lambda) \in \Lambda\}$ と書くことが出来る．

$\mathscr{M} = \bigoplus_{M\in S}$ とおき，作用 $A_\alpha(G, S) \curvearrowright \mathscr{M}$ を次で定める：$M, N \in S$, $u \in N$, $\sigma \in G$ に対して

$$\sigma \otimes e(M) \cdot u = \delta_{M,N}\phi(\sigma, M)u. \tag{3.5}$$

$\mathbb{C}$ 多元環 $A_\alpha(G,S)$ は半単純であるから，各 $(j,\lambda) \in \Lambda$ に対して $M_\lambda^j := \mathrm{Hom}_{A_\alpha(G,S)}(W_\lambda^j, \mathscr{M})$ とおくと，M_λ^j は自然に (V^G,T) 加群となり，分解

$$\mathscr{M} = \bigoplus_{(j,\lambda)\in\Lambda} M_\lambda^j \otimes_{\mathbb{C}} W_\lambda^j \tag{3.6}$$

が成り立つ．この $\mathscr{M}$ の分解に関する次の結果が主結果である：

定理 3.4. [23, Theorem 1.1] T を正の整数，V を単純な可算次元の頂点代数，$G \leq \mathrm{Aut}\, V$ を有限位数の自己同型群，S を非同型な既約 (V,T) 加群からなる G 安定な有限集合とする．分解 (3.6) に関して次が成り立つ．

(1) 各 $(j,\lambda) \in \Lambda$ に対して，$M_\lambda^j \neq 0$ で，さらに M_λ^j は既約 (V^G,T) 加群である．
(2) $(j_1,\lambda_1),(j_2,\lambda_2) \in \Lambda$ に対して，$M_{\lambda_1}^{j_1} \cong M_{\lambda_2}^{j_2} \Leftrightarrow (j_1,\lambda_1) = (j_2,\lambda_2)$.

Remark 3.5.

(1) M を任意の既約 (V,T) 加群としたとき，$S = (\{M \circ \sigma \mid \sigma \in G\}$ の同型類の完全代表系) とおいて定理 3.4 を適用すれば，M は完全可約 (V^G,T) 加群であることが分かる．
(2) $S \subset \bigcup_{g\in G}$ (g-twisted V 加群) の場合は，各 M_λ^j は V^G 加群となる．
(3) Remark 3.2 より，ある $g \in G$ が存在して S が g-twisted V 加群のみからなるためには，g が G の中心に入っていることが必要十分である．このときは $\mathscr{M}$ は g-twisted 加群となるため，(V,T) 加群を持ち出す必要はない．この場合は [12] で既に扱われており，このときは定理 3.4 は [12, Theorem 7.4] に一致する．
(4) [19, Example 2.3] に twisted 加群でない既約 (V,T) 加群の例を挙げている．

定理 3.4 の証明は，(twisted)V 加群を (V,T) 加群に置き換えて [12, Section 7] の議論をそのまま適用すれば出来る．重要な部分は，その議論が適用出来るように必要な (V,T) 加群の次の性質を示すことである．

補題 3.6. [23, Lemma 2.7] M を頂点代数 V 上の加群，N を M の有限次元部分空間，$a,b \in V, m,n \in (1/T)\mathbb{Z}$ とする．このとき，有限和 $\sum_{i\in\mathbb{Z}} \lambda_i a_i b, \lambda_i \in \mathbb{C}$ が存在して，任意の $u \in N$ に対して

$$a_m b_n u = \sum_{i\in\mathbb{Z}} \lambda_i (a_i b)_{m+n-i} u$$

となる．

Remark 3.7. 通常の環 A 上の加群 M において，「$a, b \in A$ と $u \in M$ に対して $(ab)u = a(bu)$」は加群の定義の一部である．補題 3.6 はこれの (V, T) 加群における類似であるが，証明しなければならない事項である．また，twisted V 加群においては，これはよく知られた結果である (cf. [16, Proposition 4.5.7]).

参考文献

[1] D. Adamović, C. H. Lam, V. Pedić, and N. Yu, *On irreducibility of modules of whittaker type for cyclic orbifold vertex algebras*, J. Algebra **539** (2019), 1–23.

[2] D. Adamović, C. H. Lam, V. Pedić, and N. Yu, *On irreducibility of modules of whittaker type: twisted modules and nonabelian orbifolds*, https://arxiv.org/abs/2212.14137, 2022.

[3] R. J. Blattner, M. Cohen and S. Montgomery, *Crossed products and inner actions of Hopf algebras*, Transactions of the American Mathematical Society **298** (1986), no. 2, 671–711.

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

[5] R. Borcherds, *Monstrous moonshine and monstrous Lie superalgebras*, Invent. Math. **109** (1992), 405–444.

[6] S. Carnahan and M. Miyamoto, *Regularity of fixed-point vertex operator subalgebras*, https://doi.org/10.48550/arXiv.1603.05645.

[7] R. Dijkgraaf, C. Vafa, E. Verlinde, and H. Verlinde, *The operator algebra of orbifold models*, Comm. Math. Phys. **123** (1989), 485–526.

[8] Y. Doi and M. Takeuchi, *Cleft comodule algebras for a bialgebra*, Communications in Algebra **14** (1986), no. 5, 801–817.

[9] C. Dong, H. S. Li and G Mason, *Compact automorphism groups of vertex operator algebras*, Internat. Math. Res. Notices **18** (1996), 913–921.

[10] C. Dong and G. Mason, *On quantum Galois theory*, Duke Math. J. **86** (1997), 305–321.

[11] C. Dong, L. Ren and F. Xu, *On orbifold theory*, Advances in Mathematics **321** (2017), 1–30.

[12] C. Dong, L. Ren and C. Yang, *Orbifold theory for vertex algebras and Galois*

correspondence, https://arxiv.org/abs/2302.09474, 2023.

[13] C. Dong and G. Yamskulna, *Vertex operator algebras, generalized doubles and dual pairs*, Math. Z. **241** (2002), 397–423.

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

[15] A. Hanaki, M. Miyamoto and D. Tambara, *Quantum Galois theory for finite groups*, Duke Math. J. **97** (1999), 541–544.

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

[17] M. Miyamoto and K. Tanabe, *Uniform product of $A_{g,n}(V)$ for an orbifold model V and G-twisted Zhu algebra*, J. Algebra **274** (2004), 80–96.

[18] M. E. Sweedler, *Cohomology of algebras over Hopf algebras*, Transactions of the American Mathematical Society **133** (1968), 205–239.

[19] K. Tanabe, *A generalization of twisted modules over vertex algebras*, J. Math. Soc. Japan **67** (2015), no. 3, 1109–1146.

[20] K. Tanabe, *Simple weak modules for the fixed point subalgebra of the heisenberg vertex operator algebra of rank 1 by an automorphism of order 2 and whittaker vectors*, Proc. Amer. Math. Soc. **145** (2017), 4127–4140.

[21] 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 (Part 1)*, J. Algebra **575** (2021), 31–66.

[22] 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 (Part 2)*, to appear in J. Math. Soc. Japan.

[23] K. Tanabe, *A Schur-Weyl type duality for twisted weak modules over a vertex algebra*, https://doi.org/10.48550/arXiv.2303.15692, 2023.

Explicit constructions of regular expander graphs of general degree and their applications

佐竹 翔平 (熊本大学) *

1 序

本稿では多重辺やループも許したグラフを扱う. 端的には, **エクスパンダーグラフ**とは連結性の高いスパースなグラフを意味する. その連結性の高さから断線などに対するロバスト性をもつ通信ネットワークとして, 通信理論と関連する離散数学の文脈で理論的な研究がなされてきた一方で ([2] など), スパース性の面からも低密度パリティ検査符号 (LDPC 符号) の構成などの研究 ([20] など) でも重要性が認識されている. さらに近年では, 耐量子計算機暗号の理論における同種写像暗号などの研究においても, 超特異楕円曲線グラフのエクスパンダー性に基づく暗号学的ハッシュ関数などが構成されており ([8] など), エクスパンダーグラフの注目度は年々高まっている. 一方で数学においても, 篩法の設計などの整数論の研究 ([7] など), グラフ上のランダムウォークの混合性 ([24] など) やカットオフ現象 ([16] など) といった確率論の研究などでもエクスパンダーグラフは枢要な位置を占める研究対象となっている.

エクスパンダーグラフの文脈では, n 頂点をもつグラフ G の連結性は以下で定義される **Cheeger 定数** $h(G)$ によって評価される. 以下, G の頂点集合と辺集合をそれぞれ $V(G)$, $E(G)$ と表す.

$$h(G) := \min_{\substack{S \subset V(G) \\ 1 \le |S| \le n/2}} \frac{|\partial(S)|}{|S|}$$

ただし $\partial(S)$ は, 1 点が S に属し, もう 1 点が S の外側に属するような G の辺全体の集合を表す. グラフ G が連結であることと $h(G)$ が正であることは同値であり, $h(G)$ が大きければ大きいほど G の連結性は高いことを意味する. 特に d-正則グラフ (各頂点がちょうど d 本の辺と接続するグラフ[1]) において, Cheeger 定数は, グラフの隣接行列 $A(G)$ の 2 番目に大きな固有値 $\lambda_2(G)$ と結びつくことが以下の **Cheeger 不等式**から知られている.

$$h(G) \ge \frac{d - \lambda_2(G)}{2}.$$

したがって, $\lambda_2(G)$ が小さければ小さいほど Cheeger 定数は大きいことになり, 連結性が高いことが分かる. 一方で, グラフのスパース性は, 単一のグラフに対してより, むしろ頂点数が増大するようなグラフの無限系列に対して意味をもつ. 特に固定された整数 d に対して d-正則グラフの無限系列を考えると, 辺の数が頂点数の線形オーダーで上からおさえることができるという意味で, スパース性を見ることができる[2]. そのような無限系列においては, 属する任意のグラフに対して Cheeger 定数が (頂点数に依存しない) 正の定数で下からおさえられるか否かは数学的に非自明な問題となる. 以下では, おもに正則グラフの無限系列に焦点を絞って話を進める.

