まえがき

この報告集は、2012 年 6 月 18 日（月）から 20 日（水）にわたって、弘前大学八甲田ホールでおこなわれた研究集会「第 29 回代数的組合せ論シンポジウム」の講演記録です。57 名の参加者を得る盛会でした。また 19 日に開かれた懇親会も 40 名のご参加を頂きました。

この集会に関わる講演者の旅費、およびこの報告集の作成にあたっては、科学研究費補助金基盤研究（B）課題番号：24340002（研究代表者 千葉大学教授 北詰 正顕）から援助を頂きました。加えて、講演者の旅費につきましては、科学研究費補助金基盤研究（B）課題番号：22340002（研究代表者 筑波大学教授 宮本 雅彦）、科学研究費補助金基盤研究（B）課題番号：23654029（研究代表者 山形大学准教授 原田 昌晃）および科学研究費補助金基盤研究（C）課題番号：23540002（研究代表者 弘前大学准教授 別宮 耕一）から援助を頂きました。開催に係る費用につきましては、公益社団法人青森県観光連盟から平成 24 年度コンベンション開催費助成金として援助を頂きました。この場を借りて御礼申し上げます。

最後になりましたが、講演者の方々、参加者の方々に感謝致します。

2013 年 3 月
別宮 耕一
千吉良 直紀
島倉 裕樹

第 29 回代数的組合せ論シンポジウム

下記のとおり研究集会を開催しますので、御案内申し上げます。

別宮 耕一 （弘前大学・理工学研究科）
世話人: 千吉良 直紀 （熊本大学・理学部）
島倉 裕樹 （東北大学・情報科学研究科）

記

日時: 2012 年 6 月 18 日（月）— 2012 年 6 月 20 日（水）

場所: 弘前大学八甲田ホール（弘前大学創立 60 周年記念会館「コラボ弘大」 8 階）
〒 036-8561 弘前市文京町 3

プログラム

6 月 18 日（月）

10:00 – 10:30 別宮 耕一 （弘前大学・理工学研究科）
Classification of doubly even self-dual codes of length 40

10:40 – 11:10 三枝崎 剛 （大分工業高等専門学校）
On the existence of extremal Type II $\mathbb{Z}_{2k}$-codes

11:20 – 11:50 田村 宏樹
On the relation between Kleinian codes and binary codes with a frame

14:00 – 14:50 鈴木 一克 （名古屋産業科学研究所）
$\mathbb{Z}/p\mathbb{Z}$ 上の線形符号の部分エプシュタイン・ゼータ関数について

15:00 – 15:30 大浦 学 （高知大学・理学部）
Modular forms of weight 8 for the theta group

15:40 – 16:30 冨江 雅也 （盛岡大学・文学部）
Permutation Pattern と Lehmer Code から定まる半順序集合の構造について

16:40 – 17:10 谷口 浩朗 （香川高等専門学校）
Simple expressions of the Buratti-Del Fra dual hyperoval
and the deformation of Veronesean dual hyperoval

6 月 19 日（火）

10:00 – 10:50　安部 利之 （愛媛大学・理工学研究科）
Fusion products for the symplectic-fermionic vertex operator superalgebra

11:00 – 11:50　Ching Hung Lam （台湾、Academia Sinica）
3A and 6A cases of McKay-Glauberman-Norton observation

14:00 – 14:30　山口 正男 （筑波大学・数理物質科学研究科）
多重三角形の置換群について

14:40 – 15:10　野崎 寛 （愛知教育大学）
有向グラフと複素球面上のコード

15:20 – 15:50　田中 利恵
On a class of wreath products of hypergroups and association schemes

16:00 – 16:50　萩原 学 （産業技術総合研究所）
Graph theoretic approach to rank modulations and permutation codes

17:00 – 17:30　小関 道夫
Leech lattice に内在するいくつかの組合せ的構造について

6 月 20 日（水）

10:00 – 10:50　小田 文仁 （山形大学・理学部）
丹原関手に関する注意

11:00 – 11:50　澤辺 正人 （千葉大学・教育学部）
有限群の部分群族とパス代数の表現

本研究集会に関する情報のページ：
`http://www.st.hirosaki-u.ac.jp/~betsumi/algcom2012/`
会期前に生じた予定の変更・情報の更新などの連絡は上記ページに掲載いたします。

目次

Fusion products of the symplectic-fermionic vertex operator superalgebra[1]

Toshiyuki Abe (Ehime University)
Joint work with Y. Arike

1 Introduction

In my talk, we gave a definition notions of twisted supermodules and semi-intertwining operator among them, and recalled fusion products in categories of twisted supermodules. As an example, we also considered the symplectic-fermionic vertex operator superalgebra and explained about the fusion products among its twisted supermodules.

A vertex operator superalgebra (VOSA) is a super-analog of a vertex operator algebra. Some examples has been known as Fermionic VOSA, (Lattice VOAs associated to (non-even) integral lattices (see [Xu98]), code VOSAs associated to (non doubly) even codes, and some other examples, $N = 1, 2, 3, 4$ SUSY VOSA (cf. [HK]) and VOSA associated to affine Lie superalgebras (cf. [K])and so on. Some of the VOSAs above are rational, C_2-cofinite and their even parts and odd parts have integral and half integral eigenvalues for L_0, respectively. This fact for weights enables us to introduce a $\mathbb{Z}_2$-grading on simple modules so that the lowest weight vectors are even. On the other hand, I constructed a VOSA $\mathcal{F}$ associated to a finite dimensional symplectic vector space in [A07]. The VOSA F is irrational and has only integral weights for L_0. For this VOSA, $\mathbb{Z}_2$-grading is also useful information. For example, in the category of weak modules for T (see Section 6 below), there exists a unique projective indecomposable module, and it has four composition factors which are isomorphic to the VOSA. If we take account in the $\mathbb{Z}_2$-grading, we see that the projective modules have two composition factors isomorphic to the VOSA and two ones isomorphic to the module given by switching the parity of the VOSA. This refinement gives more detail information when we calculate fusion rules. This motivates us to introduce the notion of supermodule which is a module with $\mathbb{Z}_2$-grading and study in the category of supermodules. We also discuss fusion rules, fusion products for $\mathcal{F}$.

2 Supermodules for VOSA

Definition 2.1. A vertex operator superalgebra (VOSA) is a vector superspace $V = V^{\overline{0}} \oplus V^{\overline{1}}$ which affords also a $\frac{1}{2}\mathbb{Z}_{\geq 0}$-grading $V = \bigoplus_{i \in \frac{1}{2}\mathbb{Z}_{\geq 0}} V_i$. This superspace equips a bilinear map $V \times V \ni (a, b) \mapsto a_{(n)}b \in V$ for every integer $n \in \mathbb{Z}$ satisfying the following axioms.

(1) For $a, b \in V$, $a_{(n)}b = 0$ for sufficiently large n.

[1] June 19, 2012, The 29th Symposium on Algebraic Combinatorics at Hirosaki university

(2) For $a \in V^{(\bar{i})}$ and $b \in V^{(\bar{j})}$, $a_{(n)}b \in V^{(\overline{i+j})}$. (We denote $i = p(a)$ if $a \in V^{(i)}$)

(3) Borcherds identity : For $a, b, c \in V$, $p, q, r \in \mathbb{Z}$,

$$\sum_{i=0}^{\infty} \binom{r}{i} (a_{(p+i)}b)_{(r+q-i)}c$$
$$= \sum_{i=0}^{\infty} \binom{p}{i} (-1)^i (a_{(p+r-i)}(b_{(q+i)}c) - (-1)^{p+p(a)p(b)} b_{(p+q-i)}(a_{(r+i)}c))$$

(4) The vacuum vector $\mathbf{1}$: For $m \in \mathbb{Z}$, $\mathbf{1}_{(m)}a = \delta_{m,-1}a$. $\forall n \in \mathbb{Z}_{\geq 0}$, $a_{(n)}\mathbf{1} = 0$.

(5) The Virasoro vector ω : Set $L_n := \omega_{(n+1)}$ $(n \in \mathbb{Z})$. Then there exists a constant $c_V \in \mathbb{C}$ such that

$$[L_m, L_n]a = (m-n)L_{m+n}a + \frac{m^3 - m}{12}\delta_{m+n,0}c_V.$$

The constant c_V is called the central charge of V.

(6) $L_{-1}a = a_{(-2)}\mathbf{1}$, $a \in V$.

(7) $V_d = \{a \in V | L_0 a = da\}$ and $\dim_{\mathbb{C}} V_d < \infty$.

For every superspace $M = M^{(\bar{0})} \oplus M^{(\bar{1})}$, we have a linear involution θ_M defined by $\theta_M(u) = (-1)^i u$ for $u \in M^{(\bar{i})}$. In particular we have θ_V for a VOSA V. An *automorphism* of V is defined as an element $g \in GL(V)$ satisfying

$$g(a_{(n)}b) = g(a)_{(n)}g(b), \quad g(\mathbf{1}) = \mathbf{1}, \quad g(\omega) = \omega, \quad [\theta_V, g] = 1$$

for any $a, b \in V$, $n \in \mathbb{Z}$. The last condition means that automorphisms preserve the super-structure of V. It is clear that θ_V is an automorphism.

Let g be an automorphism of V satisfying $g^T = 1$. Then V is decomposed into as follows :

$$V = \bigoplus_{i=0}^{T-1} V^{(k;g)}, \quad V^{(k;g)} = \{a \in V | g(a) = e^{-\frac{2\pi i k}{T}} a\}$$

We see that $\mathbf{1}, \omega \in V^{(0;g)}$.

Definition 2.2. Let $g \in V$ be an automorphism satisfying $g^T = 1$. A *g-twisted weak V-supermodule* M is a vector superspace $M = M^{(\bar{0})} \oplus M^{(\bar{1})}$ equipped with bilinear map

$$-_{(n)}- : V \times M \to M, \quad (a, u) \mapsto a_{(n)}u, \quad n \in \frac{1}{T}\mathbb{Z}$$

for each $n \in \frac{1}{T}\mathbb{Z}$ satisfying the following axioms.

(1) For $a \in V$ and $u \in M$, there exists $N \in \frac{1}{T}\mathbb{Z}$ such that $a_{(n)}u = 0$ for $n \geq N$.

(2) For $a \in V^{(\bar{i})}$ and $u \in M^{(\bar{j})}$, $a_{(n)}u \in M^{(\overline{i+j})}$.

(3) For $a \in V^{(k;g)}$ and $u \in M$, $a_{(n)}u = 0$ if $n \notin \frac{k}{T} + \mathbb{Z}$.

(4) (Borcherds identity) For $a \in V^{(k;g)}, b \in V^{(l;g)}$, $u \in M$, $p \in \mathbb{Z}$, $r \in \frac{k}{T} + \mathbb{Z}$ and $q \in \frac{l}{T} + \mathbb{Z}$,

$$\begin{aligned}&\sum_{i=0}^{\infty} \binom{r}{i} (a_{(p+i)}b)_{(r+q-i)}u \\ &= \sum_{i=0}^{\infty} \binom{p}{i} (-1)^i (a_{(p+r-i)}(b_{(q+i)}u) - (-1)^{p+p(a)p(u)} b_{(p+q-i)}(a_{(r+i)}u))\end{aligned}$$

(5) For $u \in M$ and $n \in \mathbb{Z}$, $\mathbf{1}_{(n)}u = \delta_{n,-1}u$.

We denote by $\mathcal{WSM}_g(V)$ the category of weak g-twisted V-supermodules. A morphism $f : M \to N$ for objects M, N in $\mathcal{WSM}_g(V)$ is a linear map satisfying

$$a_{(n)} \circ f = f \circ a_{(n)} \quad \text{and} \quad \theta_N \circ f = f \circ \theta_M$$

for $a \in V$, $n \in \frac{1}{T}\mathbb{Z}$. We denote by $\mathrm{Hom}_V^{(\bar{0})}(M, N)$ the set of morphisms from M to N.

For a g-twisted weak V-supermodule M, $-\theta_M$ gives another super-structure on M. We denote by $M^\vee$ the g-twisted V-supermodule associated to the involution $-\theta_M$.

$$(M^\vee)^{(\bar{0})} = M^{(\bar{1})}, \quad (M^\vee)^{(\bar{1})} = M^{(\bar{0})}$$

A *logarithmic* g-twisted V-module is a g-twisted weak V-module M on which L_0 acts locally finite, the real parts of eigenvalues are bounded below and every generalized eigenspace is finite dimensional. The full subcategory of $\mathcal{WSM}_g(V)$ whose objects are logarithmic is denoted by $\mathcal{LSM}_g(V)$.

3 Semi-intertwining operators

Definition 3.1. Let g_1, g_2, g_3 be mutually commutative automorphisms such that $g_i^T = 1$ and M^i g_i-twisted weak V-supermodules. A semi-intertwining operator of type $\binom{M^3}{M^1\ M^2}$ is a formal power series $\mathcal{Y}(-,z)- = \sum_{n\in\mathbb{C}}(-_{(n)}-)z^{-n-1}$ of bilinear maps

$$-_{(n)}- : M^1 \times M^2 \to M^3, \quad (u, v) \mapsto u_{(n)}v$$

for $n \in \mathbb{C}$ satisfying the following axioms.

(1) For $u \in M^1$ and $v \in M^2$, $u_{(n)}v = 0$ for $n \in \mathbb{C}$ whose real part is sufficiently large.

(2) For $u \in (M^1)^{(\bar{i})}$ and $v \in (M^2)^{(\bar{j})}$, $u_{(n)}v \in (M^3)^{(\overline{i+j})}$.

(3) (Borcherds identity) For $a \in V^{(k;g_1)} \cap V^{(l;g_2)}$, $u \in M^1$, $v \in M^2$, $p \in \frac{k}{T} + \mathbb{Z}$, $r \in \frac{l}{T} + \mathbb{Z}$ and $q \in \mathbb{C}$,

$$\sum_{i=0}^{\infty} \binom{r}{i} (a_{(p+i)}u)_{(r+q-i)}v$$
$$= \sum_{i=0}^{\infty} \binom{p}{i} (-1)^i (a_{(p+r-i)}(u_{(q+i)}v) - (-1)^{p+p(a)p(u)} u_{(p+q-i)}(a_{(r+i)}v)).$$

We denote by $\overline{I}_V \binom{M^3}{M^1\ M^2}$ the space of all semi-intertwining operators of type $\binom{M^3}{M^1\ M^2}$. We have an endomorphism $t^r \in \mathrm{End}_{\mathbb{C}} \left(\overline{I}_V \binom{M^3}{M^1\ M^2} \right)$ defined by $(t^r \mathcal{Y})(-,z)- = z^r \mathcal{Y}(-,z)-$ for any $r \in \mathbb{C}$. We also have another endomorphism $D \in \mathrm{End}_{\mathbb{C}} \left(\overline{I}_V \binom{M^3}{M^1\ M^2} \right)$ defined by

$$(D\mathcal{Y})(u,z)v = -\mathcal{Y}(L_{-1}u,z)v + \frac{d}{dz}\mathcal{Y}(u,z)v.$$

A semi-intertwining operator $\mathcal{Y}(-,z)-$ is said to be tD-nilpotent[2] if there exists $K \in \mathbb{Z}_{>0}$ such that$((tD)^K \mathcal{Y})(-,z)- = 0$. We denote by $\overline{I}_V^{nil} \binom{M^3}{M^1\ M^2}$ the space of all tD-nilpotent semi-intertwining operators of type $\binom{M^3}{M^1\ M^2}$.

We now recall the notion of logarithmic intertwining operators. A logarithmic intertwining operator of type $\binom{M^3}{M^1\ M^2}$ is a polynomial in $\log z$ of semi-intertwining operators

$$\widehat{\mathcal{Y}}(-,z)- = \sum_{i=0}^{K} (\log z)^i \mathcal{Y}^{(i)}(-,z)-$$

satisfying $\widehat{\mathcal{Y}}(L_{-1}u,z)v = \frac{d}{dz}\widehat{\mathcal{Y}}(u,z)v$ for any $u \in M^1$ and $v \in M^2$. It is denoted by $I_V^{(\bar{0})} \binom{M^3}{M^1\ M^2}$ the space of all logarithmic intertwining operators of type $\binom{M^3}{M^1\ M^2}$.

If $\widehat{\mathcal{Y}}(-,z)- = \sum_{i=0}^{K} (\log z)^i \mathcal{Y}^{(i)}(-,z)-$ is logarithmic, then $\mathcal{Y}^{(0)}(-,z)-$ is tD-nilpotent. In fact, we have the following proposition.

Proposition 3.2. *The map*

$$I_V^{(\bar{0})} \binom{M^3}{M^1\ M^2} \to \overline{I}_V^{nil} \binom{M^3}{M^1\ M^2}, \quad \widehat{\mathcal{Y}}(-,z)- \mapsto \mathcal{Y}^{(0)}(-,z)-$$

is a linear isomorphism.

[2]In my talk, I called the notion integrable.

4 Fusion products

We recall a definition of fusion product. Let g, g_1, g_2 be mutually commutative automorphisms of V of finite order, M^i logarithmic g_i-twisted V-supermodules for $i = 1, 2$.

A *fusion product* in $\mathcal{LSM}_g(V)$ of twisted supermodules M^1 and M^2 is a pair $(X, \mathcal{Y}_X(-,z))$ of an object X in $\mathcal{LSM}_g(V)$ and a tD-nilpotent semi-intertwining operator $\mathcal{Y}_X(-,z)-$ of type $\binom{X}{M^1\ M^2}$ satisfying the following universality : For any object W in $\mathcal{LSM}_g(V)$ and any tD-nilpotent, semi-intertwining operator $\mathcal{Y}(-,z)-$, there exists a unique morphism $\phi_{\mathcal{Y}} \in \mathrm{Hom}_V^{(\overline{0})}(X, W)$ such that

$$\mathcal{Y}(-,z)- = \phi_{\mathcal{Y}} \circ \mathcal{Y}_X(-,z) - .$$

As is well known, fusion product is unique up to isomorphism if it exists. A fusion product of M^1 and M^2 is denoted by $(M^1 \boxtimes M^2, \mathcal{Y}_{M^1 \boxtimes M^2}(-,z))$.

Remark 4.1. Showing the existence is a difficult problem in general. But a fusion product exists if $V^{(\overline{0})}$ satisfies a finiteness condition called C_2-cofiniteness condition ([Miya11]).

Remark 4.2. If $g \neq g_1 g_2$, then $(0,0)$ is a fusion product. Hence we may regard a fusion product M^1 and M^2 in $\mathcal{LSM}_{g_1 g_2}(V)$ for objects M^i in $\mathcal{LSM}_{g_i}(V)$.

The following proposition is fundamental.

Proposition 4.3. *Let M^i be logarithmic g_i-twisted V-supermodules for $i = 1, 2$. Suppose that a fusion product $M^1 \boxtimes M^2$ exists. Then the map $\mathcal{Y}(-,z)- \mapsto \phi_{\mathcal{Y}}$ gives rise to a linear isomorphism*

$$\overline{I}_V^{int}\binom{W}{M^1\ M^2} \cong \mathrm{Hom}_V^{(\overline{0})}(M^1 \boxtimes M^2, W)$$

5 Symplectic-fermionic VOSA

Let $\mathfrak{h}$ be a vector space of dimension $2d$ with nondegenerate skew-symmetric bilinear form$\langle -, - \rangle$. Regarding $\mathfrak{h}$ as a super-commutative Lie superalgebra, we have a loop algebra $\mathfrak{h}[t, t^{-1}] = \mathfrak{h} \otimes \mathbb{C}[t, t^{-1}]$. This loop algebra has a nontrivial central extension $\widetilde{\mathfrak{h}} = \mathfrak{h}[t, t^{-1}] \oplus \mathbb{C}K$ by a one dimensional center $\mathbb{C}K$. The super-commutation relations are given by

$$[h \otimes t^n, h' \otimes t^m]_+ = \langle h, h' \rangle \delta_{m+n,0} K$$

The VOSA $\mathcal{F}$ is given as an exterior algebra

$$\mathcal{F} = \bigwedge \left(t^{-1} \mathfrak{h}[t^{-1}] \right),$$

which is a module for $\widetilde{\mathfrak{h}}$ such that K acts by the scalar 1. The involution $\theta = \theta_{\mathcal{F}}$ is defined as an algebra automorphism of the exterior algebra $\mathcal{F}$ such that

$$\theta(1) = 1, \quad \theta = -1 \text{ on } t^{-1}\mathfrak{h}[t^{-1}].$$

Theorem 5.1. ([A07]) *$\mathcal{F}$ is a simple VOSA of central charge $-2d$, and only $\mathcal{F}$ and $\mathcal{F}^\vee$ are simple objects in $\mathcal{LSM}_1(\mathcal{F})$ up to isomorphisms.*

By using twisted affinization of $\mathfrak{h}$, we can construct a θ-twisted supermodule $\mathcal{F}_t$. The twisted supermodule $\mathcal{F}_t$ is given as an exterior algebra $\mathcal{F}_t = \bigwedge\left(t^{-\frac{1}{2}}\mathfrak{h}[t^{-1}]\right)$. The involution $\theta_{\mathcal{F}_t}$ is defined as an algebra automorphism of the exterior algebra $\mathcal{F}_t$ such that

$$\theta_{\mathcal{F}_t}(1) = 1, \quad \theta_{\mathcal{F}_t} = -1 \text{ on } t^{-\frac{1}{2}}\mathfrak{h}[t^{-1}].$$

Theorem 5.2. ([AA1]) *Only $\mathcal{F}_t$ and $(\mathcal{F}_t)^\vee$ are simple objects in $\mathcal{LSM}_\theta(\mathcal{F})$ up to isomorphisms. Moreover, they are projective.*

Remark 5.3. The category $\mathcal{LSM}_\theta(\mathcal{F})$ is semisimple. That is, every object is a direct sum of copies of $\mathcal{F}_t$ or $(\mathcal{F}_t)^\vee$.

A logarithmic supermodule $\widehat{\mathcal{F}}$ is constructed as an exterior algebra $\widehat{\mathcal{F}} = \bigwedge\left(\mathfrak{h}[t^{-1}]\right) = \mathcal{F}\otimes\bigwedge\mathfrak{h}$. The involution $\theta_{\widehat{\mathcal{F}}}$ is defined as an algebra automorphism of the exterior algebra $\widehat{\mathcal{F}}$ such that

$$\theta_{\widehat{\mathcal{F}}}(1) = 1, \quad \theta_{\widehat{\mathcal{F}}} = -1 \text{ on } \mathfrak{h}[t^{-1}].$$

Theorem 5.4. ([AA1]) *Only $\widehat{\mathcal{F}}$ and $\widehat{\mathcal{F}}^\vee$ are indecomposable projective objects in $\mathcal{LSM}_1(\mathcal{F})$ up to isomorphisms.*

The category $\mathcal{LSM}_1(\mathcal{F})$ is not semisimple because $\widehat{\mathcal{F}}$ gives a reducible indecomposable module.

6 VOSA $\mathcal{F}$ with $d = 1$

To determine fusion products among twisted modules we first consider the case $\dim\mathfrak{h} = 2$, that is, $d = 1$. We denote by $\mathcal{T}$ the VOSA $\mathcal{F}$ with $d = 1$. Then the composition factors of $\widehat{\mathcal{T}}$ are $2\mathcal{T}$, $2\mathcal{T}^\vee$. In fact, there exists a sequence $\widehat{\mathcal{T}}[0] \subset \widehat{\mathcal{T}}[1] \subset \widehat{\mathcal{T}}$ of indecomposable submodules such that

$$\widehat{\mathcal{T}}[0] \cong \mathcal{T}, \quad \widehat{\mathcal{T}}[0] \subset \widehat{\mathcal{T}}[1], \quad \widehat{\mathcal{T}}[1]/\widehat{\mathcal{T}}[0] \cong \mathcal{T}^\vee \oplus \mathcal{T}^\vee, \quad \widehat{\mathcal{T}}/\widehat{\mathcal{T}}[1] \cong \mathcal{T}.$$

From the module structure of $\widehat{\mathcal{T}}$ we can calculate

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{T}}^{(\overline{0})}(\widehat{\mathcal{T}}, \mathcal{T}) = 1, \quad \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{T}}^{(\overline{0})}(\widehat{\mathcal{T}}, \mathcal{T}^\vee) = 0$$
$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{T}}^{(\overline{0})}(\widehat{\mathcal{T}}, \widehat{\mathcal{T}}) = 2, \quad \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{T}}^{(\overline{0})}(\widehat{\mathcal{T}}, \widehat{\mathcal{T}}^\vee) = 2$$

This shows that

$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{T}}^{(\overline{0})}(\widehat{\mathcal{T}}, \mathcal{T}) + \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{T}}^{(\overline{0})}(\widehat{\mathcal{T}}, \mathcal{T}^\vee) = 1$$
$$\dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{T}}^{(\overline{0})}(\widehat{\mathcal{T}}, \widehat{\mathcal{T}}) + \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{T}}^{(\overline{0})}(\widehat{\mathcal{T}}, \widehat{\mathcal{T}}^\vee) = 4$$

On the other hand, we can show that the following lemma.

Lemma 6.1. *Let M be a logarithmic $\mathcal{T}$-module. If*

$$\begin{aligned}&\dim \mathrm{Hom}_V^{(\bar{0})}(M, \widehat{\mathcal{T}}) + \dim \mathrm{Hom}_V^{(\bar{0})}(M, \widehat{\mathcal{T}}^\vee)\\ &= 4(\dim \mathrm{Hom}_V^{(\bar{0})}(M, \mathcal{T}) + \dim \mathrm{Hom}_V^{(\bar{0})}(M, \mathcal{T}^\vee))\end{aligned}$$

then M is projective.

In [AA2], we calculate the fusion rules, i.e. the dimensions of $\overline{I}_{\mathcal{T}}^{nil}\binom{M^3}{M^1\ M^2}$ for $M^1, M^2, M^3 = \mathcal{T}, \mathcal{T}_t, \widehat{\mathcal{T}}, \mathcal{T}^\vee, \mathcal{T}_t^\vee, \widehat{\mathcal{T}}^\vee$. Some of them are given as follows.

Theorem 6.2.

$$\begin{aligned}\dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{nil}\binom{\mathcal{T}_t}{\mathcal{T}\ \mathcal{T}_t} &\cong \dim \mathrm{Hom}_{\mathcal{T}}^{(\bar{0})}(\mathcal{T}_t, \mathcal{T}_t) = 1,\\ \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{nil}\binom{\mathcal{T}_t}{\mathcal{T}^\vee\ \mathcal{T}_t} &\cong \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{(\mathcal{T}_t)^\vee}{\mathcal{T}\ \mathcal{T}_t} \cong \dim \mathrm{Hom}_{\mathcal{T}}^{(\bar{0})}(\mathcal{T}_t, (\mathcal{T}_t)^\vee) = 0,\\ \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{nil}\binom{\mathcal{T}_t}{\widehat{\mathcal{T}}\ \mathcal{T}_t} &= 2,\\ \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{nil}\binom{\mathcal{T}_t}{(\widehat{\mathcal{T}})^\vee\ \mathcal{T}_t} &= 2.\end{aligned}$$

As shown in [A07], the even part of $\mathcal{T}$ is C_2-cofinite. Hence the existence of fusion product $\mathcal{T}_t \boxtimes \mathcal{T}_t$ is guaranteed by the result in [Miya11, Prop. 7].

Theorem 6.3.

$$\mathcal{T}_t \boxtimes \mathcal{T}_t \cong \widehat{\mathcal{T}}$$

as $\mathcal{T}$-supermodules. Hence $\mathcal{T}_t \boxtimes \mathcal{T}_t$ is projective.

Proof. We see that the following equalities hold.

$$\dim \mathrm{Hom}_{\mathcal{T}}^{(\bar{0})}(\mathcal{T}_t \boxtimes \mathcal{T}_t, \mathcal{T}) = \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{\mathcal{T}}{\mathcal{T}_t\ \mathcal{T}_t} = \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{\mathcal{T}_t}{\mathcal{T}\ \mathcal{T}_t} = 1, \quad (1)$$

$$\dim \mathrm{Hom}_{\mathcal{T}}^{(\bar{0})}(\mathcal{T}_t \boxtimes \mathcal{T}_t, \mathcal{T}^\vee) = \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{\mathcal{T}^\vee}{\mathcal{T}_t\ \mathcal{T}_t} = \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{\mathcal{T}_t}{\mathcal{T}^\vee\ \mathcal{T}_t} = 0, \quad (2)$$

$$\dim \mathrm{Hom}_{\mathcal{T}}^{(\bar{0})}(\mathcal{T}_t \boxtimes \mathcal{T}_t, \widehat{\mathcal{T}}) = \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{\widehat{\mathcal{T}}}{\mathcal{T}_t\ \mathcal{T}_t} = \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{\mathcal{T}_t}{\widehat{\mathcal{T}}\ \mathcal{T}_t} = 2, \quad (3)$$

$$\dim \mathrm{Hom}_{\mathcal{T}}^{(\bar{0})}(\mathcal{T}_t \boxtimes \mathcal{T}_t, \widehat{\mathcal{T}}^\vee) = \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{\widehat{\mathcal{T}}^\vee}{\mathcal{T}_t\ \mathcal{T}_t} = \dim_{\mathbb{C}} \overline{I}_{\mathcal{T}}^{int}\binom{\mathcal{T}_t}{\widehat{\mathcal{T}}^\vee\ \mathcal{T}_t} = 2. \quad (4)$$

We have

$$\dim \mathrm{Hom}_{\mathcal{T}}(\mathcal{T}_t \boxtimes \mathcal{T}_t, \widehat{\mathcal{T}}) = 4 = 4 \times \dim \mathrm{Hom}_{\mathcal{T}}(\mathcal{T}_t \boxtimes \mathcal{T}_t, \mathcal{T}).$$

By Lemma 6.1, $\mathcal{T}_t \boxtimes \mathcal{T}_t$ is projective. Therefore, $\mathcal{T}_t \boxtimes \mathcal{T}_t$ is a direct sum of copies of $\widehat{\mathcal{T}}$ and $\widehat{\mathcal{T}}^\vee$. The multiplicity of $\widehat{\mathcal{T}}$ is 1 by (1) and that of $\widehat{\mathcal{T}}^\vee$ is 0 by (2). Hence

$$\mathcal{T}_t \boxtimes \mathcal{T}_t \cong \widehat{\mathcal{T}}$$

□

As well, by using (1)–(4) and fusion rules among $\widehat{\mathcal{T}}$ we have

$$\widehat{\mathcal{T}} \boxtimes \mathcal{T}_t \cong 2\mathcal{T}_t \oplus 2(\mathcal{T}_t)^\vee,$$
$$\widehat{\mathcal{T}} \boxtimes \widehat{\mathcal{T}} \cong 2\widehat{\mathcal{T}} \oplus 2\widehat{\mathcal{T}}^\vee.$$

We have the following proposition.

Proposition 6.4. *For any objects N in $\mathcal{LSM}_1(\mathcal{T})$, $\widehat{\mathcal{T}} \boxtimes N$ is projective.*

7 Fusion products for the case $d \geq 2$

To determine fusion products for $\mathcal{F}$ in general case, we recall some facts for tensor products of VOSAs. For VOSAs V^1, V^2, the tensor product $V^1 \otimes V^2$ of vector spaces becomes a VOSA naturally. The involution $\theta_{V^1 \otimes V^2}$ is $\theta_{V^1} \otimes \theta_{V^2}$ and n-th product are given by

$$(a \otimes b)_{(n)}(u \otimes v) = (-1)^{ij} \sum_{m \in \mathbb{Z}} (a_{(m)}u) \otimes (b_{(n-m-1)}v) \tag{5}$$

for $a \in V^1$, $b \in (V^2)^{(\bar{i})}$, $u \in (V^1)^{(\bar{j})}$ and $v \in V^2$. Let g be an automorphism of V^1 of finite order and h an automorphism of V^2 of finite order. Then $g \otimes h$ is an automorphism of $V^1 \otimes V^2$ of finite order. Now let M be an object in $\mathcal{LSM}_g(V^1)$ and N an object in $\mathcal{LSM}_h(V^2)$. Then $M \otimes N$ becomes an object in $\mathcal{LSM}_{g \otimes h}(V^1 \otimes V^2)$. The action of $V^1 \otimes V^2$ on $M \otimes N$ is given by a similar way in (5).

In the case central charge of $\mathcal{F}$ is $-2d$, we have

$$\mathcal{F} \cong \mathcal{T}^{\otimes d}$$

Moreover as $\mathcal{T}^{\otimes d}$-modules,

$$\mathcal{F}_t \cong (\mathcal{T}_t)^{\otimes d}, \quad \widehat{\mathcal{F}} \cong (\widehat{\mathcal{T}})^{\otimes d}$$

To determine fusion rules among them we use the following facts.

Theorem 7.1. ([AA1]) *Let V^1, V^2 be VOSAs, g_1, g_2, g_3 mutually commutative automorphisms of V^1 of finite order, h_1, h_2, h_3 mutually commutative automorphisms of V^2 of finite order. Let M^1 be an object in $\mathcal{LSM}_{g_1}(V^1)$, M^2 an object in $\mathcal{LSM}_{g_2}(V^1)$, and let N^1 be an object in $\mathcal{LSM}_{h_1}(V^2)$, N^2 an object in $\mathcal{LSM}_{h_2}(V^2)$.*

Suppose that $M^1 \boxtimes M^2$ exists in $\mathcal{LSM}_{g_3}(V^1)$ and that the eigenvalues for L_0 on $M^1 \boxtimes M^2$ are discrete. Suppose also that $N^1 \boxtimes N^2$ exists in $\mathcal{LSM}_{h_3}(V^2)$ and that the eigenvalues for L_0 on $N^1 \boxtimes N^2$ are discrete. Then

$$(M^1 \otimes N^1) \boxtimes (M^2 \otimes N^2) \cong (M^1 \boxtimes M^2) \otimes (N^1 \boxtimes N^2)$$

in $\mathcal{LSM}_{g_3 \otimes h_3}(V^1 \otimes V^2)$.

By Theorem 7.1, it is easy to obtain the following isomorphisms.

$$\mathcal{F}_t \boxtimes \mathcal{F}_t \cong (\mathcal{T}_t^{\otimes d}) \boxtimes (\mathcal{T}_t^{\otimes d}) \cong (\mathcal{T}_t \boxtimes \mathcal{T}_t)^{\otimes d} \cong (\mathcal{T})^{\otimes d} \cong \widehat{\mathcal{F}}$$

As well we have

$$\widehat{\mathcal{F}} \boxtimes \mathcal{F}_t \cong (\mathcal{T} \boxtimes \mathcal{T}_t)^{\otimes d} \cong 2^{2d-1}(\mathcal{F}_t \oplus \mathcal{F}_t^{\vee}),$$
$$\widehat{\mathcal{F}} \boxtimes \widehat{\mathcal{F}} \cong (\mathcal{T} \boxtimes \mathcal{T})^{\otimes d} \cong (2\mathcal{T} \oplus 2\mathcal{T}^{\vee})^{\otimes d} \cong 2^{2d-1}(\widehat{\mathcal{F}} \oplus \widehat{\mathcal{F}}^{\vee}).$$

References

[A07] T. Abe, A $\mathbb{Z}_2$-orbifold model of the symplectic fermionic vertex operator superalgebra. Math. Z. 255 , no. 4, 755–792, (2007).

