第 38 回代数的組合せ論シンポジウム報告集

2022 年 6 月 16 日 − 18 日
オンライン開催

まえがき

この報告集は 2022 年 6 月 16 日から 18 日にわたり、オンラインで行われた「第 38 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 85 名の参加登録者がありました。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。

世話人：　宗政 昭弘　（東北大学）
生田 卓也　（神戸学院大学）
島倉 裕樹　（東北大学）
中空 大幸　（神戸学院大学）

第 38 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： 宗政 昭弘 （東北大学）
生田 卓也 （神戸学院大学）
島倉 裕樹 （東北大学）
中空 大幸 （神戸学院大学）

日程：2022 年 6 月 16 日 (木) ∼18 日 (土)
会場：Zoom オンライン開催

プログラム

6 月 16 日 (木)

10:30–11:10 野崎 寛（愛知教育大学）
Bounds for sets with few distances distinct modulo a prime ideal

11:20–12:00 別宮 耕一（弘前大学）
MOG と正二十面体グラフ

13:30–14:10 櫻井 太朗（千葉大学）
形式概念分析：乱択形式分脈と漸近下界

14:20–15:00 花木 章秀（信州大学）
A construction of non-schurian Schur rings over elementary abelian groups of even rank

15:20–16:00 平坂 貢（釜山国立大学）
等長列による有限距離空間の特徴づけ

16:10–16:50 宗政 昭弘（東北大学）
Quasi-symmetric 2-(41,9,9) designs

6 月 17 日 (金)

10:00–10:30 杉元 最大（筑波大学）
既約表現に関する原田予想 II が成立する有限群の例

10:40–11:10 浦野 慧（筑波大学）
整数群環上のムーンシャイン

11:20–12:00 島倉 裕樹（東北大学）
Extra automorphisms of cyclic orbifolds of lattice vertex operator algebras

13:30–14:10 栗原 大武（山口大学）
有限群から得られる一般化アレキサンダーカンドルについて

14:20–15:00 須田 庄（防衛大学校）
On tight 3-designs in the Hamming association schemes

15:20–16:00 谷口 浩朗（大和大学）
APN 関数 $f : V \to W$ について

16:10–16:50 山田 裕理（一橋大学）
Sigma involutions associated with parafermion vertex operator algebras

6 月 18 日 (土)

10:00–10:30　田中 優帆（早稲田大学）
ヤコビ多項式とデザイン理論について

10:40–11:20　Chong Zheng（早稲田大学）
Weighted Tutte-Grothendieck polynomials of graphs

11:30–12:10　渡邊 悠太（愛知教育大学）
Generalized wreath products of association schemes over a double poset

目　次

素イデアルを法として異なる距離を持つ集合の上界

Bounds for sets with few distances distinct modulo a prime ideal

野崎寛（愛知教育大学）
Hiroshi Nozaki (Aichi University of Education)

概要

K を代数体とし，K から $\mathbb{C}$ への埋め込みを一つ固定することで，その像と K を同一視する．代数体 K の整数環を $\mathcal{O}_K$ とし，その素イデアルの一つを $\mathfrak{p}$ とする．ユークリッド空間 $\mathbb{R}^d$ の部分集合 X において，互いに異なる 2 点間の二乗距離の集合を $D(X)$ と表す．$D(X)$ が $\mathcal{O}_K \setminus \mathfrak{p}$ の部分集合であり，$D(X)$ の $\mathfrak{p}$ を法として異なる元の個数が s であるとき，$|X| \leq \binom{d+s}{s} + \binom{d+s-1}{s-1}$ という上界（mod-$\mathfrak{p}$ bound）を得ることが出来る [10]．この上界は Godsil [6] が提唱した polynomial space においても全く同じ手法で示すことが出来る．本稿では，polynomial space における上界（mod-$\mathfrak{p}$ bound）を，素イデアルとは限らないイデアル I に拡張した形で述べる．

1 はじめに

本稿は，2022 年 6 月 16 日 (木)〜6 月 18 日 (土) に行われた研究集会「第 38 回代数的組合せ論シンポジウム」における講演記録である．研究集会では，[10] に沿った形で，主定理の上界（mod-$\mathfrak{p}$ bound）を証明と共に紹介した．講演内容等は [10] にまかせ，本稿では，素イデアルとは限らないイデアル I を用いた上界を，polynomial space の言葉を用いて述べる．これは，$\mathbb{R}^d$ における mod-$\mathfrak{p}$ bound の証明と同様であるから，[10] ではコメントするに留めた部分にあたる．

距離空間 (Ω, d) に対して，Ω の有限部分集合 X が **s-距離集合（s-distance set）**と呼ばれるのは，X の互いに異なる 2 点間の距離の集合

$$A(X) = \{d(x, y) \mid x, y \in X, x \neq y\}$$

の濃度が s であるときにいう．s-距離集合の主な問題は，s を固定したときに元の個数 $|X|$ に良い上界が存在するかということと，上界が存在したとすると，上界を達成する集合や，実際に $|X|$ が最大となる s-距離集合の分類である．代数的組合せ論においては，デルサルト理論（Delsarte theory）[3] を発端に，デザイン理論と肩を並べる対象として認識されるようになった．デザインとは，全体集合をある意味で近似するような部分集合のことであるが，デルサルト理論とは，組合せデザイン（combinatorial design）や直交配列（orthogonal array）などのデザインが，アソシエーションスキーム（association scheme）の上で統一的に定義でき，調和解析的な手法で下界を得るなどの一般理論を確立したものである．組合せデザインはジョンソンスキーム（Johnson scheme）のデザインに対応しており，直交配列はハミングスキーム（Hamming scheme）のデザインに対応している．ジョンソンスキームとハミングスキームを含むアソシエーションスキームの良いクラスに Q 多項式スキームというものがある．デルサルト理論において，Q 多項式スキームにおける強さ $2s$ のデザインには自然な下界 $|X| \geq v(s)$ が示され，また s-距離集合には自然な上界 $|X| \leq u(s)$ が示されている．このとき，これらの値に対して $v(s) = u(s)$ が成り立っており，それぞれの下界・上界を達成する対象が驚くべき

ことに一致している．さらに，強さ t のデザイン X が s-距離であるとき，$t \geq 2s-2$ を満たせば，X は自然な隣接関係により Q 多項式スキームの構造を持つ．s を固定したときに出来るだけ大きい s-距離集合を構成して，そのデザインの強さを見たり，アソシエーションスキームなどの良い組合せ構造を得たいというのが，s-距離集合の組合せ論的な動機である．デルサルト理論では，アソシエーションスキーム上で符号理論も展開されている．符号としての主な問題意識は最小距離を固定したときに，出来るだけ多くの点を持つ部分集合 X を決定することである．同論文 [3] で示された線形計画限界（Linear programming bound, Delsarte's method ともいわれる）は，最小距離を固定したときの元の個数 $|X|$ に対して，良い上界を与える優れた手法であるが，これは最大な s-距離集合を決定する際にも有用に働く．

先に紹介した Q 多項式スキームではユークリッド球面 S^{d-1} に見られるような，調和解析が行える．Delsarte [3] が提唱した Q 多項式スキーム上でのデザイン・符号理論は，球面の有限部分集合にも同じ理論を展開できる [4]．より一般的な枠組みとして Godsil [6, 7] が提唱した polynomial space は，Q 多項式スキームや球面 S^{d-1} を含むクラスであり，球面の類似としての実射影空間や複素射影空間も含む．これら射影空間についてのデザイン・符号理論は Levenshtein [9] が詳しい．Q 多項式スキームの典型的なモデルとして，ジョンソンスキーム（またはハミングスキーム）が選ばれることが多く，ジョンソンスキームで調和解析的手法で得られた定理は，自然に Q 多項式スキームについても成り立つ．また球面 S^{d-1} で調和解析的な手法で得られたデザイン・符号の定理は，Q 多項式スキームや実または複素射影空間で自然に成り立つ．一方，ユークリッド空間 $\mathbb{R}^d$ は自然には polynomial space ではなく，調和解析についての道具が揃っていないため，球面のようにデザイン・符号理論が成熟しているとは言えない．

ジョンソン・ハミングスキームの s-距離集合は，組合せ幾何の文脈では L-交差族（L-intersecting family）として知られている．F を濃度 n の有限集合とし，$\mathfrak{F}$ を F の部分集合族とする．$L \subset \{1,\dots,n\}$ とし，$\mathfrak{F}$ が**L-交差族**と呼ばれるのは，任意の $A, B \in \mathfrak{F}$ に対して，$|A \cap B| \in L$ を満たすときにいう．L-交差族 $\mathfrak{F}$ が，ある $k \in \mathbb{Z}$ が存在して，任意の $A \in \mathfrak{F}$ に対して，$|A| = k$ を満たすとき，$\mathfrak{F}$ を k-一様（k-uniform）という．k-一様で $|L| = s$ であるとき，L-交差族 $\mathfrak{F}$ はジョンソンスキームの s-距離集合に対応する，このとき $|\mathfrak{F}| \leq \binom{n}{s}$ を満たす [11]．k-一様とは限らない $|F| = s$ を満たす L-交差族 $\mathfrak{F}$ は，ハミングスキームの s-距離集合に対応する．このとき $|\mathfrak{F}| \leq \sum_{=0}^{s} \binom{n}{i}$ を満たす [5]．これらの上界は本質的には Delsarte [3] に依る．ユークリッド空間 $\mathbb{R}^d$ 上の s-距離集合 X については，球面 S^{d-1} のとき，$|X| \leq \binom{d+s-1}{s} + \binom{d+s-2}{s-1}$ [4] となり，球面とは限らない場合は $|X| \leq \binom{d+s}{s}$ [1] が得られている．これらの上界は，X の各元 x に対して，X 上の実数値関数 f_x を定義し，その関数たち $\{f_x\}_{x \in X}$ が一次独立であることを示すことで，$|X|$ を $\{f_x\}$ を含む関数空間の次元で抑えるという Koornwinder [8] の手法で示されている．

本稿の主題である mod-$\mathfrak{p}$ bound は，初めに k-一様な L-交差族において示された [5]．その主張は，p を素数とし，任意の $a \in L$ に対して，$k \not\equiv a \pmod{p}$ が成り立つと仮定すると，L が p を法として s 個の異なる元しか現れないとき，$|\mathfrak{F}| \leq \binom{n}{s}$（$|L| = s$ のときと同じ上界）を満たすというものである．Blokhuis [2] はこれと同様の主張を $\mathbb{R}^d$ の s-距離集合について与えている．

定理 1.1 (mod-p bound [2])**.** X を s-距離集合とし，p を素数とする．X の互いに異なる 2 点間の二乗距離の集合を $D(X)$ とし，$D(X)$ の元が整数であると仮定する．もし，p を法として互いに異なる整数 $a_1,\dots,a_s$ が存在して，

(1) 各 $i \in \{1,\dots,s\}$ に対して，$a_i \not\equiv 0 \pmod{p}$
(2) 各 $\alpha \in D(X)$ に対して，ある $i \in \{1,\dots,s\}$ が存在して，$\alpha \equiv a \pmod{p}$

を満たすとき，

$$|X| \le \binom{d+s}{s} + \binom{d+s-1}{s-1}$$

が成り立つ．

この上界は，通常の s-距離集合の上界 $|X| \le \binom{d+s}{s}$ よりも弱いが，$s=1$ のとき上界を達成する例が存在しており，その意味では最良である．定理 1.1 は，L-交差族の mod-p bound の類似としては自然だが，$D(X) \subset \mathbb{Z}$ の仮定が強く，適応できる $X \subset \mathbb{R}^d$ が限られている．これを，代数体 K の整数環 $\mathcal{O}_K$ とその素イデアルに拡張したのが Nozaki [10] である．この [10] での証明は $\mathbb{R}^d$ の s-距離集合を扱っているが，X 上の実数値関数空間を扱うもので，自然に polynomial space に適用できる．本稿では mod-$\mathfrak{p}$ bound の Nozaki [10] の証明と同様に，一般のイデアル I における mod-I bound を polynomial space の言葉を用いて示す．

2 Polynomial space

この節では polynomial space [6, 7] の定義と，それ上の多項式関数について紹介する．Ω を（有限とは限らない）集合とする．複素数値関数 $\rho : \Omega \times \Omega \to \mathbb{C}$ を Ω 上の**分離関数（separation function）**という．一般の体への分離関数も考えられるが，本稿では複素数体で十分である．各 $a \in \Omega$ に対して，

$$\rho(a, \xi) = \rho_a(\xi)$$

は Ω から $\mathbb{R}$ への関数と見なせる．Ω 上の複素数値定数関数から成る線形空間を $\mathrm{Pol}(\Omega, 0)$ とし，

$$\mathrm{Pol}(\Omega, 1) = \mathrm{Span}_{\mathbb{R}}\{f \circ \rho_a \mid a \in \Omega, f \in \mathbb{R}[x], \deg f \le 1\}$$

とする．また帰納的に $\mathrm{Pol}(\Omega, r+1)$ を

$$\mathrm{Pol}(\Omega, r+1) = \mathrm{Span}_{\mathbb{R}}\{gh \mid g \in \mathrm{Pol}(\Omega, r), h \in \mathrm{Pol}(\Omega, 1)\}$$

で定義する．$\mathrm{Pol}(\Omega) = \bigcup_{r \ge 0} \mathrm{Pol}(\Omega, r)$ とし，$\mathrm{Pol}(\Omega)$ の元を Ω 上の**多項式（polynomial）**（または多項式関数）という．$\mathrm{Pol}(\Omega, r) \setminus \mathrm{Pol}(\Omega, r-1)$ の元は，Ω 上の次数 r の多項式と呼ばれる．

定義 2.1 (Polynomial space)**.** ρ を集合 Ω 上の分離関数とする．$\mathrm{Pol}(\Omega)$ における内積 $\langle f, g \rangle$ を一つ固定する．(Ω, ρ) が **polynomial space** と呼ばれるのは以下の 4 条件を満たすときである．

(1) 任意の $x, y \in \Omega$ に対して, $\rho(x, y) = \rho(y, x)$ を満たす．
(2) 各 r に対して $\mathrm{Pol}(\Omega, r)$ の次元が有限である．
(3) 任意の $f, g \in \mathrm{Pol}(\Omega)$ に対して, $\langle f, g \rangle = \langle 1, fg \rangle$ が成り立つ．
(4) $f(x) \ge 0$（$x \in \Omega$）を満たす $f \in \mathrm{Pol}(\Omega)$ に対して, $\langle 1, f \rangle \ge 0$ が成り立ち, $\langle 1, f \rangle = 0$ であることと $f = 0$ であることが同値である．

Ω が有限集合のときは，$\mathrm{Pol}(\Omega)$ の内積として，

$$\langle f, g \rangle = \frac{1}{|\Omega|} \sum_{x \in \Omega} f(x) g(x), \qquad f, g \in \mathrm{Pol}(\Omega).$$

を常に採用する．

Ω が 2 つの分離関数 ρ, σ を持つとする．もし $a \in \mathbb{C} \setminus \{0\}$ と $b \in \mathbb{C}$ が存在し, 任意の $x, y \in \Omega$ に対して, $\rho(x,y) = a\sigma(x,y) + b$ が成り立つなら, それぞれの分離関数を用いて定義される $\mathrm{Pol}_\rho(\Omega, r)$ と $\mathrm{Pol}_\sigma(\Omega, r)$ は各 $r \geq 0$ に対して等しい．このような ρ, σ は**アフィン同型（affinely equivalent）**と呼ばれる．Polynomial space における諸定理において，r 次以下の多項式の空間 $\mathrm{Pol}_\rho(\Omega, r)$ は本質的な役割を担い，アフィン同型ある分離関数を用いても polynomial space の性質は変わらないと言ってよい．

次に s-距離集合の定義を与える．

定義 2.2 (s-距離集合)**.** (Ω, ρ) を polynomial space とし，

$$D(X) = \{\rho(x,y) \mid x, y \in X, x \neq y\}$$

と定義する．Ω の有限部分集合 X が $|D(X)| = s$ を満たすとき，X を **s-距離集合（s-distance set）**という．

s-距離集合の元の個数に対して次の上界が知られている．

定理 2.3 ([7, Theorem 4.1])**.** (Ω, ρ) を polynomial space とし，$X \subset \Omega$ を s-距離集合とする．$\rho(a,a) \notin \{\rho(a,b) \mid b \in X, a \neq b\}$ であるとき,

$$|X| \leq \dim(\mathrm{Pol}(\Omega, s))$$

が成り立つ.

ここでは，polynomial space を仮定したが，s-距離集合の定義と上界を与えるだけであれば，定義 2.1(1), (2) の条件だけで十分である．定義 2.1(3), (4) はデザイン理論を展開する上で必要となる．Ω がユークリッド球面 S^{d-1} で，ρ は標準内積または二乗距離（これらはアフィン同型）とすれば，$\mathrm{Pol}(\Omega, s)$ は s 次以下の調和多項式から成る線形空間である．X を Q 多項式スキームとし，$\rho(x,y) = (E_1)_{xy}$（原子冪等元 E_1 の xy 成分）とすれば，$\dim(\mathrm{Pol}(\Omega, s))$ は原子冪等元 E_i の階数 m_i の和 $\sum_{i=0}^{s} m_i$ である．例えば，ジョンソンスキームは Q 多項式スキームだが，ジョンソン距離 $k - |x \cap y|$ ($|x| = |y| = s$) と $(E_1)_{xy}$ はアフィン同型である． Q 多項式スキームとは限らない一般のアソシエーションスキームに対しても $\rho(x,y) = (E_1)_{xy}$ などとして，定理 2.3 を得ることは可能だが，小さい i でも $|\Omega| = \dim \mathrm{Pol}(\Omega, i)$ となってしまい，良い評価を与えない場合が殆どである．

3　代数体の整数環と中山の補題

この節では代数体と整数環に関する基本的事項を復習する（詳細は [12] などを参照）．**代数体** K とは有理数体 $\mathbb{Q}$ の有限次拡大で，本稿では K から複素数体 $\mathbb{C}$ への埋め込みを一つ固定し，K と対応する $\mathbb{C}$ の部分体と同一視する．K の元で代数的整数であるもの全体から成る環を $\mathcal{O}_K$ と表し**整数環**という．K は $\mathcal{O}_K$ の商体であることや，$\mathcal{O}_K$ の素イデアルは極大イデアルであること，$\mathcal{O}_K$ は有限生成自由 $\mathbb{Z}$ 加群であることはよく知られている．簡単な例として，$K = \mathbb{Q}$ のときは $\mathcal{O}_K = \mathbb{Z}$ であり，平方因子を持たない d に対して $K = \mathbb{Q}(\sqrt{d})$ のときは,

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z} & d \equiv 1 \pmod 4 \text{ のとき} \\ \mathbb{Z} + \sqrt{d}\mathbb{Z} & d \equiv 2, 3 \pmod 4 \text{ のとき} \end{cases}$$

となることが知られている.

次に整数環 $A = \mathcal{O}_K$ のイデアル I に対して，局所化を定義する．剰余環 A/I の単元の集合 $(A/I)^\times$ に対

して，

$$S = \bigcup_{R \in (A/I)^\times} R$$

と定義する．A の S による**局所化**とは，次に定義される環 A_I のことである．

$$A_I = S^{-1}A = \{a/s \mid a \in A, s \in S\}.$$

$I = \mathfrak{p}_1^{\lambda_1} \cdots \mathfrak{p}_r^{\lambda_r}$ と素イデアル分解すれば，A_I の素イデアル（極大イデアルでもある）は $\mathfrak{p}_i A_I$（$\mathfrak{p}_i$ の元たちで生成される A_I のイデアル）の r 個しかない．環 A と局所化 A_I について，自然な環準同型 $A/I \to A_I/IA_I$ が同型となることが確かめられる．

次の定理は，主定理（mod-I bound）の証明に用いる．

定理 3.1 (中山の補題)**.** A を単位元を持つ可換環とする．J を A の全ての極大イデアルに含まれるイデアルとする．M を有限生成 A 加群とする．そのとき，$JM = M$ が成り立てば，$M = \{0\}$ である．

4 s-距離集合における mod-I bound

複素数値分離関数を ρ をもつ polynomial space (Ω, ρ) について，次の mod-I bound を得ることができる．

定理 4.1 (mod-I bound)**.** (Ω, ρ) を polynomial space とする．K を代数体とし，$\mathbb{C}$ への埋め込みを一つ固定し，$K \subset \mathbb{C}$ と見なす．$A = \mathcal{O}_K$ を K の整数環とし I を A のイデアルとする．

$$S = \bigcup_{R \in (A/I)^\times} R$$

とし，A_I を A の S による局所化とする．X を Ω の有限部分集合とし，$D(X) \cup \{\rho(x, x) \mid x \in X\} \subset A_I$ と仮定する．IA_I を法として互いに異なる $a_1, \ldots, a_s \in A_I$ が存在して，

(1) 任意の $x \in X$ と任意の $i \in \{1, \ldots, s\}$ に対して，$\rho(x, x) - a_i \in A_I^\times$
(2) 任意の $\alpha \in D(X)$ に対して，ある $i \in \{1, \ldots, s\}$ が存在して $\alpha \equiv a_i \pmod{IA_I}$

を満たすとすると，

$$|X| \leq \dim(\mathrm{Pol}(\Omega, s))$$

が成り立つ．

証明. 各 $x \in X$ に対して，Ω 上の関数を

$$f_x(\xi) = \prod_{i=1}^{s} (\rho(x, \xi) - a_i)$$

と定義すると，f_x は $\mathrm{Pol}(\Omega, s)$ の元である．この関数は，

$$f_x(x) = \prod_{i=1}^{s} (\rho(x, x) - a_i) \in A_I^\times$$
$$f_x(y) \equiv 0 \pmod{IA_I} \tag{4.1}$$

を満たす．

中山の補題における全ての A_I の極大イデアルに含まれるイデアル J は，$J = \mathfrak{p}_1 \cdots \mathfrak{p}_r A_I$ ととれることに注意して，$\{f_x\}_{x\in X}$ が $\mathrm{Pol}(\Omega, s)$ の元として一次独立であることを示す．ある $m_x \in \mathbb{C}$（$x \in X$）が存在して，

$$\sum_{x\in X} m_x f_x(\xi) = 0 \tag{4.2}$$

が成り立つと仮定する．M を $\{m_x\}_{x\in X}$ で生成される $\mathbb{C}$ の有限生成部分 A_I 加群とする．つまり，

$$M = \sum_{x\in X} m_x A_I.$$

(4.1) と (4.2) から，各 $y \in X$ に対して，

$$m_y f_y(y) = -\sum_{x\in X, x\neq y} m_x f_x(y) \in JM$$

が成り立つ．$f_y(y) \in A_I^\times$ より，$f_y(y)^{-1} \in A_I$ が存在して，

$$m_y = -\sum_{x\in X, x\neq y} m_x f_x(y) f_y(y)^{-1} \in JM$$

となる．M の生成系の各元 m_y が JM の元であるから $M \subset JM$ となり，$M = JM$ となる．よって，中山の補題から $M = \{0\}$ が成り立つ．これは任意の $x \in X$ に対して $m_x = 0$ であることを意味しており，$\{f_x\}_{x\in X}$ が一次独立であることが示された．したがって，

$$|X| = \{f_x\}_{x\in X} \leq \dim(\mathrm{Pol}(\Omega, s))$$

が成り立つ． □

定理 4.1 において，ρ が距離関数であるときは，$\rho(x,x)$ は常に 0 であり，$\rho(x,x) \in A_I$ という条件は必要でなくなるが，一般の分離関数 ρ においては必要である．イデアル $I \subset A$ の素イデアル分解を $I = \prod_{i=1}^r \mathfrak{p}_i^{\lambda_i}$ とする．$a \in A_I^\times$ ならば，$a = s_1/s_2$ となる $s_1, s_2 \in S = \bigcup_{R\in(A/I)^\times} R$ が存在する．中国の剰余定理より，自然な環準同型により $A/I \cong A/\mathfrak{p}_1^{\lambda_1} \times \cdots \times A/\mathfrak{p}_r^{\lambda_r}$ であることに注意すると，各 i に対して $\bigcup_{R\in(A/I)^\times} R \subset \bigcup_{R\in(A/\mathfrak{p}_i)^\times} R = S'$ である．よって，$a = s_1/s_2$ において $s_1, s_2 \in S'$ となり，$a \in A_{\mathfrak{p}_i}^\times$ である．よって，I が定理 4.1 の条件を満たすとすると，I を含む素イデアル $\mathfrak{p}_i$ についても，同じ条件が満たされる．$A_I \subset A_{\mathfrak{p}_i}$ であることに注意して，自然な環準同型たち

$$\begin{aligned} A_I/IA_I &\to A_I/\mathfrak{p}_1^{\lambda_1} A_I \times \cdots \times A/\mathfrak{p}_r^{\lambda_r} A_I \\ &\to A_I/\mathfrak{p}_1 A_I \times \cdots \times A/\mathfrak{p}_r A_I \\ &\to A_{\mathfrak{p}_1}/\mathfrak{p}_1 A_{\mathfrak{p}_1} \times \cdots \times A_{\mathfrak{p}_r}/\mathfrak{p}_r A_{\mathfrak{p}_r} \end{aligned}$$

を考えると，IA_I を法として互いに異なる元 $a_1, \cdots, a_s \in A_I$ たちは，$A_{\mathfrak{p}_i}$ の元とみて $\mathfrak{p}_i A_{\mathfrak{p}_i}$ を法として異なるとは限らない．つまり，定理 4.1 において，I を用いて得られる上界は，素イデアル $\mathfrak{p}_i$ を用いて得られる上界より弱いものになってしまう．

定理 4.1 において，$A/I \cong A_I/IA_I$ と $\mathcal{O}_K = A \subset A_I$ であることに注意すれば，A_I を $\mathcal{O}_K$ に，IA_I を I にそれぞれ置き換えた主張が系として得られることが分かる．

定理 4.1 は，局所 s-距離集合（locally s-distance set）についても同様に得られる．局所 s-距離集合 X とは，$D_x(X) = \{\rho(x,y) \mid y \in X, y \neq x\}$ とするとき，任意の $x \in X$ に対して，$|D_x(X)| \leq s$ が成り立つとき

にいう．mod-I bound では $D_x(X)$ が IA_I を法として異なる s 個以下の元をもつという仮定になり，f_x は $D_x(X) \mod I$ を用いて定義される．

講演後に東北大学の宗政昭弘先生から，$\{f_x\}_{x\in X}$ の一次独立性を示すために行列 $(f_x(y))_{x,y\in X}$ の行列式が 0 でないことを示せばよいとのご指摘を頂いた．$(f_x(y))$ は各成分が A_I の元であるから，その行列式を IA_I を法として 0 でないことを示せば，実数としても 0 でないことが言える．$(f_x(y))$ は IA_I を法として考えれば，対角成分に単元が並ぶ対角行列であるから，その行列式が 0 でないことは，すぐに分かる．この手法を用いると，全順序付けられた s-距離集合（ordered s-distance set）についても，定理 4.1 と同様の上界を得られることが分かる．全順序付けられた s-距離集合 X とは，X 上に全順序 $>$ が備わっているものとし，$D_x(X) = \{\rho(x,y) \mid y \in X, y < x\}$ としたとき，任意の $x \in X$ に対して，$|D_x(X)| \leq s$ を満たすときにいう．これから自然に得られる f_x について，行列 $(f_x(y))$ が IA_I を法として三角行列になることから，その行列式が 0 でないことが分かる．この行列式を使った手法は，[5] でも使われている．本稿で与えた中山の補題を用いた手法は，Blokhuis [2] の手法を加群の言葉で書き直し，一般化したものと捉えることができる．

謝辞：研究集会組織委員の皆様に加えまして，講演後に，上記の別証明について教えて頂きました宗政昭弘先生と，代数体の扱いと $\mathbb{R}$ に埋め込めるとは限らない K に関するご助言を頂きました松本眞先生に感謝申し上げます．

参考文献

[1] E. Bannai, E. Bannai, and D. Stanton, An upper bound for the cardinality of an s-distance subset in real Euclidean space II, *Combinatorica* **3** (1983), 147–152.

[2] A. Blokhuis, “Few-Distance Sets”, CWI Tract 7, CWI, Amsterdam, 1984.

[3] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Res. Rep. Suppl.* No. 10, (1973).

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

[5] P. Frankl and R.M. Wilson, Intersection theorems with geometric consequences, *Combinatorica* **1** (1981), 357–368.

[6] C.D. Godsil, Polynomial spaces, *Discrete Math.*, **73** (1989), 71–88.

[7] C.D. Godsil, *Algebraic Combinatorics*, Chapman and Hall Mathematics Series, Chapman & Hall, New York, 1993.

[8] T.H. Koornwinder, A note on the absolute bound for systems of lines, *Proc. Ken. Nederl. Akad. Wetensch. Ser. A* **79** (1977), 152–153.

[9] V.I. Levenshtein, Designs as maximum codes in polynomial metric spaces, *Acta Appl. Math.* **29** (1992), 1–82.

[10] H. Nozaki, Bounds for sets with few distances distinct modulo a prime ideal, arXiv:2203.04492.

[11] D.K. Ray-Chaudhuri and R.M. Wilson, On t-designs, *Osaka J. Math.* **12** (1975), 737–744.

[12] 雪江明彦，整数論 1 初等整数論から p 進数へ，日本評論社，2013 年.

MOG と正二十面体グラフ

別宮耕一

講演：2022 年 6 月 16 日
提出：2023 年 3 月 30 日

1 序

線形符号を扱う上で，各符号語の重みに関する情報を符号の基底から得ることは，多くの場合困難である。そうした困難を g_{24} について解消する方法のひとつとして，R. T. Curtis の MOG(Miracle Octad Generator) に関する歴史的な結果 [4] がある。そこでは，$[24, 12, 8]$ extended Golay code g_{24} の符号語を MOG という形で表記することによって重みに関する情報を取り出すことができることを示している。ただ，[4] で紹介されている符号語の数え上げは，表記法が一意でないため，重複した部分をそのまま数え上げ，最後に重複度で割ることで重みごとの符号語の個数を得ている。

本講演では各 MOG について，一意な表記法を与えることで，直接数え上げができることを紹介する。加えて，g_{24} には hexacode の構造が内在することが [4] で示されているが，本講演では hexacode の基底と直接対応する形で g_{24} の基底を与えている。

2 MOG

ここでは，$\mathbb{F}_4$ 上の符号である hexacode を定義した後，R. T. Curtis によって導入された MOG について説明した上で，MOG 全体の集合が $[24, 12, 8]$ extended Golay code g_{24} のひとつの実現になっていることを紹介する。

定義 1 (hexacode)**.** 次で定義される $\mathbb{F}_4^6$ の部分空間 H_6 を **hexacode** と呼ぶこととする。

$$H_6 := \left\langle \begin{pmatrix} 1 & 0 & 0 & 1 & \omega^2 & \omega \\ 0 & 1 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \right\rangle_{\mathbb{F}_4}$$

hexacode H_6 の重み枚挙多項式は次の通りである。

$$\begin{aligned} W_{H_6}(x, y) &= \sum_{j=0}^{6} a_j x^{6-j} y^j \quad (a_j := \#\{v \in H_6 \mid \mathrm{wt}(v) = j\}) \\ &= x^6 + 45x^2y^4 + 18y^6 \end{aligned} \tag{1}$$

定義 2 (MOG)**.** 図のように各行が $\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$ でラベル付けされた 6×4 array に条件 (M1), (M2) を満たすように $*$ を書き込んだものを **MOG** と呼ぶ。

(M1) 第 1 行に記入された $*$ の個数の偶奇が，任意の列に記入された $*$ の個数の偶奇と一致する。

(M2) 各列ごとに $*$ が記入されている行に対応するラベルの総和を求める。求めた $\mathbb{F}_4$ の元を成分とする $\mathbb{F}_4^6$ の元が hexacode H_6 の元である。

0						
1						
ω						
ω^2						

例 1. 次は MOG の一例となっている。実際，第 1 行に記入された $*$ の個数は 3 であり，各行に記入された $*$ の個数はそれぞれ $1,1,1,3,1,1$ となり，条件 (M1) を満たしている。加えて，各列において，$*$ が記入されているラベルの総和はそれぞれ $0,1,0,0+\omega+\omega^2=1,\omega,\omega^2$ となり，これは生成行列の第 2 行と一致する。

	1	1	1	3	1	1	
0	$*$		$*$	$*$			3
1		$*$					
ω				$*$	$*$		
ω^2				$*$		$*$	

$(\ 0,\ 1,\ 0,\ 1,\ \omega,\ \omega^2\ ) \in H_6$

MOG が次の性質を持つことは容易に得られる。

- MOG の個数は 2^{12}
- $*$ の個数が 1 以上，7 以下の MOG は存在しない。

また，4×6 array の枠にいくつか $*$ を書き入れたものは，$\boxed{*}$ を 1，$\boxed{\ }$ に 0 に対応させることで，$\mathbb{F}_2^{24}$ の元と同一視することができる。この同一視を下で，MOG 全体の集合が $\mathbb{F}_2^{24}$ における部分空間になっていることを踏まえると，次のような結論が得られる。

定理 1 (Curtis 1973 [2]). MOG 全体の集合は $[24,12,8]$ exteded Golay code g_{24} のひとつの実現となっている。

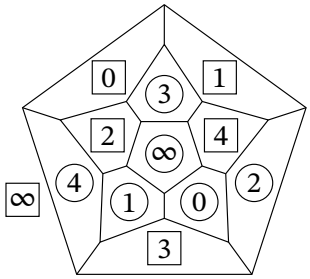
3 hexad

ここでは，正二十面体グラフが $[24,12,8]$ extended Golay code g_{24} の構造にどのように関連しているかをみるために，hexad という正二十面体グラフの部分構造を説明する。

正二十面体グラフの頂点にラベルを付ける。図で描くときにはグラフの頂点にラベルを書き入れると分かりにくいので，正二十面体グラフを正十二面体で表す。対応は次の通りとする。

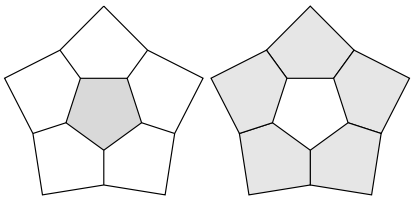
正二十面体グラフ		正十二面体
頂点	$\leftrightarrow$	面
辺で結ばれる	$\leftrightarrow$	辺を共有する

ラベルは 12 個の記号$\textcircled{0}, \boxed{0}, \textcircled{1}, \boxed{1}, \textcircled{2}, \boxed{2}, \textcircled{3}, \boxed{3}, \textcircled{4}, \boxed{4}, \textcircled{\infty}, \boxed{\infty}$とし，配置を次のように定める。

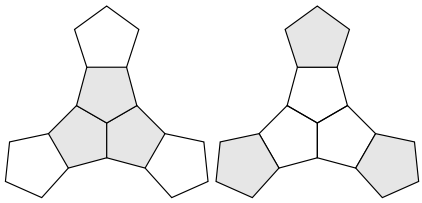


次に部分グラフについて，頂点を 2 色に塗り分けたものを考える。

まず，次のように頂点を白とグレーに塗り分けた部分グラフ全体の集合を B と表記し，その元を bull's eye と呼ぶこととする。

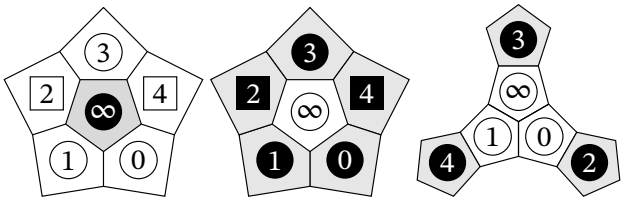


加えて，次のように頂点を白とグレーに塗り分けた部分グラフ全体の集合を T と表記し，その元を tripod と呼ぶこととする。



さらに，白で塗られた頂点には，先に定めたラベルを付け，グレーで塗られた頂点には，ラベルを黒にしたもの❶, 0, ❶, 1, ❷, 2, ❸, 3, ❹, 4, ∞, ∞ に置き換えることとする。

例 2 (bull's eye, tripod)**.** B の元と，T の元をあげる。



ただちに,

$$|B| = 12 \times 2 = 24$$
$$|T| = 20 \times 2 = 40$$

となることが分かる。

定義 3. 正二十面体グラフのラベル付き部分グラフの集合を

$$H := B \cup T$$

と定め，H の元を **hexad** と呼ぶこととする。

4 $(64, 18, 2, 6)$ 強正則グラフ

ここでは，hexad 全体の集合 H と hexacode H_6 にグラフの構造を定義する。続く節において，それらのグラフ構造が同型であることを示す。

まず，hexad 全体の集合 H に隣接関係を定義する。

$u, v \in H, u \neq v$ について，$|u \cap v| \in \{0, 2\}$ となる。ここで，グラフ G を以下のように定める。

$$V(G) := H,$$
$$E(G) := \{(u, v) \in H \times H \mid u \cap v = \emptyset\}$$

定理 2 (Curtis 1990 [4]). G は $(64, 18, 2, 6)$ 強正則グラフとなる。

次に hexacode H_6 からグラフを構成する。まず，hexacode H_6 の重み枚挙多項式 (1) より，2 値符号である。ここでグラフ Z を次のように定義する。

$$V(Z) := H_6$$
$$E(Z) := \{(u, v) \in H_6 \times H_6 \mid \mathrm{wt}(u + v) = 6\}$$

グラフ Z が $(64, 18, 2, 6)$ 強正則グラフであることはよく知られている。

5 強正則グラフ G と Z の対応

ここでは，前節で定義した 2 のグラフが同型であることを具体的な対応を与えることで示す。

hexad のラベルを 6×4 array に割り当て, **ラベル割り当て表**と呼ぶことにする。

	∞	3	0	2	1	4
0	⓪	❸	⓪	❷	①	❹
1	▯	▯	▯	▯	▯	▯
ω	■	■	■	■	■	■
ω^2	■	③	■	②	■	④

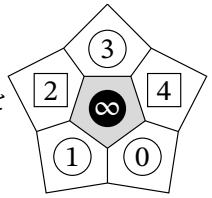
ラベル割り当て表を用いて，写像 $\varphi : H \to \mathbb{F}_4^6$ を以下のように定義する。ただし，$\mathbb{F}_4^6$ の成分の添字は左から $\infty, 3, 0, 2, 1, 4$ とする。

Step 1: ラベル割り当て表をもとに，与えられた hexad のラベルに対応する 4×6 array の枠に $*$ を書き入れる。

Step 2: 各行は $\mathbb{F}_4$ の元でラベル付けされているため，$*$ の位置により，4×6 array の列ごとに $\mathbb{F}_4$ の元が定まる。

Step 3: $\mathbb{F}_4^6$ の元が得られる。

例 3. 写像 φ によって，H の元から $\mathbb{F}_4^6$ の元を得る手順の一例をあげる。

H の元 h を 

とし，Step 1 から Step 3 の手続きを図示すると，

	∞	3	0	2	1	4
0			∗		∗	
1				∗		∗
ω	∗					
ω^2		∗				

$$(\ \omega,\ \omega^2,\ 0,\ \ 1,\ \ 0,\ \ 1\ ) \in \mathbb{F}_4^6$$

となり，

$$\varphi(h) = (\omega, \omega^2, 0, 1, 0, 1)$$

が得られる。

ここで得られた写像 φ について，64 個の H の元の像を見ることで，次が成立することが分かる。

定理 3. 写像 φ について次が成り立つ。

(i) 任意の $h \in H$ について，$\varphi(h) \in H_6$ である。
(ii) 写像 φ は G から Z へのグラフ同型を与える。

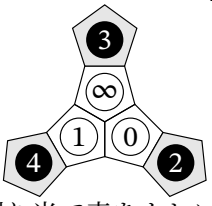
6 MOG の一意的な表記法

冒頭で述べた通り，線形符号を扱う上で，各符号語の重みに関する情報を符号の基底から得ることは多くの場合困難である。本節ではそうした困難を g_{24} について解消することを目的としている。

ここでは，まず，R. T. Curtis の歴史的な結果 [4] を紹介する。その上で，符号語の重みに関する情報を取り出しやすい MOG の表記法と，そこから得られる基底について解説する。ここで示している表記法の応用として，[24, 12, 8] extended Golay code g_{24} の符号語を重みごとに数え上げることができることを紹介する。

なお，同様の数え上げは [4] にも紹介されているが，そこでは MOG の表記法が一意でないため，重複した部分をそのまま数え上げ，最後に重複度で割ることで重みごとの符号語の個数が得られている。本節では各 MOG について，一意な表記法を与えている点が [4] と異なる。加えて，g_{24} には hexacode の構造が内在することが [4] で示されているが，本節では hexacode の基底と直接対応する形で g_{24} の基底を与えている。

[4] の結果を紹介するにあたり，4×6 array の枠にいくつか $*$ を書き入れたものについて，$\boxed{*}$を 1，$\boxed{\ }$に 0 に対応させることで，$\mathbb{F}_2^{24}$ の元と同一視することは先に述べた通りとする。

ここで，$h_0 :=$ 

$= \varphi^{-1}((0,0,0,0,0,0)) \in H$ と定める。

まず，ラベル割り当て表をもとに，与えられた hexad のラベルに対応する 4×6 array の枠に $*$ を書き入れることで，

$$\theta_1 : H \to \mathbb{F}_2^{24}$$

を定義する。

次に，$v \in \mathbb{F}_2^6$ の対して，$\mathrm{supp}(v) := \{j \in \{\infty, 3, 0, 2, 1, 4\} \mid v_j \neq 0\}$ とする。このとき，$j \in \mathrm{supp}(v)$

ならば，4×6 array の j で添え字付けられた列の 4 つの枠すべてに $*$ を書き入れ，$j\notin \mathrm{supp}(v)$ ならば，j で添え字付けられた列には何も書き入れないこととで

$$\theta_2 : \mathbb{F}_2^6 \to \mathbb{F}_2^{24}$$

を定義する。

ここで，$S := \{\theta_1(h) \mid h\in H\}\cup\{\theta_2(\mathrm{supp}^{-1}\{k\}) \mid k\in\{\infty,3,0,2,1,4\}\}$ とし，S で生成される $\mathbb{F}_2^{24}$ の部分空間を $\langle S\rangle$，S の偶数個の一次結合全体を $\langle S\rangle^{\mathrm{e}}$ と表記する。このとき，次の定理が知られている。

定理 4 (Curtis, 1990 [4]). S について，次が成立する。

(i) $\dim\langle S\rangle = 13$
(ii) $\dim\langle S\rangle^{\mathrm{e}} = 12$
(iii) $\langle S\rangle^{\mathrm{e}} = \{\mathrm{MOG}\} = g_{24}$

また，$\ell\in\left\{\textcircled{0},\blacksquare 0,\textcircled{1},\blacksquare 1,\textcircled{2},\blacksquare 2,\textcircled{3},\blacksquare 3,\textcircled{4},\blacksquare 4,\textcircled{\infty},\blacksquare\infty\right\}$ に対して，ℓ を中心に配置する bull's eye を $b(\ell)\in B$ と表記し，$r(\ell,k) := \theta_1(b(\ell)) + \theta_2(\mathrm{supp}^{-1}(\{k\}))$ とする。このとき，次が成立する。

定理 5 (Curtis, 1990 [4]). 集合

$$\left\{r(\ell,k) \mid \ell\in\left\{\textcircled{k},\blacksquare k\right\},\quad k\in\{\infty,3,0,2,1,4\}\right\}$$

は $\langle S\rangle^{\mathrm{e}}$ の基底をなす。

この定理は次のように言い換えることができる。

系 1 (Curtis, 1990 [4]). A を正二十面体グラフの隣接行列, I を 12 次の単位行列, J をすべての成分を 1 とする 12 次の正方行列とする。

このとき，$(I|J-A)\in\mathbb{F}_2^{12\times 24}$ は g_{24} の生成行列となる。

実際，定理 5 で得られた基底 $\left\{r(\ell,k) \mid \ell\in\left\{\textcircled{k},\blacksquare k\right\},\quad k\in\{\infty,3,0,2,1,4\}\right\}$ を行列の形に書き換えると次のようになる。これは，系 5 を示していることに他ならない。

	∞	3	0	2	1	4	⊛	③	⓪	②	①	④	∞	3	0	2	1	4	⊛	③	⓪	②	①	④
$r(\textcircled{\infty},\infty)$	*												*			*		*	*	*	*		*	
$r(\textcircled{3},3)$		*												*	*	*	*	*	*	*				
$r(\textcircled{0},0)$			*											*	*			*	*		*	*	*	
$r(\textcircled{2},2)$				*									*	*		*	*	*			*	*		
$r(\textcircled{1},1)$					*									*		*	*		*		*		*	*
$r(\textcircled{4},4)$						*							*	*	*	*		*					*	*
$r(\blacksquare\infty,\infty)$							*						*	*	*		*		*			*		*
$r(\blacksquare 3,3)$								*					*	*						*	*	*	*	*
$r(\blacksquare 0,0)$									*				*		*	*	*			*	*			*
$r(\blacksquare 2,2)$										*					*	*			*	*		*	*	*
$r(\blacksquare 1,1)$											*		*		*		*	*		*		*	*	
$r(\blacksquare 4,4)$												*					*	*	*	*	*	*		*

次に $v\in\mathbb{F}_2^6$ の Hamming 重み $\mathrm{wt}(v)$ について，

$$\theta : \mathbb{F}_4^3\times\mathbb{F}_2^6 \to \mathbb{F}_2^{24}$$

を次のように定義する。

$$\theta((u,v)) := \begin{cases} \theta_1(\varphi^{-1}(\tau(u))) + \theta_2(\pi(\tau(u)) + v) & \text{if } \mathrm{wt}(\pi(\tau(u)) + v) \equiv 1 \pmod 2 \\ \theta_1(\varphi^{-1}(\tau(u))) + \theta_2(\pi(\tau(u)) + v) + \theta_1(h_0) & \text{if } \mathrm{wt}(\pi(\tau(u)) + v) \equiv 0 \pmod 2 \end{cases}$$

ただし,

$$\begin{array}{ccccc} \tau: & \mathbb{F}_4^3 & \longrightarrow & H_6 & \\ & \cup & & \cup & \\ & (u_1,u_2,u_3) & \mapsto & (u_1,u_2,u_3)\begin{pmatrix} 1 & 0 & 0 & 1 & \omega^2 & \omega \\ 0 & 1 & 0 & 1 & \omega & \omega^2 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} & \\ \pi: & \mathbb{F}_4^6 & \longrightarrow & \mathbb{F}_2^6 & \\ & \cup & & \cup & \\ & (u_1,\dots,u_6) & \longmapsto & (\delta_{u_1,\omega},\dots,\delta_{u_6,\omega}) & \end{array}$$

とし，φ は前節で定義したものとする。

次が容易に確かめられる。

定理 6. 写像

$$\theta : \mathbb{F}_4^3 \times \mathbb{F}_2^6 \to g_{24}$$

は $\mathbb{F}_2$ 線形な全単射写像となる。

例 4. $u = (1, \omega, 0)$ とする。$\tau(u) = (1, \omega, 0, \omega^2, 0, \omega^2)$ となる。

$\theta_1(\varphi^{-1}(\tau(u))) =$

	∞	3	0	2	1	4
0			*		*	
1	*					
ω		*				
ω^2				*		*

$(\ 1,\ \omega,\ 0,\ \omega^2,\ 0,\ \omega^2\ ) \in \mathbb{F}_4^6$

$\pi(\tau(u)) = (0,1,0,0,0,0)$ となるので,

$\theta(u,0) = \theta_1(\varphi^{-1}(\tau(u))) + \theta_2((0,1,0,0,0,0)) =$

	*	*		*	
*	*				
	*		*		*

同様に，$u' := (1,0,0)$, $u'' := (0,\omega,0) \in \mathbb{F}_4^3$ とすると,

$\theta(u',0) = \theta_1(\varphi^{-1}(\tau(u') + \theta_2((0,0,0,0,0,1)) =$

	*	*			*
*			*		*
				*	*

$\theta(u'',0) = \theta_1(\varphi^{-1}(\tau(u''))) + \theta_2((0,1,0,1,0,0)) + \theta_1(h_0) =$

				*	*
	*		*		*
	*		*	*	

$\theta(u,0)=\theta(u'+u'',0)=\theta(u',0)+\theta(u'',0)$ となっていることが確認できる。

定理 6 は g_{24} の元が hexad と $\mathbb{F}_2^6$ の元の組で記述できることを示していることに加えて，hexad に由来する g_{24} の基底を容易に構成できることを示している。さらに，一般の基底とは異なり，この表記では各元の重みがただちに求めることができる。その性質を応用して，以下で重みごとに g_{24} の元を数えあげることができることを示す。

まず，$c=\theta(u,\pi(\tau(u))+v)$ として $u\in\mathbb{F}_4^3$ と $v\in\mathbb{F}_2^6$ に関する場合分けのもとで数え上げる。

(i) $\mathrm{wt}(v)\equiv 1 \pmod 2$ となる場合，

$\mathrm{wt}(c)$	# of c	$\mathrm{wt}(v)$
8	$384=64\times 6$	1
12	$1280=64\times\binom{6}{3}$	3
16	$384=64\times 6$	5

(ii) $\mathrm{wt}(v)\equiv 0 \pmod 2$，　$u=0$ となる場合，

$\mathrm{wt}(c)$	# of c	$\mathrm{wt}(v)$
0	1	0
8	$15=\binom{6}{2}$	2
16	$15=\binom{6}{4}$	4
24	1	6

(iii) $\mathrm{wt}(v)\equiv 0 \pmod 2$，　$\varphi^{-1}(\tau(u))\in N(h_0)\setminus\{h_0\}$ となる場合，ただし，$N(h_0)$ は第 4 節で定義したグラフ G の h_0 近傍を表す。

$\mathrm{wt}(c)$	# of c
12	$576=18\times 2^5$

(iv) $\mathrm{wt}(v)\equiv 0 \pmod 2$，　$\varphi^{-1}(\tau(u))\in H\setminus N(h_0)$ となる場合，

$\mathrm{wt}(c)$	# of c	$\mathrm{wt}(\pi(\tau(u)+(1,\dots,1))*v)$
8	$360=45\times 2^3$	0
12	$720=45\times 2^4$	1
16	$360=45\times 2^3$	2

ただし，$(a_1,a_2,\dots,a_6),(b_1,b_2,\dots,b_6)\in\mathbb{F}_2^6$ について，

$$(a_1,a_2,\dots,a_6)*(b_1,b_2,\dots,b_6)=(a_1b_1,a_2b_2,\dots,a_6b_6)$$

とする。

このように，重みの情報を失わない一意表記法を用いることで，g_{24} の重み分布はよく知られている通り，次のようになることが容易に決定することができる。

$\mathrm{wt}(c)$	0	4	8	12	16	20	24
# of c	1	0	759	2576	759	0	1

参考文献

[1] R. T. Curtis, Error-correction and the binary Golay code, London Mathematical Society Impact 150 Stories 1 (2016) 51–58.