さて, Cheeger 不等式を見ると, $\lambda_2(G)$ に対する下界が数学的な問題として浮上する. 実際には, **Alon-Boppana 不等式**とよばれる以下が下界が示されている.

*〒 860-8555 熊本県熊本市中央区黒髪 2-39-1 熊本大学 半導体・デジタル研究教育機構 総合情報学部門
E-mail: shohei-satake@kumamoto-u.ac.jp

[1]本質的ではないが, 1 つのループは接続する頂点の次数に 1 だけ貢献すると定める.

[2]仮に辺の数が頂点数の線形オーダーを下回る場合は無限系列に属するグラフは一般に連結ではないため, エクスパンダーグラフの文脈では意味をなさない.

定理 1 (Alon-Boppana 不等式, [1] など)**.** 任意の固定された整数 $d \geq 3$ と d-正則グラフの無限列 $\{G_i\}_{i\geq 1}$ (ただし, $n_i := |V(G_i)| \to \infty$ $(i \to \infty)$) に対して,

$$\lambda_2(G_i) \geq 2\sqrt{d-1} - O\Big(\frac{1}{\log_d n_i}\Big).$$

さらに Alon-Boppana 不等式を達成する d-正則グラフの無限系列も特定の d に対して明示的に構成されている. このようなグラフは **Ramanujan グラフ**とよばれ, Cheeger 不等式の意味で最適な連結性も保証される.

定義 1 ((one-sided) Ramanujan グラフ)**.** d-正則グラフ G に対して, $\lambda_2(G) \leq 2\sqrt{d-1}$ が成り立つとき, G を (one-sided) Ramanujan グラフとよぶ.

一方で, 混合補題などに代表される擬ランダムグラフの文脈やグラフ上のランダムウォークの混合時間の評価[3]では, d-正則グラフ G に対して, $\lambda_2(G)$ よりはむしろ (絶対値の中で)2 番目に大きな固有値を表す以下の $\lambda(G)$ に着目する.

$$\lambda(G) := \max\{|\lambda| \mid \lambda : |\lambda| \neq d \text{ なる } A(G) \text{ の固有値 }\}.$$

この $\lambda(G)$ に対しても Ramanujan グラフを定義することができる.

定義 2 ((two-sided) Ramanujan グラフ)**.** d-正則グラフ G に対して, $\lambda(G) \leq 2\sqrt{d-1}$ が成り立つとき, G を (two-sided) Ramanujan グラフとよぶ.

もちろん two-sided Ramanujan グラフは one-sided Ramanujan グラフでもあり, Cheeger 不等式から得られる Cheeger 定数の評価に関しては両者とも同じ下界を与える. そこで以下では, Ramanujan グラフは two-sided Ramanujan グラフを指すとする.

一般に, d-正則グラフの無限列で Cheeger 定数が (頂点数に依らない) 正定数となるもの, 特に明示的な Ramanujan グラフの無限列の構成は重要な研究課題である. ここで, ある性質を満たすグラフが**明示的** (explicit) であるとは, その頂点数 n の多項式時間で性質を満たすグラフを構成する確定的アルゴリズムが存在することを意味し, **強明示的** (strongly-explicit または fully-explicit) であるとは, 加えて, 与えられた頂点に対して隣接する頂点たちを $\log n$ の多項式オーダーの時間で計算できる確定的アルゴリズムも存在することを意味する[4].

実際に, そのような (強) 明示的なエクスパンダーグラフは上記の通信ネットワーク, 符号, 暗号学的ハッシュ関数などの設計において必要不可欠であり, 数学における各関連研究においても群の直径評価に関する Babai の予想 ([3]) や, ランダムウォークの混合時間の精密な評価 ([24] など) といった幅広い文脈で重要である. さらに, グラフ理論においては, 直径, 彩色数, 完全マッチングの存在性などのグラフの不変量の評価式や構造定理の改善や最適性を示すうえでも (強) 明示的なエクスパンダーグラフは重要な役割を果たしてきた ([15] など). しかし, 次節で述べるように (強) 明示的な Ramanujan グラフの無限列は素数べきに 1 を加えた形の次数に対してしか与えられておらず, 現在も当該分野の重要な研究課題となっている. 一方で, (強) 明示的な Ramanujan グラフの無限列が与えられていない次数 (無限に存在する!) に対しては, できるだけ $\lambda(G)$ が $2\sqrt{d-1}$ に「近い」値でおさえられるような d-正則グラフ G (**near-Ramanujan グラフ**) の構成を目指す研究が多くなされてきた. その定義も論文によって異なるが[5], 本稿では以下の定義を採用する.

定義 3 (ε-near-Ramanujan グラフ)**.** 実数 $\varepsilon > 0$ と d-正則グラフ G に対して, $\lambda(G) \leq 2\sqrt{d-1} + \varepsilon$ が成り立つとき, G を ε-near-Ramanujan グラフとよぶ.

本稿では, まず Ramanujan グラフおよび near-Ramanujan グラフの (強) 明示的構成に関する先行研究を概説したのち, 本稿における貢献として, 先行研究における一般的な次数に対する near-Ramanujan グラフの構成法の改良結果を与え, 関連する予想を提示する.

[3]混合時間の評価では, グラフ G が非 2 部的であることを想定する. このとき $-d$ は $A(G)$ の固有値にはなりえないため, $\lambda(G) = \max\{|\lambda| \mid \lambda : \lambda \neq d \text{ なる } A(G) \text{ の固有値 }\}$ となる.

[4]隣接する頂点たちを「効率的に」計算したい場合 (例えば暗号学的ハッシュ関数などで巨大なグラフの上のランダムウォークを扱う場合など) で重要である.

[5]文脈によっては, $\lambda(G) \leq (2+\varepsilon)\sqrt{d-1}$ が成り立つとき, G を ε-near-Ramanujan グラフとよぶときもある.

2 (強) 明示的な (near-)Ramanujan グラフに関する先行研究

標題の先行研究を説明するにあたり, まず Cayley グラフを定義する.

定義 4. 単位元 1 をもつ群 Γ と逆元に関して閉じた空でない部分集合 $S \subset \Gamma \setminus \{1\}$ に対して, **Cayley グラフ** $Cay(\Gamma, S)$ を, 頂点集合に Γ を, 辺集合に $\{\{g, h\} \mid g, h \in \Gamma, gh^{-1} \in S\}$ をもつグラフと定める.

Ramanujan グラフの最初の明示的構成は, 有限素体 $\mathbb{F}_r$ 上の射影特殊線形群 $\mathrm{PSL}_2(\mathbb{F}_r)$ 上の Cayley グラフとして, Lubotzky, Phillips および Sarnak による論文 [17] で与えられた.

定理 2 ([17])**.** 相異なる 2 つの素数 $p \equiv 1 \pmod 4$, $r \equiv 1 \pmod 4$, および整数 i で $i^2 = -1 \pmod r$ を満たすものに対して,

$$S_{p,r} := \left\{ \begin{pmatrix} x_0 + x_1 i & x_2 + x_3 i \\ -x_2 + x_3 i & x_0 - x_1 i \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_r) \mid x_0^2 + x_1^2 + x_2^2 + x_3^2 = p,\ x_0 > 0 \text{ は奇数, その他は偶数} \right\}$$

とおく. このとき, $r > p^8$ であるならば $X^{p,r} := Cay(\mathrm{PSL}_2(\mathbb{F}_r), S_{p,r})$ は $(p+1)$-正則 *Ramanujan* グラフである. 特に素数 p に対して, $(p+1)$-正則グラフの無限列を $\{X^{p,r} \mid r \equiv 1 \pmod 4 \text{ は } r > p^8 \text{ なる素数}\}$ と定めることで $(p+1)$-正則 *Ramanujan* グラフの無限列を得る.

注 1. 素数 $p = 2$ および $p \equiv 3 \pmod 4$ に対しても, $(p+1)$-正則 Ramanujan グラフである $\mathrm{PSL}_2(\mathbb{F}_r)$ (ただし r は所定の条件を満たす奇素数) 上の Cayley グラフを構成することができる ([9, 13, 14, 17]).

注 2. 素数 p に対して, 超特異楕円曲線を用いることでも $(p+1)$-正則 Ramanujan グラフが構成されている ([23]).

一方で, Morgenstern [21] による以下の結果も知られている.

定理 3 ([21])**.** 奇素数のべき q に対して, 平方元でない非ゼロな元 $\eta \in \mathbb{F}_q$ を固定する. $d \geq 2$ を偶数とし, 次数 d の既約多項式 $g \in \mathbb{F}_q[X]$ によって, 有限体 $\mathbb{F}_{q^d}$ を剰余体 $\mathbb{F}_q[X]/(g(X))$ として表現する. さらに, X は $g(X)$ を法としたとき平方元であると仮定する. $L \in \mathbb{F}_q^d$ は $L^2 = \eta$ なる元とおく. このとき,

$$T_{q,d} := \left\{ \begin{pmatrix} 1 & \gamma_j - \delta_j L \\ (\gamma_j + \delta_j L)(X-1) & 1 \end{pmatrix} \in \mathrm{PSL}_2(\mathbb{F}_{q^d}) \mid \delta_j^2 \eta - \gamma_j^2 = 1,\ j = 1, 2, \ldots, q+1 \right\}$$

とおくと, *Cayley* グラフ $M^{q,d} := Cay(\mathrm{PSL}_2(\mathbb{F}_{q^d}), T_{q,d})$ は $(q+1)$-正則 *Ramanujan* グラフである. 特に奇素数のべき q に対して, $(q+1)$-正則グラフの無限列を $\{M^{q,d} \mid d \geq 2 \text{ は偶数}\}$ と定めることで $(q+1)$-正則 *Ramanujan* グラフの無限列を得る.

注 3. 上述の Ramanujan グラフはすべて強明示的であることが知られている.

強明示的な Ramanujan グラフの無限列の構成として知られているのは, 著者の知る限り, 上記の定理 2, 3および関連する注で参照した論文の結果のみである. 特に, 明示的な Ramanujan グラフの無限列は素数べき $+1$ の形の次数に対してしか与えられていない現状がある. 任意の次数に対して Ramanujan グラフが存在することは示されており ([18, 19]), すべての次数に対して明示的な Ramanujan グラフが構成できるかどうかがエクスパンダーグラフの理論では大きな未解決問題となっている. 例えば 7-正則 Ramanujan グラフの (強) 明示的な無限列も現在のところ全く知られていない!