[AA1] T. Abe, Y. Arike, Fusion products of twisted supermodules for vertex operator superalgebras, in preparation.

[AA2] T. Abe, Y. Arike, The representation theory of the symplectic fermionic vertex operator superalgebra, in preparation.

[HK] R. Heluniani and V. Kac, Supersymmetric vertex algebras, *Commun. Math. Phys.*, **271**, no. 1, 103–178, (2007).

[K] V. Kac, *Vertex algebras for beginners*, Second edition, University Lecture Series **10**, American Mathematical Society, Providence, RI, 1998.

[Miya11] M. Miyamoto, Flatness and Semi-Rigidity of Vertex Operator Algebras, arXiv:1104.4675, (2011).

[Xu98] X. Xu, *Introduction to vertex operator superalgebras and their modules*, Mathematics and its applications, Kluwer Academic Publishers, 1998.

Classification of doubly even self-dual codes of length 40

別宮 耕一 Koichi BETSUMIYA

ここでは，長さ 40 の二元体上の重偶自己双対符号の分類を与えている。なお，本稿の内容は山形大学・原田昌晃氏，東北大学・宗政明弘氏との共同研究 [3] の一部である．

1 はじめに

$\mathbb{F}_2 = \{0, 1\}$ を二元体とする．$\mathbb{F}_2^n$ の k 次元部分空間 C を $[n, k]$ 符号と呼ぶ．また，$x = (x_1, x_2, \ldots, x_n) \in C$ に対して，$\mathrm{wt}(x) := |\mathrm{supp}(x)| := |\{i \in \{1, 2, \ldots, n\} \mid x_i \neq 0\}|$ を *Hamming* 重みと呼ぶ．$x := (x_1, x_2, \ldots, x_n)$, $y := (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$ に対して，内積を $x \cdot y = x_1y_1 + x_2y_2 + \cdots + x_ny_n$ とする．C と C' が置換同値であるとは，符号 C の座標の置換によって C' が得られることをいい，$C \cong C'$ と表記する．C を変化させない座標の置換を C の自己同型といい，C の自己同型全体を $\mathrm{Aut}(C)$ と記述し自己同型群と呼ぶ．

本稿で分類を与える符号のクラスの定義を与える．

定義 1. (i) 符号 $C \subset \mathbb{F}_2^n$ が重偶符号であるとは，任意の $x \in C$ に対して，$\mathrm{wt}(x) \equiv 0 \pmod 4$ となることをいう．

(ii) 符号 $C \subset \mathbb{F}_2^n$ に対して $C^\perp := \{x \in \mathbb{F}_2^n \mid x \cdot y = 0 \quad (\forall y \in C)\}$ を C の双対符号という．$[n, k]$ 符号 $C \subset \mathbb{F}_2^n$ が自己双対符号であるとは，$C = C^\perp$ を満たすことをいう．

ここで，重偶自己双対符号についてよく知られている事実を確認する．

定理 2 (Mallows, Sloane [20]). 長さ n の重偶自己双対符号について，最小重み d は次の限界式を満たす．

$$d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4 \tag{1}$$

この限界式 (1) の等号を満たす自己双対符号を極限的であるという．(1) より，長さ $n = 40$ の場合，最小重み $d \in \{4, 8\}$ であることが分かる．

重偶自己双対符号が存在するためには，長さ n が 8 の倍数であることが必要十分条件である．長さ 32 以下の重偶自己双対符号についてはすでに分類が与えられている．今回，長さ 40 の重偶自己双対符号の分類を行い，次の結果が得られた．

定理 3. 長さ 40 の非同値な重偶自己双対符号は全部で 94343 個存在し，そのうち 16470 個が極限的である．

以上の分類結果をまとめたものが表 2 である．ただし，d は符号の最小重みとする．なお，本稿でなされているコンピュータによる計算は Magma [6] を用いている．

2　分類方法

ここでは，長さ 40 の重偶自己双対符号の分類方法について述べる．

2.1　準備

長さ 40 の重偶自己双対符号の重み枚挙多項式を考える．A_i を重み i の符号語の個数とすると，重み枚挙多項式は次のようになる．[20]

$$\begin{aligned} &1 + A_4y^4 + (285 + 24A_4)y^8 + (21280 + 92A_4)y^{12} \\ &+(239970 - 600A_4)y^{16} + (525504 + 966A_4)y^{20} + \cdots + y^{40} \end{aligned} \tag{2}$$

長さ n の重偶自己双対符号の総数は次の式で与えられる．[19]

$$\prod_{i=0}^{n/2-2} (2^i + 1). \tag{3}$$

加えて，King [18] により，最小重み $d(d = 4, 8)$ ごとの長さ 40 の重偶自己双対符号の個数が求められている．具体的には，$N(40, d)$ を長さ 40，最小重み d の重偶自己双対符号の総数とすると，次のようになることが示されている．

$$\begin{aligned} N(40, 4) &= 4009357722800739726876619952910304312989584368968750, \\ N(40, 8) &= 10263335567003567415076803513287627980544163840000000. \end{aligned}$$

2.2　符号の同値判定

符号の分類問題では，ある条件を満たす符号の中で非同値のものがいくつあるかが興味の対象である．長さ 40 の自己双対符号については，次の手順を用いると比較的少ない計算量で同値，非同値を判定することができる．

C を長さ 40 の自己双対符号とする．$M(C)$ の行ベクトルを $\{w \in C \mid \mathrm{wt}(w) = 8\}$ とする行列とする．この行列の成分は $0, 1$ であるが，この成分を整数とみなすこととする．n_{ij} を $M(C)^T M(C)$ の (i, j) 成分とし，整数の集合 $N(C)$ を次のように定義する．

$$N(C) = \begin{cases} \{n_{ij} \mid 1 \le i, j \le 40\} \setminus \{57\} & C \text{ が極限的のとき}, \\ \{n_{ij} \mid 1 \le i, j \le 40\} & \text{それ以外のとき}. \end{cases}$$

ただし，重み i の符号語からなる集合は Magma 関数 `Words` で構成することができる．C に対して，$\alpha(C)$ を次のように定義する．

$$\alpha(C) = (\#\operatorname{Aut}(C), A_4, \max N(C), \min N(C), \#N(C)).$$

明らかに $\alpha(C)$ は符号の同値類における不変量となる．ただし，C の自己同型群 $\operatorname{Aut}(C)$ は Magma 関数 `AutomorphismGroup` で得られる．この不変量は長さ 40 の重偶自己双対符号の非同値性を高い精度で判定することができる．また，最終的にこの不変量で分割されたクラス内での同値性，非同値性は Magma 関数 `IsIsomorphic` で判定することができる．

2.3 最小重み 4

ここでは，長さ 36 の自己双対符号の分類結果を用いて，長さ 40，最小重み 4 の重偶自己双対符号の分類を与える．

まず，C を重偶ではない自己双対符号とし，部分符号 C_0 を $C_0 := \{v \in C \mid \mathrm{wt}(v) \equiv 0 \pmod 4\}$ とする．C_0 の $C_0^{\perp}$ における余次元は 1 となるので，$C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$ とコセット分解とすると，次の命題が成立する．

命題 4 (Brualdi, Pless [9]). C を長さ n の自己双対符号とする．$n \equiv 6 \pmod 8$ のとき，C_0, C_1, C_2, C_3 を前述の部分符号とすると，

$$C^* = \{(v,0,0) \mid v \in C_0\} \cup \{(v,1,1) \mid v \in C_2\} \cup \{(v,1,0) \mid v \in C_1\} \cup \{(v,0,1) \mid v \in C_3\}$$

は長さ $n+2$ の重偶自己双対符号となる．

C を長さ 36 の自己双対符号とし，$D := \{(0,0),(1,1)\}$ とすると，命題 4 より，$(C \oplus D)^*$ は長さ 40，最小重み 4 の重偶自己双対符号となる．即ち，長さ 36 の非同値な自己双対符号の総数は 519492 であるため [12]，519492 個の長さ 40，最小重み 4 の重偶自己双対符号を構成することができる．

節 2.2 の手法を用いることで，得られた 519492 個の符号は 77873 個の同値類に分けられることが分かる．結果，77873 個の同値類の代表系を $\mathcal{C}_{40,4}$ とすると，次の関係式を満たすことが分かる．

$$\sum_{C \in \mathcal{C}_{40,4}} \frac{40!}{\#\operatorname{Aut}(C)} = N(40,4). \tag{4}$$

このことは，長さ 40，最小重み 4 の重偶自己双対符号が他に存在しないことを示している．

表 1: 長さ 40 の重偶自己双対符号の総数

$(A_4, N(A_4))$				
$(0,16470)$	$(13,382)$	$(26,47)$	$(40,12)$	$(64,3)$
$(1,20034)$	$(14,374)$	$(27,16)$	$(41,1)$	$(66,1)$
$(2,17276)$	$(15,231)$	$(28,38)$	$(42,9)$	$(70,3)$
$(3,12168)$	$(16,236)$	$(29,13)$	$(43,3)$	$(72,1)$
$(4,8471)$	$(17,143)$	$(30,29)$	$(44,7)$	$(74,1)$
$(5,5552)$	$(18,160)$	$(31,7)$	$(46,7)$	$(78,1)$
$(6,3916)$	$(19,100)$	$(32,22)$	$(48,4)$	$(90,1)$
$(7,2610)$	$(20,104)$	$(33,3)$	$(50,4)$	$(92,1)$
$(8,1932)$	$(21,54)$	$(34,25)$	$(52,6)$	$(94,2)$
$(9,1243)$	$(22,90)$	$(35,3)$	$(54,2)$	$(106,1)$
$(10,1093)$	$(23,37)$	$(36,11)$	$(56,1)$	$(134,1)$
$(11,669)$	$(24,59)$	$(37,4)$	$(58,4)$	$(190,1)$
$(12,605)$	$(25,26)$	$(38,11)$	$(62,2)$	

2.4 最小重み 8

まず，C を $\mathbf{1} = (1, 1, \ldots, 1)$ を含む重偶符号とすると，次の関数が定義できる．

$$q_C : C^\perp / C \to \mathbb{F}_2 \quad (x + C \mapsto \frac{\mathrm{wt}(x)}{2} \bmod 2)$$

次に，$i = 1, 2$ に対して，C_i を $\mathbf{1}$ を含む長さ n_i の重偶符号とする．このとき，全単射な線形写像

$$f : C_1^\perp / C_1 \to C_2^\perp / C_2 \tag{5}$$

が等長写像であるとは $q_{C_1} = q_{C_2} \circ f$ を満たすこととする．等長写像 (5) 全体の集合を $\Phi(C_1, C_2)$ と表すこととする．等長写像 $f \in \Phi(C_1, C_2)$ に対して，符号 $D(C_1, C_2, f)$ を次のように定義する．

$$D(C_1, C_2, f) = \{(x_1, x_2) \in \mathbb{F}_2^{n_1+n_2} \mid x_1 \in C_1^\perp,\ x_2 \in f(x_1 + C_1)\} \tag{6}$$

定義より，$D(C_1, C_2, f)$ は重偶符号となる．また，

$$D(C_1, C_2, f) = \{(x_1, x_2) \in \mathbb{F}_2^{n_1+n_2} \mid x_2 \in C_2^\perp,\ x_1 \in f^{-1}(x_2 + C_2)\}$$

となることより，$\dim D(C_1, C_2, f) = n_1 - k_1 + k_2 = n_2 - k_2 + k_1 = \frac{n_1+n_2}{2}$ となり，$D(C_1, C_2, f)$ は自己双対符号となる．即ち，重偶自己双対符号となる．

生成行列を用いて表す．C_i の生成行列を R_i，C_i の生成行列を $\begin{pmatrix} R_i \\ \hline M_i \end{pmatrix}$ とする．つまり，$k_i = \dim C_i$ とし，

$$C_i = \{(x_1, \ldots, x_{k_i}) R_i \mid (x_1, \ldots, x_{k_i}) \in \mathbb{F}_2^{k_i}\},$$
$$C_i^\perp = \{(x_1, \ldots, x_{k_i}, \ldots, x_{n_i-k_i}) \begin{pmatrix} R_i \\ \hline M_i \end{pmatrix} \mid (x_1, \ldots, x_{n_i-k_i}) \in \mathbb{F}_2^{n_i-k_i}\}$$

とする．M_1 と M_2 の対応する行が f による対応と一致しているとき，$D(C_1, C_2, f)$ は次のように表すことができる．

$$D(C_1, C_2, f) = \left\{ (x_1, \ldots, x_{n_1-k_1+k_2}) \left(\begin{array}{c|c} R_1 & 0 \\ \hline 0 & R_2 \\ \hline M_1 & M_2 \end{array}\right) \;\middle|\; (x_1, \ldots, x_{n_1-k_1+k_2}) \in \mathbb{F}_2^{n_1-k_1+k_2} \right\}$$

ここで，$\Phi(C_1, C_2)$ の元の個数を求める．

命題 5. $|\Phi(C_1, C_2)| = |O^+_{n_1-2k_1}(2)|$.

証明. 任意の元 $f \in \Phi(C_1, C_2)$ を固定すると，$\Phi(C_1, C_2) = f \circ \Phi(C_1, C_1) = f \circ O(C_1^\perp / C_1, q_{C_1})$ となる．また，$O(C_1^\perp / C_1, q_{C_1}) \cong O^+_{n_1-2k_1}(2)$ であるので，求める等式が得られる． □

固定した重偶符号 C_1, C_2 に対して，$D(C_1, C_2, f)$ は等長写像 f の選び方に依存する．しかし，命題 5 より，$\Phi(C_1, C_2)$ の元の個数は直交群 $O^+_{n_1-2k_1}(2)$ の位数と一致するため，すべての f について符号を構成し，それらの同値，非同値を検証するには計算量が大きくな

り過ぎる．そこで，以下で同値な符号の検証の重複を回避し，計算量を計算可能な量に抑制する方法について述べる．

最初に，$\mathbf{1}$ を含む重偶符号 C について，$\mathrm{Aut}(C)$ の $C^\perp/C$ への作用を考えることで，$\mathrm{GL}(C^\perp/C)$ への準同型写像が得られるが，その像を $\mathcal{G}_0(C)$ と表すこととする．また，$\Phi(C,C)$ は $\mathrm{GL}(C^\perp/C)$ の部分群となり，$\mathcal{G}_1(C)$ と表すこととする．定義より，$\mathcal{G}_0(C)$ は $\mathcal{G}_1(C)$ の部分群となる．$\sigma_i \in \mathcal{G}_0(C_i)$ とし，f を $\sigma_2 \circ f \circ \sigma_1$ で置き換えると得られる符号は同値となる．即ち

$$D(C_1, C_2, f) \cong D(C_1, C_2, \sigma_2 \circ f \circ \sigma_1).$$

これは，$\{D(C_1, C_2, h) \mid h \in \Phi(C_1, C_2)\}$ の非同値なものを数え上げるためには，任意に固定した $f \in \Phi(C_1, C_2)$ に対して，両側剰余類 $(f^{-1} \circ \mathcal{G}_0(C_2) \circ f)\backslash\mathcal{G}_1(C_1)/\mathcal{G}_0(C_1)$ の代表系を H とするとき，$\{D(C_1, C_2, f \circ h) \mid h \in H\}$ を考えれば十分であることを意味している．

長さ 40 の極限的重偶自己双対符号を分類するため，$(n_1, n_2) = (16, 24)$ について，この方法を適用する．なお，長さ 16 と長さ 24 の重偶符号の分類は知られているので [21]，これを用いる．

C_1 を長さ 16，最小距離 8，$\dim C_1 \in \{3, 4, 5\}$ の重偶符号とし，C_2 を長さ 24，最小距離 8，$\dim C_2 = 4 + \dim C_1$ の重偶符号する．群 $\mathcal{G}_1(C_1)$ は Magma 関数 `GOPlus` で構成でき，両側剰余類の代表系 H は `DoubleCosetRepresentatives` で構成できる．その結果，得られた符号から節 2.2 の方法を用いて非同値なものを数え上げると 16468 個の長さ 40 の極限的重偶自己双対符号が得られた．加えて，それらに含まれない 2 個の符号の存在が知られている．ひとつは [28] で構成されている自己同型群の位数が 6840 のもの，もうひとつは，[29] で $H^{(1234)}B_6'$ と表されている自己同型群の位数 120 のものである．

結果，16470 個の同値類の代表系を $\mathcal{C}_{40,8}$ とすると，次の関係式を満たすことが分かる．

$$\sum_{C \in \mathcal{C}_{40,8}} \frac{40!}{\#\,\mathrm{Aut}(C)} = N(40, 8). \tag{7}$$

このことは，長さ 40，最小重み 8 の重偶自己双対符号が他に存在しないことを示している．(4)，(7) より，定理 3 が示された．

表 2: 長さ n の重偶自己双対符号の個数

長さ n	個数	個数 $(d = 8)$	出典
8	1	0	[23]
16	2	0	[23]
24	9	1	[24]
32	85	5	[10]
40	94343	16470	[3]

参考文献

[1] C. Aguilar-Melchor, P. Gaborit, J.-L. Kim, L. Sok and P. Solé. Classification of extremal and s-extremal binary self-dual codes of length 38. *IEEE Trans. Inform. Theory*, 58:2253–2262, 2012.

[2] E. F. Assmus, Jr. and V. Pless. On the covering radius of extremal self-dual codes. *IEEE Trans. Inform. Theory*, 29:359–363, 1983.

[3] K. Betsumiya, M. Harada and A. Munemasa, A complete classification of doubly even self-dual codes of length 40, E. J. Comb. 19(3) (2012), #P18

[4] R. T. Bilous. Enumeration of the binary self-dual codes of length 34. *J. Combin. Math. Combin. Comput.*, 59:173–211, 2006.

[5] R. T. Bilous and G. H. J. van Rees. An enumeration of self-dual codes of length 32. *Des. Codes, Cryptogr.*, 26:61–86, 2002.

[6] W. Bosma and J. Cannon. Handbook of Magma Functions. Department of Mathematics, University of Sydney, Available online at `http://magma.maths.usyd.edu.au/magma/`.

[7] S. Bouyuklieva. Some optimal self-orthogonal and self-dual codes. *Disc. Math.*, 287:1–10, 2004.

[8] S. Bouyuklieva and I. Bouyukliev. An algorithm for classification of binary self-dual codes. *IEEE Trans. Inform. Theory*, 58:3933–3940, 2012.

[9] R. Brualdi and V. Pless. Weight enumerators of self-dual codes. *IEEE Trans. Inform. Theory*, 37:1222–1225, 1991.

[10] J. H. Conway, V. Pless and N. J. A. Sloane. The binary self-dual codes of length up to 32: a revised enumeration. *J. Combin. Theory Ser. A*, 60:183–195, 1992.

[11] J. H. Conway and N. J. A. Sloane. A new upper bound on the minimal distance of self-dual codes. *IEEE Trans. Inform. Theory*, 36:1319–1333, 1990.

[12] M. Harada and A. Munemasa. Classification of self-dual codes of length 36. *Advances Math. Communications*, 6:229–235, 2012.

[13] M. Harada and A. Munemasa. Database of Self-Dual Codes. Available online at `http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm`.

[14] M. Harada, A. Munemasa and K. Tanabe. Extremal self-dual $[40, 20, 8]$ codes with covering radius 7. *Finite Fields Appl.*, 10:183–197, 2004.

[15] M. Harada and M. Ozeki. Extremal self-dual codes with the smallest covering radius. *Disc. Math.*, 215:271–281, 2000.

[16] W. C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, 11:451–490, 2005.

[17] H. J. Kim. Self-dual codes with automorphism of order 3 having 8 cycles. *Des. Codes Cryptogr.*, 57:329–346, 2010.

[18] O. D. King. The mass of extremal doubly-even self-dual codes of length 40. *IEEE Trans. Inform. Theory*, 47:2558–2560, 2001.

[19] F. J. MacWilliams, N. J. A. Sloane and J. G. Thompson. Good self dual codes exist. *Disc. Math.*, 3:153–162, 1972.

[20] C. L. Mallows and N. J. A. Sloane. An upper bound for self-dual codes. *Inform. Control*, 22:188–200, 1973.

[21] R. L. Miller. Doubly Even Codes. Available online at `http://www.rlmiller.org/de_codes/`.

[22] M. Ozeki. Jacobi polynomials for singly even self-dual codes and the covering radius problems. *IEEE Trans. Inform. Theory*, 48:547–557, 2002.

[23] V. Pless. A classification of self-orthogonal codes over GF(2). *Disc. Math.*, 3:209–246, 1972.

[24] V. Pless and N. J. A. Sloane. On the classification and enumeration of self-dual codes. *J. Combin. Theory Ser. A*, 18:313–335, 1975.

[25] E. M. Rains. Shadow bounds for self-dual codes. *IEEE Trans. Inform. Theory*, 44:134–139, 1998.

[26] E. Rains and N. J. A. Sloane. Self-dual codes. In *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman (Editors), pages 177–294, Elsevier, Amsterdam, 1998.

[27] B. Runge. Codes and Siegel modular forms. *Disc. Math.*, 148:175–204, 1996.

[28] V. Y. Yorgov. Binary self-dual codes with automorphisms of odd order. *Problems Inform. Transmission*, 19:260–270, 1984. translated from *Problemy Peredachi Informatsii*, 19:11–24, 1983 (Russian).

[29] V. Y. Yorgov and N. Zyapkov. Doubly even self-dual $[40, 20, 8]$-codes with an automorphism of odd order. *Problems Inform. Transmission*, 32:253–257, 1997. translated from *Problemy Peredachi Informatsii*, 32:41–46, 1996 (Russian).

A VERTEX OPERATOR ALGEBRA WHOSE MIYAMOTO INVOLUTIONS GENERATE A GROUP $3^2{:}2$ OF $3C$-PURE TYPE

CHING HUNG LAM

Abstract. In this article, we will describe a construction of a vertex operator algebra W generated by 3 Ising vectors such that (1) any two of them generate a 3C-algebra; (2) the group generated by the corresponding Miyamoto involutions has the shape $3^2{:}2$ on W; and (3) $W_1 = 0$.

1. Introduction

This article is based on a joint work with Hsian Yang Chen of Academia Sinica, Taiwan. We will describe briefly a vertex operator algebra W generated by 3 Ising vectors such that (1) any two of them generate a 3C-algebra; (2) the group generated by the corresponding Miyamoto involutions has the shape $3^2{:}2$ on W; and (3) $W_1 = 0$. The detail will be appeared elsewhere.

The main idea is to combine the construction of the so-called dihedral subVOA from [LYY1] and the construction of EE_8-pairs from [GL]. In fact, it is quite straightforward to find 3 Ising vectors satisfying conditions (1) and (2). The main difficulty is to show the subVOA generated by these 3 Ising vectors has zero weight 1 subspace.

First we will recall some definitions and review several basic facts.

Definition 1.1. Let V be a VOA. An element $e \in V_2$ is called an *Ising vector* if the subVOA $\mathrm{Vir}(e)$ generated by e is isomorphic to the simple Virasoro VOA $L(\frac{1}{2}, 0)$ of central charge $1/2$.

Remark 1.2. It is well known the VOA $L(\frac{1}{2}, 0)$ is rational and it has exactly 3 irreducible modules $L(\frac{1}{2}, 0)$, $L(\frac{1}{2}, \frac{1}{2})$, and $L(\frac{1}{2}, \frac{1}{16})$ (cf. [DMZ, Mi]).

Remark 1.3. Let V be a VOA and let $e \in V$ be an Ising vector. Then we have the decomposition

$$V = V_e(0) \oplus V_e(\frac{1}{2}) \oplus V_e(\frac{1}{16}),$$

2010 *Mathematics Subject Classification.* Primary 17B69; Secondary 20B25 .

Partially supported by NSC grant 100-2628-M-001005-MY4 .

where $V_e(h)$ denotes the sum of all irreducible $\mathrm{Vir}(e)$-submodules of V isomorphic to $L(\frac{1}{2}, h)$ for $h \in \{0, \frac{1}{2}, \frac{1}{16}\}$.

Theorem 1.4 ([Mi]). *The linear map $\tau_e : V \to V$ defined by*

$$\tau_e := \begin{cases} 1 & \text{on } V_e(0) \oplus V_e(\frac{1}{2}), \\ -1 & \text{on } V_e(\frac{1}{16}), \end{cases} \tag{1.1}$$

is an automorphism of V.

On the fixed point subspace $V^{\tau_e} = V_e(0) \oplus V_e(1/2)$, the linear map $\sigma_e : V^{\tau_e} \to V^{\tau_e}$ defined by

$$\sigma_e := \begin{cases} 1 & \text{on } V_e(0), \\ -1 & \text{on } V_e(\frac{1}{2}). \end{cases} \tag{1.2}$$

is an automorphism of V^{τ_e}.

1.1. **3C-algebra.** Next we recall the properties of the $3C$-algebra U_{3C} from [LYY2] (see also [Sa]). The followings can be found in [LYY2, Section 3.9].

Lemma 1.5. *Let $U = U_{3C}$ be the $3C$-algebra defined as in* [LYY2]. *Then*

(1) *$U_1 = 0$ and U is generated by its weight 2 subspace U_2 as a VOA.*
(2) *$\dim U_2 = 3$ and it is spanned by 3 Ising vectors.*
(3) *There exists exactly 3 Ising vectors in U_2, say, e^0, e^1, e^2. Moreover, we have*

$$(e^i)_1(e^j) = \frac{1}{32}(e^i + e^j - e^k), \quad \langle e^i, e^j \rangle = \frac{1}{2^8}, \quad \text{and} \quad \tau_{e^i} e^i = \tau_{e^j} e^i = e^k$$

for $i \neq j$ and $\{i, j, k\} = \{0, 1, 2\}$.
(4) *The Virasoro element of U is given by*

$$\frac{32}{33}(e^0 + e^1 + e^2).$$

(5) *Let $a = \frac{32}{33}(e^0 + e^1 + e^2) - e^0$. Then a is a simple Virasoro vector of central charge $21/22$. Moreover, the subVOA generated by e^0 and a is isomorphic to $L(\frac{1}{2}, 0) \otimes L(\frac{21}{22}, 0)$.*

The decomposition of U_{3C} as a sum of irreducible $\mathrm{Vir}(e^0) \otimes \mathrm{Vir}(a)$-modules is also obtained.

Proposition 1.6 (Theorem 3.35 of [LYY2]). *As a module of* $L(\frac{1}{2},0)\otimes L(\frac{21}{22},0)$,

$$\begin{aligned} U_{3C} \cong\ & L(\frac{1}{2},0)\otimes L(\frac{21}{22},0)\oplus L(\frac{1}{2},0)\otimes L(\frac{21}{22},8)\\ & \oplus L(\frac{1}{2},\frac{1}{2})\otimes L(\frac{21}{22},\frac{7}{2})\oplus L(\frac{1}{2},\frac{1}{2})\otimes L(\frac{21}{22},\frac{45}{2})\\ & \oplus L(\frac{1}{2},\frac{1}{16})\otimes L(\frac{21}{22},\frac{31}{16})\oplus L(\frac{1}{2},\frac{1}{16})\otimes L(\frac{21}{22},\frac{175}{16}). \end{aligned}$$

For simplicity, we shall use $[h_1,h_2]$ to denote the module $L(\frac{1}{2},h_1)\otimes L(\frac{21}{22},h_2)$. The following classification theorem can be found in [LYY2].

Theorem 1.7 (Theorem 3.38. of [LYY2]). *There are exactly five irreducible U_{3C}-modules. As $L(\frac{1}{2},0)\otimes L(\frac{21}{22},0)$-modules, they are of the following form:*

$$\begin{aligned} U(0) &\cong [0,0]\oplus[0,8]\oplus[\frac{1}{2},\frac{7}{2}]\oplus[\frac{1}{2},\frac{45}{2}]\oplus[\frac{1}{16},\frac{31}{16}]\oplus[\frac{1}{16},\frac{175}{16}]\,(=U_{3C}),\\ U(2) &\cong [0,\frac{13}{11}]\oplus[0,\frac{35}{11}]\oplus[\frac{1}{2},\frac{15}{22}]\oplus[\frac{1}{2},\frac{301}{22}]\oplus[\frac{1}{16},\frac{21}{176}]\oplus[\frac{1}{16},\frac{901}{176}],\\ U(4) &\cong [0,\frac{6}{11}]\oplus[0,\frac{50}{11}]\oplus[\frac{1}{2},\frac{1}{22}]\oplus[\frac{1}{2},\frac{155}{22}]\oplus[\frac{1}{16},\frac{85}{176}]\oplus[\frac{1}{16},\frac{261}{176}],\\ U(6) &\cong [0,\frac{1}{11}]\oplus[0,\frac{111}{11}]\oplus[\frac{1}{2},\frac{35}{22}]\oplus[\frac{1}{2},\frac{57}{22}]\oplus[\frac{1}{16},\frac{5}{176}]\oplus[\frac{1}{16},\frac{533}{176}],\\ U(8) &\cong [0,\frac{20}{11}]\oplus[0,\frac{196}{11}]\oplus[\frac{1}{2},\frac{7}{22}]\oplus[\frac{1}{2},\frac{117}{22}]\oplus[\frac{1}{16},\frac{133}{176}]\oplus[\frac{1}{16},\frac{1365}{176}]. \end{aligned}$$

2. Lattice VOA $V_{E_8\perp E_8\perp E_8}$

Next we shall describe the construction of W using the lattice VOA $V_{E_8\perp E_8\perp E_8}$.

Our notation for the lattice vertex operator algebra

$$V_L = M(1)\otimes\mathbb{C}\{L\} \tag{2.1}$$

associated with a positive definite even lattice L is standard [FLM]. In particular, $\mathfrak{h}=\mathbb{C}\otimes_{\mathbb{Z}} L$ is an abelian Lie algebra and we extend the bilinear form to $\mathfrak{h}$ by $\mathbb{C}$-linearity. $\hat{\mathfrak{h}}=\mathfrak{h}\otimes\mathbb{C}[t,t^{-1}]\oplus\mathbb{C}k$ is the corresponding affine algebra and $\mathbb{C}k$ is the 1-dimensional center of $\hat{\mathfrak{h}}$. The subspace $M(1)=\mathbb{C}[\alpha_i(n)|1\le i\le d, n<0]$ for a basis $\{\alpha_1,\dots,\alpha_d\}$ of $\mathfrak{h}$, where $\alpha(n)=\alpha\otimes t^n$, is the unique irreducible $\hat{\mathfrak{h}}$-module such that $\alpha(n)\cdot 1=0$ for all $\alpha\in\mathfrak{h}$ and n nonnegative, and $k=1$. Also, $\mathbb{C}\{L\}=span\{e^\beta\mid\beta\in L\}$ is the twisted group algebra of the additive group L such that $e^\beta e^\alpha=(-1)^{\langle\alpha,\beta\rangle}e^\alpha e^\beta$ for any $\alpha,\beta\in L$. The vacuum vector $\mathbb{1}$ of V_L is $1\otimes e^0$ and the Virasoro element ω is $\frac{1}{2}\sum_{i=1}^d\beta_i(-1)^2\cdot\mathbb{1}$ where $\{\beta_1,...,\beta_d\}$ is an orthonormal basis of $\mathfrak{h}$. For the explicit definition of the corresponding vertex operators, we shall refer to [FLM] for details.

Definition 2.1. Let A and B be integral lattices with the inner products $\langle\ ,\ \rangle_A$ and $\langle\ ,\ \rangle_B$, respectively. *The tensor product of the lattices* A and B is defined to be the integral lattice which is isomorphic to $A \otimes_{\mathbb{Z}} B$ as a $\mathbb{Z}$-module and has the inner product given by

$$\langle \alpha \otimes \beta, \alpha' \otimes \beta' \rangle = \langle \alpha, \alpha' \rangle_A \cdot \langle \beta, \beta' \rangle_B, \quad \text{for any } \alpha, \alpha' \in A, \text{ and } \beta, \beta' \in B.$$

We simply denote the tensor product of the lattices A and B by $A \otimes B$.

Now let $L = E_8 \perp E_8 \perp E_8$ be the orthogonal sum of 3 copies of the root lattice of type E_8. Set

$$\begin{aligned} M &= \{(\alpha, -\alpha, 0) \mid \alpha \in E_8\} < L, \quad \text{and} \\ N &= \{(0, \alpha, -\alpha) \mid \alpha \in E_8\} < L. \end{aligned} \tag{2.2}$$

Then $M \cong N \cong \sqrt{2}E_8$ and $M + N \cong A_2 \otimes E_8$ (see [GL]). Note that there is a third $\sqrt{2}E_8$-sublattice

$$\tilde{N} = \{(\alpha, 0, -\alpha) \mid \alpha \in E_8\} < M + N.$$

We shall fix a (bilinear) 2-cocyle $\varepsilon_0 : E_8 \times E_8 \to \mathbb{Z}_2$ such that

$$\begin{aligned} \varepsilon_0(\alpha, \alpha) &\equiv \frac{1}{2}\langle \alpha, \alpha \rangle \mod 2, \\ \text{and} \quad \varepsilon_0(\alpha, \beta) - \varepsilon_0(\beta, \alpha) &\equiv \langle \alpha, \beta \rangle \mod 2, \end{aligned} \tag{2.3}$$

for all $\alpha, \beta \in E_8$. Note that such a 2-cocycle exists (cf. [FLM, (6.1.27)-(6.1.29)]). Moreover, $e^{\alpha}e^{-\alpha} = -e^0$ for any $\alpha \in E_8, \langle \alpha, \alpha \rangle = 2$.

We shall extend ε_0 to L by defining

$$\varepsilon_0\Big((\alpha, \alpha', \alpha''), (\beta, \beta', \beta'')\Big) = \varepsilon_0(\alpha, \beta) + \varepsilon_0(\alpha', \beta') + \varepsilon_0(\alpha'', \beta'').$$

It is easy to check by direct calculations that ε_0 is trivial on M, N or $\tilde{N}$.

Consider the lattice VOA

$$V_L \cong V_{E_8} \otimes V_{E_8} \otimes V_{E_8}.$$

We use s to denote the automorphism that acts as a cyclic permutation of the 3 copies of V_{E_8} in $V_L = V_{E_8} \otimes V_{E_8} \otimes V_{E_8}$.

Definition 2.2. Let α^0 be a root of E_8 such that

$$K := \{\beta \in E_8 \mid \langle \beta, \alpha^0 \rangle \in 3\mathbb{Z}\} \cong A_8.$$

Set $\tilde{\alpha} = (\alpha^0, -\alpha^0, 0)$ and define an automorphism ρ of V_L by

$$\rho = \exp\left(\frac{2\pi i}{3}\tilde{\alpha}(0)\right).$$

Then ρ has order 3 and the fixed point subspace $V_M^\rho \cong V_{\sqrt{2}A_8}$.