[2] J. H. Conway and N. J. A. Sloane, “Sphere Packings, Lattices and Groups”, Grundlehren der Mathematischen Wissenschaften, vol. 290 (Berlin: Sringer, 1988)

[3] R. T. Curtis, A new combinatorial approach to M24, Math. Proc. Cambridge Phil. Soc., 79 (1976), 25–42.

[4] R. T. Curtis, The regular dodecahedron and the binary Golay code, Ars Combinatoria 29B (1990), 55–64.

形式概念分析：乱択形式文脈と漸近下界

千葉大学・大学院理学研究院　櫻井　太朗 *
Taro Sakurai
Graduate School of Science,
Chiba University

1　はじめに

形式概念分析（Formal Concept Analysis, FCA）は束論の応用分野のひとつである．R. Wille [10] によって 1980 年代に創始された分野で，定性的なデータの解析と視覚化や知識処理の支援に用いられている．この分野における基本文献は Ganter–Wille による [3] である．逆にこれを引用している文献を調べれば形式概念分析に関する資料はほぼ網羅されるだろう．

日本では 2007 年 4 月に日本知能情報ファジィ学会誌による形式概念の特集があった．解説 [9] はおそらく日本語で読める唯一のまとまった概説である．最近ではクラフトビールのホップに関する応用事例などもあり，色々なメディアで取り上げられている [1, 4].

形式概念分析の基本的な用語すら知られているとは言えないので，まずは基本的な定義を述べるところからはじめる．

2　形式概念分析

定義 2.1. 集合 G, M と部分集合 $I \subseteq G \times M$ が与えられたとき組 $K = (G, M, I)$ を**形式文脈**（formaler Kontext）とよぶ．形式文脈 $K = (G, M, I)$ に関して G の元を**対象**（Gegenstände），M の元を**属性**（Merkmale）とよぶ．対象 g と属性 m に関して (g, m) が I に属するとき対象 g は属性 m を**もつ**という．

Wille による最初の論文にあった「惑星[†]」の形式文脈が具体例として挙げられることが多い（表 1）．また形式文脈は二部グラフとも思える（図 1）．

定義 2.2. 形式文脈 $K = (G, M, I)$ と対象の集合 $A \subseteq G$，属性の集合 $B \subseteq M$ が与えられたとす

* https://orcid.org/0000-0003-0608-1852
† 論文が出版されたのは 1982 年なので太陽系には冥王星を含む 9 つの「惑星」がある．

	半径			太陽		衛星	
	小	中	大	近	遠	有	無
☿ 水星	×			×			×
♀ 金星	×			×			×
♁ 地球	×			×		×	
♂ 火星	×			×		×	
♃ 木星			×		×	×	
♄ 土星			×		×	×	
♅ 天王星		×			×	×	
♆ 海王星		×			×	×	
♇ 冥王星	×				×	×	

表 1　「惑星」の形式文脈

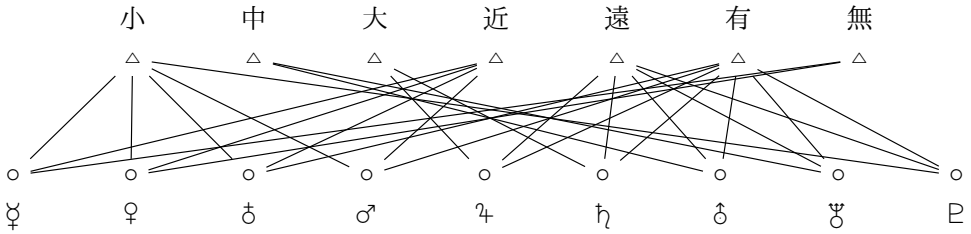


図 1　形式文脈の二部グラフによる表現

る．A に属するすべての対象が共通にもつ属性の集合を

$$A' = \bigcap_{g \in A} \{\, m \in M \mid (g, m) \in I \,\}$$

と表す．双対的に B に属するすべての属性をもつ対象の集合を

$$B' = \bigcap_{m \in B} \{\, g \in G \mid (g, m) \in I \,\}$$

と表す．条件 $A' = B$ と $B' = A$ が成立するとき組 (A, B) を形式文脈 K の**形式概念**（formaler Begriff）とよぶ．また形式概念 (A, B) に関して A を**外延**，B を**内包**とよぶ．形式文脈 K の形式概念全体を $\mathfrak{B}(K)$ と表す．

定義 2.3. 形式文脈 K の形式概念 (A, B) と (C, D) が与えられたとする．条件 $C \subseteq A$ が成立するとき (A, B) は (C, D) の**上位概念**である，あるいは (C, D) は (A, B) の**下位概念**であるとよび $(C, D) \leq (A, B)$ と書く．これは $D \supseteq B$ とも同値である．二項関係 $\leq$ によって形式概念全体 $\mathfrak{B}(K)$ は束になる．これを**形式概念束**とよぶ．

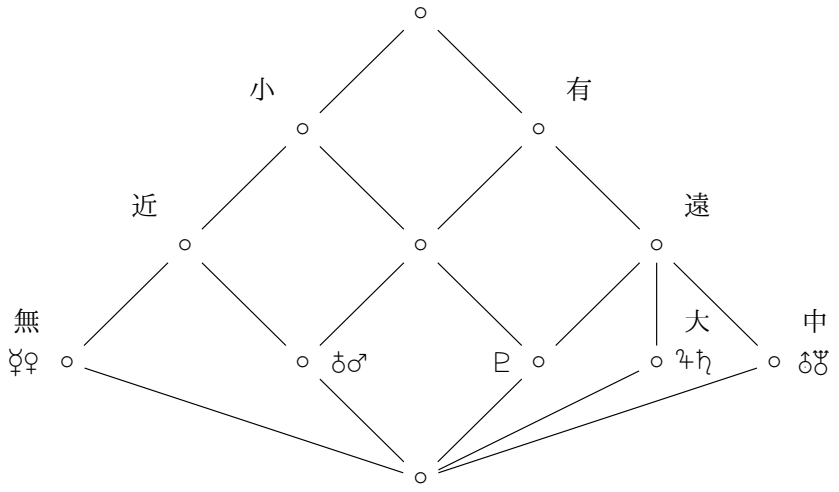


図 2　「惑星」の形式概念束

先程の「惑星」の形式文脈における形式概念束のハッセ図を描くと図 2 のようになる．この図では形式概念の階層を示すだけではなくて対象や属性によるラベルづけがされている．ここで対象 g によるラベルづけがされているのは $(\{g\}'', \{g\}')$ の形をした対象 g の現れる最小の形式概念であり，属性 m によるラベルづけがされているのは $(\{m\}', \{m\}'')$ の形をした属性 m の現れる最大の形式概念である．たとえば図 2 の一番左にある点は形式概念 $(\{\☿, \♀\}, \{\text{無}, \text{近}, \text{小}\})$ に対応する．図からただちに衛星が無いならば太陽に近いことや，太陽に近いならば半径の小さいことなどを読み取ることができる．逆にこのような図からもとの形式文脈を完全に復元することもできる．

3　乱択形式文脈

定性的なデータを解析するとき，小規模なものに限れば，形式概念束による視覚化は有用な手段である．データが大規模になるにつれて形式概念の数が急激に増え，視覚的に階層構造を捉えるのが難しくなる．理論的には与えられた形式文脈が形式概念をいくつもつのかを決定する問題が#P 完全であることも知られている [6].

具体例を挙げるために $U = \{1, 2, \ldots, n\}$ とおく．たとえば形式文脈 $K^c = (U, U, \neq)$ を考えると形式概念は

$$\mathfrak{B}(K^c) = \{\, (A, B) \mid A + B = U \,\}$$

なので $|\mathfrak{B}(K^c)| = 2^n$ 個である．したがって指数関数的に増加する可能性があるとわかる．ところが形式文脈 $K^f = (U, U, U \times U)$ を考えると形式概念は

$$\mathfrak{B}(K^f) = \{(U, U)\}$$

なので $|\mathfrak{B}(K^f)| = 1$ 個である．つまり定数関数となる可能性もあるとわかる．それでは〈平均的〉に形式概念はいくつあるだろうか？この問題に答えるためにはまず適当な確率模型を設定する必要

がある．

定義 3.1 (Sakurai [7])．自然数 n と実数 $p, q \in [0,1]$ をとる．$U = \{1, 2, \ldots, n\}$ とおく．このとき $G + M = U$ となる形式文脈 (G, M, I) 全体からなる集合を Ω とおく．ここで $G + M$ は集合の直和である．冪集合 2^Ω 上に確率測度 $P = \kappa_{n,p,q}$ を

$$P\{(G, M, I)\} = p^{|G|}(1-p)^{|M|}\, q^{|I|}(1-q)^{|G\times M - I|}$$

により定めると $(\Omega, 2^\Omega, P)$ は確率空間である．

定義 3.2 (Sakurai [7])．Ω に値をもつ確率変数 $\boldsymbol{K}$ の分布が $\kappa_{n,p,q}$ であるとき $\boldsymbol{K}$ を**乱択形式文脈**とよび $\boldsymbol{K} \sim \kappa_{n,p,q}$ と書く．

ここで採用したのとは少し異なる定義が [2, 5] ではなされ研究されている．定義から期待値の明示式を導くのはやさしい．

命題 3.3 (Sakurai [7])．乱択形式文脈 $\boldsymbol{K} \sim \kappa_{n,p,q}$ に対して

$$E(|\mathfrak{B}(\boldsymbol{K})|) = \sum_{(a,b,c,d)} \binom{n}{a\ b\ c\ d} p^{a+c}(1-p)^{b+d}\, q^{ab}(1-q^a)^d(1-q^b)^c$$

が成立する．ただし和は $a + b + c + d = n$ となるすべての非負整数の組をわたる．

4　漸近下界

乱択形式文脈がもつ形式概念の期待値は明示式が与えられた．ただしこの等式は期待値の大きさに関する情報を陽に示していないという意味で役に立たない命題である．これに対して次の不等式は期待値の大きさに関する情報を陽に示しているという意味で役に立つ定理である．

定理 4.1 (Sakurai [7])．実数 $p, q, \varepsilon \in (0,1)$ をとる．乱択形式文脈列 $(\boldsymbol{K}_n)$ が $\boldsymbol{K}_n \sim \kappa_{n,p,q}$ を満たすならば

$$E(|\mathfrak{B}(\boldsymbol{K}_n)|) > n^{-\frac{1-\varepsilon}{\log q}} \log n$$

が有限個の n を除いて成立する．

したがって定確率 p, q のもとで乱択形式文脈のもつ形式概念の数を考えると，期待値の漸近下界は任意の多項式より大きいことがわかる．

5　おわりに

代数的組合せ論シンポジウムでの発表をきっかけにして琉球大学の徳重典英氏と共同研究を後日はじめました．ランダム・グラフがもつクリークの数に関する研究をして，期待値の漸近表示を得

ることなどができました [8]．最後になりますが，このような機会をいただいた世話人の先生方に感謝の意を表します．

参考文献

[1] ‘理想のホップ、数学から導く’, 朝日新聞（ちば首都圏）朝刊, 2022 年 2 月 5 日.

[2] R. Emilion, G. Lévy, ‘Size of random Galois lattices and number of closed frequent itemsets’, *Discrete Appl. Math.* 157 (2009) 2945–2957, doi:10.1016/j.dam.2009.02.025, MR 2537496, Zbl 1187.68389.

[3] B. Ganter, R. Wille, *Formal concept analysis* (Springer, Berlin, 1999) MR 1707295, Zbl 0909.06001.

[4] 萩原学, ‘数学応用のクラフトビール’, 数学セミナー 9 月号 (2022) 50–55.

[5] L. Kovács, ‘Efficient approximation for counting of formal concepts generated from formal context’, *Miskolc Math. Notes* 19 (2018) 983–996, doi:10.18514/MMN.2018.2529, MR 3915517, Zbl 1425.68400.

[6] S. O. Kuznetsov, ‘On computing the size of a lattice and related decision problems’, *Order* 18 (2001) 313–321, doi:10.1023/A:1013970520933, MR 1884424, Zbl 0991.06006.

[7] T. Sakurai, ‘On formal concepts of random formal contexts’, *Infom. Sci.* 578 (2021) 615–620, doi:10.1016/j.ins.2021.07.065, MR 4293021.

[8] T. Sakurai, N. Tokushige, ‘Counting cliques in a random graph’, Preprint, 2022, arXiv:2208.07492.

[9] 鈴木治, 室伏俊明, ‘形式概念分析：入門・支援ソフト・応用’, 知能と情報 19 (2007) 103–142. doi:10.3156/jsoft.19.2_103.

[10] R. Wille, ‘Restructuring lattice theory: An approach based on hierarchies of concepts’, *Ordered sets*, Proceedings of the NATO Advanced Study Institute held at Banff, Canada, August 28 to September 12, 1981 (ed. I. Rival; Reidel, Dordrecht, 1982) 445–470, doi:10.1007/978-94-009-7798-3_15, MR 661303, Zbl 0491.06008.

A construction of non-schurian Schur rings over elementary abelian groups of even rank

花木章秀 (信州大学理学部)

第 38 回代数的組合せ論シンポジウム 2022.06.16

1 はじめに

有限可移置換群によって定義されるアソシエーションスキームをシュアー的であるという。いきなりではあるが、一つの予想から始める。

予想 1.1. ほとんどすべてのアソシエーションスキームは非シュアー的である。

知られている多くの例はシュアー的であり、この予想に根拠はないが、考える集合の要素の数が大きくなればシュアー的であるものは極めて珍しいのであろう、と思っている。知られている一番極端な例は、位数 31 の場合で、同型類 98307 個のうちシュアー的であるものは 8 個だけである [3]。

シュアー環は有限群の分割から得られる環で、Wielandt [5] に詳しく書いてあるので知っている人も多いであろう ([5] には S-ring と書いてある)。正則な部分群をもつ有限可移置換群はシュアー環を定め、このようにして得られるシュアー環をシュアー的であるという。シュアー環からは自然にアソシエーションスキームが得られる。このときシュアー環がシュアー的であることと、それから得られるアソシエーションスキームがシュアー的であることは同値である。そこで、非シュアー的なシュアー環を構成することによって非シュアー的なアソシエーションスキームを構成することを考える。これまでには

- Wielandt [5] : 位数 p^2 の基本アーベル群上のランク 5 の非シュアー的シュアー環
- Evdokimov-Ponomarenko [1] : 巡回群上の非シュアー的シュアー環
- Ponomarenko-Vasil'ev [4] : その上の全てのシュアー環がシュアー的であるような有限群

などの結果が知られている。ここでは Wielandt の結果を一般化し、偶数ランクの基本アーベル p-群上にたくさんの非シュアー的シュアー環を構成する。その同型類の個数は膨大であり、有限群の位数の指数関数となる。

今回の結果は平井拓人の 2021 年度信州大学修士論文の内容を一般化したものであり、公表済みの論文 Hanaki-Hirai-Ponomarenko [2] に基づくものである。

2 シュアー環

H を有限群とする。$U \subset H$ に対して、群環の中での和を考え、$\underline{U} = \sum_{u \in U} u \in \mathbb{Z}H$ とおく。

$$P = \{H_0, \ldots, H_r\}$$

を H の分割 ($H = H_0 \cup \cdots \cup H_r$, $H_i \neq \emptyset$, $i \neq j$ に対して $H_i \cap H_j = \emptyset$) とする。分割 P に対して

$$\mathcal{S}(P) := \bigoplus_{i=0}^{r} \mathbb{Z}\underline{H_i} \subset \mathbb{Z}H$$

とおく。$\mathcal{S}(P)$ が H 上の**シュアー環** (Schur ring, S-ring) であるとは、次の条件を満たすこととする。

(1) $H_0 = \{1_H\}$ である。

(2) すべての $i \in \{0, \ldots, r\}$ に対して、ある $i' \in \{0, \ldots, r\}$ が存在して $\{h^{-1} \mid h \in H_i\} = H_{i'}$ となる。

(3) $\mathcal{S}(P)$ は $\mathbb{Z}H$ の部分環である。

H 上のシュアー環が与えられたとき、H の正則置換表現による表現行列の和を考えれば、それがアソシエーションスキームを定めることは簡単に分かる。このようにしてシュアー環はアソシエーションスキームの特別なものと考えることができる。

例 2.1. 以下の分割は H 上のシュアー環を定める。

(1) $H = \{1_H\} \cup (H \setminus \{1_H\})$

(2) $H = \bigcup_{h \in H} \{h\}$

(3) H の共役類への分割

(4) $G \leq \mathrm{Aut}(H)$ とするとき、H の G-軌道への分割

G を正則部分群 H をもつ有限置換群とする。このとき G は H に作用すると見ることができる。G_1 を $1_H \in H$ の安定部分群とし、H 上の G_1-軌道で H の分割を定めれば、これはシュアー環を定める。この様にして得られるシュアー環を**シュアー的** (schurian) という。上の例は全てシュアー的である。

シュアー環からアソシエーションスキームを定義するとき、シュアー環がシュアー的であることと得られるアソシエーションスキームがシュアー的であることは同値である。

3 構成

p を素数、 $n \in \mathbb{N}$, $q = p^n$ とする。$\mathbb{F}_q$ で q-元体を表すものとする。2 次元 $\mathbb{F}_q$-ベクトル空間 $V = \mathbb{F}_q^2$ の原点を通る直線の集合

$$\mathcal{L} := \{L_\alpha \mid \alpha \in \mathbb{F}_q \cup \{\infty\}\}$$

を考える。ただし

$$\begin{aligned} L_\alpha &:= \{(x, \alpha x) \mid x \in \mathbb{F}_q\} \quad (\alpha \in \mathbb{F}_q) \\ L_\infty &:= \{(0, x) \mid x \in \mathbb{F}_q\} \end{aligned}$$

である。$L_\alpha^\sharp := L_\alpha \setminus \{(0,0)\}$ とおく。

2 次元ベクトル空間の異なる 2 直線は全体を張ることから次の命題が得られる。2 次元でないとうまく行かない理由の一つがこれである。

命題 3.1. 分割 $\{\{(0,0)\}\} \cup \{L_\alpha^\sharp \mid \alpha \in \mathbb{F}_q \cup \{\infty\}\}$ は V (位数 p^{2n} の基本アーベル p-群) 上の amorphic なシュアー環を定める。(任意の融合がまたシュアー環になる。)

これによって $\mathcal{L}$ の分割ごとにシュアー環が得られ、たくさんのシュアー環が得られる。この中で非シュアー的になるものを考察するのが本研究の主題である。

4 主結果

命題 3.1 で得られるシュアー環がシュアー的になるための必要条件を考え、そうでないときには非シュアー的である、という方針で主結果を述べる。そのために少し準備が必要である。

$\Pi := \{P_1, \ldots, P_r\}$ を $\mathcal{L}$ の分割とする。各 P_i に対して $\widetilde{P}_i = \bigcup_{L_\alpha \in P_i} L_\alpha^\sharp$ とおく。このとき V の分割

$$\widetilde{\Pi} := \{\{(0,0)\}, \widetilde{P}_1, \ldots, \widetilde{P}_r\}$$

が得られる。これによって与えられるシュアー環を $\mathcal{S}(\Pi)$ と表すことにする。また

$$\mathcal{M}(\Pi) := \{\alpha \in \mathbb{F} \cup \{\infty\} \mid \{L_\alpha\} \in \Pi\}$$

とおく。

定理 4.1. $\{0, 1, \infty\} \subset \mathcal{M}(\Pi)$ とする。また $\mathcal{M}(\Pi) \setminus \{\infty\}$ は $\mathbb{F}_q$ の部分体ではないとする。このときシュアー環 $\mathcal{S}(\Pi)$ はシュアー的ではない。

この定理で $\{0, 1, \infty\} \subset \mathcal{M}(\Pi)$ という仮定は本質的ではない。$\mathcal{M}(\Pi)$ は L_α を決める座標のとり方に依存する。$|\mathcal{M}(\Pi)| \geq 3$ であれば、適当な座標変換で $\{0, 1, \infty\} \subset \mathcal{M}(\Pi)$ とすることができる。また $\{0, 1, \infty\} \subset \mathcal{M}(\Pi)$ という仮定の下で、$\mathcal{M}(\Pi) \setminus \{\infty\}$ が部分体であるという性質は座標変換で保存される。(ある座標で部分体にならないものが別の座標で部分体になることはない。)

以下に証明の方針を説明する。$\{0, 1, \infty\} \subset \mathcal{M}(\Pi)$ を満たす $\mathcal{S}(\Pi)$ がシュアー的であるとし、$\mathcal{M}(\Pi) \setminus \{\infty\}$ が部分体となることを示せばよい。

(1) $\{0, 1, \infty\} \subset \mathcal{M}(\Pi)$ とする。$H \cong V$ を正則部分群にもつ置換群 G が存在したとする。

(2) $H \lhd G$ である。したがって $G_1 \leq \mathrm{Aut}(H) \cong \mathrm{GL}(2n, p)$ と思うことができる。

(3) $\alpha, \beta \in \mathcal{M}(\Pi) \setminus \{\infty\}$ ならば $\alpha + \beta, \alpha\beta \in \mathcal{M}(\Pi)$ である。したがって $\mathcal{M}(\Pi) \setminus \{\infty\}$ は $\mathbb{F}_q$ の部分体となる。

証明は [2] を参照してほしい。(2) は本質的に Wielandt [5] にある内容である。したがって、証明が必要なのは (3) のみであり、これもほぼ基本的な線形代数で説明される。

5　残された問題

本講演の結果では、命題 3.1 で得られるシュアー環について、そのすべてに対してシュアー的であるかどうかを決定できたわけではない。小さな例を調べたところ、定理が適用できない場合 ($\mathcal{M}(\Pi) \setminus \{\infty\}$ が部分体である場合、$|\mathcal{M}(\Pi)| \leq 2$ の場合)、シュアー的、非シュアー的のいずれの例も得られるようである。

また、この結果で得られるのはランクが偶数の基本アーベル群上のシュアー環だけなので、奇数ランクの場合の非シュアー的シュアー環の自明でない構成法も考えてみたい。

References

[1] S. Evdokimov and I. Ponomarenko, *On a family of Schur rings over a finite cyclic group*, Algebra i Analiz **13** (2001), no. 3, 139–154.

[2] A. Hanaki, T. Hirai, and I. Ponomarenko, *On a Huge Family of Non-Schurian Schur Rings*, Electron. J. Combin. **29** (2022), no. 2, Paper No. 2.14–.

[3] A. Hanaki, H. Kharaghani, A. Mohammadian, and B. Tayfeh-Rezaie, *Classification of skew - Hadamard matrices of order 32 and association schemes of order 31*, J. Combin. Des. **28** (2020), no. 6, 421–427.

[4] I. Ponomarenko and A. Vasil'ev, *On non-abelian Schur groups*, J. Algebra Appl. **13** (2014), no. 8, 1450055, 22.

[5] H. Wielandt, *Finite permutation groups*, Translated from the German by R. Bercov, Academic Press, New York, 1964.

有限距離空間の等長列による特徴づけ

平坂貢（釜山国立大学）, 篠原雅史（滋賀大学）

令和 4 年 6 月 16 − 18 日

概 要

(X,d) を $|X|=n$ となる有限距離空間とする．正の整数 k に対して $A_k(X)$ を X の k 点部分集合全体を合同関係で割った商集合であると定義する．$|A_k(X)|$ を a_k と記す．$(a_1,a_2,\ldots,a_n)$ は (X,d) の等長列と呼ばれる．本講演では次のどれかの仮定のもとで (X,d) を特徴づけることを目標とする: (i) $a_k=1$ かつ $2\leq k\leq n-2$; (ii) $a_k=2$ かつ $4\leq k\leq \frac{n-2}{2}$; (iii) $a_3=2$; (iv) $a_2=a_3=3$.

1 はじめに

私は数年前に ALS という病気を発症し, 気管切開手術後, 声を発せなくなりました．今回, 宗政昭弘先生から講演依頼をいただき, 更に「原稿の代読ならやります」とおっしゃっていただき, 恐れ多いと思いながらも, ご厚意に甘えることにしました．代読のみならず講演のスライドの内容を理解し手書きの図表を加え「生きた」講演を実現された宗政昭弘先生に最大限の感謝をお伝えします．

今回の講演内容は，滋賀大学の篠原さんとの共同研究によるもので, 2016 年にアーカイブにアップロードした論文（https://arxiv.org/abs/1802.06097）に基づいています．改めてその論文を読み返してみて, ある定理の仮定を弱める事ができることに気づいたので, そのことを報告します．

距離集合の研究において ([2] , [1] を参照) ユークリッド空間の有限部分集合をその起こり得る距離の個数によって特徴づけることが主要課題とされる．本研究では「距離だけでなく起こり得る三角形の合同類の個数に注目しよう」という方針のもとで, 等長列という概念を導入してより一般的な対象である有限距離空間を特徴づけることを目的としている．

(X,d) を距離空間とする, ただし $d : X \times X \to \mathbb{R}_{\geq 0}$ は距離関数である. 部分集合 $A, B \subseteq X$ に対して以下の条件を満たす時 A は B と合同 であるという：全単射 $f : A \to B$ が存在して, すべての $x, y \in A$ に対して $d(x,y) = d(f(x), f(y))$ が成り立つ.

正の整数 k に対して X の k 点部分集合全体からなる集合族を $\binom{X}{k}$ と記す. すなわち,

$$\binom{X}{k} = \{Y \subseteq X \mid |Y| = k\},$$

そして $A_k(X)$ を $\binom{X}{k}$ の距離関数 d によって誘導される合同類による $\binom{X}{k}$ 上の商集合として定義する. すなわち,

$$A_k(X) = \left\{ [Y] \mid Y \in \binom{X}{k} \right\}$$

ただし $[Y] = \left\{ Z \in \binom{X}{k} \mid Y \text{ は } Z \text{ と合同である} \right\}$.

X が有限集合であるとき, (X,d) の等長列 を以下のように定義する：

$$(a_1, a_2, \ldots, a_n)$$

ただし $a_i = |A_i(X)|$ そして $|X| = n$. 明らかに $a_1 = a_n = 1$ であり, $a_2 = 1$ ならばすべての項が 1 となる. 以下はユークリッド空間内の有限集合の等長列の例である：

(i) 正方形の 4 頂点： $(1, 2, 1, 1)$;

(ii) 正五角形の 5 頂点：$(1, 2, 2, 1, 1)$;

(iii) 正八面体の 6 頂点：$(1, 2, 2, 2, 1, 1)$;

$x, y, z, w \in X$ に対して以下が成り立つ：

$$[\{x, y\}] = [\{z, w\}] \iff d(x,y) = d(z,w).$$

このようにして, $A_2(X)$ の元たちは以下の集合の元たちと同一視される：

$$\{d(x,y) \mid x, y \in X, x \neq y\}.$$

連結グラフはグラフ上の距離を距離関数とする距離空間である. 以下は有限連結グラフの等長列の例である：

(i) 完全グラフ K_n: $(1, 1, \ldots, 1)$;

(ii) 完全二部グラフ $K_{3,3}$: $(1,2,2,2,1,1)$;

(iii) サイクル C_6: $(1,3,3,3,1,1)$.

等長列を生成するには以下の $\binom{X}{2}$ の分割が必要になる：$\{E_\alpha\}_{\alpha\in A_2(X)}$ ただし

$$E_\alpha = \{\{x,y\} \mid d(x,y) = \alpha\}$$

一方で $\alpha \in A_2(X)$ の値は必要ない. 実際, $\binom{X}{2}$ の離散分割の等長列は以下の通りである：$(1, \binom{n}{2}, \binom{n}{3}, \ldots, \binom{n}{n-1}, 1)$.

ここで $(1,2,1,1)$ という等長列を持つ距離空間を考える. $\binom{X}{2}$ は E_α と E_β に分割され, (X, E_α) は長さ 4 のサイクル, (X, E_β) はその補集合であることがわかる. 次にユークリッド空間への埋め込みを考える. [3] では Neumair がその方法を与えている：D を有限距離空間 (X,d) の距離行列とする. すなわち, D の各成分は $X \times X$ の元で指定され, その (x,y)-成分は $d(x,y)^2$. として定義される. 行列 G を次のように定義する.

$$G = -(I - 1/nJ)D(I - 1/nJ) \tag{1}$$

ただし I は単位行列で, J は成分が全て 1 の行列である. そのとき X が G の行として $\mathbb{R}^d$ に埋め込まれるための必要十分条件は G が半正定値であることである, ただし, $d = \mathrm{rank}(G)$. 例えば, 上記の分割の距離行列は X の元を適当に並べ替えて以下の行列となる：

$$\begin{pmatrix} 0 & a & b & b \\ a & 0 & b & b \\ b & b & 0 & a \\ b & b & a & 0 \end{pmatrix}$$

ただし $a, b \in \mathbb{R}_{>0}$ かつ $a \neq b$ である. G の特性多項式 $\det(tI - G)$ は以下のように計算される：

$$t(t-a)^2(t-2b+a).$$

G の行がユークリッド空間への埋め込みとなるための必要十分条件は $a \leq 2b$ であり, 等号が成立するとき, X は $\mathbb{R}^2$ に正方形の頂点として埋め込まれることがわかる.

投稿した論文では以下の等長列 $(a_1, a_2, \ldots, a_n)$ を持つ距離空間の特徴づけを行った：

(i) $a_k = 1$ かつ $2 \leq k \leq n-2$;

(ii) $a_k = 2$ かつ $4 \leq k \leq \frac{1+\sqrt{1+4n}}{2}$;

(iii) $a_3 = 2$;

(iv) $a_2 = a_3 = 3$.

本講演では (ii) における k の範囲を $4 \leq k \leq \frac{n-2}{2}$; 改善したことを報告する.

2 記号と準備

本節では (X, d) は等長列 $(a_1, a_2, \ldots, a_n)$ を持つ有限距離空間であると仮定する. 簡便のため $\{x_1, x_2, \ldots, x_k\} \in \binom{X}{k}$ に対して $[\{x_1, x_2, \ldots, x_k\}]$ を $x_1x_2\cdots x_k$ と記す. その結果, 任意の $\sigma \in S_k$ に対して

$$x_1x_2\cdots x_k = x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(k)}$$

である. ただし S_k は k 次対称群である. $x_1x_2\cdots x_k$ は距離行列 $(d(x_i, x_j)^2)_{1\leq i,j\leq k}$ から復元される. $(d(x_i, x_j)^2)_{1\leq i,j\leq k}$ は対角成分が 0 である対称行列なので, 次の同一視が可能である:

$$x_1x_2 \text{ と } d(x_1, x_2), \text{ そして, } x_1x_2x_3 \text{ と } (d(x_1, x_2), d(x_2, x_3), d(x_3, x_1)),$$

これを次のように記す：

$$\alpha\beta\gamma$$

ただし $\alpha = d(x_1, x_2)$, $\beta = d(x_2, x_3)$ そして $\gamma = d(x_3, x_1)$.

$\alpha \in A_2(X)$ に対して X 上の二項関係 R_α を

$$R_\alpha = \{(x, y) \in X \times X \mid d(x, y) = \alpha\}$$

のように定義する. その結果, $\{R_\alpha\}_{\alpha\in A_2(X)}$ は $\{(x, y) \in X \times X \mid x \neq y\}$ の分割となる. 次が成り立つ：

$$E_\alpha = \left\{\{x, y\} \in \binom{X}{2} \mid (x, y) \in R_\alpha\right\}$$

(X, E_α) は単純グラフであることに気付こう. X 上の二項関係 R と $x \in X$ に対して

$$R(x) = \{y \in X \mid (x, y) \in R\}$$

のように定義する. 有限距離空間 (X_1, d_1) に対して次が成り立つとき, (X, d) は (X_1, d_1) と同型であるという：次の条件を満たす 2 つの全単射 $f : X \to X_1$ と $g : A_2(X) \to A_2(X_1)$ が存在する：任意の $x, y \in X$ に対して

$$g(d(x, y)) \Leftrightarrow d_1(f(x), f(y)).$$

合同な有限距離空間は同型であるが, その逆は一般には成り立たない.

$S, T \subseteq X$ に対してベクトル $v(S, T)$ を次のように定義する：その成分は $A_2(X)$ の元でインデックスされ, 次に等しい：

$$v(S, T)_\alpha = |(S \times T) \cap R_\alpha|$$

ただし $x, y \in X$ に対して $v(\{x\}, T)$ と $v(S, \{y\})$ はそれぞれ $v(x, T)$ と $v(S, y)$ のように記される.

Lemma 2.1 任意の $S, T, U \subseteq X$ に対して次が成り立つ：

(i) $v(S, T) = v(T, S)$;

(ii) $S \cap T = \emptyset$ ならば $v(S \cup T, U) = v(S, U) + v(T, U)$;

(iii) S と T が合同ならば $v(S, S) = v(T, T)$;

(iv) $|\{v(S, S) \mid S \in \binom{X}{k}\}| \leq a_k$;

(v) 任意の $S \in \binom{X}{k-1}$ に対して $|\{v(x, S) \mid x \in X \setminus S\}| \leq a_k$.

（証明）R_α は対称なので, (i) が成り立つ.

$(S \cup T) \times U = (S \times U) \cup (T \times U)$ かつ $(S \times U) \cap (T \times U) = \emptyset$ なので,

$$[(S \cup T) \times U] \cap R_\alpha = [(S \times U) \cap R_\alpha] \cup [(T \times U) \cap R_\alpha],$$

それゆえ, (ii) が成り立つ.

(iii) は合同の定義から明らか.

(iii) の対偶により, (iv) が成り立つ.

(i),(ii) により,

$$v(\{x\} \cup S, \{x\} \cup S) = v(x, x) + v(x, S) + v(S, x) + v(S, S) = 2v(x, S) + v(S, S).$$

$\{v(\{x\} \cup S, \{x\} \cup S) \mid x \in X \setminus S\} \subseteq \{v(T, T) \mid T \in \binom{X}{k}\}$ なので, (iv) から (v) が成り立つ. □

Lemma 2.2 異なる $\alpha, \beta \in A_2(X)$ と $A, B \in \binom{X}{k}$ に対して, (X, E_α) の A による誘導部分グラフがスパニングスターを含み, (X, E_β) の B による誘導部分グラフがスパニングスターを含むならば, A と B は合同ではない.

(証明) (X, E_α) の B による誘導部分グラフには次数 $k-1$ の頂点が存在しないので, 両者間の等長写像は存在しない. □

正の整数 k に対して以下を定義する：
$M_k := \{\alpha \in A_2(X) \mid \exists x \in X; v(x, X)_\alpha \geq k\}$,
その結果, $M_k \subseteq M_{k-1}$ である.

Lemma 2.3 $S \in \binom{X}{k}$ と $\alpha \in A_2(X)$ に対して, $\{x \in S \mid v(x, S)_\alpha < k-1\}$ の任意の元を固定する S の置換は等長写像である.

(証明) 等長写像の定義を確認すればよい. □

3 主定理

本節では (X, d) は等長列 $(a_1, a_2, \ldots, a_n)$ を持つ有限距離空間であると仮定する.

Theorem 3.1 $a_k = 1$ かつ $2 \leq k \leq n-2$ ならば, $a_2 = 1$ である.

(証明) そうでないと仮定する. すなわち, $a_2 > 1$. そのとき $d(x, y) \neq d(y, z)$ となる互いに異なる $x, y, z \in X$ が存在する.

次が成り立つことを示す：任意の $w \in X \setminus \{x, z\}$ に対して $d(x, w) = \alpha$ かつ $d(w, z) = \beta$ ただし $\alpha := d(x, y)$ そして $\beta := d(y, z)$ である.

$w \in X \setminus \{x, y, z\}$ そして $S \in \binom{X \setminus \{x,y,z,w\}}{k-2}$ とする. 次のように定義する：

$$S_1 := S \cup \{x, y\}, S_2 := S \cup \{x, z\}, S_3 := S \cup \{x, w\}, S_4 := S \cup \{z, w\},$$

その結果, $a_k = 1$ と $|S_j| = k$ の条件から S_j たちは互いに合同となる. それゆえ, 補題 2.1 から $v(S_j, S_j)_\alpha$ の値が一致し, $u \in \{x, y, z, w\}$ に対して $r(u) := v(u, S)_\alpha$ とおくと次が成り立つ：

$$r(x)+r(y)+1 = r(y)+r(z) = r(x)+r(w)+v(x, w)_\alpha = r(z)+r(w)+v(z, w)_\alpha.$$

それゆえ,

$$r(x) + 1 = r(z), r(x) + v(x, w)_\alpha = r(z) + v(z, w)_\alpha,$$

さらに,

$$1 \leq v(z,w)_\alpha + 1 = v(x,w)_\alpha \leq 1.$$

このことは $\alpha = d(x,w)$ を意味し, 同様な議論により $\beta = d(z,w)$ を得る. w は任意に選ばれているので, 補題 2.2 から $\{x,y\} \cup S$ と $\{x,z\} \cup S$ は合同でないことが導かれる. このことは $a_k = 1$ に矛盾する. □

Theorem 3.2 $a_k = 2$ かつ $4 \leq k \leq \frac{n-1}{2}$, ならば, $a_2 = 2$ かつ次のどれかが成り立つ.

(i) $(X, E_\alpha) \simeq K_n \setminus K_2$ ただし $\alpha \in A_2(X)$;

(ii) $(X, E_\alpha) \simeq K_{1,n-1}$ ただし $\alpha \in A_2(X)$;

(証明の概略) 定理の結果は完全グラフの辺集合に関するもので, 距離の具体的な値に言及するものではない. 更に等長列もその分割のみに依存する. 故に距離の公理を無視した議論が可能になる. その分割のいかなる張り合わせに対してその等長列の各項はもとの項以下になる. まず, $a_2 = 2$ のときに特徴づけを行い, それを用いて $a_2 > 2$ は起こらないことを示す. $2k+2 \leq n = 1 + v(x,X)_\alpha + v(x,X)_\beta$ なので, $\emptyset \neq M_{k+1} \subseteq M_{k-1} \subseteq M_2$ である. 次の場合分けを行う：

- Case 1: $\alpha \in M_{k+1} \subseteq M_{k-1} = \{\alpha, \beta\}$;
- $\exists x \in X, \exists S \in \binom{X}{k+1}; S \subseteq R_\alpha(x)$;
- $\forall U, V \in \binom{S}{k-1}, \{x\} \cup U \simeq \{x\} \cup V$;
- 補題 2.3 により, $U \simeq V$. 定理 3.1 により, $|A_2(S)| = 1$;
- Case 1-1. $A_2(S) = \{\alpha\}$;
- $W \in \binom{S}{k-1}$ を固定する;
- $v(W, X-W)_\beta \neq 0$ である. そうでなかったら, $A_2(X) = \{\alpha\}$ である. このことは $A_2(S) = \{\alpha\}$ と $v(W, X-W)_\beta = 0$ から導かれる. よって矛盾；
- それゆえ, $\exists z \in X; v(z,W)_\beta \neq 0.$;
- $v(z,W)_\beta = k-1$ である. そうでなかったら, $A_2(\{z\} \cup W) = \{\alpha\}$, よって矛盾；

- $v(z,X)_\beta = n-1$ である. そうでなかったら, $a_k > 2$, よって矛盾;
- このことは $(X, E_\beta) \simeq K_{1,n-1}$ を意味する;
- Case 1-2. $A_2(S) = \{\beta\}$;
- $v(x,X)_\alpha = n-1$ である. そうでなかったら, $a_k > 2$, よって矛盾;
- このことは $(X, E_\alpha) \simeq K_{1,n-1}$ を意味する;
- Case 2: $\alpha \in M_{k+1} \subseteq M_{k-1} = \{\alpha\}$;
- $(x,y) \in R_\beta$ とする. そのとき, $\exists z \in X; x,y \in R_\alpha(z)$ である. それは $|R_\alpha(x) \cap R_\alpha(y)| = |R_\alpha(x)| + |R_\alpha(y)| - |R_\alpha(x) \cup R_\alpha(y)| \geq 2(n-1-(k-2)) - n = n - 2k + 2 > 0$ から導かれる;
- $S \in \binom{R_\alpha(z)}{k+2}; x,y \in S$ とする;
- $|A_k(S)| = 2$ である. そうでなかったら, $|A_k(S)| = 1$ で, 定理から $|A_2(S)| = 1$ で, $\beta \notin M_{k-1}$ に矛盾.
- $T \in \binom{S}{k}; x,y \in T$ とする. そのとき, $\{U \cup \{z\} \mid U \in \binom{S}{k-1}\}$ は非合同な 2 つの k 点部分集合を含むので, $\exists w \in T; v(w,T)_\alpha = k-1$ である.
- $U := (T - \{x\}) \cup \{z\}$ とする. そのとき, $U \in \binom{X}{k}; v(U,U)_\beta < v(T,T)_\beta$ である.
- 同じ議論を用いて $v(U,U)_\beta$ が 0 でない限り減らすことができる.
- 補題により, $v(U,U)_\beta = 0$ かつ $v(T,T)_\beta = 1$ である.
- $k \geq 4$ なので, $\{x,y\}$ は (X, E_β) の唯一の辺である.

これらの議論は証明を完成させる. □

以下の定理たちの証明は煩雑なので結果のみを記す.

Theorem 3.3 $a_3 = 2$ かつ $n \geq 5$ ならば, 適当な $\alpha \in A_2(X)$ に対して (X, E_α) は次のどれかと同型である:

(i) 完全二部グラフ;

(ii) X 上のマッチング;

(iii) 五角形.

Theorem 3.4 $a_2 = a_3 = 3$ かつ $5 \leq n$ ならば (X, d) は以下の例のどれかと同型である.

Example 3.1 $\{Y, Z\}$ を W の分割で $|Y| = |Z| = 4$ となるものとする. E_γ を W 上の完全マッチングで $\binom{Y}{2} \cup \binom{Z}{2}$ に含まれるものとする. $E_\beta = (\binom{Y}{2} \cup \binom{Z}{2}) \setminus E_\gamma$ で E_α を $E_\beta \cup E_\gamma$ の補集合とする. W の部分集合 X に対して, $|X| \geq 5$ ならば $A_3(X) = \{\alpha\alpha\beta, \alpha\alpha\gamma, \beta\beta\gamma\}$ である.

Example 3.2 $\{Y, Z\}$ を X の分割とする. $E_\alpha = \binom{Y}{2} \cup \binom{Z}{2}$ と定義して, E_γ を Y と Z の間のマッチングで, E_β を $E_\alpha \cup E_\gamma$ の補集合とする. そのとき $A_3(X) = \{\alpha\alpha\alpha, \alpha\beta\gamma, \beta\beta\alpha\}$ である.