このような状況に鑑み, (強) 明示的な Ramanujan グラフの無限列が知られていないような次数 (すなわち素数べき $+1$ のような形以外の次数) d に対して, near-Ramanujan グラフの明示的構成を行い, 少しでも上界式 $2\sqrt{d-1}$ とのエラーを削減する方向の研究も活発に行われている.

以下では, 本稿の内容に関わる 2 つの先行研究とその証明のアイデアを述べていくが, その前に 2 つの有用な補題を準備しておく.

補題 1. 同じ頂点集合をもつ 2 つの連結な n 頂点 d-正則グラフ G_1, G_2 に対し, G_1, G_2 の辺集合の和をとって得られるグラフを $G_1 \cup G_2$ と記す. このとき,

$$\lambda(G_1 \cup G_2) \leq \lambda(G_1) + \lambda(G_2)$$

が成り立つ.

証明. まず各 $i = 1, 2$ に対して,

$$\lambda(G_i) = \max_{\substack{\mathbf{v}\in\mathbb{R}^n \\ \mathbf{v}\perp\mathbf{1}}} \left| \frac{\mathbf{v}^T A(G_i)\mathbf{v}}{||\mathbf{v}||^2} \right|$$

が成り立つ. G_1, G_2 の辺集合の和をとって得られるグラフ $G_1 \cup G_2$ の隣接行列は $A(G_1) + A(G_2)$ であるから,

$$\begin{aligned}\lambda(G_1 \cup G_2) &= \max_{\substack{\mathbf{v}\in\mathbb{R}^n \\ \mathbf{v}\perp\mathbf{1}}} \left| \frac{\mathbf{v}^T (A(G_1) + A(G_2))\mathbf{v}}{||\mathbf{v}||^2} \right| \\ &\leq \max_{\substack{\mathbf{u}\in\mathbb{R}^n \\ \mathbf{u}\perp\mathbf{1}}} \left| \frac{\mathbf{u}^T A(G_1)\mathbf{u}}{||\mathbf{u}||^2} \right| + \max_{\substack{\mathbf{v}\in\mathbb{R}^n \\ \mathbf{v}\perp\mathbf{1}}} \left| \frac{\mathbf{v}^T A(G_2)\mathbf{v}}{||\mathbf{v}||^2} \right| = \lambda(G_1) + \lambda(G_2)\end{aligned}$$

が成り立つ. □

さらに, 補題 1の証明と全く同じ議論で, 以下の補題を得る.

補題 2. n 頂点 d-正則グラフ G_1 と d'-正則 $(d' < d)$ な G_1 の全域部分グラフ G_2 に対して, $G_1 \setminus G_2$ を辺集合 $E(G_1) \setminus E(G_2)$ をもつグラフとする. このとき,

$$\lambda(G_1 \setminus G_2) \leq \lambda(G_1) + \lambda(G_2)$$

が成り立つ.

定理 4 ([10], [22])**.** $d-1$ が素数ではない整数 $d \geq 3$ に対して, p を $d-1$ を超える最小の素数とおく. このとき, 無限個の自然数 n に対して, $\lambda(G) \leq 2\sqrt{p} + (p + 1 - d)$ となる明示的な n 頂点グラフ G が存在する. 特に, 素数の間隔に関する *[5]* の結果より, 任意の $d \geq 3$ に対して, $O(d^{0.525})$-*near-Ramanujan* グラフの明示的な無限列が存在する. さらに, 素数の間隔に関する *Cramér* の予想を仮定すると, 任意の d に対して, $O((\log d)^2)$-*near-Ramanujan* グラフの明示的な無限列が存在する.

定理 4における構成のアイデアは, 定理 2の Ramanujan グラフ $X^{p,r}$ に対し, $X^{p,r}$ 内の完全マッチング (1-正則な全域部分グラフ) を $(p+1-d)$ 個除去して d-正則グラフを得るというものである. また $\lambda(G)$ の評価は実対称行列に関する Weyl の不等式 ([12] を参照) から従う. ここで, p' を p 未満の最大の素数とおくと $p + 1 - d \leq (p + 1) - (p' + 1)$ より, $\lambda(G)$ は素数の間隔の上界式から評価できることから, 定理 4の最後の主張を得る.

注 4. 完全マッチング自体は r の多項式時間で見つけることができるため上記で構成されたグラフは明示的である (ただし強明示的とは必ずしも言えない). 一方で, $X^{p,r}$ の内周 (最短閉路長) は少なくとも $2\log_p(r)$ であることが知られ, 最適なオーダーの内周をもつ. したがって, 定理 4のグラフも少なくとも同じ値の内周をもつことになる. 高い内周をもつ near-Ramanujan グラフは暗号学的ハッシュ関数や LDPC 符号の設計への重要な応用がある. 一方で, そのようなグラフは高い内周と彩色数をもつグラフの明示的構成に関する Erdős の問題 ([11], [17]) への解となる点などでも興味深い. 実際に混合補題の系として, 任意の n 頂点 d-正則グラフ G に対して, G の彩色数 $\chi(G)$ に対して,

$$\chi(G) \geq 1 + \frac{d}{\lambda(G)}$$

が成り立つ (詳細は [15] などを参照). よって, 正整数 d と $\varepsilon = O(\sqrt{d})$ に対して d-正則 ε-near-Ramanujan グラフの彩色数は少なくとも $\sqrt{d}$ のオーダーをもつことがわかる.

一方で, Alon [4] は $d-1$ が素数ではない整数 $d \geq 3$ に対して, 以下の方法で強明示的な near-Ramanujan グラフの構成を与えた.

1. $d-1$ を超えない最大の素数 $p_0 \equiv 1 \pmod 4$ を取り, $d_1 := d - (p_0 + 1)$ とおく.

2. $d_1 > 5$ ならば, $p_1 \equiv 1 \pmod 4$ を $d_1 - 1$ を超えない最大の素数とし, $d_2 := d_1 - (p_1 + 1)$ とおく. 以下, $i \geq 2$ に対して, $d_i > 5$ であるならば同様にして素数 $p_i \equiv 1 \pmod 4$ および整数 d_{i+1} を定める.

3. $i = k$ で $d_{i+1} \leq 5$ となったとき, $f := d - \{(p_0 + 1) + (p_1 + 1) + \cdots + (p_k + 1)\} \leq 5$ となる. このとき, 以下のようにして d-正則グラフ G を構成する.

   ・$f = 0$ ならば, 定理 2から $S := S_{p_0,r} \cup S_{p_1,r} \cup \cdots \cup S_{p_k,r}$ とおき, G を $Cay(\mathrm{PSL}_2(\mathbb{F}_r), S)$ とおく.

   ・$f = 1$ ならば, S に位数 2 の元を 1 つ加えて得られる Cayley グラフを G とおく.

   ・$2 \leq f \leq 5$ ならば, f 個の元からなる逆元について閉じた集合を S に 1 つ加えて得られる Cayley グラフを G とおく.

以上の構成法と補題 1より次の定理が得られる.

定理 5 ([4])**.** $d - 1$ が素数ではない整数 $d \geq 3$ に対して, 上記で得られた d-正則グラフ G は強明示的な *ε-near-Ramanujan* グラフである. ただし,

$$(2(\sqrt{p_0} + \sqrt{p_1} + \cdots \sqrt{p_k}) + 2\sqrt{f-1} - 2\sqrt{d-1}) \leq \varepsilon \leq (2(\sqrt{p_0} + \sqrt{p_1} + \cdots \sqrt{p_k}) + f - 2\sqrt{d-1}).$$

特に, 素数の間隔に関する *[5]* の結果より, 任意の $d \geq 3$ に対して, G は強明示的な $O(d^{0.2625})$-*near-Ramanujan* グラフである.

注 5. 同論文で Alon は任意の $\varepsilon > 0$ に対して, 明示的な ε-near-Ramanujan グラフを構成している ([4, Theorem 1.3]). しかし, 強明示的とは言えないことに注意されたい.

3 定理 4, 定理 5の改良

まず定理 4に関して改良を与える以下の結果を得る.

命題 1. $d, d+1$ のいずれもが素数ではない整数 $d \geq 3$ に対して, p を $d-1$ を超える最小の素数とおく. このとき, ある $0 < \delta = \delta(d) < 1$ が存在し, 無限個の素数 r に対して, $\lambda(G) \leq 2\sqrt{p} + \delta(p + 1 - d)$ となる強明示的な $\frac{r(r^2-1)}{2}$ 頂点グラフ G が存在する. さらに, G の内周は少なくとも $2\log_p(r)$ である.

証明の概略. $d, d+1$ のいずれもが素数ではない[6] 整数 $d \geq 3$ に対して, Ramanujan グラフ $X^{p,r}$ を定める $\mathrm{PSL}_2(\mathbb{F}_r)$ の $(p+1)$-点部分集合 $S_{p,r}$ から, 逆元について閉じた $(p+1-d)$-点集合 $U \subset S_{p,r}$ をえらぶ. このとき $p + 1 - d \geq 3$ であることから, Bourgain-Gamburd [6] の結果より, ある $0 < \delta = \delta(d) < 1$ が存在して, $\lambda(Cay(\mathrm{PSL}_2(\mathbb{F}_r), U)) \leq \delta(p - d)$ が成り立つ. よって, 補題 2より $Cay(\mathrm{PSL}_2(\mathbb{F}_r), S_{p,r} \setminus U)$ が所望のグラフとなる. □

注 6. 命題 1に登場する定数 δ に関しては, 現在のところ明示的な値を決定できない.

次に定理 5の拡張として, 以下の命題を示す.

命題 2. 整数 $k \geq 2$ と奇素数 p に対して $q = p^k$ とおき, $d = q + p + 2$ とおく. このとき, 無限個の整数 $n \geq 1$ に対して, 強明示的な d-正則 $(2(\sqrt{q} + \sqrt{p}) - 2\sqrt{q + p + 1})$-*near-Ramanujan* グラフが存在する.