Notation 2.3. Let M, N and ρ be defined as above. Set

$$e := e_M = \frac{1}{16}\omega_M + \frac{1}{32}\sum_{\alpha\in M(4)} e^\alpha,$$

$$f := e_N = \frac{1}{16}\omega_N + \frac{1}{32}\sum_{\alpha\in N(4)} e^\alpha, \quad \text{and}$$

$$e' := \rho(e).$$

Then e, f, e' are Ising vectors (see [LYY1]).

The following lemma can be proved by direct calculations (see [GL, LYY1, LYY2]).

Lemma 2.4. *We have* $\langle e, f\rangle = \langle e, e'\rangle = \langle f, e'\rangle = 1/2^8$. *Moreover, the sub VOA* $\mathrm{VOA}(e, f)$, $\mathrm{VOA}(e, g)$, $\mathrm{VOA}(f, g)$ *generated by* $\{e, f\}$, $\{e, e'\}$ *and* $\{f, e'\}$, *respectively, are isomorphic to the* $3C$*-algebra* U_{3C}.

Notation 2.5. Let $W := \mathrm{VOA}(e, f, e')$. We also denote $h = \tau_e\tau_f$ and $g = \tau_e\tau_{e'}$. Then g and h both have order 3. Note also that $e, f, e' \in V_{M+N}$ and thus $W < V_{M+N} \cong V_{A_2\otimes E_8}$.

Lemma 2.6. *As automorphisms of* W, g *commutes with* h.

Proof. Recall that $g = \tau_e\tau_{e'} = \rho$ on V_L (see [LYY1]). Moreover, $h(e) = f = e_N$ and $h^2(e) = e_{\tilde{N}}$.

By a direct calculation, we have

$$hg(e) = hgh^{-1}h(e) = \rho^h(e_N),$$

where $\rho^h = h\rho h^{-1} = \exp\left(\frac{2\pi i}{3}(0, \alpha_0, -\alpha_0)(0)\right)$.

Since $\langle(0, \beta, -\beta), (0, \alpha, -\alpha)\rangle = 2\langle\beta, \alpha\rangle$ and $\langle(0, \beta, -\beta), (\alpha, -\alpha, 0)\rangle = -\langle\beta, \alpha\rangle$, we have

$$gh(e) = \rho(e_N) = \rho^h(e_N) = hg(e).$$

Similarly, we have

$$hg(e') = hg^2(e) = (\rho^h)^2(e_N), \quad gh(e') = ghg(e) = g(\rho^h(e_N)) = (\rho^h)^2(e_N)$$

and

$$hg(f) = hgh(e) = (hgh^2)h^2(e) = \rho^h(e_{\tilde{N}}), \quad gh(f) = g(e_{\tilde{N}}) = \rho(e_{\tilde{N}}).$$

Hence $gh = hg$ on W. ∎

Notation 2.7. For any $0 \leq i, j \leq 2$, denote

$$e^{i,j} = g^i h^j(e).$$

In particular, we have

$$\begin{aligned} e^{0,0} &= e_M, & e^{0,1} &= e_N, & e^{0,2} &= e_{\tilde{N}}, \\ e^{1,0} &= \rho e_M, & e^{1,1} &= \rho e_N, & e^{1,2} &= \rho e_{\tilde{N}}, \\ e^{2,0} &= \rho^2 e_M, & e^{2,1} &= \rho^2 e_N, & e^{2,2} &= \rho^2 e_{\tilde{N}}. \end{aligned}$$

Lemma 2.8. *Let G be the subgroup of $Aut(W)$ generated by τ_e, τ_f and $\tau_{e'}$. Then G has the shape $3^2 : 2$.*

Proof. Use Lemma 2.6. ∎

3. Affine VOA $L_{\widehat{sl}_9(\mathbb{C})}(3, 0)$

Recall from Definition 2.2 that the sublattice

$$K = \{\beta \in E_8 \mid \langle \beta, \alpha^0 \rangle \in 3\mathbb{Z}\} \cong A_8.$$

Thus, we have an embedding

$$V_{K \perp K \perp K} \cong V_K \otimes V_K \otimes V_K \hookrightarrow V_L.$$

It is also well known [FLM] that $V_K \cong V_{A_8}$ is an irreducible level 1 representation of the affine Lie algebra $\widehat{sl}_9(\mathbb{C})$. Moreover, the weight 1 subspace $(V_K)_1$ is a simple Lie algebra isomorphic to $sl_9(\mathbb{C})$.

Let $\iota_i : K \to K \perp K \perp K$, $i = 1, 2, 3$, be the embedding of K into the i-th direct summand of $K \perp K \perp K$, i.e.,

$$\iota_1(\alpha) = (\alpha, 0, 0), \quad \iota_2(\alpha) = (0, \alpha, 0), \quad \iota_3(\alpha) = (0, 0, \alpha),$$

for any $\alpha \in K$.

For any $\alpha \in K(2) := \{\alpha \in K \mid \langle \alpha, \alpha \rangle = 2\}$, set

$$\begin{aligned} H_\alpha &= (\alpha, \alpha, \alpha)(-1) \cdot \mathbb{1}, \\ E_\alpha &= e^{\iota_1(\alpha)} + e^{\iota_2(\alpha)} + e^{\iota_3(\alpha)}. \end{aligned}$$

Then $\{H_\alpha, E_\alpha \mid \alpha \in K(2)\}$ generates a subVOA isomorphic to the affine VOA $L_{\hat{sl}_9(\mathbb{C})}(3, 0)$ in V_L (see [DL, Proposition 13.1] and [FZ]). Moreover, the Virasoro element of $L_{\hat{sl}_9(\mathbb{C})}(3, 0)$

is given by

$$\Omega = \frac{1}{2(3+9)}\left[\sum_{k=1}^{8}(h^k,h^k,h^k)(-1)^2\cdot\mathbb{1} + \sum_{\alpha\in K(2)}(E_\alpha)_{-1}(-E_{-\alpha})\right],$$

where $\{h^1,\dots,h^8\}$ is an orthonormal basis of $K\otimes\mathbb{C} = E_8\otimes\mathbb{C}$.

Notation 3.1. Let $E = \{(\alpha,\alpha,\alpha) \mid \alpha\in E_8\}$ be a sublattice of L. Note also that

$$E = Ann_L(M+N) := \{\beta\in L \mid \langle\beta,\beta'\rangle = 0 \text{ for all } \beta'\in M+N\}.$$

Lemma 3.2. *Denote the Virasoro element of a lattice VOA V_S by ω_S. Then we have*

$$\begin{aligned}\Omega &= \omega_E + \frac{3}{4}\omega_{M+N} - \frac{1}{12}\sum_{\substack{\alpha\in K(2)\\1\le i,j\le 3, i\neq j}} e^{\iota_i(\alpha)-\iota_j(\alpha)},\\ &= \omega_L - \frac{8}{9}\sum_{0\le i,j\le 2} e^{i,j}.\end{aligned}$$

Proof. Let $\{h^1,\dots,h^8\}$ be an orthonormal basis of $A_8\otimes\mathbb{C} = E_8\otimes\mathbb{C}$. Then

$$\begin{aligned}\Omega =& \frac{1}{2(3+9)}\left[\sum_{k=1}^{8}(h^k,h^k,h^k)(-1)^2\cdot\mathbb{1}\right.\\ &\left. - \sum_{\alpha\in K(2)}(e^{\iota_1(\alpha)}+e^{\iota_2(\alpha)}+e^{\iota_3(\alpha)})_{-1}(e^{-\iota_1(\alpha)}+e^{-\iota_2(\alpha)}+e^{-\iota_3(\alpha)})\right],\\ =&\frac{1}{24}\left[6\omega_E + \sum_{\alpha\in K(2)}\sum_{i=1}^{3}\frac{1}{2}(\iota_i(\alpha)(-2)\cdot\mathbb{1} + \iota_i(\alpha)(-1)^2\cdot\mathbb{1})\right.\\ &\left. -2\sum_{\substack{\alpha\in K\\1\le i,j\le 3, i\neq j}} e^{\iota_i(\alpha)-\iota_j(\alpha)}\right],\\ =&\frac{1}{4}\omega_E + \frac{18}{24}\omega_L - \frac{1}{12}\sum_{\substack{\alpha\in K(2)\\1\le i,j\le 3, i\neq j}} e^{\iota_i(\alpha)-\iota_j(\alpha)}.\end{aligned}$$

Since $\omega_L = \omega_{M+N} + \omega_E$, we have

$$\Omega = \omega_E + \frac{3}{4}\omega_{M+N} - \frac{1}{12}\sum_{\substack{\alpha\in K(2)\\1\le i,j\le 3, i\neq j}} e^{\iota_i(\alpha)-\iota_j(\alpha)},$$

as desired. ∎

Lemma 3.3. *For any $0 \leq i_0, j_0 \leq 2$, we have $e^{i_0,j_0} \in \mathrm{Com}_{V_L}\left(L_{\widehat{sl}_9(\mathbb{C})}(3,0)\right)$. Hence $W \subset \mathrm{Com}_{V_L}\left(L_{\widehat{sl}_9(\mathbb{C})}(3,0)\right)$.*

Proof. By Lemma 1.5, we have

$$(e^{i,j})_1(e^{i_0,j_0}) = \begin{cases} \frac{1}{32}(e^{i_0,j_0} + e^{i,j} - e^{i',j'}) & \text{if } (i,j) \neq (i_0,j_0), \\ 2e^{i_0,j_0} & \text{if } (i,j) = (i_0,j_0). \end{cases}$$

Thus,

$$\Omega_1(e^{i_0,j_0}) = 2e^{i_0,j_0} - \frac{8}{9}(2e^{i_0,j_0} + \frac{1}{32} \cdot 8e^{i_0,j_0}) = 0$$

as desired. ∎

Theorem 3.4. *Let W be the subVOA generated by e, f and e' in V_L. Then $W_1 = 0$.*

Proof. Since $h(-1) \cdot \mathbb{1} \in L_{\hat{sl}_9(\mathbb{C})}(3,0)$ for all $h \in E$, the commutant subVOA

$$\mathrm{Com}_{V_L}\left(L_{\widehat{sl}_9(\mathbb{C})}(3,0)\right) \subset V_{M+N}.$$

Therefore, it suffices to show $W \cap (V_{M+N})_1 = 0$.

Recall that $M + N \cong A_2 \otimes E_8$ has no roots. Thus,

$$(V_{M+N})_1 = span_{\mathbb{C}}\{h(-1) \cdot \mathbb{1} \mid h \in (M+N) \otimes_{\mathbb{Z}} \mathbb{C}\}.$$

However,

$$\Omega_1 h(-1) \cdot \mathbb{1} = \left(\omega_E + \frac{3}{4}\omega_{M+N} - \frac{1}{12} \sum_{\substack{\alpha \in K(2) \\ 1 \leq i,j \leq 3, i \neq j}} e^{\iota_i(\alpha) - \iota_j(\alpha)}\right)_1 h(-1) \cdot \mathbb{1} = \frac{3}{4} h(-1) \cdot \mathbb{1} \neq 0$$

for any $0 \neq h \in (M+N) \otimes_{\mathbb{Z}} \mathbb{C}$. Thus, $\left(\mathrm{Com}_{V_L}(L_{\widehat{sl}_9(\mathbb{C})}(3,0))\right) \cap (V_{M+N})_1 = 0$ and we have $W_1 = 0$. ∎

Remark 3.5. By using a theorem of Dong and Wang [DW], it is also possible to show that $W = \mathrm{Com}_{V_L}\left(L_{\widehat{sl}_9(\mathbb{C})}(3,0)\right)$, which is an extension of the parafermion vertex operator algebra $K_{sl_3}(9,0)$.

References

[CL] H. Y. Chen and C. H. Lam, A Majoranna representation of the group 3^2:2 of $3C$-pure type and the corresponding vertex operator algebra, in preparation.

[DL] C. Dong and J. Lepowsky, Generalized vertex algebras and relative vertex operators, Progress in Math. **112**, Birkhäuser, Boston, 1993.

[DMZ] C. Y. Dong, G. Mason, and Y. Zhu, Discrete series of the Virasoro algebra and the Moonshine module, *Proceedings of Symposia in Pure Mathematics* **56** *Part 2* (1994) 295-316.

[DW] C. Dong and Q. Wang, The structure of parafermion vertex operator algebras: general case, *Commun. Math. Phys.* **299** (2010), 783–792.

[FLM] I. Frenkel, J. Lepowsky, and A. Meurman, Vertex operator algebras and the Monster, *Academic Press, New York*, 1988.

[FZ] Igor B. Frenkel, and Y. C. Zhu, Vertex operator algebras associated to representations of affine and Virasoro algebras, *Duke Mathematical Journal* **66** (1992) 123-168.

[GL] R.L. Griess and C. H. Lam, EE_8 lattices and dihedral groups, Pure and Applied Math Quarterly (special issue for Jacques Tits), **7** (2011), no. 3, 621-743. `arXiv:0806.2753`.

[LYY1] C. H. Lam, H. Yamada, H. Yamauchi, Vertex operator algebras, extended E_8 diagram, and McKay's observation on the Monster simple group, *Transactions of the American Mathematical Society* **359** (2007) 4107-4123.

[LYY2] C.H. Lam, H. Yamada and H. 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.

[Mi] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *Journal of Algebra* **179** (1996) 523-548.

[Sa] S. Sakuma, 6-transposition property of τ-involutions of vertex operator algebras, *International Mathematics Research Notices* **2007**, Article ID rnm 030, 19 pages.

Institute of Mathematics, Academia Sinica, Taipei 10617, Taiwan and National Center for Theoretical Sciences, Taiwan

E-mail address: `chlam@math.sinica.edu.tw`

On the existence of extremal Type II $\mathbb{Z}_{2k}$-codes

三枝崎 剛 Tsuyoshi Miezaki *

この原稿は，2012年6月18日の第20回代数的組合せ論シンポジウム（弘前大学）の三枝崎による上の題での講演の記録です．原田昌晃氏（山形大学）とのプレプリント（Math. Comp. に掲載予定）に基づいています．

1 導入

n次元自己双対格子Lのn個のベクトルの組$\{f_1, \ldots, f_n\}$がk-frameを成すとは，$(f_i, f_j) = k\delta_{i,j}$ を満たす事である．ここで，$\delta_{i,j}$ はクロネッカーのデルタ．k-frameの理論は，$\mathbb{Z}_{2k}$-符号の存在問題や頂点作用素代数とも関係し，多方面から興味を持たれてきた．特に，偶な自己双対格子で extremal な格子に対する k-frame の存在問題は最も興味深いといえよう．その様な格子でもっとも興味深い例の一つである Leech 格子については，任意の正整数 k に対して，$2k$-frameの存在がわかっており ([1, 3])，更に2010年のRIMSの研究集会にて，宗政昭弘氏（東北大学）により，4-frameの集合は自己同型群の作用を除いて分類されたとの報告があった．

さて，k-frameの存在を決める際，強力な道具が2つある：

補題 1.1 (Chapman [1, Lemma 5.1])**.** $n \equiv 0 \pmod 4$ とする．n-次元格子 L が k-frame を持てば，任意の正整数 m に対し km-frame を持つ．

これにより，全ての k でなく，素数 p に対し p-frame の存在を示せば良いことになる．更に，

補題 1.2 ([1, 5])**.** 自己双対格子 L が k-frame をもつ事は，$A_k(C) \cong L$ なる $\mathbb{Z}_k$-符号 C の存在と同値である．ここで，$A_k(C)$ は $\mathbb{Z}_k$-符号 C から構成法 A で得られた格子とする．

偶な自己双対格子の minimum norm は，

$$2\lfloor \frac{n}{24} \rfloor + 2$$

でえられる事により，次を得る：

補題 1.3. $n \leq 136$ かつ $k \geq \lfloor n/24 \rfloor + 1$ とする．その時，n 次元の偶で自己双対な extremal 格子 L が $2k$-frame を持つことと，長さ n の extremal Type II $\mathbb{Z}_{2k}$-符号の存在は同値である．

*Department of Mathematics, Oita National College of Technology, 1666 Oaza-Maki, Oita, 870–0152, Japan. email: miezaki@oita-ct.ac.jp

以下, extremal な自己双対格子を考える. 8 次元の E_8-格子を考えよう. $\tilde{H}_8$ を長さ 8 の拡大ハミング $\mathbb{Z}_2$-符号とすると, $E_8 = A_2(\tilde{H}_8)$ より, 補題 1.2 を用いて 2-frame の存在が分かる. 更に, 補題 1.1 より, 全ての正整数 k に対して, $2k$-frame の存在及び長さ 8 の extremal Type II $\mathbb{Z}_{2k}$-符号の存在がわかる. 16 次元の格子 $E_8 \oplus E_8$, D_{16}^+ に対しても, 何れも $\mathbb{Z}_2$-符号から構成法 A で得られる事から, E_8 と同様の考察で, $2k$-frame の存在及び長さ 16 の extremal Type II $\mathbb{Z}_{2k}$-符号の存在がわかる.

さて, 24 次元 Leech 格子 Λ_{24} である. Λ_{24} は, ノルム 2 の元がない事により, $\mathbb{Z}_2$-符号から構成法 A で得られない. しかし, Chapman は McKay による Λ_{24} の構成法を用い, $k \neq 11^r$ に対し, $2k$-frame の存在を示した. その後, Gulliver–Harada によって, extremal Type II $\mathbb{Z}_{22}$-符号が構成され, 全ての正整数 k に対し, $2k$-frame の存在, 長さ 24 の extremal Type II $\mathbb{Z}_{2k}$-符号の存在がわかった.

以下では, Section 2 において, Λ_{24} における Chapman の議論を紹介する. そして, Section 3 で主結果の一部である, 長さ 48 の extremal Type II $\mathbb{Z}_{2k}$-符号の存在を示す.

2 Chapman の議論

この節では, Chapman の議論を復習する. 詳細は, [1] を参照されたい.

行列 S を以下で定義する :

$$S = \begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & A & \\ -1 & & & \end{pmatrix},$$

ここで, A は巡回行列で最初の行は

$$(0, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1).$$

法 11 に関し, 平方剰余である所に 1 を並べたものである. C を, 次の生成行列 $M = (I_{12}, 2I_{12} + S)$ を持つ長さ 24 の $\mathbb{Z}_4$-符号とする. すると, $A_4(C) \simeq \Lambda_{24}$. これが McKay による Leech 格子の構成である.

$S^T = -S$, $S^2 = -11I$ である事により, $c \equiv 2a + b \pmod 4$ かつ $d \equiv a + 2b \pmod 4$, に対して,

$$P = \begin{pmatrix} aI + bS & cI + dS \\ -cI + dS & aI - bS \end{pmatrix}$$

は, すべて Leech 格子の元となる. 更に $PP^T = (a^2 + 11b^2 + c^2 + 11d^2)I_{24}$, なので, Leech 格子は, $k = (a^2 + 11b^2 + c^2 + 11d^2)/4$ に対し k-frame を持つ事がわかった. つまり素数 p に対し, 条件

$$c \equiv 2a + b \pmod 4 \text{ かつ } d \equiv a + 2b \pmod 4 \tag{1}$$

で

$$2p = (a^2 + 11b^2 + c^2 + 11d^2)/4 \tag{2}$$

を満たすような a,b,c,d が存在すれば，Leech 格子は，$2p$-frame を持つことになる．Chapman は，重さ 2 のモジュラー形式を用いる事により，$p \neq 11$ に対しては，a,b,c,d の存在を決定した．証明の概略を説明しよう．条件 (1) を満たす a,b,c,d 及び (2) から誘導される内積をもつ格子のテータ級数 $(\sum_{m=0}^{\infty} a(m)q^m)$ は，重さ 2 の群 $\Gamma_0(11)$ に関するモジュラー形式になる．すると，重さ 2 のアイゼンシュタイン級数 $E_2(z) = 1 - 24\sum_{m=1}\sigma_1(m)q^m$ 及び群 $\Gamma_0(11)$ に関する唯一のカスプ形式

$$\eta(z)^2\eta(11z)^2 = \sum_{m=1}^{\infty} b(m)q^m$$

を用いてテータ級数を表示すると，$p \neq 11$ に対し，

$$a(p) = p + 1 - b(p)$$

と書ける事がわかる．$\eta(z)^2\eta(11z)^2$ は，Hecke eigen form なので，Deligne の結果から $b(p) < 2\sqrt{p}$ を満たし，$a(p) = p + 1 - b(p) > p + 1 - 2\sqrt{p} = (\sqrt{p} - 1)^2 > 0$ となる．

Gulliver–Harada の結果と合わせて，任意の正整数 k に対し Leech 格子の $2k$-frame の存在及び長さ 24 の extremal Type II $\mathbb{Z}_{2k}$-符号の存在がわかったのである．

3　48 次元

24×24 $(0, \pm 1)$-行列 W を以下で定める：

$$\begin{pmatrix} 0 & 1 & \cdots & 1 \\ -1 & & & \\ \vdots & & A & \\ -1 & & & \end{pmatrix},$$

ここで，A は巡回行列で最初の行は

$$(0,1,1,1,1,-1,1,-1,1,1,-1,-1,1,1,-1,-1,1,-1,1,-1,-1,-1,-1).$$

法23に関し，平方剰余である所に1を並べたものである．C を，次の生成行列 $M = (I_{24}, S)$ を持つ長さ 24 の $\mathbb{Z}_3$-符号とする．格子 $A_3(C)$ を考えよう．$W^T = W$，$W^2 = -23W$ である事により，$a \equiv d \pmod 3$ かつ $b \equiv c \pmod 3$，に対して，

$$P = \begin{pmatrix} aI + bS & cI + dS \\ -cI + dS & aI - bS \end{pmatrix}$$

は，すべて $A_3(C)$ 格子の元となる．更に $PP^T = (a^2 + 23b^2 + c^2 + 23d^2)I_{24}$, なので，$A_3(C)$ は，$k = (a^2 + 23b^2 + c^2 + 23d^2)/3$ に対し k-frame を持つ事がわかった．つまり素数 p に対し，条件

$$a \equiv d \pmod 3 \text{ かつ } b \equiv c \pmod 3 \tag{3}$$

で

$$p = (a^2 + 23b^2 + c^2 + 23d^2)/3 \tag{4}$$

を満たすような a, b, c, d が存在すれば，$A_3(C)$ は，p-frame を持つことになる．実際，重さ 2 のモジュラー形式の議論を用いて，$p \neq 2, 5, 7, 23$ に対して，その様な a, b, c, d の存在を示した．Section 2 で述べた方法と手法は同じであるが，群が $\Gamma_0(119)$ と複雑になるため大変な計算を要する．詳しくは，論文をご覧いただきたい．

さて，48 次元格子は，$P_{48p}, P_{48q}, P_{48n}$ と 3 つ知られているが，実は，$A_3(C)$ の 1 つの偶で自己双対な neighbor が P_{48p} と同型である ([2])．$A_3(C)$ の $2k$-frame は，明らかに偶で自己双対な neighbor に含まれる．従って，$k \neq 2^{m_1}5^{m_2}7^{m_3}23^{m_4}$ に対して，P_{48p} の $2k$-frame の存在がわかり，長さ 48 の extremal Type II $\mathbb{Z}_{2k}$-符号の存在がわかった．さて，現在まで，$1 \leq k \leq 6$ に対して，extremal Type II $\mathbb{Z}_{2k}$-符号の存在はわかっている．今回，$k = 14, 46$ に対しても，extremal Type II $\mathbb{Z}_{2k}$-符号 $(C_{14,48}, C_{46,48})$ を構成し，従って，全ての正整数 k に対し，extremal Type II $\mathbb{Z}_{2k}$-符号の存在がわかった．

注意 3.1. 講演では，新たに構成した 2 つの符号 $C_{14,48}, C_{46,48}$ が，知られている 3 つの格子と同型かどうかわかっていないと紹介したが，その後 Nebe 氏より，それぞれ P_{48n}, P_{48p} と同型である事がわかったとの連絡を受けた．(詳細な証明も受け取った．) 3 つの偶で自己双対な extremal 格子の全自己同型群も決定し，それを用い具体的に同型写像を与えたとの事である．なお，Nebe 氏により構成された 72 次元の偶で自己双対な extremal 格子の全自己同型群も決定したとの事である．

注意 3.2. $k \geq 3$ に対して P_{48p} の $2k$-frame の存在を決める事は，興味ある問題である．

参考文献

[1] R. Chapman, Double circulant constructions of the Leech lattice, *J. Austral. Math. Soc. Ser. A* **69** (2000), 287–297.

[2] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups (3rd ed.)*, Springer-Verlag, New York, 1999.

[3] T.A. Gulliver and M. Harada, Orthogonal frames in the Leech lattice and a Type II code over $\mathbb{Z}_{22}$, *J. Combin. Theory Ser. A* **95** (2001), 185–188.

[4] M. Harada and T. Miezaki, On the existence of extremal Type II $\mathbb{Z}_{2k}$-codes, submitted.

[5] M. Harada, A. Munemasa and B. Venkov, Classification of ternary extremal self-dual codes of length 28, *Math. Comp.* **78** (2009), 1787–1796.

有向グラフと複素球面上のコード

野崎寛
愛知教育大学数学教育講座
hnozaki@auecc.aichi-edu.ac.jp

1 はじめに

ユークリッド空間 $\mathbb{R}^d$ 上の有限集合 X に対して，

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

と定義する．ここで，$d(x,y)$ は通常のユークリッド距離を表している．$D(X)$ の元の個数が s であるとき，集合 X は s-距離集合と呼ばれる．s-距離集合の主な問題のひとつが，距離の個数 s，次元 d を固定して，出来るだけ元の個数の大きい s-距離集合を構成することである．特に 1 つの球面にのる s-距離集合は，球面デザインやアソシエーションスキームと深く関連する重要な対象である [2].

ここでは特に 2-距離集合を考える．2-距離集合から，短いほうの距離を持つ 2 頂点を辺で結ぶことにより，グラフの構造が自然に得られる．では，グラフを先に与えた場合，どの様に，そのグラフ構造を持つ 2-距離集合を与えることが出来るだろうか？与えられた単純グラフの構造を持つ 2-距離集合を，そのグラフの埋め込みと呼んでいる．n 頂点の単純グラフを与えたときに，$n-2$ 次元以下の空間への埋め込みが唯一存在することが知られる [3]．この $n-2$ 次元以下の空間への埋め込みのことを極小埋め込みと呼ぶことにする．一方 $n-1$ 次元の埋め込みは無数に存在している．このことから，d 次元 $d+2$ 頂点以上の 2-距離集合と単純グラフが 1 対 1 に対応していることが分かる．2-距離集合の議論が，有限個のグラフの議論に落ちている．グラフの分類を用いることで，7 次元までの最大 2-距離集合の分類は完了している [4]．また，極小埋め込みの次元と $D(X)$ の元に関しては，隣接行列の固有空間の情報で，簡明な記述が Roy により与えられている [9]．また，グラフの 2-距離集合としての埋め込みの次元に関しては，Maehara の [5] などの文献もある．一般の s-距離集合について，同様の議論を行いたいが，そこには大きなギャップが存在していて，現在のところ上手くいっていない．

上に述べたような，単純グラフと 2-距離集合の関係を，複素空間 $\mathbb{C}^d$ における球面上の集合と有向グラフとの関係に応用したいというのが，ここでの目標である．複素球面上の集合を考える意義は，最近の Roy，Suda [10] の仕事による部分が大きい．Roy，Suda [10] は，Delsarte–Goethals–Seidel [2] が示したユークリッド空間上のデザイン，コード，アソシエーションスキームの理論を，複素球面上において確立させた．複素球面上における，その理論は実球面上の理論よりも若干複雑ではあるが，コードとして重要であるのが複素球

面 s-コードであると言ってよい．複素球面 s-コードとは，まさに s-距離集合の複素球面版であり，異なる二点間の通常の複素内積の個数が s であるときに，そう呼ばれる．

この稿での目標は，[7] に記した結果の一部である，有向グラフの複素球面上への埋め込み理論と，最大複素球面 2, 3-コードの分類の紹介である．また，最大複素球面 2-コードを分類するにあたって，歪アダマール行列の部分行列の固有値の情報からの特徴づけにも成功した．歪アダマール行列の特徴づけについては，Linear algebra and its application に掲載済みである [6].

2　定義と諸結果

ここでは，後に必要となる定義と既存の結果について紹介したい．$u = (u_1 \dots u_d)^T, v = (v_1 \dots v_d)^T \in \mathbb{C}^d$ に対して，

$$u^* v := \sum_{k=1}^{d} \overline{u_k} v_k$$

とする．ここで，$\overline{a}$ は a の複素共役を意味する．$\Omega(d)$ と書いて，複素球面を意味する．つまり

$$\Omega(d) := \{x \in C^d \mid x^* x = 1\}$$

である．$\Omega(d)$ 上の二つの部分集合がユニタリ変換で写りあうとき，二つの集合は同型であるという．有限集合 $X \subset \Omega(d)$ に対して，

$$D(X) := \{u^* v \mid u, v \in X, u \neq v\}$$

と定義する．$D(X)$ の元の個数が s，つまり $|D(X)| = s$ であるとき，X を複素球面 s-コード，または単に s-コードと呼ぶ．s-コードの基本的な問題のひとつは，d と s を固定したときに，出来るだけ元の個数の大きい s-コードを構成，分類することである．元の個数の大きい s-コードは，デザイン，アソシエーションスキームと密接に関係しているというのが，ひとつの動機である．この稿では，2-コード，3-コードを扱う．$u, v \in \mathbb{C}^d$ に対して，$\overline{u^* v} = v^* u$ であることに注意すれば，$\alpha \in D(X)$ のとき，$\overline{\alpha} \in D(X)$ である．よって，X が 2-コードであれば，$D(X) = \{\alpha, \overline{\alpha}\}$（$\alpha$ は虚数），3-コードであれば，$D(X) = \{\alpha, \overline{\alpha}, \beta\}$（$\alpha$ は虚数，β は実数）であることが分かる．

この稿で有向グラフ $G = (V, E)$ と言うときは，それぞれの辺は一方向の向きしか持たないと仮定する．つまり，$(x, y) \in E$ であるならば，$(y, x) \notin E$ であると仮定しておく．すべての 2 頂点間に辺を持つ有向グラフをトーナメントと呼ぶ。G の隣接行列 A とは，V で添え字付けられる行列で，その (x, y) 成分は

$$A_{xy} = \begin{cases} 1, \ (x, y) \in E \text{ のとき}, \\ 0, \ \text{その他} \end{cases}$$

と定義される．有向グラフ $G = (V, E)$ に対して，

$$\varphi(u)^* \varphi(v) = \begin{cases} \alpha, \ (u, v) \in E \text{ のとき}, \\ \overline{\alpha}, \ (v, u) \in E \text{ のとき}, \\ \beta, \ \text{その他} \end{cases}$$

を満たす，V から $\Omega(d)$ への単射 φ，虚部が正の $\alpha \in \mathbb{C}$, 実数 β が存在するとき，$\varphi(V)$ を G の複素球面埋め込み，または単に埋め込みと呼ぶ．トーナメントの埋め込みは 2-コードとなり，トーナメントでない有向グラフの埋め込みは 3-コードとなる．逆の操作を行うことで，2-コード，3-コードから容易に有向グラフの構造が得られる．また，2,3-コードが同型であれば，得られる有向グラフも同型であり，非同型な二つの有向グラフからは，同型なコードが得られないことも直ちに分かる．

与えられた有向グラフから，非同型な $2,3$-コードが得られる可能性があるが，ここでは，複素空間の次元が極小となる埋め込み（極小埋め込み）を考えたい．次元が小さければ小さいほど，次元に対して元の個数が大きくなり，s-コードとして良いものであると言うことが出来る．

トーナメントの中でも，特に重要である二重正則トーナメントを紹介する．トーナメント (V, E) に対して，ある自然数 m_1, m_2 が存在して，全ての頂点 x に対して，

$$|\{y \in V \mid (x, y) \in E\}| = m_1,$$

また，全ての異なる 2 頂点 x, y に対して，

$$|\{z \in V \mid (x, z), (y, z) \in E\}| = m_2$$

を満たすとき，二重正則トーナメントであると呼ばれる．特に最初の条件を満たすトーナメントは正則であると呼ばれる．二重正則トーナメントの存在性と歪アダマール行列の存在性が同値であることは良く知られている．

Theorem 2.1 ([8])**.** n 頂点の二重正則トーナメントが存在することと，サイズが $n+1$ の歪アダマール行列が存在することが同値である．

二重正則トーナメントの隣接行列を A とし，I を単位行列，j を成分が全て 1 のベクトルとする．そのとき，

$$\begin{bmatrix} 1 & j^T \\ -j & I + A - A^T \end{bmatrix}$$

は歪アダマール行列となる．また逆の操作により，第一行の成分を 1 に正規化した歪アダマール行列から二重正則トーナメントの構造を得ることが出来る．

3 最大複素 $2,3$-コード

有向グラフ G の隣接行列を A とし，J を全て成分が 1 の正方行列，I を単位行列とする．また，行列 B を次で定義する：

$$B := J - I - A - A^T.$$

そのとき，G の複素球面埋め込みのグラム行列は，

$$M = I + a(A + A^T) + \sqrt{-1}b(A - A^T) + cB \tag{3.1}$$

とかける．ここで a,b,c は実数である．ここでは，次元が極小となる複素球面埋め込みを与えたいので，(3.1) の格好をした M が正定値で，ランクが極小となる $a,b,c \in \mathbb{R}$ を見つければよい．複素球面 2-コードの場合は $B=0$ となり，二つの変数 a,b で済むことになる．2-コードの場合は，行列 $S := \sqrt{-1}(A-A^T)$ のある種素直な固有空間の解析により，極小次元を与える a,b を決定できる．S は Seidel 行列と呼ばれている．ところが，変数が 1 つ増えると，同様の議論が全く働かなくなる．しかし，最大複素球面 3-コードを与えるアルゴリズムを与えることには成功した．非常に煩雑であり，多くの補題を必要とするため，この報告集では割愛する．[7] を参照されたい．

トーナメントの複素球面埋め込み，つまり 2-コードとしての埋め込みの極小次元を与える定理を紹介する前に，いくつか記号を用意する．T を n 頂点トーナメントとし，A をその隣接行列とする．S を Seidel 行列とし，τ_i を i 番目に小さい S の異なる固有値とする．P_i を τ_i の固有空間への直交射影行列とする．β_i を次で定義し，main angle と呼ぶ．

$$\beta_i := \frac{1}{\sqrt{n}}\sqrt{(P_i \cdot j)^*(P_i \cdot j)}.$$

次の定理が，トーナメントの複素球面埋め込みに対する極小次元を表すものである．

Theorem 3.1 ([7])**.** $\mathrm{Rep}(T)$ を複素球面埋め込みの極小次元であるとする．また α をその埋め込みが持つ内積の値であるとする．そのとき，次が成立する．

(1) $\beta_1 = 0$ ならば, $\mathrm{Rep}(T) = n - m_1 - 1$ かつ $\alpha = (1/c_1 - \sqrt{-1})/\tau_1$ が成立．ここで $c_1 = \sum_{i=2}^{s} n\beta_i^2/(\tau_i - \tau_1)$.