Example 3.3 $\{E_\beta, E_\gamma\}$ を X 上のマッチングの分割とする. E_α を $E_\beta \cup E_\gamma$ の補集合とする. そのとき $A_3(X) = \{\alpha\alpha\alpha, \alpha\alpha\beta, \alpha\alpha\gamma\}$ である.

Example 3.4 $\{Y, Z\}$ を X の分割で $|Z| = 2$ となるものとする. $E_\alpha = \binom{Y}{2}$, $E_\gamma = \binom{Z}{2}$ と定義して, E_β を $E_\alpha \cup E_\gamma$ の補集合とする. そのとき $A_3(X) = \{\alpha\alpha\alpha, \beta\beta\alpha, \beta\beta\gamma\}$ である.

参考文献

[1] E. Bannai, Et. Bannai, D. Stanton, An upper bound for the cardinality of an s-distance subset in real Euclidean space II, *Combinatorica* 3 (1983), no. 2, 147-152.

[2] D. G. Larman, C. A. Rogers, J. J. Seidel, On two-distance sets in Euclidean space, *Bull. London Math. Soc.* 9 (1977), no. 3, 261-267.

[3] A. Neumaier, Distance matrices, dimension, and conference graphs, *Nederl. Akad. Wetensch. Indag. Math.* 43 (1981), no. 4, 385-391.

Quasi-symmetric 2-$(41, 9, 9)$ designs

宗政　昭弘
(東北大学情報科学研究科)

2022 年 6 月 16 日

整数 $v \geq k > t \geq 1$, $\lambda \geq 1$ に対して，t-(v, k, λ) design とは組 $\mathcal{D} = (X, \mathcal{B})$ で X は v 個の「点」からなる集合，$\mathcal{B}$ は X の k 元部分集合の族であり，X の任意の t 元部分集合はちょうど λ 個の $\mathcal{B}$ に属する部分集合に含まれる，という条件をみたすものをいう。$\mathcal{B}$ に属す部分集合のことを「ブロック」と呼ぶ。

2-(v, k, λ) デザイン $\mathcal{D}$ は

$$|B \cap B'| = \lambda \quad (B, B' \in \mathcal{B},\ B \neq B')$$

をみたすとき対称的（symmetric）であるという。例えば，有限射影平面がその例であり，逆に $\lambda = 1$ をみたす対称的 2-(v, k, λ) デザインは有限射影平面に限られる。

2-(v, k, λ) デザイン $\mathcal{D}$ は

$$\exists x < \exists y,\ \{|B \cap B'| \mid B, B' \in \mathcal{B},\ B \neq B'\} = \{x, y\} \tag{1}$$

をみたすとき quasi-symmetric であるという。例えば，有限アフィン平面がその例であり，その場合は $(x, y) = (0, 1)$ である。

Quasi-symmetric なデザインの例は以下のように分類されている。

(i) 有限射影平面を除く 2-$(v, k, 1)$ デザイン $((x, y) = (0, 1))$,

(ii) strongly resolvable designs (例えばアフィン空間とその超平面 $AG_{n-1}(n, q)$, $x = 0$),

(iii) biplane のひとつのブロックの外部に定義されるデザイン，つまり 2-$((k+1)k/2, k, 2)$ デザイン $(x = 1,\ y = 2)$,

(iv) 上記以外（例外的 quasi-symmetric デザイン）。

例外的 quasi-symmetric デザインのパラメータ (v, k, λ, x, y) は文献 [6] に表がある。例えば

$$(v, k, \lambda, x, y) = (37, 9, 8, 1, 3)$$

については，Bouyuklieva, Varbanov [3] が位数 5 の自己同型の存在を仮定した上での非存在を示した後，Harada, Munemasa and Tonchev [4] が無条件での非存在を示した。

$$(v, k, \lambda, x, y) = (41, 9, 9, 1, 3)$$

も同じ x, y の値を持ち，v, λ が少し増えただけなので，同様に非存在が示せそうであるが，最近ようやくできたのが，いくつかの位数の自己同型の存在を仮定した上での非存在である（詳しくは [5] 参照)。そのうち最も簡単に述べられるのは以下の定理 1 である。

ここで，quasi-symmetric 2-$(41, 9, 9)$ デザインは必ず (1) における $\{x, y\}$ は $\{1, 3\}$ となることがわかる。これは，[6, Theorem 48.13.2] において

$$(v, k, \lambda, b, r) = (41, 9, 9, 205, 45)$$

とおくと

$$17xy - 33(x + y) + 81 = 0$$

がわかり，これをみたす $x, y \in \{0, 1, \ldots, k\}$ は $\{x, y\} = \{1, 3\}$ に限られるからである。したがって以後，quasi-symmetric 2-$(41, 9, 9)$ デザインにおいてパラメータ x, y は言及しないことにする。

定理 1. もし quasi-symmetric 2-$(41, 9, 9)$ デザインが存在したとすると，その自己同型群の位数は 7 以上の素数で割り切れない。

この定理の証明は素数 41 以外は理論的にできる ([5] 参照)。位数 41 の自己同型をもつ quasi-symmetric 2-$(41, 9, 9)$ デザインは 2 元体上の長さ 41 の巡回符号を生成し，その分類により平方剰余符号に一致することがわかる。すると，このデザインは平方剰余符号の重み 9 の符号語を集めた 2-$(41, 9, 18)$ デザインに含まれることになる。そのような quasi-symmetric 2-$(41, 9, 9)$ デザインは存在しないことが次の補題よりわかる。

補題 2. 2 元体上の長さ 41 の平方剰余符号に含まれる重み 9 の符号語全体の集合を X とする。このとき，ブロック集合が X の部分集合となるような quasi-symmetric 2-$(41, 9, 9)$ デザインは存在しない。

この補題はコンピュータによ検証できるので，それをここに記す。使用するのは magma [2] である。まず，2 元体上の長さ 41 の巡回符号を定義し，その重み 9 の符号語を集めて 2-$(41, 9, 18)$ デザインを作る。

```
QR41:=QRCode(GF(2),41);
w9:=[ Support(x) : x in Words(QR41,9) ];
#w9 eq 410;
t,l:=IsDesign(IncidenceStructure< 41 | w9 >,2);
t and l eq 18;
```

このデザインのブロックの集合 $\mathcal{B}$ は 410 個のブロックを含んでおり，所望の quasi-symmetric 2-$(41,9,9)$ デザインは 205 個のブロックを含んでいる。410 個から 205 個を選び出すのが不可能であることを示すのではなく，特定の点を含むブロック全体 (45 個) を作れないことを示せば良い。そのためには，点 1 を含む 90 個のブロックを列挙し，この中からどのように 45 個を選んでも交わりを 1 または 3 点とすることができないことを確認すればよい。したがって，90 点のグラフ

$$\text{頂点集合} = \{B \in \mathcal{B} \mid 1 \in B\},$$
$$\text{辺集合} = \{\{B, B'\} \mid |B \cap B'| = 1, 3\}$$

においてサイズ 45 のクリークの非存在を確認すれば良い。

```
B1:={@ x : x in w9 | 1 in x @};
#B1 eq 90;
{ #(x meet y) : x,y in B1 | x ne y } eq { 1, 2, 3, 4 };
int1or3:=func< i,j | #(B1[i] meet B1[j]) in {1,3} >;
E:={ { i,j } : i,j in [1..#B1] | int1or3(i,j) };
G:=Graph< #B1 | E >;
not HasClique(G,45,false);
```

Quasi-symmetric 2-$(41,9,9)$ デザインの存在は依然として未解決であるが，quasi-symmetric ではない 2-$(41,9,9)$ デザインは，位数 $41\cdot 40$ の 2 重可移置換群 $AGL(1,41)$ の軌道として構成される。また，2-$(41,9,18)$ デザインも存在する。このようなデザインは，位数 41 の自己同型の存在という仮定の下で一意的である。これは，長さ 41 の 2 元平方剰余符号の重み 9 の符号語（410 個）の台として構成法される。

一般に， t-(v,k,λ) デザインの結合行列 $A = (a_{i,j})$ とは，成分が $0,1$ のみからなる $b \times v$ 行列であって j 番目の点が i 番目のブロックに属している時 $a_{i,j} = 1$ とし，そうでないとき $a_{i,j} = 0$ として定義されたものをいう。$\mathcal{D} = (X, \mathcal{B})$ を 2-(v,k,λ) デザインとし，$x \in X$ とすると，derived デザイン $\mathcal{D}^x$ は次のように定義され，それは 1-$(v-1,k-1,\lambda)$ デザインになる。点の集合は $X \setminus \{x\}$ であり，ブロックの集合は

$$\{B \setminus \{x\} \mid B \in \mathcal{B}, x \in B\}$$

である。もし 1-$(v-1,k-1,\lambda)$ デザイン $\mathcal{D}'$ がある 2-(v,k,λ) デザイン $\mathcal{D}$ の derived デザインに同型となるとき，$\mathcal{D}'$ は $\mathcal{D}$ に拡張可能であるという。

$(X, \mathcal{B})$ を quasi-symmetric 2-$(41,9,9)$ デザインとすると，

$$|X| = 41, \quad \mathcal{B} \subseteq \binom{X}{9}, \quad |\mathcal{B}| = 205.$$

$$\{|B \cap B'| \mid B, B' \in \mathcal{B},\ B \neq B'\} = \{1, 3\}.$$

また，A を $(X, \mathcal{B})$ の結合行列とすると，A は 205×41 行列であり，

$$\mathrm{rank}_2 A \leq \mathrm{rank}_2[A\ \mathbf{1}] \leq 21.$$

$\mathcal{D}$ を quasi-symmetric 2-$(41, 9, 9)$ デザインとすると，その derived デザインは 1-$(40, 8, 9)$ デザインであり，しかも２つのブロックは 0 または 2 点で交わる。その結合行列は 45×40 行列となり，それを２元体上の行列とみなして行空間を考えると，長さ 40 の重偶二元符号となる。したがって，長さ 40 の重偶自己双対符号に含まれるが，そのような自己双対符号は分類されている ([1] 参照)。このことを使って 1-$(40, 8, 9)$ デザイン，ひいては quasi-symmetric 2-$(41, 9, 9)$ デザインが分類できないかと考えているが，計算量が多くて現時点では打開策が見当たらない。唯一できたのは以下のような仮定をつけた 1-$(40, 8, 9)$ デザインが quasi-symmetric 2-$(41, 9, 9)$ デザインに拡張可能でないことである。

定理 3. $\mathcal{D}'$ を 1-$(40, 8, 9)$ デザインでどの２つのブロックは 0 または 2 点で交わり，しかもその結合行列の二元体上の階数が 20 と仮定する。さらに，$\mathcal{D}'$ は位数 5 の自己同型をもつと仮定すると，$\mathcal{D}'$ は quasi-symmetric 2-$(41, 9, 9)$ デザインに拡張可能でない。

参考文献

[1] K. Betsumiya, M. Harada and A. Munemasa, A complete classification of doubly even self-dual codes of length 40. *Electronic J. Combin.* **19**, #P18 (12 pp.) (2012).

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

[3] S. Bouyuklieva and Z. Varbanov, Quasi-symmetric 2-$(37, 9, 8)$ designs and self-orthogonal codes with automorphisms of order 5, *Math Balkanica (N.S.)* **19** (2005), 33–38.

[4] M. Harada, A. Munemasa and V. D. Tonchev Self-dual codes and the non-existence of a quasi-symmetric 2-$(37, 9, 8)$ design with intersection numbers 1 and 3, *J. Combin. Des.* **25** (2017), 469–476.

[5] A. Munemasa and V.D. Tonchev, Quasi-symmetric 2-$(41, 9, 9)$ designs and doubly even self-dual codes of length 40, Applicable Algebra in Engineering, Communication and Computing, 2022.

[6] M. S. Shrikhande, *Quasi-Symmetric Designs*, Chapter VI.48 in: *Handbook of Combinatorial Designs*, 2nd Edition, C.J. Colbourn and J.H. Dinitz, eds., Chapman & Hall/CRC, Boca Raton, 2007, pp. 578–582.

既約表現に関する原田予想 II が成立する有限群の例

杉元 最大 *

筑波大学大学院 数理物質科学研究群 数学学位プログラム 博士後期課程 2 年，2022 年 6 月

1 はじめに

本稿は任意の有限群に対する予想 1.1 が成立する具体的な群の考察である．予想 1.1 は一言で言えば群 G の全ての共役類の大きさの積を全ての既約指標の次数の積で割った数 $h(G)$ は整数であるというものである．

予想 1.1. [1] 任意の有限群 G について $h(G) \in \mathbb{Z}$ である．

$h(G)$ が G のどのような性質を反映しているのかは不明だが，以下のような状況で現れることが分かっている．既約表現 $\rho_i : G \to \mathrm{GL}_{n_i}(\mathbb{C})$ を線型に拡張すると $\mathbb{C}$ 代数の準同型 $\tilde{\rho}_i : \mathbb{C}G \to M_{n_i}(\mathbb{C})$ となる．族 $(\tilde{\rho}_i)_{1\leq i\leq l}$ によってえられる写像 $\mathbb{C}G \to \prod_{i=1}^{l} M_{n_i}(\mathbb{C})$ の中心 $Z(\mathbb{C}G)$ への制限 $\omega : Z(\mathbb{C}G) \to \mathbb{C}^l$ は同型写像である．W を $Z(\mathbb{C}G)$ の基底 $\{\sum_{x\in K_i} x\}_{1\leq i\leq l}$ と $\mathbb{C}^l$ の標準基底に関する ω の表現行列とし，X を G の指標表とすると，これらの行列式の比が，

$$h(G) = \frac{\det W}{\det X} = \prod_{i=1}^{l} \frac{\#K_i}{\deg \chi_i}$$

である．

例えば G が可換群なら全ての共役類の大きさと全ての既約指標の次数が 1 なので $h(G) = 1$ である．位数が最小の非可換群である 3 次の対称群 S_3 について，

$$h(S_3) = \frac{1 \cdot 3 \cdot 2}{1 \cdot 1 \cdot 2} = 3$$

と計算できる．

先行研究として対称群と交代群については Hida[10] で 予想 1.1 が成立することが示されている．また，G の全ての Sylow p-部分群が可換ならば 予想 1.1 が成立することは Kiyota[9] で証明されている．

さらに千吉良直紀氏によって $h(G)$ は交換子部分群 G' の位数との関係が示唆されている．

予想 1.2. 任意の有限群 G について $h'(G) := h(G)/|G'| \in \mathbb{Z}$ である．

* sugimoto-m@math.tsukuba.ac.jp

2 主結果

2.1 巡回群による半直積

アーベル群 A と群 H の半直積 $G = A \rtimes H$ の全ての既約表現は，H の部分群の既約表現を使って構成できる．その方法は Serre [2, §8.2] で “the method of little groups of Wigner and Mackey” として紹介されている．

これにより巡回群による半直積 $\mathbb{Z}/n\mathbb{Z} \rtimes C_m$ の既約表現の次数の積を共役類の大きさで表すことができるというのが補題 2.1 である．

補題 2.1. $G = \mathbb{Z}/n\mathbb{Z} \rtimes C_m$ のとき，

$$\prod_{\chi \in \mathrm{Irr}(G)} \deg \chi = \prod_{k \in R_0} \#[k,1]^{m/\#[k,1]}$$

さらに $h(G)$ はその特別な剰余群に帰着させて計算できる．

補題 2.2. $N = \{\sigma^i \in C_m \mid r^i = 1\}$ は中心 $Z(G)$ の部分群で，$h'(G/N) \in \mathbb{Z}$ ならば $h'(G) \in \mathbb{Z}$.

以上の準備をもとに，計算機を用いて次の定理を得た．

定理 2.3. $1 \leq n \leq 8$ のとき，任意の $m \in \mathbb{Z}_{>0}$ に対して

$$h'(\mathbb{Z}/2^n\mathbb{Z} \rtimes C_m) \in \mathbb{Z}$$

2.2 有限体上の一般線型群

一般線型群 $\mathrm{GL}(n,q)$ の指標に関する理論は Steinberg や Green によって確立された．$n = 2, 3$ では予想 1.1,1.2 が成立することが確認できたが，一般の n で成立するかは今後の課題となった．以下は共役類の大きさと既約表現の次数をまとめた表である．

表 1 The sizes of conjugacy class and the degrees of irrep. of $\mathrm{GL}(2,q)$

size	degree	number
1	1	$q-1$
q^2-1	q	$q-1$
$q(q+1)$	$q+1$	$(q-1)(q-2)/2$
$q(q-1)$	$q-1$	$(q^2-q)/2$

表 2　The sizes of conjugacy class and the degrees of irrep. of $\mathrm{GL}(3,q)$

size	degree	number
1	1	$q-1$
$(q^2-1)(q^2+q+1)$	$q(q+1)$	$q-1$
$q(q^2-1)(q^3-1)$	q^3	$q-1$
$q^2(q^2+q+1)$	q^2+q+1	$(q-1)(q-2)$
$q^2(q^2-1)(q^2+q+1)$	$q(q^2+q+1)$	$(q-1)(q-2)$
$q^3(q+1)(q^2+q+1)$	$(q+1)(q^2+q+1)$	${}_{q-1}C_3$
$q^3(q-1)(q^2+q+1)$	$(q-1)(q^2+q+1)$	$q(q-1)^2/2$
$q^3(q-1)^2(q+1)$	$(q-1)^2(q+1)$	$q(q^2-1)/3$

参考文献

[1] K. Harada, *Revisiting character theory of finite groups*, Bulletin of the Inst. Math. Academia Sinica (New Series) 13 (2018) 383–395.

[2] J. P. Serre, *Linear Representations of Finite Groups*, Graduate Text in Mathematics 42, Springer-Verlag, 1977.

[3] S. Lang, *Algebra, Revised Third Edition*, Graduate Texts in Mathematics 211, Springer-Verlag, 2002.

[4] Basheer, Ayoub Basheer Mohammed, *Character tables of the general linear group and some of its subgroups*, 2008.

[5] Green, J. A., *Discrete Series Characters for GL(n, q)*, Algebras and Representation Theory 2, 61–82. (1999).

[6] Green, J. A., *The Characters of the Finite General Linear Groups*, Transactions of the American Mathematical Society, 80(2), 402–447. (1955).

[7] Steinberg, R., *The Representations of GL(3,q), GL(4,q), PGL(3,q), and PGL(4,q)*, Canadian Journal of Mathematics, 3, 225–235. (1951).

[8] Steinberg, R., *A Geometric Approach to the Representations of the Full Linear Group Over a Galois Field*, Transactions of the American Mathematical Society, 71(2), 274–282. (1951).

[9] M. Kiyota, *Harada conjecture II and its block refinement*, 数理解析研究所講究録 2061(2018), 56–60.

[10] A. Hida, *Harada's conjecture on character degrees and class sizes –symmetric and alternating groups–*, 数理解析研究所講究録 2086(2018), 144–153.

Moonshine for integral dihedral group rings

浦野　慧 (Satoru Urano)

筑波大学

1 Introduction

In 1979, Conway and Norton proposed the monstrous moonshine conjecture [6] that the McKay-Thompson series $T_g(\tau) := \sum_{n\in\mathbb{Z}} \mathrm{Tr}(g|V_n^\natural)q^{n-1}$ $(q = e^{2\pi i\tau})$ is a Hauptmodul for some genus 0 congruence subgroup of $SL_2(\mathbb{R})$, where g is any element of the monster simple group $\mathbb{M}$ and $V_n^\natural$ is the eigenspace of the monster vertex algebra $V^\natural = \bigoplus_{n\in\mathbb{Z}} V_n^\natural$ that was constructed by Frenkel-Lepowsky-Meurman [7] in 1988. In 1992, Borcherds proved the monstrous moonshine conjecture [1] by using string theory and the notion of vertex operator algebras and generalized Kac-Moody algebras. In 1994, Ryba proposed the modular moonshine conjecture that for prime order p and elements g in conjugacy class pA of $\mathbb{M}$, there exists a vertex algebra with characteristic p with an actions of the centralizer $C_{\mathbb{M}}(g)$ of g such that the graded Brauer character of any p-regular element of $C_{\mathbb{M}}(g)$ is a Hauptmodul. In 1998, Borcherds and Ryba proved the modular moonshine conjecture [2], [3] by using the notion of Tate cohomology under the assumption that there exists an integral form V of $V^\natural$. In 2019, Carnahan proved this assumption [4], so modular moonshine is completely proved.

It is natural to consider modular moonshine for elements of composite order. To prove generalized modular moonshine for composite order, it is sufficient to decompose an integral form V of $V^\natural$ as a direct sum of indecomposable $\mathbb{Z}[g]$-modules, but the biggest problem is that the larger the order of g is, the more complicated indecomposable modules over the group ring $\mathbb{Z}[g]$ can be.

In this report, we shall briefly explain modular moonshine for prime order and monstrous moonshine for integral group rings.

2 Modular moonshine

In this section, we briefly explain modular moonshine for elements of prime order based on [2],[3].

Borcherds and Ryba proved modular moonshine by using theories of Tate cohomology and the vertex operator algebra for Leech lattice.

Definition 2.1 (Tate cohomology)**.** Suppose that G is a finite group. Let A be G-module and N_G be the norm map $A \to A; a \mapsto \sum_{g\in G} g(a)$. Then, the i-th Tate cohomology $\hat{H}^i(G, A)$ of G with coefficients in A is defined to be the following:

$$\hat{H}^i(G,A)=\begin{cases} H_{-i-1}(G,A) & (i\leq -2)\\ \mathrm{Ker}(N_G)/\langle ga-a|a\in A,g\in G\rangle & (i=-1)\\ A^G/\mathrm{Im}(N_G) & (i=0)\\ H^i(G,A) & (i\geq 1)\end{cases},$$

where A^G is the largest G-invariant submodule of A, $H_i(G,A)$ is the i-th homology, and $H^i(G,A)$ is the i-th cohomology. For $g\in G$, the i-th Tate cohomology $\hat{H}^i(\langle g\rangle,A)$ of cyclic group $\langle g\rangle$ is denoted by $\hat{H}^i(g,A)$.

Let $\mathbb{Z}_p$ be the p-adic integers. We regard $\mathbb{Z}$-modules as $\mathbb{Z}_p$-modules in the Tate cohomology;

Lemma 2.2 ([3] Lemma 2.1)**.** *Let G be a finite group including an element g of prime order p. If A is a free $\mathbb{Z}[1/n]$-module acted on by a p-group G with $(p,n)=1$, then the natural map from $\hat{H}^i(G,A)$ to $\hat{H}^i(G,A\otimes\mathbb{Z}_p)$ is an isomorphism for any $i\in\mathbb{Z}$.*

Borcherds and Ryba proved the modular moonshine conjectures by using the fact that there are exactly 3 indecomposable finitely generated modules over the group ring $\mathbb{Z}_p[g]$ which are free as $\mathbb{Z}_p$-modules [8]. These are the trivial module $\mathbb{Z}_p$, the group ring $\mathbb{Z}_p[g]$, and the module I which is the kernel of the natural map $\mathbb{Z}_p[g]\to\mathbb{Z}_p$. Borcherds caluculated all ring homomorphisms from the Green ring for cyclic group of prime order p to rational numbers by direct sum and tensor product of indecomposable modules:

Lemma 2.3 ([2] Lemma 2.3)**.** *Let K be the Green ring of $\mathbb{Z}_p[g]$, where the Green ring of $\mathbb{Z}_p[g]$ is a free $\mathbb{Q}$-module with a basis of 3 elements $[\mathbb{Z}_p],[\mathbb{Z}_p[g]]$, and $[I]$. There are exactly 3 ring homomorphisms* $\dim,\mathrm{Tr}(g|\cdot)$*, and f from $K\to\mathbb{Q}$. They are given by*

- $\dim([\mathbb{Z}_p])=1,\dim([\mathbb{Z}_p[g]])=p,\dim([I])=p-1$.
- $\mathrm{Tr}(g|[\mathbb{Z}_p])=1,\mathrm{Tr}(g|[\mathbb{Z}_p[g]])=0,\mathrm{Tr}(g|[I])=-1$.
- $f([\mathbb{Z}_p])=1,f([\mathbb{Z}_p[g]])=0,f([I])=1$.

Let h be a p-regular element of $C_{\mathbb{M}}(g)$ and $V=\bigoplus_{n\in\mathbb{Z}}V_n$ be an integral form of $V^\natural$. The graded homomophism $\sum_{n\in\mathbb{Z}}f(V_n)q^{n-1}$ is equal to $\sum_{n\in\mathbb{Z}}(\dim\hat{H}^0(g,V_n)+\dim\hat{H}^1(g,V_n))q^{n-1}$. We have the following complete description of the grader Brauer character $\sum_{n\in\mathbb{Z}}\widetilde{\mathrm{Tr}}(h|\hat{H}^i(g,V_n))q^{n-1}$ $(i=0,1)$ by using the vertex algebra of Leech lattice and computer calculation.

Theorem 2.4 (Modular moonshine [2],[3],[4])**.** *Suppose that $g\in\mathbb{M}$ has prime order p. Let V be an integral form of $V^\natural$ and h be a p-regular element of $C_{\mathbb{M}}(g)$. Then, we have*

$$\sum_{n\in\mathbb{Z}}\widetilde{\mathrm{Tr}}(h|\hat{H}^0(g,V_n))q^{n-1}=\begin{cases} T_{gh}(\tau) & (g\in pA,3C)\\ \dfrac{T_{gh}(\tau)-T_{gh}(\tau+1/2)}{2} & (g\in 2B)\\ \dfrac{T_{gh}(\tau)+T_{gh\sigma}(\tau)}{2} & (g\in pB,2|(p-1))\end{cases},$$

$$\sum_{n\in\mathbb{Z}} \widetilde{\mathrm{Tr}}(h|\hat{H}^1(g,V_n))q^{n-1} = \begin{cases} 0 & (g \in pA, 3C) \\ \dfrac{-T_{gh}(\tau) - T_{gh}(\tau+1/2)}{2} & (g \in 2B) \\ \dfrac{-T_{gh}(\tau) + T_{gh\sigma}(\tau)}{2} & (g \in pB, 2|(p-1)) \end{cases},$$

where $\sigma \in C_{\mathbb{M}}(g)/O_p(C_{\mathbb{M}}(g))$ is the involution which acts as 1 on $\hat{H}^0(g,V)$ and as -1 on $\hat{H}^1(g,V)$ and $O_p(C_{\mathbb{M}}(g))$ is the largest normal p-subgroup of $C_{\mathbb{M}}(g)$.

By Theorem 2.4, we have that the graded homomophism $\sum_{n\in\mathbb{Z}} f(V_n)q^{n-1}$ is the following Hauptmodul;

$$\sum_{n\in\mathbb{Z}} f(V_n)q^{n-1} = \begin{cases} T_g(\tau) & (g \in pA, 3C) \\ T_{4A}(\tau) & (g \in 2B) \\ T_{g\sigma}(\tau) & (g \in pB, 2|(p-1)) \end{cases}.$$

3 Monstrous moonshine for integral group rings

In this section, we explain monstrous moonshine for integral group rings based on [5] and the recent results.

By Lemma 2.3 and Theorem 2.4, if cyclic subgroup of $\mathbb{M}$ with prime order p, then any ring homomophism produces a Hauptmodul. It is natural to propose the following conjecture:

Conjecture 3.1 (Monstrous moonshine for integral group rings [5])**.** *Let R be a subring of $\mathbb{C}$, and let G be a subgroup of $\mathbb{M}$. Then for any ring homomorphism $\phi : Rep_R(G) \to \mathbb{C}$, the "generalized McKay-Thompson series"*

$$T_\phi(\tau) := \sum_{n\geq 0} \phi(V^\natural_{n,R})q^{n-1}$$

is the q-expansion of a finite level Hauptmodul. That is, the holomorphic function $T_\phi(\tau)$ on the complex upper half plane $\mathbb{H}$ is invariant under a discrete subgroup $\Gamma_\phi < SL_2(\mathbb{R})$ containing $\Gamma_0(N)$ for some N, such that the quotient $\mathbb{H}/\Gamma_\phi$ is genus zero, with function field generated by T_ϕ. Here, $V^\natural_{n,R}$ is the weight n subspace of $V \otimes R$.

If $R = \mathbb{C}$, then Conjecture 3.1 means well-known monstrous moonshine.

We consider Conjecture 3.1 in the following cases: (1) cyclic groups of order p^2. (2) dihedral groups D_{2p}.

3.1 Cyclic groups of order p^2

Let $g \in \mathbb{M}$ be an element of order p^2. Then indecomposable finitely generated $\mathbb{Z}_p[g]$-modules are classified:

Theorem 3.2 ([8])**.** *There are $4p+1$ indecomposable finitely generated $\mathbb{Z}_p[g]$-modules which are free as $\mathbb{Z}_p$-modules. They are given by $A := \mathbb{Z}_p$, $D := \mathbb{Z}_p[g]$, $B := D/(1+g+\cdots+g^{p-1})D$,*

$E := D/(g^p - 1)D$,

- $C := D/(1 + g^p + \cdots + g^{p(p-1)})D$,
- C^A *with* $0 \to A \to C^A \to C \to 0$ *exact,*
- C^B *with* $0 \to B \to C^B \to C \to 0$ *exact,*
- $C_i^{A\oplus B}(1 \le i \le p-1)$ *with* $0 \to A \oplus B \to C_i^{A\oplus B} \to C \to 0$ *exact,*
- $C_i^E(1 \le i \le p-1)$ *with* $0 \to E \to C_i^E \to C \to 0$ *exact,*
- $C_i^B(1 \le i \le p-2)$ *with* $0 \to B \to C_i^B \to C \to 0$ *exact,*
- $C_i^{A\oplus E}(1 \le i \le p-2)$ *with* $0 \to A \oplus E \to C_i^{A\oplus E} \to C \to 0$ *exact.*

Let g be an element of order 4 in $\mathbb{M}$ and $V = \bigoplus_{n\in\mathbb{Z}} V_n$ be a self-dual integral form of $V^\natural$. We caluculated all ring homomorphisms from the Green ring for cyclic group of order 4 to rational numbers by direct sum and tensor product of indecomposable modules [11]:

Lemma 3.3 ([5] Theorem 6.2)**.** *Let K be the Green ring of $\mathbb{Z}[g]$, which is a free $\mathbb{Q}$-module with a basis of 9 elements formed from indecomposable $\mathbb{Z}[g]$-modules. We have the following ring homomorphisms $K \to \mathbb{Q}$;*

	dim	$\mathrm{Tr}(g\|\cdot)$	ψ_1	ψ_2	ψ_3	$\mathrm{Tr}(g^2\|\cdot)$	f	θ
$[A]$	1	1	1	1	1	1	1	1
$[B]$	1	−1	−1	1	1	1	1	1
$[C]$	2	0	0	0	0	−2	2	0
$[D]$	4	0	0	0	0	0	0	0
$[E]$	2	0	0	0	0	2	2	0
$[C^A]$	3	1	−1	1	−1	−1	1	1
$[C^B]$	3	−1	1	1	−1	−1	1	1
$[C^{A\oplus B}]$	4	0	0	0	0	0	2	2
$[C^E]$	4	0	0	0	0	0	2	2

From monstrous moonshine, modular moonshine and Lemma 3.3 by comparing values of homomorphisms, we have that V_n consists of the several indecomposable modules.

Lemma 3.4 ([5] Lemma 6.4)**.** *Let $g \in 4A(2B), 4C(2B), 4D(2B)$. We have that A, B, D, E are the only possible summands in V_n for even n and that C, D, C^A, C^B are the only possible summands in V_n for odd n.*

Theorem 3.5 ([5] Theorem 6.5)**.** *Let $g \in 4A(2B)$. The multiplicities a_n, d_n, α_n of indecomposable modules A, D, C^A in V_n are given by the generating function formula*

$$\begin{pmatrix} \sum_{n\in\mathbb{Z}} a_n q^{n-1} \\ \sum_{n\in\mathbb{Z}} d_n q^{n-1} \\ \sum_{n\in\mathbb{Z}} \alpha_n q^{n-1} \end{pmatrix} = \begin{pmatrix} 0 & 1/2 & 1/2 \\ 1/4 & 1/4 & -1/2 \\ 0 & -1/2 & 1/2 \end{pmatrix} \begin{pmatrix} T_{1A}(\tau) \\ T_{2B}(\tau) \\ T_{4A}(\tau) \end{pmatrix}.$$

In particular, from Theorem 3.5 if $g \in 4A(2B)$, then we clearly understand the number of indecomposable modules A, D, C^A in V_n. Hence, the graded ring homomorphisms $\sum_n \phi([V_n])q^{n-1}$

are the following well-known Hauptmoduls;

	dim	$\mathrm{Tr}(g\|\cdot)$	ψ_1	ψ_2	ψ_3	$\mathrm{Tr}(g^2\|\cdot)$	f	θ
$[A]$	1	1	1	1	1	1	1	1
$[D]$	4	0	0	0	0	0	0	0
$[C^A]$	3	1	-1	1	-1	-1	1	1
$\sum_n \phi([V_n])q^{n-1}$	T_{1A}	T_{4A}	T_{2B}	T_{4A}	T_{2B}	T_{2B}	T_{4A}	T_{4A}

3.2 Dihedral groups D_{2p}

In this report, the main results is monstrous moonshine for integral dihedral group rings.

Let D_{2p} be the dihedral group for prime number $p > 2$. In particular, we define $D_{2p} = \langle a, b | a^2 = b^p = 1, ab = b^{-1}a \rangle$. Then indecomposable finitely generated $\mathbb{Z}[D_{2p}]$-modules are classified;

Theorem 3.6 ([10])**.** *There are $7h+3$ indecomposable finitely generated $\mathbb{Z}[D_{2p}]$-modules which are free as $\mathbb{Z}$-modules, where h is the class number of $\mathbb{Z}[e^{2\pi i/p}]$. They are given by $S := \mathbb{Z}$ with trivial action, $S' := \mathbb{Z}$ with $a \cdot 1 = -1$ and $b \cdot 1 = 1$, $L := \mathbb{Z}[a]$, where b acts trivially, and for $i = 1, \cdots, h$,*

- $R_i \sim \mathbb{Z}[b]/(1 + b + \cdots + b^{(p-1)})\mathbb{Z}[b]$, *where a acts trivially.*
- $R'_i \sim \mathbb{Z}[b]/(1 + b + \cdots + b^{(p-1)})\mathbb{Z}[b]$, *where a acts by -1.*
- (R'_i, S) *with* $0 \to R'_i \to (R'_i, S) \to S \to 0$ *exact.*
- (R_i, S') *with* $0 \to R_i \to (R_i, S') \to S' \to 0$ *exact.*
- (R_i, L) *with* $0 \to R_i \to (R_i, L) \to L \to 0$ *exact.*
- (R'_i, L) *with* $0 \to R'_i \to (R'_i, L) \to L \to 0$ *exact.*
- $D_i := (R_i \oplus R'_i, L)$ *with* $0 \to R_i \to (R_i \oplus R'_i, L) \to (R'_i, L) \to 0$ *exact.*

We calculated all ring homomorphisms from the Green ring to rational numbers by direct sum, tensor product and by restricting over $\mathbb{Z}[a]$ and $\mathbb{Z}[b]$:

Theorem 3.7. *Let K be the Green ring of $\mathbb{Z}[D_{2p}]$, which is a free $\mathbb{Q}$-module with a spanning set of 10 elements formed from indecomposable $\mathbb{Z}[D_{2p}]$-modules. We have the following ring homomorphisms $\phi : K \to \mathbb{Q}$ and the graded ring homomorphisms $\sum_n \phi([V_n])q^{n-1}$ are given by the following Hauptmodul;*

	dim	$\mathrm{Tr}(a\|\cdot)$	f_2	$\mathrm{Tr}(b\|\cdot)$	f_p
$[S]$	1	1	1	1	1
$[S']$	1	-1	1	1	1
$[L]$	2	0	0	2	2
$[R]$	$p-1$	0	0	-1	1
$[R']$	$p-1$	0	0	-1	1
$[(R',S)]$	p	1	1	0	0
$[(R,S')]$	p	-1	1	0	0
$[(R,L)]$	$p+1$	0	0	1	1
$[(R',L)]$	$p+1$	0	0	1	1
$[D]$	$2p$	0	0	0	0
$\sum_n \phi([V_n])q^{n-1}$	T_{1A}	T_a	T_{2A} *or* T_{4A}	T_b	T_b *or* $T_{\sigma b}$

where "T_{2A} or T_{4A}" means that if $a \in 2A$, then $\sum_n f_2([V_n])q^{n-1}$ is T_{2A} and that if $a \in 2B$, then $\sum_n f_2([V_n])q^{n-1}$ is T_{4A}, and "T_b or $T_{\sigma b}$" means that if $b \in pA, 3C$, then $\sum_n f_2([V_n])q^{n-1}$ is T_b and that if $b \in pB$, then $\sum_n f_2([V_n])q^{n-1}$ is $T_{\sigma b}$.

By Theorem 3.7, the generalized McKay-Thompson series for any ring homomorphism $\phi : Rep_{\mathbb{Z}}(D_{2p}) \to \mathbb{C}$ is a well-known Hauptmoduls.

Generally, for an element $g \in G$ of order N and prime factor p of N, the number of indecomposable finitely generated modules over $\mathbb{Z}[g]$ can be infinite. In particular, this holds when $p^3|N$ [9]. Hence, to prove the moonshine for integral group rings in the case order p^3, we need to consider another way.

参考文献

[1] R. E. Borcherds, "Monstrous moonshine and monstrous Lie superalgebras", Invent. Math. 109, 405-444, (1992).

[2] R. E. Borcherds, "Modular Moonshine III", Duke Math. Journal Vol. 93 No. 1, 129-154, (1998).

[3] R. E. Borcherds, A.J. E. Ryba, "Modular Moonshine II", Duke Math. Journal Vol. 83 No. 2, 435-459, (1996).

[4] S. Carnahan, "A self-dual integral form of the moonshine module", SIGMA Vol. 15, 030, 36 pages, (2019).

[5] S. Carnahan, S. Urano, "Monstrous Moonshine for integral group rings", arXiv: 2111.09404, (2021).

[6] J. H. Conway, S. Norton, "Monstrous moonshine", Bull. London. Math. Soc. 11, 308-339, (1979).

[7] I. B. Frenkel, J. Lepowsky, A. Meurman, "Vertex operator algebras and monster", Academic Press, (1988).

[8] A. Heller, I. Reiner, "Representations of cyclic groups in rings of integers, I", Ann. of Math.

Vol. 76, No. 1, 73-92, (1962).

[9] A. Heller, I. Reiner, "Representations of cyclic groups in rings of integers, II", Ann. of Math. Vol. 77, No. 2, 318-328, (1963).

[10] M. P. Lee, "Integral representations of dihedral groups of order $2p$", TAMS. Vol. 110(2), 213-231, (1964).

[11] I. Reiner, "The integral representation ring of a finite group", Michigan Math. J. 12, 11-22, (1965).

Extra automorphisms of cyclic orbifolds of lattice vertex operator algebras

島倉 裕樹 (Hiroki Shimakura)

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

本稿では, [LS] で得られた格子頂点作用素代数 (VOA) の有限位数の自己同型による固定点 (cyclic orbifold) の例外自己同型に関する結果を紹介する.

1 背景

頂点作用素代数 (VOA) から新しい VOA を作る一つの方法として, 自己同型群による固定点 (orbifold) がある. 特に, "良い[注 1]" VOA の有限自己同型群[注 2]による orbifold も "良い" 性質を持つことが予想され, 研究されてきた. 最近, 自己同型群が巡回群の場合にこれら予想が解決され ([Mi15, CM]), これら結果を基にして cyclic orbifold construction の理論が整備された ([EMS20]). そして, その応用として, 中心電荷 24 の正則 VOA の分類問題が概ね解決された.

一方で, cyclic orbifold の自己同型群も興味深い. 一般に, V を VOA, σ を V の有限自己同型群とし, $V^\sigma = \{v \in V \mid \sigma(v) = v\}$ としたときに, 群準同型

$$\varphi : N_{\mathrm{Aut}(V)}(\langle\sigma\rangle) \to \mathrm{Aut}(V^\sigma)$$

が制限写像として得られる. 明らかに $\langle\sigma\rangle \subset \mathrm{Ker}\ \varphi$ であり, V が strongly regular の時は $\langle\sigma\rangle = \mathrm{Ker}\ \varphi$ となる ([DJX13, Sh04]). したがって, φ が全射かどうかが問題となる. そこで $\mathrm{Im}\ \varphi$ に属さない V^σ の自己同型を**例外**自己同型と呼ぶことにし, 次の問題を考えたい.

問題 1.1. V^σ が例外自己同型を持つための条件を与え, 対称性の高い V^σ を見つけよ.

次の V^σ の既約表現を用いた例外自己同型の特徴づけがある.

注 [1] strongly regular, すなわち, rational, C_2-cofinite, CFT-type, self-contragredient
注 [2] 無限群の場合には良い性質が引き継がれないことがある.

命題 1.2. [Sh04] V を *strongly regular* な *VOA* とする. このとき, $\tau \in \mathrm{Aut}(V^\sigma)$ が例外であるための必要十分条件は V^σ-加群として $V \circ \tau \ncong V$ である.[注 3]

V^σ の表現論が十分にわかっているならば, この命題を用いて調べることができる. そこで, [LS] では, V として格子 VOA V_L を考え, σ が fixed-point free の L の自己同型 g の持ち上げの場合 $\hat{g}$ を考える. この場合は $V^{\hat{g}}$ の既約加群は分類されており, $|\hat{g}| = |g|$ となる.[注 4] さらに L がルート (長さ 2 のベクトル) を持たないことを仮定する. すると $\mathrm{Aut}(V_L^{\hat{g}})$ は有限群[注 5]となる.

2 位数 2 の場合

偶格子 L の fixed-point free な自己同型 g の位数が 2 のとき, $g = -1$ となる. この場合の $\mathrm{Aut}(V_L^{\hat{g}})$ は [Sh04] で研究されている. この章では [Sh04] の結果をまとめておく.

長さ m の二元重偶符号 $C \subset \mathbb{F}_2^m$ に対して,

$$L_B(C) = \frac{1}{\sqrt{2}}\{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid (x_i \pmod 2) \in C,\ \sum_{i=1}^{m} x_i \in 4\mathbb{Z}\}$$

は階数 m の偶格子である. この格子の構成は**構成法 B** と呼ばれている.[注 6]

定理 2.1. [Sh04] L をルートを持たない偶格子とし, $\theta \in \mathrm{Aut}(V_L)$ を -1 の *(standard) lift* とする.[注 7] このとき, 次が同値である.

- V_L^θ が例外自己同型を持つ.
- ある二元符号 C があって, $L \cong L_B(C)$ となる.

注意 2.2.

- 長さ 8 の 1 次元二元符号 $\langle(11111111)\rangle_{\mathbb{F}_2}$ に構成法 B を適用すると $\sqrt{2}E_8$ が得られる. そして $\mathrm{Aut}(V^\theta_{\sqrt{2}E_8}) \cong O^+(10,2)$ となる *([Gr98, Sh04]).* 一方で, $N_{\mathrm{Aut}(V_{\sqrt{2}E_8})}(\langle\theta\rangle)/\langle\theta\rangle \cong 2^8.O^+(8,2)$ であり, この群は $O^+(10,2)$ の *maximal subgroup* である.
- 長さ 24 の *extended binary Golay* 符号 G_{24} から得られる $L_B(G_{24})$ に対して, $V^\theta_{L_B(G_{24})}$ は例外自己同型を持つ *([FLM88]).* この例外自己同型から $2^{1+24}.Co_1$ に属さない $\mathrm{Aut}(V^\natural)$ の元が得られる.

[注 3] 一般に VOA U の加群 (M, Y_M) と $h \in \mathrm{Aut}(U)$ に対して, $M \circ h = (M, Y_{M\circ h})$, $Y_{M\circ h}(v,z) = Y_M(hv,z)$ である.

[注 4] 一般には $|\hat{g}| = 2|g|$ の可能性もあるが, fixed-point free からこの場合は起こらない. 詳細は [EMS20] 参照.

[注 5] $N_{\mathrm{Aut}(V_L)}(\langle\hat{g}\rangle)/\langle\hat{g}\rangle$ が有限群であり, この群が $\mathrm{Aut}(V_L^{\hat{g}})$ の (有限個の) 既約加群の同型類全体への作用における V_L の既約部分加群の固定部分群になることからわかる.

[注 6] 構成法 B に着目した研究は [Sh04, Sh06] と [KKM91] 以外はないように思われる. しかし, rank 16 の Barnes-Wall 格子などの重要な例が構成される. また, 長さ 24 の extended Golay 符号 G_{24} に対して, $L_B(G_{24})$ の index 2 の拡大した格子としてリーチ格子が得られるなどの応用がある.

[注 7] -1 の $\mathrm{Aut}(V_L)$ への持ち上げ (lift) は一意ではないが, 共役となる.

定理 2.1 の拡張を考えることで, 次の自然な問題を得る.

問題 2.3. L を *(*ルートを持たない*)* 偶格子とし, g を *fixed-point free* な自己同型とする. $V_L^{\hat{g}}$ が例外自己同型を持つための L と g に関する必要十分条件を求めよ.

[Sh04] の証明では V_L^+ の表現論と命題 1.2 が使われている. したがって, 同様の議論を適用するには, $V_L^{\hat{g}}$ の表現論が必要であった. 近年になって, $V_L^{\hat{g}}$ の表現論の一般論は [DRX17] で確立されため, 結果を拡張するための準備は整っていた.

3 主結果

L を階数 m のルートを持たない偶格子とし, g を fixed-point free な L の自己同型とする.

定理 3.1. [LS] L が $\bigoplus_{i=1}^{t} \mathbb{Z}_{k_i}$ の部分群から *"*構成法 B*"* で構成されていたならば, $V_L^{\hat{g}}$ は例外自己同型を持つ.

これは例外自己同型を具体的に構成することで証明される. 基本的なアイデアは [FLM88] で構成されたルート格子 A_1 に付随する位数 2 の例外自己同型を A_k に付随する位数 $k+1$ の例外自己同型に拡張することである (一般の構成法 B などの詳細は [LS] 参照).

次の定理を述べるために必要な定義を与える. N を偶格子, f を N の自己同型とする. このとき, $N^f = \{v \in N \mid fv = v\}$ は f の固定点の部分格子であり, $N_f = \{v \in N \mid (v|N^f) = 0\}$ を f の **coinvariant 格子**という. このとき, N の共役な自己同型から作られる coinvariant 格子は同型であり, f の N_f への制限は fixed-point free である.

定理 3.2. [LS] g の位数が**奇素数と仮定**する. このとき, $V_L^{\hat{g}}$ が例外自己同型を持つための必要十分条件は次のいずれかを満たすことである.

- L が長さ $m/(p-1)$ で *Hamming weight* $m/(p-1)$ の符号語を持つ自己双対符号から 構成法 B で構成される.
- $p = 11$ または $p = 23$ であって, L はリーチ格子の自己同型の共役類 $11A$ または $23A$ に付随する *coinvariant* 格子と同型になる.