証明の概略. Alon [4] の構成法のアイデアを定理 3の Ramanujan グラフに拡張する. $d = (p^k + 1) + (p+1)$ であることに注意すると, 定理 3から, 各偶数 $d \geq 2$ に対して, $T := T_{p^k,d} \cup T_{p,kd}$ とおくと, 補題 1より $Cay(\mathrm{PSL}_2(\mathbb{F}_{p^{kd}}), T)$ が所望のグラフである. □

注 7. より一般的な d に対しても, T の定義を微修正することで d-正則 near-Ramanujan グラフを得ることができるが, 簡単のために命題 2の次数の場合のみを考える.

[6] $d = p, p-1$ ($p \geq 3$ は素数) であるとき, 命題 1の構成では $\lambda(G) \leq 2\sqrt{p} + (p + 1 - d)$ としか評価できないため, 定理 4の結果と一致する.

ここで興味深いことに, 定理 5のグラフと比較すると, いくつかの d に対して, 命題 2のグラフの方が $2\sqrt{d-1}$ からのエラーをより小さく評価できる.

例 1. $d = 11^3 + 11 + 2 = 1344$ とおくと, $2\sqrt{d-1} = 73.2939$ より, 命題 2の 1344-正則グラフは 6.30507-near-Ramanujan グラフである. 一方で, 定理 5の d-正則グラフは, $p_0 = 1321$, $p_1 = 13$, $p_2 = 5$, $f = 2$ であることから, 13.0804-near-Ramanujan グラフとなる.

例 2. $d = 5^5 + 5 + 2 = 3132$ とおくと, $2\sqrt{d-1} = 111.911...$ であるから, 命題 2の 3132-正則グラフは 4.36486-near-Ramanujan グラフである. 一方で, 定理 5の d-正則グラフは, $p_0 = 3121$, $p_1 = 5$, $f = 4$ であることから, $\varepsilon \geq 7.75738$ に対する ε-near-Ramanujan グラフとなる.

例 3. $d = 23^3 + 23 + 2 = 12192$ のとき, $2\sqrt{d-1} = 220.826...$ であるから, 命題 2の 12192-正則グラフは 9.37419-near-Ramanujan グラフである. 一方で, 定理 5の d-正則グラフは, $p_0 = 12161$, $p_1 = 29$, $f = 0$ であることから, 10.4985-near-Ramanujan グラフとなる.

例 4. $d = 5^7 + 5 + 2 = 78132$ のとき, $2\sqrt{d-1} = 559.038...$ であるから, 命題 2の 78132-正則グラフは 4.45067-near-Ramanujan グラフである. 一方で, 定理 5の d-正則グラフは, $p_0 = 78121$, $p_1 = 5$, $f = 4$ であることから, $\varepsilon \geq 7.93982$ に対する ε-near-Ramanujan グラフとなる.

実際には, 命題 2の構成法は無限個の整数 $d \geq 3$ に対して, 定理 5の改良を与えるものと予想される.

予想 1. 整数 $d \geq 3$ および定理 5で構成された d-正則グラフ G に対して, $\varepsilon_d := (2(\sqrt{p_0} + \sqrt{p_1} + \cdots \sqrt{p_k}) + 2\sqrt{f-1} - 2\sqrt{d-1})$ とおく. このとき, 次を満たす整数 $d \geq 3$ であって, $d-1$ が素数べきでないものが無限個存在する : ある $0 < \varepsilon'_d < \varepsilon_d$ が存在し, 無限個の整数 $n \geq 1$ に対して, 強明示的な n 頂点 d-正則グラフで ε'_d-near-Ramanujan となるグラフが存在する.

4 本稿のまとめ

本稿では, 一般的な次数に対する明示的な (near-)Ramanujan グラフに焦点を当て, いくつかの既存結果の (マイナーではあるが) 改良を与えた. 一般に明示的な (near-)Ramanujan グラフの構成研究は様々な文脈で重要であるにもかかわらず, まだ満足すべき成果は得られておらず, 特定の near-Ramanujan グラフのエラーの評価さえもその改善はまったく容易ではない.

謝辞

今回の講演の機会をくださった代数的組合せ論シンポジウムの世話人の皆様に厚く御礼申し上げます. また, 本稿の内容に関して多くの有益なコメントをくださった山﨑 義徳 教授 (愛媛大学), 杉山 真吾 准教授 (金沢大学) に心より御礼申し上げます. 本研究は JSPS 科研費 JP23K13007 の助成, ならびに九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点（2022 年度若手・学生研究-短期共同研究「エクスパンダーグラフの新しい構成手法の確立とその応用」（2022a017））の支援を受けております.

References

[1] N. Alon, Eigenvalues and expanders, *Combinatorica* **6** (1986), 83–96.

[2] N. Alon, F. R. K. Chung, Explicit construction of linear sized tolerant networks, *Discrete Math.* **72** (1988), 15–19.

[3] L. Babai, A. Seress, On the diameter of permutation groups. *Eur. J. Combin.* **13** (1992), 231—243.

[4] N. Alon, Explicit expanders of every degree and size, *Combinatorica* **41** (2021), 447–463.

[5] R. C. Baker, G. Harman, J. Pintz, The difference between consecutive primes II, *Proc. London Math. Soc.* **83** (2001), 532–562.

[6] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, *Ann. Math. (2)* **167** (2008), 625–642.

[7] J. Bourgain, A. Gamburd, P. Sarnak, Affine linear sieve, expanders, and sum-product. *Invent. math.* **179** (2010), 559—644.

[8] D. X. Charles, K. E. Lauter, E. Z. Goren, Cryptographic hash functions from expander graphs, *J. Cryptol.* **22** (2009), 93–113.

[9] P. Chiu, Cubic Ramanujan graphs, *Combinatorica* **12** (1992), 275–285.

[10] S. M. Cioabă, M. R. Murty, Expander graphs and gaps between primes, *Forum Math.* **20** (2008), 745–756.

[11] P. Erdős, Graph theory and probability, *Canad. J. Math.* **11** (1959), 34–38.

[12] R. A. Horn, C. R. Johnson, Matrix Analysis, Cambridge University Press, 1990.

[13] H. Jo, Y. Yamasaki, LPS-type Ramanujan graphs, In: Proc. of 2018 International Symposium on Information Theory and Its Applications (ISITA), pp.399-403, 2018.

[14] H. Jo, S. Sugiyama, Y. Yamasaki, Ramanujan graphs for post-quantum cryptography, In: International Symposium on Mathematics, Quantum Theory, and Cryptography: Proceedings of MQC 2019, pp. 231-250, 2021.

[15] M. Krivelevich, B. Sudakov, Pseudo-random graphs, In: More Sets, Graphs and Numbers, Springer, pp. 199–262, 2006.

[16] E. Lubetzky, A. Sly, Explicit expanders with cutoff phenomena *Electron. J. Probab.* **16** (2011), 419–435.

[17] A. Lubotzky, R. L. Phillips, P. Sarnak, Ramanujan graphs, *Combinatorica* **8** (1988), 261–277.

[18] A. Marcus, D. A. Spielman, N. Srivastava, Interlacing families I: Bipartite Ramanujan graphs of all degrees, In: Foundations of Computer Science (FOCS) 2013 IEEE 54th Annual Symposium, pp. 529-537, 2013.

[19] A. W. Marcus, D. A. Spielman, N. Srivastava, Interlacing families IV: Bipartite Ramanujan graphs of all sizes, In: Foundations of Computer Science (FOCS) 2015 IEEE 56th Annual Symposium, pp. 1358-1377, 2015.

[20] G. A. Margulis, Explicit constructions of graphs without short cycles and low density codes, *Combinatorica* **2** (1988), 71–78,

[21] M. Morgenstern, Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q, *J. Comb. Theory. Ser. B* **62** (1994), 44–62.

[22] A. Musitelli, P. de la Harpe, Expanding graphs, Ramanujan graphs and 1-factor perturbations, *Bull. Belg. Math. Soc. Simon Stevin* **13** (2006), 673–680.

[23] A. K. Pizer, Ramanujan graphs and Hecke operators, *Bull. Amer. Math. Soc. (N.S.)* **23**, 127–137.

[24] A. Terras, Fourier Analysis on Finite Groups and Applications, Cambridge University Press, 1999.

拡大平方剰余符号から得られる 3-デザインについて

三枝崎剛 *

1 はじめに

拡大平方剰余符号から 3-デザインを構成する手法を解説する．詳細は [1] を参照されたい．t-デザインの定義を復習しよう．

定義 1.1. $X = \{1, 2, \ldots, n\}$ を有限集合，$\mathscr{B}$ を X の k 点部分集合族とする：

$$\mathscr{B} \subset \binom{X}{k}.$$

$(X, \mathscr{B})$ が t-デザイン（t-n, k, λ）とは，ある自然数 λ が存在して次を満たすときである：全ての $T \in \binom{X}{t}$ に対して $\lambda = |\{B \in \mathscr{B} \mid T \subseteq B\}|$.

一つ例を見てみよう．

例 1.1. 次のように集合族を定める．

$$\begin{cases} X = \{1, 2, 3, 4, 5, 6, 7\}, \\ \mathscr{B} = \{\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{5, 6, 1\}, \{6, 7, 2\}, \{7, 1, 3\}\}. \end{cases}$$

$\mathscr{B}$ は $\mathbb{F}_7$ の平方剰余 $\{1, 2, 4\}$ から $+1$ して構成したものである。するとこれは 2-デザインの構造を与える。つまり任意の 2 点集合 T に対して，それを含む $\mathscr{B}$ の元はただ一つに定まる．

$$\text{任意の } T \in \binom{X}{2} \text{に対して}, |\{B \in \mathscr{B} \mid T \subseteq B\}| = 1.$$

したがって $(X, \mathscr{B})$ は 2-$(7, 3, 1)$ デザインである．

t-デザインならば $(t-1)$-デザインであることに注意する．したがって t の値の大きいデザインの構成が基本問題となる．ではどのように構成するか．本稿では符号を用いる手法を紹介する．

*早稲田大学基幹理工学部

定義 1.2. $\mathbb{F}_2^n$ の k-次元部分空間を符号，特に $[n,k]$ 符号と呼ぶ．

C の元 $c=(c_1,c_2,\dots,c_n)\in C$ に対して，記号を用意しておこう．

- $\mathrm{supp}(c):=\{i\mid c_i\neq 0\}$,
- $\mathrm{wt}(c):=|\mathrm{supp}(c)|$,
- $C_\ell:=\{c\in C\mid \mathrm{wt}(c)=\ell\}$.