(2) $\beta_1 \neq 0$ かつ $m_1 > 1$ のとき, $\mathrm{Rep}(T) = n - m_1$ かつ $\alpha = -\sqrt{-1}/\tau_1$ が成立.

(3) $m_1 = 1$, $\beta_2 = 0$, かつ $c_2 < 0$ ならば, $\mathrm{Rep}(T) = n - m_2 - 1$ かつ $\alpha = (1/c_2 - \sqrt{-1})/\tau_2$ が成立．ここで $c_2 = n\beta_1^2/(\tau_1 - \tau_2) + \sum_{i=3}^{s} n\beta_i^2/(\tau_i - \tau_2)$.

(4) それ以外のとき $\mathrm{Rep}(T) = n - 1$.

特に Theorem 3.1 の (1), (2), (3) においては，極小次元の埋め込みは一意的に定まることに注意されたい．その埋め込みを極小埋め込みと呼ぶ．Theorem 3.1 の (i) の条件たちは，disjoint であり，(i) の条件を満たすトーナメントをタイプ (i) のトーナメントと呼ぶ．複素球面 2-コードの元の個数には次の自然な上界（Fisher type）が知られている．

Theorem 3.2 ([10])**.** X を複素球面 $\Omega(d)$ 上の 2-コードであるとする．そのとき，

$$|X| \leq \begin{cases} 2d+1, & d \text{ が奇数のとき}, \\ 2d, & 2d \text{ が偶数のとき}, \end{cases} \tag{3.2}$$

が成立する．

Theorem 3.1 と，さらに固有値の解析を行うことで，Fisher type の上界を達成する複素球面 2-コードの特徴づけに成功した．

Theorem 3.3. X をトーナメント T の極小埋め込みであるとする．A を T の隣接行列であるとする．そのとき次が成立する．

(1) d が奇数のとき，X が (3.2) の等式を達成することと，T が二重正則トーナメントであることが同値．

(2) d が偶数のとき，X が (3.2) の等式を達成することと，$I + A - A^T$ が歪アダマール行列であることが同値．

二重正則トーナメントと歪アダマール行列の存在性が同値であることは前に述べたから，Fisher type の上界を達成する 2-コードの存在性は二重正則トーナメントの存在性と一致することが示された．二重正則トーナメントの分類が完了している次元については，最大 2-コードを分類することが可能である．特に，非同型な最大 2-コードの個数は Magma などを用いれば，[1] の数え上げの手法を用いて計算することができる．最大 2-コードの個数を $N(d)$ とする．

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\|X\|$	3	4	7	8	11	12	15	16	19	20	23	24	27	28
$N(d)$	1	2	1	4	1	8	2	240	2	8956	37	11339044	722	9897616700

最大複素球面 3-コードについては，Theorem 3.1 と同様の結果を得ることが難しいため，状況はかなり複雑である．次が，複素球面 3-コードにおける Fisher 型の上界である．

Theorem 3.4 ([10])**.** X を複素球面 $\Omega(d)$ 上の 3-コードであるとする．そのとき，

$$|X| \leq \begin{cases} 4, & d = 1 \text{ のとき}, \\ d^2 + 2d, & d \geq 2 \text{ のとき}, \end{cases} \tag{3.3}$$

が成立する．

上の上界は自然なもので，それを達成する 3-コードはアソシエーションスキームの構造を持つことが示され [10]，その分類問題は非常に重要な課題であった．付随するアソシエーションスキームの性質を用いて，等式を達成する 3-コードを分類することに成功した．

Theorem 3.5 ([7])**.** $X \subset \Omega(d)$ を (3.3) を達成する 3-コードであるとする．そのとき次が成立．

(1) $d = 1$ かつ $D(X) = \{\pm\sqrt{-1}, -1\}$,

(2) $d = 2$ かつ $D(X) = \{\pm\sqrt{-1/3}, -1\}$,

(3) $d \geq 3$ のとき非存在．

証明の方針は，Fisher 型の上界を満たす 3-コードはアソシエーションスキームの構造を持つため，そのアソシエーションスキームのパラメータから非存在を示す．Theorem 3.1 と同様の定理を 3-コードについて与えるのは難しいが，特に次元に対して元の個数の大きい 3-コードを与える有向グラフについては，埋め込みを与えるアルゴリズムを与えること

が可能である．特に良い性質を持つ有向グラフを分類することで，最大複素球面 3-コードを分類することができる．しかし，それには $2d$ 次元以下の実球面 2-距離集合の分類が必要であるため，$d \leq 3$ についてしか，現在のところ分類が成功していない．次にその表を与える．$N(d)$ が最大複素球面 3-コードの非同型なものの個数である [7].

d	1	2	3
$\lvert X\rvert$	4	8	9
$N(d)$	1	1	35

$d = 1$ のとき，最大 3-コードは正方形の頂点集合．$d = 2$ のとき，Y をサイズ 4 の歪アダマール行列（一意的）の極小埋め込みとし，$Y \cup (-Y)$ が最大 3-コード．$d = 1, 2$ のときは Fisher 型の上界を達成している．$d = 3$ のとき，最大 3-コードの 1 つは，サイズ 3 の正則トーナメントを 3 つ disjoint union させたもの，残りの 34 個は 6 次元最大実 2-距離集合の部分構造から得られる．

4　歪アダマール行列の特徴づけ

サイズ $n+1$ の歪アダマール行列と，n 頂点二重正則トーナメントの存在性が同値であることは先に述べた．これは，正規化された歪アダマール行列が，その部分構造により特徴付けられていることに他ならない．サイズ $n+1$ の歪アダマール行列から得られるトーナメント構造 T_1，n 頂点二重正則トーナメントを T_2 とすると，そのスペクトラムなどの情報は次のように書くことが出来る．

	$\tau_i^{m_i}$	β_i	type	$\mathrm{Rep}(T_i)$
T_1	$\{(-\sqrt{n})^{\frac{n+1}{2}}, (\sqrt{n})^{\frac{n+1}{2}}\}$	$(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$	(2)	$\frac{n+1}{2}$
T_2	$\{(-\sqrt{n})^{\frac{n-1}{2}}, 0^1, \sqrt{n}^{\frac{n-1}{2}}\}$	$(0, 1, 0)$	(1)	$\frac{n-1}{2}$

逆に，上記の様なスペクトラム，main angle を持つトーナメントは，歪アダマール行列，二重正則トーナメントと特徴付けることが出来る．今，T_1 から 1 頂点除いた T_2 に対して，スペクトラムからの特徴づけが出来たのであるが，さらに T_2 から，勝手に 1 頂点を除いた T_3 を考える．勝手に 1 頂点を除くために，どの頂点を除くかに依って，T_3 はトーナメントとしての構造が異なってくる．しかし，スペクトラムなどの情報は，どの頂点を除いても以下のようになることが分かる．

	$\tau_i^{m_i}$	β_i	type	$\mathrm{Rep}(T_i)$
T_3	$\{(-\sqrt{n})^{\frac{n-3}{2}}, (-1)^1, 1^1, \sqrt{n}^{\frac{n-3}{2}}\}$	$(0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0)$	(1)	$\frac{n-1}{2}$

逆にこのスペクトラムを持つトーナメントはどの様に特徴付けられるだろうかというのが，ここでの視点である．実際に，このスペクトラムをもつトーナメントは必ず二重正則トーナメントの部分構造を持つことが示された．つまり，このスペクトラムをもつ T_3 を構成することで，二重正則トーナメント，歪アダマール行列を構成することが出来る．正規化された歪アダマール行列から 2 頂点を除いた部分トーナメントのスペクトラムの情報から，歪アダマール行列を特徴付けることに成功した．

Theorem 4.1 ([6])**.** サイズ $n+1$ の歪アダマール行列の存在性と以下のスペクトラムを持つ $n-1$ 頂点トーナメントの存在性が同値である：

$$\{(-\sqrt{n})^{\frac{n-3}{2}}, (-1)^1, 1^1, \sqrt{n}^{\frac{n-3}{2}}\}, (\beta_i)_{i=1}^4 = (0, \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0).$$

References

[1] L. Babai and P.J. Cameron, Automorphisms and enumeration of switching classes of tournaments, *Electron. J. Combin.* 7 (2000), Research Paper 38, 25 pages.

[2] P. Delsarte, J.M. Goethals, and J.J. Seidel, Spherical codes and designs, *Geom. Dedicata* 6 (1977), no. 3, 363–388.

[3] S.J. Einhorn and I.J. Schoenberg, On euclidean sets having only two distances between points. I. II. *Nederl. Akad. Wetensch. Proc. Ser. A* 69=*Indag. Math.* 28 (1966), 479–488, 489–504.

[4] P. Lisoněk, New maximal two-distance sets, *J. Combin. Theory, Ser. A* 77 (1997), 318–338.

[5] H. Maehara, Regular embeddings of a graph, *Pacific J. Math.* 107 (1983), no. 2, 393–402.

[6] H. Nozaki and S. Suda, A characterization of skew Hadamard matrices and doubly regular tournaments, *Linear Algebra Appl.* 437 (3) (2012) 1050–1056.

[7] H. Nozaki and S. Suda Complex spherical codes with small degree, preprint.

[8] K.B. Reid, E. Brown, Doubly regular tournaments are equivalent to skew Hadamard matrices, *J. Combin. Theory, Ser. A*, 12 (1972), 332–338.

[9] A. Roy, Minimal Euclidean representation of graphs, *Discrete math.* 310 (2010), 727–733.

[10] A. Roy and S. Suda, Complex spherical designs and codes, preprint, arXiv:1104.4692.

Hiroshi Nozaki
Department of Mathematics,
Aichi University of Education
1 Hirosawa, Igaya-cho,
Kariya, Aichi 448-8542,
Japan.
hnozaki@auecc.aichi-edu.ac.jp

丹原関手に関する注意

山形大学・理学部 小田文仁 (Fumihito Oda)

1 はじめに

G を有限群とする．Dress が導入した Mackey 関手は，有限 G-集合の圏からアーベル圏への二つの関手である [Dr73]. それは，有限群の表現論における制限写像を一般化した反変関手 M^* と誘導写像の一般化である共変関手 $M_!$ の組 $M = (M_!, M^*)$ であった．Tambara は，Mackey 関手の公理に，[Dr71] で紹介され [DS88]，[DS89] 等で論じられた乗法的誘導写像もその枠組みに取り入れた TNR-関手 $T = (T_!, T^*, T_\star)$ を紹介した [Ta93]. Brun はそれを Tambara functor と呼んだ [Br05]. 本稿では特に Burnside Tambara functor $\Omega = (\Omega_!, \Omega^*, \Omega_\star)$ について $\Omega_\star$ が導出する多項式について論じる．

G-集合はすべて有限とする．G-集合と G-写像の圏を $\mathbf{set}^G$ と書く．有限集合 X の要素の個数を $|X|$ と書く．G-集合 X の同型類を $[X]$ と書く．G のすべての部分群の集合を s_G，その G-共役類の集合を $[s_G]$ と書く．H が G の部分群であるとき，$H \leq G$ と書く．G の単位元を e，また，自明な部分群 $\{e\}$ も e と書く．剰余類 G/H の要素を gH，ただし，$g \in G$ と書く．

2 Exponential diagrams

$f : X \longrightarrow Y$ を G-写像とする．G-写像 $\alpha : A \longrightarrow X$ に対し集合

$$\Pi_f(A) \;=\; \left\{ (y,\sigma) \;\middle|\; \begin{array}{l} y \in Y,\, \sigma : f^{-1}(y) \longrightarrow A :\ \text{map}\ , \\ \alpha \circ \sigma = \mathrm{id}_{f^{-1}(y)} \end{array} \right\}$$

に G-作用を

$$g(y,\sigma) := (gy, {}^g\sigma), \quad {}^g\sigma(x) := g\sigma(g^{-1}x).$$

で定め，$\Pi_f(A)$ から Y への射影 $(y,\sigma) \mapsto y$ を $\Pi_f\alpha$ と書く．G-写像 $\alpha : A \longrightarrow X$ に対し pullback functor

$$\begin{array}{rccc} f^* & : & \mathbf{set}^G/Y & \longrightarrow & \mathbf{set}^G/X, \\ & & (B \longrightarrow Y) & \longmapsto & (X \times_Y B \xrightarrow{\mathrm{pr}} X) \end{array}$$

は左随伴関手

$$\begin{array}{rccc} \Sigma_f & : & \mathbf{set}^G/X & \longrightarrow & \mathbf{set}^G/Y, \\ & & (A \xrightarrow{\alpha} X) & \longmapsto & (A \xrightarrow{\alpha} X \xrightarrow{f} Y) \end{array}$$

と右随伴関手

$$\begin{array}{rccc} \Pi_f & : & \mathbf{set}^G/X & \longrightarrow & \mathbf{set}^G/Y, \\ & & (A\xrightarrow{\alpha}X) & \longmapsto & (\Pi_f(A)\xrightarrow{\Pi_f\alpha}Y) \end{array}$$

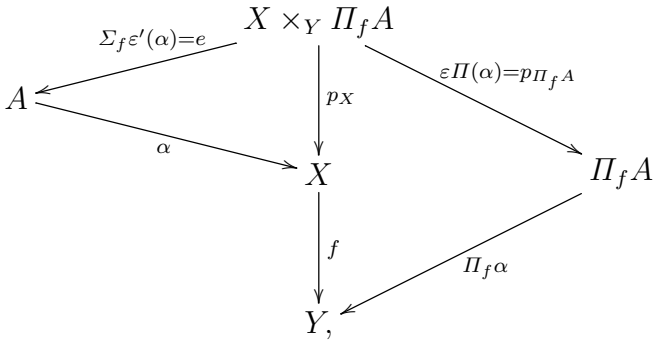
をもつ．二つの自然変換

$$\Sigma_f \xleftarrow{\Sigma_f\varepsilon'} \Sigma_f f^*\Pi_f \xrightarrow{\varepsilon\Sigma_f} \Pi_f,$$

(ただし，ε' は随伴 $f^* \dashv \Pi_f$ の余単位射，ε は随伴 $\Sigma_f \dashv f^*$ の余単位射) は $A \xrightarrow{\alpha} X$ に対し図式

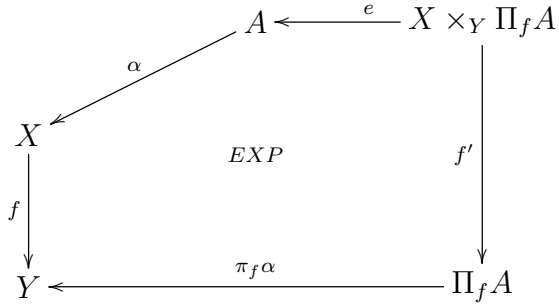
$$\Sigma_f \begin{pmatrix} A \\ \downarrow\alpha \\ X \end{pmatrix} \xleftarrow{\Sigma_f\varepsilon'(\alpha)} \Sigma_f f^*\Pi_f \begin{pmatrix} A \\ \downarrow\alpha \\ X \end{pmatrix} \xrightarrow{\varepsilon\Pi_f(\alpha)} \Pi_f \begin{pmatrix} A \\ \downarrow\alpha \\ X \end{pmatrix},$$

すなわち



$$(e : X \times_Y \Pi_f A \ni (x,(y,\sigma)) \longmapsto \sigma(x) \in A, \quad p_X,\, p_{\Pi_f A} \text{ は射影 })$$

を与える．この図式



($f' = p_{\Pi_f A}$ とする) を Tambara は exponential diagram と呼び，TNR-関手の公理化を行った．Brun はそれを丹原関手と呼んだ [Br05].

3 Tambara functors

集合と写像の圏を **Set**，二つの G-集合 X, Y の非交和を $X + Y$ と書く．
G-集合 X, Y と G-写像 $f : X \longrightarrow Y$ に対し関手の三つ組

$$\boldsymbol{T} = (\boldsymbol{T}_!, \boldsymbol{T}^*, \boldsymbol{T}_\star) : \mathbf{set}^G \longrightarrow \mathbf{Set},$$

$$\boldsymbol{T}(X) := \boldsymbol{T}_!(X) = \boldsymbol{T}^*(X) = \boldsymbol{T}_\star(X),$$

$$f_! := \boldsymbol{T}_!(f), f_\star := \boldsymbol{T}_\star(f) : \boldsymbol{T}(X) \longrightarrow \boldsymbol{T}(Y), f^* : \boldsymbol{T}(Y) \longrightarrow \boldsymbol{T}(X)$$

を考える．

三つ組 $\boldsymbol{T} = (\boldsymbol{T}_!, \boldsymbol{T}^*, \boldsymbol{T}_\star)$ は以下の条件を満たすとき *semi-Tambara functor* と呼ばれる:

(T.1) (Additivity) 任意の $\mathbf{set}^G$ の余積図式

$$X \xrightarrow{i} X + Y \xleftarrow{j} Y$$

に対し

$$\boldsymbol{T}(X) \xleftarrow{i^*} \boldsymbol{T}(X+Y) \xrightarrow{j^*} \boldsymbol{T}(Y)$$

が **Set** における積図式を与える，$\boldsymbol{T}(\emptyset) = 0 (:= \{0\})$.

(T.2) (Pullback formula)

$$\begin{array}{ccc} X & \xrightarrow{a} & Y \\ {\scriptstyle b}\downarrow & PB & \downarrow{\scriptstyle c} \\ Z & \xrightarrow[d]{} & W \end{array} \quad \Rightarrow \quad \begin{array}{ccc} \boldsymbol{T}(X) & \xrightarrow{a_!} & \boldsymbol{T}(Y) \\ {\scriptstyle b^*}\uparrow & \circlearrowright & \uparrow{\scriptstyle c^*} \\ \boldsymbol{T}(Z) & \xrightarrow[d_!]{} & \boldsymbol{T}(W), \end{array} \quad \begin{array}{ccc} \boldsymbol{T}(X) & \xrightarrow{a_\star} & \boldsymbol{T}(Y) \\ {\scriptstyle b^*}\uparrow & \circlearrowright & \uparrow{\scriptstyle c^*} \\ \boldsymbol{T}(Z) & \xrightarrow[d_\star]{} & \boldsymbol{T}(W). \end{array}$$

(T.3) (Distributive law)

$$\begin{array}{ccccc} X & \xleftarrow{a} & A & \xleftarrow{e} & X \times_Y \Pi_f A \\ {\scriptstyle f}\downarrow & & EXP & & \downarrow{\scriptstyle f'} \\ Y & & \xleftarrow[q]{} & & \Pi_f A \end{array} \quad \Rightarrow \quad \begin{array}{ccccc} \boldsymbol{T}(X) & \xleftarrow{a_!} & \boldsymbol{T}(A) & \xrightarrow{e^*} & \boldsymbol{T}(X \times_Y \Pi_f A) \\ {\scriptstyle f_\star}\downarrow & & \circlearrowright & & \downarrow{\scriptstyle f'_\star} \\ \boldsymbol{T}(Y) & & \xleftarrow[q_!]{} & & \boldsymbol{T}(\Pi_f A). \end{array}$$

すべての $\boldsymbol{T}(X)$ が可換環で $f_!, f^*, f_\star$ がそれぞれ加法群，環，乗法的モノイドの準同型であるならば，$\boldsymbol{T}$ は *Tambara functor* と呼ばれる．

4 例

二つの例を述べる．

1. Invariant ring functors

R を G-ring とする．任意の G-集合 X に対し X から R への G-写像の集合を

$$\tilde{R}(X) = \mathrm{Hom}_G(X, R)$$

とする．H が G の部分群であるならば，$\tilde{R}(G/H)$ は invariant ring R^H と同型である．G-写像 $f : X \longrightarrow Y$ は 3 つの写像を誘導する:

$$\begin{aligned} f_! &: \tilde{R}(X) \longrightarrow \tilde{R}(Y); \varphi \longmapsto f_!(\varphi)(y) = \sum_{x \in f^{-1}(y)} \varphi(x), \\ f^* &: \tilde{R}(Y) \longrightarrow \tilde{R}(X); \psi \longmapsto f^*(\psi)(x) = \psi(f(x)), \\ f_\star &: \tilde{R}(X) \longrightarrow \tilde{R}(Y); \varphi \longmapsto f_\star(\varphi)(y) = \prod_{x \in f^{-1}(y)} \varphi(x). \end{aligned}$$

このとき $\tilde{R}(X), f_!, f^*, f_\star$ は semi-Tambara functor $\tilde{R}$ を構成する．

2. Burnside functors.

任意の G-集合 X に対し $\Omega_+(X)$ を X 上の G-集合の同型類 $[A \longrightarrow X]$ 全体の集合とする．このとき $\Omega_+(X)$ はコンマ圏 G-**set**$/X$ の coproducts と products に関する半環である．G-写像 $f : X \longrightarrow Y$ は 3 つの写像を誘導する:

$$\begin{aligned} f_! &: \Omega_+(X) \longrightarrow \Omega_+(Y); [A \xrightarrow{\alpha} X] \longmapsto [A \xrightarrow{\alpha} X \xrightarrow{f} Y], \\ f^* &: \Omega_+(Y) \longrightarrow \Omega_+(X); [B \longrightarrow Y] \longmapsto [X \times_Y B \xrightarrow{p_X} X], \\ f_\star &: \Omega_+(X) \longrightarrow \Omega_+(Y); [A \xrightarrow{\alpha} X] \longmapsto [\Pi_f(A) \xrightarrow{\Pi_f \alpha} Y]. \end{aligned}$$

このとき $\Omega_+(X), f_!, f^*, f_\star$ は semi-Tambara functor Ω_+ を構成する．

5 Burnside ring の乗法的誘導射

G のバーンサイド環 $\Omega(G)$ は，自由 $\mathbb{Z}$-加群基底 $\{[G/H] | H \in [s_G]\}$ をもち，積は G-集合のデカルト積から定義される．$S \in s_G$ に対し，線型形式 $\varphi_S^G : \Omega(G) \to \mathbb{Z}$ で，任意の G-集合 X に対し $\varphi_S^G([X]) = |X^S|$ を満たすものが一意的に存在する．また，φ_S^G は環準同型である．G の *mark homomorphism* は，環準同型

$$\varphi^G = \prod_{(S)\in[s_G]} \varphi_S^G : \Omega(G) \to \widetilde{\Omega}(G),$$

ただし，$\widetilde{\Omega}(G) = \prod_{(S)\in[s_G]} \mathbb{Z}$，である．

Lemma 5.1. 環準同型 φ^G は単射である．

バーンサイド環の乗法的誘導写像（テンソル誘導写像）の性質を復習する（詳細は [Yo90] を参照）．$H \leq G$ のとき, 以下のように与えられる関手

$$\mathrm{Jnd}_H^G : \mathbf{set}^H \to \mathbf{set}^G$$

が存在する：対象については

$$\mathrm{Jnd}_H^G : X \mapsto \mathrm{Map}_H(G, X),$$

ただし $\mathrm{Map}_H(G, X)$ は H-maps $\alpha : G \to X$ ですべての $h \in H$, $g \in G$ に対し $\alpha(h \cdot g) = h \cdot \alpha(g)$ を満たすもの全体とする．このとき G-作用は $(k \cdot \alpha)(g) = \alpha(gk)$，ただし $k \in G$, X は H-set とする．

Lemma 5.2. 部分群 $H \leq G$ に対し，$f : G/H \to G/G$ を標準的な全射とする．任意の G-写像 $\alpha : A \to G/H$ に対し，G-集合の同型写像

$$\Pi_f(A) \cong \mathrm{Map}_H(G, \alpha^{-1}(eH))$$

が存在する．

Proof. G/G が一点集合で f が全射なので

$$\Pi_f(A) = \{\sigma : G/H \to A \mid \sigma : \text{ map}, \alpha \circ \sigma = \mathrm{id}_{G/H}\}$$

と同一視してよい．このとき，写像 $\varphi : \Pi_f(A) \to \mathrm{Map}_H(G, \alpha^{-1}(eH))$,

$$\varphi : s \mapsto \varphi(s) : G \to \alpha^{-1}(eH) : g \mapsto gs(g^{-1}H)$$

が同型写像を与えることがわかる． □

全射 $f : G/H \to G/G$ と Burnside Tambara functor $\Omega = (\Omega_!, \Omega^*, \Omega_\star)$ について Lemma 5.2 から $\Omega_\star(f) : \Omega(G/H) \to \Omega(G/G)$ の像が

$$\Omega_\star(f)([A \xrightarrow{\alpha} G/H]) = [\mathrm{Map}_H(G, \alpha^{-1}(eH)) \to G/G]$$

となることがわかる．$q \in \mathbb{Z}$ に対し $H = e$ の場合の $\Omega_\star(f)(q[A \xrightarrow{\alpha} G/H])$ を計算することが本稿の主題であった．

部分群 $H \leq G$ と H-集合 X について $\mathrm{Jnd}_H^G(X)$ の G-集合としての構造は以下の補題を用いて計算できる．

Lemma 5.3. *H を G の部分群 X を H-集合とせよ．$S \leq G$ ならば,*

$$\varphi_S^G(\mathrm{Jnd}_H^G(X)) = \prod_{g \in [S\backslash G/H]} \varphi_{H \cap {}^g S}^H(X).$$

が成り立つ．

Lemma 5.4. *S が G の部分群, $q \in \mathbb{Z}$ であるならば,*

$$\varphi_S^G(\mathrm{Jnd}_e^G(q[e/e])) = q^{|G/S|}$$

が成り立つ．

Proof. Lemma 5.3 から,

$$\varphi_S^G(\mathrm{Jnd}_e^G(q[e/e])) = \prod_{g \in [S\backslash G/e]} \varphi_{e \cap {}^g S}^e(q[e/e]) = \prod_{g \in [S\backslash G]} q\varphi_e^e([e/e]) = \prod_{g \in [S\backslash G]} q$$

が従う． □

Gluck ([Gl81]) と Yoshida ([Yo83]) により独立に与えられた $\mathbb{Q}$-代数 $\mathbb{Q} \otimes_{\mathbb{Z}} \Omega(G)$ の $H \leq G$ に対応する原始的べき等元 e_H^G の公式は

$$e_H^G = \frac{1}{|N_G(H)|} \sum_{K \subseteq H} |K| \mu(K, H)[G/K], \tag{5.1}$$

ただし $\mu(K, H)$ は s_G の Möbius 関数の値，で与えられる．

NH (resp. WH) で，部分群 $H \leq G$ の G 内における正規化群 $N_G(H)$ (resp. 剰余群 $H_G(H)/H$) とする．$e \leq G$ と $q \in \mathbb{Z}$ に対し $q^G = \mathrm{Jnd}_e^G(q[e/e])$ とおく．

Lemma 5.5. q が整数のとき,

$$q^G = \sum_{(D)\in[s_G]} |WD|^{-1} \sum_{S\leq G} \mu(D,S) q^{|G/S|}[G/D]$$

が成り立つ.

Proof. Lemma 5.4 とべき等元公式 (5.1) より, 以下の等式が成り立つ：

$$\begin{aligned}
q^G &= \sum_{S\in[s_G]} \varphi_S^G(q^G) e_S^G \\
&= \sum_{S\in[s_G]} q^{|G/S|} |NS|^{-1} \sum_{D\leq S} |D|\mu(D,S)[G/D] \\
&= \sum_{S\leq G} (G:NS)^{-1} q^{|G/S|} |NS|^{-1} \sum_{D\leq G} |D|\mu(D,S)[G/D] \\
&= |G|^{-1} \sum_{D\leq G} |D| \left(\sum_{S\leq G} \mu(D,S) q^{|G/S|} \right) [G/D] \\
&= |G|^{-1} \sum_{D\in[s_G]} (G:ND)|D| \left(\sum_{S\leq G} \mu(D,S) q^{|G/S|} \right) [G/D] \\
&= \sum_{D\in[s_G]} |WD|^{-1} \left(\sum_{S\leq G} \mu(D,S) q^{|G/S|} \right) [G/D].
\end{aligned}$$

□

特に, q^G の $[G/D]$ における係数は整数である.

Proposition 5.6. G と有理整数 q について,

$$|WD|^{-1} \sum_{S\leq G} \mu(D,S) q^{|G/S|}$$

は有理整数, ただし $D \leq G$, である.

Lemma 5.5 を Burnside Tambara functor Ω に戻すと以下のように表される.

Proposition 5.7. G-写像 $f : G/1 \to G/G$, $q \in \mathbb{Z}$, *Burnside Tambara functor* Ω について

$$\Omega_\star(f)(q[G/e \xrightarrow{\mathrm{id}} G/e]) = \sum_{(D)\in[s_G]} |WD|^{-1} \sum_{S\leq G} \mu(D,S) q^{|G/S|}[G/D \to G/G]$$

が成り立つ.

q を変数 x に換えると, 以下のような integer-valued polynomials $f_D^G(x)$ を得る.

Theorem 5.8. 部分群 $D \leq G$ に対し

$$f_D^G(x) = \frac{1}{|WD|} \sum_{S\leq G} \mu(D,S) x^{|G/S|}$$

とおく. このとき $f_D^G(x)$ は *integer-valued polynomial* である.

6 Necklace polynomials

この節では Theorem 5.8 の多項式 $f_D^G(x)$ がネックレス多項式の一般化であることを示す．α-色のビーズを用いた長さ n の原始的（非周期的）ネックレスの個数 $M(\alpha, n)$ は，公式

$$M(\alpha, n) = \frac{1}{n}\sum_{d|n} \mu\left(\frac{n}{d}\right)\alpha^d = \frac{1}{n}\sum_{d|n} \mu(d)\,\alpha^{\frac{n}{d}},$$

ただし，μ は古典的な Möbius function，で計算されることがよく知られている (see [MR83] for instance)．それは *necklace polynomial* と呼ばれている．位数 n の巡回群を C_n で表す．G の部分群の包含関係に関するポセット $(s_G, \leq)$ を $\mathscr{S}_G$ で表す．正整数 n の整除関係に関するポセットを $\mathscr{D}(n)$ で表す．m が n の約数であるならば，閉区間 $[C_m, C_n]_{\mathscr{S}_G}$ から $\mathscr{D}\left(\frac{n}{m}\right)$ へのポセット同型が存在する．以下の補題はよく知られている．

Lemma 6.1. *C_d が $[C_m, C_n]_{\mathscr{S}_G}$ の要素であるならば,*

$$\mu_{\mathscr{S}_G}(C_m, C_d) = \mu_{\mathscr{D}(\frac{n}{m})}\left(1, \frac{d}{m}\right)$$

が成り立つ．特に, $\mu_{\mathscr{S}_G}(C_m, C_d) = \mu\left(\frac{d}{m}\right)$ が成り立つ.

Theorem 6.2. *G が位数 n の巡回群であるならば, n の任意の約数 m に対し $f_{C_m}^G(x) = M\left(x, \frac{n}{m}\right)$ が成り立つ.*

Proof. $f_{C_m}^G(x)$ の定義と Lemma 6.1 から以下の等式が成り立つ:

$$\begin{aligned} f_{C_m}^G(x) &= |WC_m|^{-1}\sum_{S\leq C_n} \mu(C_m, S)x^{|G/S|} \\ &= \left|\frac{n}{m}\right|^{-1}\sum_{C_d\leq C_n} \mu(C_m, C_d)x^{|C_n/C_d|} \\ &= \left|\frac{n}{m}\right|^{-1}\sum_{\frac{d}{m}|\frac{n}{m}} \mu\left(\frac{d}{m}\right)x^{\frac{n/m}{d/m}} \\ &= M\left(x, \frac{n}{m}\right). \end{aligned}$$

□

Theorem 6.2 と Theorem 5.8 から以下の系が従う.

Corollary 6.3. *G が位数 n の巡回群，q が任意の正整数であるならば,*

$$q^G = \sum_{m|n} M\left(q, \frac{n}{m}\right)[G/C_m]$$

が成り立つ.

最後に，丹原大介先生が所属している弘前大学での集会で講演する機会を与えてくださった世話人の方々に深く感謝する.

参考文献

[Br05] Brun, M.: *Witt vectors and Tambara functors.* Advances in Mathematics **193** (2005), 233–256.

[Dr71] Dress, A. W. M.:*Operations in representation rings*, Proc. Symposia in Pure Math., 21 (1971), 39–45.

[Dr73] Dress, A. W. M.:*Contributions to the theory of induced representations, Algebraic K-theory, II: "Classical" algebraic K-theory and connections with arithmetic.* Springer, Berlin, LNM. **342** (1973), 183–240.

[DS88] Dress, A. W. M.; Siebeneicher, C.:*The Burnside Ring of Profinite Groups and the Witt Vector Construction*, Advances in Math. **70**, (1988).

[DS89] Dress, A. W. M.; Siebeneicher, C.:*The Burnside ring of the infinite cyclic group and its relations to the necklace algebra, λ-rings, and the universal ring of Witt vectors*, Advances in Math. **78**, (1989) 1–41.

[Gl81] Gluck, D.: *Idempotent formula for the Burnside ring with applications to the p-subgroup simplicial complex.* Illinois J. Math. **25** No.1 (1981), 63–67.

[MR83] Metropolis, N.; Rota, Gian-Carlo.: *Witt vectors and the algebra of necklaces.* Adv. Math. **50** (2) (1983), 95–125.

[Ta93] D. Tambara, On multiplicative transfer, *Comm. Algebra* **21** (1993) 1393-1420.

[Yo83] Yoshida, T.: *Idempotents of the Burnside rings and Dress induction theorem.* J. Algebra **80** (1983), 90–105.

[Yo90] Yoshida, T.: *On the unit groups of Burnside rings.* J. Math. Soc. Japan **42** (1990), 31–64.

Permutation Codes

Manabu Hagiwara
hagiwara.hagiwara@aist.go.jp

National Institute of Advanced Industrial Science and Technology,
Chuo University (as a visiting associate professor),

at Hirosaki Univ.

Permutation Codes

S_n: the symmetric group on a set $\{0, 1, \ldots, n-1\}$.

Remark

S_n acts on $\mathbb{R}^n$ by

$$\sigma\mu := (\mu_{\sigma^{-1}(0)}, \mu_{\sigma^{-1}(1)}, \ldots, \mu_{\sigma^{-1}(n-1)}),$$

where $\mu = (\mu_0, \mu_1, \ldots, \mu_{n-1})$.

Definition (Permutation Code (Narrow Sense))

G: a subset of S_n.
μ: a vector in $\mathbb{R}^n$.
A permutation code $\langle G, \mu \rangle$ for G and μ is the orbit, *i.e.*,

$$\langle G, \mu \rangle := \{g\mu \mid g \in G\}.$$

Permutation Codes

$\mathcal{M}$: a set s.t. $|\mathcal{M}| = |(G, \mu)|$.
$\mathrm{enc} : \mathcal{M} \to (G, \mu)$: a bijection.
$\mathrm{dec} : (G, \mu) \to \mathcal{M}$ a bijection.
$\mathrm{ec} : \mathbb{R}^n \to (G, \mu)$.