注意 3.3. 本研究の最初の動機は定理 *3.1* を証明し, リーチ格子の自己同型の共役類 $2A$, $2C$, $3B$, $4C$, $5B$, $6F$, $6G$, $7B$, $8E$, $10F$ の *coinvariant* 格子に付随する *orbifold VOA* の自己同型群の決定に応用することであった *([BLS22+])*. これら 10 個の *VOA* の自己同型群を用いて, 中心電荷 24 の正則 *VOA* の自己同型群の決定した *([BLS])*.

4 構成法 B

ここでは $\mathbb{Z}_p$ 上の符号に付随する構成法 B について説明する. もっと一般の $\bigoplus_{i=1}^{t} \mathbb{Z}_{k_i}$ の部分群に付随する構成法 B については [LS] を参照せよ.

p を素数とし, R を A_{p-1} 型のルート格子の t 個の直和とする. すると $R^*/R \cong \mathbb{Z}_p^t$ である. ここで R^* は双対格子である. $\nu : R^* \to R^*/R$ を自然な写像とし, $C \subset R^*/R$ に対して, $L_A(C) = \nu^{-1}(C)$ とおく. すると $L_A(C)$ の階数は $t(p-1)$ である. A_{p-1} の単純ルートを固定し, ρ を Weyl vector とする. $\chi = (1/p)(\rho, \ldots, \rho)$ とおき,

$$L_B(C) = \{v \in L_A(C) \mid (v|\chi) \in \mathbb{Z}\}$$

とする. この格子の構成を **構成法 B** と呼ぶことにする. $L_B(C)$ の階数も $t(p-1)$ である.

補題 4.1. p を奇素数とする.

- $L_B(C)$ が偶であることの必要十分条件は C が自己双対.
- $|L_A(C) : L_B(C)| = p$.
- $C^\perp$ が *(Hamming) weight* t の符号語を持つならば, R の *Coxeter element* は位数 p の *fixed-point free* な $L_B(C)$ の自己同型となる.

注意 4.2. $p = 2$ の場合は *2* 章で述べた構成法 B と一致し, *[CS99]* と同じである. 一方で, $p > 2$ の場合は *[CS99]* の構成法 B とは異なる構成であり, ほとんど研究されていないように思われる.

次の命題と定理は完全に組み合わせ論的な議論で証明される. ただし, 定理 4.4 の条件は次章で述べるように VOA の考察から得られた.

命題 4.3. L を偶格子とする. ある自己双対符号 $C \subset \mathbb{Z}_p^t$ に対して $L \cong L_A(C)$ となるための必要十分条件は L が A_{p-1} 型のルート格子の t 個の直和を含むことである.

定理 4.4. [LS] L をルートを持たない階数 m の偶格子とする. p を奇素数とする. このとき, 次の 2 つは同値である.

- 次を満たす $\lambda + L \in L^*/L$ と *fixed-point free* な L の自己同型 g が存在する.
  - $p\lambda \in L$;
  - $N = \mathbb{Z}\{\lambda, L\}$ としたとき, $|\{v \in N \mid |v|^2 = 2\}| = pm$;
  - $g(\lambda + L) = \lambda + L$.
- ある $\mathbb{Z}_p$ 上の長さ $m/(p-1)$ の自己双対符号 C で $C^\perp$ が *(Hamming) weight* $m/(p-1)$ の符号語を持ち $L \cong L_B(C)$ となるものが存在する.

注意 4.5. *[Sh04]* で $p = 2$ の場合に同様の $L_B(C)$ で得られる格子の特徴づけの結果が得られている.

5 定理 3.2 の証明の概略

$|g| = p$ が奇素数であり, $V_L^{\hat{g}}$ が例外自己同型 σ を持つと仮定する.

- V_L の既約 $V_L^{\hat{g}}$-部分加群 $V_L^{\hat{g}}(1) = \{v \in V_L \mid \hat{g}(v) = \exp(2\pi\sqrt{-1}/p)v\}$ を考える.
- 命題 1.2 より, $V_L^{\hat{g}}(1) \circ \sigma$ は V_L の既約 $V_L^{\hat{g}}$-部分加群と同型でない. すると, [DRX17] による既約 $V_L^{\hat{g}}$-加群の分類から, 次の 2 通りのうち少なくとも 1 つが起こる.

  (I) $V_L^{\hat{g}}(1) \circ \sigma \cong V_{\lambda+L}(j)$;
  (II) $V_L^{\hat{g}}(1) \circ \sigma \cong V_L^T[\hat{g}^s](j')$.

- (I) の場合は両辺の共形重み 1 の部分空間の次元を比較することで, $\lambda + L$ と g が定理 4.4 の前半の条件を満たすことがわかり, $L \cong L_B(C)$ となる.
- (II) の場合は, $V_L^T[\hat{g}^s](j')$ が単純カレントとなる. この既約加群の量子次元が 1 であるので, 指標の計算から L に関するかなりの制約が得られる. 特に, $(p, \mathrm{rank}L) = (3,12), (3,18), (5,16), (5,20), (7,18), (11,20), (23,22)$ のいずれかとなる. さらに L^*/L の構造も決まり, 上の 7 個のパラメータからルートを持たない偶格子が一つに決まることがわかる. 特に, これら 7 個の偶格子はすべてリーチ格子の coinvariant 格子となり, 最初の 5 個の場合は構成法 B で得られる.

注意 5.1. $p = 2$ の場合は, *(II)* の状況から, L が $\sqrt{2}E_8$ と階数 16 の *Barnes-Wall* 格子のいずれかと同型がわかる *([Sh04])*. したがって, *(*現在知られている*) (II)* が起こる格子はリーチ格子の自己同型に付随する *coinvariant* 格子だけである.

6 今後の課題

[LS] では g や L にいくつかの仮定をしている. これらの仮定を外して何が起こるかを考察するのは一つの研究の方向性だと思われる. 例えば, 次の設定が考えられる.

- $|g|$ が素数でない場合

実際に, $|g|$ が素数でない場合に, $V_L^{\hat{g}}$ が例外自己同型を持ち (II) が起こる例を $L = \Lambda_g$ として見つけている ([BLS22+]).

特に, 現在知られている限り, ルートを持たない偶格子 L で前節の (II) が起こるのは L がリーチ格子の coinvariant 格子のみであり, これが $|g|$ が素数でない場合でも正しいかどうかには興味がある.[注 8]

さらに, (II) が起こる場合は対称性が高い場合であるため, これらの場合に全自己同型群の構造がどうなるかは興味がある.

また, 次について考えてみると良いと思う.

[注 8] リーチ格子の coinvariant 格子がすべての例外を与えているならば、面白い結果だと思う.

- L がルートを持つ場合[注 9]

この場合は, $L_B(C)$ の特徴づけの証明が複雑になると思われる. また, $|g| = 2$ の場合で $L = E_8$ ならば (II) が起こるので, リーチ格子の coinvariant 格子でない (II) を満たす例がある. 他にもリーチ格子の coinvariant 格子から得られない (II) を満たす格子があるかどうかには興味がある.

今回の研究で扱った $L_B(C)$ で C が binary code の場合は [KKM91] での研究成果がある. したがって, 次の問題が考えられる.

- [KKM91] の結果を $p > 2$ の場合の $L_B(C)$ へ拡張せよ.

これは代数的組合せ論の範疇の問題の一つである. 特に, [Sh12] では [KKM91] を参考に, 二元符号 C に対して, $L_B(C) \cong L_B(C')$ がいつ起こるかを考え, 必要十分条件として $C \cong C'$ or $\{C, C'\} = \{e_8^2, d_{16}^+\}$ を得ている. 同様な同型問題を $\mathbb{Z}_p$-符号 C に対しても考えてみるのは一つの問題である.

参考文献

[BLS22+] K. Betsumiya, C.H. Lam and H. Shimakura, Automorphism groups of cyclic orbifold vertex operator algebras associated with the Leech lattice and some non-prime isometries; arXiv:2105.04191, (to appear in *Israel J. Math*).

[BLS] K. Betsumiya, C.H. Lam and H. Shimakura, Automorphism groups and uniqueness of holomorphic vertex operator algebras of central charge 24; arXiv:2203.15992.

[CM] S. Carnahan and M. Miyamoto, Regularity of fixed-point vertex operator subalgebras; arXiv:1603.05645.

[CS99] J.H. Conway and N.J.A. Sloane, Sphere packings, lattices and groups, 3rd Edition, Springer, New York, 1999.

[DJX13] C. Dong, X. Jiao and F. Xu, Quantum dimensions and quantum Galois theory. *Trans. Amer. Math. Soc.* **365** (2013), 6441-6469.

[DRX17] C. Dong, L. Ren and F. Xu, On Orbifold Theory, *Adv. Math.* **321** (2017), 1–30.

[EMS20] J. van Ekeren, S. Möller and N. Scheithauer, Construction and classification of holomorphic vertex operator algebras, *J. Reine Angew. Math.*, **759** (2020), 61–99.

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

[Gr98] R.L. Griess, A vertex operator algebra related to E_8 with automorphism group $\mathrm{O}^+(10, 2)$, *Ohio State Univ. Math. Res. Inst. Publ.* **7** (1998), 43–58.

[KKM91] M. Kitazume, T. Kondo and I. Miyamoto, Even lattices and doubly-even codes, *J. Math. Soc. Japan* **43** (1991), 67–87.

[LS] C.H. Lam and H. Shimakura, Extra automorphisms of cyclic orbifolds of lattice vertex operator algebras; arXiv:2103.08085.

[注 9] $|g| = 2$ の場合は [Sh06] で研究されている.

[Mi15] M. Miyamoto, C_2-cofiniteness of cyclic-orbifold models, *Comm. Math. Phys.* **335** (2015), 1279–1286.

[Sh04] H. Shimakura, The automorphism group of the vertex operator algebra V_L^+ for an even lattice L without roots, *J. Algebra* **280** (2004), 29–57.

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

[Sh12] H. Shimakura, On isomorphism problems for vertex operator algebras associated with even lattices, *Proc. Amer. Math. Soc.* **140** (2012), 3333–3348.

有限群から得られる一般化アレキサンダーカンドルについて

栗原　大武
山口大学大学院創成科学研究科
kurihara-hiro@yamaguchi-u.ac.jp

1　序

今回の講演および報告集の内容は前回 2021 年のシンポジウムの続編であり，東谷 章弘氏（大阪大学）との共同研究に基づくものである．

カンドルの概念は元々 Joyce [4] によって結び目理論の文脈から導入された．集合 Q と Q 上の二項演算 $*\colon Q\times Q\to Q$ の組 $(Q,*)$ が**カンドル**とは以下の条件を満たすことである：

(Q1) $x*x=x$ for $\forall x\in Q$;

(Q2) for $\forall x,y\in Q$, $\exists! z\in Q$ such that $z*y=x$;

(Q3) for $\forall x,y,z\in Q$, $(x*y)*z=(x*z)*(y*z)$.

上記の 3 つの公理は結び目理論における Reidemeister 変形にそれぞれ対応する．一方でこの公理を対称空間論の類似としてとらえなおすこともできる．$(Q,*)$ をカンドルとするとき，$x\in Q$ における**点対称** $s_x : Q\to Q$ を $s_x(y)=y*x$ により定める．すると (Q1)∼(Q3) は以下のように言い直すことができる：

(Q1') $s_x(x)=x$ for $\forall x\in Q$;

(Q2') for $\forall x\in Q$, s_x は Q 上の全単射写像;

(Q3') $s_x\circ s_y=s_{s_x(y)}\circ s_x$ for $\forall x,y\in Q$.

対称空間は (Q1')∼(Q3') を満たすことが知られているので，対称空間はカンドルである (cf. [4])．対称空間論の立場からのカンドルの研究も多くあり (例えば [3, 5, 7] など)，これらの研究では特に**等質カンドル**が主な研究対象である．等質カンドルの定義や性質は 3 節で扱う．

カンドルは特別な二項演算をもつ集合であり，同じ二項演算をもつ群と似た性質もあればそうでない場合もある．この報告集では，特に群に“近い” 性質をもつ一般化アレキサンダーカンドルについて，様々な性質を調べた結果を記載する．一般化アレキサンダーカンドルは群 G と G の自己同型写像 ψ の組 (G, ψ) から得られる (定義は 3.2 節で与える)．一般化アレキサンダーカンドルについての大きな問題として，問 3.3 が考えられる．この問いに関して，Higashitani–Kurihara [1] では G が対称群 $\mathfrak{S}_n$ のとき n が小さい場合の一部解決を与えた．さらに [1] の後続の共同研究 (Higashitani–Kurihara [2]) として，条件 (P1), (P2) を導入し，条件 (P1), (P2) を満たす一般化アレキサンダーカンドルのクラスに対しては，二つのカンドルがカンドル同型であるための必要十分条件を与えることができた．さらにこの必要十分条件を用いていくつかの系を得ることができた．

この報告集の内容は 4 節までが前回の報告集 [8] の内容のまとめである．そして 5 節以降で最近 [2] によって得られた内容を紹介する．

2　準備

以降では，カンドルの演算 $*$ の代わりに点対称の記号 s を用いて，カンドルを (Q, s) のように表す．また点対称 s を省略して，カンドルを単に Q と書くこともある．

2.1　カンドルの記号の準備

(Q, s) と (Q', s') をカンドルとする．写像 $f : Q \to Q'$ が以下の条件を満たすとき，f を**カンドル準同型写像**と呼ぶ：

$$f \circ s_x = s'_{f(x)} \circ f \quad \text{for any } x \in Q.$$

さらにカンドル準同型 f が全単射であるとき，f を**カンドル同型写像**と呼ぶ．もし Q と Q' の間にカンドル同型写像が存在するとき，Q と Q' は**カンドル同型**であるといい，$Q \cong_{\mathrm{qu}} Q'$ で表す．$\mathrm{Aut}_{\mathrm{qu}}(Q, s)$ (もしくは単に $\mathrm{Aut}_{\mathrm{qu}}(Q)$) を (Q, s) 上のカンドル自己同型写像の集合とし，これを (Q, s) の**カンドル自己同型群**と呼ぶ．カンドルの公理 (Q3') から $s_x \in \mathrm{Aut}_{\mathrm{qu}}(Q)$ であることがわかる．$\mathrm{Inn}_{\mathrm{qu}}(Q, s)$ (もしくは単に $\mathrm{Inn}_{\mathrm{qu}}(Q)$) を $\{s_x : x \in Q\}$ で生成される $\mathrm{Aut}_{\mathrm{qu}}(Q)$ の部分群を (Q, s) の**カンドル内部自己同型群**と呼ぶ．

2.2 群の記号の準備

G を単位元 e をもつ群とする．$\mathrm{Aut}_{\mathrm{gr}}(G)$ を G の自己同型群とする．2つの群 G, G' が同型のとき，$G \cong_{\mathrm{gr}} G'$ で表す．

$g, h \in G$ に対して, $g^h = hgh^{-1}$ と書くことにする．$\mathrm{Inn}_{\mathrm{gr}}(G)$ を G の内部自己同型群とする．$\psi \in \mathrm{Aut}_{\mathrm{gr}}(G)$ が**外部自己同型写像**とは, $\psi \notin \mathrm{Inn}_{\mathrm{gr}}(G)$ であることとする．

$\psi \in \mathrm{Aut}_{\mathrm{gr}}(G)$ に対して,

$$\mathrm{Fix}(\psi, G) = \{g \in G : \psi(g) = g\}$$

とおく．なお，$\mathrm{Fix}(\psi, G)$ は G の部分群であり，ψ が内部自己同型，つまり $\psi = (\cdot)^g$ と書けるときには，$\mathrm{Fix}((\cdot)^g, G)$ は g の中心化群 $C_G(g)$ と一致する．

3 等質カンドル

3.1 等質カンドルとカンドル三つ組

Q をカンドルとする．Q に $\mathrm{Aut}_{\mathrm{qu}}(Q)$ が推移的に作用するとき，Q を**等質**であるという．またもっと強い条件として，Q に $\mathrm{Inn}_{\mathrm{qu}}(Q)$ が推移的に作用するとき，Q を**連結**であるという．

定義 3.1 ([3, Definition 3.1])**.** G を群として，K を G の部分群とする．また $\psi \in \mathrm{Aut}_{\mathrm{gr}}(G)$ とする．これらが $K \subset \mathrm{Fix}(\psi, G)$ を満たすとき，三つ組 (G, K, ψ) をカンドル三つ組と呼ぶ.

等質カンドル (Q, s) からカンドル三つ組を得ることができる．$G = \mathrm{Aut}_{\mathrm{qu}}(Q, s)$ とし，$x \in Q$ を一つ固定して $K = \{f \in \mathrm{Aut}_{\mathrm{qu}}(Q, s) : f(x) = x\}$ とおく．さらに $\psi : G \to G$ を $f \mapsto s_x \circ f \circ s_x^{-1}$ で定めると，(G, K, ψ) はカンドル三つ組になる．上記の証明は例えば [3, Proposition 3.3] などを参考にしていただきたい.

逆にカンドル三つ組 (G, K, ψ) から以下のようにして等質カンドルを得ることができる：$G/K = \{[g] : g \in G\}$ を G の K による左剰余空間を表すことにして，G/K 上に点対称を

$$s_{[g]}([h]) := [g\psi(g^{-1}h)] \quad ([g], [h] \in G/K)$$

によって定めるとこれは well-defined であり, カンドルの公理を満たす．さらにこのカンドル $(G/K, s)$ は等質である．上記の証明は例えば [3, Proposition 3.2] などを参考にしていただきたい．今後このカンドルを $Q(G, K, \psi)$ で表すことにする．

3.2　一般化アレキサンダーカンドル

カンドル三つ組の K を $\{e\}$ として取ると，どのような G と ψ に対しても，$(G, \{e\}, \psi)$ は必ずカンドル三つ組になる．これから得られる等質カンドルは $Q = G$ であり，点対称は

$$s_g(h) = g\psi(g^{-1}h) \quad \text{for any } g, h \in G$$

となる．このカンドルを**一般化アレキサンダーカンドル**と呼び，$Q(G, \psi)$ で表す．なお G がアーベル群のとき，アレキサンダーカンドルと呼ばれている．

等質カンドルの研究には，以下の命題から一般化アレキサンダーカンドルを調べることが重要であると思われる．

命題 3.2 (Higashitani–K. [1])**.** $\psi, \psi' \in \mathrm{Aut}_{\mathrm{gr}}(G)$ とし，$K = \mathrm{Fix}(\psi, G)$, $K' = \mathrm{Fix}(\psi', G)$ とする．もし $Q(G, \psi) \cong_{\mathrm{qu}} Q(G, \psi')$ ならば, $Q(G, K, \psi) \cong_{\mathrm{qu}} Q(G, K', \psi')$ である．

証明は [1] を参考にされたい．

有限群 G に対して，$\mathcal{Q}(G)$ を $Q(G, \psi)$ の同型類の集合とする．つまり，

$$\mathcal{Q}(G) := \{Q(G, \psi) : \psi \in \mathrm{Aut}_{\mathrm{gr}}(G)\}/\cong_{\mathrm{qu}}$$

とする．以下の問題がこの報告集の主題である．

問題 3.3. 与えられた G に対して，$\mathcal{Q}(G)$ を決定せよ．

以下の命題は $\mathcal{Q}(G)$ を大雑把に把握するのに役に立つ．

命題 3.4 (Higashitani–K. [1])**.** $\psi, \psi' \in \mathrm{Aut}_{\mathrm{gr}}(G)$ は共役とする．つまり $\psi' = \tau \circ \psi \circ \tau^{-1}$ となる $\tau \in \mathrm{Aut}_{\mathrm{gr}}(G)$ が存在すると仮定する．このとき，$Q(G, \psi) \cong_{\mathrm{qu}} Q(G, \psi')$ が成り立つ．

したがって $\mathcal{Q}(G)$ は $\mathrm{Aut}_{\mathrm{gr}}(G)$ の共役類の集合と同じになるかということが気になる．しかし，そうはならない例が存在する．C_n を位数 n の巡回群とする．Nelson [6] は $\mathcal{Q}(C_n)$ を決定した．以下で $\mathcal{Q}(C_n)$ について説明する．まず $\mathrm{Aut}(C_n) \cong_{\mathrm{gr}} U(C_n)$ であることが知られている．ただし，$U(C_n) = \{x \in C_n : x \text{ is coprime to } n\}$ であり，$a \in U(C_n)$ に対して，$x \mapsto ax$ によって C_n 上に自己同型が定まる．この a に関するアレキサンダーカンドルを $Q(C_n, \times a)$ で表す．$N(n, a) = \frac{n}{\gcd(n, 1-a)}$ とおくとき，$Q(C_n, \times a) \cong_{\mathrm{qu}} Q(C_n, \times b)$ の必要十分条件は $N(n, a) = N(n, b)$ かつ $a \equiv b \pmod{N(n, a)}$ である．つまり，$\mathcal{Q}(C_n)$ は完全に特徴づけられている．

例えば，$Q(C_9, \times 4) \cong_{\mathrm{qu}} Q(C_9, \times 7)$ である．一方で，$U(C_n)$ は可換群だから，$U(C_n)$ の共役類は $U(C_n)$ 自身である．したがって，この例は $\mathrm{Aut}_{\mathrm{gr}}(C_n)$ の共役類と $\mathcal{Q}(C_n)$ は一対一に対応しないことを示している．

問題 3.3 の解決に向けて，等質カンドルや，その中でも $Q(G, \psi)$ の不変量をいくつか紹介する．この節では G は有限群を表すものとする．以下では，命題 3.4 や [1] に記載しているいくつかの不変量を少し一般化した形で紹介する．

定理 3.5 (cf. Higashitani–K. [1])**.** G, G' を有限群とし，$\psi \in \mathrm{Aut}(G)$, $\psi' \in \mathrm{Aut}(G')$ とし，$Q = Q(G, \psi)$, $Q' = Q(G', \psi')$ とする．

(*a*) $\tau \circ \psi = \psi' \circ \tau$ をみたす群同型写像 $\tau\colon G \to G'$ が存在するならば，$Q \cong_{\mathrm{qu}} Q'$ が成り立つ．

(*b*) もし $Q \cong_{\mathrm{qu}} Q'$ ならば以下が成り立つ．

- $|G| = |G'|$;
- $\mathrm{ord}_{\mathrm{Aut}(G)} \psi = \mathrm{ord}_{\mathrm{Aut}(G')} \psi'$;
- $|\mathrm{Fix}(\psi, G)| = |\mathrm{Fix}(\psi', G')|$;
- $\mathrm{Inn}_{\mathrm{qu}}(Q) \cong_{\mathrm{gr}} \mathrm{Inn}_{\mathrm{qu}}(Q')$;
- $Q(G, \psi^i) \cong_{\mathrm{qu}} Q(G', \psi'^i)$ *for any* $i \in \mathbb{Z}_{>0}$.

4 単位連結成分 P

G を有限群とし，$\psi \in \mathrm{Aut}_{\mathrm{gr}}(G)$ を恒等写像でないものとする．また $Q = Q(G, \psi)$ とする．このとき，$P = P(Q)$ を $\mathrm{Inn}_{\mathrm{qu}}(Q)$ による単位元 e の軌道とする．つまり，

$$P = \{x \in G : \exists a_1, \ldots, a_r \in G \text{ s.t. } x = s_{a_1} \circ \cdots \circ s_{a_r}(e)\}$$

とする．ここでは P を Q の**単位連結成分**と呼ぶことにする．前回の報告集で，P について以下の性質が成り立つことを紹介した．

定理 4.1. P について以下が成り立つ．

(*a*) P は G の正規部分群であり，$\psi|_P$ は P 上の自己同型写像である．

(*b*) $Q(P, \psi|_P)$ は Q の部分カンドルになる．

(*c*) $\psi|_{P_Q}$ は P_Q 上のカンドル自己同型写像である．

定理 4.2. G, G' をそれぞれ単位元 e, e' をもつ有限群とする．$\psi \in \mathrm{Aut}_{\mathrm{gr}}(G)$, $\psi' \in \mathrm{Aut}_{\mathrm{gr}}(G')$ に対して，$Q = Q(G, \psi)$, $Q' = Q(G', \psi')$ とおく．また $P = P(Q)$, $P' = P(Q')$ とおく．$Q(G, \psi) \cong_{\mathrm{qu}} Q(G', \psi')$ を仮定し，$f : Q(G, \psi) \to Q(G', \psi')$ を $f(e) = e'$ であるようなカンドル同型写像とする（このような f は必ず存在する）と次が成り立つ．

(*a*) $f|_P$ は P と P' の間のカンドル同型写像である．したがって $P \cong_{\mathrm{qu}} P'$ である．

(*b*) $f|_P$ は P と P' の間の群同型写像である．したがって $P \cong_{\mathrm{gr}} P'$ である．

(*c*) $\psi' \circ f|_P = f|_P \circ \psi$ が成り立つ．

系 4.3. G が有限単純群のとき，$\mathcal{Q}(G)$ と $\mathrm{Aut}_{\mathrm{gr}}(G)$ の共役類集合の間に一対一対応がある．

さらに系 4.3 を用いれば，[1] の主結果は一般の n の場合に拡張され，対称群に対しての問 3.3 は完全に解決される．

系 4.4. $\mathcal{Q}(\mathfrak{S}_n)$ と $\mathrm{Aut}_{\mathrm{gr}}(\mathfrak{S}_n)$ の共役類集合の間に一対一対応がある．

5　新しい結果

この節では，[8] 以降で得られた新たな結果を紹介する．詳細は [2] に記載予定である．

まずは一般化アレキサンダーカンドルのカンドル内部自己同型群の構造を P を用いて記述する．以下の命題 5.1, 5.2 は [1] で対称群の場合に示された結果の一般化となっている．

命題 5.1 (Higashitani–K.)**.** $Q = Q(G, \psi)$ に対して，$P = P(Q)$，$m = \mathrm{ord}_{\mathrm{Aut}_{\mathrm{gr}}(G)}(\psi)$ とおく．このとき，

$$\mathrm{Inn}_{\mathrm{qu}}(Q) \cong_{\mathrm{gr}} P \rtimes_{\phi} C_m$$

が成り立つ．ただしこの半直積 $\rtimes_{\phi}$ は $\phi : C_m \to \mathrm{Aut}_{\mathrm{gr}}(P)$, $i \mapsto \psi|_P^i$ から定まるものとする．

命題 5.2 (Higashitani–K.)**.** さらに，もし P の中心が自明ならば，次が成り立つ：

- $\psi|_P \in \mathrm{Inn}_{\mathrm{gr}}(P)$ ならば，$P \rtimes_{\phi} C_m \cong_{\mathrm{gr}} P \times C_m$;
- $\psi|_P \notin \mathrm{Inn}_{\mathrm{gr}}(P)$ ならば，$P \rtimes_{\phi} C_m \ncong_{\mathrm{gr}} P \times C_m$.

次に今回の主結果に用いられる条件 (P1), (P2) について説明をする．$P(Q) = Q(P, \psi|_P)$ は一般化アレキサンダーカンドルなので, $P^2 := P(P(Q))$ を定義することができる．P^2 に関して以下の二つの条件を考える．

(P1) P^2 は G の正規部分群である．

(P2) $P^2 = \{s_p(e) : p \in P\}$ が成り立つ．

注意 5.3. 一般的には *(P1), (P2)* は成り立たない．さらに *(P1), (P2)* は独立な条件であることが以下の例からわかる．*8* 元数群 Q_8 上の位数 *3* の自己同型写像 ψ から得られる一般化アレキサンダーカンドル $Q(Q_8, \psi)$ は，*(P1)* は満たさないが，*(P2)* は満たす．一方で，$G' = \mathfrak{S}_3 \times \mathfrak{S}_3$ 上の自己同型写像 $\tau' \colon G' \to G'$ を $\psi'(a, b) := (b, a)$ で定めると，この一般化アレキサンダーカンドル $Q(G', \psi')$ は，*(P1)* は満たすが，*(P2)* は満たさない．

命題 5.4 (Higashitani–K.)**.** 一般化アレキサンダーカンドル $Q = Q(G, \psi), Q' = Q(G', \psi')$ に対して，$P^2 = P(P(Q)), P'^2 = P(P(Q'))$ とおく．このとき，$Q \cong_{\mathrm{qu}} Q'$ ならば次が成り立つ：

(*i*) $P^2 \cong_{\mathrm{qu}} P'^2$ かつ $P^2 \cong_{\mathrm{gr}} P'^2$*;*

(*ii*) Q は *(P1)* を満たす $\iff$ Q' は *(P1)* を満たす*;*

(*iii*) Q は *(P2)* を満たす $\iff$ Q' は *(P2)* を満たす*.*

つまり P^2 と (P1) と (P2) はカンドル不変量である．

Example 5.5. アレキサンダーカンドル $Q(G, \psi)$ は *(P1), (P2)* を満たす．

Proof.

- (P1) を満たすことは，G がアーベル群であることから自明．
- $s_x(e) = x + \psi(-x + e) = (\mathrm{Id}_G - \psi)(x)$ より，$\rho = \mathrm{Id}_G - \psi$ とおくと， $s_x(e) = \rho(x)$．さらにこれより $P = \mathrm{Im}\,\rho$ である．また $P^2 = \mathrm{Im}\,\rho^2 = \{\rho(p) : p \in \mathrm{Im}\,\rho\} = \{s_p(e) : p \in P\}$ より (P2) が言える．

□

アーベル群以外にも，二面体群から得られる一般化アレキサンダーカンドルは (P1), (P2) をみたす．そのほかにも (P1), (P2) をみたす一般化アレキサンダーカンドルは存在する．

以下が (P1), (P2) を満たす一般化アレキサンダーカンドルのクラスにおける同値条件であり，この報告集の主結果である．

定理 5.6 (Higashitani–K.)**.** 一般化アレキサンダーカンドル $Q = Q(G, \psi), Q' = Q(G', \psi')$ について，Q と Q' はそれぞれ (P1), (P2) を満たすと仮定する．このとき $Q \cong_{\mathrm{qu}} Q'$ であることの必要十分条件は以下の (A), (B), (C) を満たすことである：

(A) $|G| = |G'|$;

(B) $|\operatorname{Fix}(\psi, G)| = |\operatorname{Fix}(\psi', G')|$;

(C) 以下を満たす群同型写像 $h\colon P = P(Q) \to P' = P(Q')$ が存在する;

- *(C-1)* $h \circ \psi|_P = \psi'|_{P'} \circ h$;
- *(C-2)* 任意の $a \in G$ に対して，$h(s_a(e)) = s'_{a'}(e')$ を満たす $a' \in G'$ が存在する.

証明のアイディア：

- (C-1) により $h\colon P \to P'$ はカンドル同型写像である.
- (A), (B), (C-2) により特別な全単射 $k\colon G/P \to G'/P'$ を作り，$k \times h\colon G \cong G/P \times P \to G' \cong G'/P' \times P'$ がカンドル同型写像であることを示せばよい.

定理 5.6 から以下の 4 つの系が得られる．この報告集では証明の細部は割愛する．詳しくは [2] に記載する予定である.

系 5.7 (Nelson [6] の Theorem 2.1 の群論的な解釈)**.** 有限アーベル群 G, G' に対して，$Q = Q(G, \psi), Q' = Q(G', \psi')$ とし，$\rho = \mathrm{Id}_G - \psi, \rho' = \mathrm{Id}_{G'} - \psi'$ とおく．このとき $Q \cong_{\mathrm{qu}} Q'$ であることの必要十分条件は次を満たすことである：

(A') $|G| = |G'|$;

(C') $h \circ \psi|_{\operatorname{Im}\rho} = \psi'|_{\operatorname{Im}\rho'} \circ h$ を満たす群同型写像 $h : \operatorname{Im}\rho \to \operatorname{Im}\rho'$ が存在する.

Proof.

- $\operatorname{Fix}(\psi, G) = \ker\rho$ より (C') から (B) が従う.
- $h(s_a(e)) = h(\rho(a))$ より (C') から (C-2) が従う.

□

D_n を位数 $2n$ の二面体群とする．このとき $\mathrm{Aut}_{\mathrm{gr}}(D_n)$ と $\{(a, b) : a \in C_n^\times, b \in C_n\}$ が一対一に対応することが知られている．以降 (a, b) に対応する D_n の自己同型写像を $\varphi_{a,b}$ で表す.

系 5.8. *$a, a' \in C_n^\times$, $b, b' \in C_n$ とし，$d = \gcd(n, 1-a, b)$ and $d' = \gcd(n, 1-a', b')$ とおく．このとき $Q(D_n, \varphi_{a,b}) \cong_{\mathrm{qu}} Q(D_n, \varphi_{a',b'})$* であることの必要十分条件は次を満たすことである：

(B') $|\operatorname{Fix}(\varphi_{a,b}, D_n)| = |\operatorname{Fix}(\varphi_{a',b'}, D_n)|$;

(C') $d = d'$;

(C-1') $a \equiv a' \pmod{\frac{n}{d}}$.

系 5.9. C_{2n} を位数 $2n$ の巡回群とする．このとき任意の $a \in C_{2n}^{\times}$ に対して，$Q(C_{2n}, \times a)$ とカンドル同型になる二面体群から得られる一般化アレキサンダーカンドル $Q(D_n, \varphi_{a',b'})$ が存在する．つまり，$\mathcal{Q}(C_{2n}) \subset \mathcal{Q}(D_n)$ である．

n を自然数とし，要素数 n の一般化アレキサンダーカンドルの同型類を $\mathcal{Q}_{GAQ}(n)$ で表す．つまり

$$\mathcal{Q}_{GAQ}(n) := \{Q(G, \psi) : |G| = n,\ \psi \in \mathrm{Aut}_{\mathrm{gr}}(G)\}/\cong_{\mathrm{qu}}$$

とする．また $q(n) := |\mathcal{Q}_{GAQ}(n)|$ とする．$q(n)$ の決定は問 3.3 の発展的な問題であるが，n が小さい場合は $q(n)$ を決定することができた．

系 5.10. n が *15* 以下の $q(n)$ は下の表の通りである．

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$q(n)$	1	1	2	3	4	3	6	9	11	5	10	11	12	7	8

注意 5.11. $n = 16$ のとき，*(P2)* をみたさない二つの一般化アレキサンダーカンドル $Q(C_2 \times Q_8, \psi)$, $Q((C_4 \times C_2) \rtimes C_2, \psi')$ があり，これらの様々なカンドル不変量はすべて一致する．しかし，*Theorem 5.6* の仮定を満たさないので，これらがカンドル同型かどうか判定できていない．

参考文献

[1] A. Higashitani and H. Kurihara, Homogeneous quandles arising from automorphisms of symmetric groups. *arXiv preprint* arXiv:2005.12057. https://arxiv.org/abs/2005.12057

[2] A. Higashitani and H. Kurihara, generalized Alexander quandles of finite groups and their characterizations. 準備中.

[3] Y. Ishihara and H. Tamaru, Flat connected finite quandles. *Proc. Amer. Math. Soc.* **144** (2016), no. 11, 4959–4971. https://doi.org/10.1090/proc/13095

[4] D. Joyce, A classifying invariant of knots, the knot quandle. *J. Pure Appl. Algebra* **23** (1982), no. 1, 37–65. https://doi.org/10.1016/0022-4049(82)90077-9

[5] S. Kamada, H. Tamaru, and K. Wada, On classification of quandles of cyclic type. *Tokyo J. Math.* **39** (2016), no. 1, 157–171. https://doi.org/10.3836/tjm/1459367262

[6] S. Nelson, Classification of finite Alexander quandles. In *Proceedings of the Spring Topology and Dynamical Systems Conference*. 2003, 245–258

[7] L. Vendramin, Doubly transitive groups and cyclic quandles. *J. Math. Soc. Japan* **69** (2017), no. 3, 1051–1057. https://doi.org/10.2969/jmsj/06931051

[8] 栗原大武, 有限群から得られる等質カンドルについて. 第 37 回代数的組合せ論シンポジウム報告集 (2021), 68–80.

On tight 3-designs in Hamming association schemes

須田　庄
防衛大学校　総合教育学群　数学教育室
ssuda@nda.ac.jp

1　Tight 3-designs in Hamming association schemes

本研究ではハミングアソシエーションスキーム $H(n,q)$ の tight 3-デザインの存在性に関する新たな必要条件を与える。考えている設定・道具は 2019 年に開催された本シンポジウムの著者による報告集とほぼ同じである。

野田 [9] による $H(n,q)$ の tight 4-デザインに関する部分的な分類結果の後、[10] で $H(n,q)$ の tight $3,5$-デザインに関する部分的な分類結果（5-デザインの場合は完全な分類結果）が得られた。tight 3-デザインの部分的な分類結果は以下のとおりである。

定理 1. C をハミングアソシエーションスキーム $H(n,q)$ の *tight* 3-デザインとしたとき、次のいずれかが成り立つ。

1. $(|C|,n,q)=(2n,n,2)$, n は 4 の倍数
2. $(|C|,n,q)=(q^3,q+2,q)$, q は偶数

1 のパラメータの場合の存在性は位数が n のアダマール行列の存在性と同値である。本研究の主結果は以下の通りである。

定理 2. C をハミングアソシエーションスキーム $H(q+2,q)$ の *tight* 3-デザインとする。このとき、$q>2$ ならば q は 4 の倍数である。

本研究は Alexander Gavrilyuk との共同研究に基づくものであり、定理 2 の詳細な証明はいずれ公開される [5] を参照されたい。

2　Association schemes

X を有限集合、$R_0,R_1,\dots,R_D$ を $X\times X$ の空でない部分集合とし、A_i $(0\le i\le D)$ をグラフ (X,R_i) の隣接行列とする。このとき、$(X,\{R_i\}_{i=0}^D)$ がクラスが D の（対称）アソシエーションスキームであるとは、次の条件を満たすときとする：

1. $A_0=I_{|X|}$ (I_n はサイズが n の単位行列),
2. $\sum_{i=0}^D A_i=J_{|X|}$ (J_n は $n\times n$ の成分がすべて 1 の行列),
3. $A_i^\top=A_i$ $(1\le i\le D)$,
4. 任意の i,j,k に対しある非負整数 p_{ij}^k が存在して、$A_iA_j=\sum_{k=0}^D p_{ij}^kA_k$ が成り立つ。

隣接行列で生成される実数体上のベクトル空間 $\mathcal{A} := \langle A_0, A_1, \ldots, A_D \rangle_{\mathbb{R}}$ は上記の条件 4 より代数となる (Bose-Mesner 代数と呼ばれる)。このとき、$\mathcal{A}$ は半単純な可換代数であるので、原始べき等元 $E_0 = \frac{1}{|X|} J_{|X|}, E_1, \ldots, E_D$ からなる $\mathcal{A}$ の基底が存在する。代数 $\mathcal{A}$ は成分ごとの積（$\circ$ と記す）についても閉じているので、クライン数 (Krein parameters) q_{ij}^k $(0 \leq i, j, k \leq D)$ を次で定める：$E_i \circ E_j = \frac{1}{|X|} \sum_{k=0}^{D} q_{ij}^k E_k$. ここで、クライン数は非負実数であることが知られている。集合 $\{A_0, A_1, \ldots, A_D\}$, $\{E_0, E_1, \ldots, E_D\}$ はベクトル空間 $\mathcal{A}$ の基底であるので、基底変換行列 $Q = (Q_{ij})_{i,j=0}^{D}$ を $E_i = \frac{1}{|X|} \sum_{j=0}^{D} Q_{ji} A_j$ で定める。この行列 Q を第二固有行列という。

アソシエーションスキーム $(X, \{R_i\}_{i=0}^{D})$ が Q-多項式 (Q-polynomial) であるとは、原始べき等元のある順序付け $E_1, \ldots, E_D$ が存在して、クライン数がなす行列 $L_1^* := (q_{1j}^k)_{k,j=0}^{D}$ が三重対角行列となり、対角成分の一つ上と一つ下の成分がすべて正となるときとする。$a_i^* = q_{1,i}^i$, $b_i^* = q_{1,i+1}^i$, $c_i^* = q_{1,i-1}^i$ とおいて、$\{b_0^*, b_1^*, \ldots, b_{D-1}^*; c_1^*, c_2^*, \ldots, c_D^*\}$ を Krein array という。Q-多項式アソシエーションスキームにおいて、Krein array からアソシエーションスキームのパラメータ $(p_{ij}^k, q_{ij}^k, Q = (Q_{ji})$ やここでは未定義な第一固有行列 $P = (P_{ji}))$ がすべて計算される。

例 1. $V = \{1, 2, \ldots, q\}$ $(q \geq 2)$ とし、$X = V^n$ とする。$x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in X$ に対して、x, y のハミング距離 $d(x, y)$ を $x_j \neq y_j$ となる j の個数とする。$i = 0, 1, \ldots, n$ に対して $R_i = \{(x, y) \mid x, y \in X, d(x, y) = i\}$ としたとき、$(X, \{R_i\}_{i=0}^{n})$ は、第二固有行列が $Q = (K_{n,q,j}(i))_{i,j=0}^{n}$ となる Q-多項式アソシエーションスキームとなる。ここで $K_{n,q,i}(x) = \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{x}{j} \binom{n-x}{i-j}$ は *Krawtchouk polynomial* である。これをハミングアソシエーションスキームといい、$H(n, q)$ と記す。

3 Designs in Q-polynomial association schemes and orthogonal arrays

Q-多項式アソシエーションスキーム $(X, \{R_i\}_{i=0}^{D})$ の頂点集合 X の部分集合 C が t-デザイン (t-design) であるとは、C の特性ベクトル $\chi = \chi_C$ が $\chi^\top E_i \chi = 0$ $(1 \leq i \leq t)$ を満たすこととする。

Q-多項式アソシエーションスキームがハミングアソシエーションスキームのとき、デザインの概念は組合せ論的に定義される直交配列と等価である。直交配列 $\mathrm{OA}(N, n, q, t)$ (orthogonal array) とは成分を $1, 2, \ldots, q$ とする $N \times n$ 行列 M であって次の性質をみたすものである：M の任意の $N \times t$ 部分行列の行ベクトルは $\{1, 2, \ldots, q\}^t$ の各要素を $\lambda := N/q^t$ 回含む。(ハミングアソシエーションスキーム $H(n, q)$ の部分集合 C に対して、C の各要素を行ベクトルとする行列を M としたとき、C が t-デザインであることとが M が直交配列 $\mathrm{OA}(|C|, n, q, t)$ であることが同値である。)

t-デザイン C に対して、$|C|$ の下界は Rao [11] により次の通り与えられた:

$$|C| \geq \begin{cases} \sum_{k=0}^{e} \binom{n}{k} (q-1)^k & \text{if } t = 2e, \\ \sum_{k=0}^{e} \binom{n}{k} (q-1)^k + \binom{n-1}{e} (q-1)^{e+1} & \text{if } t = 2e+1. \end{cases}$$

この不等式において等号が成立するデザインを tight という。

t-デザインから $(t-1)$-デザインを構成する、いわゆる derived design に関しては次が成り立つことが直ちにわかる。

定理 3. C を $H(n, q)$ の t-デザインとする。$i \in \{1, 2, \ldots, q\}$ に対して、C_i を次で定める：

$$C_i = \{(x_2, \ldots, x_n) \mid (i, x_2, \ldots, x_n) \in C\}.$$

このとき、次が成り立つ。

1. C_i は $H(n-1, q)$ の $(t-1)$-デザインである。

2. C が *tight* $(2e+1)$-デザインであれば、C_i は *tight* $2e$-デザインである。

Tight $(2e+1)$-デザインに関する Wilson 型の定理については次が知られている。$H(n,q)$ の部分集合 C に対して、$S(C)=\{d(x,y) \mid x,y \in C, x \neq y\}$ と定め、$|S(C)|$ を C の次数という。

定理 4 ([3, 10])**.** C を $H(n,q)$ の *tight* $(2e+1)$-デザインとする。

1. $n \in S(C), |S(C)| = e+1$ が成り立つ。
2. $S(C)=\{\alpha_1,\ldots,\alpha_e,\alpha_{e+1}=n\}$ とする。このとき、$|C|\prod_{i=1}^{e}(1-x/\alpha_i)=\sum_{j=0}^{e}K_{n-1,q,j}(x)$ が成り立つ。

Tight $2e$-デザインに関する Wilson 型の定理により、以下のパラメーターの $H(n,q)$ の tight $2e$-デザインは非存在が示されていた。(n が明記されていない場合は、任意の n に対して非存在が示された。)

- $e=2, q \neq 6$ [9], $e=2, q=6$ [6]
- $e \geq 3, q \geq 3$ [7],
- $e=3, q=2$ and $e=4,5,6, q=2, n \leq 10^9$ [8].