符号 C から集合族を以下のように構成することができる．

$$\begin{cases} X=\{1,2,\dots,n\},\\ \mathscr{B}(C_\ell)=\{\mathrm{supp}(c)\mid c\in C_\ell\}\subset\binom{X}{\ell}. \end{cases}$$

したがって $(X,\mathscr{B}(C_\ell))$ が t-デザインかどうか，という問題を考えることができる．符号からデザインを構成する手法とは，うまく C を選んで，高い t の t-デザインを構成しようというものである．一つ例を見てみよう．

例 1.2. H を以下の生成行列を持つ $[7,4]$ ハミング符号としよう．

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

H の $\mathrm{wt}(c)=3$ となる元 c を列挙すると以下のようになる．

$H_3=\{c\in C\mid \mathrm{wt}(c)=3\}$：

$(1,1,0,1,0,0,0)$
$(0,1,1,0,1,0,0)$
$(0,0,1,1,0,1,0)$
$(0,0,0,1,1,0,1)$
$(1,0,0,0,1,1,0)$
$(0,1,0,0,0,1,1)$
$(1,0,1,0,0,0,1)$

H_3 を用いて集合族を構成すると以下を得る：

$$\begin{cases} X=\{1,2,3,4,5,6,7\},\\ \mathscr{B}(H_3)=\{\{1,2,4\},\{2,3,5\},\{3,4,6\},\{4,5,7\},\{5,6,1\},\{6,7,2\},\{7,1,3\}\}, \end{cases}$$

これは最初に紹介した 2-デザインに他ならない．

$(\widetilde{Q}_{p+1})$ を拡大平方剰余符号とする．このとき全ての ℓ に対して，$(\widetilde{Q}_{p+1})_\ell$ は 2-デザインであることが知られている．(もちろん $(\widetilde{Q}_{p+1})_\ell\neq\emptyset$ の場合は除外している．今後このようなことは断らない.）しかし一般に 3-デザインは得られない．

次が本稿の主結果である．

定理 1.1. 全ての ℓ に対して $(\widetilde{Q}_{p+1})_\ell \cup (\widetilde{Q}_{p+1}^{\perp})_\ell$ $(\neq \emptyset)$ は 3-デザインである．

以下ではこの定理に関して，

1. ヤコビ多項式，
2. 調和重さ多項式

を用いた 2 通りの証明を紹介したい．

注意 1.1. $(\widetilde{Q}_{p+1})_\ell$ は一般に 3-デザインにはならないと述べた．しかし特別な ℓ に対して，$(\widetilde{Q}_{p+1})_\ell$ が 3-デザインになる例が複数発見されている．

- [Bonnecaze–Sóle (2021), [3]]
  $(\widetilde{Q}_{42})_{10}$ は 3-デザイン．
- [Ishikawa, arXiv:2305.03285, [5]]
  $(\widetilde{Q^3}_{14})_{10}$ は 3-デザイン．
  $(\widetilde{Q^4}_{18})_{10}$ と $(\widetilde{Q^4}_{18})_{13}$ は 3-デザイン．

2　拡大平方剰余符号

拡大平方剰余符号の構成法を復習しよう．p を素数とする．p に対して，$\mathbb{F}_2$ 上のベクトル

$$c_p = (d_1, d_2, \ldots, d_p),$$

を以下のように定める：

$$d_i = \begin{cases} 1 \ (i \in (\mathbb{F}_p^*)^2), \\ 0 \ (\text{o.w.}). \end{cases}$$

長さ p の平方剰余符号 Q_p とは，c_p で生成される巡回符号である．つまり c_p の成分を右に一つずつずらしてベクトルを作り，それらで生成された符号である．

例 2.1. $p = 7$ としよう．すると $(\mathbb{F}_7^*)^2 = \{1, 2, 4\}$ であり，

$$c_7 = (1, 1, 0, 1, 0, 0, 0)$$

と定まる．したがって Q_7 は次を生成行列に持つ符号である．

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

$\widetilde{Q}_{p+1}$ で Q_p の拡大符号を表す．つまり

$$\widetilde{Q}_{p+1} = \{(c_1, \ldots, c_p, c_{p+1}) \mid (c_1, \ldots, c_p) \in Q_p, c_1 + \cdots + c_p + c_{p+1} = 0\}$$

である．$\widetilde{Q}_{p+1}$ を拡大平方剰余符号と呼ぼう．たとえば $\widetilde{Q}_8$ は以下の行列で生成された符号となる．

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

以下では

$$p \equiv 1 \pmod 8$$

を仮定する．$\widetilde{Q}_{p+1}$ の座標を $\{1, \ldots, p-1, p, \infty\}$ と表記しよう．∞ は拡大した座標である．

拡大平方剰余符号について以下のことが知られている．

- $\mathrm{Aut}(\widetilde{Q}_{p+1}) = PSL_2(p)$, ここで $\mathrm{Aut}(C) = \{\sigma \in S_n \mid C^\sigma = C\}$, $C^\sigma = \{(c_{\sigma(1)}, \ldots, c_{\sigma(n)}) \mid (c_1, \ldots, c_n) \in C\}$.

- $$PSL_2(p) := \langle \sigma, \tau_a, \rho \mid a \in (\mathbb{F}_p^*)^2 \rangle,$$
  ここで $\begin{cases} \sigma : i \mapsto i+1 \pmod p, \infty \mapsto \infty, \\ \tau_a : i \mapsto ai \pmod p, \infty \mapsto \infty, \\ \rho : i \mapsto -1/i \pmod p, i \neq 0, 0 \mapsto \infty, \infty \mapsto 0. \end{cases}$

- $\widetilde{Q}_{p+1}$ の座標は $X = \{1, \ldots, p-1, p, \infty\}$ であった．このとき $PSL_2(p)$ は 2-homogeneous (すなわち，任意の $A, B \in \binom{X}{2}$ に対して，ある $\sigma \in PSL_2(p)$ が存在して $\sigma(A) = B$).
  したがって任意の ℓ に対して $(\widetilde{Q}_{p+1})_\ell$ $(\neq \emptyset)$ は 2-デザインである．

- 一般に $(\widetilde{Q}_{p+1})_\ell$ は 3-デザインでない．実際 $G = \mathrm{Aut}(\widetilde{Q}_{p+1})$ は 3-homogeneous でなく，$\binom{X}{3}$ は次のように 2 つの軌道に分解する：ある $\theta \in X$ が存在して，
  $$\binom{X}{3} = G\{\infty, 0, -1\} \sqcup G\{\infty, 0, \theta\},$$
  さらに $|G\{\infty, 0, -1\}| = |G\{\infty, 0, \theta\}|$.

- $\widetilde{Q}_{p+1}$ は isodual 符号である．つまりある $\sigma \in S_{p+1} \setminus G$ が存在して $C^\perp = C^\sigma$．このとき $\sigma(G\{\infty, 0, -1\}) = G\{\infty, 0, \theta\}$ である．

3　ヤコビ多項式とデザイン理論

ヤコビ多項式を用いると C から t-デザインが得られるかどうか判定できる．

定義 3.1 (Ozeki (1997), [6])**.** C を $[n,k]$ 符号とし，$T \subset \{1,\dots,n\} = [n]$ とする．次をヤコビ多項式と呼ぶ．

$$J_{C,T}(x_0,x_1,y_0,y_1) := \sum_{c\in C} x_0^{m_0(c)} x_1^{m_1(c)} y_0^{n_0(c)} y_1^{n_1(c)},$$

ここで

$$\begin{aligned} m_0(c) &:= |\{i \in T \mid c_i = 0\}|, \\ m_1(c) &:= |\{i \in T \mid c_i = 1\}|, \\ n_0(c) &:= |\{i \in [n]\setminus T \mid c_i = 0\}|, \\ n_1(c) &:= |\{i \in [n]\setminus T \mid c_i = 1\}|. \end{aligned}$$

例 3.1. C を次の $[4,2]$ 符号とする．

$$C = \{(0,0,0,0),(0,1,0,1),(1,0,1,0),(1,1,1,1)\}.$$

$T = \{1\}$ とおく．そのときヤコビ多項式は次のようになる．

$$J_{C,T}(x_0,x_1,y_0,y_1) = x_0^1x_1^0y_0^3y_1^0 + x_0^1x_1^0y_0^1y_1^2 + x_0^0x_1^1y_0^2y_1^1 + x_0^0x_1^1y_0^0y_1^3.$$

$J_{C,T}$ の項 $x_1^t y_0^{n-\ell} y_1^{\ell-t}$ の係数は

$$|\{c \in C_\ell \mid T \subset \mathrm{supp}(c)\}|$$

を表すことに注意しよう．したがって次の定理を得る．

定理 3.1.
1. 任意の $T \subset \{1,\dots,n\}$ $(|T| = t)$ に対して，$J_{C,T}$ が $T \subset \{1,\dots,n\}$ $(|T| = t)$ の選び方によらないと仮定する．このとき任意の ℓ に対して，C_ℓ $(\neq \emptyset)$ は t-デザインである．
2. 任意の $T \subset \{1,\dots,n\}$ $(|T| = t)$ に対して，$J_{C,T} + J_{C^\perp,T}$ が $T \subset \{1,\dots,n\}$ $(|T| = t)$ の選び方によらないと仮定する．このとき任意の ℓ に対して，$C_\ell \cup (C^\perp)_\ell$ $(\neq \emptyset)$ は t-デザインである．

以上の準備の下，以下の主結果を証明しよう．

定理 3.2. 全ての ℓ に対して $(\widetilde{Q}_{p+1})_\ell \cup (\widetilde{Q}_{p+1}^\perp)_\ell$ $(\neq \emptyset)$ は 3-デザインである．