Definition (Permutation Code (Wider Sense))

$(\mathrm{enc}, \mathrm{ec}, \mathrm{dec}, G, \mu, \mathcal{M})$: a permutation code
$\Longleftrightarrow$
$\mathrm{dec} \circ \mathrm{enc} = \mathrm{id}$.

Background

$$\mathcal{M} \to (G, \mu) \to \mathbb{R}^n \to (G, \mu) \to \mathcal{M}$$

"hello" $\to (x_1, x_2, \ldots, x_n) \to (\lambda_1, \lambda_2, \ldots, \lambda_n) \to (x'_1, x'_2, \ldots, x'_n) \to$ "hell"

The above one is "a" definition.

Fundamental Goal for Permutation Codes

$\mathrm{d}(,)$: a distance metric on R ($\subset \mathbb{R}^n$)

Problem

For a given $\lambda \in R$,
"find" $g_0\mu \in \langle G, \mu \rangle$ *or* $g_0 \in G$ *s.t.*

$$\mathrm{d}(\lambda, g_0\mu) = \min_{g \in G} \mathrm{d}(\lambda, g\mu)$$

Rank Modulation (Wider Sense)

Definition (Rank Modulation)

a permutation code (G, μ) is a rank modulation
$\iff \mu = (1, 2, \ldots, n)$

Example

$G = S_n, \mu = (1, 2, \ldots, n)$

Example

$$\to (G, \mu) \to \mathbb{R}^n \to (G, \mu) \to$$

Rank Modulation (Narrow Sense)

Definition (Rank Modulation)

a permutation code (G, μ) is a rank modulation
$\iff$ $\mu = (1, 2, \ldots, n)$ and

$$\mathcal{M} \to (G, \mu) \to S_n \to (G, \mu) \to \mathcal{M}$$

My Interests

Problem

Solve the following simultaneously:

- *To define* G
- *To construct* enc *and* dec
  $\Rightarrow$ *determine* $|G|$
  $\Rightarrow$ *realize* enc *and* dec *as combinatorial bijections*
- *To construct* ec
  and analyze a (topological) optimality

Exercise

$G := \{g \in S_n | g^2 = \mathrm{id}, g(i) \neq i (1 \leq \forall i \leq n)\}$

- Can you count $|G|$?
- Can you find a comb. bije.: $\{1, 2, \ldots, |G|\} \to G$ and its inverse?
- For a given $\sigma \in S_n$, can you find $g \in G$ s.t.

$$d(g, \sigma) \leq d(g, \tau) \forall \tau \in S_n$$

for a given measure $d(,)$.

Easy Examples: Cyclic Group

$G := C_n := \langle [2, 3, \ldots, n, 1] \rangle$.
$\mathcal{M} := \{0, 1, \ldots, n-1\}$.

Example

Define $\mathrm{enc}_{C_n} : \mathcal{M} \to C_n$ as

$$\mathrm{enc}_{C_n}(i) := [i+1, i+2, \ldots, n, 1, \ldots, i].$$

Easy Examples: Dihedral Group

$G := D_{2n} := C_n \sqcup w_0 C_n$,
where $w_0 := [n, n-1, \ldots, 2, 1]$
$\mathcal{M} := \{0, 1, \ldots, 2n-1\}$.

Example

Define $\mathrm{enc}_{D_{2n}} : \mathcal{M} \to D_{2n}$ as
if $0 \leq i \leq n-1$

$$\mathrm{enc}_{D_{2n}}(i) := [i+1, i+2, \ldots, n, 1, \ldots, i],$$

if $n \leq i \leq 2n-1$

$$\mathrm{enc}_{D_{2n}}(i) := w_0[i+1, i+2, \ldots, n, 1, \ldots, i],$$

Easy Examples: Symmetric Group

$G := S_n$.
$\mathcal{M} := \{0, 1, \ldots, n! - 1\}$.

Example

Define $\mathrm{enc} : \mathcal{M} \to S_n$ as
a composite map of enc_1 and enc_2, where
$\mathrm{enc}_1(i) := (f_1, f_2, \ldots, f_{n-1})$, so that $i = \sum_{1 \leq j \leq n-1} f_j(j!)$,
$\mathrm{enc}_2(f_1, f_2, \ldots, f_{n-1}) := \sigma$, so that $\mathrm{inv}(\sigma) = (f_1, f_2, \ldots, f_{n-1})$.

Extension: Wreath Product

$G := G_0 \wr S_R$. $(G_0 = C_\nu, D_{2\nu}, S_\nu)$
$\mathcal{M} := \{0, 1, \ldots, |G_0|R! - 1\}$.

Example

Define $\mathrm{enc} : \mathcal{M} \to G_0 \wr S_R$ as
a composite map of enc_1 and enc_2, where
$\mathrm{enc}_1(i) := (i_1, i_2)$, so that $i = i_1 R! + i_2$, $0 \le i_1 < |G_0|, 0 \le i_2 < R!$
$\mathrm{enc}_2(i_1, i_2) := \mathrm{enc}_{G_0}(i_1)\mathrm{enc}S_R(i_2)$.

Graph Automorphism

$$C_n = \mathrm{Aut}(\Gamma_{C_n}), D_{2n} = \mathrm{Aut}(\Gamma_{D_{2n}}), S_n = \mathrm{Aut}(\Gamma_{S_n})$$

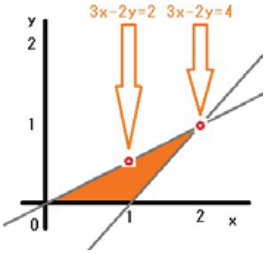
$$G_0 \wr S_R = \mathrm{Aut}(\Gamma_G \sqcup \Gamma_G \sqcup \cdots \sqcup \Gamma_G).$$

Linear Programming Method

Maximize a **value of linear function** over a **polytope**.

- $y \geq 0$
- $y \geq x - 1$
- $y \leq \frac{1}{2}x$

Find $x, y \in \mathbb{R}$
maximizing $3x - 2y$
over the right region.



Remark

A solution exists uniquely $\Rightarrow$ the solution is a vertex.

This kind of problem is called
a **Linear Programming (LP) Problem**.

Remark

A poly. time algo. is known for LP problems.

Birkhoff Polytope

—Connection btw LP problem and S_n—

Definition (Birkhoff Polytope)

DSM_n is the set of square matrices $(X_{i,j})$ satisfying:

- (Positivity) $X_{i_0,j_0} \geq 0$, for $0 \leq i_0, j_0 < n$,
- (Row Const.) $\sum_{0 \leq i < n} X_{i,j_0} = 1$ for $0 \leq j_0 < n$,
- (Column Const.) $\sum_{0 \leq j < n} X_{i_0,j} = 1$ for $0 \leq i_0 < n$,

and is called the **Birkhoff Polytope**.

Theorem (Birkhoff von-Neumann Theorem)

$\mathrm{Ver}(\mathrm{DSM}_n)$*: the set of vertices for* DSM_n

$$\mathrm{Ver}(\mathrm{DSM}_n) = S_n,$$

i.e., vertex = permutation matrix,
by regarding a perm. mat. as a perm. on indices.

LP-decoding for Permutation Code

Theorem (Wadayama and H)

$\mu, \lambda \in \mathbb{R}^n$:

$$\sigma \text{ minimizes } ||\lambda - \sigma\mu|| \iff \sigma \text{ maximizes } \lambda X^\sigma \mu^T,$$

where $\sigma \in S_n, X^\sigma \in \mathrm{DSM}_n$ *and* $||\cdot||$ *is the Euclidean distance metric.*

Definition (LP-decoding algorithm)

- Input: $\mu, \lambda \in \mathbb{R}^n$
- Output: $X \in S_n$

1. Solve $\max_{X \in \mathrm{DSM}_n} \lambda X \mu^T$ (*i.e.*, maximize a linear function).
2. Output the solution $X \in \mathrm{DSM}_n$ if $X \in S_n$ or terminate.

LP-decoding works as ML-decoding for $\langle S_n, \mu \rangle$ and runs in polynomial time on n.

Toward ML-Certificate

Let us generalize the decoding.
$\mathcal{L}$: a set of lin. eq. and lin. ineq.
$\mathcal{D}_\mathcal{L}$: the set of mat. satisfying $\mathcal{L}$

Definition (LP-decoding algorithm)

- Input: μ, λ
- Output: $X \in S_n$

1. Solve $\max_{X \in \mathcal{D}_\mathcal{L}} \lambda X \mu^T$
2. Output the solution $X \in \mathcal{D}_\mathcal{L}$ if $X \in S_n$ or terminate.

Remark

If we find $\mathcal{L}$ *such that*

$$\mathrm{Ver}(\mathcal{D}_\mathcal{L}) \subset S_n,$$

LP-decoding works as ML-decoding for $\langle \mathrm{Ver}(\mathcal{D}_\mathcal{L}), \mu \rangle$ *and may run in polynomial time on* n.

Construction for Linear Constraints

$\mathcal{L}$: a set of lin. eq. and lin. ineq.
$\mathcal{D}_{\mathcal{L}}$: the set of mat. satisfying $\mathcal{L}$

Problem

Is there any non-trivial linear constraint $\mathcal{L}$ so that

$$\mathrm{Ver}(\mathcal{D}_{\mathcal{L}}) \subset S_n?$$

- Give a construction for $\mathcal{L}$ satisfies above.
- Characterize $\mathrm{Ver}(\mathcal{D}_{\mathcal{L}})$.

i.e., Our Goal: construct a perm. code s.t.
LP-decoding works as ML-decoding.

Graph Approach

Γ: a graph
A_Γ: the adj. mat. of Γ

Definition (Graph Constraints and its Polytope)

$\mathcal{D}_\Gamma := \{X \in \mathrm{DSM}_n \mid A_\Gamma X = X A_\Gamma\}$.

i.e.,

- $X_{i_0,j_0} \geq 0$, for $0 \leq i_0, j_0 < n$,
- $\sum_{0 \leq i < n} X_{i,j_0} = 1$ for $0 \leq j_0 < n$,
- $\sum_{0 \leq j < n} X_{i_0,j} = 1$ for $0 \leq i_0 < n$,
- $(A_\Gamma X)_{i_0,j_0} = (X A_\Gamma)_{i_0,j_0}$ for $0 \leq i_0, j_0 < n$.

Definition (Compact Graph)

Γ is compact $\iff \mathrm{Ver}(\mathcal{D}_\Gamma) = \mathrm{Aut}(\Gamma)$.

Known Results and my Results

Remark (Known Results)

"Circle" and "Tree" are compact graphs.

Remark (mine)

"Cycle" is a compact graph. Γ is compact $\Rightarrow$ Union of compact graphs is compact.

Summary

- Construction of Linear Constraints from Graphs.
- Graph approach works well.
- In particular, Enc, Ec, Dec are in class P.

Modular forms of weight 8 for the theta group[1]

大浦　学（高知大学）

今回お話しする内容は、すでに出版されている

M.Oura, C.Poor, R.Salvati Manni, D.Yuen
Modular Forms of weight 8 for $\Gamma_g(1,2)$
Math.Ann. 346(2010), 477-498.

で、細かい話しはせずに大まかな流れがわかるように話したいと思います。この論文では超弦理論から投げかけられた問いに対して答えを与えているのですが、物理の話しは省略させていただきます。もともと数学的にこの辺りに存在する問題から説明していきます。$A(\Gamma_g)$ で $\Gamma_g = Sp_{2g}(\mathbf{Z}) \subset GL_{2g}(\mathbf{Z})$ に関するモジュラー形式のなす次数付き環とします。僕のこれまでの研究の立場からこれらの環を述べると、低い種数の場合は有限群の不変式環であり、組合せ論的解釈もうまくいく場合が多いです。種数３までの次数付き環は知られており、

$$\begin{aligned} A(\Gamma_1) &\cong \mathbf{C}[x_1, x_2]^{H_1} \\ A(\Gamma_2)^{(2)} &\cong \mathbf{C}[x_1, \ldots, x_4]^{H_2} \\ A(\Gamma_3) &\cong \mathbf{C}[x_1, \ldots, x_8]^{H_3}/(W^{(3)}_{e_8^2} - W^{(3)}_{d_{16}^+}) \end{aligned}$$

となります。ここでいくつか記号を説明します。H_g は $GL_{2^g}(\mathbf{C})$ のある特別な有限部分群で自然に 2^g 変数多項式環に作用します。この作用で不変な元全体を $\mathbf{C}[x_1, \cdots, x_{2^g}]^{H_g}$ で表しています。これを有限群 H_g の不変式環と呼んでいます。上にでてくる $W^{(g)}_C$ は 2^g-変数多項式で、２元体上の符号 C の種数 g の重み多項式を表します。$A(\Gamma_2)^{(2)}$ の (2) は重さが偶数のモジュラー形式に限ることを表しています。種数 $g = 3$ のところを見てみます。簡単のため、$I_g = W^{(g)}_{e_8^2} - W^{(g)}_{d_{16}^+}$ とおきます。上で割り算をしているところからもわかる通り、$I_3 \neq 0$ です。ですが、$I_1 = I_2 = 0$ です。後で述べる Witt の問題もここで考えられて

$$I_g \neq 0 \Leftrightarrow g \geq 3$$

です。

次に多項式の世界からモジュラー形式を得ることを考えます。そのために、多項式の変数は、上では $x_1, \ldots, x_{2^g}$ と書きましたが、以後、縦ベクトルからなる $\mathbf{F}_2^g = \underbrace{\mathbf{F}_2 \oplus \cdots \oplus \mathbf{F}_2}_{g}$ の元で添え字をつけます: $\mathbf{C}[x_a : a \in \mathbf{F}_2^g]$。これにうまく対応するのですが、$a, b \in \mathbf{F}_2^g$ に対して次のテータ関数を思い出しておきましょう:

$$\theta_{ab}(\tau) = \sum_{n \in \mathbf{Z}^g} \exp 2\pi\sqrt{-1}\left\{ {}^t(n + \frac{a}{2})\frac{\tau}{2}(n + \frac{a}{2}) + \frac{{}^t a}{2} b \right\}$$

[1]これは第２９回代数的組合せ論シンポジウムにおける講演をほぼ忠実に記録したものです。

ここで τ は種数 g の上半空間 $\mathbf{H}_g$ の元です。さて、多項式からモジュラー形式は次のテータ写像

$$Th:\ x_a \longmapsto \theta_{a0}(2\tau)$$

から得られます。実際、符号の重み多項式をテータ写像で写すと構成 A により符号から得られる格子のテータ関数が得られます。特に

$$Th(I_g) = \vartheta^{(g)}_{E_8^2} - \vartheta^{(g)}_{D_{16}^+}$$

なのですが、少し詳しくみてみましょう。上に述べたとおり多項式として $I_3 \neq 0$ でしたが、実は $Th(I_3) = 0$ となります。これは Witt の問題と呼ばれるものです。Witt は論文 Eine Identitäte zwischen Modulformen zwiten Grades (1941)[2]の中で、まず長さ１６の even unimodular lattice が E_8^2, D_{16}^+ の二つであることを示したのち、$Th(I_2) = 0$ を明らかにしてあります。さらに Witt は $Th(I_4) \neq 0$ はわかっているが、$Th(I_3)$ に関しておそらくゼロだろうが計算が途方もなく、決定できなかったと述べています。この問題は井草準一 (1967) と Martin Kneser(1967) により独立に $Th(I_3) = 0$ が示されました。ともかく

$$Th(I_g) \neq 0 \Leftrightarrow g \geq 4$$

が得られました。これがオリジナルな Witt の問題です。

もう少し $Th(I_3)$ をみていきましょう。この関数の定義域は $\mathbf{H}_g$ だった訳ですが、小さな部分 Jac_g を考えてみます。これは種数 g のコンパクトリーマン面の周期行列の集合です。$g \leq 3$ ですと Jac_g は $\mathbf{H}_g$ で稠密であり、両者の違いが本質的に表れるのは $g = 4$ の場合です。Schottky(1888) は $Th(I_4)$ が Jac_4 上消滅することを示します。以後、$A(\Gamma_g)$ の元で、Jac_g 上消滅するもののなすイデアルを記述することが問題となりました（Schottky の問題)。種数 $g = 4$ に関しては、Schottky, 井草 (*cf.* Freitag) らにより解決、種数 $g = 5$ に関しては色々進展はあるようですが、未解決と思われます。

では物理の超弦理論から投げかけられた問題に移っていきます。それは次の３条件を満たすようなテータ群 $\Gamma_g(1,2)$ に関する重さ８のモジュラー形式 $\Xi[0]$ を見つけよ、というものです。一つ目の条件は splitting property

$$\Xi^{(g)}[0]\begin{pmatrix}\tau_1 & 0\\ 0 & \tau_2\end{pmatrix} = \Xi^{(g-k)}[0](\tau_1)\Xi^{(k)}[0](\tau_2), \tau_1 \in \mathrm{Jac}_{g-k}, \tau_2 \in \mathrm{Jac}_k$$

です。二つ目は vanishing trace property で、

$$\sum_{\gamma \in \Gamma_g(1,2)\backslash\Gamma_g} \Xi^{(g)}[0]|_8\gamma = \sum_m \Xi^{(g)}[m]$$

[2]この論文に関しては小関道夫先生の解説
http://www.math.is.tohoku.ac.jp/~taya/sendaiNC/2004/report/ozeki.pdf
があります。

は Jac_g 上消滅するというものです。ここで m は $\mathbf{F}_2^{2g}$ の even characteristic をわたります。最後は uniqueness property で $\Xi^{(1)}[0] = \eta^{12}\theta_0^4$ とおくとき、上で述べた二つの条件を満たすモジュラー形式があったら、それらは Jac_g 上一致する、というものです。$\Gamma_g(1,2)$ に対する重さ８のモジュラー形式ですが、unimodular な格子から得られるテータ関数がまず考えられます。長さ１６の unimodular 格子は even が E_8^2, D_{16}^+ の二つ、odd が６個あります。我々はここにおける Witt の問題を考え、これら８つの格子のテータ関数が一次独立になる必要十分条件は $g \geq 5$ であることを示します。$g \leq 4$ では重さ８のモジュラー形式がすべて格子のテータ関数から得られることも示されます。最終的に、６個の odd unimodular 格子のテータ関数と Schottky invariant $Th(I_g)$ の一次結合で上で述べた３条件を満たす $\Xi^{(g)}[0]$ を $g \leq 4$ の場合に構成しました。この部分の結果は、D'Hoker, Phong により先鞭をつけられ、Cacciatori, Dalla Piazza, van Geemen, Grushevsky らにより高い種数へ拡張されてきたものを、結果を条件つきであった部分を取り除いたり、再構成したことになります。

Combinatorial Structures immanent in the Leech lattice.

Michio Ozeki

19th June 2012

1 Introduction

In an effort to compute some Fourier coefficients of Siegel theta series of various degrees associated with the Leech lattice we have encountered many interesting parameters (such as 4600,336,170 for instance) that would be connected with combinatorial structures, and we could derive many combinatorial structures, some of which are already known by another approaches and another structures are may be new.

In this talk we will treat **spherical codes**, spherical designs (only mentioning), **association schemes**, **distance regular graphs**[1].

Advantages of our method: synthetic in deriving many combinatorial structures, could analyze detailed structures

Disadvantages: computational, not complete in that we can not treat the uniqueness questions on such structures within our current scope.

2 Leech lattice

The generator matrix of [24,12,8] Golay code.

$$\begin{pmatrix}
1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&0&0&1&0&1\\
0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&0&0&1&1\\
0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&0&0&1\\
0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&0&1\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&0&1\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&1&1&1&1\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&1&0&1&1&0&1&1&1\\
0&0&0&0&0&0&0&1&0&0&0&0&1&1&0&0&0&1&0&1&1&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&1&1&0&1\\
0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&1&0&0&0&1&0&1&1&1\\
0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&1&1&0
\end{pmatrix}.$$

[1] In the talk at the meeting in Hirosaki the reporter talked of strongly regular graph associated with the Leech lattice, but this part is not accurate. The correct connection would be the distace regular graph.

When C =Golay code above we put

$$\begin{array}{ccccc} \rho & : & \mathbb{Z}^n & \to & \mathbb{F}_2^n \\ & & \Downarrow & & \Downarrow \\ & & \mathbf{x} & \mapsto & \mathbf{x} \bmod 2 \end{array}$$

$$M(C) = \frac{1}{\sqrt{2}} \left\{ \mathbf{x} = (x_1, x_2, \dots, x_{24}) \in \rho^{-1}(C) | \sum_{i=1}^{24} x_i \equiv 0 \pmod 4 \right\}$$

$$\gamma = \tfrac{1}{\sqrt{8}}(1, \dots, 1, -3),$$

$$N(C) = M(C) \cup (\gamma + M(C)).$$

Then the obtained lattice $N(C)$ is called the Leech lattice.

We use $\mathcal{L}$ to denote the Leech lattice.
References:J.H. Conway and N.J.A. Sloane [5], J. Leech [10], J. Leech and N.J.A. Sloane [11].

3 theta series

3.1 ordinary theta series in one complex variable

In an even lattice L, for the non-zero vector $\mathbf{x}$ in L $(\mathbf{x}, \mathbf{x})$ is an even integer, and we say that $\mathbf{x}$ is a 2m-vector if $(\mathbf{x}, \mathbf{x}) = 2m$ holds for some natural number m. Let $\Lambda_{2m}(L)$ be the set defined by

$$\Lambda_{2m}(L) = \{\mathbf{x} \in L \mid (\mathbf{x}, \mathbf{x}) = 2m\}.$$

Let L be an even unimodular lattice of rank 8k, then the theta series for L is defined by

$$\vartheta(z, L) = \sum_{\mathbf{x} \in L} \exp(\pi i (\mathbf{x}, \mathbf{x}) z),$$

where $\mathfrak{H}_1 = \{z = x + yi \in \mathbb{C} \mid y > 0\}$ be the complex upper-half plane, and z is a variable on $\mathfrak{H}_1$. This series is rewritten as

$$\vartheta(z, L) = \sum_{m=1}^{\infty} a(2m, L) \exp(2\pi i m z),$$

where $a(2m, L) = |\Lambda_{2m}(L)|$.

In particular the Fourier expansion of $\vartheta(z, \mathcal{L})$:

$$\vartheta(z, \mathcal{L}) = 1 + 196560\mathbf{e}(2z) + 16773120\mathbf{e}(3z) + 398034000\mathbf{e}(4z) + \cdots,$$

where $\mathbf{e}(z)$ is the abreviation of $\exp(2\pi i z)$.

3.2 theta series with spherical function

To define theta series with spherical function, some informations on the Gegenbauer polynomials are necessary. The Gegenbauer polynomial $H_\nu(u)$ of degree ν is a solution of the differential equation of the second order:

$$(1-u^2)\frac{d^2H_\nu}{du^2} - u(8k-1)\frac{dH_\nu}{du} + \nu(8k+\nu-2)H_\nu = 0.$$

The explicit form of the polynomial $H_\nu(u), (\nu \equiv 0 \pmod 2)$ is given by

$$H_\nu(u) = \sum_{r=0}^{\nu/2} \frac{(-1)^r \begin{pmatrix} \nu \\ 2r \end{pmatrix} (2r-1)!!}{\prod_{i=1}^{r}(8k+2\nu-4-2(r-i))} u^{\nu-2r},$$

Here we understand that $\prod_{i=1}^{r}(8k+2\nu-4-2(r-i)) = 1$ and $(2r-1)!! = 1$ when $r = 0$, where $(2r-1)!!$ is the product of odd integers from 1 up to $2r-1$.
Using $H_\nu(u)$, the spherical function $P_\nu(\mathbf{x}, \alpha)$ of degree ν is defined by

$$P_\nu(\mathbf{x};\alpha) = H_\nu\left(\frac{(\mathbf{x},\alpha)}{\sqrt{(\mathbf{x},\mathbf{x})(\alpha,\alpha)}}\right)((\mathbf{x},\mathbf{x})(\alpha,\alpha))^{\frac{\nu}{2}}$$

Theta series with the spherical function is defined by

$$\vartheta(z, P_\nu, L) = \sum_{\mathbf{x}\in L} P_\nu(\mathbf{x};\alpha)\exp(\pi i(\mathbf{x},\mathbf{x})z). \tag{3.1}$$

where α is any vector in $\mathbb{R}^{8k}$ with $8k = rank(L)$. This series is rewritten as

$$\vartheta(z, P_\nu, L) = \sum_{m=1}^{\infty}\sum_{\mathbf{x}\in\Lambda_{2m}(L)} P_\nu(\mathbf{x};\alpha)\exp(2\pi i m z) \tag{3.2}$$

3.3 Basic Relations

Using theta series with spherical function the following relations are derived: Let $\mathcal{L}$ be the Leech lattice and $\Lambda_4 = \Lambda_4(\mathcal{L})$, then we have

$$\sum_{\mathbf{x}\in\Lambda_4}(\mathbf{x},\alpha)^2 = 32760(\alpha,\alpha) \tag{3.3}$$

$$\sum_{\mathbf{x}\in\Lambda_4}(\mathbf{x},\alpha)^4 = 15120(\alpha,\alpha)^2 \tag{3.4}$$

$$\sum_{\mathbf{x}\in\Lambda_4}(\mathbf{x},\alpha)^6 = 10800(\alpha,\alpha)^3 \tag{3.5}$$

$$\sum_{\mathbf{x}\in\Lambda_4}(\mathbf{x},\alpha)^8 = 10080(\alpha,\alpha)^4 \tag{3.6}$$

$$\sum_{\mathbf{x}\in\Lambda_4}(\mathbf{x},\alpha)^{10} = 11340(\alpha,\alpha)^5 \tag{3.7}$$

$$\sum_{\mathbf{x}\in\Lambda_4}(\mathbf{x},\alpha)^{14} - \frac{91\cdot(\alpha,\alpha)}{12}\sum_{\mathbf{x}\in\Lambda_4}(\mathbf{x},\alpha)^{12} = -90090\cdot(\alpha,\alpha)^7 \tag{3.8}$$

References:B. Schöneberg [19], E. Hecke [9], B. Schöneberg [20], B.B. Venkov [23], B.B. Venkov,[24], B.B. Venkov [25].

4 More Tools

4.1 Siegel Theta Series

The Siegel theta series of degree g attached to the lattice L is defined by

$$\vartheta_g(Z,L) = \sum_{\mathbf{x}_1,\cdots,\mathbf{x}_g\in L} exp(\pi i\sigma([\mathbf{x}_1,\ldots,\mathbf{x}_g]Z)),$$

where Z is the variable on Siegel upper-half space of degree g, $[\mathbf{x}_1,\ldots,\mathbf{x}_g]$ is a g by g square matrix whose (i,j) entry is $(\mathbf{x}_i,\mathbf{x}_j)$ and σ is the trace of the matrix.

Siegel theta series of degree g can be expanded to

$$\vartheta_g(Z,L) = \sum_{T\in\hat{\mathcal{P}}_g^s(\mathbb{Z})} a(T,L)e^{2\pi i\sigma(TZ)}.$$

Here $\hat{\mathcal{P}}_g^s(\mathbb{Z})$ is the set of positive semi-definite semi-integral symmetric square matrices of degree g, and $a(T,L) = \#\{\langle\mathbf{x}_1,\ldots,\mathbf{x}_g\rangle \in L^g \mid [\mathbf{x}_1,\ldots,\mathbf{x}_g] = 2T\}$.

4.2 Reduction Theory of Quadratic Forms

Let T be a symmetric square matrix of size g written by

$$T = \begin{pmatrix} t_{11} & t_{12}/2 & \cdots & t_{1g}/2 \\ t_{12}/2 & t_{22} & \cdots & t_{2g}/2 \\ \vdots & \vdots & \vdots & \vdots \\ t_{1g}/2 & t_{2g} & \cdots & t_{gg} \end{pmatrix},$$

then associated with it a quadratic form $\mathbf{Q}_T[\xi_1,\cdots,\xi_g]$ is defined by

$$\mathbf{Q}_T = \mathbf{Q}_T[\xi_1,\cdots,\xi_g] = \sum_{1\le i\le j\le g} t_{ij}\xi_i\xi_j,$$

where $\xi_1, \cdots, \xi_g$ are real independent variables. Let $GL_g(\mathbb{Z})$ be the group of all unimodular square matrices of size g. Two quadratic forms $Q_{T_1}[\xi] = \sum_{1\le i\le j\le g} t_{ij}^{(1)}\xi_i\xi_j$ and $Q_{T_2}[\xi] = \sum_{1\le i\le j\le g} t_{ij}^{(2)}\xi_i\xi_j$ are said to be integrally equivalent if there is an element $U \in GL_g(\mathbb{Z})$ such that the equality $U'T_1U = T_2$ holds, where U' is the transposed of the matrix U. A quadratic form $Q_T[\xi]$ with real entries t_{ij} is said to be positive semi-definite if it satisfies the condition that $Q_T[\xi] \ge 0$ for any set of real numbers $\xi_1, \cdots, \xi_g$, and the form $Q_T[\xi]$ is called positive definite if it satisfies the condition: $Q_T[\xi] > 0$ for any set of real numbers $\xi_1, \cdots, \xi_g$, where at least one of them is not zero. When $Q_T[\xi]$ is positive definite the matrix T is also called positive definite. Let $\mathcal{P}_g(\mathbb{R})$ be the set of positive definite symmetric matrices whose entries are real numbers.
The reduction theory of positive definite symmetric real matrices treats the conditions by which one can find all representatives of matrices of equivalence classes. For the precise conditions on the reduction one may consult the references Minkowski [12], or van-der-Waerden [26].
An element $T \in \mathcal{P}_g(\mathbb{R})$ is called semi-integral if the diagonal entries of T are all integers and the off-diagonal entries are integers or half the integers. If T is a semi-integral then the associated quadratic form $Q_T[\xi] = \sum_{1\le i\le j\le g} t_{ij}\xi_i\xi_j$ has integer coefficients, and $Q_T[\xi]$ takes integer value whenever $\xi_1, \cdots, \xi_g$ are all integers. When T is a semi-integral and positive definite the discriminat d_T of $Q_T[\xi]$ is defined by

$$d_T = \begin{cases} \det(2T) & \text{if } g \text{ is even,} \\ \frac{1}{2}\det(2T) & \text{if } g \text{ is odd} \end{cases}.$$

We denote by $\mathcal{P}_g^s(\mathbb{Z})$ the subset of $\mathcal{P}_g(\mathbb{R})$ consisting of semi-integral matrices. We will use the table of the reduced elements in $\mathcal{P}_g^s(\mathbb{Z})$ with $n = 3, 4, 5$. Thanks to N.J.A. Sloane's home page we can utilize the tables of the reduced quadratic forms of sizes 3,4,and 5 Brandt-Intrau [4], G. Nipp [14], G. Nipp [15]. One may note that in these tables mostly primitive forms are recorded. Here the quadratic form is called primitive if the coefficients $t_{ii}, 2t_{ij}(i \ne j)$ are coprime integers, and the forms without this condition are called imprimitive.
We add one unusual terminology. A positive definite semi-integral quadratic form (or matrix) $Q_T[\xi] = \sum_{1\le i\le j\le g} t_{ij}\xi_i\xi_j$ is called 2-special if $Q_T[\xi]$ satisfies the following property: when T is reduced then the diagonal entries of the obtained form are all 2. We give instances of 2-special quadratic forms.