Tight $2e$-デザインの非存在の結果と定理 3 を組み合わせることで、分類が完成していない tight $(2e+1)$-デザインのパラメーターは

1. $e=1$
2. $q=2$, $e \geq 3$

となる。$e=1$ の場合に関する定理 1 を証明するために必要な定理を述べる。次の定理から、tight design はアソシエーションスキームの構造を持つことが知られている。次数が s の C に対して、$S(C)=\{\alpha_1,\ldots,\alpha_s\}$, $\alpha_0=0$ とし、$S_i=\{(x,y)\in C\times C \mid d(x,y)=\alpha_i\}$ $(0\leq i\leq s)$ と定める。

定理 5 ([3])**.** C を $H(n,q)$ の t-デザインとし、次数を s とする。このとき $t \geq 2s-2$ であれば、$(C,\{S_i\}_{i=0}^{s})$ はクラスが s の Q-多項式アソシエーションスキームである。

よって、tight 3-デザインからはクラスが 2 の Q-多項式アソシエーションスキーム（強正則グラフ）が得られる。定理 1 は、上記で得られる強正則グラフのパラメーターを調べることで証明される。

4 主結果の証明の概略

定理 2 は次の二つの内容から従う。

(1) $H(q+2,q)$ の tight 3-デザインに付随するクラスが 2 の Q-多項式アソシエーションスキームから、クラスが 3 の Q-多項式アソシエーションスキームの構成

(2) (1) で得られたクラスが 3 の Q-多項式アソシエーションスキームと同じパラメータを持つアソシエーションスキームの三重正則数の整数性

4.1 Q-polynomial association schemes of class 3

C を $H(q+2,q)$ の tight 3-デザインとする。このとき、$\alpha_1 = q, \alpha_2 = q+2$ とすると、$S(C) = \{\alpha_1, \alpha_2\}$ となる (α_1 は 1 次方程式 $\sum_{i=0}^{1} K_{q+1,q,i}(x) = 0$ の解である)。

$i \in \{1, 2, \ldots, q\}$ に対して、C_i を次で定める：

$$C_i = \{(x_2, \ldots, x_{q+2}) \mid (i, x_2, \ldots, x_{q+2}) \in C\}.$$

このとき、$\tilde{C} := \bigcup_{i=1}^{q} C_i$ は $H(q+1,q)$ の部分集合であり、$S(\tilde{C}) = \{\alpha_1, \alpha_1 - 1, \alpha_2 - 1\}$ となる。$\tilde{C} \times \tilde{C}$ の部分集合 $\tilde{S}_0, \tilde{S}_1, \tilde{S}_2, \tilde{S}_3$ を次で定める：$\tilde{S}_0 = \{(x,y) \in \tilde{C} \times \tilde{C} \mid d(x,y) = 0\}$ とし、

$$\tilde{S}_1 = \{(x,y) \in \tilde{C} \times \tilde{C} \mid d(x,y) = \alpha_1\},$$
$$\tilde{S}_2 = \{(x,y) \in \tilde{C} \times \tilde{C} \mid d(x,y) = \alpha_1 - 1\},$$
$$\tilde{S}_3 = \{(x,y) \in \tilde{C} \times \tilde{C} \mid d(x,y) = \alpha_2 - 1\}.$$

このとき次の定理が成り立つ。

定理 6. C を $H(q+2,q)$ の *tight* 3-デザインとする。このとき $(\tilde{C}, \{\tilde{S}_i\}_{i=0}^{3})$ はクラスが 3 の Q-多項式アソシエーションスキームであり、その *Krein array* は

$$\{q^2 - 1, q^2 - q, 1; 1, q, q^2 - 1\}.$$

である。

注意 1. $\tilde{C}$ は $H(q+1,q)$ の部分集合として、$t := 2$-デザインかつ次数 $s := 3$ である。$t = 2s - 4$ となるので、定理 5 の仮定 "$t \geq 2s - 2$" を満たさない。よって定理 6 は、従来の Delsarte 理論では導かれない結果である。

定理 6 は、各 C_i が $H(n-1,q)$ の 3-デザインであり次数が 2 であることと、さらに相異なる i, j に対して

$$|\{d(x,y) \mid x \in C_i, y \in C_j\}| = 2$$

であることを用いて、(一つの部分集合に関する) 従来の Delsarte 理論の "$t \geq 2s - 2$ 型の定理 (定理 5)" を複数の部分集合に拡張することで得られる [12, 13]。

4.2 Triple intersection numbers for some Q-polynomial association schemes

定理 6 のアソシエーションスキームのパラメータを持つアソシエーションスキームに関して次が成り立つ。

定理 7. $(X, \{R_i\}_{i=0}^{3})$ を Q-多項式アソシエーションスキームとし、その *Krein array* を $\{q^2 - 1, q^2 - q, 1; 1, q, q^2 - 1\}$ とする。このとき、q が偶数かつ $q > 2$ ならば、q は 4 の倍数である。

定理 7 の証明には以下の三重交差数 (triple intersection number) とその性質を用いる [2]。頂点 $u, v, w \in X$ と整数 i, j, k $(0 \leq i, j, k \leq D)$ に対して、

$$\begin{bmatrix} u & v & w \\ i & j & k \end{bmatrix} := |\{x \in X \mid (u,x) \in R_i, (v,x) \in R_j, (w,x) \in R_k\}|$$

を三重交差数と呼ぶ。三重交差数とクライン数、第二固有行列の間には次の重要な関係が成り立つ。

定理 8. ([2, Theorem 3], cf. [1, Theorem 2.3.2]) $(X, \{R_i\}_{i=0}^{D})$ をクラスが D の対称なアソシエーションスキームとし、その第二固有行列を Q、クライン数を q_{ij}^{k} $(0 \leq i, j, k \leq D)$ とする。このとき、

$$q_{ij}^{k} = 0 \quad \Longleftrightarrow \quad \sum_{r,s,t=0}^{D} Q_{ri} Q_{sj} Q_{tk} \begin{bmatrix} u & v & w \\ r & s & t \end{bmatrix} = 0 \quad \textit{for all } u, v, w \in X.$$

が成り立つ。

定理 7 の証明の概略は以下の通りである。与えられたアソシエーションスキームは Q-多項式であるので、多数の i,j,k に対して $q_{ij}^k = 0$ となる。そのような i,j,k に対して、定理 8 から適当な三頂点（具体的には $p_{2,2}^2 = q(q+3)(q-2)/4 > 0$ が仮定 $q > 2$ から従うので、$(x,y),(y,z),(z,x) \in R_2$ となる三頂点 u,v,w）に対する三重交差数に関する一次関係式が得られる。三重交差数を未知数とする連立一次方程式の解を求めると、$\begin{bmatrix} u & v & w \\ 1 & 2 & 3 \end{bmatrix} = \frac{q^2-q}{4}$ となる。これが整数でなければならないので、q が偶数であることに注意すると、q は 4 の倍数となる。

謝辞

講演の機会を与えてくださった主催者の皆様に感謝いたします。本研究は JSPS 科研費 JP18K03395, JP22K03410 の助成を受けたものです。

参考文献

[1] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1989.

[2] K. Coolsaet and A. Jurišić. Using equality in the Krein conditions to prove nonexistence of certain distance-regular graphs. *J. Combin. Theory Ser. A*, 115(6):1086–1095, 2008.

[3] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.

[4] P. Delsarte, J.-M. Goethals, and J. J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, 6(3):363–388, 1977.

[5] A. Gavrilyuk and S. Suda, On tight 3-designs in Hamming association schemes, in preparation.

[6] A. Gavrilyuk, S. Suda, and J. Vidali, On tight 4-designs in Hamming association schemes, *Combinatorica* **40** (2020), no. 3, 345–362.

[7] Y. Hong. On the nonexistence of nontrivial perfect e-codes and tight $2e$-designs in Hamming schemes $H(n,q)$ with $e \geq 3$ and $q \geq 3$. *Graphs Combin.*, 2(2):145–164, 1986.

[8] R. Mukerjee and S. Kageyama. On existence of two symbol complete orthogonal arrays. *J. Combin. Theory Ser. A*, 66(1):176–181, 1994.

[9] R. Noda. On orthogonal arrays of strength 4 achieving Rao's bound. *J. London Math. Soc. (2)*, 19(3):385–390, 1979.

[10] R. Noda, On orthogonal arrays of strength 3 and 5 achieving Rao's bound, *Graphs and Combin.* (1986) 2, 277–282.

[11] R. C. Rao. Factorial experiments derivable from combinatorial arrangements of arrays. *Suppl. J. Roy. Statist. Soc.*, 9:128–139, 1947.

[12] S. Suda. Coherent configurations and triply regular association schemes obtained from spherical designs. *J. Combin. Theory Ser. A*, 117(8):1178–1194, 2010.

[13] S. Suda, Q-polynomial coherent configurations, *Linear Algebra its Appl.*, **643** (2022), 166–195.

APN 関数 $f : V \to W$ について

谷口浩朗 *
大和大学教育学部

1 はじめに

以下は 2022 年 6 月 17 日に第 38 回代数的組合せ論シンポジウムで発表させていただいた内容をまとめたものです。講演をさせていただき感謝しています。講演内容に関してはすでに専門誌に投稿しているのですが [6]，何度か書き直しを命ぜられていて (9 月現在 4 回目) minor revision という扱いが続いており，まだ accept されていません。(補足：2023 年 1 月 2 日に accept されました。) 第 3 節以降の結果には長くなるため証明をつけていませんが，もし興味を持たれましたら [6] をご参照ください (preprint をお送りします)。また現在知られている APN 関数に関しては,[2], [3], [5] をご覧ください。本稿は，$m > n$ である場合に APN 関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ を考察するための足がかりとして D-property という性質について調べ，また D-property を満たすような一連の例を構成する，という内容です。

2 D-property について

2 元体 $\mathbb{F}_2$ 上のベクトル空間上の関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ が APN 関数であるとは, f がすべての $a \in \mathbb{F}_2^n \backslash \{0\}$ と $b \in \mathbb{F}_2^m$ に対して，解の個数 $|\{x \in \mathbb{F}_2^n \mid f(x+a) + f(x) = b\}| \leq 2$ を満たすことである。APN 関数は 1993 年に Nyberg によって差分攻撃に強い耐性をもつ暗号の設計のため導入された。f が 2 次的であるとは $f(x+y) + f(x) + f(y) + f(0)$ が $x, y \in \mathbb{F}_2^n$ について $\mathbb{F}_2$-bilinear であることである。2 個の関数 f_1, f_2 について，直積 $\mathbb{F}_2^n \times \mathbb{F}_2^m$ の適当な $\mathbb{F}_2$-アフィン同型写像によってグラフ $\{(x, f_1(x)) \mid x \in \mathbb{F}_2^n\}$ がグラフ $\{(x, f_2(x)) \mid x \in \mathbb{F}_2^n\}$ に移されるとき，関数 f_1 と f_2 は CCZ 同値であるという。

J. Dillon は「すべての APN 関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ は $\{f(x)+f(y)+f(z)+f(x+y+z) \mid x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^n$ を満たす」ことを観察した (現在は証明されている)。この条件を Dillon の観察と呼ぶことにする。本稿では「Dillon の観察」条件を関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ $(n \leq m)$ に対して一般化し，**D-property** と呼ぶ (命名は C. Carlet 氏のアドバイスによる)。

定義 1 (D-property)
関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ が条件 $\{f(x) + f(y) + f(z) + f(x+y+z) \mid x, y, z \in \mathbb{F}_2^n\} = \mathbb{F}_2^m$ を満たすとき「f が *D-property* を満たす」という。

$n = m$ のときには，Dillon の観察により APN 関数について D-property が常に成り立つが，本稿では第 5 節において，$n < m$ のときにも D-property が成り立つような APN 関数の一連の例が存在することを示す。さて $B_f(x, t)$ を

$$B_f(x, t) = f(x + t) + f(x) + f(t) + f(0)$$

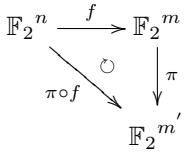
*taniguchi.hiroaki@yamato-u.ac.jp

と定めると，D-property は次のようにも表現できる。

$$\{B_f(x,t)+B_f(y,t) \mid x,y,t \in \mathbb{F}_2^n\} = \mathbb{F}_2^m,$$

実際 $B_f(x,t)+B_f(y,t) = f(x+t)+f(x)+f(t)+f(0)+f(y+t)+f(y)+f(t)+f(0) = f(x+y+z)+f(x)+f(y)+f(z)$(ただし $t=y+z$) である。f が 2 次的な関数のとき，定義より $B_f(x,t)+B_f(y,t) = B_f(x+y,t)$ が成り立つので D-property は 2 次的な関数については「$\{B_f(x,t) \mid x,t \in \mathbb{F}_2^n\} = \mathbb{F}_2^m$」のように表現できる。

D-property について以下の基本的な性質が成り立つことが示せた。



集合 $D_f := \{B_f(x,t)+B_f(y,t) \mid x,y,t \in \mathbb{F}_2^m \text{ with } x \neq y, t \neq 0 \text{ and } x \neq y+t\}$ と定める。f が APN 関数であるための必要十分条件は $D_f \not\ni 0$ であることがすぐにわかる。次の補題 2 の非常に簡明な証明は C. Carlet 氏のアドバイスによる。

補題 2
$f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ を APN 関数，$\pi : \mathbb{F}_2^m \to \mathbb{F}_2^{m_1}$ を $\mathbb{F}_2$-linear surjection とする。このとき, $\pi \circ f$ が APN 関数であるための必要十分条件は $D_f \cap Ker(\pi) = \emptyset$ である。

証明 $\pi \circ f$ が APN 関数であるための必要十分条件は $D_{\pi \circ f} = \pi(D_f) \not\ni 0$ である。仮定より $D_f \not\ni 0$ であるので, $\pi(D_f) \not\ni 0$ であるための必要十分条件は $D_f \cap Ker(\pi) = \emptyset$ であることがわかる。 ∎
$D_f \cup \{0\} = \{B_f(x,a)+B_f(y,a) \mid x,y,a \in \mathbb{F}_2^n\}$ であることより 次の命題 3，命題 4 がわかる:

命題 3
$f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ を APN 関数とする。 このとき f が D-property $\{B_f(x,a)+B_f(y,a) \mid x,y,a \in \mathbb{F}_2^n\} = \mathbb{F}_2^m$ を満たすための必要十分条件は，どのような $\mathbb{F}_2$-linear surjection $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^{m_1}$ （$m_1 < m$）に対しても $\pi \circ f$ が APN 関数にならないことである。

証明 D-property を満たしているならば，$D_f \cap Ker(\pi) \neq \emptyset$ であるので，$\pi \circ f$ は APN 関数にならない。D-property を満たしていないならば，$D_f \cap \langle p \rangle = \emptyset$ となる点 $p \in \mathbb{F}_2^m$ が存在するので，補題 2 より $Ker(\pi) = \langle p \rangle$ となる π に対して $\pi \circ f$ が APN 関数になる。 ∎

命題 4
$f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ を D-property を満たさない APN 関数とする。このとき $\mathbb{F}_2$-linear surjection $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^{m_1}$ （$m_1 < m$）が存在して $\pi \circ f$ が D-property を満たす APN 関数となる。

証明 仮定より f は D-property を満たしていないので，$D_f \neq (\mathbb{F}_2^m)^\times$ であり，$D_f \cap \langle p \rangle = \emptyset$ となる点 $p \in \mathbb{F}_2^m$ が存在する。M を $\mathbb{F}_2^m$ の $\mathbb{F}_2$-ベクトル空間 V で，条件 $D_f \cap V = \emptyset$ を満たすもの全体の集合とする。$V_1, V_2 \in M$ に対し, 順序 $V_1 \geq V_2$ を $V_1 \supseteq V_2$ であることとして定める。W をこの順序に関する M の極大元とする。また $\pi : \mathbb{F}_2^m \to \mathbb{F}_2^{m_1}$ を $Ker(\pi) = W$ である $\mathbb{F}_2$-linear surjection とする。このとき，補題 2 より $\pi \circ f$ は APN 関数である。π が $\mathbb{F}_2$-linear surjection であることより $D_{\pi \circ f} = \pi(D_f)$ がわかる。$D_{\pi \circ f} = (\mathbb{F}_2^{m_1})^\times$ を背理法で証明する。$p \in (\mathbb{F}_2^{m_1})^\times$ で $p \notin D_{\pi \circ f}$ となるものが存在すると仮定する。$V := \pi^{-1}(\langle p \rangle)$ とすると $V \supset W$ でありまた $D_f \cap V = \emptyset$ を満たすが これは W の極大性に反する。 ∎

次の例 1 は 補題 2 と Edel と Pott のスイッチング構成 [4] が関係していることを示している。

例 1 $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ を *APN*関数, $g:\mathbb{F}_2^n \to \mathbb{F}_2$ を非自明な関数とする。このとき $f_1:\mathbb{F}_2^n \ni x \to (f(x),g(x)) \in \mathbb{F}_2^m \oplus \mathbb{F}_2$ は *APN* 関数となる。$\pi:\mathbb{F}_2^m \oplus \mathbb{F}_2 \to \mathbb{F}_2^m$ を $\mathbb{F}_2$-*linear surjection* で $\ker(\pi) = \langle (u,1) \rangle$, $u \neq 0$ とする。すると $(\pi \circ f_1)(x) = f(x) + ug(x)$ となっている。補題 *2* より $\pi \circ f_1$ が *APN* 関数である必要十分条件は $(u,1) \notin \{B_{f_1}(x,t) + B_{f_1}(y,t) \mid x,y,t \in \mathbb{F}_2^m \oplus \mathbb{F}_2\}$ であるが, この条件は *Edel-Pott* の条件 "$f(x+t)+f(x)+f(y+t)+f(y) = u$ のとき $g(x+t)+g(x)+g(y+t)+g(y) = 0$" と同値である。

3 Nonlinearity について

関数 $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ の nonlinearity $nl(f)$ は以下のように定義される。

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n, b \in (\mathbb{F}_2^m)^\times} |\sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b * f(x)}|.$$

ここで $\cdot$ と $*$ は $\mathbb{F}_2^n$ と $\mathbb{F}_2^m$ の内積である。$\mathbb{F}_2 \oplus \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ において, $((\epsilon,x,a),(\epsilon',y,b)) := \epsilon\epsilon' + x \cdot y + a * b$, ここに $(\epsilon,x,a),(\epsilon',y,b) \in \mathbb{F}_2 \oplus \mathbb{F}_2^n \oplus \mathbb{F}_2^m$, と内積を定める。nonlinearity は関数 f がどれだけ線形関数から離れているかという一つの指標であるが，線形攻撃法という暗号解読の方法に対してどれだけ強い耐性を持つかということに対する指標としても考えられている様である [3]。以下のことがわかった。

命題 5
関数 $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ が $f(0) = 0$ であるとき， $nl(f) = 0$ であるための必要十分条件は 線形部分空間 $L \subsetneq \mathbb{F}_2 \oplus \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ で $\{(1,x,f(x)) \mid x \in \mathbb{F}_2^n\} \subset L$ となるものが存在することである。

ところが, f が D-property を満たすとき次のことがわかる。

命題 6
関数 $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ が *D-property* を満たすとすると, $\{(1,x,f(x)) \mid x \in \mathbb{F}_2^n\}$ が $\mathbb{F}_2 \oplus \mathbb{F}_2^n \oplus \mathbb{F}_2^m$ を生成する。

結局，f が D-property を満たし $f(0) = 0$ のときは nonlineality は 0 にならないことがわかる。

系 7
関数 $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ が $f(0) = 0$ であるとき， *D-property* を満たすならば $nl(f) > 0$ が成り立つ。

$a \in \mathbb{F}_2^n$，$b \in (\mathbb{F}_2^m)^\times$ に対して「$W_f(a,b) := \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x + b * f(x)}$」と定義する。$K = \mathbb{F}_{2^{n+1}}$ とする。APN 関数 $f:K \to K$ が $\{W_f(a,b) \mid a \in K, b \in K^\times\} = \{0, \pm 2^{(n+2)/2}\}$ を満たすとき Almost Bent (AB) 関数という。AB 関数は最も高い nonlinearity を持つ関数である。

次の命題は関数 $f:\mathbb{F}_2^n \to \mathbb{F}_2^{n+1}$ で高い nonlinearity を持つものが存在することを示している。一般に「$n < m$ の場合には関数 $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ は nonlinearity が 0 であるか非常に低い値しかとらない」との誤解が多くの研究者達にあったようである。そのために系 7 および次の命題 8 を示して誤解を解く必要があった。

命題 8
L を $K = \mathbb{F}_{2^{n+1}}$ の n-次元部分空間とし，$f|_L : L \to K$ を，K 上の *APN* 関数 f を L に制限した *APN* 関数とする。このとき,

- $nl(f|_L) \geq 2^{n-1} - \frac{1}{2} \max_{a \in K, b \in K^\times} |W_f(a,b)|$,
- $f:K \to K$ が *AB (Almost Bent)* 関数ならば $nl(f|_L) = 2^{n-1} - 2^{n/2}$。

4 CCZ 同値について

CCZ 同値に関しては以下のことがわかった。

命題 9
$f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m$ を *CCZ*-同値 な関数とする。 もし f が $\{B_f(x,t) \mid x,t \in \mathbb{F}_2^n\} = \mathbb{F}_2^m$ を満たすならば g は *D-property* を満たす。

系 10
$f, g : \mathbb{F}_2^n \to \mathbb{F}_2^m$ を *CCZ*-同値な関数とする。もし f が *2* 次的な関数で *D-property* を満たすとすると, g は *D-property* を満たす。

系 10 より，2 次的な関数に関しては D-property という性質は CCZ 同値で保たれることがわかる。2 次的ではない関数に関しては D-property は CCZ 同値で保たれるかどうかはまだ不明である。しかし 2 次的ではない APN 関数で $\{B_f(x,t) \mid x,t \in \mathbb{F}_2^n\} = \mathbb{F}_2^m$ を満たすものが多く存在する (例 3，例 4)。それらの APN 関数に関しては D-property は CCZ 同値で保たれていることが命題 9 よりわかる。

5 D-property を満たす APN 関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2^{n+1}$ の一連の例

この節では $n < m$ の場合にも，D-property を満たす APN 関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ の一連の例が存在することを $m = n+1$ の場合に示す。以下，$K = \mathbb{F}_{2^{n+1}}$ とし，$T_0 = \{x \in K \mid \mathrm{Tr}(x) = 0\}$ とする。

定理 11
$n+1 = 2m$，$m \geq 3$ とする。 F を $K = \mathbb{F}_{2^{n+1}}$ 拡大次数 $[K : F] = 2$ であるような部分体とする。

$$f(x) = \sum_{i<j} a_{ij} x^{2^i+2^j} + \sum_k b_k x^{2^k} + c$$

を K 上の *2* 次的な *APN* 関数で $a_{ij}, b_k, c \in F$ であり $i + j \equiv 1 \pmod 2$ であると仮定する。このとき $f : T_0 \simeq \mathbb{F}_2^n \to K \simeq \mathbb{F}_2^{n+1}$ は *D-property* を満たす。

この定理の証明は準備が必要で長くなりますので省略します。この定理の証明が出来たことが，[6] を書き始めるきっかけとなりました。以下の補題 12 は D-property を満たす 2 次的な APN 関数 $f : \mathbb{F}_2^n \to \mathbb{F}_2^{n+1}$ の構成において非常に有用であったので，特にここに記録しておきたいと思います。

補題 12
$f(x) = \sum_{i<j} a_{ij} x^{2^i+2^j} + \sum_k b_k x^{2^k} + c$ を K 上の *2* 次的な *APN* 関数で $a_{ij}, b_k, c \in F$ とする。ここに F は K の部分体で $F \neq \mathbb{F}_2, \mathbb{F}_4$ とする。また t を F の 0 でない元とし $a \in K$ とする。 このとき，もし $\mathrm{Tr}_F^K(a) \in \{B_f(t, x_1) \mid x_1 \in F\}$ ならば, $a \in \{B_f(t,x) \mid x \in K\}$ である。

定理 11 の応用として，以下の D-property を満たす APN 関数 $f : T_0 \simeq \mathbb{F}_2^n \to K \simeq \mathbb{F}_2^{n+1}$ の例が存在することがわかった。

例 2 $n+1 = 2m$，$m \geq 3$ とし，$f(x) = x^{\sigma+1}$ を K 上の *Gold* 関数とする。*(σ は $Gal(K/\mathbb{F}_2)$ の生成元)*。このとき $f : T_0 \simeq \mathbb{F}_2^n \to K \simeq \mathbb{F}_2^{n+1}$ は *D-property* を満たす。

証明 $x^\sigma := x^{2^i}$ とすると，$x^{\sigma+1} = x^{2^i+2^0}$ において，$\gcd(i, n+1) = 1$ および $n+1 = 2m$ より $i + 0 \equiv 1 \pmod 2$ となる。よって定理 11 の仮定は満たされている。 ∎

例 3 $n+1=2m$，$m\geq 3$ とし，$f(x)=x^3+a^{-1}\operatorname{Tr}(a^3x^9)$ を K 上定義された *Budaghyan, Carlet, and Leander* の *APN* 関数とする *[1]*。 さらに F を K の $[K:F]=2$ である部分体とし，$a\in F^\times$ とする。このとき $f:T_0\simeq\mathbb{F}_2^n\to K\simeq\mathbb{F}_2^{n+1}$ は *D-property* を満たす。

証明 $x^3=x^{2^1+2^0}$ で $1+0\equiv 1 \pmod 2$ であり，また $(x^9)^{2^i}=x^{2^{3+i}+2^{0+i}}$ において $(3+i)+(0+i)\equiv 1 \pmod 2$ である。 さらに $a^{-1+3\cdot 2^i}\in F$ なので, $f(x)=x^3+a^{-1}\operatorname{Tr}(a^3x^9)=x^3+\sum_{i=0}^{n-1}a^{-1+3\cdot 2^i}(x^9)^{2^i}$ に対して定理 11 の仮定は満たされている。 ∎

5.1 $f|_{T_0(K)}$ has the D-property if $f|_{T_0(F)}$ has the D-property

F を K の部分体とし，$T_0(K)=\{x\in K\mid \operatorname{Tr}(x)=0\}$, $T_0(F)=\{x\in F\mid \operatorname{Tr}_{\mathbb{F}_2}^F(x)=0\}$ とする。この節では K 上の 2 次的なまたは単項式で表される APN 関数 f について，f を K のある部分体 F に制限したときに $f|_{T_0(F)}:T_0(F)\to F$ が D-property を満たしているならば，$f|_{T_0(K)}:T_0(K)\to K$ も D-property を満たしていることを示すことにより多くの D-property を満たす APN 関数 $f:T_0(K)\to K$ の例が構成できることを見ます。以下の定理 13 の証明では補題 12 がキーになりました。

定理 13
$K=\mathbb{F}_{2^{n+1}}$ とし, F を K の部分体で $F\neq\mathbb{F}_2,\mathbb{F}_4$ とする。$f(x)=\sum_{i<j}a_{i,j}x^{2^i+2^j}+\sum_k b_kx^{2^k}+c$ を K 上の *2* 次的な *APN* 関数で $a_{i,j},b_k,c\in F$ とする。このときもし $f|_{T_0(F)}:T_0(F)\to F$ が *D-property* を満たすならば, $f|_{T_0(K)}:T_0(K)\to K$ も *D-property* を満たす。

単項式で表される APN 関数に関しては，次の「Dobbertin の観察」といわれる結果が基本的である。

事実 1 (Dobbertin の観察) $f(x)=x^m$ を $K=\mathbb{F}_{2^{n+1}}$ 上の単項式で表される *APN* 関数とする。このとき，もし $n+1$ が奇数なら $\gcd(m,2^{n+1}-1)=1$, $n+1$ が偶数なら $\gcd(m,2^{n+1}-1)=3$ が成り立つ。

単項式で表される APN 関数に関しては，次の命題 14 がうまく機能して定理 15, 定理 16 が証明できました。これらの定理を用いると，体 F の拡大次数が小さい場合に $f|_{T_0(F)}:T_0(F)\to F$ が D-property を満たすことをコンピュータでチェックしておくことにより，F の拡大体 K において $f|_{T_0(K)}:T_0(K)\to K$ に関しても D-property が成り立つことがわかり，多くの D-property を満たす例を構成できます。

命題 14
$f(x)=x^m$ を K 上の単項式とし，F を K の部分体, $\alpha\in F^\times$ とする。もし $\{\alpha a_1^m\mid a_1\in F\}\subset\{B_f(x_1,t_1)+B_f(y_1,t_1)\mid x_1,y_1,t_1\in T_0(F)\}$ であれば, $\{\alpha a^m\mid a\in K\}\subset\{B_f(x,t)+B_f(y,t)\mid x,y,t\in T_0(K)\}$ が成り立つ。

定理 15
$f(x)=x^m$ を $K=\mathbb{F}_{2^{n+1}}$ 上の単項式で表される *APN* 関数で $\gcd(m,2^{n+1}-1)=1$ とする。また F を K の部分体とする。このときもし $f|_{T_0(F)}:T_0(F)\to F$ が *D-property* を満たすならば, $f|_{T_0(K)}:T_0(K)\to K$ も *D-property* を満たす。

定理 16
$f(x)=x^m$ を $K=\mathbb{F}_{2^{n+1}}$ 上の単項式で表される *APN* 関数で $\gcd(m,2^{n+1}-1)=3$ とする。 また F を K の部分体で $F\supset\mathbb{F}_4$ とする。このときもし $f|_{T_0(F)}:T_0(F)\to F$ が *D-property* を満たすならば, $f|_{T_0(K)}:T_0(K)\to K$ も *D-property* を満たす。

次の定理は，2 次的ではない APN 関数であるにもかかわらず，性質 $\{B_f(x,t) \mid x,t \in T_0(\mathbb{F}_{2^{n+1}})\} = \mathbb{F}_{2^{n+1}}$ を満たすことがあることを示している。この性質は 2 次的な関数については D-property と同値な性質であるが，2 次的ではない APN 関数については D-property よりも強い性質であり，この性質を満たしていないが D-property を満たしている（2 次的ではない）単項 APN 関数をコンピュータを用いていくつも見出すことが出来る。

定理 17
$f(x) = x^m$ を体 $K = \mathbb{F}_{2^{n+1}}$ 上の単項式で表された *APN* 関数とする。f を部分体 F ($n+1$ が偶数のときは $F \supset \mathbb{F}_4$ とする) に制限した関数が $\{B_f(x,t) \mid x,t \in T_0(F)\} = F$ を満たすとすると $f|_{T_0(K)} : T_0(K) \to K$ は $\{B_f(x,t) \mid x,t \in T_0(K)\} = K$ を満たす。

この定理とコンピュータの使用により以下のような $\{B_f(x,t) \mid x,t \in T_0(K)\} = K$ を満たす (D-property も満たしている，定義域を $T_0(K)$ に制限した)APN 関数 $f|_{T_0(K)} : T_0(K) \to K$ の一連の例の存在がわかった。

例 4
- *(Kasami APN* 関数の制限*)* $f(x) = x^{2^{2i}-2^i+1}$ $i \equiv 3,4 \pmod 7$ *on* $K = \mathbb{F}_{2^{7s}}$ *with* s *an odd integer, any Kasami APN functions on* $K = \mathbb{F}_{2^{9s}}, \mathbb{F}_{2^{11s}}, \mathbb{F}_{2^{13s}}$ *with* s *an odd integer, and any Kasami APN functions on* $K = \mathbb{F}_{2^{8s}}, \mathbb{F}_{2^{10s}}, \mathbb{F}_{2^{12s}}, \mathbb{F}_{2^{14s}}$ *with* s *a positive integer;*
- *(Welch APN* 関数の制限*)* $f(x) = x^m$ $m = 2^{3+7l} + 3$ *on* $\mathbb{F}_{2^{7s}}$, $m = 2^{4+9l} + 3$ *on* $K = \mathbb{F}_{2^{9s}}$, $m = 2^{5+11l} + 3$ *on* $K = \mathbb{F}_{2^{11s}}$, *and* $m = 2^{6+13l} + 3$ *on* $K = \mathbb{F}_{2^{13s}}$ *with* $s = 2l+1$ *and* l *a positive integer;*
- *(Niho APN* 関数の制限*)* $f(x) = x^m$, *where* $m = 2^t + 2^{(3t+1)/2} - 1$ *with* $t = 22l + 5$ *on* $K = \mathbb{F}_{2^{11s}}$ *and* $t = 30l + 7$ *on* $K = \mathbb{F}_{2^{15s}}$, *or* $m = 2^t + 2^{t/2} - 1$ *with* $t = 26l + 6$ *on* $K = \mathbb{F}_{2^{13s}}$ *for* $s = 4l + 1$ *and* l *a positive integer; and*
- *(Inverse APN* 関数の制限*)* $f(x) = x^{2^{ks}-2}$ *on* $K = \mathbb{F}_{2^{ks}}$ *for* $k = 7, 9, 11, 13, 15$ *and for odd integer* s.

また，定理 17 を用いることにより以下の例の存在がわかる。

例 5 $t = 2l$, $l \geq 3$ とし，$K = \mathbb{F}_{2^{5t}}$ とする。$f(x) = x^m$（ただし $m = 2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$）を K 上定義された *Dobbertin* の単項 *APN* 関数とする。 このとき $\{B_f(x,t) \mid x,t \in T_0(K)\} = K$ が成り立つ。

参 考 文 献

[1] L. Budaghyan, C. Carlet and G. Leander, Constructing new APN functions from known ones, Finite Fields and Their Applications, 15, pp. 150–159 (2009).

[2] M. Calderini, L. Budaghyan and C. Carlet, On known constructions of APN and AB functions and their relation to each other, Proceedings of the 20th Central European Conference on Cryptography, Matematicke znanosti 25, pp. 79–105 (2021).

[3] C. Carlet, Boolean Functions for Cryptography and Coding Theory, Cambridge University Press, Cambridge (2021).

[4] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Advances in Mathematics of Communications 3, pp. 59–81 (2009).

[5] https://boolean.h.uib.no/mediawiki/index.php/ .

[6] H. Taniguchi, D-property for APN functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n+1}$, Cryptography and Communications, accepted.

Sigma involutions associated with parafermion vertex operator algebras

一橋大学名誉教授　山田裕理[1]

1　はじめに

頂点作用素代数のヒュージョン代数に関する対称性は，興味深い研究対象である．ヒュージョン代数の対称性に基づく自己同型が自明に作用するような部分代数は，それ自身が新しい対称性を持つことがある．本稿ではこのような場合を取り上げる．

$\mathfrak{sl}_2$ 型のパラフェルミオン頂点作用素代数 $K(\mathfrak{sl}_2,k)$ のヒュージョン代数は，位数 k の自己同型 τ を持つ．この自己同型 τ が自明に作用するような $K(\mathfrak{sl}_2,k)$ の既約加群を σ 型の既約加群という．$k\geq 3$ ならば $K(\mathfrak{sl}_2,k)$ の自己同型群 $\mathrm{Aut}(K(\mathfrak{sl}_2,k))$ は位数 2 で，その単位元以外の元を θ で表すと，σ 型の既約加群は θ 不変である．したがって，σ 型の既約加群は $\langle\theta\rangle$ による $K(\mathfrak{sl}_2,k)$ のオービフォールド $K(\mathfrak{sl}_2,k)^{\langle\theta\rangle}$ の 2 個の既約加群の直和になる．これらの既約 $K(\mathfrak{sl}_2,k)^{\langle\theta\rangle}$ 加群で張られる $K(\mathfrak{sl}_2,k)^{\langle\theta\rangle}$ のヒュージョン代数の部分代数は，位数 2 の自己同型 σ を持つ．これが表題にある sigma involution である．

$k=3$ のときの σ は Miyamoto [12] により導入され，Lam-Yamauchi [10] により詳しい研究がなされている．$k=2$ のときは，$\mathrm{Aut}(K(\mathfrak{sl}_2,2))=1$ なので事情は少し異なるが，$K(\mathfrak{sl}_2,2)$ のヒュージョン代数において τ が自明に作用する部分代数は位数 2 の自己同型 σ を持つことが Miyamoto [11] により示されている．自己同型を表す τ と σ という記号は，この論文 [11] で最初に導入された．

本稿では，Ching Hung Lam 氏との共同研究 [8] に基づいて，任意の $k\geq 3$ に対して τ と σ を考察する．

2　パラフェルミオン頂点作用素代数 $K(\mathfrak{sl}_2,k)$

$k\geq 2$ を整数とする．この節では，$\mathfrak{sl}_2$ 型のパラフェルミオン頂点作用素代数 $K(\mathfrak{sl}_2,k)$ に関して，本稿で必要となる性質をまとめておく．

$K(\mathfrak{sl}_2,k)$ は自己双対，有理的，C_2 余有限で CFT 型の単純頂点作用素代数で，中心電荷は $\frac{2(k-1)}{k+2}$ である．自己同型群 $\mathrm{Aut}(K(\mathfrak{sl}_2,k))$ は $k=2$ のときは 1 で，$k\geq 3$ ならば $\mathrm{Aut}(K(\mathfrak{sl}_2,k))=\langle\theta\rangle$ は位数 2 である．

[1]e-mail: yamada.h@r.hit-u.ac.jp

以下，簡単のため $M^0 = K(\mathfrak{sl}_2, k)$ とおくことにする．M^0 の既約加群は

$$M^{i,l};\ 0 \le i \le k,\ 0 \le l < 2k,\ i \equiv l \pmod 2$$

で表される．ここで，$M^{i,l}$ の 2 番目の添字 l は modulo $2k$ で考える．なお $M^{0,0} = M^0$ である．これらの既約加群に対して

$$M^{i,l} \cong M^{k-i,k+l} \tag{2.1}$$

という同型が成り立つので，M^0 の既約加群の同型類の完全代表系として

$$\mathrm{Irr}(M^0) = \{M^{i,l} \mid 0 \le i \le k,\ 0 \le l < k,\ i \equiv l \pmod 2\}$$

をとることができる．特に，$|\mathrm{Irr}(M^0)| = \frac{1}{2}k(k+1)$ である．θ は $\mathrm{Irr}(M^0)$ 上に次の置換

$$M^{i,l} \circ \theta = M^{i,2k-l} \tag{2.2}$$

を引き起こす．なお，$M^{i,l}$ のトップレベルは 1 次元である．

$k \ge 3$ のときは，定数倍を除いて一意的なウエイト 3 のプライマリー元 W^3 で M^0 は頂点作用素代数として生成される．自己同型 θ の W^3 への作用は，$\theta(W^3) = -W^3$ である．

注意 2.1 [8] では $K(\mathfrak{sl}_2, k)$ の既約加群を $M^{i,j}$ と $\widetilde{M}^{i,l}$ の 2 通りに表記している．本稿の $M^{i,l}$ は，[8] の $\widetilde{M}^{i,l}$ である．$K(\mathfrak{sl}_2, k)$ の既約加群を [8] の $M^{i,j}$ ではなく，本稿のように $M^{i,l}$ で表すほうが，後でヒュージョン積を議論する際に都合がよい．

$k = 2,\ 3$ のときの $K(\mathfrak{sl}_2, k)$ は，Virasoro 頂点作用素代数を用いて記述できる．$L(c, 0)$ を中心電荷 c の Virasoro 頂点作用素代数とし，$L(c, h)$ をその最高ウエイト h の既約加群とする．

$k = 2$ のとき

$K(\mathfrak{sl}_2, 2) = L(\frac{1}{2}, 0)$ で，その既約加群は

$$\begin{aligned} M^{0,0} &= M^{2,2} = L(\tfrac{1}{2}, 0), \\ M^{0,2} &= M^{2,0} = L(\tfrac{1}{2}, \tfrac{1}{2}), \\ M^{1,1} &= M^{1,3} = L(\tfrac{1}{2}, \tfrac{1}{16}) \end{aligned}$$

の 3 個である．このうち $M^{0,0} = M^0$ と $M^{2,0}$ が σ 型の既約加群である．

$k = 3$ のとき

$K(\mathfrak{sl}_2, 3) = L(\frac{4}{5}, 0) \oplus L(\frac{4}{5}, 3)$ で，その既約加群は

$$\begin{aligned} &M^{0,0} = M^{3,3}, \quad M^{0,2} = M^{3,5}, \quad M^{0,4} = M^{3,1}, \\ &M^{1,1} = M^{2,4}, \quad M^{1,3} = M^{2,0}, \quad M^{1,5} = M^{2,2} \end{aligned}$$

の 6 個である．このうち

$$M^{0,0} = L(\tfrac{4}{5},0) \oplus L(\tfrac{4}{5},3), \quad M^{2,0} = L(\tfrac{4}{5},\tfrac{2}{5}) \oplus L(\tfrac{4}{5},\tfrac{7}{5})$$

の 2 個が σ 型の既約加群である．

既約 $K(\mathfrak{sl}_2,3)$ 加群は，$L(\frac{4}{5},0)$ の加群としては 1 個または 2 個の既約加群の直和である．$L(\frac{4}{5},0)$ の単純カレント $L(\frac{4}{5},3)$ とのヒュージョン積により，$K(\mathfrak{sl}_2,3)$ の既約加群としての構造が定まる．$L(\frac{4}{5},0)$ の既約加群の同型類は 10 個であるが，それらと $L(\frac{4}{5},3)$ とのヒュージョン積から $K(\mathfrak{sl}_2,3)$ の既約加群が定まる様子は，Miyamoto [12] で説明されている．なお，そこで基本となる Virasoro 頂点作用素代数のヒュージョン積は，Wang [14] により決定されている．

3　自己同型 τ と τ_W

$k \geq 2$ とする．この節では，$K(\mathfrak{sl}_2,k)$ のヒュージョン積に基づいて τ と τ_W を定義する．$M^0 = K(\mathfrak{sl}_2,k)$ のヒュージョン積は，

$$M^{i_1,l_1} \boxtimes_{M^0} M^{i_2,l_2} = \sum_{r \in R(i_1,i_2)} M^{r,\,l_1+l_2} \tag{3.1}$$

であることが Dong-Wang [1] により決定されている．ここで，

$$R(i_1,i_2) = \{r \in \mathbb{Z} \mid |i_1 - i_2| \leq r \leq \min\{i_1+i_2,\, 2k-i_1-i_2\},\, i_1+i_2+r \in 2\mathbb{Z}\}$$

である．

注意 3.1 ヒュージョン積 $\boxtimes_{M^0}$ は可換で結合的な二項演算で，頂点作用素代数 M^0 自身は $\boxtimes_{M^0}$ に関して単位元，すなわち $M^0 \boxtimes_{M^0} M^{i,l} = M^{i,l}$ である．

$\mathrm{Irr}(M^0)$ を基底とする $\mathbb{C}$ 上のベクトル空間は，ヒュージョン積 $\boxtimes_{M^0}$ により可換で結合的な代数になる．この代数を M^0 のヒュージョン代数という．ヒュージョン代数の対称性はヒュージョン積 (3.1) から導かれるが，実際には以下のことが Zamolodchikov-Fateev [15] によりかなり以前から知られていた．

定理 3.2 ([15], c.f. [8, Theorem 3.1])

$$\tau : M^{i,l} \longmapsto \exp(2\pi\sqrt{-1}/k)^l M^{i,l}; \quad 0 \leq i \leq k,\ 0 \leq l < 2k,\ i \equiv l \pmod 2$$

は，M^0 のヒュージョン代数の位数 k の自己同型である．

注意 3.3 $M^{i,l}$ の l は modulo $2k$ で考えるが，τ の定義において $\exp(2\pi\sqrt{-1}/2k)^l$ ではなく $\exp(2\pi\sqrt{-1}/k)^l$ とする理由は，同型 (2.1) と矛盾しないようにするためである．

τ が 1 として作用する M^0 の既約加群を，**σ 型**という．σ 型の既約 M^0 加群は，

$$M^{2j,0};\quad 0 \le j \le \lfloor k/2 \rfloor$$

の $\lfloor k/2 \rfloor + 1$ 個である．

V を頂点作用素代数とし，$V \supset W \cong K(\mathfrak{sl}_2, k)$ とする．このとき，V は W の加群として既約 W 加群いくつかの直和に分解される．

$0 \le l < k$ を固定する．V を既約 W 加群の直和に分解したとき，$M^{i,l};\ 0 \le i \le k$, $i \equiv l \pmod 2$ と同型な既約成分全部の和を $V_W[l]$ で表すと，

$$V = \bigoplus_{l=0}^{k-1} V_W[l]$$

が成り立つ．ここでは，l を modulo k で考える．定理 3.2 により次の定理が得られる．

定理 3.4 ([8, Theorem 3.3]) 上記の記号のもとで，線形写像 $\tau_W : V \to V$ を

$$\tau_W(v) = \exp(2\pi\sqrt{-1}/k)^l v\,;\quad v \in V_W[l],\ 0 \le l < k$$

と定義すると，τ_W は頂点作用素代数 V の自己同型である．

$\tau_W = 1$ であるとき，すなわち $V = V_W[0]$ であるとき，V は W 加群として**σ 型**という．また，W を**σ 型**のパラフェルミオン部分頂点作用素代数という．

4　自己同型 σ と σ_W

$k \ge 3$ とし，

$$K(\mathfrak{sl}_2, k)^{\langle\theta\rangle} = \{v \in K(\mathfrak{sl}_2, k) \mid \theta(v) = v\}$$

とおく．$K(\mathfrak{sl}_2, k)^{\langle\theta\rangle}$ の既約加群の分類，およびヒュージョン積の決定は Jiang-Wang [5, 6] によりなされている．この節では，その結果を用いて σ と σ_W を定義する．

$M^0 = K(\mathfrak{sl}_2, k)$ について，$M^{0,\pm} = \{v \in M^0 \mid \theta(v) = \pm v\}$ とおく．$M^{0,+} = K(\mathfrak{sl}_2, k)^{\langle\theta\rangle}$ で，$M^0 = M^{0,+} \oplus M^{0,-}$ である．$M^{0,-}$ は既約 $M^{0,+}$ 加群で，$M^{0,-}$ のトップレベルは M^0 のウエイト 3 のプライマリー元 W^3 で張られる．

(2.2) により $M^{2j,0};\ 0 \le j \le \lfloor k/2 \rfloor$ は θ-不変でなので，$M^{2j,0}$ は

$$M^{2j,0} = (M^{2j,0})^0 \oplus (M^{2j,0})^1 \tag{4.1}$$

と，θ の固有空間に分解される．ここでは，θ の固有空間 $(M^{2j,0})^0$ と $(M^{2j,0})^1$ は

$$\begin{aligned}\text{conformal weight of } M^{2j,0} &= \text{conformal weight of } (M^{2j,0})^0 \\ &< \text{conformal weight of } (M^{2j,0})^1\end{aligned} \tag{4.2}$$

という条件を満たすように指定する．$(M^{2j,0})^0$ と $(M^{2j,0})^1$ は，ともに既約 $M^{0,+}$ 加群である．なお，$(M^{0,0})^0 = M^{0,+}$ で，$(M^{0,0})^1 = M^{0,-}$ である．

注意 4.1 [6] では，θ の固有空間を $(M^{2j,0})^{\pm} = \{v \in M^{2j,0} \mid \theta(v) = \pm v\}$ ではなく $(M^{2j,0})^0$ と $(M^{2j,0})^1$ で表すことにより，$M^{0,+}$ のヒュージョン積が見やすい形で記述できるように工夫されている．

次の定理は，Jiang-Wang [6] で決定されている $M^{0,+}$ のヒュージョン積のうち，ヒュージョン代数の自己同型 σ を定義する際に必要なことをまとめたものである．

定理 4.2 ([8, Theorem 3.4])
(1) $0 \leq j \leq \lfloor k/2 \rfloor$ と $\epsilon_1, \epsilon_2 \in \{0, 1\}$ に対して

$$(M^{0,0})^{\epsilon_1} \boxtimes_{M^{0,+}} (M^{2j,0})^{\epsilon_2} = (M^{2j,0})^{\epsilon_1+\epsilon_2}.$$

ただし，$\epsilon_1 + \epsilon_2$ は modulo 2 で考える．
(2) $k \geq 4$ のとき，$1 \leq j \leq \lfloor k/2 \rfloor - 1$ に対して

$$(M^{2,0})^0 \boxtimes_{M^{0,+}} (M^{2j,0})^0 = (M^{2(j-1),0})^0 + (M^{2j,0})^1 + (M^{2(j+1),0})^0.$$

(3) $j = \lfloor k/2 \rfloor$ に対して，k が奇数ならば

$$(M^{2,0})^0 \boxtimes_{M^{0,+}} (M^{2j,0})^0 = (M^{2(j-1),0})^0 + (M^{2j,0})^1.$$

k が偶数ならば

$$(M^{2,0})^0 \boxtimes_{M^{0,+}} (M^{k,0})^0 = (M^{k-2,0})^0.$$

注意 4.3 ヒュージョン積 $\boxtimes_{M^{0,+}}$ は可換で結合的な二項演算で，$M^{0,+} \boxtimes_{M^{0,+}} (M^{2j,0})^{\epsilon} = (M^{2j,0})^{\epsilon}$ である．したがって，定理 4.2 の (1), (2), (3) によりすべての $1 \leq j_1, j_2 \leq \lfloor k/2 \rfloor$ と $\epsilon_1, \epsilon_2 \in \{0, 1\}$ について $(M^{2j_1,0})^{\epsilon_1} \boxtimes_{M^{0,+}} (M^{2j_2,0})^{\epsilon_2}$ は定まる．