Proof. $C = \widetilde{Q}_{p+1}$，$G = \mathrm{Aut}(C) = PSL_2(p)$ とおく．$C^\perp = C^\sigma$ であり，以下のように軌道分解されたことを思い出す．

$$\binom{X}{3} = G\{\infty, 0, -1\} \sqcup G\{\infty, 0, \theta\} = GT_1 \sqcup GT_2,$$

$\sigma(GT_1) = GT_2$. 任意の $T \in \binom{X}{3}$ に対して，$J_{C,T}+J_{C^\perp,T}$ が $T \subset \{1, \ldots, n\}$ $(|T| = t)$ の選び方によらないことを示せばよい．実際，

$$\begin{aligned} J_{C,T} + J_{C^\perp,T} &= J_{C,T} + J_{C^\sigma,T} \ (\because C^\perp = C^\sigma) \\ &= J_{C,T} + J_{C,T^{\sigma^{-1}}} \\ &= J_{C,T_1} + J_{C,T_2}. \end{aligned}$$

□

4　調和重さ多項式とデザイン理論

調和重さ多項式も C から t-デザインが得られるかどうか判定する．以下の記号を導入する．

- $X = \{1, \ldots, n\}$
- $\mathbb{R}2^X = \{\sum_{z \in 2^X} c_z z \mid \forall z, c_z \in \mathbb{R}\}$
- $\mathbb{R}\binom{X}{k} = \{\sum_{z \in \binom{X}{k}} c_z z \mid \forall z, c_z \in \mathbb{R}\}$

任意の $f \in \mathbb{R}\binom{X}{k}$ に対して，f を次のように表記しよう．

$$f = \sum_{z \in \binom{X}{k}} f(z) z$$

すると f を $\binom{X}{k}$ 上の関数と考えることができる．さらに，$u \in 2^X$ に対して，

$$\widetilde{f}(u) = \sum_{z \in \binom{X}{k}, z \subset u} f(z)$$

と定義して，f を 2^X 上の関数 $\widetilde{f} \in \mathbb{R}2^X$ に拡張できる：
　例を見てみよう．

例 4.1. $X = \{1, 2, 3\}$, $f = \{1, 2\}+\{2, 3\} \in \mathbb{R}\binom{X}{2}$ とおく．このとき $\widetilde{f}(\{1, 2\}) = 1, \widetilde{f}(\{1\}) = 0, \widetilde{f}(\{1, 2, 3\}) = 2$ である．

定義 4.1.
- $\gamma : \mathbb{R}\binom{X}{k} \to \mathbb{R}\binom{X}{k-1}$ を任意の $z \in \binom{X}{k}$ に対して $\gamma(z) = \sum_{y \in \binom{X}{k-1}, y \subset z} y$ と定義して，一般の $\mathbb{R}\binom{X}{k}$ の元に線形に拡張する．
- $\mathrm{Harm}_k = \ker(\gamma|_{\mathbb{R}\binom{X}{k}})$.
- $\mathrm{Harm}_k^{\mathrm{Aut}(C)} = \{f \in \mathrm{Harm}_k \mid f^\sigma = f, \forall \sigma \in \mathrm{Aut}(C)\}$, ここで f^σ は以下のように k 点集合に対して定義して，
$$\{i_1, \ldots, i_k\}^\sigma = \{\sigma(i_1), \ldots, \sigma(i_k)\}$$
それを Harm_k の元に線形に拡張する．
- C と $f \in \mathrm{Harm}_k$ の重さ調和多項式とは [Bachoc (1999), [2]] により以下のように定義された：
$$w_{C,f}(x,y) = \sum_{c \in C} \widetilde{f}(\mathrm{supp}(c)) x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)}.$$

再び例を見てみよう．

例 4.2. $X = \{1,2,3,4\}$, $f = \{1,2\} + \{1,3\} - 2\{1,4\} - 2\{2,3\} + \{2,4\} + \{3,4\}$ とおく．すると
$$\begin{aligned}\gamma(f) =& (\{1\} + \{2\}) + (\{1\} + \{3\}) \\ & - 2(\{1\} + \{4\}) - 2(\{2\} + \{3\}) \\ & + (\{2\} + \{4\}) + (\{2\} + \{4\}) = 0\end{aligned}$$
であり，$f \in \mathrm{Harm}_2$ である．

例 4.3. $C = \{(0,0,0,0), (1,1,0,0), (0,0,1,0), (1,1,1,0)\}$, $f = -2\{1,2\} + \{1,3\} + \{1,4\} + \{2,3\} + \{2,4\} - 2\{3,4\}$ とおく．すると $\mathrm{Aut}(C) = \langle (1,2) \rangle$, $f \in \mathrm{Harm}_2^{\mathrm{Aut}(C)}$ である．

これらの概念を用いて，t-デザインかどうかを以下のように判定できる．

定理 4.1 (Delsarte (1978), [4])**.** C_ℓ は t-デザイン $\Leftrightarrow \sum_{c \in C_\ell} \widetilde{f}(\mathrm{supp}(c)) = 0, \forall f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$ $(1 \le k \le t)$

調和重さ多項式は次のように書ける．
$$\begin{aligned} w_{C,f}(x,y) &= \sum_{c \in C} \widetilde{f}(\mathrm{supp}(c)) x^{n-\mathrm{wt}(c)} y^{\mathrm{wt}(c)} \\ &= \sum_{\ell=0}^{n} (\sum_{c \in C_\ell} \widetilde{f}(\mathrm{supp}(c))) x^{n-\ell} y^\ell. \end{aligned}$$

したがって次の定理を得た．

定理 4.2. 1. 全ての $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$ $(1 \le k \le t)$ に対して，$w_{C,f}(x,y) = 0$ と仮定する．このとき全ての ℓ に対して C_ℓ $(\neq \emptyset)$ は t-デザインである．

2. 全ての $f \in \mathrm{Harm}_k^{\mathrm{Aut}(C)}$ $(1 \le k \le t)$ に対して，$w_{C,f}(x,y)+w_{C^\perp,f}(x,y) = 0$ と仮定する．このとき全ての ℓ に対して $C_\ell \cup (C^\perp)_\ell$ $(\neq \emptyset)$ は t-デザインである．

以上の準備の下，以下の主結果を証明しよう．

定理 4.3. 全ての ℓ に対して $(\widetilde{Q}_{p+1})_\ell \cup (\widetilde{Q}_{p+1}^\perp)_\ell$ $(\neq \emptyset)$ は 3-デザインである．

Proof. $C = \widetilde{Q}_{p+1}$，$G = \mathrm{Aut}(C) = PSL_2(p)$ とおく．$\binom{X}{3} = G\{\infty, 0, -1\} \sqcup G\{\infty, 0, \theta\}$，$|G\{\infty, 0, -1\}| = |G\{\infty, 0, \theta\}|$ を思い出そう．すると

$$\mathrm{Harm}_3^G = \langle c(R(T_1) - R(T_2)) \rangle,$$

がわかる．ここで $R(T_i) = \sum_{g \in G} T_i^g$ である．すると $f = R(T_1) - R(T_2) \in \mathrm{Harm}_3^G$ に対して，$w_{C,f} + w_{C^\perp,f} = 0$ である．実際，

$$\begin{aligned} w_{C,f} + w_{C^\perp,f} &= w_{C,f} + w_{C^\sigma,f} \ (\because C^\perp = C^\sigma) \\ &= w_{C,f} + w_{C,f^{\sigma^{-1}}} \\ &= w_{C,f} + w_{C,-f} \\ &= w_{C,f} - w_{C,f} = 0. \end{aligned}$$

□

5 今後の課題

主結果は以下のように一般化される．

定理 5.1. C を長さ n の isodual 符号とする．$X := \{1, \ldots, n\}$，$G = \mathrm{Aut}(C)$ とおく．このとき G は $\binom{X}{t}$ に作用するが，その軌道が以下のように分解したとしよう．

$$\binom{X}{t} = GT_1 \sqcup GT_2,$$

$(GT_1)^\sigma = GT_2$. すると次が成立する．

(1) $J_{C,T} + J_{C^\sigma,T}$ は $T \in \binom{X}{t}$ の選び方によらない．

(2) f を次数 t の調和重さ多項式として，$\mathrm{Aut}(C)$ で不変なものとしよう．このとき

$$w_{C,f} + w_{C^\sigma,f} = 0.$$

この定理の仮定を，以下のように 3 つの軌道に分かれるように一般化することも可能である．

$$\binom{X}{t} = GT_1 \sqcup GT_2 \sqcup GT_3.$$

これを用いて符号から 6-デザインを構成することは興味ある問題である．

6 謝辞

第 39 回代数的組合せ論シンポジウムで講演の機会を与えてくださった関係者の皆様に感謝申し上げます．

本研究は科学研究費補助金 (22K03277) の助成を受けております．

References

[1] M. Awada, T. Miezaki, A. Munemasa, and H. Nakasora, A note on a t-design in isodual codes, in preparation.

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

[3] A. Bonnecaze and P. Sole, The extended binary quadratic residue code of length 42 holds a 3-design, *J. Combin. Des.* **29** (2021), no. 8, 528–532.

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

[5] R. Ishikawa, Exceptional designs in ternary and quaternary extended quadratic residue codes, submitted.

[6] M. Ozeki, On the notion of Jacobi polynomials for codes. *Math. Proc. Cambridge Philos. Soc.* **121** (1997), no. 1, 15–30.