5 How to Compute Fourier Coefficients

5.1 Principal Sequence of Matrices

$$\mathfrak{T}_{22} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \mathfrak{T}_{30} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}, \mathfrak{T}_{40} = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}, \mathfrak{T}_{50} = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 1 & 1 & 1 & 2 \end{pmatrix}.$$

5.2 Computations

In the equations (3.1)$\sim$(3.6) we take any one vector $\alpha \in \Lambda_4(\mathcal{L})$, we put

$$\lambda_a = \#\{\mathbf{x} \in \Lambda_4 |\ (\mathbf{x}, \alpha) = a\}.$$

The number a are proved to be one of $\pm 4, \pm 2, \pm 1, 0$. Note that $\lambda_4 = \lambda_{-4} = 1$ and $\lambda_a = \lambda_{-a}$ holds for $a = 2, 1$. By putting these quantities into the equation (3.1) we get

$$2 \cdot 4\lambda_2 + 2 \cdot \lambda_1 + 2 \cdot 4^2 = 32760 \cdot 4. \tag{5.1}$$

In the same way from (3.2) we get

$$2 \cdot 2^4\lambda_2 + 2 \cdot \lambda_1 + 2 \cdot 4^4 = 15120 \cdot 4^2. \tag{5.2}$$

We can solve the equations (3.14) and (3.15), and the solution is $\lambda_2 = 4600, \lambda_1 = 47104$. By the setting of λ_a's $2\lambda_4 + 2\lambda_2 + 2\lambda_1 + \lambda_0$ counts all members of the set Λ_4 non-overlappingly, hence we have

$$2\lambda_4 + 2\lambda_2 + 2\lambda_1 + \lambda_0 = |\Lambda_4| = 196560,$$

and $\lambda_0 = 93150$.
As a summary of the above arguments we give For any one of elements $\alpha \in \Lambda_4(\mathcal{L})$ there are (i) 93150 elements $\mathbf{x} \in \Lambda_4(\mathcal{L})$ with $(\mathbf{x}, \alpha) = 0$, (ii) 47104 elements $\mathbf{x} \in \Lambda_4(\mathcal{L})$ with $(\mathbf{x}, \alpha) = 1$, (iii) 4600 elements $\mathbf{x} \in \Lambda_4(\mathcal{L})$ with $(\mathbf{x}, \alpha) = 2$. Consequently we have

$$a(\mathfrak{T}_{20}, \mathcal{L}) = 196560 \cdot 93150, a(\mathfrak{T}_{21}, \mathcal{L}) = 196560 \cdot 47104, a(\mathfrak{T}_{22}, \mathcal{L}) = 196560 \cdot 4600,$$

where

$$\mathfrak{T}_{20} = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \mathfrak{T}_{21} = \begin{pmatrix} 2 & 1/2 \\ 1/2 & 2 \end{pmatrix}, \mathfrak{T}_{22} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}. \tag{4.4}$$

We use the convention $(\mathfrak{T}, \{a/2, b/2\}, 2)$ to denote the matrix

$$\begin{pmatrix} t_{11} & t_{12}/2 & a/2 \\ t_{12}/2 & t_{22} & b/2 \\ a/2 & b/2 & 2 \end{pmatrix},$$

where

$$\mathfrak{T} = \begin{pmatrix} t_{11} & t_{12}/2 \\ t_{12}/2 & t_{22} \end{pmatrix}.$$

We use the matrices (3.16) again. First we seek all possible pairs of integers a, b under the conditions:
(i) $(\mathfrak{T}_{22}, \{a/2, b/2\}, 2)$ is positive semi-definite,
(ii) when $(\mathfrak{T}_{22}, \{a/2, b/2\}, 2)$ is reduced under unimodular transformations: $U^t(\mathfrak{T}_{22}, \{a/2, b/2\}, 2)U$, the minimal value of the non-zero diagonal entries of the resulting matrix is 2.
The pair of integers $\langle a, b \rangle$ satisfying the conditions (i),(ii) are grouped into the sets according to the determinant of $2(\mathfrak{T}_{22}, \{a/2, b/2\}, 2)$ and the equivalence by the unimodular transformations. In the ternary quadratic forms $\det(2(\mathfrak{T}_{22}, \{a/2, b/2\}, 2))/2$ is called

the discriminant of the matrix $T = (\mathfrak{T}_{22}, \{a/2, b/2\}, 2)$ (c.f. the Section 2.4). We denote it by d. We write $C_d(\mathfrak{T}_{22}, \langle a, b\rangle)$ to denote the set of ordered pairs $\langle a', b'\rangle$ such that $\det(2(\mathfrak{T}_{22}, \{a/2, b/2\}, 2))/2 = \det(2(\mathfrak{T}_{22}, \{a'/2, b'/2\}, 2))/2 = d$ and $(\mathfrak{T}_{22}, \{a/2, b/2\}, 2)$ is equivalent to $(\mathfrak{T}_{22}, \{a'/2, b'/2\}, 2)$. The total sets thus defined are called admissible sets with respect to $\mathfrak{T}_2$.
We set, for a fixed pair $\mathbf{x}, \mathbf{y} \in \Lambda_4$ satisfying $(\mathbf{x}, \mathbf{y}) = 2$,

$$\lambda_{a,b}(2\mathfrak{T}_{22}; \mathbf{x}, \mathbf{y}) = \#\{\mathbf{z} \in \Lambda_4 | (\mathbf{x}, \mathbf{z}) = a, (\mathbf{y}, \mathbf{z}) = b\}.$$

We may consider all possible pairs of integers a, b under the conditions (i) and (ii), but this time $\mathfrak{T}_{22}$ is replaced by $\mathfrak{T}_{21}$ or $\mathfrak{T}_{20}$. As a result of searching we find that $C_{24}(\mathfrak{T}_{22}, \langle 0, 0\rangle) = \{\langle 0, 0\rangle\}$ and

$$\begin{aligned}
&C_{22}(\mathfrak{T}_{22}, \langle 1, 0\rangle) = \{\langle 1, 0\rangle, \langle 1, 1\rangle, \langle 0, 1\rangle, \langle -1, 0\rangle, \langle -1, -1\rangle, \langle 0, -1\rangle\},\\
&C_{18}(\mathfrak{T}_{22}, \langle 2, 1\rangle) = \{\langle 2, 1\rangle, \langle 1, -1\rangle, \langle 1, 2\rangle, \langle -1, 1\rangle, \langle -1, -2\rangle, \langle -2, -1\rangle\},\\
&C_{16}(\mathfrak{T}_{22}, \langle 2, 0\rangle) = \{\langle 2, 0\rangle, \langle 2, 2\rangle, \langle 0, 2\rangle, \langle 0, -2\rangle, \langle -2, 0\rangle, \langle -2, -2\rangle\},\\
&C_0(\mathfrak{T}_{22}, \langle 2, -2\rangle) = \{\langle 2, -2\rangle, \langle -2, 2\rangle, \langle 4, 2\rangle, \langle -4, -2\rangle, \langle 2, 4\rangle, \langle -2, 4\rangle\}
\end{aligned}$$

exhaust all possible admissible sets. Let $\langle a, b\rangle$ be an element of one of the above admissible sets and $\lambda_{a,b}(2\mathfrak{T}_{22}; \mathbf{x}, \mathbf{y})$ be as above. We take $\alpha = u\mathbf{x} + v\mathbf{y}$, where u and v are real independent variables, then we see that for $\mathbf{z} \in \Lambda_4$

$$(\mathbf{z}, \alpha) = au + bv,$$

holds for some a, b. One may note that $\lambda_{a,b}(2\mathfrak{T}_{22}; \mathbf{x}, \mathbf{y}) = 1$ for each ordered pair $\langle a, b\rangle \in C_0(2, -2)$ and that $(\alpha, \alpha) = 4u^2 + 4uv + 4v^2$. Note also that the equality

$$\lambda_{a,b}(2\mathfrak{T}_{22}; \mathbf{x}, \mathbf{y}) = \lambda_{-a,-b}(2\mathfrak{T}_{22}; \mathbf{x}, \mathbf{y})$$

holds for any element in one of the above admissible sets. The relation (3.1) in our present case implies that ($\lambda_{a,b} = \lambda_{a,b}(2\mathfrak{T}_{22}; \mathbf{x}, \mathbf{y})$ for short)

$$\begin{aligned}
&[\lambda_{1,0}\{(1u + 0v)^2 + ((-1)u + 0v)^2\} + \lambda_{0,1}\{(0u + 1v)^2 + (0u + (-1)v)^2\}\\
&+\lambda_{1,1}\{(1u + 1v)^2 + ((-1)u + (-1)v)^2\}] + [\lambda_{2,1}\{(2u + 1v)^2 + ((-2)u + (-1)v)^2\}\\
&+\lambda_{1,2}\{(1u + 2v)^2 + ((-1)u + (-2)v)^2\} + \lambda_{1,-1}\{(1u + (-1)v)^2 + ((-1)u + 1v)^2\}]\\
&+ [\lambda_{2,0}\{(2u + 0v)^2 + ((-2)u + 0v)^2\} + \lambda_{2,2}\{(2u + 2v)^2 + ((-2)u + (-2)v)^2\}\\
&+\lambda_{0,2}\{(0u + 2v)^2 + (0u + (-2)v)^2\}]\\
&+\{(2u - 2v)^2 + (-2u + 2v)^2 + (4u + 2v)^2 + ((-4)u + (-2)v)^2 + (2u + 4v)^2 + ((-2)u + (-4)v)^2)\}\\
&= 32760(4u^2 + 4uv + 4v^2).
\end{aligned}$$

Since this equation is an identity for the polynomials in u, v, we must have equations in the coefficients such as

$$\begin{aligned}
&2\lambda_{0,1} + 2\lambda_{1,1} + 2\lambda_{2,1} + 2\lambda_{1,-1} + 8\lambda_{1,2} + 8\lambda_{2,2} + 8\lambda_{0,2} = 130992,\\
&4\lambda_{1,1} + 8\lambda_{2,1} - 4\lambda_{1,-1} + 8\lambda_{1,2} + 16\lambda_{2,2} = 130992,\\
&2\lambda_{1,0} + 2\lambda_{1,1} + 8\lambda_{2,1} + 2\lambda_{1,-1} + 2\lambda_{1,2} + 8\lambda_{2,0} + 8\lambda_{2,2} = 130992.
\end{aligned}$$

Using the relations (3.2)$\sim$(3.5) we obtain other 32 equations on λ's. These plentiful equations are enough to determine all λs. We compute that

$$\begin{aligned}
&\lambda_{1,0} = \lambda_{0,1} = \lambda_{1,1} = \lambda_{-1,0} = \lambda_{0,-1} = \lambda_{-1,-1} = 20736,\\
&\lambda_{2,1} = \lambda_{1,-1} = \lambda_{1,2} = \lambda_{-2,-1} = \lambda_{-1,1} = \lambda_{-1,-2} = 2816,\\
&\lambda_{2,0} = \lambda_{2,2} = \lambda_{0,2} = \lambda_{-2,0} = \lambda_{-2,-2} = \lambda_{0,-2} = 891.
\end{aligned}$$

The same lines of tricks go up to degree 5. The reason for not being able to use this trick in degree 6 is that we do not know the reduction table of quadratic .

6 Combinatorial Structures in the Leech lattice

6.1 Spherical Code

Let

$$\Omega_n = \{(x_1, \cdots, x_n) | \sum_{i=1}^{n} x_i^2 = 1\}$$

be the unit sphere in the n-dimensional Euclidean space $\mathbf{R}^n$. An (n, M, s) spherical code is a subset $\mathcal{C}$ of Ω_n of size M for which $(\mathbf{u}, \mathbf{v}) \leq s$ holds for all $\mathbf{u}, \mathbf{v} \in \mathcal{C}, \mathbf{u} \neq \mathbf{v}$. Where $(\mathbf{u}, \mathbf{v})$ is the inner product in $\mathbf{R}^n$.

Theorem 6.1. *In a packing of unit sheres in $\mathbf{R}^n$ let $S_1, \ldots, S_k$ be a set of sheres such that S_i touches S_j for all $i \neq j$. Suppose there are further sheres $T_1, \ldots, T_M$ each of which touches all the S_i. Then, after rescaling, the centers of $T_1, \ldots, T_M$ form an $(n-k+1, M, 1/(k+1))$ spherical code.*

If we put a sphere of radius 1 with the center at each lattice point of Leech lattice $\mathcal{L}$, then we get the so-called lattice packing of spheres with respect $\mathcal{L}$. Two such spheres S_1 with the center $\mathbf{x}$ and S_2 with the center $\mathbf{y}$ have one common point (the touching point) if and only if the distance $\sqrt{(\mathbf{x}-\mathbf{y}, \mathbf{x}-\mathbf{y})}$ between $\mathbf{x}$ and $\mathbf{y}$ equals 2. The last condition is rewritten as

$$(\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}) = 4. \tag{6.1}$$

When $\mathbf{y} = \mathbf{0}$ and $\mathbf{x} \in \Lambda_4$ then the condition (6.1) is simply $(\mathbf{x}, \mathbf{x}) = 4$. Thus the number of spheres that touch the sphere S_0 with the center $\mathbf{0}$ equals $|\Lambda_4| = 196560$.
Next we consider the problem of the number M_1 of the spheres that touch both the sphe S_0 and the sphere S_1 with the fixed center $\mathbf{x}_1 \in \Lambda_4$. Let S be one of such spheres and $\mathbf{x}$ its center. Then $\mathbf{x}$ must satisfy $\mathbf{x} \in \Lambda_4$ and

$$(\mathbf{x}, \mathbf{x}_1) = 2.$$

The number M_1 is simply the number λ_2 discussed in the Section 4.1 and it equals 4600. We fix two vectors $\mathbf{x}_1, \mathbf{x}_2 \in \Lambda_4$ satisfying $(\mathbf{x}_1, \mathbf{x}_2) = 2$. The spheres S_0, S_1 and S_2 (its center is $\mathbf{x}_2$) touch mutually. The number M_2 of the spheres that touch the spheres S_0, S_1 and S_2 is equals the number of $\mathbf{x} \in \Lambda_4$ which satisfies the conditions $(\mathbf{x}, \mathbf{x}_1) = (\mathbf{x}, \mathbf{x}_2) = 2$. This number M_2 equals $\lambda_{2,2}(\mathfrak{T}_{22}; 4) = 891$ discussed in the Section 4.2.1. Likewise the number M_3 of spheres that touch the spheres S_0, S_1, S_2 and S_3, that touch mutually, equals the number $\lambda_{2,2,2}(\mathfrak{T}_{30}; \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) = 336$, discussed in the Section 5.1. The number M_4 of spheres that touch the spheres S_0, S_1, S_2, S_3 and S_4, that touch mutually, equals the number $\lambda_{2,2,2,2}(\mathfrak{T}_{40}; \mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4) = 170$, discussed in the Section 6. By applying the Theorem 6.1 to the above discussion we derive

Theorem 6.2. *Viewing the lattice packing of the Leech lattice $\mathcal{L}$ we obtain the spherical codes of the parameters* $(24, 196560, 1/2), (23, 4600, 1/3), (22, 891, 1/4), (21, 336, 1/5), (20, 170, 1/6)$.

6.2 Spherical Design

A finite non-empty set X of unit vectors in Euclidean space $\mathbb{R}^{d+1}$ is said to form a spherical t-design for some positive integer t if the following holds for $k = 0, 1, \cdots, t$:

$$\frac{1}{vol(\mathcal{S}^d)} \int_{\mathcal{S}^d} f(\xi) d\xi = \frac{1}{|X|} \sum_{\xi \in X} f(\xi),$$

where $\mathcal{S}^d$ is the unit sphere with the center at origin in $\mathbb{R}^{d+1}$ and $f(\xi) = f(\xi_1, \cdots, \xi_{d+1})$ is any polynomial in real variables $\xi_1, \cdots, \xi_{d+1}$ of degree k. As to the spherical design obtained from $\mathcal{L}$ we can not add any further result than the ones obtained by B.Venkov:

Theorem 6.3. *Let $L \subset \mathbb{R}^{24k}$ be an extremal lattice, $m \geq k+1$ and $\Lambda_{2m} = \{\mathbf{x} \in L \mid (\mathbf{x}, \mathbf{x}) =\}$ then $X = \frac{1}{\sqrt{2m}} \Lambda_{2m}$ is a $11-$design.*

By this Theorem $\frac{1}{2}\Lambda_4, \frac{1}{\sqrt{6}}\Lambda_6, \cdots$ are spherical $11-$designs.

6.3 Association Scheme

As to the precise definitions for the theory of association scheme one may refer (10) or (13).

Here we give a brief definition of the association scheme. An association scheme with d classes is a pair $(X, \mathcal{P})$, where X is a finite set with at least two elements and $\mathcal{P}$ is a partition of $X \times X$ with the following properties:
(i) $\mathcal{P} = \{P_0, P_1, \ldots, P_d\}$
(ii) $P_0 = \{\langle x, x \rangle | x \in X\}$,
(iii) if P_i is a member of $\mathcal{P}$ then the set $P_i^T = \{\langle y, x \rangle | \langle x, y \rangle \in P_i\}$ is also a member of $\mathcal{P}$ for $i = 0, 1, \cdots, d$,
(iv) for any pair $\langle x, y \rangle \in P_k$ the number $p_{i,j}^k$ of $z \in X$ such that both the conditions $\langle x, z \rangle \in P_i$ and $\langle y, z \rangle \in P_j$ hold does not depend on the choice of $\langle x, y \rangle \in P_k$. The numbers $p_{i,j}^k$ are called the intersection numbers of this association scheme $(X, \mathcal{P})$.
The number $n_i = p_{i,i}^0$ is called the valency of P_i, and it holds that

$$|X| = \sum_{i=0}^{d} n_i.$$

Let $\Lambda_4(\mathcal{L})$ be the subset of the norm 4 vectors in $\mathcal{L}$. It is easy to show that for two vectors $\mathbf{x}, \mathbf{y}$ in $\Lambda_4(\mathcal{L})$ it holds that $(\mathbf{x}, \mathbf{y}) \in \mathcal{V} = \{\pm 4, \pm 2, \pm 1, 0\}$. We define the relations among the elements in $\Lambda_4(\mathcal{L})$ in the following way:
Two elements $\mathbf{x}, \mathbf{y} \in \Lambda_4(\mathcal{L})$ are related to the relation R_a for $a \in \mathcal{V}$ if and only if $(\mathbf{x}, \mathbf{y}) = a$. Since the relations R_a are defined through the inner product, $R_a^T = R_a$ holds automatically.

Theorem 6.4. *Let Λ_4 be the set of vectors of norm 4 in the Leech lattice $\mathcal{L}$, and $\mathcal{R} = \{R_4, R_2, R_1, R_0, R_{-1}, R_{-2}, R_{-4}\}$ be a set of relations on Λ_4 defined above. Then the pair $(\Lambda_4, \mathcal{R})$ forms an association scheme.*

We fix a vector $\mathbf{x}_0 \in \Lambda_4(\mathcal{L})$ and consider a subset of $\Lambda_4(\mathcal{L})$ defined by

$$\Lambda_{4,2}(\mathcal{L}) = \{\mathbf{x} \in \Lambda_4(\mathcal{L}) \mid (\mathbf{x}, \mathbf{x}_0) = 2\}.$$

We can show that the cardinality of $\Lambda_{4,2}(\mathcal{L})$ is 4600. We are going to prove that the subset $\Lambda_{4,2}(\mathcal{L})$ forms an association scheme with respect to the inner product relation. Before doing so, we may show that for two vectors $\mathbf{x}, \mathbf{y}$ in $\Lambda_{4,2}(\mathcal{L})$ it holds that $(\mathbf{x}, \mathbf{y}) \in \mathcal{V}_1 = \{4, \pm 2, 1, 0\}$. We define the relations among the elements in $\Lambda_{4,2}(\mathcal{L})$ in the following way:
Two elements $\mathbf{x}, \mathbf{y} \in \Lambda_{4,2}(\mathcal{L})$ are related to the relation $\widehat{R}_a$ for $a \in \mathcal{V}_1$ if and only if $(\mathbf{x}, \mathbf{y}) = a$. We use the notation $q_{i,j}^k$ instead of $p_{i,j}^k$ used in the previous Theorem.

Theorem 6.5. *Let $\Lambda_{4,2}$ be the set defined as above, and $\widehat{\mathcal{R}} = \{\widehat{R}_4, \widehat{R}_2, \widehat{R}_1, \widehat{R}_0, \widehat{R}_{-2}\}$ be a set of relations on $\Lambda_{4,2}$ defined above. Then the pair $(\Lambda_{4,2}, \widehat{\mathcal{R}})$ forms an association scheme.*

6.4 Diatance Regular Graph

From the Leech lattice we may obtain some distance regular graphs, but at the present stage it is not appropriate to mention any definitive potential results. The reporter is reluctant to give any slight hints to the readers.

References: E. Bannai and T. Ito [2], E. Bannai and N.J.A. Sloane [3], E. Bannai and E. Bannai [1], P. Delsarte [6], P. Delsarte, J.M. Goethals and J.J. Seidel [7], J. Martinet (Ed.) [13],

6.5 Concluding Remark

Most of the results in Section 5 and Section 6 are covered in the preprint [17]. The reporter hopes that the readers may find the paper in the published form.

References

[1] 坂内英一，坂内悦子，球面上の代数的組合せ理論　Springer Tokyo, (1999)

[2] E. Bannai and T. Ito, Algebraic Combinatorics I: Association Schemes, Benjamin 1984

[3] E. Bannai and N.J.A. Sloane, Chapter 14 of [5].

[4] The Brandt-Intrau tables of primitive positive-definite ternary quadratic forms, originally in

`http://www2.research.att.com/~njas/lattices/Brandt_1.html`

now in

`http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/Brandt_1.html`

[5] J.H. Conway and N.J.A. Sloane, Sphere Packings, Lattices and Groups, Springer-Verlag 1988. Third Edition (1998)

[6] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Reports Supplements, No. 10 (1973)

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

[8] V.A. Erokhin, Theta series of even unimodular 24-dimensional lattices, LOMI **86** (1979), 82-93, J. Soviet Math. **17**(1981) 1999-2008

[9] E. Hecke, Analytische Arithmetik der positiven quadratischen Formen, Kgl. Danske Vid. Selskab. Mat.-fys. Medd. **13** (1940)

[10] J. Leech, Notes on sphere packings, Can. J. Math. **19** (1967)

[11] J. Leech and N.J.A. Sloane, Sphere packings and Errol-correcting codes, Can. J. Math. **23** (1971)

[12] H. Minkowski, Gesamelte Abhandlungen, Chelsea, New-York, 1967

[13] J. Martinet (Ed.), Réseaux Euclidiens, Designs Sphériques et Formes Modulaires, Monographie L'enseignement Mathématique (2001)

[14] G. Nipp, Tables of Quaternary Quadratic Forms (Computer Generated Tables), originally in

`http://www2.research.att.com/~njas/lattices/nipp.html`

,but moved to

`http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/nipp.html`

[15] G. Nipp, Tables of Quinary Quadratic Forms, originally in

`http://www2.research.att.com/~njas/lattices/nipp5.html`

,but now moved to

`http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/nipp5.html`

[16] M. Ozeki, On a problem posed by R. Salvati Manni, Acta Arithm. **151** (2011) 1-22

[17] M. Ozeki, Siegel theta series of various degrees for the Leech lattice, submitted to a jounal, 2012

[18] R. Salvati Manni, Slopes of cusp forms and theta series, J. Num. Th. **83** (2000) 282-296

[19] B. Schöneberg, Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen. Math. Ann. **116** (1939) 511-523

[20] B. Schöneberg, Elliptic Modular Functions, Springer (1974)

[21] C.L. Siegel, Einführung in die Theorie der Modulfunktionen n-ten Grades, Math. Ann. **116** (1939) 617-657

[22] C.L. Siegel, Lectures on Quadratic Forms, Tata Institute of Fundamental Research, Bombay (1967)

[23] B.B. Venkov, The classification of integral even unimodular 24-dimensional quadratic forms, Trudy Math. Inst. Steklov **148** (1978), 65-76 Proc. Steklov Inst. Math. **148** (1980) 63-74

[24] B.B. Venkov, On even unimodular Euclidean lattices of dimension 32, LOMI **116** (1982),44-45, 161-162, J. Soviet Math. **26**(1984), 1860-1867

[25] B.B. Venkov, On even unimodular Euclidean lattices of dimension 32, II, LOMI **134** (1982),34-58, J. Soviet Math. **36**(1987), 21-38

[26] B.L. van der Waerden and H. Gross, editors, Studien zur Theorie der quadratischen Formen, Birkhäuser, Basel, 1968

Michio Ozeki
Emeritus Professor at the Department of
Mathematical Sciences,
Faculty of Science, Yamagata University
permanent address: Postal code: 036-8155
4-8-27, Nakano, Hirosaki City, Aomori
Japan
E-mail: ozeki.mitio@ruby.plala.or.jp

Partial Epstein zeta functions on linear codes over $\mathbb{Z}_p$ and their functional equations

Kazuyoshi SUZUKI
Nagoya Industrial Science Research Institute,
Nagoya, Japan

Abstract

In this paper, partial Epstein zeta functions on linear codes over $\mathbb{Z}_p$, which are related with Lee weight enumerators of linear codes over $\mathbb{Z}_p$, are newly defined. Then functional equations for those zeta functions on codes are presented. In particular, it is clarified that simple functional equations hold for partial Epstein zeta functions on linear self-dual codes over $\mathbb{Z}_p$.

1 Introduction

MacWilliams identities are important formulae in coding theory. The minimum distance of a code determines the error correction / detection capability of the code. The distance distribution of a linear code is equivalent to the weight distribution of the code, because the difference between any two codewords is equal to another codeword. MacWilliams identities for weight enumerators provide the relationship between the weight distribution of a code and that of the dual code [11, 12]. By using a MacWilliams identity, the weight enumerator of the dual code of a code is derived from that of the code, and vice versa. Several types of weight enumerators and MacWilliams identities for them have been known [11, 12].

Broué and Enguehard provided a construction method of elliptic modular forms using the weight enumerators of self-dual codes [4]. The relationship between several types of modular forms such as Hilbert, Jacobi, and Siegel modular forms and those of weight enumerators, e.g. Hamming weight enumerators and Lee weight enumerators, of codes over finite fields, finite rings have been extensively studied [1, 2, 3, 4, 5, 6, 7, 8, 14, 15].

Modular forms closely relate to the Dirichlet series and zeta functions. One classical reason why modular forms were studied is their use in investigating the number of ways of representing an integer by a quadratic form. For example, the number of ways an integer can be represented as a sum of squares is equal to the coefficient in the q-expansion of the power of a modular form. P. Epstein introduced a zeta function associated with positive definite quadratic forms [9]. In [16], partial Epstein zeta functions, which are summands of Epstein zeta functions associated with quadratic forms, have been introduced and

their functional equations have been proved by using the Mellin transform of theta series which are related with modular forms on binary linear codes. Moreover, in [17], partial Epstein zeta functions for binary linear codes, which are related with Hamming weight enumerators of binary linear codes, have been newly defined and functional equations of those zeta functions for codes have been presented. In particular, it has been clarified that simple functional equations hold for binary linear self-dual codes. In this paper, from the numerical interests, partial Epstein zeta functions for binary linear codes are expanded to those for linear codes over the integer residue class ring $\mathbb{Z}_p$ with odd prime p by using Lee weight enumerators of those codes. Then partial Epstein zeta functions for linear codes over $\mathbb{Z}_p$ are analytically continued to entire functions on whole complex plane except for a simple pole and functional equations of those zeta functions are derived.

The organization of this paper is as follows: Section 2 presents some definitions and basic facts concerning linear codes over $\mathbb{Z}_p$ and explains the MacWilliams identity for Lee weight enumerators of linear codes over $\mathbb{Z}_p$. Section 3 describes theta series and their transformation formulae. Section 4 presents partial Epstein zeta functions for linear codes over $\mathbb{Z}_p$ and their functional equations that are the main theme of this paper.

2 Preliminaries

This section presents the definitions and the basic properties of linear codes over $\mathbb{Z}_p$ and explains the MacWilliams identity for Lee weight enumerators of linear codes over $\mathbb{Z}_p$.

2.1 Linear codes over $\mathbb{Z}_p$

Let p be an odd prime and let $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ be a residue class ring of the integer ring $\mathbb{Z}$. A k-dimensional subspace of n-dimensional vector space $\mathbb{Z}_p^n$ is called an $[n, k]$ linear code over $\mathbb{Z}_p$, where n and k are called the code length and the dimension of the code, respectively. An element of a code is called a codeword of the code. An $[n, k]$ linear code may be specified by a basis of k linearly independent codewords. A matrix whose rows are a basis of a code is called a generator matrix of the code. Let G be a $k \times n$ generator matrix of an $[n, k]$ linear code over $\mathbb{Z}_p$ and let us denote G as

$$G = \begin{bmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{bmatrix},$$

where $g_{j,l}$ are elements of $\mathbb{Z}_p$ and the rows of G are a basis of C. All rows of G and all linear combinations of them are codewords in C. Therefore, C contains p^k codewords. The null space of C is spanned by the rows of the following matrix H that satisfies the

relation $G\ {}^tH = O_{k\times(n-k)}$:

$$H = \begin{bmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,n} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,n} \\ \vdots & \vdots & & \vdots \\ h_{n-k,1} & h_{n-k,2} & \cdots & h_{n-k,n} \end{bmatrix},$$

where $h_{j,l}$ are elements of $\mathbb{Z}_p$, ${}^tH$ denotes the transpose of H, and $O_{k\times(n-k)}$ denotes the $k \times (n-k)$ zero matrix. The matrix H is called a parity-check matrix of C and generates the dual code of C. The dual code $C^\perp$ of C is defined by

$$C^\perp = \left\{ \mathbf{v} \in \mathbb{Z}_p^n \mid \langle \mathbf{c}, \mathbf{v} \rangle = 0 \text{ for all } \mathbf{c} \in C \right\},$$

where $\langle \mathbf{c}, \mathbf{v} \rangle = \sum_{j=1}^{n} c_j v_j$ for $\mathbf{c} = (c_1, c_2, \ldots, c_n)$ and $\mathbf{v} = (v_1, v_2, \ldots, v_n)$, which is the inner product of $\mathbf{c}$ and $\mathbf{v}$. For a linear code C, its dual code $C^\perp$ consists of all rows of H and all linear combinations of them. In other words, H is a generator matrix of $C^\perp$. If $C = C^\perp$, then C is called a self-dual code.

Example 1 The following matrices G_5 and H_5 indicate a generator matrix of a $[5, 3]$ linear code over $\mathbb{Z}_5$ and a parity-check matrix of the code:

$$G_5 = \begin{bmatrix} 4 & 3 & 1 & 4 & 4 \\ 0 & 4 & 3 & 1 & 4 \\ 0 & 0 & 4 & 3 & 1 \end{bmatrix}, \quad H_5 = \begin{bmatrix} 1 & 2 & 1 & 0 & 1 \\ 2 & 0 & 3 & 1 & 0 \end{bmatrix}.$$

Hereinafter, we call this code C_5.

Example 2 The following matrix G_6 is a parity-check matrix of a $[6, 3]$ self-dual code over $\mathbb{Z}_5$ as well as a generator matrix of the code:

$$G_6 = \begin{bmatrix} 0 & 0 & 1 & 1 & 2 & 3 \\ 2 & 3 & 0 & 0 & 1 & 1 \\ 1 & 1 & 2 & 3 & 0 & 0 \end{bmatrix}.$$

Hereinafter, we call this code C_6.

2.2 MacWilliams identity for Lee weight enumerators of linear codes over $\mathbb{Z}_p$

The distance distribution of a code closely relates to the error correction / detection capability of the code. Any two codewords in a code have to be definitely far from each other for ensuring the specific error correction / detection capability. The distance distribution of a linear code is equivalent to the weight distribution of the code, because the distance between two codewords is equal to the weight of another codeword.

Definition 1 (Lee weight [12]) Let $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ be an element of $\mathbb{Z}_p^n$, where u_i is the ith component of $\mathbf{u}$. The Lee weight of u_i, denoted by $w_{\mathrm{L}}(u_i)$, is defined by

$$w_{\mathrm{L}}(u_i) := \min(u_i,\, p - u_i).$$

Then the Lee weight of $\mathbf{u}$, denoted by $w_{\mathrm{L}}(\mathbf{u})$, is defined by

$$w_{\mathrm{L}}(\mathbf{u}) := \sum_{i=1}^{n} w_{\mathrm{L}}(u_i).$$

The Lee composition of $\mathbf{u}$, denoted by $\mathrm{Comp}(\mathbf{u})$, is $(l_0, l_1, \ldots, l_q)$, where $q = (p-1)/2$ and $l_j = l_j(\mathbf{u})$ denotes the number of compositions of Lee weight j in $\mathbf{u}$.

Let $L_{p,n}$ be the set of Lee compositions $\{(l_0, l_1, \ldots, l_q) \mid l_0, l_1, \ldots, l_q \geq 0 \text{ and } l_0 + l_1 + \cdots + l_q = n\}$.

Definition 2 (Lee weight enumerator [12]) Let $x_0, x_1, \ldots, x_q$ be indeterminates, where $q = (p-1)/2$. Let C be an $[n, k]$ linear code over $\mathbb{Z}_p$. The Lee weight enumerator $W_C(x_0, x_1, \ldots, x_q)$ of C is defined by

$$W_C(x_0, x_1, \ldots, x_q) = \sum_{\mathbf{c} \in C} x_0^{l_0(\mathbf{c})} x_1^{l_1(\mathbf{c})} \cdots x_q^{l_q(\mathbf{c})} = \sum_{l \in L_{p,n}} W_l \prod_{j=0}^{q} x_j^{l_j},$$

where W_l denotes the number of codewords $\mathbf{c}$ with Lee composition $\mathrm{Comp}(\mathbf{c}) = l = (l_0, l_1, \ldots, l_q)$ in C and $\sum_{l \in L_{p,n}}$ denotes the summation over all $l \in L_{p,n}$. In the same way, for the dual code $C^\perp$ of C, the Lee weight enumerator $W_{C^\perp}(x_0, x_1, \ldots, x_q)$ of $C^\perp$ is defined by

$$W_{C^\perp}(x_0, x_1, \ldots, x_q) = \sum_{\mathbf{c}' \in C^\perp} x_0^{l_0^\perp(\mathbf{c}')} x_1^{l_1^\perp(\mathbf{c}')} \cdots x_q^{l_q^\perp(\mathbf{c}')} = \sum_{l^\perp \in L_{p,n}} W_{l^\perp}^\perp \prod_{j=0}^{q} x_j^{l_j^\perp},$$

where $W_{l^\perp}^\perp$ denotes the number of codewords $\mathbf{c}'$ with Lee composition $\mathrm{Comp}(\mathbf{c}') = l^\perp = (l_0^\perp, l_1^\perp, \ldots, l_q^\perp)$ in $C^\perp$ and $\sum_{l^\perp \in L_{p,n}}$ denotes the summation over all $l^\perp \in L_{p,n}$. Both the weight enumerators $W_C(x_0, x_1, \ldots, x_q)$ and $W_{C^\perp}(x_0, x_1, \ldots, x_q)$ are homogeneous polynomials of degree n in $q+1 = (p+1)/2$ indeterminates $x_0, x_1, \ldots, x_q$.

The following Theorem 1 holds for Lee weight enumerators of linear codes over $\mathbb{Z}_p$.

Theorem 1 (MacWilliams identity for Lee weight enumerators [12]) *Let C be an $[n, k]$ linear code over $\mathbb{Z}_p$ with dual code $C^\perp$. Then the following relation holds between the Lee weight enumerator of C and that of $C^\perp$:*

$$W_{C^\perp}(x_0, x_1, \ldots, x_q) = \frac{1}{|C|} W_C\left(x_0 + \sum_{s=1}^{q} (\xi_p^{0\cdot s} + \xi_p^{-0\cdot s}) x_s, x_0 + \sum_{s=1}^{q} (\xi_p^{1\cdot s} + \xi_p^{-1\cdot s}) x_s, \ldots, x_0 + \sum_{s=1}^{q} (\xi_p^{q\cdot s} + \xi_p^{-q\cdot s}) x_s\right), \tag{1}$$

where $\xi_p = \exp(2\pi i/p)$ is a primitive pth root of unity and $|C|$ denotes the number of codewords in C.