定理 4.2 により，次のような自己同型 σ が定義できる．

定理 4.4 ([8, Theorem 3.6])

$$\sigma : (M^{2j,0})^{\epsilon} \longmapsto (-1)^{j+\epsilon} (M^{2j,0})^{\epsilon}; \quad 0 \leq j \leq \lfloor k/2 \rfloor,\ \epsilon \in \{0, 1\}$$

は，$(M^{2j,0})^{\epsilon};\ 0 \leq j \leq \lfloor k/2 \rfloor,\ \epsilon \in \{0, 1\}$ で張られる $M^{0,+}$ のヒュージョン代数の部分代数の位数 2 の自己同型である．

V は頂点作用素代数で，$V \supset W \cong K(\mathfrak{sl}_2, k),\ k \geq 3$ とする．さらに，$V = V_W[0]$，すなわち V は W 加群として σ 型と仮定する．V を既約 $M^{0,+}$ 加群の直和に分解したとき，$(M^{2j,0})^{\epsilon}$ と同型な既約成分全部の和を $V_{W^+}[j, \epsilon]$ で表すと，

$$V = \bigoplus_{j=0}^{\lfloor k/2 \rfloor} \bigoplus_{\epsilon \in \{0,1\}} V_{W^+}[j, \epsilon]$$

が成り立つ．このとき，定理 4.4 により次の定理が得られる．

定理 4.5 ([8, Theorem 3.7]) 上記の記号のもとで，線形写像 $\sigma_W : V \to V$ を

$$\sigma_W(v) = (-1)^{j+\epsilon} v\,; \quad v \in V_{W^+}[j,\epsilon],\ 0 \le j \le \lfloor k/2 \rfloor,\ \epsilon \in \{0,1\}$$

と定義すると，σ_W は頂点作用素代数 V の位数 2 の自己同型である．

σ_W を，W に付随する頂点作用素代数 V の **σ-involution** という．

$k = 2, 3$ のときの τ と σ は Miyamoto [11, 12] で考察されている．$k = 2$ の場合は $\theta = 1$ であることに注意する．

$k = 2$ のとき ([11])

$M^0 = K(\mathfrak{sl}_2, 2) = L(\frac{1}{2}, 0)$ で，ヒュージョン積は

$$\begin{aligned} L(\tfrac{1}{2},\tfrac{1}{2}) \boxtimes L(\tfrac{1}{2},\tfrac{1}{2}) &= L(\tfrac{1}{2},0), \\ L(\tfrac{1}{2},\tfrac{1}{2}) \boxtimes L(\tfrac{1}{2},\tfrac{1}{16}) &= L(\tfrac{1}{2},\tfrac{1}{16}), \\ L(\tfrac{1}{2},\tfrac{1}{16}) \boxtimes L(\tfrac{1}{2},\tfrac{1}{16}) &= L(\tfrac{1}{2},0) + L(\tfrac{1}{2},\tfrac{1}{2}) \end{aligned}$$

である．τ と σ の定義は次のようになる．

$$\tau = \begin{cases} 1 & \text{on } L(\frac{1}{2},0),\ L(\frac{1}{2},\frac{1}{2}), \\ -1 & \text{on } L(\frac{1}{2},\frac{1}{16}). \end{cases}$$

$$\sigma = \begin{cases} 1 & \text{on } L(\frac{1}{2},0), \\ -1 & \text{on } L(\frac{1}{2},\frac{1}{2}). \end{cases}$$

$k = 3$ のとき ([12])

$M^0 = K(\mathfrak{sl}_2, 3)$ の既約加群は 6 個で，そのうち σ 型のものは

$$M^0 = L(\tfrac{4}{5},0) \oplus L(\tfrac{4}{5},3), \quad M^{2,0} = L(\tfrac{4}{5},\tfrac{2}{5}) \oplus L(\tfrac{4}{5},\tfrac{7}{5})$$

の 2 個である．さらに，

$$M^{0,+} = (M^{0,0})^0 = L(\tfrac{4}{5},0), \quad M^{0,-} = (M^{0,0})^1 = L(\tfrac{4}{5},3),$$

$$(M^{2,0})^0 = L(\tfrac{4}{5},\tfrac{2}{5}), \quad (M^{2,0})^1 = L(\tfrac{4}{5},\tfrac{7}{5})$$

で，σ の定義は次のようになる．

$$\sigma = \begin{cases} 1 & \text{on } M^{0,+},\ (M^{2,0})^1, \\ -1 & \text{on } M^{0,-},\ (M^{2,0})^0. \end{cases}$$

5 $V_{\sqrt{2}A_{k-1}}$ に基づく σ-involution

$N = \sqrt{2}A_{k-1}$ とおく．ただし，$k \geq 3$ で A_{k-1} は階数 $k-1$ の A 型ルート格子を表す．この節では，格子頂点作用素代数 V_N から標準的に σ-involution が得られることを説明する．

格子頂点作用素代数 V_N には，次のような頂点作用素代数 $T \otimes M^0$ が含まれる．

$$V_N \supset T \otimes M^0. \tag{5.1}$$

ここで，$M^0 = K(\mathfrak{sl}_2, k)$ で，

$$T = L(c_1, 0) \otimes \cdots \otimes L(c_{k-1}, 0)$$

は中心電荷が

$$c_m = 1 - \frac{6}{(m+2)(m+3)}; \quad 1 \leq m \leq k-1$$

の Virasoro 頂点作用素代数のテンソル積である．V_N は M^0 加群として σ 型なので，定理 4.5 により M^0 に付随する σ-involution $\sigma_{M^0} \in \mathrm{Aut}(V_N)$ が定義できる．これについて次の定理が成り立つ．

定理 5.1 ([8, Theorem 4.3]) $\mathrm{Aut}(V_N)$ の元として，σ_{M^0} は格子 N の -1-isometry の持ち上げと一致する．

次に，σ_{M^0} を V_N より大きい頂点作用素代数の自己同型に拡張することを考える．N の双対格子

$$N^* = \{\alpha \in \mathbb{Q} \otimes_{\mathbb{Z}} N \mid \langle \alpha, N \rangle \subset \mathbb{Z}\}$$

について，

$$N^*/N \cong \mathbb{Z}_2^{k-2} \times \mathbb{Z}_{2k}$$

であり，このうちの $\mathbb{Z}_k$ の部分が位数 k の自己同型 τ_{M^0} と対応する．特に，$N \subset L \subset N^*$ を満たす有理格子 L について，V_L が M^0 加群として σ 型であるための必要十分条件は，$2L \subset N$ が成り立つことである．

$N \subset L \subset N^*$ を満たす格子 L よりさらに大きい格子を扱うために，RSSD 部分格子および RSSD involution を用いる．RSSD involution は通常の鏡映 (reflection) の一般化として Griess [2] により導入された．

$(L, \langle \cdot, \cdot \rangle)$ を正定値整格子とする．$\mathbb{Q} \otimes_{\mathbb{Z}} L$ を簡単のため $\mathbb{Q}L$ とも書くことにする．L の部分格子 A に対して，

$$\mathrm{Ann}_L(A) = \{\alpha \in L \mid \langle \alpha, A \rangle = 0\}$$

を A の L における annihilator と呼ぶ．$A \cap \mathrm{Ann}_L(A) = 0$ で，階数について

$$\mathrm{rank}\, L = \mathrm{rank}\, A + \mathrm{rank}\, \mathrm{Ann}_L(A)$$

が成り立つ．さらに，

$$A \oplus \mathrm{Ann}_L(A) \subset L \subset L^* \subset A^* \oplus \mathrm{Ann}_L(A)^* \subset \mathbb{Q}L = \mathbb{Q}A \oplus \mathbb{Q}\mathrm{Ann}_L(A)$$

で，$\mathbb{Q}\mathrm{Ann}_L(A)$ は $\mathbb{Q}A$ の QL における直交補空間 $(\mathbb{Q}A)^\perp$ に一致する．

$$2L \subset A + \mathrm{Ann}_L(A)$$

が成り立つとき，A は L において **relatively semiselfdual (RSSD)** であるという．

整格子 A が $2A^* \subset A$ を満たすとき，A は **semiselfdual (SSD)** であるという．A がユニモジュラー格子の $\sqrt{2}$ 倍ならば $2A^* = A$ なので，A は SSD 格子である．L が A を含む整格子のとき，A が SSD 格子ならば A は L において RSSD である．第 6 節で $A = \sqrt{2}E_8$ の場合を扱う．

例 5.2 $A = \mathbb{Z}\alpha_1$ を A_1 格子，$L = \mathbb{Z}\alpha_1 + \mathbb{Z}\alpha_2$ を A_2 格子とする．すなわち，$\langle \alpha_1, \alpha_1 \rangle = \langle \alpha_2, \alpha_2 \rangle = 2$, $\langle \alpha_1, \alpha_2 \rangle = -1$ である．$\mathrm{Ann}_L(A) = \mathbb{Z}(\alpha_1 + 2\alpha_2)$ だから，

$$2L = 2\mathbb{Z}\alpha_1 + 2\mathbb{Z}\alpha_2 \subset \mathbb{Z}\alpha_1 + 2\mathbb{Z}\alpha_2 = A + \mathrm{Ann}_L(A)$$

が成り立つので，A は L において RSSD である．$|L : A + \mathrm{Ann}_L(A)| = 2$ であること，および A は SSD 格子であることに注意する．

A が L において RSSD のとき，直交変換 $t_A : \mathbb{Q}L \to \mathbb{Q}L$ を

$$t_A = \begin{cases} -1 & \text{on } \mathbb{Q}A, \\ 1 & \text{on } \mathbb{Q}\mathrm{Ann}_L(A) \end{cases}$$

と定義する．このとき $t_A(L) = L$ が成り立つので，t_A は格子 L の isometry すなわち $t_A \in O(L)$ である．t_A を，L の RSSD 部分格子 A に付随する **RSSD involution** という．t_A は，格子 L の isometry であること，および格子 A は階数 1 とは限らないことから，通常の鏡映の一般化と言える．

定理 5.3 ([8, Theorem 4.5]) L は正定値偶格子で，$L \supset N = \sqrt{2}A_{k-1}$ は L において RSSD であるとする．

(1) V_L は M^0 加群として σ 型である．

(2) $L(2) = \varnothing$ ならば，M^0 に付随する σ-involution $\sigma_{M^0} \in \mathrm{Aut}(V_L)$ は，L の RSSD 部分格子 N に付随する RSSD involution $t_N \in O(L)$ と対応する．ただし，

$$L(2) = \{\alpha \in L \mid \langle \alpha, \alpha \rangle = 2\}$$

である．

6 $V_{\sqrt{2}A_{k-1}}$ を経由しない σ-involution

第 5 節では (5.1) の形で $V_{\sqrt{2}A_{k-1}}$ に含まれる $K(\mathfrak{sl}_2, k)$ に付随する σ-ivolution を扱ったが，この節では $k = 5$ の場合にそれとは異なるタイプの $K(\mathfrak{sl}_2, k)$ に付随する σ-ivolution を紹介する．

Griess-Lam [3, 4] で考察されている次のような格子 Q を用いる．

$$Q \text{ は階数 } 16 \text{ の正定値偶格子で, } Q^*/Q \cong 5^4,\ Q(2) = \varnothing.$$

この性質を満たす格子 Q は，同型を除いて一意的に存在する．具体的には次のように記述できる．

(a) $Q = \mathrm{Ann}_\Lambda(\Lambda^g)$，ここで g は $O(\Lambda) = Co_0$ の $5B$ 元，$\Lambda^g = \{\alpha \in \Lambda \mid g(\alpha) = \alpha\}$ で，Λ は Leech 格子である．

(b) $Q = E + E'$，$E \cap E' = 0$ で，$E \cong E' \cong \sqrt{2}E_8$ である．ただし，E と E' は直交しない．

E と E' は SSD 格子だから，どちらも Q において RSSD である．付随する RSSD involution を，それぞれ $t_E, t_{E'} \in O(Q)$ とする．t_E と $t_{E'}$ の積を ν とおく: $\nu = t_E t_{E'} \in O(Q)$．$\nu$ は位数 5 で，Q には fixed-point-free に作用する．

Lam-Yamada-Yamauchi [9], Sakuma [13], Zheng [16] により，格子頂点作用素代数 V_Q は次のような頂点作用素代数を含むことがわかる．

$$V_Q \supset U_{5A} \supset W_1 \otimes W_2, \quad W_1 \cong W_2 \cong K(\mathfrak{sl}_2, 5).$$

U_{5A} は $W_1 \otimes W_2$ の $\mathbb{Z}_5$ 次数付き単純カレント拡大になっていて，このパラフェルミオン頂点作用素代数 W_1 と W_2 は (5.1) のような形で $V_{\sqrt{2}A_4}$ に含まれるものとして得られるのではない．

$\hat{\nu} \in \mathrm{Aut}(V_Q)$ を $\nu \in O(Q)$ の持ち上げとすると，$\langle\hat{\nu}\rangle = \langle\tau_{W_1}\rangle = \langle\tau_{W_2}\rangle$ が成り立つ．すなわち，$\hat{\nu}, \tau_{W_1}, \tau_{W_2}$ は $\mathrm{Aut}(V_Q)$ において同じ位数 5 の部分群を生成する．さらに，$\hat{\nu}$ の固定点について

$$V_Q^{\langle\hat{\nu}\rangle} \supset U_{5A}^{\langle\hat{\nu}\rangle} = W_1 \otimes W_2$$

が成り立つ．ただし，τ_{W_i} は定理 3.4 のものである．

$i = 1, 2$ について，$V_Q^{\langle\hat{\nu}\rangle}$ は W_i 加群として σ 型であるが，V_Q は σ 型ではない．したがって，σ_{W_i} は $V_Q^{\langle\hat{\nu}\rangle}$ の自己同型として定義できるが，V_Q の自己同型には拡張できない．

$V_Q^{\langle\hat{\nu}\rangle}$ の自己同型群は Lam [7] により決定されている．

定理 6.1 ([7]) $\mathrm{Aut}(V_Q^{\langle\hat{\nu}\rangle})$ は，$SO_6^+(5)$ とは異なる $GO_6^+(5)$ の指数 2 の部分群である．

格子 Q は，ν 不変な部分格子 $N \cong \sqrt{2}A_4$ の 4 個の直交和 N^4 を含み，$Q/N^4 \cong \mathbb{Z}_2^8$ となる．特に，N は Q において RSSD である．V_N において，(5.1) の M^0 に対応するものを W とおく．$W \subset V_Q^{\langle\hat{\nu}\rangle}$ であることに注意する．

定理 5.3 (1) により，W に付随する σ-involution $\sigma_W \in \mathrm{Aut}(V_Q)$ が定義できる．$W \subset V_Q^{\langle\hat{\nu}\rangle}$ なので，σ_W は $\hat{\nu}$ と可換で $V_Q^{\langle\hat{\nu}\rangle}$ の自己同型を引き起こす．$g \in N_{\mathrm{Aut}(V_Q)}(\langle\hat{\nu}\rangle)$ とすると，$g\sigma_W g^{-1} = \sigma_{g(W)}$ も $V_Q^{\langle\hat{\nu}\rangle}$ の自己同型を引き起こす．このような $g(W)$ 全部の集合を $\mathcal{W}$ とおく．上記の $\sigma_{W_i};\ i = 1, 2$ は V_Q の自己同型には拡張できないような $V_Q^{\langle\hat{\nu}\rangle}$ の自己同型である．一方で，$W \in \mathcal{W}$ ならば σ_W は V_Q の自己同型なので，それらは $\sigma_{W_i};\ i = 1, 2$ とは異なる σ-involution である．

$\sigma_W;\ W \in \mathcal{W}$ たちだけでは $\mathrm{Aut}(V_Q^{\langle\hat{\nu}\rangle})$ は生成できないが，$\sigma_{W_i};\ i = 1, 2$ も付け加えれば $\mathrm{Aut}(V_Q^{\langle\hat{\nu}\rangle})$ は生成される．すなわち，次の定理が成り立つ．

定理 6.2 ([8, Theorem 7.25]) 頂点作用素代数 $V_Q^{\langle\hat{\nu}\rangle}$ の自己同型群 $\mathrm{Aut}(V_Q^{\langle\hat{\nu}\rangle})$ は，σ-involution $\sigma_W;\ W \in \mathcal{W} \cup \{W_1, W_2\}$ たちで生成される．

注意 6.3 定理 6.2 の σ_{W_1}, σ_{W_2} のような特別な σ-involution は，$k = 3$ のときにも Lam-Yamauchi [10] で知られている．

参考文献

[1] Chongying Dong and Qing Wang, Quantum dimensions and fusion rules for parafermion vertex operator algebras, *Proc. Amer. Math. Soc.* **144** (2016), 1483–1492.

[2] Robert L. Griess, Jr., *An introduction to groups and lattices: finite groups and positive definite rational lattices*, Advanced Lectures in Mathematics (ALM), 15. International Press, Somerville, MA; Higher Education Press, Beijing, 2011.

[3] Robert L. Griess Jr. and Ching Hung Lam, EE_8-Lattices and dihedral groups, *Pure Appl. Math. Q.* **7** (2011), no. 3, Special Issue: In honor of Jacques Tits, 621–743.

[4] Robert L. Griess Jr. and Ching Hung Lam, A moonshine path for $5A$ and associated lattices of rank 8 and 16, *J. Algebra* **331** (2011), 338–361.

[5] Cuipo Jiang and Qing Wang, Representations of $\mathbb{Z}_2$-orbifold of the parafermion vertex operator algebra $K(sl_2, k)$, *J. Algebra* **529** (2019), 174–195.

[6] Cuipo Jiang and Qing Wang, Fusion rules for $\mathbb{Z}_2$-orbifolds of affine and parafermion vertex operator algebras, *Israel J. Math.* **240** (2020), 837–887.

[7] Ching Hung Lam, Automorphism group of an orbifold vertex operator algebra associated with the Leech lattice, *Vertex operator algebras, number theory and related topics*, *Contemp. Math.* **753**, Amer. Math. Soc., Providence, RI, (2020), 127–138.

[8] Ching Hung Lam and Hiromichi Yamada, Sigma involutions associated with parafermion vertex operator algebra $K(\mathfrak{sl}_2, k)$, arXiv:2012.10050.

[9] Ching Hung Lam, Hiromichi Yamada, and Hiroshi Yamauchi, McKay's observation and vertex operator algebras generated by two conformal vectors of central charge 1/2, *Internat. Math. Res. Papers* **3** (2005), 117–181.

[10] Ching Hung Lam and Hiroshi Yamauchi, On 3-transposition groups generated by σ-involutions associated to $c = 4/5$ Virasoro vectors, *J. Algebra* **416** (2014), 84–121.

[11] Masahiko Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra* **179** (1996), 523–548.

[12] Masahiko Miyamoto, 3-state Potts model and automorphisms of vertex operator algebras of order 3, *J. Algebra* **239** (2001), 56–76.

[13] Shinya Sakuma, 6-transposition property of τ-involutions of vertex operator algebras, *Internat. Math. Res. Not. IMRN 2007*, no. 9, Art. ID rnm 030, 19 pp.

[14] Weiqiang Wang, Rationality of Virasoro vertex operator algebras, *Int. Math. Res. Not.* **1993** (1993), no. 7, 197–211.

[15] A. B. Zamolodchikov and V. A. Fateev, Nonlocal (parafermion) currents in two-dimensional conformal quantum field theory and self-dual critical points in Z_N-symmetric statistical systems, *Sov. Phys. JETP* **62** (1985), 215–225.

[16] Wen Zheng, The VOAs generated by two Ising vectors e and f with $\langle e, f\rangle = \frac{1}{2^8}$, $|\tau_e\tau_f| = 3$ or $\frac{3}{2^9}$, *J. Algebra* **572** (2021), 60–75.

ヤコビ多項式とデザイン理論について

田中 優帆 *

Key Words: Codes, Jacobi polynomials, designs, invariant theory.
2010 *Mathematics Subject Classification.* Primary 11T71; Secondary 94B05, 11F11.

1 はじめに

本研究は，Himadri Shekhar Chakraborty 氏，三枝崎 剛氏，大浦 学氏との共同研究である．本稿は 2022 年 6 月 18 日に行った講演の内容に加筆したものであり，内容は，[4] に基づく．

本稿では，複数の参照ベクトルに関する符号のヤコビ多項式という概念を導入し，それに対する MacWilliams type identity を与える．さらに，Type III，IV の符号から得られたヤコビ多項式とデザインの関係を解釈するいくつかの事実について述べる．最後に，generalized t-デザインという概念を導入し，例を用いてヤコビ多項式との関係について述べる．

本稿の全てのコンピュータ計算は，Magma によって行った．

2 準備

ある素数 p に対して $q = p^f$ とし，$\mathbb{F}_q$ を位数 q の有限体とする．このとき，$\mathbb{F}_q^n$ を $\mathbb{F}_q$ 上の n 次元ベクトル空間とし，$\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_q^n$ の Hamming weight $\mathrm{wt}(\mathbf{u})$ を以下のように定義する．

$$\mathrm{wt}(\mathbf{u}) := |\mathrm{supp}(\mathbf{u})|, \text{ ここで, } \quad \mathrm{supp}(\mathbf{u}) = \{j \mid u_j \neq 0,\ 1 \leq j \leq n\}.$$

$\mathbf{u} = (u_1, u_2, \ldots, u_n), \mathbf{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q$ としたとき，2 つのベクトル $\mathbf{u}, \mathbf{v}$ の内積は以下のように定義する．

$$\mathbf{u} \cdot \mathbf{v} := \begin{cases} u_1 v_1 + \cdots + u_n v_n & \text{if } f \text{ is odd}, \\ u_1 \overline{v_1} + \cdots + u_n \overline{v_n} & \text{if } f \text{ is even}, \end{cases}$$

ここで，$\overline{v_i} := v_i^{\sqrt{q}}$ である．

n 次元ベクトル空間 $\mathbb{F}_q^n$ の部分空間 C を長さ n の $\mathbb{F}_q$ 線形符号といい，$\mathbb{F}_q$ 線形符号 C の元は符号語という．$\mathbb{F}_q$ 線形符号 C の双対符号 $C^\perp$ を以下のように定義する．

$$C^\perp := \{\mathbf{v} \in \mathbb{F}_q^n \mid \mathbf{u} \cdot \mathbf{v} = \mathbf{0} \text{ for all } \mathbf{u} \in C\}.$$

$C = C^\perp$ であるとき，$\mathbb{F}_q$ 線形符号 C は自己双対であるという．このとき，符号 C の長さ n は偶数であり，次元は $n/2$ であることが知られている．

*早稲田大学基幹理工学研究科

定義 2.1 (weight enumerator)**.** C **を長さ** n **の** $\mathbb{F}_q$ **線形符号とする．このとき，**C **の** weight enumerator $W_C(x,y)$ **は以下のように定義される．**

$$W_C(x,y) := \sum_{\mathbf{u}\in C} x^{n-\mathrm{wt}(\mathbf{u})} y^{\mathrm{wt}(\mathbf{u})}.$$

定義 2.2 (ヤコビ多項式). C **を長さ** n **の** $\mathbb{F}_q$ **線形符号とし，**1 **つの参照ベクトル** $\mathbf{w}\in\mathbb{F}_q^n$ **に対応する集合** T **を以下のように定義する．**

$$T := \mathrm{supp}(\mathbf{w}) \quad (T\subseteq\{1,2,\ldots,n\}) .$$

このとき，ヤコビ多項式 $J_{C,T}(w,z,x,y)$ **は次のように定義される．**

$$J_{C,T}(w,z,x,y) := \sum_{\mathbf{u}\in C} w^{m_0(\mathbf{u})} z^{m_1(\mathbf{u})} x^{n_0(\mathbf{u})} y^{n_1(\mathbf{u})},$$

ここで，

- $m_i(\mathbf{u}) = |\{j \mid u_j = i,\ j\in T\}|\ (i=0,1)$
- $n_i(\mathbf{u}) = |\{j \mid u_j = i,\ j\in [n]\setminus T\}|\ (i=0,1)$

である．

3 MacWilliams type identity

1 **つの参照ベクトルに関する** $\mathbb{F}_q$ **線形符号のヤコビ多項式に対する** MacWilliams type identity **は** [8] **で与えられている．本節では，**1 **つの参照ベクトルのみならず，複数の参照ベクトルに関する** $\mathbb{F}_q$ **線形符号のヤコビ多項式に対する** MacWilliams type identity **を与えたい．そのために，まず，複数の参照ベクトルに関する** $\mathbb{F}_q$ **線形符号のヤコビ多項式を定義する．**

定義 3.1 (ヤコビ多項式). C **を長さ** n **の** $\mathbb{F}_q$ **線形符号とする．そして，**ℓ **個の参照ベクトル** $\mathbf{w}_1,\ldots,\mathbf{w}_\ell\in\mathbb{F}_q^n$ **に関する** C **のヤコビ多項式を** $J_{C,\mathbf{w}_1,\ldots,\mathbf{w}_\ell}(\{x_{\mathbf{a}}\}_{\mathbf{a}\in\mathbb{F}_2^{\ell+1}})$ **と表し，**

$$J_{C,\mathbf{w}_1,\ldots,\mathbf{w}_\ell}(\{x_{\mathbf{a}}\}_{\mathbf{a}\in\mathbb{F}_2^{\ell+1}}) := \sum_{\mathbf{u}\in C}\prod_{\mathbf{a}\in\mathbb{F}_2^{\ell+1}} x_{\mathbf{a}}^{N_{\mathbf{a}}(\mathbf{u},\mathbf{w}_1,\ldots,\mathbf{w}_\ell)}.$$

のように定義する．ここで，

$$\phi(u_{ji}) = \begin{cases} 1 & \text{if } u_{ji}\neq 0, \\ 0 & \text{otherwise,}\end{cases}$$

とし，$\mathbf{a}=(\phi(u_{1i}),\ldots,\phi(u_{gi}))\in\mathbb{F}_2^g$ **を満たす** i **の数を** $N_{\mathbf{a}}(\mathbf{u}_1,\ldots,\mathbf{u}_g)$ **で表す．**

$\ell=1$ **のとき，この定義は** 1 **つの参照ベクトルに関するヤコビ多項式 （定義** 2.2**）と完全に同値であることに注意する．**

次に，$\mathbb{F}_q$ **の指標について見ていく（参考文献** [3, 6]**）．**$\mathbb{F}_q$ **の指標とは，加群** $\mathbb{F}_q$ **から複素数体の乗法群** $\mathbb{C}^\times$ **への準同型写像のことである．以下，非自明な** $\mathbb{F}_q$ **の指標を導く．**$F(x)$ **を** $\mathbb{F}_p$ **上の次数** f **の原始既約多項式とし，**λ **を** $F(x)$ **の根とする．このとき，任意の** $a\in\mathbb{F}_q$ **は次のように一意的に表される．**

$$a = a_0 + a_1\lambda + a_2\lambda^2 + \cdots + a_{f-1}\lambda^{f-1} \quad (a_i\in\mathbb{F}_p) .$$

各 $b \in \mathbb{F}_q$ に対して，$\mathbb{F}_q$ 上で χ_b を

$$\chi_b(a) = \zeta_p^{a_0 b_0 + \cdots + a_{f-1} b_{f-1}}, \quad \text{ここで，} \quad \zeta_p = e^{2\pi i/p} \quad (a \in \mathbb{F}_q).$$

と定義する．特に，$b = 0$ のとき，任意の $a \in \mathbb{F}_q$ に対して $\chi_b(a) = 1$ となり，これを $\mathbb{F}_q$ の自明な指標と呼ぶ．$b \neq 0$ のとき，χ_b は，ある $\mathbb{F}_q$ の非自明な指標である．χ を，ある $\mathbb{F}_q$ の非自明な指標とすると，χ は，任意の $a \in \mathbb{F}_q$ に対して以下のような性質を持つ.

$$\sum_{b \in \mathbb{F}_q} \chi(ab) := \begin{cases} q & \text{if} \quad a = 0, \\ 0 & \text{if} \quad a \neq 0. \end{cases}$$

指標 χ を用いると，以下の補題が成り立つ．

補題 3.1 ([6])．C を長さ n の $\mathbb{F}_q$ 線形符号とする．$\mathbf{v} \in \mathbb{F}_q^n$ に対して，$\delta_{C^\perp}(\mathbf{v})$ を以下のように定義する．

$$\delta_{C^\perp}(\mathbf{v}) := \begin{cases} 1 & \text{if } \mathbf{v} \in C^\perp, \\ 0 & \text{otherwise.} \end{cases}$$

このとき，以下が成り立つ．

$$\delta_{C^\perp}(\mathbf{v}) = \frac{1}{|C|} \sum_{\mathbf{u} \in C} \chi(\mathbf{u} \cdot \mathbf{v}).$$

上記の補題を用いることで，複数の参照ベクトルに関する $\mathbb{F}_q$ 線形符号のヤコビ多項式に対する MacWilliams type identity が得られた．

定理 3.1 (MacWilliams Identity)．C を長さ n の $\mathbb{F}_q$ 線形符号とし，χ を $\mathbb{F}_q$ の非自明な指標とする．$J_{C,\mathbf{w}_1,\ldots,\mathbf{w}_\ell}(\{x_{\mathbf{a}}\}_{\mathbf{a} \in \mathbb{F}_2^{\ell+1}})$ を参照ベクトル $\mathbf{w}_1, \ldots, \mathbf{w}_\ell \in \mathbb{F}_q^n$ に関する C のヤコビ多項式とする．このとき，

$$\begin{aligned} &J_{C^\perp,\mathbf{w}_1,\ldots,\mathbf{w}_\ell}(\{x_{\mathbf{a}}\}_{\mathbf{a} \in \mathbb{F}_2^{\ell+1}}) \\ &\quad = \frac{1}{|C|} J_{C,\mathbf{w}_1,\ldots,\mathbf{w}_\ell}\left(\left\{ \sum_{b \in \mathbb{F}_q} \chi(a_1 b) x_{(\phi(b),\phi(a_2),\ldots,\phi(a_{\ell+1}))} \right\}_{\mathbf{a} \in \mathbb{F}_q^{\ell+1}} \right). \end{aligned}$$

Proof. 補題 3.1 より，以下が成り立つ．

$$
\begin{aligned}
&J_{C^\perp,\mathbf{w}_1,\ldots,\mathbf{w}_\ell}(\{x_{\mathbf{a}}\}_{\mathbf{a}\in\mathbb{F}_2^{\ell+1}}) \\
&= \sum_{\mathbf{u}\in C^\perp} \prod_{\mathbf{a}\in\mathbb{F}_2^{\ell+1}} x_{\mathbf{a}}^{N_{\mathbf{a}}(\mathbf{u},\mathbf{w}_1,\ldots,\mathbf{w}_\ell)} \\
&= \sum_{\mathbf{v}\in\mathbb{F}_q^n} \delta_{C^\perp}(\mathbf{v}) \prod_{\mathbf{a}\in\mathbb{F}_2^{\ell+1}} x_{\mathbf{a}}^{N_{\mathbf{a}}(\mathbf{v},\mathbf{w}_1,\ldots,\mathbf{w}_\ell)} \\
&= \frac{1}{|C|} \sum_{\substack{\mathbf{u}\in C \\ \mathbf{v}\in\mathbb{F}_q^n}} \chi(\mathbf{u}\cdot\mathbf{v}) \prod_{\mathbf{a}\in\mathbb{F}_2^{\ell+1}} x_{\mathbf{a}}^{N_{\mathbf{a}}(\mathbf{v},\mathbf{w}_1,\ldots,\mathbf{w}_\ell)} \\
&= \frac{1}{|C|} \sum_{\substack{\mathbf{u}\in C \\ \mathbf{v}\in\mathbb{F}_q^n}} \chi(u_1v_1+\cdots+u_nv_n) \prod_{1\le i\le n} x_{(\phi(v_i),\phi(w_{1i}),\ldots,\phi(w_{\ell i}))} \\
&= \frac{1}{|C|} \sum_{\mathbf{u}\in C} \prod_{1\le i\le n} \left\{ \sum_{v_i\in\mathbb{F}_q} \chi(u_iv_i) x_{(\phi(v_i),\phi(w_{1i}),\ldots,\phi(w_{\ell i}))} \right\} \\
&= \frac{1}{|C|} \sum_{\mathbf{u}\in C} \prod_{\mathbf{a}\in\mathbb{F}_q^{\ell+1}} \left(\sum_{b\in\mathbb{F}_q} \chi(a_1b) x_{(\phi(b),\phi(a_2),\ldots,\phi(a_{\ell+1}))} \right)^{N_{\mathbf{a}}(\mathbf{u},\mathbf{w}_1,\ldots,\mathbf{w}_\ell)} \\
&= \frac{1}{|C|} J_{C,\mathbf{w}_1,\ldots,\mathbf{w}_\ell} \left(\left\{ \sum_{b\in\mathbb{F}_q} \chi(a_1b) x_{(\phi(b),\phi(a_2),\ldots,\phi(a_\ell+1))} \right\}_{\mathbf{a}\in\mathbb{F}_q^{\ell+1}} \right).
\end{aligned}
$$

□

4 デザインと Molien 級数

A. Bonnecaze 氏らは，Type II 符号を用いて，ヤコビ多項式とデザインとの関係に着目した（参考文献 [1]）．本節では，Type III，IV 符号を用いてヤコビ多項式とデザインの関係に着目する．なお，本節では，1 つの参照ベクトルに関するヤコビ多項式を用いて，表記や記号については [1] と同様のものを用いる．

まず，本節に必要な定義や概念を述べる．

定義 4.1 (Type III 符号)．C を長さ n（$n \equiv 0 \pmod 4$）の $\mathbb{F}_3$ 線形自己双対符号であるとする．任意の $c \in C$ に対して，$3 \mid \mathrm{wt}(c)$ であるとき，C を Type III 符号という．

定義 4.2 (Type IV 符号)．C を長さ n（$n \equiv 0 \pmod 2$）の $\mathbb{F}_4$ 線形自己双対符号であるとする．任意の $c \in C$ に対して，$2 \mid \mathrm{wt}(c)$ であるとき，C を Type IV 符号という．

以降，長さ n の Type III 符号を C_n^{III}，長さ n の Type IV 符号を C_n^{IV} で表す．

次に，本節で用いるデザインについて定義する．

定義 4.3 (t-$(n,k,\lambda_1^{a_1},\ldots,\lambda_N^{a_N})$ デザイン)．C を長さ n の $\mathbb{F}_q$ 線形符号とし，$C_k = \{\mathbf{u}\in C \mid \mathrm{wt}(\mathbf{u}) = k\}$ とする．$n > k > t > 0$ とする．

- $V = \{1,2,\ldots,n\}$
- $\mathcal{B}_k = \{\mathrm{supp}(\mathbf{u}) \mid \mathbf{u}\in C_k\}$

とおく．C_k がパラメータ t-$(v, k, \lambda_1^{a_1}, \ldots, \lambda_N^{a_N})$ を持つデザインであるとは，以下を満たすものである．

$\binom{V}{t} = \bigcup_{i=1}^{N} A_i$ (disjoint)，$A_1, \ldots, A_N \subseteq \binom{V}{t}$ ($a_i = |A_i|$) とおくと，任意の $i \in \{1, \ldots, N\}$，任意の $T \in A_i$ に対して，

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

を満たす λ_i（$\lambda_i \geq 0$）が存在する．

$N = 1$ のとき，単に C_k は t-デザインであるという．

定義 4.4 (t-homogeneous)．任意の k（$k \in \{1, 2, \ldots, n\}$，$C_k \neq \emptyset$）に対して，$C_k$ が t-デザインであるとき，符号 C は t-homogeneous であるという．

符号 C が t-homogeneous であるとき，ヤコビ多項式 $J_{C,T}$ は $|T| = t$ に対して，T に依存しない（補題 4.1）．便宜上，このヤコビ多項式は $J_{C,t}$ で表す．$J_{C,t}$ は符号 C の weight enumerator を用いて与えることができる．そのために，作用素について次のように定義する．

$P(w, z, x, y)$ を 4 変数多項式とし，作用素 A を以下のように定義する．

$$A.P(w, z, x, y) := w\frac{\partial}{\partial_x}P + z\frac{\partial}{\partial_y}P.$$

このとき，以下の補題が成り立つ．

補題 4.1 ([1])．符号 C が t-homogeneous であり，任意の $\mathbf{u} \in C$ に対して $\mathrm{wt}(\mathbf{u}) > t$ であるとき，

$$J_{C,t} = \frac{1}{n(n-1)\cdots(n-t+1)}A^t W_C.$$

次に，ヤコビ多項式について解析するために，必要な概念である，Molien 級数について述べる（参考文献 [7, 9]）．G を $GL(2, \mathbb{C})$ の有限部分群とし，G を 2 変数 x, y の多項式環に作用させるとする．このとき，1 変数 Molien 級数によって線形独立な同次不変多項式が得られることは，[9, Theorem 1] より知られている．その後，R.P. Stanley [10] は，w, z と x, y が同次である G の多項式を計算する 2 変数 Molien 級数という概念を導入し，次のように定義した．

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

以下，2 変数 Molien 級数 $f(u, v)$ の次数 d の部分を $f[d]$ と表記する．A. Bonnecaze 氏らは，符号のヤコビ多項式とデザインとの関係を記述するのに，2 変数 Molien 級数が重要な役割を果たすことを示した．その必要な 2 つのデザインについて，以下のように定義する．

定義 4.5 (packing design，covering design)．C を長さ n の $\mathbb{F}_q$ 線形符号とする．

- C_k は t-$(n, k, \lambda_1^{a_1}, \ldots, \lambda_N^{a_n})$ デザイン
- $\lambda = \max_i(\lambda_i)$（resp. $\lambda = \min_i(\lambda_i)$）

とする．このとき，C_k をパラメーター t-(n, k, λ) を持つ packing（resp. covering） design と呼び，ブロックの最大（resp. 最小）個数を $D_\lambda(n, k, t)$（resp. $C_\lambda(n, k, t)$）で表す．

なお，本稿で用いる packing （resp. covering） design は simple design である．

以下の例では，パラメータ t-(v, k, λ) を持つ t-デザインを保持する Type III，IV の 2 種類の符号を研究する．デザインのパラメータに対応する packing (resp. covering) design の $D_\lambda(v, k, t)$ (resp. $C_\lambda(v, k, t)$) の上界 (resp. 下界) を与えたい．そのために，まず，長さ d の符号に対応する $f[d]$ を計算する．$f[d]$ の係数は，$|T| = t$ である集合 T に対応するヤコビ多項式の空間を生成するために必要な多項式の数を決定する．そのヤコビ多項式の本数によって t-$(n, k, \lambda_1^{a_1}, \ldots, \lambda_N^{a_N})$ の λ の個数が決定される．最後に，符号の weight enumerator の項 $x^{n-k}y^k$ の係数から $D_\lambda(v, k, t)$（resp. $C_\lambda(v, k, t)$）の上界（resp. 下界）が得られる．

4.1 Type III 符号

Type III 符号の weight enumerator は，以下の 2 つの行列で生成される位数 48 の群 G_3 の作用に対して不変である．

$$\frac{1}{\sqrt{3}}\begin{bmatrix}1 & 2\\ 1 & -1\end{bmatrix} \text{ and } \begin{bmatrix}1 & 0\\ 0 & e^{2\pi i/3}\end{bmatrix}.$$

この 2 つの行列は，それぞれ MacWilliams identity と，法 3 に関して合同であることに対応している．群 G_3 の場合，Magma の計算から $f(u,v)$ の分母が $d(u)d(v)$ の形であることがわかる．ここで，$d(u)$ は以下の通りである．

$$d(u) = (u-1)^2(u+1)^2(u^2+1)^2(u^2-u+1)(u^2+u+1)(u^4-u^2+1).$$

以下，具体例を用いて，ヤコビ多項式とデザインの関係を観察する．

例 4.1 (length 8)．C_8^{III} を [5] における，長さ 8 の $\mathbb{F}_3$ 自己双対符号とする．

$$f[8] = u^8 + u^7v + 2u^6v^2 + 2u^5v^3 + 2u^4v^4 + 2u^3v^5 + 2u^2v^6 + uv^7 + v^8.$$

C_8^{III} は 1-デザインを持つから，補題 4.1 より，ヤコビ多項式は以下の通りである．

$$J_{C_8^{\mathrm{III}},1} = \frac{1}{8}AW_{C_8^{\mathrm{III}}}(x,y) = w(x^7 + 10x^4y^3 + 16xy^6) + z(6x^5y^2 + 48x^2y^5).$$

$|T| = 2$ のヤコビ多項式 $J_{C_8^{\mathrm{III}},T}$ の空間は以下の 2 本の多項式により生成される．

$$J^1_{C_8^{\mathrm{III}},2} = w^2(x^6 + 8x^3y^3) + wz(4x^4y^2 + 32xy^5) + z^2(4x^5y + 32x^2y^4),$$
$$J^2_{C_8^{\mathrm{III}},2} = w^2(4x^3y^3 + 4y^6) + wz(12x^4y^2 + 24xy^5) + 36z^2x^2y^4.$$

2 本の多項式を組み合わせると，以下のパラメータを持つ 2-デザインが得られる．

$$2\text{-}(8,3,(2^{12},0^{16})),$$
$$2\text{-}(8,6,(8^{12},9^{16})).$$

$k = 3\ell$ $(1 \le \ell \le 2)$ より，各ヤコビ多項式の z^ty^{k-t} $(t = 2,3)$ の項の係数を 2^ℓ で割ると，λ_1, λ_2 が得られる．さらに，weight enumerator の $x^{8-k}y^k$ の項を 2^ℓ で割ることにより，$D_\lambda(8,k,t)$ の上界 (resp. $C_\lambda(8,k,t)$ の下界) が得られるから，以下のような関係式が成り立つ．

$$D_2(8,3,2) \le 8 \le C_0(8,3,2),$$
$$D_9(8,6,2) \le 16 \le C_8(8,6,2).$$

同様に，$|T| = 3$ のヤコビ多項式 $J_{C_8^{\mathrm{III}},T}$ の空間は以下の 2 本の多項式により生成される．

$$J^1_{C_8^{\mathrm{III}},3} = w^3(x^5 + 8x^2y^3) + wz^2(6x^4y + 48xy^4) + z^3(2x^5 + 16x^2y^3),$$
$$J^2_{C_8^{\mathrm{III}},3} = w^3(x^5 + 2x^2y^3) + w^2z(10x^3y^2 + 8y^5) + wz^2(4x^4y + 32xy^4) + 24z^3x^2y^3,$$

さらに，以下のような関係式が得られる．

$$D_1(8,3,3) \le 8 \le C_0(8,3,3),$$
$$D_6(8,6,3) \le 16 \le C_4(8,6,3).$$

4.2 Type IV 符号

Type IV 符号の weight enumerator は，次の 2 つの行列で生成される位数 12 の群 G_4 の作用に対して不変であることがわかっている（参考文献 [7]）．

$$\frac{1}{2}\begin{bmatrix}1 & 3\\ 1 & -1\end{bmatrix} \text{ and } \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix},$$

この 2 つの行列は，それぞれ MacWilliams identity と法 2 に関して合同であることに対応している．群 G_4 の場合，Magma の計算から $f(u,v)$ の分母が $d(u)d(v)$ の形であることがわかる．ここで，$d(u)$ は以下の通りである．

$$d(u) = (1-u+u^2)(1+u+u^2)(1+2u^6+3u^{12}+4u^{18}+5u^{24}+6u^{30}+7u^{36}).$$

以下，Type III 符号と同様に，具体例を用いて，ヤコビ多項式とデザインの関係を観察する．

例 4.2 (length 6)．C_6^{IV} を [5] における，1 番目の長さ 6 の $\mathbb{F}_4$Hermitian 自己双対符号とする．

$$f[6] = 2u^6+2u^5v+3u^4v^2+3u^3v^3+3u^2v^4+2uv^5+2v^6.$$

C_6^{IV} は 1-デザインを持つから，補題 4.1 より，ヤコビ多項式は以下の通りである．

$$J_{C_6^{\mathrm{IV}},1} = \frac{1}{6}AW_{C_6^{\mathrm{IV}}}(x,y) = wx^5+6wx^3y^2+9wxy^4+3zx^4y+18zx^2y^3+27y^5.$$

$|T|=2$ のヤコビ多項式 $J_{C_6^{\mathrm{IV}},T}$ の空間は以下の 2 本の多項式により生成される．

$$J^1_{C_6^{\mathrm{IV}},2} = w^2(x^4+6x^2y^2+9y^4)+z^2(3x^4+18x^2y^2+27y^4),$$
$$J^2_{C_6^{\mathrm{IV}},2} = w^2(x^4+3x^2y^2)+wz(6x^3y+18xy^3)+z^2(9x^2y^2+27y^4).$$

2 本の多項式を組み合わせると，以下のパラメータを持つ 2-デザインが得られる．

$$2\text{-}(6,2,0^{12},1^3),$$
$$2\text{-}(6,4,1^{12},2^3).$$

$k=2\ell$ $(1\le\ell\le 2)$ より，各ヤコビ多項式の z^2y^{k-2} の項の係数を 3^ℓ で割ると，λ_1,λ_2 が得られる．さらに，以下のような関係式が得られる．

$$D_1(6,2,2)\le 3\le C_0(6,2,2),$$
$$D_2(6,4,2)\le 3\le C_1(6,4,2).$$

5 generalized t-デザインとヤコビ多項式

本節では前節の応用として，複数の参照ベクトルに関するヤコビ多項式を研究する．さらに，新たにデザインを定義し，ヤコビ多項式とデザインの関係にも着目する（参考文献 [2]）．

定義 5.1 (generalized t-デザイン)．C を長さ n の $\mathbb{F}_2$ 線形符号とし，$C_k=\{\mathbf{u}\in C \mid \mathrm{wt}(\mathbf{u})=k\}$ とする．

- $\{1,2,\ldots,n\}=\bigcup_{i=1}^m X_i$（disjoint）

- $\mathrm{supp}_{X_i}(\mathbf{u}) = \{j \in X_i \mid u_j \neq 0\}$（$\mathbf{u} \in C$）.
- $\mathcal{B}_w = \{(\mathrm{supp}_{X_1}(\mathbf{u}), \ldots, \mathrm{supp}_{X_m}(\mathbf{u})) \mid \mathrm{wt}(\mathbf{u}) = w,\ \mathbf{u} \in C\}$.
- $\mathbf{t} = (t_1, \ldots, t_m)$ such that $0 \leq t_i \leq \mathrm{supp}_{X_i}(\mathbf{u})$，$t = \sum_{i=1}^{m} t_i$ for all i.
- $\mathbf{v} = (|X_1|, |X_2|, \ldots, |X_m|)$
- $\mathbf{k} = (|\mathrm{supp}_{X_1}(\mathbf{u})|, |\mathrm{supp}_{X_2}(\mathbf{u})|, \ldots, |\mathrm{supp}_{X_m}(\mathbf{u})|)$