符号の重み多項式に関する話題 *

大浦　学
金沢大学理工研究域

本講演の最終目標は、長岡昇勇先生（近畿大学名誉教授）との共同研究の結果 [4] を紹介することです。目標はそうなのですが、所々脱線しながら話しを進めたいと思います。ここで紹介する研究には、長岡先生と竹森翔さん [5] の先行研究（格子、テータ関数）があり、それに忠実に従った形で本研究は行われました。講演ではその先行研究については触れずに、符号理論に関する部分についてのみ述べました。この報告集でもそれに倣います。

1　符号の一般論

まず、$\mathbf{F}_2 = \{0, 1\}$ を 2 元体とします。2 元体以外での議論も可能ですが、この講演では 2 元体のみ扱います。この体の n 次元ベクトル空間 $\mathbf{F}_2^n$ の元 $u = (u_1, \ldots, u_n)$ に対して、0 でない座標の数を u の重さと言い、$wt(u)$ と表します。ベクトル空間 $\mathbf{F}_2^n$ の元 $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n)$ に対して、内積を

$$u \cdot u = u_1 v_1 + \cdots + u_n v_n$$

で定義します。さて、$\mathbf{F}_2$ 上の符号を取り扱う訳ですが、講演では線形符号のみ扱います。そこで、部分空間 $\mathcal{C}$ を、長さ n の符号（線形符号とは呼ばないこと）と呼ぶことにします。単にベクトル空間というだけでは色々な結果も得られづらく、我々は符号にいくつかの条件を課します。長さ n の符号 $\mathcal{C}$ に対して、その双対符号 $\mathcal{C}^\perp$ を

$$\mathcal{C}^\perp = \{u \in \mathbf{F}_2^n : \ u \cdot v = 0, \ \forall v \in \mathcal{C}\}$$

で定義します。この $\mathcal{C}$ は、次元 $n - \dim \mathcal{C}$ を持ちます。符号 $\mathcal{C}$ が自己双対符号とは、$\mathcal{C} = \mathcal{C}^\perp$ が成り立つときに言います。もし、$\mathcal{C}$ が自己双対であれば、一般に成り立つ関係式

$$\dim \mathcal{C} + \dim \mathcal{C}^\perp = n$$

から、n は偶数で、さらに $\dim \mathcal{C} = n/2$ であることがわかります。自己双対に加えて、別のクラス、重偶符号は、任意の $u \in \mathcal{C}$ に対して

$$wt(u) \equiv 0 \pmod 4$$

が成り立つときに言います。我々が興味があるのは

$$\text{自己双対} + \text{重偶}$$

の 2 つの性質を持つクラスです。このクラスを Type II 符号と呼びます。すなわち

$$\text{Type II} \ = \text{自己双対} + \text{重偶}$$

* 第３９回代数的組合せ論シンポジウムにおける講演をかなり忠実に再現したものです。

です。

一般的な符号の定義は終わりまして、次に符号から得られる多項式に話しを移します。今、$\mathcal{C}$ を長さ n の符号とします。それに付随する重み多項式を

$$\begin{aligned} W_{\mathcal{C}}(x,y) &= \sum_{u\in\mathcal{C}} x^{n-wt(u)}y^{wt(u)} \\ &= \sum_{i=0}^{n} A_i x^{n-i}y^i, \end{aligned}$$

ただし $A_i = \sharp\{u\in\mathcal{C}:\ wt(u)=i\}$、で定義します。これは、次数 n の斉次多項式となっています。ここで、この重み多項式の一般化を念頭においた、テクニカルな話題を入れておきます。重さを復習しておくと、u の重さとは、$0\in\mathbf{F}_2$ とは異なる u の座標の数でした。ところで、u は 0 か 1 がならんでいるので、0 と異なるとは、つまり 1 ということです。なぜ最初から 0 とは異なる、ではなく、1 である、という言い方をしないのかと言うと、2 元体以外を取り扱う場合を考えて、なのです。しかし、$\mathbf{F}_2$ のみ扱います、と最初に宣言しているので、まあ最初から重さを 1 が現れる個数と言っても良さそうですが。戻ります。次でした。

$$\begin{aligned} wt(u) &= \sharp\{i:\ u_i\neq 0\} \\ &= \sharp\{i:\ u_i = 1\}. \end{aligned}$$

変数 x のべきも同様に考えると

$$n - wt(u) = \sharp\{i:\ u_i = 0\}$$

となります。そう理解すると、

$$n_a(u) = \sharp\{i:\ u_i = a\},\ a\in\mathbf{F}_2$$

を導入することで

$$\begin{aligned} W_{\mathcal{C}}(x_0,x_1) &= \sum_{u\in\mathcal{C}} x_0^{n_0(u)}x_1^{n_1(u)} \\ &= W_{\mathcal{C}}(x_a : a\in\mathbf{F}_2) \end{aligned}$$

という表示ができます。この表示が、重み多項式の一般化（多変数化）には都合がいいようです。

上で、我々は Type II 符号に興味がある、と述べましたが

我々は Type II 符号の重み多項式に興味がある

というのが、より適切かもしれません。では、その重み多項式について、我々は何が言えるのでしょうか。

2　重み多項式の性質

長さ n の符号 $\mathcal{C}$ に対して

$$W_{\mathcal{C}^\perp}(x,y) = \frac{1}{|\mathcal{C}|}W_{\mathcal{C}}(x+y,x-y)$$

が知られています（MacWilliams）。変数 x,y の代わりに x_0,x_1 を導入するんじゃなかったの、と言われそうですが、ここでは x,y の方が簡単だから、ということです。使い分けていきます。さて、MacWilliams 恒等式は、双対符号の重み多項式は、もとの符号の重み多項式から代数的な操作で得ることができると述べてい

ます。例えば、双対符号の構造が複雑で、双対符号の重み多項式が直接には求めづらい場合で、もとの符号の符号の重み多項式が比較的容易に得られる場合などに有効です。我々は、MacWilliams 恒等式を長さ n の自己双対符号 $\mathcal{C} = \mathcal{C}^{\perp}$ に適用します。この場合、n は偶数で $\dim \mathcal{C} = n/2$、言い換えると $|C| = 2^{n/2}$ でした。これらを MacWilliams 恒等式にあてはめると

$$\begin{aligned} W_{\mathcal{C}}(x,y) &= \left(\frac{1}{\sqrt{2}}\right)^{n} W_{\mathcal{C}}(x+y, x-y) \\ &= W_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) \end{aligned}$$

となります。つぎに $\mathcal{C}$ が重偶の場合に考えます。今、$\mathcal{C}$ を重偶符号とすると

$$\begin{aligned} W_{\mathcal{C}}\left(x, \sqrt{-1}y\right) &= \sum_{u \in \mathcal{C}} x^{n-wt(u)} \left(\sqrt{-1}y\right)^{wt(u)} \\ &= \sum_{u \in \mathcal{C}} x^{n-wt(u)} y^{wt(u)} \\ &= W_{\mathcal{C}}(x,y) \end{aligned}$$

となります。

今までの話しを Type II 符号についてまとめますと、Type II 符号 $\mathcal{C}$ の重み多項式は

$$\begin{aligned} W_{\mathcal{C}}\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) &= W_{\mathcal{C}}(x,y), \\ W_{\mathcal{C}}\left(x, \sqrt{-1}y\right) &= W_{\mathcal{C}}(x,y) \end{aligned}$$

を満たすことになります。

ここで、個人的な思い出話しを挿入します。吉田知行先生の数学セミナー（１９８７年４月号、数学との出会い）の記事です。実際には、それらがまとめられた増刊号だったかもしれません。吉田先生は「２４との出会いと再会」と題する文章で、次で締めくくられています。「最後に計算問題をひとつ。

$$f(x,y) = x^{24} + 759x^{16}y^{8} + 2576x^{12}y^{12} + 759x^{8}y^{16} + y^{24}$$

とおけば

$$\begin{aligned} f\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) &= f(x,y), \\ f\left(x, \sqrt{-1}y\right) &= f(x,y) \end{aligned}$$

であることを示せ。」この $f(x,y)$ はあとで出てくる、長さ 24 の Type II 符号、いわゆる Golay 符号の重み多項式です。今までの議論から、この $f(x,y)$ が上記 2 つの等式を満たすことは分かります。

重み多項式と有限群の不変式論を結びつける Gleason の定理に移っていきます。Gleason の定理への入門的な論文を引用します。N. J. A. Sloane [11] は符号理論を不変式論の観点から解説しました。その論文では、Type II 符号の重み多項式が 2 つの等式

$$W\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right) = W(x,y), \tag{1}$$

$$W\left(x, \sqrt{-1}y\right) = W(x,y) \tag{2}$$

を満たすことを注意したあと、つぎのように述べます。“The problem we want to solve is to find all polynomials $W(x,y)$ satisfying (1) and (2).” 求めたいのは

$$\{W(x,y) \in \mathbf{C}[x,y] :\ W(x,y) \text{ satisfies } (1)+(2)\}$$

で、この集合は環をなすことが分かります。今、

$$G = \left\langle \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{-1} \end{pmatrix} \right\rangle$$

とおくと、我々がターゲットとしている環は、群 G の不変式環

$$R^G = \left\{ W(x,y) \in \mathbf{C}[x,y] :\ W(ax+by, cx+dy) = W(x,y),\ \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G \right\}$$

です。ここで、G は位数 192 の複素鏡映群で、Shephard-Todd [10] のリストにおいて、No. 9 です。今までの議論から

$$\begin{array}{c} R^G \\ \cup \\ \text{Type II 符号の重み多項式で生成される } \mathbf{C}[x,y] \text{ の部分環} \\ \cup \\ \mathbf{C}[W_{e_8}, W_{g_{24}}] \end{array}$$

の包含関係が成り立ちます。ここで、e_8 は長さ 8 の Type II 符号で Hamming 符号、g_{24} は長さ 24 の Type II 符号で Golay 符号、とそれぞれ呼ばれるものです。Gleason は、1970 年の国際数学者会議で、不変式環 R^G が 2 つの Type II 符号の重み多項式 W_{e_8}, $W_{g_{24}}$ で生成されることを発表します [3]、すなわち、3 つの環

$$\boxed{R^G}, \boxed{\text{Type II 符号の重み多項式で生成される } \mathbf{C}[x,y] \text{ の部分環}}, \boxed{\mathbf{C}[W_{e_8}, W_{g_{24}}]}$$

は一致します。

3 Type II 符号の分類

ここで、Type II 符号がどれほどあるのか、述べておきます。長さ n の 2 つの符号がある程度同じ性質を持つ場合を除くため、同値の概念を導入します。長さ n の符号 $\mathcal{C}$, $\mathcal{C}'$ が同値であるとは、$\mathcal{C}$ の座標の置換をした後、$\mathcal{C}'$ と一致するときに言います。つまり、

$$\mathcal{C} \text{ と } \mathcal{C}' \text{ が同値} \Leftrightarrow \exists \sigma \in S_n,\ \mathcal{C}^\sigma = \mathcal{C}'$$