Equation (1) is the **MacWilliams identity for Lee weight enumerators of linear codes over** $\mathbb{Z}_p$. Equation (1) is symmetric with respect to the roles of C and $C^\perp$, that is,

$$W_C(x_0, x_1, \ldots, x_q) = \frac{1}{|C^\perp|} W_{C^\perp}\left(x_0 + \sum_{s=1}^{q} (\xi_p^{0\cdot s} + \xi_p^{-0\cdot s}) x_s, x_0 + \sum_{s=1}^{q} (\xi_p^{1\cdot s} + \xi_p^{-1\cdot s}) x_s, \ldots, x_0 + \sum_{s=1}^{q} (\xi_p^{q\cdot s} + \xi_p^{-q\cdot s}) x_s \right). \tag{2}$$

The MacWilliams identity represents that the weight enumerator of $C^\perp$ is derived from that of C, and vice versa. In particular, if C is self-dual, then $n = 2k$ and $|C| = p^k = \sqrt{p^n}$. Therefore, Eq. (1) results in the following form:

$$W_C(x_0, x_1, \ldots, x_q) = W_C\left(\frac{x_0 + \sum_{s=1}^{q} (\xi_p^{0\cdot s} + \xi_p^{-0\cdot s}) x_s}{\sqrt{p}}, \frac{x_0 + \sum_{s=1}^{q} (\xi_p^{1\cdot s} + \xi_p^{-1\cdot s}) x_s}{\sqrt{p}}, \ldots, \frac{x_0 + \sum_{s=1}^{q} (\xi_p^{q\cdot s} + \xi_p^{-q\cdot s}) x_s}{\sqrt{p}} \right). \tag{3}$$

Equation (3) shows that the Lee weight enumerators of linear self-dual codes over $\mathbb{Z}_p$ are invariant under the transform

$$\sigma_p : \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_q \end{pmatrix} \longmapsto \frac{1}{\sqrt{p}} \begin{pmatrix} 1 & \xi_p^{0\cdot 1} + \xi_p^{-0\cdot 1} & \cdots & \xi_p^{0\cdot q} + \xi_p^{-0\cdot q} \\ 1 & \xi_p^{1\cdot 1} + \xi_p^{-1\cdot 1} & \cdots & \xi_p^{1\cdot q} + \xi_p^{-1\cdot q} \\ \vdots & \vdots & & \vdots \\ 1 & \xi_p^{q\cdot 1} + \xi_p^{-q\cdot 1} & \cdots & \xi_p^{q\cdot q} + \xi_p^{-q\cdot q} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_q \end{pmatrix}.$$

Example 3 The code C_5, which was given in Example 1, contains 5^3 codewords shown in Table 1. Then the weight enumerator of C_5 is

$$\begin{aligned} W_{C_5}(x_0, x_1, x_2) = {} & x_0^5 + 2x_0x_1^4 + 2x_0x_2^4 + 4x_0^2x_1^3 + 4x_0^2x_2^3 + 4x_0^3x_1x_2 \\ & + 8x_1^3x_2^2 + 8x_1^2x_2^3 + 10x_0^2x_1^2x_2 + 10x_0^2x_1x_2^2 + 12x_1^4x_2 \\ & + 12x_1x_2^4 + 14x_0x_1^3x_2 + 14x_0x_1x_2^3 + 20x_0x_1^2x_2^2. \end{aligned} \tag{4}$$

On the other hand, the dual code $C_5^\perp$ contains 5^2 codewords shown in Table 2. The weight enumerator of $C_5^\perp$ is

$$W_{C_5^\perp}(x_0, x_1, x_2) = x_0^5 + 2x_0^2x_1^2x_2 + 2x_0^2x_1x_2^2 + 4x_1^3x_2^2 + 4x_1^2x_2^3 + 6x_0x_1^3x_2 + 6x_0x_1x_2^3. \tag{5}$$

Substitute $(x_0 + 2x_1 + 2x_2)$, $\left(x_0 + \frac{-1+\sqrt{5}}{2}x_1 + \frac{-1-\sqrt{5}}{2}x_2\right)$, and $\left(x_0 + \frac{-1-\sqrt{5}}{2}x_1 + \frac{-1+\sqrt{5}}{2}x_2\right)$ into x_0, x_1, and x_2 of $W_{C_5}(x_0, x_1, x_2)$, respectively, then

Table 1: Lee compositions of codewords in C_5 and the numbers of codewords with them

Lee comp.	No.	Lee comp.	No.	Lee comp.	No.
(5,0,0)	1	(1,4,0)	2	(1,0,4)	2
(2,3,0)	4	(2,0,3)	4	(3,1,1)	4
(0,3,2)	8	(0,2,3)	8	(2,2,1)	10
(2,1,2)	10	(0,4,1)	12	(0,1,4)	12
(1,3,1)	14	(1,1,3)	14	(1,2,2)	20

$$
\begin{aligned}
&W_{C_5}\left(x_0+2x_1+2x_2, x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2, x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)\\
=\ &(x_0+2x_1+2x_2)^5+2\,(x_0+2x_1+2x_2)\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)^4\\
&+2\,(x_0+2x_1+2x_2)\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)^4\\
&+4\,(x_0+2x_1+2x_2)^2\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)^3\\
&+4\,(x_0+2x_1+2x_2)^2\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)^3\\
&+4\,(x_0+2x_1+2x_2)^3\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)\\
&+8\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)^3\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)^2\\
&+8\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)^2\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)^3\\
&+10\,(x_0+2x_1+2x_2)^2\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)^2\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)\\
&+10\,(x_0+2x_1+2x_2)^2\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)^2\\
&+12\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)^4\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)\\
&+12\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)^4\\
&+14\,(x_0+2x_1+2x_2)\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)^3\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)\\
&+14\,(x_0+2x_1+2x_2)\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)^3\\
&+20\,(x_0+2x_1+2x_2)\left(x_0+\tfrac{-1+\sqrt{5}}{2}x_1+\tfrac{-1-\sqrt{5}}{2}x_2\right)^2\left(x_0+\tfrac{-1-\sqrt{5}}{2}x_1+\tfrac{-1+\sqrt{5}}{2}x_2\right)^2\\
=\ &5^3W_{C_5^{\perp}}(x_0,x_1,x_2).
\end{aligned}
$$

Conversely, $W_{C_5}(x_0,x_1,x_2)$ is derived from $W_{C_5^{\perp}}(x_0,x_1,x_2)$.

Table 2: Lee compositions of codewords in $C_5^{\perp}$ and the numbers of codewords with them

Lee comp.	No.	Lee comp.	No.	Lee comp.	No.
(5,0,0)	1	(2,2,1)	2	(2,1,2)	2
(0,3,2)	4	(0,2,3)	4	(1,3,1)	6
(1,1,3)	6	—	—	—	—

Table 3: Lee compositions of codewords in C_6 and the numbers of codewords with them

Lee comp.	No.	Lee comp.	No.	Lee comp.	No.
(6,0,0)	1	(2,2,2)	60	(0,3,3)	40
(1,5,0)	12	(1,0,5)	12	—	—

Example 4 The self-dual code C_6, which was given in Example 2, contains 5^3 codewords. The Lee compositions of codewords in C_6 are shown in Table 3. Since the generator matrix of $C_6^{\perp}$ is identical with that of C_6, both the weight enumerators of C_6 and $C_6^{\perp}$ are

$$W_{C_6}(x_0,x_1,x_2) = W_{C_6^{\perp}}(x_0,x_1,x_2) = x_0^6 + 60x_0^2x_1^2x_2^2 + 40x_1^3x_2^3 + 12x_0x_1^5 + 12x_0x_2^5. \quad (6)$$

In fact, $W_{C_6}(x_0,x_1,x_2)$ is invariant under the transform σ_5:

$$\begin{aligned}
&W_{C_6}\left(\frac{x_0+2x_1+2x_2}{\sqrt{5}}, \frac{x_0+\frac{-1+\sqrt{5}}{2}x_1+\frac{-1-\sqrt{5}}{2}x_2}{\sqrt{5}}, \frac{x_0+\frac{-1-\sqrt{5}}{2}x_1+\frac{-1+\sqrt{5}}{2}x_2}{\sqrt{5}}\right)\\
&= \left(\frac{x_0+2x_1+2x_2}{\sqrt{5}}\right)^6\\
&\quad + 60\left(\frac{x_0+2x_1+2x_2}{\sqrt{5}}\right)^2\left(\frac{x_0+\frac{-1+\sqrt{5}}{2}x_1+\frac{-1-\sqrt{5}}{2}x_2}{\sqrt{5}}\right)^2\left(\frac{x_0+\frac{-1-\sqrt{5}}{2}x_1+\frac{-1+\sqrt{5}}{2}x_2}{\sqrt{5}}\right)^2\\
&\quad + 40\left(\frac{x_0+\frac{-1+\sqrt{5}}{2}x_1+\frac{-1-\sqrt{5}}{2}x_2}{\sqrt{5}}\right)^3\left(\frac{x_0+\frac{-1-\sqrt{5}}{2}x_1+\frac{-1+\sqrt{5}}{2}x_2}{\sqrt{5}}\right)^3\\
&\quad + 12\left(\frac{x_0+2x_1+2x_2}{\sqrt{5}}\right)\left(\frac{x_0+\frac{-1+\sqrt{5}}{2}x_1+\frac{-1-\sqrt{5}}{2}x_2}{\sqrt{5}}\right)^5\\
&\quad + 12\left(\frac{x_0+2x_1+2x_2}{\sqrt{5}}\right)\left(\frac{x_0+\frac{-1-\sqrt{5}}{2}x_1+\frac{-1+\sqrt{5}}{2}x_2}{\sqrt{5}}\right)^5\\
&= x_0^6 + 60x_0^2x_1^2x_2^2 + 40x_1^3x_2^3 + 12x_0x_1^5 + 12x_0x_2^5 = W_{C_6}(x_0,x_1,x_2).
\end{aligned}$$

Here, it should be noted that $\xi_5 + \xi_5^{-1} = \frac{-1+\sqrt{5}}{2}$ and $\xi_5^2 + \xi_5^{-2} = \frac{-1-\sqrt{5}}{2}$.

Equation (1) provides the relationship between the coefficients of $W_C(x_0, x_1, \ldots, x_q)$ and those of $W_{C^\perp}(x_0, x_1, \ldots, x_q)$. To indicate the relationship explicitly, we introduce the following notation in Definition 3.

Definition 3 Let us denote the expansion of $\prod_{j=0}^{q} \left(x_0 + \sum_{s=1}^{q} (\xi_p^{j\cdot s} + \xi_p^{-j\cdot s}) x_s\right)^{l_j}$ for $l = (l_0, l_1, \ldots, l_q) \in L_{p,n}$ as

$$P_{p,n}(l) = \sum_{\rho \in L_{p,n}} \mu_{p,n,l,\rho} \prod_{j=0}^{q} x_j^{\rho_j},$$

where $\sum_{\rho \in L_{p,n}}$ denotes the summation over all $\rho = (\rho_0, \rho_1, \ldots, \rho_q) \in L_{p,n}$. The polynomial $P_{p,n}(l)$ is a homogeneous polynomial of degree n in indeterminates x_0, x_1, …, x_q.

Proposition 1 *The coefficients $\mu_{p,n,l,\rho}$ have the following properties:*

(i) $$\sum_{\rho \in L_{p,n}} \mu_{p,n,l,\rho} \mu_{p,n,\rho,\lambda} = \begin{cases} p^n & \text{if } l = \lambda, \\ 0 & \text{otherwise,} \end{cases}$$

(ii) $$\sum_{\rho \in L_{p,n}} \mu_{p,n,l,\rho} = \begin{cases} p^n & \text{if } l = (n, 0, \ldots, 0), \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Replace x_s in $\prod_{j=0}^{q} \left(x_0 + \sum_{s=1}^{q} \left(\xi_p^{j\cdot s} + \xi_p^{-j\cdot s}\right) x_s\right)^{l_j}$ with $x'_s = x_0 + \sum_{r=1}^{q} \left(\xi_p^{s\cdot r} + \xi_p^{-s\cdot r}\right) x_r$ for $s = 0, 1, \ldots, q$, we obtain the following relation from Definition 3:

$$\prod_{j=0}^{q} \left\{ \left(x_0 + \sum_{r=1}^{q} \left(\xi_p^{0\cdot r} + \xi_p^{-0\cdot r}\right) x_r \right) + \sum_{s=1}^{q} \left(\xi_p^{j\cdot s} + \xi_p^{-j\cdot s}\right) \left(x_0 + \sum_{r=1}^{q} \left(\xi_p^{s\cdot r} + \xi_p^{-s\cdot r}\right) x_r \right) \right\}^{l_j}$$
$$= \sum_{\rho \in L_{p,n}} \mu_{p,n,l,\rho} \prod_{s=0}^{q} \left(x_0 + \sum_{r=1}^{q} (\xi_p^{s\cdot r} + \xi_p^{-s\cdot r}) x_r \right)^{\rho_s}. \tag{7}$$

The right-hand side of Eq. (7) is transformed into

$$\sum_{\lambda \in L_{p,n}} \left(\sum_{\rho \in L_{p,n}} \mu_{p,n,l,\rho} \mu_{p,n,\rho,\lambda} \right) \prod_{r=0}^{q} x_r^{\lambda_r}. \tag{8}$$

On the other hand, the left-hand side of Eq. (7) is equal to

$$p^n \prod_{j=0}^{q} x_j^{l_j}. \tag{9}$$

Upon comparing the coefficients of the polynomial in Eq. (8) with those in Eq. (9), we therefore obtain Property (i).

If we put $x_0 = x_1 = \cdots = x_q = 1$ in the equations

$$\prod_{j=0}^{q}\left(x_0+\sum_{s=1}^{q}(\xi_p^{j\cdot s}+\xi_p^{-j\cdot s})x_s\right)^{l_j} = \sum_{\rho\in L_{p,n}}\mu_{p,n,l,\rho}\prod_{j=0}^{q}x_j^{\rho_j} \text{ for } l=(l_0,l_1,\ldots,l_q)\in L_{p,n},$$

then we obtain Property (ii). □

By using the coefficients $\mu_{p,n,l,\rho}$, the right-hand side of Eq. (1) is rewritten as follows :

$$\begin{aligned}
&\frac{1}{p^k}W_C\left(x_0+\sum_{s=1}^{q}\left(\xi_p^{0\cdot s}+\xi_p^{-0\cdot s}\right)x_s, x_0+\sum_{s=1}^{q}\left(\xi_p^{1\cdot s}+\xi_p^{-1\cdot s}\right)x_s,\ldots,x_0+\sum_{s=1}^{q}\left(\xi_p^{q\cdot s}+\xi_p^{-q\cdot s}\right)x_s\right)\\
&=\frac{1}{p^k}\sum_{l\in L_{p,n}}W_l\prod_{j=0}^{q}\left(x_0+\sum_{s=1}^{q}\left(\xi_p^{j\cdot s}+\xi_p^{-j\cdot s}\right)x_s\right)^{l_j}\\
&=\frac{1}{p^k}\sum_{l\in L_{p,n}}W_l\left(\sum_{\rho\in L_{p,n}}\mu_{p,n,l,\rho}\prod_{j=0}^{q}x_j^{\rho_j}\right)\\
&=\frac{1}{p^k}\sum_{\rho\in L_{p,n}}\left(\sum_{l\in L_{p,n}}W_l\,\mu_{p,n,l,\rho}\right)\prod_{j=0}^{q}x_j^{\rho_j}. \qquad (10)
\end{aligned}$$

Compare the coefficients of Eq. (10) with those of the left-hand side of Eq. (1), then it is clarified that the following relation holds between the coefficients of $W_C(x_0,x_1,\ldots,x_q)$ and those of $W_{C^\perp}(x_0,x_1,\ldots,x_q)$:

$$W^{\perp}_{\rho^\perp}=\frac{1}{p^k}\sum_{l\in L_{p,n}}W_l\,\mu_{p,n,l,\rho^\perp} \text{ for all } \rho^\perp\in L_{p,n}. \qquad (11)$$

In the same way, the following relation is obtained from Eq. (2):

$$W_\rho=\frac{1}{p^{n-k}}\sum_{l^\perp\in L_{p,n}}W^{\perp}_{l^\perp}\,\mu_{p,n,l^\perp,\rho} \text{ for all } \rho\in L_{p,n}. \qquad (12)$$

Equations (11) and (12) play importaint roles in Section 4.

3 Theta series

In this section, we deal with one-variable theta series that are essential to derive the functional equations for partial Epstein zeta functions on linear codes over $\mathbb{Z}_p$ in Section 4.

Definition 4 Let τ be a complex variable in the upper half-plane $\mathbb{H}$ of $\mathbb{C}$. For $\tau \in \mathbb{H}$ and for all $\mathbf{v}_{p,n} \in \mathbb{Z}_p^n$, the theta series $\theta_{p,n}(\tau; \mathbf{v}_{p,n})$ are defined by

$$\begin{aligned}\theta_{p,n}(\tau; \mathbf{v}_{p,n}) &:= \sum_{\substack{\mathbf{m}\in\mathbb{Z}^n \\ \mathbf{m}\equiv\mathbf{v}_{p,n} \pmod p}} \exp\left(\pi i\tau \frac{\langle \mathbf{m}, \mathbf{m}\rangle}{p}\right) \\ &= \sum_{\mathbf{m}\in\mathbb{Z}^n} \exp\left(\pi i\tau \frac{\langle p\mathbf{m}+\mathbf{v}_{p,n}, p\mathbf{m}+\mathbf{v}_{p,n}\rangle}{p}\right),\end{aligned}$$

where $\langle \mathbf{u}, \mathbf{v}\rangle$ is the standard inner product of $\mathbf{u}$ and $\mathbf{v}$.

The following relation holds for $j = 0, 1, \ldots, q$:

$$\theta_{p,1}(\tau; j) = \theta_{p,1}(\tau; p-j),$$

where $\theta_{p,1}(\tau; j) = \sum_{m\in\mathbb{Z}} \exp(\pi i\tau(pm+j)^2/p)$. Therefore, if $\mathbf{v}_{p,n}$ has Lee composition l, the theta series $\theta_{p,n}(\tau; \mathbf{v}_{p,n})$ consists of the powers of $\theta_{p,1}(\tau; 0)$, $\theta_{p,1}(\tau; 1)$, …, $\theta_{p,1}(\tau; q)$:

$$\theta_{p,n}(\tau; \mathbf{v}_{p,n}) = \theta_{p,1}(\tau; 0)^{l_0}\theta_{p,1}(\tau; 1)^{l_1}\cdots\theta_{p,1}(\tau; q)^{l_q} = \prod_{j=0}^{q} \theta_{p,1}(\tau; j)^{l_j}. \tag{13}$$

Let $\mathbf{u}_{p,n,l} = (0, \ldots, 0, 1, \ldots, 1, \ldots, q, \ldots, q) \in \mathbb{Z}_p^n$ such that l_0 zero, l_1 one, …, l_q q are aligned in $\mathbf{u}_{p,n,l}$ in this order from left to right. Then the theta series $\theta_{p,n}(\tau; \mathbf{v}_{p,n})$ is equal to $\theta_{p,n}(\tau; \mathbf{u}_{p,n,l})$. Hereinafter, we deal with the theta series in Definition 4.

Definition 5 Let τ be a complex variable in $\mathbb{H}$. Let $U_{p,n} = \{\mathbf{u}_{p,n,l} \mid l = (l_0, l_1, \ldots, l_q)$ with $l_0, l_1, \ldots, l_q \geq 0$ and $l_0 + l_1 + \cdots + l_q = n\}$. For $\tau \in \mathbb{H}$, the theta series $\theta_{p,n}(\tau; \mathbf{u}_{p,n,l})$ for $l = (l_0, l_1, \ldots, l_q) \in L_{p,n}$ are defined by

$$\begin{aligned}\theta_{p,n}(\tau; \mathbf{u}_{p,n,l}) &:= \sum_{\substack{\mathbf{m}\in\mathbb{Z}^n \\ \mathbf{m}\equiv\mathbf{u}_{p,n,l} \pmod p}} \exp\left(\pi i\tau \frac{\langle \mathbf{m}, \mathbf{m}\rangle}{p}\right) \\ &= \sum_{\mathbf{m}\in\mathbb{Z}^n} \exp\left(\pi i\tau \frac{\langle p\mathbf{m}+\mathbf{u}_{p,n,l}, p\mathbf{m}+\mathbf{u}_{p,n,l}\rangle}{p}\right).\end{aligned}$$

Proposition 2 *The theta series $\theta_{p,n}(\tau; \mathbf{u}_{p,n,l})$ for all $\mathbf{u}_{p,n,l} \in U_{p,n}$ satisfy the following two transformation formulae:*

(i) $\theta_{p,n}(\tau + 2; \mathbf{u}_{p,n,l}) = \xi_p^{\sum_{j=1}^q j^2 l_j}\theta_{p,n}(\tau; \mathbf{u}_{p,n,l})$,

(ii) $\theta_{p,n}\left(\frac{-1}{\tau}; \mathbf{u}_{p,n,l}\right) = \left(\sqrt{\frac{\tau}{i}}\right)^n \frac{1}{\sqrt{p^n}} \sum_{\rho\in L_{p,n}} \mu_{p,n,l,\rho}\theta_{p,n}(\tau; \mathbf{u}_{p,n,\rho})$,

where $i = \sqrt{-1}$, $-\pi/4 < \arg\sqrt{\tau/i} < \pi/4$, and $\mu_{p,n,l,\rho}$ denotes the constants in Definition 3.

Proof. The first formula follows directly from the definition of $\theta_{p,n}(\tau; \mathbf{u}_{p,n,l})$.

To obtain the second formula, the Poisson summation formula is applied to the function $f\left(\sqrt{\frac{t}{p}}(p\mathbf{x}+\mathbf{u}_{p,n,l})\right)$ with $f(\mathbf{x}) = e^{-\pi\langle \mathbf{x},\, \mathbf{x}\rangle}$ for $t > 0$. Let us denote $f\left(\sqrt{\frac{t}{p}}(p\mathbf{x}+\mathbf{u}_{p,n,l})\right)$ as follows:

$$g_(\mathbf{x}) = f\left(\sqrt{\frac{t}{p}}(p\mathbf{x}+\mathbf{u}_{p,n,l})\right).$$

Then the Fourier transform $\widehat{g}(\mathbf{x})$ of $g(\mathbf{x})$ is

$$\widehat{g}(\mathbf{y}) = \frac{1}{(\sqrt{pt})^n}\xi_p^{\langle \mathbf{u}_{p,n,l},\mathbf{y}\rangle}\exp\left(-\pi\frac{1}{pt}\langle \mathbf{y},\mathbf{y}\rangle\right).$$

By using the Poisson summation formula, the following relation is obtained:

$$\sum_{\mathbf{m}\in\mathbb{Z}^n}\exp\left(-\pi t\frac{\langle p\mathbf{m}+\mathbf{u}_{p,n,l},\, p\mathbf{m}+\mathbf{u}_{p,n,l}\rangle}{p}\right) = \frac{1}{(\sqrt{pt})^n}\sum_{\mathbf{m}\in\mathbb{Z}^n}\xi_p^{\langle \mathbf{u}_{p,n,l},\,\mathbf{m}\rangle}\exp\left(-\pi\frac{1}{t}\frac{\langle \mathbf{m},\,\mathbf{m}\rangle}{p}\right). \tag{14}$$

Equation (14) still holds for $\tau \in \mathbb{H}$ by the principle of analytic continuation. That is, both sides of Eq. (14) are analytic functions of τ/i on the right half-plane. Equation (14) and the analytically continued function of it must be equal everywhere for $\Re(\tau/i) > 0$, because these two functions agree on the positive real axis of a complex plane. Therefore we obtain the relation

$$\sum_{\mathbf{m}\in\mathbb{Z}^n}\exp\left(\pi i\tau\frac{\langle p\mathbf{m}+\mathbf{u}_{p,n,l},\, p\mathbf{m}+\mathbf{u}_{p,n,l}\rangle}{p}\right) = \left(\sqrt{\frac{i}{p\tau}}\right)^n\sum_{\mathbf{m}\in\mathbb{Z}^n}\xi_p^{\langle \mathbf{u}_{p,n,l},\,\mathbf{m}\rangle}\exp\left(\pi i\frac{-1}{\tau}\frac{\langle \mathbf{m},\,\mathbf{m}\rangle}{p}\right), \tag{15}$$

where $-\pi/4 < \arg\sqrt{\tau/i} < \pi/4$. The summation on the left-hand side of Eq. (15) is $\theta_{p,n}(\tau; \mathbf{u}_{p,n,l})$. On the other hand, the summation on the right-hand side of Eq. (15) is expressed by the linear combination of $\theta_{p,n}(\frac{-1}{\tau}; \mathbf{u}_{p,n,l})$ for $\mathbf{u}_{p,n,l} \in U_{p,n}$ as follows:

$$\sum_{\mathbf{m}\in\mathbb{Z}^n}\xi_p^{\langle \mathbf{u}_{p,n,l},\,\mathbf{m}\rangle}\exp\left(\pi i\frac{-1}{\tau}\frac{\langle \mathbf{m},\,\mathbf{m}\rangle}{p}\right) = \sum_{\rho\in L_{p,n}}\mu_{p,n,l,\rho}\,\theta_{p,n}\left(\frac{-1}{\tau}; \mathbf{u}_{p,n,\rho}\right). \tag{16}$$

Finally, the following relations are obtained for all $\mathbf{u}_{p,n,l} \in U_{p,n}$:

$$\theta_{p,n}(\tau; \mathbf{u}_{p,n,l}) = \left(\sqrt{\frac{i}{\tau}}\right)^n\frac{1}{\sqrt{p^n}}\sum_{\rho\in L_{p,n}}\mu_{p,n,\rho}\theta_{p,n}\left(\frac{-1}{\tau}; \mathbf{u}_{p,n,\rho}\right).$$

From Proposition 1 (ii), the second transformation formula is obtained. □

4 Epstein zeta functions on linear codes over $\mathbb{Z}_p$

Definition 6 (Epstein zeta functions [9]) Let s be a complex variable with $\Re s > n/2$, let Y be an $n \times n$ matrix of a positive definite quadratic form, and let $\mathbf{g}$ and $\mathbf{h}$ be n-dimensional real vectors. Then the Epstein zeta function associated with $(Y, \mathbf{g}, \mathbf{h})$ is defined by

$$Z_n(Y, \mathbf{g}, \mathbf{h}, s) := \sum_{\substack{\mathbf{a} \in \mathbb{Z}^n \\ \mathbf{a}+\mathbf{g} \neq \mathbf{0}_n}} \frac{e^{2\pi i \langle \mathbf{h}, \mathbf{a} \rangle}}{\left({}^t(\mathbf{a}+\mathbf{g})\, Y\, (\mathbf{a}+\mathbf{g})\right)^s},$$

where $\mathbf{a}$ runs over all elements in $\mathbb{Z}^n$ except for any vectors such that $\mathbf{a} + \mathbf{g} = \mathbf{0}_n$, and $\mathbf{0}_n$ is the n-dimensional zero vector.

Let us substitute the $n \times n$ identity matrix I_n into Y and substitute $\mathbf{0}_n$ into $\mathbf{g}$ and $\mathbf{h}$, respectively. Then we have

$$Z_n(I_n, \mathbf{0}_n, \mathbf{0}_n, s) = \sum_{\substack{\mathbf{a} \in \mathbb{Z}^n \\ \mathbf{a} \neq \mathbf{0}_n}} \frac{1}{\langle \mathbf{a},\, \mathbf{a} \rangle^s},$$

where $\langle \mathbf{a},\, \mathbf{a} \rangle$ denotes the standard inner product of $\mathbf{a}$ and itself. We denote the function $Z_n(I_n, \mathbf{0}_n, \mathbf{0}_n, s)$ by $Z_n(s)$ and define the partial Epstein zeta functions of $Z_n(s)$ as follows.

Definition 7 (Partial Epstein zeta functions) Let s be a complex variable with $\Re s > n/2$. Partial Epstein zeta functions $Z_{p,n}(s; \mathbf{u}_{p,n,l})$ for $\mathbf{u}_{p,n,l} \in U_{p,n}$ are defined by

$$Z_{p,n}(s; \mathbf{u}_{p,n,l}) := \sum_{\substack{\mathbf{m} \in \mathbb{Z}^n \\ p\mathbf{m} + \mathbf{u}_{p,n,l} \neq \mathbf{0}_n}} \frac{1}{\langle p\mathbf{m} + \mathbf{u}_{p,n,l},\, p\mathbf{m} + \mathbf{u}_{p,n,l} \rangle^s},$$

where the vectors $\mathbf{u}_{p,n,l}$ are those given in Definition 5.

It should be noted that

$$Z_{p,1}(s; j) = Z_{p,1}(s; p - j) \text{ for } j = 1, 2, \ldots, q.$$

If the Lee composition of $\mathbf{v}_{p,n} \in \mathbb{Z}_p$ is l, then

$$Z_{p,n}(s; \mathbf{v}_{p,n}) = Z_{p,n}(s; \mathbf{u}_{p,n,l}).$$

Theorem 2 *Partial Epstein zeta functions $Z_{p,n}(s; \mathbf{u}_{p,n,l})$ for all $\mathbf{u}_{p,n,l} \in U_{p,n}$, which are defined for $\Re s > n/2$, extend analytically to entire functions on the whole complex s-plane except for a simple pole at $s = n/2$ with residue $(\pi/p^2)^{n/2}/\Gamma(n/2)$, where $\Gamma(s)$ is the gamma function. Let*

$$\Lambda_{p,n}(s; \mathbf{u}_{p,n,l}) := \left(\frac{\pi}{p}\right)^{-s} \Gamma(s)\, Z_{p,n}(s; \mathbf{u}_{p,n,l}).$$

Then the following relation holds for all $\mathbf{u}_{p,n,l} \in U_{p,n}$*:*

$$\Lambda_{p,n}(s; \mathbf{u}_{p,n,l}) = \frac{1}{\sqrt{p^n}} \sum_{\rho \in L_{p,n}} \mu_{p,n,\rho} \Lambda_{p,n}\left(\frac{n}{2} - s; \mathbf{u}_{p,n,\rho}\right), \tag{17}$$

where $\mu_{p,n,l,\rho}$ *is the constant given in Definition 3. These relations for all* $\mathbf{u}_{p,n,l} \in U_{p,n}$ *are equivalent to the following single equation:*

$$\left(\frac{\pi}{p}\right)^{-s} \Gamma(s)\, Z_{p,n}(s; \mathbf{u}_{p,n,l}) = \left(\frac{\pi}{p}\right)^{-(n/2-s)} \Gamma\left(\frac{n}{2} - s\right) \frac{1}{\sqrt{p^n}} \sum_{\rho \in L_{p,n}} \mu_{p,n,l,\rho} Z_{p,n}\left(\frac{n}{2} - s; \mathbf{u}_{p,n,\rho}\right). \tag{18}$$

Proof. The proof of Eq. (18) is closely parallel to that of the functional equation for the Riemann zeta function in [10]. □

The above type of partial Epstein zeta functions are components of partial Epstein zeta functions on linear codes over $\mathbb{Z}_p$ which are defined as follows.

Definition 8 (Partial Epstein zeta functions on linear codes over $\mathbb{Z}_p$) Let C be an $[n, k]$ linear code over $\mathbb{Z}_p$ and let $\Lambda_p(C)$ be the following set:

$$\Lambda_p(C) := \{\mathbf{c} + p\mathbf{m} \mid \mathbf{c} \in C \text{ and } \mathbf{m} \in \mathbb{Z}^n\}.$$

For a complex variable $s \in \mathbb{C}$ with $\Re s > n/2$, the partial Epstein zeta function on C is defined by

$$Z_{\Lambda_p(C)}(s) := \sum_{\substack{\mathbf{r} \in \Lambda_p(C) \\ \mathbf{r} \neq \mathbf{0}_n}} \frac{1}{\langle \mathbf{r}, \mathbf{r} \rangle^s} = \sum_{\mathbf{c} \in C} \sum_{\substack{\mathbf{m} \in \mathbb{Z}^n \\ p\mathbf{m} + \mathbf{c} \neq \mathbf{0}_n}} \frac{1}{\langle p\mathbf{m} + \mathbf{c}, p\mathbf{m} + \mathbf{c} \rangle^s}.$$

In the same way, for the dual code $C^\perp$ of C, the set $\Lambda_p(C^\perp)$ is defined by

$$\Lambda_p(C^\perp) := \left\{\mathbf{c}' + p\mathbf{m} \mid \mathbf{c}' \in C^\perp \text{ and } \mathbf{m} \in \mathbb{Z}^n\right\}.$$

For a complex variable $s \in \mathbb{C}$ with $\Re s > n/2$, the partial Epstein zeta function on $C^\perp$ is defined by

$$Z_{\Lambda_p(C^\perp)}(s) := \sum_{\substack{\mathbf{r}' \in \Lambda_p(C^\perp) \\ \mathbf{r}' \neq \mathbf{0}_n}} \frac{1}{\langle \mathbf{r}', \mathbf{r}' \rangle^s} = \sum_{\mathbf{c}' \in C} \sum_{\substack{\mathbf{m} \in \mathbb{Z}^n \\ p\mathbf{m} + \mathbf{c}' \neq \mathbf{0}_n}} \frac{1}{\langle p\mathbf{m} + \mathbf{c}', p\mathbf{m} + \mathbf{c}' \rangle^s}.$$

Sorting the order of the components of $\mathbf{u}_{p,n,l}$ does not change the summation $Z_{p,n}(s; \mathbf{u}_{p,n,l})$. Therefore replacing $\mathbf{u}_{p,n,l}$ in $Z_{p,n}(s; \mathbf{u}_{p,n,l})$ with a codeword $\mathbf{c}$ of Lee weight j does not change $Z_{p,n}(s; \mathbf{u}_{p,n,l})$. If the Lee weight enumerator of C is $W_C(x_0, x_1, \ldots, x_q) = \sum_{l \in L_{p,n}} W_l \prod_{j=0}^{q} x_j^{l_j}$, then $Z_{\Lambda_p(C)}(s)$ is denoted by using the coefficients W_l of $W_C(x_0, x_1, \ldots, x_q)$:

$$Z_{\Lambda_p(C)}(s) = \sum_{l \in L_{p,n}} W_l \sum_{\substack{\mathbf{m} \in \mathbb{Z}^n \\ p\mathbf{m} + \mathbf{u}_{p,n,l} \neq \mathbf{0}_n}} \frac{1}{\langle p\mathbf{m} + \mathbf{u}_{p,n,l},\ p\mathbf{m} + \mathbf{u}_{p,n,l} \rangle^s} = \sum_{l \in L_{p,n}} W_l Z_{p,n}(s; \mathbf{u}_{p,n,l}). \tag{19}$$

In the same way, for the Lee weight enumerator $W_{C^\perp}(x_0, x_1, \ldots, x_q) = \sum_{l^\perp \in L_{p,n}} W_{l^\perp}^\perp \prod_{j=0}^q x_j^{l_j^\perp}$ of $C^\perp$, the partial Epstein zeta function $Z_{\Lambda_p(C^\perp)}(s)$ is denoted as

$$\begin{aligned} Z_{\Lambda_p(C^\perp)}(s) &= \sum_{l^\perp \in L_{p,n}} W_{l^\perp}^\perp \sum_{\substack{\mathbf{m}\in\mathbb{Z}^n \\ p\mathbf{m}+\mathbf{u}_{p,n,l^\perp}\neq \mathbf{0}_n}} \frac{1}{\left\langle p\mathbf{m}+\mathbf{u}_{p,n,l^\perp},\ p\mathbf{m}+\mathbf{u}_{p,n,l^\perp}\right\rangle^s} \\ &= \sum_{l^\perp \in L_{p,n}} W_{l_j^\perp}^\perp Z_{p,n}(s; \mathbf{u}_{p,n,l^\perp}). \end{aligned} \tag{20}$$

The following Theorem 3 is the main result in this paper.

Theorem 3 *The partial Epstein zeta function $Z_{\Lambda_p(C)}(s)$ extends analytically to an entire function on the whole complex plane except for a simple pole at $s = n/2$ with residue $p^k(\pi/p^2)^{n/2}/\Gamma(n/2)$. Then $Z_{\Lambda_p(C)}(s)$ satisfies the following functional equation:*

$$\left(\frac{\pi}{p}\right)^{-s} \Gamma(s) \frac{1}{\sqrt{p^k}} Z_{\Lambda_p(C)}(s) = \left(\frac{\pi}{p}\right)^{-(n/2-s)} \Gamma\left(\frac{n}{2}-s\right) \frac{1}{\sqrt{p^{n-k}}} Z_{\Lambda_p(C^\perp)}\left(\frac{n}{2}-s\right).$$

In particular, if C is self-dual, we have

$$\left(\frac{\pi}{p}\right)^{-s} \Gamma(s)\, Z_{\Lambda_p(C)}(s) = \left(\frac{\pi}{p}\right)^{-(n/2-s)} \Gamma\left(\frac{n}{2}-s\right) Z_{\Lambda_p(C)}\left(\frac{n}{2}-s\right)$$

and the residue of $Z_{\Lambda_p(C)}(s)$ at the pole $s = n/2$ is $(\pi/p)^{n/2}/\Gamma(n/2)$.