とおく．C_w がパラメータ $\mathbf{t}$-$(\mathbf{v}, \mathbf{k}, \lambda_1^{a_1}, \ldots, \lambda_N^{a_N})$ を持つデザインであるとは，以下を満たすものである．

$\binom{X_1}{t_1} \times \cdots \times \binom{X_m}{t_m} = \bigcup_{j=1}^{N} A_j$ （disjoint），$A_1, \ldots, A_N \subseteq \binom{X_1}{t_1} \times \cdots \times \binom{X_m}{t_m}$（$a_j = |A_j|$）とすると，任意の $j \in \{1, \ldots, N\}$，任意の $\mathbf{T} = (T_1, \ldots, T_m) \in A_j$（$t_i = |T_i|$）に対して，

$$\lambda_j = |\{(\mathrm{supp}_{X_1}(\mathbf{u}), \ldots, \mathrm{supp}_{X_m}(\mathbf{u})) \in \mathcal{B}_w \mid T_i \subseteq \mathrm{supp}_{X_i}(\mathbf{u}),\ 1 \leq \forall i \leq m\}|$$

を満たす λ_j（$\lambda_j \geq 0$）が存在する．

ただし，$\mathbf{k} = (k)$, $\mathbf{v} = (v)$，$N = 1$ の場合は，t-(v, k, λ) デザインまたは t-デザインの定義であることに注意する．

以下，具体例を用いて，ヤコビ多項式とデザインの関係を観察する．

例 5.1 (長さ 8 の $\mathbb{F}_2$ 線形自己双対符号). e_8 を [5] における，長さ 8 の $\mathbb{F}_2$ 線形自己双対符号とする．このとき，$X_1 = \{1, 2, 3, 6\},\ X_2 = \{4, 5, 7, 8\})$ とおくと，

$$\begin{aligned}\mathcal{B}_4 = \{&\{\{1,2\},\{5,7\}\}, (\{1,2\},\{4,8\}), (\{1,3\},\{4,5\}), (\{1,3\},\{7,8\}),\\ &(\{1,6\},\{5,8\}), (\{1,6\},\{4,7\}), (\{2,3\},\{4,7\}), (\{2,3\},\{5,8\}),\\ &(\{2,6\},\{4,5\}), (\{2,6\},\{7,8\}), (\{3,6\},\{4,8\}), (\{3,6\},\{5,7\})\}\end{aligned}$$

となる．$(e_8)_4$ が持つデザインのパラメータを考える．

$$\begin{aligned}\mathbf{t} &= (2,2),\\ a_1 = |A_1| &= |\{(\{1,2\},\{4,5\}), (\{1,2\},\{4,7\}), \ldots\}| = 24,\\ a_2 = |A_2| &= |\{(\{1,2\},\{5,7\}), (\{1,2\},\{4,8\}), \ldots\}| = 12,\end{aligned}$$

とおくと，

任意の $\mathbf{T} \in A_1$ に対して，

$\lambda_1 = |\{(\mathrm{supp}_{X_1}(\mathbf{u}), \mathrm{supp}_{X_2}(\mathbf{u})) \in \mathcal{B}_4 | T_i \subseteq \mathrm{supp}_{X_i}(\mathbf{u}), i = 1, 2\}| = 0,$

任意の $\mathbf{T} \in A_2$ に対して，

$\lambda_2 = |\{(\mathrm{supp}_{X_1}(\mathbf{u}), \mathrm{supp}_{X_2}(\mathbf{u})) \in \mathcal{B}_4 | T_i \subseteq \mathrm{supp}_{X_i}(\mathbf{u}), i = 1, 2\}| = 1$

したがって，$(e_8)_4$ は $(2,2)$-$((4,4),(2,2),0^{24},1^{12})$ デザインとなる．

さらに，2 つの参照ベクトルに対応する集合を $T_1, T_2 \subseteq \{1, 2, \ldots, 8\}$ とし，ヤコビ多項式 $J_{e_8,T_1,T_2}(w_0, z_0, x_0, y_0, w_1, z_1, x_1, y_1)$ を以下のように定義する．

$$J_{e_8,T_1,T_2}(w_0, z_0, x_0, y_0, w_1, z_1, x_1, y_1) := \sum_{\mathbf{u} \in e_8} w_0^{k_0(\mathbf{u})} z_0^{l_0(\mathbf{u})} x_0^{m_0(\mathbf{u})} y_0^{s_0(\mathbf{u})} w_1^{k_1(\mathbf{u})} z_1^{l_1(\mathbf{u})} x_1^{m_1(\mathbf{u})} y_1^{s_1(\mathbf{u})},$$

ここで，

- $k_i(\mathbf{u}) = |\{j \mid u_j = i,\ j \in T_1 \cap T_2\}|\ (i = 0, 1)$
- $l_i(\mathbf{u}) = |\{j \mid u_j = i,\ j \in T_1 \setminus T_2\}|\ (i = 0, 1)$
- $m_i(\mathbf{u}) = |\{j \mid u_j = i,\ j \in T_2 \setminus T_1\}|\ (i = 0, 1)$
- $s_i(\mathbf{u}) = |\{j \mid u_j = i,\ j \in \{1, 2, \ldots, 8\} \setminus T_1 \cup T_2\}|\ (i = 0, 1)$

である．これは $\ell = 2$ のときの定義 3.1 と同値であることに注意する．

ヤコビ多項式 J_{e_8,T_1,T_2} が $|T_1| = t_1, |T_2| = t_2$（$T_1 \cap T_2 = \emptyset$）に対して T_1, T_2 に依存しないとき，便宜上，このヤコビ多項式は $J_{e_8,(t_1,t_2)}$ で表す．このとき，以下のヤコビ多項式が得られる．

$$
\begin{aligned}
J_{e_8,(1,1)} &= z_0x_0y_0^6 + 4z_1x_0y_0^3y_1^3 + 3z_1x_1y_0^4y_1^2 + 3z_0x_0y_0^2y_1^4 + 4z_0x_1y_0^3y_1^3 + z_1x_1y_1^6,\\
J_{e_8,(2,1)} &= z_0^2x_0^2y_0^4 + 2z_1^2x_0y_0^3y_1^2 + z_1^2x_1y_0^4y_1 + 4z_0z_1x_0y_0^2y_1^3 + 4z_0z_1x_1y_0^3y_1^2\\
&\quad + z_0^2x_0y_0y_1^4 + 2z_0^2x_1y_0^2y_1^3 + z_1^2x_1y_1^5,\\
J_{e_8,(1,2)} &= z_0^2x_0^2y_0^4 + 2z_0x_1^2y_0^3y_1^2 + z_1x_1^2y_0^4y_1 + 4z_0x_0x_1y_0^2y_1^3 + 4z_1x_0x_1y_0^3y_1^2\\
&\quad + z_0x_0^2y_0y_1^4 + 2z_1x_0^2y_0^2y_1^3 + z_1x_1^2y_1^5.
\end{aligned}
$$

$|T_1| = 2, |T_2| = 2$（$T_1 \cap T_2 = \emptyset$）のヤコビ多項式 J_{e_8,T_1,T_2} の空間は以下の通りである．

$$
\begin{aligned}
J_{e_8,(2,2),1} &= z_0^2x_0^2y_0^4 + 2z_1^2x_0^2y_0^2y_1^2 + z_1^2x_1^2y_0^4 + 8z_0z_1x_0x_1y_0^2y_1^2 + z_0^2x_0^2y_1^4 + 2z_0^2x_1^2y_0^2y_1^2 + z_1^2x_1^2y_1^4,\\
J_{e_8,(2,2),2} &= z_0^2x_0^2y_0^4 + z_1^2x_0^2y_0^2y_1^2 + 2z_1^2x_0x_1y_0^3y_1 + 2z_0z_1x_0^2y_0y_1^3 + 4z_0z_1x_0x_1y_0^2y_1^2 + 2z_0z_1x_1^2y_0^3y_1\\
&\quad + 2z_0^2x_0x_1y_0y_1^3 + z_0^2x_1^2y_0^2y_1^2 + z_1^2x_1^2y_1^4.
\end{aligned}
$$

ヤコビ多項式 $J_{e_8,(t_1,t_2)}$ の本数と，$(e_8)_4$ が持つ (t_1, t_2)-デザインのパラメータにおける λ の個数は一致している．

6 謝辞

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

[2] P.J. Cameron, A generalisation of t-designs, *Discrete Math.*, **309**(2009), 4835–4842.

[3] H.S. Chakraborty, T. Miezaki, Variants of Jacobi polynomials in coding theory, *Des. Codes Cryptogr.*, https://doi.org/10.1007/s10623-021-00923-2

[4] H.S. Chakraborty, T. Miezaki, M. Oura, Y. Tanaka, Jacobi polynomials and design theory I, https://arxiv.org/abs/2207.10911

[5] M. Harada and A. Munemasa, Database of self-dual codes, https://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm.

[6] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, first edition, Elsevier/North Holland, New York, 1977.

[7] G. Nebe, E.M. Rains, N.J.A. Sloane, *Self-Dual Codes and Invariant Theory*, Algorithms and Computation in Mathematics, vol. **17**, Springer-Verlag, Berlin, 2006.

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

[9] N.J.A. Sloane, Error-correcting codes and invariant theory: New applications of a nineteenth-century technique, *Amer. Math. Monthly* **84** (1977), 82–107.

[10] R.P. Stanley, Invariants of finite groups and their applications to combinatorics, *Bull. (New Series) Amer. Math. Soc.* **1**(3) (1979), 475–511.

ON THE WEIGHTED TUTTE-GROTHENDIEC POLYNOMIALS OF GRAPHS

CHONG ZHENG

Faculty of Science and Engineering, Waseda University

1. Introduction

This note is based on the paper [6], which is a joint work with H. Chakraborty and T. Miezaki. In this note, we first give the notion of weighted (harmonic) chromatic polynomials of graphs. Moreover, we introduce the concept of weighted (harmonic) Tutte–Grothendieck polynomials of graphs and show a relation between the harmonic Tutte–Grothendieck polynomials of graphs and the harmonic Tutte polynomials of matroids. Furthermore, we present the concept of weighted Tutte–Grothendieck invariants of graphs and weighted Tutte invariants of matroids and give a relation between them. Finally, we give a remark on the categorification of the harmonic chromatic polynomials of graphs and harmonic Tutte polynomials of matroids. All the proof can be found in paper [6], and will not be given in this note.

2. Preliminaries

In this section, we give a brief discussion on graphs and matroids including the basic definitions and notations. We review [1, 4, 12] for this discussion. We also recall [2, 8] for the definition and properties of the (discrete) homogenous functions and (discrete) harmonic functions.

2.1. **Graphs.** Let $G := (V, E)$ be a graph, where V denotes the set of vertices, and E is the set of edges. An edge is usually incident with two vertices. But if the edge incident with equal end vertices, the edge is called a *loop*. A graph is called *simple* if it has neither loops nor multiple edges. A *path* in G is a sequence of edges $(e_1, e_2, \ldots, e_{m-1})$ having a sequence of vertices $(v_1, v_2, \ldots, v_n)$ satisfying $e_i \mapsto \{v_i, v_{i+1}\}$ for $i = 1, 2, \ldots, m-1$. A *circuit* in G is a sequence of edges $(e_1, e_2, \ldots, e_{m-1})$ having a sequence of vertices $(v_1, v_2, \ldots, v_n)$ satisfying $e_i \mapsto \{v_i, v_{i+1}\}$ for $i = 1, 2, \ldots, m-1$ and $v_1 = v_n = v$. A circuit that does not repeat vertices is called *cycle*. The *connected component* of G is a connected subgraph of G which is not a proper subgraph of another connected subgraph of G. A *bridge* of G is an edge whose removal increase the number of connected components of G by 1. Throughout this note, we assume that the graphs are finite and not necessary to be simple.

2.2. **Matroids.** Let E be a finite set of cardinality n and 2^E denotes the set of all subsets of E. A (finite) *matroid* M is an ordered pair $(E, \mathcal{I})$, where $\mathcal{I}$ is the collection of subsets of E satisfying the following conditions:

(M1) $\emptyset \in \mathcal{I}$.
(M2) $I \in \mathcal{I}$ and $J \subset I$ implies $J \in \mathcal{I}$.
(M3) $I, J \in \mathcal{I}$ with $|I| < |J|$ then there exists $j \in J$ such that $I \cup \{j\} \in \mathcal{I}$.

E-mail address: c_zheng@ruri.waseda.jp.
Key words and phrases. Tutte polynomials, chromatic polynomials, graphs, harmonic functions.

The elements of $\mathcal{I}$ are called the *independent* sets of M, and E is called the *ground set* of M. A subset of the ground set E that is not belongs to $\mathcal{I}$ is called *dependent*. For example, let $G = (V, E)$ be a finite graph. Let $\mathcal{I}$ be the set of all subsets A of E for which the subgraph (V, A) contains no cycle. Then G is a matroid (See [4, 14]). Such a matroid is called *graphic matroid*, and is denoted by M_G.

An independent set I is called a *maximal independent set* if it becomes dependent on adding any element of $E \setminus I$. It follows from the axiom (M3) that the cardinality of all the maximal independent sets in a matroid M is equal, called the *rank* of M. These maximal independent sets are called the *bases* of M. The *rank* $\rho(J)$ of an arbitrary subset J of E is the size of the largest independent subset of J. That is, $\rho(J) := \max_{I \subset J}\{|I| : I \in \mathcal{I}\}$. This implies ρ maps 2^E into $\mathbb{Z}$. This function ρ is called the *rank function* of M. In particular, $\rho(\emptyset) = 0$. We shall denote $\rho(E)$ the rank of M. We refer the readers to [12] for detailed discussion.

2.3. **Discrete homogeneous and harmonic functions.** Let $\Omega = \{1, 2, \ldots, n\}$ be a finite set. We define $\Omega_d := \{X \in 2^\Omega : |X| = d\}$ for $d = 0, 1, \ldots, n$. We denote by $\mathbb{R}2^\Omega$, $\mathbb{R}\Omega_d$ the real vector spaces spanned by the elements of 2^Ω, Ω_d, respectively. An element of $\mathbb{R}\Omega_d$ is denoted by

$$f := \sum_{Z \in \Omega_d} f(Z)Z \tag{1}$$

and is identified with the real-valued function on Ω_d given by $Z \mapsto f(Z)$. Such an element $f \in \mathbb{R}\Omega_d$ can be extended to an element $\widetilde{f} \in \mathbb{R}2^\Omega$ by setting, for all $X \in 2^\Omega$,

$$\widetilde{f}(X) := \sum_{Z \in \Omega_d, Z \subset X} f(Z). \tag{2}$$

If an element $g \in \mathbb{R}2^\Omega$ is equal to some $\widetilde{f}$, for $f \in \mathbb{R}\Omega_d$, we say that g has degree d. We call the vector space $\mathbb{R}\Omega_d$ the *homogeneous space* of degree d and denote by $\mathrm{Hom}_d(n)$. The differentiation γ is the operator defined by the linear form

$$\gamma(Z) := \sum_{Y \in \Omega_{d-1}, Y \subset Z} Y \tag{3}$$

for all $Z \in \Omega_d$ and for all $d = 0, 1, \ldots n$, and $\mathrm{Harm}_d(n)$ is the kernel of γ:

$$\mathrm{Harm}_d(n) := \ker\left(\gamma\big|_{\mathbb{R}\Omega_d}\right).$$

Remark 2.1 ([2, 8])**.** Let $f \in \mathrm{Harm}_d(n)$. Then $\gamma^{i-1}(f) = 0$ for all $0 \le i \le d-1$. That is, from (3) $\sum_{\substack{Z \in \Omega_d, \\ X \subset Z}} f(Z) = 0$ for any $X \in \Omega_i$.

Now we have the following technical lemma.

Lemma 2.1 ([2])**.** *Let $f \in \mathrm{Harm}_d(n)$ and $J \subset \Omega$. Let*

$$f^{(i)}(J) := \sum_{\substack{Z \in \Omega_d \\ |J \cap Z| = i}} f(Z).$$

Then for all $0 \le i \le d$, $f^{(i)}(J) = (-1)^{d-i}\binom{d}{i}\widetilde{f}(J)$.

Remark 2.2. From the definition of $\widetilde{f}$ for $f \in \mathrm{Harm}_d(n)$, we have $\widetilde{f}(J) = 0$ for any $J \in 2^\Omega$ such that $|J| < d$. Let $I, J \in 2^\Omega$ such that $I = \Omega \setminus J$. Then

$$\widetilde{f}(J) = \sum_{\substack{Z \in \Omega_d \\ Z \subset J}} f(Z) = \sum_{\substack{Z \in \Omega_d \\ |Z \cap I| = 0}} f(Z) = f^{(0)}(I) = (-1)^d \widetilde{f}(\Omega \setminus J).$$

We have from the above equality that if $|J| > n - d$, then $\widetilde{f}(J) = 0$.

For $X, Y \in 2^\Omega$, we introduce an operator $\circ$ on $\mathbb{R}2^\Omega$ as

$$\widetilde{f}(X) \circ \widetilde{f}(Y) := \widetilde{f}(X \cup Y),$$

which is associative, and distributive with respect to addition. Then we have the following remark.

Remark 2.3. Let $I \subset \Omega$ and $J \subset \Omega \setminus I =: I^c$. Then for $f \in \mathrm{Harm}_d(n)$ and by Remark 2.2, it is clear that

(i) $\widetilde{f}(I) \circ \widetilde{f}(I^c \setminus J) = \widetilde{f}(I) \circ \widetilde{f}(\Omega \setminus (J \cup I)) = (-1)^d \widetilde{f}(J)$,
(ii) $\widetilde{f}(I^c \setminus J) = \widetilde{f}(E \setminus (J \cup I)) = (-1)^d \widetilde{f}(I) \circ \widetilde{f}(J)$.

3. Weighted chromatic polynomials

In this section, we discuss the weighted chromatic polynomial of a graph which is sometimes called the homogeneous chromatic polynomial of a graph. For the definitions and notations of the classical chromatic polynomials of graphs we refer the readers to [1, 4].

Let $G = (V, E)$ be a graph. We assume that the number of edges is $|E| = n$. Let s be a bijective map from the edge set E to Ω, and $G(s)$ be a graph, where the edges are indexed by s. We call $G(s)$ the *labelled graph* and s the *label* of the graph G. For $A \subset E$, we denote by $N_A(\lambda)$ the number of λ-colouring such that the vertices adjacent to A have the same colour. Let f be a homogeneous function of degree d. Then the *weighted chromatic polynomial* of G associated with f and s is defined as:

$$\chi_f(G(s); \lambda) := \sum_{A \subset E} \widetilde{f}(s(E \setminus A))(-1)^{|A|} N_A(\lambda).$$

Let $G_A := (V, A)$ be the subgraph of G identified by A. We denote by $k(G_A)$ the number of connected components of G_A. Then $N_A(\lambda) = \lambda^{k(G_A)}$. Therefore the weighted chromatic polynomial $\chi_f(G(s); \lambda)$ can be written as:

$$\chi_f(G(s); \lambda) = \sum_{A \subset E} \widetilde{f}(s(E \setminus A))(-1)^{|A|} \lambda^{k(G_A)}.$$

In the same manner as above, we can define the weighted chromatic polynomial of a graph related to any map s instead of a bijective map. We will discuss the properties of such weighted chromatic polynomials in some subsequent papers [7]. In this paper, we only consider s as bijective.

If f is a harmonic function of degree d, we call $\chi_f(G(s); \lambda)$ the *harmonic chromatic polynomial* of G associated with f and s. When $f = 1$, we get the classical chromatic polynomial $\chi(G; \lambda)$ which is independent of the choice of s.

Remark 3.1. For a graph G with no edge and m vertices, we have

$$\chi_f(G(s); \lambda) = \widetilde{f}(\emptyset)\lambda^m,$$

where $f \in \mathrm{Hom}_d(n)$ and s is any label of G.

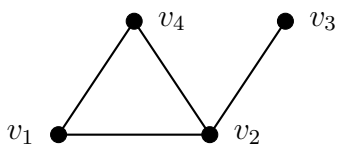


Figure 1. A graph with 4 vertices and 4 edges

Example 3.1. Let the graph G given in Figure 1. Let $\mathrm{Hom}_1(4) \ni f = a_1\{1\} + a_2\{2\} + a_3\{3\} + a_4\{4\}$. Let us consider the following label s for G: $\{v_1, v_2\} \mapsto 4$, $\{v_2, v_3\} \mapsto 1$, $\{v_2, v_4\} \mapsto 2$, $\{v_1, v_4\} \mapsto 3$. Then we have

$$\chi_f(G(s); \lambda) = (a_1 + a_2 + a_3 + a_4)(\lambda^4 - 3\lambda^3 + 3\lambda^2) - (a_1\lambda + a_2 + a_3 + a_4)\lambda.$$

For $f \in \mathrm{Harm}_1(4)$, we put $a_1 + a_2 + a_3 + a_4 = 0$.

Let $G = (V, E)$ be a graph. For an edge e of G, the *deletion* $G\backslash e$ is the graph obtained by removing e from the edge set E, and the *contraction* G/e is the graph obtained identifying end vertices of e keeping all other adjacencies remain the same.

Now we give the following recurrence formula that can be used to calculate the weighted chromatic polynomials.

Proposition 3.1. *Let $G = (V, E)$ be a graph and $f \in \mathrm{Hom}_d(n)$. Suppose e be an edge of G. Then for a label s of G, we have*

$$\chi_f(G(s); \lambda) = \widetilde{f}(s(e)) \circ \chi_f(G(s)\backslash e; \lambda) - \chi_f(G(s)/e; \lambda).$$

Now from the above proposition together with Remark 3.1 we have the following inductive formulation:

Proposition 3.2. *The weighted chromatic polynomials satisfies the following recursion:*

(a) *If G has m vertices and no edge, then $\chi_f(G(s); \lambda) = \widetilde{f}(\emptyset)\lambda^m$.*

(b) *If e is a loop, then*

$$\chi_f(G(s); \lambda) = \widetilde{f}(s(e)) \circ \chi_f(G(s) \setminus e; \lambda) - \chi_f(G(s) \setminus e; \lambda).$$

(c) *If e is a bridge, then*

$$\chi_f(G(s); \lambda) = \widetilde{f}(s(e)) \circ \chi_f(G(s) \setminus e; \lambda) - \frac{1}{\lambda}\chi_f(G(s) \setminus e; \lambda).$$

(d) *If e is neither a loop nor a bridge, then*

$$\chi_f(G(s); \lambda) = \widetilde{f}(s(e)) \circ \chi_f(G(s) \setminus e; \lambda) - \chi_f(G(s)/e; \lambda).$$

4. Weighted Tutte polynomials

In this section, we present a correspondence between the harmonic chromatic polynomials of a graph associated with a harmonic function of a degree d and the harmonic Tutte polynomials of a matroid associated with a harmonic function of degree d. We refer the reader to [1, 4] for the basic definitions and notations of the usual Tutte polynomial of a matroid.

Let $M = (E, \mathcal{I})$ be a matroid with rank function ρ. We assume that the cardinality of $|E| = n$. Let s be a bijective map from ground set E to Ω, and $M(s)$ be a matroid, where the elements of the ground set E are indexed by s. We call $M(s)$ the *labelled matroid* and s the *label* of the matroid M. Let f be a homogeneous function of degree d. Then the *weighted Tutte polynomial* of M associated with f and s is defined in [5] as follows:

$$T_f(M(s); x, y) := \sum_{J \subset E} \widetilde{f}(s(J))(x-1)^{\rho(E)-\rho(J)}(y-1)^{|J|-\rho(J)}.$$

In a graphic matroid, s is a label for the matroid if and only if s is a label for the underlying graph.

In the definition of the weighted Tutte polynomial of a matroid, we can consider any map s instead of only a bijective map in a similar way as above. We will discuss the properties of such weighted Tutte polynomials in some subsequent papers [7]. In this paper, we consider s as a bijective mapping.

If f is a harmonic function of degree d, then $T_f(M(s); x, y)$ is called the *harmonic Tutte polynomial* of M associated to f and s. If $f = 1$, then the weighted (harmonic) Tutte polynomials

become the classical Tutte polynomial $T(M;x,y)$ independent of the label s. Let $G=(V,E)$ be graph. Then for any $A\subset E$, we define

$$\rho(A) := |V| - k(G_A).$$

Therefore, we find that M_G is a matroid associated to G having rank function ρ.

Example 4.1. From Example 3.1, we have the weighted Tutte polynomial as below:

$$\begin{aligned} T_f(M_G(s);x,y) = (a_1+a_2+a_3+a_4)(x-1)^2 + (a_2+a_3+a_4)(x-1)(y-1) \\ + 3(a_1+a_2+a_3+a_4)(x-1) + 2(a_1+a_2+a_3+a_4) + a_1 \end{aligned}$$

Remark 4.1. For $A\subset E$, $\rho(A)+k(G_A)=|V|=\rho(E)+k(G)$.

Before giving a recurrence formula for the calculation of the weighted Tutte polynomials, we recall [4] for the definitions of the loop, coloop, deletion and contraction from the matroid theoretical point of view.

Let $M=(E,\mathcal{I})$ be a matroid. An element $e\in E$ is called a *loop* if $\{e\}\notin\mathcal{I}$, or equivalently, if $\rho(\{e\})=0$. In a graphic matroid, e is a loop if and only if it is a loop of the underlying graph. An element $e\in E$ is a *coloop* if it is contained in every basis of M. This implies $\rho(A\cup\{e\})=\rho(A)+1$, whenever $e\notin A$. In a graphic matroid, e is a coloop if and only if it is a bridge. The *deletion* of $e\in E$ is a matroid $M\backslash e$ on the set $E\setminus\{e\}$ containing the independent sets of M which are contained in $E\setminus\{e\}$. In a graphic matroid, deletion of e corresponds to deletion of the edge e from the graph. The *contraction* of e is the matroid M/e on the set $E\setminus\{e\}$ in which a set A is independent if and only if $A\cup\{e\}$ is independent in M. In a graphic matroid, contraction of e corresponds to contraction of the edge e.

Proposition 4.1. *Let $M=(E,\mathcal{I})$ be a matroid with rank function ρ and $f\in \mathrm{Hom}_d(n)$. Suppose $e\in E$. Then for a label s of M, we have*

(a) $T_f(\emptyset;x,y)=\widetilde{f}(\emptyset)$, *where $\emptyset$ is the empty matroid.*
(b) *If e is a loop, then* $T_f(M(s);x,y)=T_f(M(s)\backslash e;x,y)+(y-1)\widetilde{f}(s(e))\circ T_f(M(s)\backslash e;x,y)$.
(c) *If e is a coloop, then* $T_f(M(s);x,y)=(x-1)T_f(M(s)/e;x,y)+\widetilde{f}(s(e))\circ T_f(M(s)/e;x,y)$.
(d) *If e is neither a loop nor a coloop, then*

$$T_f(M(s);x,y)=T_f(M(s)\backslash e;x,y)+\widetilde{f}(s(e))\circ T_f(M(s)/e;x,y).$$

The following result shows a correspondence between the harmonic chromatic polynomials and the harmonic Tutte polynomials.

Theorem 4.1. *Let $G=(V,E)$ be a graph with $|V|=m$ and $|E|=n$. Let $f\in \mathrm{Harm}_d(n)$. Then for any label s of G, we have*

$$\chi_f(G(s);\lambda)=(-1)^{\rho(E)+d}\lambda^{k(G)}T_f(M_G(s);1-\lambda,0).$$

5. Harmonic Tutte–Grothendieck polynomials

In this section, we present the concept of harmonic Tutte–Grothendieck polynomial (harmonic T–G polynomial). Moreover, we give a generalization of the classical relation known as the recipe theorem between the Tutte–Grothendieck invariants and the Tutte polynomials to the case of harmonic T–G polynomials.

Definition 5.1. Let $G=(V,E)$ be a graph with number of edges n. Let s be a label of G, and e be an edge of G. Let $f\in \mathrm{Hom}_d(n)$. Then the *weighted Tutte-Grothendieck polynomial* of G associated to f and s is denoted by $\Phi_f(G(s)) := \Phi_f(G(s);X,Y,\alpha,\beta)$ and defined recursively for $\alpha\neq 0$ and $\beta\neq 0$ as follows:

(a) If G has no edge, then $\Phi_f(G(s))=\widetilde{f}(\emptyset)$.
(b) If e is a loop, then

$$\Phi_f(G(s))=\alpha\widetilde{f}(s(e))\circ\Phi_f(G(s)\backslash e)+(Y-\alpha)\Phi_f(G(s)\setminus e).$$

(c) If e is a bridge, then

$$\Phi_f(G(s)) = X'Y'\widetilde{f}(s(e)) \circ \Phi_f(G(s)\backslash e) + \beta Y'\Phi_f(G(s)\backslash e),$$

where $X' = X - \beta$ and $Y' := \dfrac{Y-\alpha}{\alpha}$.

(d) If e is neither a loop nor a bridge, then

$$\Phi_f(G(s)) = \alpha\widetilde{f}(s(e)) \circ \Phi_f(G(s)\backslash e) + \beta\Phi_f(G(s)/e).$$

If f is a harmonic function of degree d, then we call $\Phi_f(G(s))$ the *harmonic Tutte–Grothendieck polynomial* of G associated to f and s.

Remark 5.1. If $f \in \mathrm{Harm}_d(n)$, then by Remark 2.3, we have instantly that $\Phi_f(G(s)) = (-1)^d P_f(G(s))$, where $P_f(G(s)) := P_f(G(s); X, Y, \alpha, \beta)$ is a polynomial of G associated with f and s satisfying the following recurrence for $\alpha \neq 0$ and $\beta \neq 0$:

(a) If G has no edge, then $P_f(G(s)) = \widetilde{f}(\emptyset)$.

(b) If e is a loop, then

$$P_f(G(s)) = \alpha P_f(G(s)\backslash e) + (Y-\alpha)\widetilde{f}(s(e)) \circ P_f(G(s)\backslash e).$$

(c) If e is a bridge, then

$$P_f(G(s)) = X'Y'P_f(G(s)\backslash e) + \beta Y'\widetilde{f}(s(e)) \circ P_f(G(s)\backslash e),$$

where $X' = X - \beta$ and $Y' = \dfrac{Y-\alpha}{\alpha}$.

(d) If e is neither a loop nor a bridge, then

$$P_f(G(s)) = \alpha P_f(G(s)\backslash e) + \beta\widetilde{f}(s(e)) \circ P_f(G(s)/e).$$

Now we give a generalization of the recipe theorem which presents a relation between the harmonic T–G polynomial and the harmonic Tutte polynomial as follows.

Theorem 5.1. *Let $G = (V, E)$ be a graph with $|E| = n$, and M_G be a matroid associated with G. Let $\Phi_f(G(s); X, Y, \alpha, \beta)$ be a harmonic T–G polynomial of G related to $f \in \mathrm{Harm}_d(n)$ and a label s of G. Then for $\alpha \neq 0$ and $\beta \neq 0$, we have*

$$\Phi_f(G(s); X, Y, \alpha, \beta) = (-1)^d \alpha^{|E|-|V|+k(G)} \beta^{|V|-k(G)} T_f\left(M_G(s); \frac{X}{\beta}, \frac{Y}{\alpha}\right). \tag{4}$$

Example 5.1. If we take $\Phi_f(G(s)) = \dfrac{\chi_f(G(s))}{\lambda^{k(G)}}$ with $f \in \mathrm{Hom}_d(n)$, $X = \lambda - 1$, $Y = 0$, $\alpha = 1$ and $\beta = -1$, we immediately get the weighted chromatic polynomial. Moreover, Theorem 5.1 implies Theorem 4.1 when $f \in \mathrm{Harm}_d(n)$.

6. Weighted invariants for graphs and matroids

Tutte [13] pointed out an idea of graph invariant which is known as Tutte–Grothendieck invariant (T–G invariant) for all functions that satisfy deletion-contraction recurrence was thoroughly developed and generalized by Brylawski [3]. Motivated by the concept of T–G invariant, in this section, we introduce the notion of weighted T–G invariant which is also called harmonic T–G invariant in some particular cases.

Weighted T–G invariants. Let $G = (V, E)$ be a graph with $|E| = n$. Let s be a label of G. We denote the set of all labels s of G by $S(G)$. It is easy to compute that $\sharp S(G) = n!$. Now we define

$$\widehat{\Phi}_f(G) := \sum_{s \in S(G)} \Phi_f(G(s)). \tag{5}$$

Remark 6.1. For $f = 1$, $\widehat{\Phi}_f(G) = n!\Phi(G)$, where $\Phi(G)$ is the classical T–G invariant.

We denote by S_n the symmetric group of order n. Then the following result is immediate from the construction of $\widehat{\Phi}_f(G)$.

Theorem 6.1. *Let $G = (V, E)$ be a graph with $|E| = n$. Then for any $f \in \mathrm{Hom}_d(n)$, we have*

(i) *$\widehat{\Phi}_f(G)$ is an invariant for graphs.*
(ii) *Let $R(f) := \sum_{\sigma \in S_n} \sigma f$. Then $\Phi_{R(f)}(G)$ is an invariant for graphs, where $\Phi_{R(f)}(G)$ denotes the weighted T–G polynomial of G associated to $R(f)$ and independent of the choice of s. Moreover, $\widehat{\Phi}_f(G) = \Phi_{R(f)}(G)$.*
(iii) *Let $\sigma f = f$ for all $\sigma \in S_n$. Then $\Phi_f(G)$ is an invariant for graphs. Also, $\widehat{\Phi}_f(G) = n!\Phi_f(G)$.*

We call $\widehat{\Phi}_f(G)$ the *weighted Tutte–Grothendieck invariant* for graphs. If $f \in \mathrm{Harm}_d(n)$, we call $\widehat{\Phi}_f(G)$ the *harmonic Tutte–Grothendieck invariant* for graphs, which is zero for $d \neq 0$.

Weighted Tutte invariants. Let M be a matroid with ground set E of cardinality n. Let s be a label of M. Define

$$\widehat{T}_f(M; x, y) := \sum_{s \in S(M)} T_f(M(s); x, y),$$

where $S(M)$ interprets a similar meaning as $S(G)$ for the case of graphs.

Remark 6.2. For $f = 1$, $\widehat{T}_f(M; x, y) = n!T(M; x, y)$.

Theorem 6.2. *Let $M = (E, \mathcal{I})$ be a matroid with $|E| = n$. Then for any $f \in \mathrm{Hom}_d(n)$, we have*

(i) *$\widehat{T}_f(M)$ is an invariant for graphs.*
(ii) *Let $R(f) := \sum_{\sigma \in S_n} \sigma f$. Then $T_{R(f)}(M)$ is an invariant for matroids, where $T_{R(f)}(M)$ denotes the weighted Tutte polynomial of M associated to $R(f)$ and independent of the choice of label s. Moreover, $\widehat{T}_f(M) = T_{R(f)}(M)$.*
(iii) *Let $\sigma f = f$ for all $\sigma \in S_n$. Then $T_f(M)$ is an invariant for matroids. Also, $\widehat{T}_f(M) = n!T_f(M)$.*

We call $\widehat{T}_f(M; x, y)$ the *weighted Tutte invariant* for matroids. If $f \in \mathrm{Harm}_d(n)$, we call $\widehat{T}_f(M; x, y)$ the *harmonic Tutte invariant* for matroids which is zero for $d \neq 0$.

Example 6.1. Let M_1 be a vector matroid over $\mathbb{F}_2$ and M_2 be a vector matroid over $\mathbb{F}_3$ as given below:

$$M_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 2 & 1 & 0 & 1 & 0 & 1 & 2 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 \end{pmatrix}.$$

We have checked numerically that for all $f \in \mathrm{Hom}_d(7)$ $(1 \leq d \leq 7)$, $\widehat{T}_f(M_1, x, y) = \widehat{T}_f(M_2, x, y)$. For the construction of vector matroids, we refer the readers to [4].

Problem 6.1. Find a non-isomorphic matroid pair (M_1, M_2) having the same Tutte polynomial but the different weighted Tutte invariants.

The following result gives a correspondence between the weighted T–G invariant and the weighted Tutte invariant which is an analogue to Theorem 5.1.

Theorem 6.3. *Let $\widehat{\Phi}_f$ be a weighted T–G invariant associated to $f \in \mathrm{Hom}_d(n)$. Then for all graphs $G = (V, E)$ we have*

$$\widehat{\Phi}_f(G) = \alpha^{|E|-|V|+k(G)} \beta^{|V|-k(G)} \widehat{T}_f\left(M_G; \frac{X}{\beta}, \frac{Y}{\alpha}\right), \tag{6}$$

where X, Y, α, β interpret the same meaning as in weighted T–G polynomials associated to f.

Weighted chromatic invariant. Let s be a label of a graph G with n edges. Then from Example 5.1, if we take $\Phi_f(G(s)) = \frac{\chi_f(G(s))}{\lambda^{k(G)}}$ with $f \in \mathrm{Hom}_d(n)$, $X = \lambda - 1$, $Y = 0$, $\alpha = 1$ and $\beta = -1$, we get from definition (5) that

$$\widehat{\chi}_f(G(s)) = \sum_{s \in S(G)} \chi_f(G(s)),$$

which is from Theorem 6.1, an invariant for graphs. We call this invariant the *weighted chromatic invariant* for graphs. When $f \in \mathrm{Harm}_d(n)$, we call this invariant the *harmonic chromatic invariant* for graphs which is zero for $d \neq 0$. Moreover, Theorem 6.3 yields therefore the following corollary.

Corollary 6.1. *We have*

$$\widehat{\chi}_f(G;\lambda) = (-1)^{\rho(E)}\lambda^{k(G)}\widehat{T}_f(M_G; 1-\lambda, 0).$$

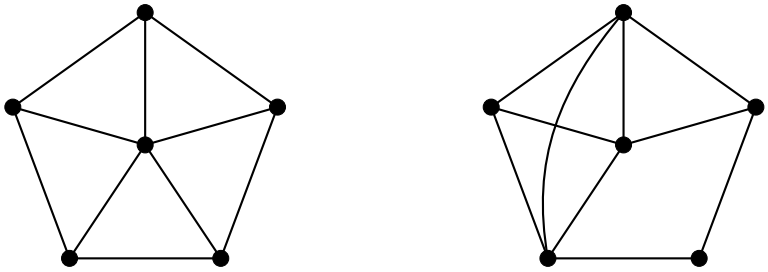


FIGURE 2. Two non-isomorphic graphs

Example 6.2. Let G_1 and G_2 be two non-isomorphic graphs shown in Figure 2 having the same classical chromatic polynomials. Then we have $\Omega = \{1, 2, \ldots, 10\}$. Let $f = \sum_{X \in \Omega_4} X$. Then the weighted chromatic invariant for G_1 is

$$\widehat{\chi}_f(G_1;\lambda) = 10! \times (210\lambda^6 - 1260\lambda^5 + 2975\lambda^4 - 3450\lambda^3 + 1960\lambda^2 - 435\lambda),$$

whereas the weighted chromatic invariant for G_2 is

$$\widehat{\chi}_f(G_2;\lambda) = 10! \times (210\lambda^6 - 1260\lambda^5 + 2975\lambda^4 - 3434\lambda^3 + 1925\lambda^2 - 416\lambda).$$

Therefore, $\widehat{\chi}_f(G_1;\lambda) \neq \widehat{\chi}_f(G_2;\lambda)$. This concludes that the weighted chromatic invariants is stronger than the classical chromatic polynomials.

7. Homological Categorifications of weighted polynomials

Originated from category theory, a *categorification* in homology theory usually means to categorify a quantity or a polynomial with some homology groups. For example, Khovanov homology is a categorification of Jone's polynomial, Floer homology is a categorification of Alexander-Conway polynomial, and Magnitude homology is a categorification of magnitude.

In this section, we apply the method in [10] and [11] to construct chain complexes and give categorifications to the weighted chromatic polynomial and weighted Tutte polynomial, respectively. We omit some basic facts of algebraic topology and homological algebra. Some definitions succeeded from [10] and [11] are also omitted.

We categorify the weighted polynomial by assigning a real-valued weight to the specially constructed chain complexes, and show the relationship between the chain complexes and our invariant in Section 6. We will write another paper to discuss general weighted chain complex, and discuss only special cases in this paper.

7.1. **A Categorification of Harmonic Chromatic Polynomial.** Let $\mathcal{M}$ be a free $\mathbb{Z}$-module with $\mathcal{M} = M_0 \oplus M_1$, where M_0 and M_1 are subgroups of $\mathcal{M}$ and are generated by basis element 1 and x, respectively. Hence $\mathcal{M}$ can be considered as a graded free $\mathbb{Z}$-module with non-trivial elements only at degree 0 and 1.

Definition 7.1. Let $G(s) = (V, E)$ be a labelled graph with n edges. We use a vector $\epsilon = (\epsilon_1, \epsilon_2, \ldots, \epsilon_n) \in \{0,1\}^n$ to represent any given subgraph $G(s)'$ of $G(s)$ whose vertices are V. Precisely, for $i = 1, 2, \ldots, n$, if the i-th edge exists in $G(s)'$, then we let $\epsilon_i = 1$; and $\epsilon_i = 0$ otherwise. We call ϵ the *edge vector* of $G(s)$. Given any edge vector, we also denote the corresponding subgraph G_ϵ. We denote by $l(\epsilon)$ the number of 1s in edge vector ϵ. Let $\mathcal{E}^a(G(s))$ be the set of all edge vectors ϵ with $l(\epsilon) = a$, $a \in \mathbb{N}$.

In order to construct a cochain complex with M, we first define the cochain group as follows.

Definition 7.2. The *q-th chromatic cochain group* of a graph G is defined as

$$C^q(G(s)) := \bigoplus_{l(\epsilon)=q} M^{\otimes k(G_\epsilon)},$$

where $\otimes$ denotes tensor product.

We also write

$$C^q(G(s)) = \bigoplus_{j \geq 0} C^{i,j}(G(s)),$$

where $C^{q,j}(G(s))$ denotes the elements of degree j of $C^q(G(s))$. Hence $C^q(G(s))$ can also be considered as a bigraded module.

Let $f : 2^\Omega \to \mathbb{R}$ be a discrete function of degree d. Since each $M^{\otimes k(G_\epsilon)}$ corresponds to an edge vector ϵ, by the definition, it also corresponds to an f-value. Therefore, besides the dimension of the graded module, we can assign a weighted dimension to the graded module, where the weight is given by f-values. We begin with the definition of weighted rank as follows.

Definition 7.3. Let G be a $\mathbb{Z}$-module with decomposition $G = \bigoplus_i G_i$. We suppose that for each G_i, there is a corresponding f-value. Then we define the f-rank of G as

$$f\mathrm{rank}(G) := \sum_i f(G_i) \cdot \dim_{\mathbb{Q}}(G_i \otimes \mathbb{Q}).$$

Note that $\dim_{\mathbb{Q}}(G_i \otimes \mathbb{Q})$ is known as the *rank* of G_i.

Definition 7.4. Let $\mathcal{N} = \bigoplus_i N_i$ be a graded $\mathbb{Z}$-module with an f-value $f(\mathcal{N})$, where N_i denotes the set of homogeneous elements of degree i. The *graded dimension* of $\mathcal{N}$ is defined as

$$q\dim(\mathcal{N}) := \sum_i q^i \cdot \mathrm{rank}(N_i),$$

and the *f-value graded dimension of $\mathcal{N}$* is defined as

$$fq\dim(\mathcal{N}) := \sum_i q^i \cdot f\mathrm{rank}(N_i).$$

Lemma 7.1. *Let $\mathcal{N}$, $\mathcal{G}$, and $\mathcal{H}$ be graded modules with f-values and $\mathcal{N} = \mathcal{G} \oplus \mathcal{H}$. Then*

$$fq\dim(\mathcal{N}) = fq\dim(\mathcal{G}) + fq\dim(\mathcal{H}).$$

According to the above lemma, we can calculate as an example that for two graded module $\mathcal{M}$ defined above, suppose that they correspond to f-values a_1 and a_2, then $fq\dim(\mathcal{M} \oplus \mathcal{M}) = (a_1 + a_2)(1 + q)$, and $fq\dim(\mathcal{M}^{\otimes m} \oplus \mathcal{M}^{\otimes n}) = a_1(1 + q)^m + a_2(1 + q)^n$.

The desired chain complex is constructed by the cochain group above and a *coboundary operator*. A coboundary operator is a module homomorphism between two cochain groups whose dimensions differ by 1. By the correspondence between cochain groups and edge vectors, the coboundary operator is induced by a map that increases exactly one edge.

We define the coboundary operator by defining a map for its each element module, and then linearly extend them. Let $d_\epsilon : \mathcal{E}^a(G(s)) \to \mathcal{E}^{a+1}(G(s))$ be a map that is identity on all elements but changes exact one 0 to 1. For an edge $\tilde{e}$, if adding the edge does not change the number of connected components, then we define the element module map $\tilde{d_\epsilon} : M^{\otimes k} \to M^{\otimes k}$ to be the identity map. On the other hand, if the added edge $\tilde{e}$ joins two connected components, that is, the number of connected components decreases by one, then we define the element module map $\tilde{d_\epsilon} : M^{\otimes k} \to M^{\otimes k-1}$ to be identity on the tensor elements which are irrelevant to this process. Moreover, for the two components that are connected, the map is defined to be $M \otimes M \to M$ with $m(1 \otimes 1) = 1$, $m(1 \otimes x) = m(x \otimes 1) = x$, and $m(x \otimes x) = 0$.

Definition 7.5. The coboundary operator $d^q : C^q(G(s)) \to C^{q+1}(G(s))$ is defined as

$$d^q := \sum_{l(\epsilon)=q} (-1)^{n(\epsilon)} \tilde{d}_\epsilon,$$

where $n(\epsilon) = \sum_{i=1}^{k_0} \epsilon_i$, and k_0 is the index of the new-added edge in the given order.

By definition and simple calculation, it is uncomplicated to verify the following statements.

Lemma 7.2. *The following statements are true.*

(1) *d is degree preserving.*
(2) *$d \circ d = 0$.*

(2) of Lemma 7.2 implies that $(C^\star, d^\star)$ forms a cochain complex. We denote by $H^\star(G) := \ker(d^q)/\mathrm{im}(d^{q-1})$, the corresponding cohomology, where $\ker(d^q)$ denotes the kernel of d^q, and $\mathrm{im}(d^{q-1})$ denotes the image of d^{q-1}. It is shown in [10] that, the cochain complex does not depend on the choice of the order s.