です。この同値関係のもと、Type II 符号の分類を述べる訳ですが、その前に次の命題を述べておきます。

命題 1. 長さ n の *Type II* 符号が存在するための必要十分条件は $n \equiv 0 \pmod 8$ である。

Type II 符号の同値類を除いた個数はつぎの表 1 になります ([8, 9, 2, 1])。

長さを固定した場合の重み多項式のなす空間について述べます。まず同値な符号の重み多項式は一致します。しかし、非同値な符号であっても、同じ重み多項式を持つ場合があります。長さ 16 の Type II 符号は 2

表 1　長さ 24 の Type II 符号の分類

符号の長さ n	8	16	24	32	40	≥ 48
Type II 符号の個数	1	2	9	85	94343	unknown

つ（e_8^2, d_{16}^+ と表される）ありますが、それの重み多項式は一致します。この点は、種数の概念を取り入れることで、ある意味、解決します。符号 $\mathcal{C}$ の種数 g の重み多項式は

$$W_{\mathcal{C}}^{(g)}(x_a:\ a\in\mathbf{F}_2^g)=\sum_{u_1,\dots,u_g\in\mathcal{C}}\prod_{a\in\mathbf{F}_2^g}x_a^{n_a(u_1,\dots,u_g)}$$

ここで

$$n_a(u_1,\dots,u_g)=\sharp\{i:\ a=(u_{1i},\dots,u_{gi})\}$$

です。すると長さ 16 の Type II 符号の種数 g の重み多項式ですが

$$W_{e_8^2}^{(g)}\neq W_{d_{16}^+}^{(g)}\Leftrightarrow g\geq 3$$

が知られています。同様の問題を長さ 24 の場合に考えますと

$$\dim\langle W_{\mathcal{C}_1}^{(g)},\dots,W_{\mathcal{C}_9}^{(g)}\rangle=9\Leftrightarrow g\geq 6$$

となります（[6]. *cf.* [7]）。

4　結果（長岡昇勇先生との共同研究）

長さ 24 の Type II 符号を述べるため、具体的な符号を生成行列の形で表しておきます。添え字が符号の長さを表し、行ベクトルがその符号の基底となります。

$$d_n:\ \begin{pmatrix}111100 & \dots & 0000\\ 001111 & \dots & 0000\\ & \ddots & \\ 000000 & \dots & 1111\end{pmatrix},\quad n\equiv 0\pmod 2,$$

$$e_7:\ \begin{pmatrix}0111100\\ 0110011\\ 1101010\end{pmatrix},$$

$$e_8:\ \begin{pmatrix}11110000\\ 00111100\\ 00001111\\ 10101010\end{pmatrix}.$$

すでに何度かでてきましたが、長さ 24 の 2 元体上の Golay 符号を g_{24} で表します。この符号 g_{24} は重さ 4 の元を持たず、最小重みが 8 です。

一つ、記号を導入しましょう。長さ n, n' の符号 $\mathcal{C}$, $\mathcal{C}'$ をとります。このとき、長さ $n+n'$ の符号となる、$\mathcal{C}$ と $\mathcal{C}'$ の直和を積の形で表します：

$$\mathcal{C}\mathcal{C}'=\{(u\ u'):\ u\in\mathcal{C},\ u'\in\mathcal{C}'\}.$$

後の計算で必要となる h_i $(i = 1, 2, \ldots, 9)$ について述べておきます。例で説明します。2 番目の符号 $\mathcal{C}_2$ を考えます。この符号の成分は $d_{10}e_7^2$ です。d_{10} の重さ 4 の元の個数は 10 で、e_7 の重さ 4 の元の個数は 7 です。重さ 4 の元の個数をその符号の長さで割ると

$$\frac{10}{10} = \frac{7}{7} = 1$$

となります。この数字を h_2 とします。このように計算しますと、長さ 24 の Type II 符号の成分と h_i は次のようになります。

表 2　長さ 24 の Type II 符号

i	1	2	3	4	5	6	7	8	9
Components	d_{12}^2	$d_{10}e_7^2$	d_8^3	d_6^4	d_{24}	d_4^6	g_{24}	$d_{16}e_8$	e_8^3
h_i	$\frac{5}{4}$	1	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{11}{4}$	$\frac{1}{4}$	0	$\frac{7}{4}$	$\frac{7}{4}$

ここで

$$\begin{aligned}\Delta &= \frac{1}{42}\left(W_{\mathcal{C}_9}^{(1)} - W_{\mathcal{C}_7}^{(1)}\right)\\ &= x^4y^4(x^4 - y^4)^4\end{aligned}$$

とおきましょう。種数 1 の場合の結果を述べます。

定理 2.　(1) $i = 1, 2, \ldots, 9$ のとき、

$$W_{C_i}^{(1)} = W_{C_9}^{(1)} + 6(4h_i - 7)\Delta$$

が成り立つ。

(2) i, j は $1, 2, \ldots, 8$ の整数で、異なるとする。このときある整数 m について $4h_i \equiv 4h_j \pmod{m}$ が成り立つならば

$$W_{C_i}^{(1)} \equiv W_{C_j}^{(1)} \pmod{6m}$$

である。

(3) C_α, C_β を長さ 24 の *Type II* で $h_\alpha < h_\beta$ とする。このとき、$i = 1, 2, \ldots, 9$ について

$$W_{C_i}^{(1)} = \frac{h_i - h_\beta}{h_\alpha - h_\beta}W_{C_\alpha}^{(1)} + \frac{h_i - h_\alpha}{h_\beta - h_\alpha}W_{C_\beta}^{(1)}$$

が成り立つ。

種数 2 について結果を述べるため、つぎの整数係数の多項式を準備します。

$$\begin{aligned}X &= \frac{1}{42}\left(W_{C_9}^{(2)} - W_{C_7}^{(2)}\right),\\ Y &= -\frac{11}{7}W_{C_9}^{(2)} + \frac{4}{7}W_{C_7}^{(2)} + W_{C_5}^{(2)}\end{aligned}$$

に対して、

$$X_{24} = X - \frac{1}{44}Y,$$
$$Y_{24} = \frac{1}{2^4 3 \cdot 11}Y.$$

とおきます。種数 2 の多項式は、Φ 作用素

$$\Phi : \mathbf{C}[x_a \in \mathbf{F}_2^g] \to \mathbf{C}[x_{a'} : a' \in \mathbf{F}_2^{g-1}]$$
$$x_a \mapsto \begin{cases} x_{a'} & \text{if } a = \begin{pmatrix} a' \\ 0 \end{pmatrix}, \\ 0 & \text{if } a = \begin{pmatrix} a' \\ 1 \end{pmatrix} \end{cases}$$

で、種数 1 の多項式と結びつきます。

命題 3. $\Phi(X_{24}) = \Delta$ および $\Phi(Y_{24}) = 0$.

種数 2 の場合の結果を述べます。

定理 4. (1) $i = 1, 2, \ldots, 9$ に対して

$$W_{C_i}^{(2)} = W_{C_9}^{(2)} + 6(4h_i - 7)X_{24} + 24(2h_i + 3)(4h_i - 7)Y_{24}$$

が成り立つ。

(2) i, j は $1, 2, \ldots, 8$ の整数で、異なるとする。このときある整数 m について $4h_i \equiv 4h_j \pmod{m}$ が成り立つならば

$$W_{C_i}^{(2)} \equiv W_{C_j}^{(2)} \pmod{6m}.$$

である。

(3) $C_\alpha, C_\beta, C_\gamma$ を長さ 24 の *Type II* 符号とし $h_\alpha < h_\beta < h_\gamma$ が成り立っている。このとき、$i = 1, 2, \ldots, 9$ に対して

$$W_{C_i}^{(2)} = \ell_\alpha(h_i)W_{C_\alpha}^{(2)} + \ell_\beta(h_i)W_{C_\beta}^{(2)} + \ell_\gamma(h_i)W_{C_\gamma}^{(2)}.$$

が成り立つ。ここで $\epsilon \in \{\alpha, \beta, \gamma\}$ に対して

$$\ell_\epsilon(x) = \prod_{\substack{\mu \in \{\alpha,\beta,\gamma\} \\ \mu \neq \epsilon}} \frac{x - x_\mu}{x_\epsilon - x_\mu}$$

である。

すでに出てきた事実 $W_{e_8}^{(3)} \neq W_{d_{16}^+}^{(3)}$ と $h_8 = h_9$ から、定理 2 と定理 4 それぞれにおける (1) の等式の種数 3 への拡張はないことを注意して終わりたいと思います。

参考文献

[1] Betsumiya, K., Harada, M., Munemasa, A.: A complete classification of doubly even self-dual codes of length 40. Electron. J. Combin. **19** (2012), no.3, Paper 18, 12 pp.

[2] Conway, J. H., Pless, V., Sloane, N. J. A.: The binary self-dual codes of length up to 32: a revised enumeration. J. Combin. Theory Ser. A **60** (1992), no.2, 183-195.

[3] Gleason, A. M.: Weight polynomials of self-dual codes and the MacWilliams identities. Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 3, pp. 211-215. Gauthier-Villars, Paris, 1971.

[4] Nagaoka, S., Oura, M.: Note on the Type II codes of length 24. Preprint.

[5] Nagaoka, S., Takemori, S.: Notes on theta series for Niemeier lattices Ramanujan J. **42** (2017), no. 2, 385-400.

[6] Nebe, G.: Kneser-Hecke-operators in coding theory. Abh. Math. Sem. Univ. Hamburg **76** (2006), 79-90.

[7] Oura, M., Poor, C.,; Yuen, D.: Towards the Siegel ring in genus four. Int. J. Number Theory **4** (2008), no. 4, 563-586.

[8] Pless, V.: A classification of self-orthogonal codes over GF(2). Discrete Math. **3** (1972), 209-246.

[9] Pless, V., Sloane, N. J. A.: On the classification and enumeration of self-dual codes. J. Combinatorial Theory Ser. A **18** (1975), 313-335.

[10] Shephard, G. C., Todd, J. A.: Finite unitary reflection groups. Canad. J. Math. **6** (1954), 274–304.

[11] Sloane, N. J. A.: Error-correcting codes and invariant theory: new applications of a nineteenth-century technique. Amer. Math. Monthly **84** (1977), no.2, 82-107.