Definition 7.6. The *graded Euler number* of a cochain complex $(C^\star, d^\star)$ is defined as $Euler_i(C) := \sum_i (-1)^i \cdot q\dim(H^i)$. Also, the *weighted graded Euler number* corresponding to a function f of $(C^\star, d^\star)$ is defined as $wEuler(C)_i := \sum_i (-1)^i \cdot fq\dim(H^i)$.

By (1) of Lemma 7.2, the coboundary operator d is degree preserving, hence the (weighted) graded Euler number is also equal to the alternative sum of the $(f)q\dim$ of cochain groups, those are $Euler_i(C) = \sum_i (-1)^i q\dim(C^i)$, and $wEuler_i(C) = \sum_i (-1)^i fq\dim(C^i)$.

When f is a discrete harmonic function it follows from the definition of harmonic polynomial, we have the following relationship between harmonic polynomial and the chain complex constructed. This relationship gives a weighted categorification to harmonic chromatic polynomials.

Theorem 7.1. *Let $G(s) = (V, E)$ be a labelled graph and f a discrete harmonic function on E, then*

$$\chi_f(G(s)) = \sum_i (-1)^{i+1} \cdot fq\dim(C^i(G(s))).$$

Also,

$$\widehat{\chi}_f(G) = \sum_s \sum_i (-1)^{i+1} \cdot fq\dim(C^i(G(s))).$$

Example 7.1. We calculate the weighted chain complex and the weighted chromatic polynomial of graph G as an example. Let $G = (V, E)$ be the following graph, and $f : E \to \mathbb{R}$ be a discrete harmonic function with degree 1 on E. The f-values of each edges are a_1, a_2, a_3, and a_4 as follows. The label is denoted by s.

Thus the sequence of chromatic cochain group is

$$0 \to C^0(G(s)) \to C^1(G(s)) \to C^2(G(s)) \to C^3(G(s)) \to C^4(G(s)) \to 0.$$

By definition,

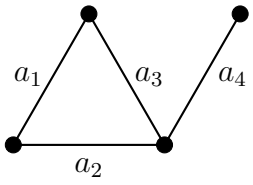
$$\begin{aligned}
&C^0 \cong M^{\otimes 4};\\
&C^1 \cong M^{\otimes 3} \oplus M^{\otimes 3} \oplus M^{\otimes 3} \oplus M^{\otimes 3};\\
&C^2 \cong M^{\otimes 2} \oplus M^{\otimes 2} \oplus M^{\otimes 2} \oplus M^{\otimes 2} \oplus M^{\otimes 2} \oplus M^{\otimes 2};\\
&C^3 \cong M^{\otimes 2} \oplus M \oplus M \oplus M;\\
&C^4 \cong M.
\end{aligned}$$

Then, we calculate the $fq\dim$ of $C^i(G(s))$ for $i = 0, 1, 2, 3, 4$.

$$\begin{aligned}
fq\dim(C^0) &= 0 \cdot (1+q)^4 = 0;\\
fq\dim(C^1) &= a_1(1+q)^3 + a_2(1+q)^3 + a_3(1+q)^3 + a_4(1+q)^3\\
&= (a_1+a_2+a_3+a_4)(1+q)^3 = 0;\\
fq\dim(C^2) &= (a_1+a_2)(1+q)^2 + (a_1+a_3)(1+q)^2 + (a_1+a_4)(1+q)^2\\
&\quad + (a_2+a_3)(1+q)^2 + (a_2+a_4)(1+q)^2 + (a_3+a_4)(1+q)^2\\
&= 2(a_1+a_2+a_3+a_4)(1+q)^2 = 0;\\
fq\dim(C^3) &= (a_1+a_2+a_3)(1+q)^2 + (a_1+a_2+a_4)(1+q)\\
&\quad + (a_1+a_3+a_4)(1+q) + (a_2+a_3+a_4)(1+q)\\
&= -a_4(1+q)^2 + a_4(1+q);\\
fq\dim(C^4) &= (a_1+a_2+a_3+a_4)(1+q)^4 = 0.
\end{aligned}$$

Note that since f is a discrete harmonic function, $(a_1+a_2+a_3+a_4) = 0$, and $(a_1+a_2+a_3) = -a_4$.

We suppose that $\lambda = 1+q$, then the weighted graded Euler number of $C^\bullet(G(s))$ is $a_4\lambda^2 - a_4\lambda$, which coincidences to the opposite of the weighted chromatic polynomial $\chi_f(G(s))$ that is calculated in Example 3.1.



G

FIGURE 3. An example of harmonic chromatic chain complex

7.2. **A Categorification of Harmonic Tutte Polynomial.** In this subsection, we apply the method in [11] to give a categorification to the Harmonic Tutte Polynomial defined in Section 4. Similar to the last subsection, we give a construction of a cochain complex and calculate its weighted alternative sum to categorify the harmonic Tutte polynomial. We omit some proofs in [11]. We use the notation $TC^\bullet(G)$ and boundary operator $td^\bullet$ in this section to distinguish the notations in this subsection and the last subsection.

The cochain group corresponding to the harmonic Tutte polynomial is constructed by a $\mathbb{Z}$-*bigraded module*. A $\mathbb{Z}$-*bigraded module* is a module $\mathcal{A}$ consisting of a decomposition $\mathcal{A} = \bigoplus_{(i,j)\in\mathbb{Z}\oplus\mathbb{Z}} A_{i,j}$. The graded dimension of $\mathcal{A}$ is defined as a two-variable power series $q\dim\mathcal{A} := \sum_{i,j} \dim_{\mathbb{Q}}(A_i \otimes \mathbb{Q})$.

Let A and B be polynomial rings and $A = \mathbb{Z}[x]/(x^2)$, $B = \mathbb{Z}[y]/(y^2)$, where deg $x = (1,0)$, deg $y = (0,1)$. The *degree* of a polynomial is the largest natural number such that the coefficient is not zero. A simple calculation implies that $q\dim A = 1 + x$, $q\dim B = 1 + y$, and $q\dim(A^{\otimes m} \otimes B^{\otimes n}) = (1+x)^m(1+y)^n$, for any $n, m \in \mathbb{N}$.

Let $G(s) = (V, E)$ be a labelled graph, and $f : 2^\Omega \to \mathbb{R}$ be a discrete function of degree d. Similar to the construction in the last subsection, we represent any subgraph G' of G whose vertices are V by the edge vector. We define the cochain group as following.

Definition 7.7. The q-th *Tutte chain group* of $G(s)$ is defined as

$$TC^q(G(s)) := \bigoplus_{l(\epsilon)=q} A^{\otimes k(G_\epsilon)} \otimes B^{\otimes \beta_1(G_\epsilon)},$$

where $\beta_1(G_\epsilon)$ denotes the one-dimensional Betti number of graph (G_ϵ).

Next, we define a Tutte differential operator $td_q : TC^q(G) \to TC^{q+1}(G)$. We begin with a map from $\mathcal{E}^a(G)$ to $\mathcal{E}^{a+1}(G)$ that is identity on all elements but change exact one 0 to 1. That is, the map adds an edge into some subset $D \subset E$. Known as a basic fact of algebraic topology, adding an edge $\tilde{e}$ to $D \subset E$ leads to only two cases, those are,

(1) $\tilde{e}$ joins two connected components of G_D;
(2) $\tilde{e}$ forms a cycle in G_D.

In the first case, $k(G_{D\cup\tilde{e}}) = k(G_D) - 1$, and $\beta_1(G_{D\cup\tilde{e}}) = \beta_1(G_D)$. In the second case, $k(G_{D\cup\tilde{e}}) = k(G_D)$, and $\beta_1(G_{D\cup\tilde{e}}) = \beta_1(G_D) + 1$.

For the first case, we define $td^A_\epsilon : A^{\epsilon_1}(G) \to A^{\epsilon_2}(G)$ to be the identity on all tensor factors other than those two tensor factors that are induced by two connected components joined. For the two joined tensor factors, we map $a_1 \otimes a_2 \in A \otimes A$ to $a_1 a_2 \in A$. We also define $td^B_\epsilon : B^{\epsilon_1}(G) \to B^{\epsilon_2}(G)$ to be the identity map.

For the second case, we define $td^A_\epsilon : A^{\epsilon_1}(G) \to A^{\epsilon_2}(G)$ be the identity map, and $td^B_\epsilon : B^{\epsilon_1}(G) \to B^{\epsilon_2}(G)$ be the module homomorphism mapping $b \in B^{\epsilon_1}(G) \mapsto b \otimes 1 \in B^{\epsilon_2}(G) = B^{\epsilon_1}(G) \otimes B$.

Now by combining td^A_ϵ and td^B_ϵ in two different cases we can define the differential operator. More precisely,

Definition 7.8. The differential operator

$$td^q : TC^q(G(s)) \to TC^{q+1}(G(s))$$

is defined as $td^q = \sum_{l(\epsilon)=q} (-1)^{n(\epsilon)} (td^A_\epsilon \otimes td^B_\epsilon)$, where $n(\epsilon) = \sum_{i=1}^{k_0} \epsilon_i$, and k_0 is the index of the new-added edge in the given order.

Lemma 7.3. *The following statements are true.*

(1) $td \circ td = 0$.
(2) td *is degree preserving.*

Since $td \circ td = 0$, $\{TC^\bullet(G), td^\bullet\}$ is a cochain complex. We denote by $TH^\bullet(G)$ for its cohomology. It is shown in [11] that, the cochain complex does not depend on the choice of the order s. The following theorem implies that the constructed cochain complex combined with a harmonic function is a weighted categorification to harmonic Tutte polynomial.

Theorem 7.2. *Let $G = (V, E)$ be a graph with an order s and f a discrete harmonic function on E, then*

$$T_f(M_G(s); x, y) = \sum_i (-1)^{i+1} \cdot fq\dim(TC^i(G(s))).$$

Also,

$$\widehat{T}_f(M_G; x, y) = \sum_s \sum_i (-1)^{i+1} \cdot fq\dim(TC^i(G(s))).$$

References

[1] M. Aigner, Counting Polynomials, *A Course in Enumeration*, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, 393–450.
[2] C. Bachoc, On harmonic weight enumerators of binary codes, *Des. Codes Cryptogr.* **18** (1999), no. 1–3, 11–28.
[3] T.H. Brylawski, A decomposition for combinatorial geometries. *Trans. Amer. Math. Soc.* **171** (1972), 235–282.
[4] P.J. Cameron, *Combinatorics 2: Structure, Symmetry and Polynomials*, Lecture note.
[5] H.S. Chakraborty, T. Miezaki and M. Oura, Harmonic Tutte polynomials of matroids, submitted.
[6] H. Chakraborty, T. Miezaki and C. Zheng Weighted Tutte–Grothendieck polynomials of graphs Arxiv
[7] H.S. Chakraborty and T. Miezaki, Weighted Tutte–Grothendieck polynomials of graphs II, in preparation.
[8] P. Delsarte, Hahn polynomials, discrete harmonics, and t-designs, *SIAM J. Appl. Math.* **34** (1978), no. 1, 157–166.
[9] C. Greene, Weight enumeration and the geometry of linear codes, *Studia Appl. Math.* **55** (1976), 119–128.
[10] L. Helme-Guizon and Y. Rong, A categorification for the chromatic polynomial, *Algebr. Geom. Topol.*, Vol. **5** (2005), 1365–1388.
[11] L. Helme-Guizon and Y. Rong, A categorification for the Tutte polynomial, *Algebr. Geom. Topol.*, Vol. **5** (2006), 2031–2049.
[12] J.C. Oxley, *Matroid Theory*, Oxford University Press, New York, 1992.
[13] W.T. Tutte, A ring in graph theory, *Proc. Cambridge Philos. Soc.* **43** (1947), 26–40.
[14] W.T. Tutte, Matroids and graphs, *Trans. Amer. Math. Soc.* **90**(3) (1959), 527–552.

The generalized weath product of association schemes over a double poset

渡邊悠太 (愛知教育大学)

1 はじめに

集合 X に対して、その直積集合 $X \times X$ の分割 $\mathcal{R}$ 次の条件(1)(2)(3)を満たしているときに、$\mathcal{R}$ を X 上の**対称アソシエーションスキーム(symmetric association scheme)**という。$\mathcal{R}$ の要素を**関係(relation)**と呼ぶ。

(1) $1_X = \{(x,x) \mid x \in X\}$ は $\mathcal{R}$ の要素である。これを**自明な関係(trivial relation)**と呼ぶ。
(2) 各 $R \in \mathcal{R}$ に対して、$R^\top = \{(y,x) \mid (x,y) \in R\}$ が R と一致する。
(3) $S,T,R \in \mathcal{R}$ を任意に固定したときに、基数 $|\{y \mid (x,y) \in S, (y,z) \in T\}|$ が各 R に対して $(x,y) \in R$ 上で一定の値をとる。

非対称なアソシエーションスキームというものも自然に定義できるが、本稿では非対称なものは扱わないので、ここでは紹介しない。興味のある場合は [5] を参照されたい。以降は(「対称」を省略して、)単にアソシエーションスキームと表記することにする。また、X を有限集合に限定する定義もあるが、ここでは X が無限集合であることを許容していることに注意してほしい。有限集合上のアソシエーションスキームについては [2] を参照されたい。

例 1 (クラス1のアソシエーションスキーム)**.** 集合 X に対して、$1_X = \{(x,x) \mid x \in X\}$、$R = \{(x,y) \in X \times X \mid x \neq y\}$ と定める。このとき、組 $\mathcal{K}_X = \{1_X, R\}$ は X 上のアソシエーションスキームとなる。非自明な関係が1つしかないので、**クラス1のアソシエーションスキーム(1-class association scheme)**と呼ばれている。

例 2 (置換群から得られるアソシエーションスキーム)**.** 群 G が集合 X にgenerously transitiveに作用しているとする。つまり、任意の X の2つの元に対して、それらを互いに移し合う G の元が存在するとする。さらに、直積集合 $X \times X$ への G の作用を $g \cdot (x,y) = (g \cdot x, g \cdot y)$, $x,y \in X$, $g \in G$ で定義する。このとき、直積集合 $X \times X$ の G の作用による軌道全体からなる集合は X 上のアソシエーションスキームとなる。これを群 G の作用から得られるアソシエーションスキームと呼ぶ。

$\mathbf{F}$ を体とし、n を自然数とする。$\mathbf{F}$ 上の n 次元列ベクトル全体からなる集合を $\mathbf{F}^n$ で表し、原点を「忘れる」ことでアフィン空間とみる。アフィン空間 $\mathbf{F}^n$ 上の正則アフィン変換全体の成す群(一般アフィン群)を $\mathrm{GA}_n(\mathbf{F})$ で表す。つまり、

$$\mathrm{GA}_n(\mathbf{F}) = \{x \mapsto Ax + b \mid A \in \mathrm{GL}_n(\mathbf{F}), b \in \mathbf{F}^n\}$$

ここで、$\mathrm{GL}_n(\mathbf{F})$ は $\mathbf{F}$ 上の n 次正則行列全体の成す群(一般線形群)である。一般アフィン群 $\mathrm{GA}_n(\mathbf{F})$ は写像の合成に関して群をなしているので、群としては $\mathrm{GL}_n(\mathbf{F}) \ltimes \mathbf{F}^n$ と同型である。

ここで、$\mathrm{GA}_n(\mathbf{F})$ の $\mathbf{F}^n$ への(アフィン変換による)自然な作用を考える。任意の $y,z \in \mathbf{F}^n$ に対して、アフィン変換

$x \mapsto -I_n x + (y+z) \in \mathrm{GA}_n(\mathbf{F})$ を考える[*1]と、このアフィン変換は y, z を互いに移し合うことが分かる。したがって、$\mathrm{GA}_n(\mathbf{F})$ の $\mathbf{F}^n$ への作用はgenerously transitiveである。例2よりこの作用から $\mathbf{F}^n$ 上のアソシエーションスキームが得られることが分かる。このアソシエーションスキームについて以下の命題が成り立つ。

命題 3. 一般アフィン群 $\mathrm{GA}_n(\mathbf{F})$ の $\mathbf{F}^n$ への自然な作用から得られるアソシエーションスキームは、クラスIのアソシエーションスキーム $\mathcal{K}_{\mathbf{F}^n}$ である。

証明. $R = \{(y,z) \in \mathbf{F}^n \times \mathbf{F}^n \mid y \neq z\}$ が軌道になっていることを示せば良い。任意に $(y,z), (y',z') \in R$ をとる。このとき、$A(y-z) = y'-z'$ を満たす $A \in \mathrm{GL}_n(\mathbf{F})$ が存在する。さらに、$b = y' - Ay = z' - Az \in \mathbf{F}^n$ とおけば、アフィン変換 $x \mapsto Ax + b$ は、(y,z) を (y',z') に移す。したがって、R は一般アフィン群 $\mathrm{GA}_n(\mathbf{F})$ の $\mathbf{F}^n$ への自然な作用による軌道であることが示された。 □

命題3を言い換えると、アフィン変換全体を使えば任意の相異なるペア同士を移すことができてしまう。そこで、本稿では、一部のアフィン変換だけを考える(つまり、一般アフィン群の良い部分群を考える)ことで得られるアソシエーションスキームを調べることにする。具体的には、一般アフィン群と $\mathrm{GL}_n(\mathbf{F}) \ltimes \mathbf{F}^n$ が同型であることに注意して、$\mathrm{GL}_n(\mathbf{F})$ の部分群 G に対して、$G \ltimes \mathbf{F}^n$ (に対応する一般アフィン群の部分群)の作用を考える。

2 $B_n \ltimes \mathbf{F}^n$ の作用

正則な上三角行列全体からなる一般線形群 $\mathrm{GL}_n(\mathbf{F})$ の部分群を B_n とする。このとき、$B_n \ltimes \mathbf{F}^n$ に対応する一般アフィン群の部分群を G_1 とする。つまり、

$$G_1 = \{x \mapsto Ax + b \in \mathrm{GA}_n(\mathbf{F}) \mid A \in B_n, b \in \mathbf{F}^n\}$$

$-I_n \in B_n$ であることから、一般アフィン群 $\mathrm{GA}_n(\mathbf{F})$ の場合と同様に、G_1 の $\mathbf{F}^n$ への作用はgenerously transitiveであることが分かる。このとき、G_1 の作用によるアソシエーションスキームについて以下の命題が成り立つ。

命題 4. G_1 の $\mathbf{F}^n$ への作用から得られるアソシエーションスキーム $\mathcal{R}$ は、n 個の $\mathbf{F}$ 上のクラスIのアソシエーションスキームのリース積である。つまり、$\mathcal{R} = \{1_{\mathbf{F}^n}, R_1, \ldots, R_n\}$ であり、各 $i \in \{1,2,\ldots,n\}$ に対して、

$$R_i = \{(x,y) \in \mathbf{F}^n \times \mathbf{F}^n \mid x_i \neq y_i,\ x_k = y_k\ (k = i+1, \ldots, n)\}$$

を満たす。

証明. n に関する帰納法で示す。$n=1$ のとき、$B_1 = \mathrm{GL}_1(\mathbf{F})$ なので、命題3よりこのアソシエーションスキームはクラスIのアソシエーションスキーム $\mathcal{K}_{\mathbf{F}^n}$ である。$n \geq 2$ のとき、各 R_i が軌道になることを次の 2 つの場合に分けて示す。(1) $(y,z) \in R_i$, $g \in G_1$ ならば $g \cdot (y,z) \in R_i$ を満たす。(2) $(y,z), (y',z') \in R_i$ ならば $g \cdot (y,z) = (y',z')$ を満たす $g \in G_1$ が存在する。

(1) $(y,z) \in R_i$, $g \in G_1$ とし、$g : x \mapsto Ax + b$ を満たす $A = [a_{i,j}] \in B_n$, $b \in \mathbf{F}^n$ をとる。このとき、$g \cdot (y,z) = (Ay+b, Az+b) \in R_i$ を示す。つまり、$[A(y-z)]_i \neq 0$, $[A(y-z)]_k = 0\ (k = i+1, \ldots, n)$ を示せば良い。$i=1$ のときは、$[A(y-z)]_1 = a_{1,1}(y-z)_1 \neq 0$, $[A(y-z)]_k = \sum_{j=k}^{n} a_{k,j}(y-z)_j = 0\ (k = 2, \ldots, n)$ である。$i \geq 2$ のときは、行列 A, y, z を次のように分割する。

[*1] 一般線形群 $\mathrm{GL}_n(\mathbf{F})$ の単位元(単位行列)を I_n で表す。

$$A = \left[\begin{array}{c|ccc} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ \hline 0 & & & \\ \vdots & & \tilde{A} & \\ 0 & & & \end{array}\right], \qquad y = \left[\begin{array}{c} y_1 \\ \hline \\ \tilde{y} \\ \\ \end{array}\right], \qquad z = \left[\begin{array}{c} z_1 \\ \hline \\ \tilde{z} \\ \\ \end{array}\right]$$

このとき、$[A(y-z)]_\ell = [\tilde{A}(\tilde{y}-\tilde{z})]_{\ell-1}$ $(\ell = 2, \ldots, n)$ なので、帰納法の仮定より、$[A(y-z)]_i \neq 0$, $[A(y-z)]_k = 0$ $(k = i+1, \ldots, n)$ が成り立つ。

(2) $(y, z), (y', z') \in R_i$ とし、y, z, y', z' を次のように分割する。

$$y = \left[\begin{array}{c} y_1 \\ \hline \\ \tilde{y} \\ \\ \end{array}\right], \qquad z = \left[\begin{array}{c} z_1 \\ \hline \\ \tilde{z} \\ \\ \end{array}\right], \qquad y' = \left[\begin{array}{c} y'_1 \\ \hline \\ \tilde{y}' \\ \\ \end{array}\right], \qquad z' = \left[\begin{array}{c} z'_1 \\ \hline \\ \tilde{z}' \\ \\ \end{array}\right]$$

$i = 1$ のときは、$\tilde{y} = \tilde{z}$, $\tilde{y}' = \tilde{z}'$ なので $(\tilde{y}, \tilde{z})$, $(\tilde{y}', \tilde{z}') \in 1_{\mathbf{F}^{n-1}}$ である。$i \geq 2$ のときは、$\tilde{R}_i = \{(\tilde{x}, \tilde{y}) \in \mathbf{F}^{n-1} \times \mathbf{F}^{n-1} \mid x_i \neq y_i,\ x_k = y_k\ (k = i+1, \ldots, n-1)\}$ とすれば、$(\tilde{y}, \tilde{z})$, $(\tilde{y}', \tilde{z}') \in \tilde{R}_i$ である。帰納法の仮定より、全ての i で $(\tilde{y}, \tilde{z})$ を $(\tilde{y}', \tilde{z}')$ に移すアフィン変換 $x \mapsto \tilde{A}x + \tilde{b}$ $(\tilde{A} \in B_{n-1}, \tilde{b} \in \mathbf{F}^{n-1})$ が存在する。さらに、$i = 1$ のとき $y_1 \neq z_1$, $y'_1 \neq z'_1$ なので、$\alpha(y_1 - z_1) = y'_1 - z'_1$ を満たす $\alpha \in \mathbf{F} \setminus \{0\}$ が存在するので、

$$A = \left[\begin{array}{c|ccc} \alpha & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \tilde{A} & \\ 0 & & & \end{array}\right] \in B_n, \qquad b = \left[\begin{array}{c} y'_1 - \alpha y_1 \\ \hline \\ \tilde{b} \\ \\ \end{array}\right] = \left[\begin{array}{c} z'_1 - \alpha z_1 \\ \hline \\ \tilde{b} \\ \\ \end{array}\right] \in \mathbf{F}^n$$

とおけば、アフィン変換 $x \mapsto Ax + b$ は、(y, z) を (y', z') に移す。$i \geq 2$ のとき、$y_i \neq z_i$ なので、$(y_1 - z_1) + \beta_i(y_i - z_i) = y'_1 - z'_1$ を満たす $\beta_i \in \mathbf{F}$ が存在するので、

$$A = \left[\begin{array}{c|ccccc} 1 & 0 & \cdots & \beta_i & \cdots & 0 \\ \hline 0 & & & & & \\ \vdots & & & \tilde{A} & & \\ 0 & & & & & \end{array}\right] \in B_n, \qquad b = \left[\begin{array}{c} y'_1 - y_1 - \beta_i y_i \\ \hline \\ \tilde{b} \\ \\ \end{array}\right] = \left[\begin{array}{c} z'_1 - z_1 - \beta_i z_i \\ \hline \\ \tilde{b} \\ \\ \end{array}\right] \in \mathbf{F}^n$$

とおけば、アフィン変換 $x \mapsto Ax + b$ は、(y, z) を (y', z') に移す。つまり、全ての i で (y, z) を (y', z') に移す G_1 の元が存在することが分かる。 □

3 $B_P \ltimes \mathbf{F}^n$ の作用

P を位数 n の半順序集合とする。この節では、$\mathbf{F}^n$ と $\mathrm{GL}_n(\mathbf{F})$ の要素の行と列をそれぞれ P の元で添字付けて考えることにする。その上で、一般線形群 $\mathrm{GL}_n(\mathbf{F})$ の部分群 B_P を次のように定義する。

$$B_P = \{A \in \mathrm{GL}_n(\mathbb{F}) \mid p \not\leq q \Rightarrow A_{p,q} = 0\ (p, q \in P)\}$$

特に、P が鎖(どの2元も比較可能)の場合には B_P は上三角行列全体の集合と一致する。また、P が反鎖(どの2元も比較不可能)の場合には B_P は対角行列全体の集合と一致する。つまり、B_P は上三角行列全体からなる部分群と対角行列全体からなる部分群を一般化した部分群である。このとき、$B_P \ltimes \mathbf{F}^n$ に対応する一般アフィン群の部分群を G_2 とする。つまり、

$$G_2 = \{x \mapsto Ax + b \in \mathrm{GA}_n(\mathbf{F}) \mid A \in B_P, b \in \mathbf{F}^n\}$$

$-I_n \in B_n$ であることから、一般アフィン群 $\mathrm{GA}_n(\mathbf{F})$ の場合と同様に、G_2 の $\mathbf{F}^n$ への作用はgenerously transitiveであることが分かる。このとき、G_2 の作用によるアソシエーションスキームについて以下の命題が成り立つ。

命題 5. G_2 の $\mathbf{F}^n$ への作用から得られるアソシエーションスキーム $\mathcal{R}$ は、$\mathbb{F}$ 上のクラス l のアソシエーションスキームの P 上の一般化リース積[*2]である。つまり、$\mathcal{R} = \{R_C \mid C \subset P \text{ は反鎖}\}$ であり、各反鎖 $C \subset P$ に対して

$$R_C = \{(x, y) \in \mathbf{F}^n \times \mathbf{F}^n \mid x_p \neq y_p \ (p \in C), x_q = y_q \ (q \leq \nexists p \in C)\}$$

を満たす。

証明. 命題4と同様に示すことができる。 □

4 $(\mathrm{GL}_k(\mathbf{F}) \otimes \mathrm{GL}_\ell(\mathbf{F})) \ltimes \mathbf{F}^n$ の作用

$n = k\ell$ を満たす自然数 k, ℓ をとる。一般線形群 $\mathrm{GL}_n(\mathbf{F})$ の部分群として、テンソル積 $\mathrm{GL}_k(\mathbf{F}) \otimes \mathrm{GL}_\ell(\mathbf{F})$ を考える。このとき、$(\mathrm{GL}_k(\mathbf{F}) \otimes \mathrm{GL}_\ell(\mathbf{F})) \ltimes \mathbf{F}^n$ に対応する一般アフィン群の部分群を G_3 とする。つまり、

$$G_3 = \{x \mapsto Ax + b \in \mathrm{GA}_n(\mathbf{F}) \mid A \in \mathrm{GL}_k(\mathbf{F}) \otimes \mathrm{GL}_\ell(\mathbf{F}), b \in \mathbf{F}^n\}$$

G_3 の群作用を見やすくするために、以下の対応を考える。$n(= k\ell)$ 次元列ベクトル x を、l 行目から k 個ずつ k 次元の部分列ベクトル $y_1, y_2, \ldots, y_\ell$ に分割して、それら $y_1, y_2, \ldots, y_\ell$ を横に並べて $k \times \ell$ 行列 x' を構成する。

$$x = \begin{bmatrix} y_1 \\ \hline y_2 \\ \hline \vdots \\ \hline y_\ell \end{bmatrix} \qquad \to \qquad x' = \begin{bmatrix} y_1 & y_2 & \cdots & y_\ell \end{bmatrix}$$

この構成は全単射であることが分かるので、$\mathbf{F}^n$ は「$\mathbb{F}$ 上の $k \times \ell$ 行列全体」と一対一で対応する。この節では、$\mathbf{F}^n$ を $k \times \ell$ 行列全体として扱うことにする。この同一視によって、G_3 の作用は以下のように書き換えることができる。

$$G_3 = \{x \mapsto A_1 x A_2^\top + b \in \mathrm{GA}_n(\mathbf{F}) \mid A_1 \in \mathrm{GL}_k(\mathbf{F}), A_2 \in \mathrm{GL}_\ell(\mathbf{F}), b \in \mathbf{F}^n\}$$

$-I_n = -I_k \otimes I_\ell \in \mathrm{GL}_k(\mathbf{F}) \otimes \mathrm{GL}_\ell(\mathbf{F})$ であることから、一般アフィン群 $\mathrm{GA}_n(\mathbf{F})$ の場合と同様に、G_3 の $\mathbf{F}^n$ への作用はgenerously transitiveであることが分かる。このとき、G_3 の作用によるアソシエーションスキームについて以下の命題が成り立つ。

[*2] 一般化リース積については [1] を参照されたい。

命題 6. G_3 の $\mathbf{F}^n$ への作用から得られるアソシエーションスキーム $\mathcal{R}$ は、$k \times \ell$ の双線形形式スキーム[*3]である。つまり、$d = \min\{k, \ell\}$ とするとき、$\mathcal{R} = \{R_0, R_1, \ldots, R_d\}$ であり、各 $i \in \{0, 1, \ldots, d\}$ に対して、

$$R_i = \{(x, y) \in \mathbf{F}^n \times \mathbf{F}^n \mid \mathrm{rank}(x - y) = i\}$$

を満たす。

証明. 各 R_i が軌道になることを次の 2 つの場合に分けて示す。(1) $(y, z) \in R_i$, $g \in G_3$ ならば $g \cdot (y, z) \in R_i$ を満たす。(2) $(y, z), (y', z') \in R_i$ ならば $g \cdot (y, z) = (y', z')$ を満たす $g \in G_3$ が存在する。

(1) $(y, z) \in R_i$, $g \in G_3$ とし、$g : x \mapsto A_1 x A_2^\top + b$ を満たす $A_1 \in \mathrm{GL}_k(\mathbf{F})$, $A_2 \in \mathrm{GL}_\ell(\mathbf{F})$, $b \in \mathbf{F}^n$ をとる。このとき、$g \cdot (y, z) = (A_1 y A_2^\top + b, A_1 z A_2^\top + b)$ なので、

$$\mathrm{rank}((A_1 y A_2^\top + b) - (A_1 z A_2^\top + b)) = \mathrm{rank}(A_1 (y - z) A_2^\top) = \mathrm{rank}(y - z) = i$$

である。つまり、$g \cdot (y, z) \in R_i$ が従う。

(2) $(y, z), (y', z') \in R_i$ とすると、$\mathrm{rank}(y - z) = \mathrm{rank}(y' - z') = i$ なので、$A_1 (y - z) A_2^\top = y' - z'$ を満たす $A_1 \in \mathrm{GL}_k(\mathbf{F})$, $A_2 \in \mathrm{GL}_\ell(\mathbf{F})$ が存在する。このとき、$b = y' - A_1 y A_2^\top = z' - A_1 z A_2^\top$ に対して、アフィン変換 $x \mapsto A_1 x A_2^\top + b$ は (y, z) を (y', z') に移す。 □

5 $(B_k \otimes B_\ell) \ltimes \mathbf{F}^n$ の作用

$n = k\ell$ を満たす自然数 k, ℓ をとる。k 次の正則な上三角行列全体からなる部分群を B_k、ℓ 次の正則な上三角行列全体からなる部分群を B_ℓ とする。このとき、テンソル積 $B_k \otimes B_\ell$ が一般線形群 $\mathrm{GL}_n(\mathbf{F})$ の部分群であることに注意して、$(B_k \otimes B_\ell) \ltimes \mathbf{F}^n$ に対応する一般アフィン群の部分群を G_4 とする。つまり、

$$G_4 = \{x \mapsto Ax + b \in \mathrm{GA}_n(\mathbf{F}) \mid A \in B_k \otimes B_\ell, b \in \mathbf{F}^n\}$$

前節と同様に、G_4 の群作用を見やすくするために、$\mathbf{F}^n$ を $k \times \ell$ 行列全体として扱うことにする。また、以下の記号を準備する。$k \times \ell$ 行列 $x \in \mathbf{F}^n$ に対して、x の (i, j) 成分よりも右下にある $(k - i + 1) \times (\ell - j + 1)$ 部分小行列を $x[i, j]$ で表す。つまり、

$$x = \left[\begin{array}{ccc|ccc} x_{1,1} & \cdots & & x_{1,j} & \cdots & x_{1,\ell} \\ \vdots & \ddots & & \vdots & \ddots & \vdots \\ \hline x_{i,1} & \cdots & & x_{i,j} & \cdots & x_{i,\ell} \\ \vdots & \ddots & & \vdots & \ddots & \vdots \\ x_{k,1} & \cdots & & x_{k,j} & \cdots & x_{k,\ell} \end{array}\right] \in \mathbf{F}^n \qquad \Rightarrow \qquad x[i, j] = \begin{bmatrix} x_{i,j} & \cdots & x_{i,\ell} \\ \vdots & \ddots & \vdots \\ x_{k,j} & \cdots & x_{k,\ell} \end{bmatrix}$$

同様に、$A_1 \in B_k$ や $A_2 \in B_\ell$ に対しても、(i, j) 成分よりも右下にある小行列を $A_1[i, j]$, $A_2[i, j]$ で表す。さらに、$x \in \mathbf{F}^n$ に対して、$\mathrm{rank}_{i,j}(x) = \mathrm{rank}(x[i, j])$ で定める。$-I_n = -I_k \otimes I_\ell \in B_k \otimes B_\ell$ であることから、これまでと同様に G_4 の $\mathbf{F}^n$ への作用はgenerously transitiveであることが分かる。このとき、G_4 の作用によるアソシエーションスキームを記述するために次のような同値関係を導入する。$(x, y), (x', y') \in \mathbf{F}^n \times \mathbf{F}^n$ に対して、

$$(x, y) \sim (x', y') \qquad \Leftrightarrow \qquad \mathrm{rank}_{i,j}(x - y) = \mathrm{rank}_{i,j}(x' - y') \qquad (i = 1, 2, \ldots, k,\ j = 1, 2, \ldots, \ell)$$

[*3] 有限体上の双線形形式スキームについては [3] を参照されたい。

主定理 7. G_4 の $\mathbf{F}^n$ への作用から得られるアソシエーションスキームは、$\mathbf{F}^n \times \mathbf{F}^n$ の同値関係 $\sim$ による商集合と一致する。

証明. k, ℓ に関する帰納法で示す。

$k = 1$ のとき、$B_1 \otimes B_\ell = B_\ell$ なので、命題4よりこのアソシエーションスキームは ℓ 個の $\mathbf{F}$ 上のクラス1のアソシエーションスキームのリース積である。つまり、$\mathcal{R} = \{1_{\mathbf{F}^n}, R_1, \ldots, R_\ell\}$ であり、各 $i \in \{1, 2, \ldots, \ell\}$ に対して、$R_i = \{(x, y) \in \mathbf{F}^n \times \mathbf{F}^n \mid x_i \neq y_i,\ x_k = y_k\ (k = i+1, \ldots, \ell)\}$ を満たす。このとき、$x, y \in \mathbf{F}^n = \mathbf{F}^\ell$ が行ベクトルであることに注意すると、$0 \leq \mathrm{rank}_{1,\ell}(x-y) \leq \cdots \leq \mathrm{rank}_{1,1}(x-y) \leq 1$ であり、

$$\mathrm{rank}_{1,i}(x-y) = 1 \text{ かつ } \mathrm{rank}_{1,i+1}(x-y) = 0 \quad \Leftrightarrow \quad (x, y) \in R_i$$

$$\mathrm{rank}_{1,1}(x-y) = \cdots = \mathrm{rank}_{1,\ell}(x-y) = 0 \quad \Leftrightarrow \quad (x, y) \in 1_{\mathbf{F}^n}$$

これは、各 R_i, $1_{\mathbf{F}^n}$ が同値関係 $\sim$ による同値類であることを示している。つまり、同値関係 $\sim$ による商集合と一致する。同様に、$\ell = 1$ の場合も、アソシエーションスキームは同値関係 $\sim$ による商集合と一致する。

$k \geq 2$ かつ $\ell \geq 2$ のとき、同値関係 $\sim$ による同値類 R が軌道になることを次の 2 つの場合に分けて示す。(1) $(y, z) \in R$, $g \in G_4$ ならば $g \cdot (y, z) \in R$ を満たす。(2) $(y, z), (y', z') \in R$ ならば $g \cdot (y, z) = (y', z')$ を満たす $g \in G_4$ が存在する。

(1) $(y, z) \in R$, $g \in G_4$ とし、$g : x \mapsto A_1 x A_2^\top + b$ を満たす $A_1 \in B_k$, $A_2 \in B_\ell$, $b \in \mathbf{F}^n$ をとる。このとき、$g \cdot (y, z) = (A_1 y A_2^\top + b, A_1 z A_2^\top + b) \in R$ を示す。つまり、$\mathrm{rank}_{i,j}(y - z) = \mathrm{rank}_{i,j}(A_1(y-z)A_2^\top)$ $(i = 1, 2, \ldots, k,\ j = 1, 2, \ldots, \ell)$ を示せば良い。行列 A_1, A_2, y, z の部分小行列 $\tilde{A}_1, \tilde{A}_2, \tilde{y}, \tilde{z}$ を次のように定める。

$$\tilde{A}_1 = A_1[i, i], \qquad \tilde{A}_2 = A_2[j, j], \qquad \tilde{y} = y[i, j], \qquad \tilde{z} = y[i, j]$$

このとき、A_1, A_2 が上三角行列であることに注意すると、$\mathrm{rank}_{i,j}(y-z) = \mathrm{rank}(\tilde{y} - \tilde{z}) = \mathrm{rank}(\tilde{A}_1(\tilde{y} - \tilde{z})\tilde{A}_2^\top) = \mathrm{rank}_{i,j}(A_1(y-z)A_2^\top)$ が成り立つことが示される。

(2) $(y, z), (y', z') \in R$ とし、$w = y - z$, $w' = y' - z'$ とおく。行列 w, w' の部分小行列 $\tilde{w}, \tilde{w}'$ を次のように定める。

$$\tilde{w} = w[2, 1] \qquad \tilde{w}' = w'[2, 1]$$

帰納法の仮定より、$\tilde{A}_1' \tilde{w} (A_2')^\top = \tilde{w}'$ を満たす $\tilde{A}_1' \in B_{k-1}$, $A_2' \in B_\ell$ が存在する。$A_1' = 1 \oplus \tilde{A}_1' \in B_k$ と定める。さらに、$w'' = A_1' w (A_2')^\top$ とおく。

$$w'' = A_1' w (A_2')^\top = \left[\begin{array}{c|c} 1 & 0 \\ \hline 0 & \tilde{A}_1' \end{array}\right] \left[\begin{array}{ccc} w_{1,1} & \cdots & w_{1,\ell} \\ \hline \multicolumn{3}{c}{\tilde{w}} \end{array}\right] (A_2')^\top = \left[\begin{array}{ccc} w''_{1,1} & \cdots & w''_{1,\ell} \\ \hline \multicolumn{3}{c}{\tilde{w}'} \end{array}\right]$$

このとき、$A_1'' w'' (A_2'')^\top = w'$ を満たす $A_1'' \in B_k$, $A_2'' \in B_\ell$ を見つければよい。$\mathrm{rank}_{1,1}(w'') = \mathrm{rank}_{2,1}(w'')$ のとき、w'' の1行目は $\tilde{w}'$ の行の線型結合で表すことができる。このとき、R が同値類であることから、$\mathrm{rank}_{1,1}(w') = \mathrm{rank}_{2,1}(w')$ でもあり、w' の1行目も $\tilde{w}'$ の行の線型結合で表すことができる。したがって、$\beta_2, \ldots, \beta_k$ が存在して、

$$\left[\begin{array}{c|ccc} 1 & \beta_2 & \cdots & \beta_k \\ \hline & \multicolumn{3}{c}{\multirow{3}{*}{I_{k-1}}} \\ & & & \\ & & & \end{array}\right] w'' = w'$$

となる。一方で、$\mathrm{rank}_{1,1}(w'') > \mathrm{rank}_{2,1}(w'')$ のとき、

$$\mathrm{rank}_{1,j+1}(w'') = \mathrm{rank}_{2,j+1}(w''), \qquad \mathrm{rank}_{1,j}(w'') > \mathrm{rank}_{2,j}(w'')$$

を満たす j が存在する。$w''[1, j+1]$ の 1 行目は $w''[2, j+1]$ の行の線型結合で表すことができ、$w''[1, j]$ の 1 行目は $w''[2, j]$ の行の線型結合で表すことができるない。さらに、$w''[2, j]$ の 1 列目は $w''[2, j+1]$ の列の線型結合で表すことができ、$w''[1, j]$ の 1 列目は $w''[1, j+1]$ の列の線型結合で表すことができない。R が同値類であることから、w' についても同様のことが言える。したがって、$\alpha, \beta_2, \ldots, \beta_k, \gamma_{j,1}, \ldots, \gamma_{\ell,j-1}$ が存在して、

$$\left[\begin{array}{c|ccc} \alpha & \beta_2 & \cdots & \beta_k \\ \hline & & & \\ & & I_{k-1} & \\ & & & \end{array}\right] w'' \left[\begin{array}{ccc|c} & I_{j-1} & & \\ \hline \gamma_{j,1} & \cdots & \gamma_{j,j-1} & \\ \vdots & \ddots & \vdots & I_{\ell-j+1} \\ \gamma_{\ell,1} & \cdots & \gamma_{\ell,j-1} & \end{array}\right] = w'$$

となる。 □

6 おわりに

本稿では、アフィン変換の作用から定まるアソシエーションスキームを通して、クラス I のアソシエーションスキーム・リース積・一般化リース積・双線形形式スキームを系統的に整理した。まとめると以下の通りである。

permutation groups	association schemes
$\mathrm{GL}_n(\mathbf{F}) \ltimes \mathbf{F}^n$	$\mathcal{K}_{\mathbf{F}^n}$
$B_n \ltimes \mathbf{F}^n$	wreath product of n copies of $\mathcal{K}_{\mathbf{F}}$
$B_P \ltimes \mathbf{F}^P$	generalized wreath product of $\mathcal{K}_{\mathbf{F}}$ over P
$(\mathrm{GL}_k(\mathbf{F}) \otimes \mathrm{GL}_\ell(\mathbf{F})) \ltimes \mathbf{F}^n$	$m \times n$ bilinear forms
$(B_k \otimes B_\ell) \ltimes \mathbf{F}^n$	defined by $\mathrm{rank}_{i,j}(x-y)$
$(B_P \otimes B_Q) \ltimes \mathbf{F}^{P \times Q}$	???

上記表の $(B_P \otimes B_Q) \ltimes \mathbf{F}^{P\times Q}$ のアソシエーションスキームについては、本稿では触れなかったが、自然に定義できることが見てとれる。このアソシエーションスキームの特徴付けについては今後の課題である。

最後に、講演では時間の関係で触れることができなかったのだが、$(B_k \otimes B_\ell) \ltimes \mathbf{F}^n$ のアソシエーションスキームが、グラスマン多様体のattenuated space上に定まるアソシエーションスキーム[*4]として自然に構成されるものであることをコメントしておく。自然数 k, ℓ に対して、$n = k\ell$, $m = k + \ell$ とする。ベクトル空間 $\mathbf{F}^m$ の ℓ 次元部分空間全体を**グラスマン多様体(Grassmannian)**と呼び、$\mathrm{Gr}(\ell, m)$ で表す。グラスマン多様体 $\mathrm{Gr}(\ell, m)$ には一般線形群 $\mathrm{GL}_m(\mathbb{F})$ が(左からの行列の積として)自然に作用しているが、ここでは、上三角行列からなる部分群(ボレル部分群) B_m の作用を考える。$\mathrm{Gr}(\ell, m)$ の B_m の作用による軌道のうち、一番大きいものを**attenuated space**と呼ぶ。具体的に書き下

[*4] グラスマン多様体のattenuated space上に定まるアソシエーションスキームについては [4] を参照されたい。

すと、$\mathbf{F}^m$ の標準基底 $e_1, \ldots, e_m$ に対して、

$$X = \{x \in \mathrm{Gr}(\ell, m) \mid \dim(x \cap \langle e_1, \ldots, e_k \rangle) = 0\}$$

がグラスマン多様体のattenuated spaceである。$m = k + \ell$ であり、$\{e_1, \ldots, e_m\}$ が標準基底であることに注意すると、

$$X = \left\{ \text{column space of } \left[\begin{array}{c} x' \\ \hline J \end{array}\right] \,\middle|\, k \times \ell \text{ matrix } x' \right\}, \qquad \text{where } J = \begin{bmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{bmatrix}$$

である。この X に合わせて B_m の上三角行列も分割すると、

$$B_m = \left\{ \left[\begin{array}{c|c} A_1 & b \\ \hline & A_2 \end{array}\right] : A_1 \in B_k, A_2 \in B_\ell, k \times \ell \text{ matrix } b \right\}$$

となる。上記のように、X の元を $k \times \ell$ 行列 x' と同一視すれば、B_m の X への作用は

$$x' \mapsto A_1 x' (J A_2^{-1} J) + (b A_2^{-1} J)$$

と表せる。これは $(B_k \otimes B_\ell) \ltimes \mathbf{F}^n$ に対応するアフィン変換である。つまり、$(B_k \otimes B_\ell) \ltimes \mathbf{F}^n$ のアソシエーションスキームは、グラスマン多様体のattenuated space上に定まるアソシエーションスキームとして自然に構成されることが分かった。

参考文献

[1] R. A. Bailey, Generalized wreath products of association schemes. European J. Combin. 27 (2006), no. 3, 428–435.

[2] 坂内 英一, 坂内 悦子, 伊藤 達郎, 代数的組合せ論入門. 共立出版, 2016.

[3] Ph. Delsarte, Bilinear forms over a finite field, with applications to coding theory. J. Combin. Theory Ser. A 25 (1978), no. 3, 226–241.

[4] Hirotake Kurihara, Character tables of association schemes based on attenuated spaces. Ann. Comb. 17 (2013), no. 3, 525–541.

[5] Paul-Hermann Zieschang, Theory of association schemes. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.