Proof. Let us substitute Eq. (12) into $Z_{\Lambda_p(C)}(s)$. We then have

$$\begin{aligned} Z_{\Lambda_p(C)}(s) &= \sum_{l\in L_{p,n}} W_l Z_{p,n}(s; \mathbf{u}_{p,n,l}) \\ &= \sum_{l\in L_{p,n}} \left(\frac{1}{p^{n-k}} \sum_{l^\perp \in L_{p,n}} \mu_{p,n,l^\perp,l} W_{l^\perp}^\perp \right) Z_{p,n}(s; \mathbf{u}_{p,n,l}) \\ &= \frac{1}{p^{n-k}} \sum_{l^\perp \in L_{p,n}} \left(\sum_{l\in L_{p,n}} \mu_{p,n,l^\perp,l} Z_{p,n}(s; \mathbf{u}_{p,n,l}) \right) W_{l^\perp}^\perp \end{aligned} \tag{21}$$

Multiplying both sides of Eq. (21) by $(\pi/p)^{-s}\Gamma(s)/\sqrt{p^k}$ yields

$$\begin{aligned} &\left(\frac{\pi}{p}\right)^{-s} \Gamma(s) \frac{1}{\sqrt{p^k}} Z_{\Lambda(C)}(s) \\ &= \left(\frac{\pi}{p}\right)^{-s} \Gamma(s) \frac{1}{p^{n-k}\sqrt{p^k}} \sum_{l^\perp \in L_{p,n}} \left(\sum_{l\in L_{p,n}} \mu_{p,n,l^\perp,l} Z_{p,n}(s; \mathbf{u}_{p,n,l}) \right) W_{l^\perp}^\perp. \end{aligned} \tag{22}$$

Using Eq. (18), the right-hand side of Eq. (22) is rewritten as

$$\left(\frac{\pi}{p}\right)^{-(n/2-s)} \Gamma\left(\frac{n}{2}-s\right) \frac{1}{\sqrt{p^{n-k}}} Z_{\Lambda_p(C^\perp)}\left(\frac{n}{2}-s\right). \tag{23}$$

The residue of $Z_{\Lambda_p(C)}(s)$ at the pole $s = n/2$ is the sum of those of $Z_{p,n}(s; \mathbf{u}_{p,n,l})$. Therefore the residue of $Z_{\Lambda_p(C)}(s)$ at the pole $s = n/2$ is $p^k \left(\pi/p^2\right)^{n/2} / \Gamma(n/2)$. In particular, if in Eq. (23) $C = C^\perp$, the equation becomes

$$\left(\frac{\pi}{p}\right)^{-s} \Gamma(s)\, Z_{\Lambda_p(C)}(s) = \left(\frac{\pi}{p}\right)^{-(n/2-s)} \Gamma\left(\frac{n}{2}-s\right) Z_{\Lambda_p(C)}\left(\frac{n}{2}-s\right).$$

Put $k = n/2$ into $p^k \left(\pi/p^2\right)^{n/2} / \Gamma(n/2)$, then the residue of $Z_{\Lambda_p(C)}(s)$ at the pole $s = n/2$ is $(\pi/p)^{n/2} / \Gamma(n/2)$. □

Example 5 For all $s \in \mathbb{C}$ with $\Re s > 5/2$, the partial Epstein zeta function on the code C_5 given in Example 1 is

$$\begin{aligned} Z_{\Lambda(C_5)}(s) = {} & Z_{5,5}(s;(5,0,0)) + 2Z_{5,5}(s;(1,4,0)) + 2Z_{5,5}(s;(1,0,4)) + 4Z_{5,5}(s;(2,3,0)) \\ & + 4Z_{5,5}(s;(2,0,3)) + 4Z_{5,5}(s;(3,1,1)) + 8Z_{5,5}(s;(0,3,2)) + 8Z_{5,5}(s;(0,2,3)) \\ & + 10Z_{5,5}(s;(2,2,1)) + 10Z_{5,5}(s;(2,1,2)) + 12Z_{5,5}(s;(0,4,1)) \\ & + 12Z_{5,5}(s;(0,1,4)) + 14Z_{5,5}(s;(1,3,1)) + 14Z_{5,5}(s;(1,1,3)) \\ & + 20Z_{5,5}(s;(1,2,2)). \end{aligned}$$

On the other hand, the partial Epstein zeta function on the dual code $C_5^\perp$ is

$$\begin{aligned} Z_{\Lambda(C_5^\perp)}(s) = {} & Z_{5,5}(s;(5,0,0)) + 2Z_{5,5}(s;(2,2,1)) + 2Z_{5,5}(s;(2,1,2)) \\ & + 4Z_{5,5}(s;(0,3,2)) + 4Z_{5,5}(s;(0,2,3)) + 6Z_{5,5}(s;(1,3,1)) + 6Z_{5,5}(s;(1,1,3)). \end{aligned}$$

Two zeta functions $Z_{\Lambda(C_5)}(s)$ and $Z_{\Lambda(C_5^\perp)}(s)$ satisfy the equation

$$\left(\frac{\pi}{p}\right)^{-s} \Gamma(s) \frac{1}{\sqrt{5^3}} Z_{\Lambda(C_5)}(s) = \left(\frac{\pi}{p}\right)^{-(5/2-s)} \Gamma\left(\frac{5}{2}-s\right) \frac{1}{\sqrt{5^2}} Z_{\Lambda(C_5^\perp)}\left(\frac{5}{2}-s\right).$$

Example 6 For all $s \in \mathbb{C}$ with $\Re s > 3$, the partial Epstein zeta function on C_6 given in Example 2 is

$$\begin{aligned} Z_{\Lambda(C_6)}(s) = {} & Z_{5,6}(s;(6,0,0)) + 60Z_{5,6}(s;(2,2,2)) + 40Z_{5,6}(s;(0,3,3)) \\ & + 12Z_{5,6}(s;(1,5,0)) + 12Z_{5,6}(s;(1,0,5)). \end{aligned}$$

This zeta function satisfies the functional equation

$$\left(\frac{\pi}{p}\right)^{-s} \Gamma(s)\, Z_{\Lambda(C_6)}(s) = \left(\frac{\pi}{p}\right)^{-(3-s)} \Gamma(3-s)\, Z_{\Lambda(C_6)}(3-s).$$

References

[1] B. V. Asch and F. Martens, "Lee weight enumerators of self-dual codes and theta functions," *Adv. Math. Commun.*, **2** (2008), 393–402.

[2] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura, "Type II codes, even unimodular lattices, and invariant rings," *IEEE Trans. Inform. Theory*, **45** (1999), 1194–1205.

[3] E. Bannai and M. Ozeki, "Construction of Jacobi forms from certain combinatorial polynomials," *Proc. Japan. Acad. Ser. A Math. Sci.*, **72** (1996), 12–15.

[4] M. Broué and M. Enguehard, "Polynômes des poids de certains codes et fonctions theta de certains réseaux," *Ann. Sci. Éc. Norm. Supér. (4)*, **5** (1972), 157–181.

[5] Y. Choie and N. Kim, "The complete weight enumerator of Type II codes over $\mathbb{Z}_{2m}$ and Jacobi forms," *IEEE Trans. Inform. Theory*, **47** (2001), 396–399.

[6] Y. Choie and P. Solé, "Ternary codes and Jacobi forms," *Discrete Math.*, **282** (2004), 81–87.

[7] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer-Verlag, New York, 1999.

[8] W. Ebeling, *Lattices and Codes*, a course partially based on lectures by F. Hirzebruch, 2nd rev. ed., Vieweg, (2002).

[9] P. Epstein, "Zur Theorie allgemeiner Zetafunctionen," *Math. Ann.*, **56** (1903), 615–644.

[10] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, 2nd ed., Springer-Verlag, New York, 1993.

[11] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic code," *Bell Syst. Tech. J.*, **42** (1963), 79–94.

[12] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[13] D. P. Maher, "Lee polynomials of codes and theta functions of lattices," *Canad. J. Math.*, **30** (1978), 738–747.

[14] D. P. Maher, "Modular forms from codes," *Canad. J. Math.*, **32** (1980), 40–58.

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

[16] K. Suzuki, "Complete m-spotty weight enumerators of binary codes, Jacobi forms, and partial Epstein zeta functions," *Discrete Math.*, **312** (2012), 265–278.

[17] K. Suzuki, "Partial Epstein zeta functions on binary linear codes and their functional equations," Functions in Number Theory and Their Probabilistic Aspects — Kyoto 2010, *RIMS Kôkyûroku Bessatsu*, **B34** (Autumn 2012), by RIMS, Kyoto Univ. (to appear).

有限群の部分群族とパス代数の表現

－共同研究：山口大学 飯寄信保 氏－

千葉大学（教育） 澤辺正人

0 はじめに

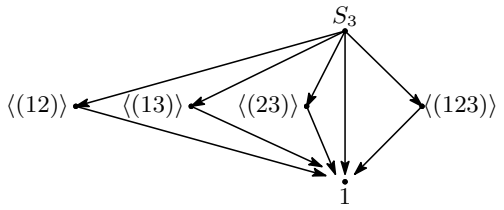
この原稿は平成２４年６月２０日（水）に筆者が行った講演の再現である。まず最初に今回の話に至った動機を説明する。次にパス代数やその表現、あるいはパス代数上の加群に関する一般的な設定をする。さらにその応用として部分群全体からなる族を考える。最後にここでの題目からは少し外れてしまうが、群指標への応用についても一言述べる。なお本稿及びその他の結果に関する詳細は [IS12] を参照されたい。

1 動機

記号を準備する。G を有限群とする。$\mathrm{Sgp}(G)$ で G の部分群全体からなる族を表す。G の部分群族 $\mathcal{H} \subseteq \mathrm{Sgp}(G)$ に対して $\Delta(\mathcal{H})$ は $\mathcal{H}$ に属する部分群からなる包含列全体の集合とする。即ち

$$\Delta(\mathcal{H}) := \{(H_0 > H_1 > \cdots > H_m) \mid H_i \in \mathcal{H},\ m \geq 0\}$$

と定める。このとき組 $(\mathcal{H}, \Delta(\mathcal{H}))$ には $\mathcal{H}$ を頂点集合、$\Delta(\mathcal{H})$ を単体集合とする有限抽象単体複体の構造が入る。そこでこの複体 $(\mathcal{H}, \Delta(\mathcal{H}))$ を G の部分群複体と呼ぶ。即ち部分群複体は部分群族 $\mathcal{H}$ を取るごとに定義されるものである。この部分群複体に関してはこれまで特に p-部分群に着目して研究を進めてきた。具体的には複体の間のホモトピー同値性や、複体から定義される Lefschetz 加群の構造、さらには山形大学の小田文仁氏との共同研究において一般バーンサイド環との関連等を追求してきた。このようにトポロジカルなことに加えて、表現論や代数系に関わる対象は既に出てきているが、さらに代数や表現論を用いた、より直接的な考察がしたいということである。そこで以下に示す 3 次対称群 S_3 の部分群全体 $\mathrm{Sgp}(S_3)$ からなる部分群複体を用いて説明する。



部分群複体と見なす場合は矢印の向きは無いものとする。この複体は 6 点の 0-単体（頂点）、9 本 の 1-単体、4 枚の 2-単体によって構成されている。ここで改めて矢印の定義であるが、上記の図から明らかなように $H_1, H_2 \in \mathrm{Sgp}(S_3)$ に対して $H_1 > H_2$ なるときに $H_1 \to H_2$ と定める。そこで $(Q_{S_3})_0$ を部分群全体 $\mathrm{Sgp}(S_3)$ としこれを頂点集合とする。さらに $(Q_{S_3})_1$ を矢印全体の集合とする。このとき組 $Q_{S_3} := \Big((Q_{S_3})_0, (Q_{S_3})_1\Big)$ はクイバーを成す。即ち上記のような有向グラフを成す。このクイバーがあれば付随するパス代数 $\mathbb{Z}Q_{S_3}$ が定義される。そこでパス代数上の加群やその間の準同型を考察することによって部分群複体や群 G の構造などを調べようというのである。以上のことを踏まえて一般的な設定を試みる。

2 一般的な設定

2.1 パス代数 $\mathbb{Z}Q$ と R-加群 RQ_0

$Q = \Big(Q_0, Q_1, (s : Q_1 \to Q_0), (s : Q_1 \to Q_0)\Big)$ をクイバーとする。即ち Q_0 は頂点集合、Q_1 は矢印の集合、s, r は Q_1 から Q_0 への写像であり $\alpha = (a \to b) \in Q_1$ に対して $s(\alpha) := a$ および $r(\alpha) := b$ により定義されるものである。さらに Q のパス Δ とは次のような合成可能な矢印の列のことである。

$$\Delta = \Big(a_0 \overset{\alpha_1}{\to} a_1 \overset{\alpha_2}{\to} \cdots \overset{\alpha_\ell}{\to} a_\ell\Big) \quad (\alpha_i \in Q_1)$$

我々としては部分群の包含列を想定しているものである。s, r をパス上にも拡張して $s(\Delta) := a_0$ および $r(\Delta) := a_\ell$ とする。また自明なパスとして各頂点 $a \in Q_0$ に対し $\Delta = e_a$ というシンボルを置いておく。この場合 $s(e_a) := a$ および $s(e_a) := a$ と定める。さらに Q のパス代数 $\mathbb{Z}Q$ とは Q のパス全体で生成される $\mathbb{Z}$-自由加群であり、かつパスの合成により積が定義される $\mathbb{Z}$-結合代数のことである。勿論パス代数は一般の可換環上で定義されるものであるが、我々は有理整数環 $\mathbb{Z}$ 上で考察していくことから $\mathbb{Z}Q$ に着目している。さて $\mathbb{Z}Q$ の部分代数として自明なパス全体で生成される $\mathbb{Z}Q_0$ がある。

$$\mathbb{Z}Q_0 := \bigoplus_{a \in Q_0} a\mathbb{Z} \subseteq \mathbb{Z}Q$$

ここで頂点 $a \in Q_0$ と a に付随する自明なパス e_a とを同一視している。更に可換環 R に対して $\mathbb{Z}Q_0$ に R-テンソルした R-加群を

$$RQ_0 := R \otimes_{\mathbb{Z}} \mathbb{Z}Q_0$$

とする。以下パス代数 $\mathbb{Z}Q$ から R-加群 RQ_0 への作用を導入する。

2.2 $\mathbb{Z}Q$ の RQ_0 上への作用

作用を導入する前に矢印上の重み関数 w を我々独自に設定する。即ち矢印全体の集合からから可換環 R への写像 $w : Q_1 \longrightarrow R$ を設定しておく。さらに w をパス Δ 上にも拡張して

$$w(\Delta) = \begin{cases} w\Big(a_0 \overset{\alpha_1}{\to} a_1 \overset{\alpha_2}{\to} \cdots \overset{\alpha_\ell}{\to} a_\ell\Big) := w(\alpha_1) \cdots w(\alpha_\ell) \\ w(a = e_a) := 1 \end{cases}$$

と定める。ここでパス Δ に対して RQ_0 から RQ_0 への写像を次のように定義する。

$$\rho_w(\Delta) : RQ_0 \longrightarrow RQ_0 \quad \text{by} \quad a \mapsto a\Delta := w(\Delta)\Big(\delta_{a,s(\Delta)} \cdot r(\Delta)\Big)$$
$$\lambda_w(\Delta) : RQ_0 \longrightarrow RQ_0 \quad \text{by} \quad b \mapsto \Delta b := w(\Delta)\Big(\delta_{r(\Delta),b} \cdot s(\Delta)\Big)$$

まず Δ として先程の部分群の包含列を想定していることに注意する。このとき写像 $\rho_w(\Delta)$ は次のように説明出来る。即ち包含列 Δ と列の一番上にある部分群がぶつかれば、それは Δ の重み $w(\Delta)$ を拾いながら一番下の部分群に移される。それ以外は 0 の値を取る。ここで $\rho_w : \mathbb{Z}Q \longrightarrow \mathrm{End}(RQ_0)$ は各 Δ を右からぶつけていることから RQ_0 に右 $\mathbb{Z}Q$-加群の構造が入る。同様に $\lambda_w(\Delta)$ は次のように説明出来る。即ち包含列 Δ と列の一番下にある部分群がぶつかれば、それは Δ の重み $w(\Delta)$ を拾いながら一番上の部分群に移される。それ以外は 0 の値を取る。ここで $\lambda_w : \mathbb{Z}Q \longrightarrow \mathrm{End}(RQ_0)$ は各 Δ を左からぶつけていることから RQ_0 に左 $\mathbb{Z}Q$-加群の構造が入る。

そこで我々の研究対象として自己準同型環 $\mathrm{End}(RQ_0)$ の R-部分代数で $\rho_w(\Delta)$, $\lambda_w(\Delta)$ 全体で生成される $\mathsf{UD}(Q,w;R)$ を考察してはどうかということである。

$$\mathsf{UD}(Q,w;R) := \left\langle \rho_w(\Delta), \lambda_w(\Delta) \mid \Delta = \mathrm{path} \right\rangle \leq \mathrm{End}(RQ_0)$$

上で説明したように $\rho_w(\Delta)$, $\lambda_w(\Delta)$ は部分群列 Δ 上の Up-Down 作用素と呼ばれるべきものである。また R-代数 $\mathsf{UD}(Q,w;R)$ はクイバー Q, 重み関数 w, 係数環 R によって定まる対象である。以下 $\mathsf{UD}(Q,w;R)$ の構造を考察する。

2.3 R-代数 $\mathsf{UD}(Q,w;R)$ の構造

次のような自然な命題が成立している。

命題 (Proposition 3.10 in [IS12]) $\mathsf{UD}(Q,w;R)$ は以下の R-行列代数と R-代数同型である。

$$\mathsf{UD}(Q,w;R) \cong \left(\sum_{\Delta \in \mathsf{P}_{a\Rightarrow b}} w(\Delta)\cdot R \right)_{a,b\in Q_0}$$

注意 右辺の行列成分は頂点集合 Q_0 で index 付けされており (a,b) 成分は有限和 $\sum_{\Delta\in\mathsf{P}_{a\Rightarrow b}} w(\Delta)\cdot R$ の任意の要素を取るというものである。ここで $\mathsf{P}_{a\Rightarrow b}$ は頂点 a から頂点 b への矢印の向きを考えないルート全体の集合である。言い換えれば各矢印 $\alpha = (a \to b) \in Q_1$ に対して逆向きの矢印 ${}^t\alpha := (a \leftarrow b)$ を付け加えた第二のクイバーを考え、そこに於ける a から b へのパス全体の集合ということになる。

■証明の概略 パス Δ に対して $\rho_w(\Delta)$ の表現行列 $M_{\rho_w(\Delta)}$ は定義から次のようになる。

$$(M_{\rho_w(\Delta)})_{i,j} = \begin{cases} w(\Delta) & (i,j) = (s(\Delta), r(\Delta)) \\ 0 & \text{otherwise} \end{cases}$$

さらに ρ_w はパス代数上の加群を誘導することから写像の合成とパスの合成が

$$\rho_w(\Delta_1)\circ\rho_w(\Delta_2) = \rho_w(\Delta_1\Delta_2)$$

のように連動する。一方 Δ を構成する矢印の向きを全て逆にした新たなパスを Δ^{opp} で表わす。このときもう一方の $\lambda_w(\Delta)$ は $r(\Delta)$ を $s(\Delta)$ に移すことから $\lambda_w(\Delta) = \rho_w(\Delta^{\mathrm{opp}})$ が成り立つ。この場合、先の注意で述べたように拡張されたクイバーを再設定する必要があるが細かいことは省略する。以上から $\rho_w(\Delta)$ と $\lambda_w(\Delta')$ 達の積は $\rho_w(\Delta_1^*\Delta_2^*\cdots\Delta_\ell^*)$ のようになる。ここで $*$ は通常のパス Δ と Δ^{opp} が交互に現れることを意味する。即ち矢印の Up-Down が繰り返されることに他ならない。この場合の表現行列も $s(\Delta_1^*)$ と $r(\Delta_\ell^*)$ に対応する成分にのみ重みの値が来て残りは全て 0 になる。これらを全て足し合わせることにより求める同型が導かれる。

2.4 $\mathbb{Z}$-代数 $\mathsf{UD}(Q,w;\mathbb{Z})$ の構造定数

係数環 R を有理整数環 $\mathbb{Z}$ とする。このときの $\mathbb{Z}$-代数を $\mathsf{UD}(Q,w) := \mathsf{UD}(Q,w;\mathbb{Z})$ で表わす。また $\mathbb{Z}$ は単項イデアル整域であることから $a,b\in Q_0$ に対して $\sum_{\Delta\in\mathsf{P}_{a\Rightarrow b}} w(\Delta)\cdot\mathbb{Z} = \mathfrak{s}_{a,b}\mathbb{Z}$ なる非負整数 $\mathfrak{s}_{a,b}\in\mathbb{Z}$ が一意的に存在する。即ち先の命題と合わせると次の $\mathbb{Z}$-代数同型を得る。

$$\mathsf{UD}(Q,w) \cong (\mathfrak{s}_{a,b}\mathbb{Z})_{a,b\in Q_0}$$

つまり $\{\mathfrak{s}_{a,b}\}_{a,b\in Q_0}$ は $\mathsf{UD}(Q,w)$ の構造を決定するものであることからこれを $\mathsf{UD}(Q,w)$ の**構造定数**と呼ぶことにする。そこでこの場合の具体的な研究課題はこの構造定数 $\{\mathfrak{s}_{a,b}\}_{a,b\in Q_0}$ の性質を調べるということになる。以上のことを踏まえて群 G の部分群全体からなる族への応用を考える。

3 $\mathsf{Sgp}(G)$ への応用

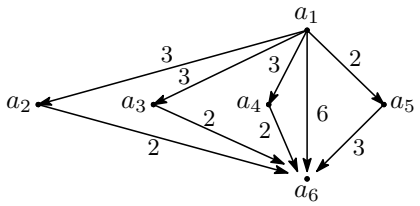
3.1 $\mathsf{Sgp}(G)$ に付随するクイバー Q_G

第 1 節で述べた 3 次対称群の例に於ける記号を改めて整理する。$(Q_G)_0$ を部分群全体 $\mathrm{Sgp}(G)$ としこれを頂点集合とする。$(Q_G)_1$ を矢印全体の集合とする。ここで $K,H\in(Q_G)_0$ に対して $H>K$ なるときに矢印 $H\to K$ を定義する。このとき $Q_G:=\big(\,(Q_G)_0,\ (Q_G)_1,\ s,\ r\,\big)$ はクイバーを成す。更に矢印上の重み関数 $w_G:(Q_G)_1\longrightarrow\mathbb{Z}$ を部分群の指数 $w_G(H\to K):=|H:K|$ で定義する。このとき $\mathbb{Z}$-代数 $\mathsf{UD}(Q_G,w_G)$ を単に $\mathsf{UD}(G)$ と表わしこの構造定数 $\{\mathfrak{s}^G_{A,B}\}_{A,B\in(Q_G)_0}$ の性質が問題となる。まず定義から導かれる算術的な性質として次を挙げることが出来る。

補題　(1) $\mathfrak{s}^G_{A,B}$ は G の位数の約数である。
(2) $\mathfrak{s}^G_{A,B}$ は $\mathfrak{s}^H_{A,B}$ $(A,B\le H\le G)$ の約数である。
(3) $H\trianglelefteq G$ ならば $\mathfrak{s}^G_{A,B}=\mathfrak{s}^H_{A,B}$ $(A,B\le H)$ が成り立つ。

この他の様々な性質については [IS12, Section 4] を参照されたい。

■$\mathsf{UD}(S_3)$ の構造定数　再び 3 次対称群 S_3 の例を観察する。まずクイバー Q_{S_3} は次のようになる。



これは第 1 節で描いた Q_{S_3} に対してその頂点（部分群）を記号 a_i $(i=1,2,\dots,6)$ で置き換えたものである。さらに矢印上の重みとして部分群の指数が付してある。このとき $\mathsf{UD}(S_3)$ の構造定数 $\mathfrak{s}^{S_3}_{a_i,a_j}$ は次のように計算される。

$$\begin{array}{c} \\ a_1\\ a_2\\ a_3\\ a_4\\ a_5\\ a_6 \end{array}\!\!\begin{array}{c} \begin{array}{cccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array}\\ \begin{pmatrix} 1 & 3 & 3 & 3 & 2 & 6\\ 3 & 1 & 1 & 1 & 6 & 2\\ 3 & 1 & 1 & 1 & 6 & 2\\ 3 & 1 & 1 & 1 & 6 & 2\\ 2 & 6 & 6 & 6 & 1 & 3\\ 6 & 2 & 2 & 2 & 3 & 1 \end{pmatrix} \end{array}$$

第 2.3, 2.4 節で説明したように構造定数は Up-Down の両方を考慮して定義されていることから行列で書けば上記のように対称行列となる。さらに直前の補題で見たように構造定数 $\mathfrak{s}^{S_3}_{A,B}$ は群 S_3 の位数の約数になっていることが確認出来る。さてこの構造定数の中で特徴的なものは S_3 の位数 6 を与えている場合である。これを与えている組は S_3 と単位群の組、および 3-サイクルと互換の組である。言い換えれば S_3 を生成する部分群の組ということになる。ここで一般に次のことを証明することが出来る。

3.2 構造定数 $\mathfrak{s}_{A,B}^G = |G|$ の特徴付け

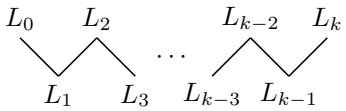
定理 (Theorem 4.14 in [IS12]) $A, B \in (Q_G)_0 = \mathrm{Sgp}(G)$ に対して次は同値である。

(1) $\mathfrak{s}_{A,B}^G = |G|$
(2) $G = AB$ and $A \cap B = \{1\}$

■証明の概略 (1) $\Rightarrow$ (2) は先の算術補題などから位数を比較して導かれる。よって問題は (2) $\Rightarrow$ (1) である。最終的には Up-Down の両方を考えた A から B への任意のパス

$$\Delta = (A =: L_0 - L_1 - \cdots - L_k := B)$$

に対して G の位数が重み $w_G(\Delta)$ を割り切ることを示せば良い。これをパスの長さ $\ell(\Delta) = k$ に関する数学的帰納法で示す。まず $k = 1$ の時は $\Delta = (A - B)$ より $w_G(\Delta) = |A : B|$ $(A > B)$ としてよい。仮定から $\{1\} = A \cap B = B$ かつ $G = AB = A$ より $w_G(\Delta) = |G|$ となる。次に $k \geq 2$ の場合は帰納法の仮定などを用いて Δ は次のようなパスに帰着される。



即ちジグザグの Up-Down パス Δ である。一方、部分群 L_i $(i = 0, 1, \ldots, k)$ から定義される coset 幾何の極大旗のようなものを考える。

$$\mathcal{F} := \Big\{ \big(g_0 L_0, \ldots, g_k L_k\big) \mid g_i L_i \subseteq g_{i+1} L_{i+1} \text{ or } g_i L_i \supseteq g_{i+1} L_{i+1} \ (0 \leq i \leq k-1) \Big\}$$

即ち coset の組であり、かつ隣り合う coset との間に包含関係があるもの全体である。このとき G が $\mathcal{F}$ 上に半正則で作用することを確認する。さらに重み $w_G(\Delta)$ と $|\mathcal{F}|$ を具体的に計算し $\sqrt{w_G(\Delta)/|G|} = |\mathcal{F}|/|G|$ を導く。ここで半正則性から $|\mathcal{F}|/|G|$ が整数となり求める結果を得る。以上が概略である。

特にこの定理の系として次が成り立つ。

系 (Corollary 4.15 in [IS12]) あるベキ零部分群 $A, B \leq G$ に対して $\mathfrak{s}_{A,B}^G = |G|$ ならば G は可解群である。

まず Scott の群論 [Sco64, 13.2.9] の中に G が 2 つのベキ零部分群の積で書けているならば G は可解群であるという結果がある。従って上記系は Scott の結果を我々の構造定数の言葉で書き換えたものに他ならない。特に構造定数は群 G の構造に色濃く反映していることが分かる。

4 群指標への応用

4.1 構造定数の特徴づけ

最後に群指標への応用について述べる。まず $(Q_G^{\mathrm{ch}})_0 := \{(H, \chi) \mid H \leq G,\ \chi \in \mathrm{Irr}(H)\}$ を部分群 $H \leq G$ と H の既約指標の組全体からなる集合とする。さらに $(K, \theta), (H, \chi) \in (Q_G^{\mathrm{ch}})_0$ に対して $K > H$ かつ $(\theta|_H, \chi)_H \neq 0$ なるとき矢印 $(K, \theta) \to (H, \chi)$ を定義する。$(Q_G^{\mathrm{ch}})_1$ を矢印全体の集合とする。このとき $Q_G^{\mathrm{ch}} := \big(\ (Q_G^{\mathrm{ch}})_0,\ (Q_G^{\mathrm{ch}})_1,\ s,\ r\ \big)$ はクイバーを成す。ここで矢印上の重み関数 $w_G^{\mathrm{ch}} : (Q_G^{\mathrm{ch}})_1 \longrightarrow \mathbb{Z}$ は指標の重複度

$$\big((K, \theta) \to (H, \chi)\big) \mapsto (\theta|_H, \chi)_H \in \mathbb{Z}$$

によって定義する。このとき $\mathbb{Z}$-代数 $\mathsf{UD}\big(Q_G^{\mathrm{ch}}, w_G^{\mathrm{ch}}\big)$ の構造定数 $\mathfrak{s}_{\mathbf{x},\mathbf{y}}$ の性質に興味が向かう。これについては Brauer の指標の特徴づけ等を用いて次を証明することが出来る。

定理 **(Theorem 5.20 in [IS12])** 任意の有限群 G と任意の頂点 $\mathbf{x}, \mathbf{y} \in (Q_G^{\mathrm{ch}})_0$ に対して対応する構造定数 $\mathfrak{s}_{\mathbf{x},\mathbf{y}}$ は 1 である。

4.2 Bratteli 作用素

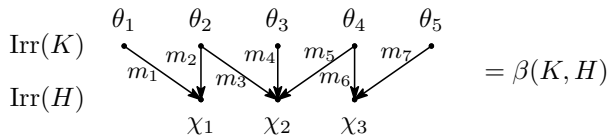
一方、既約指標の誘導と制限の操作は $\mathbb{Z}$-代数 $\mathsf{UD}\big(Q_G^{\mathrm{ch}}, w_G^{\mathrm{ch}}\big)$ の中で自然に解釈することが出来る。まず部分群 $H < K \leq G$ に対して $\mathsf{P}_{K,H}$ を次のように定義する。

$$\mathsf{P}_{K,H} := \big\{\big((K,\theta) \to (H,\chi)\big) \mid \theta \in \mathrm{Irr}(K),\ \chi \in \mathrm{Irr}(H)\big\}$$

即ち長さが 1 のパスの集まりであり、部分群 K, H を固定し、それぞれの既約指標を走らせるというものである。さらに $\beta(K,H)$ としてこれらのパスの総和をパス代数 $\mathbb{Z}Q_G^{\mathrm{ch}}$ の中で考える。

$$\beta(K,H) := \sum_{\Delta \in \mathsf{P}_{K,H}} \Delta \ \in\ \mathbb{Z}Q_G^{\mathrm{ch}}$$

具体的な絵を描くと次のような感じになる。



$= \beta(K,H)$

即ち K と H の既約指標をそれぞれ一列に並べる。さらに $\theta \in \mathrm{Irr}(K)$ を H に制限した $\theta|_H$ における $\chi \in \mathrm{Irr}(H)$ の重複度 $m = (\theta|_H, \chi)_H$ が 0 でないときに重み m と共に矢印 $\theta \to \chi$ を引くのである。これはいわゆる Bratteli 図形である。この Bratteli 図形を以下のように我々の $\mathbb{Z}$-代数 $\mathsf{UD}\big(Q_G^{\mathrm{ch}}, w_G^{\mathrm{ch}}\big)$ の要素として反映させるのである。

$$B_{\downarrow}(K,H) := \ \rho_{w_G^{\mathrm{ch}}}\big(\beta(K,H)\big), \quad B_{\uparrow}(K,H) := \ \lambda_{w_G^{\mathrm{ch}}}\big(\beta(K,H)\big)$$

即ち $B_{\downarrow}(K,H)$ はパス $\beta(K,H)$ に対して上部の頂点を下部の頂点に移す写像とする。$B_{\uparrow}(K,H)$ はパス $\beta(K,H)$ に対して下部の頂点を上部の頂点に移す写像とする。この際に $\rho_{w_G^{\mathrm{ch}}}$ と $\lambda_{w_G^{\mathrm{ch}}}$ には重みも付随していることから、例えば上記の図形を用いれば次のような計算が成り立つ。

$$\begin{aligned}
(K,\theta_2)^{B_{\downarrow}(K,H)} &= m_2(H,\chi_1) + m_3(H,\chi_2) = (H, m_2\chi_1 + m_3\chi_2) = (H, \theta_2|_H) \\
(H,\chi_2)^{B_{\uparrow}(K,H)} &= m_3(K,\theta_2) + m_4(K,\theta_3) + m_5(K,\theta_4) \\
&= (K, m_3\theta_2 + m_4\theta_3 + m_5\theta_4) = \big(K, (\chi_2)^K\big)
\end{aligned}$$

即ち $B_{\downarrow}(K,H),\ B_{\uparrow}(K,H) \in \mathsf{UD}\big(Q_G^{\mathrm{ch}}, w_G^{\mathrm{ch}}\big)$ は制限と誘導の操作に対応している。詳しくは [IS12, Section 5.1] を参照されたい。

参考文献

[IS12] N. Iiyori and M. Sawabe, Representations of path algebras with applications to subgroup lattices and group characters, preprint (version of June 21, 2012).

[Sco64] W.R. Scott, "Group theory", Prentice-Hall, Inc., Englewood Cliffs, N.J. (1964).

Kleinian codes and binary codes

Shun Tabata and Hiroki Tamura

1 Introduction

In [3], Kleinian codes, that is, additive codes over Kleinian four group is introduced, and two constructions of binary codes from Kleinian codes are given. These constructions are analogous to constructions of lattices from binary codes found in [2], [8].

In [4], a frame of an integral lattice is defined, and frames are classified into three types. A lattice generated by construction A (resp. B, C) has a frame of Type A (resp. B, C). In this paper, we define a frame and its type with respect to a binary code so that a binary code generated by each construction from a Kleinian code has a frame of the corresponding type. In fact, this definition of a frame of a binary code coincides with that of a T-decomposition in [4], but for analogies, we use the term "frame".

In Section 2–4, we give a proof of our main result:

Theorem (Theorems 5,6)**.** Let $\mathcal{D}$ be a self-orthogonal binary code of length $4n$ with a frame F_0. We assume $\mathcal{D}$ is doubly-even when F_0 is of Type C. Let $\mathcal{C}$ be a Kleinian code defined as follows:

$$\mathcal{C} = \{x \in K^n \mid (d_4^n + \iota(x, \mathbf{0})) \cap \mathcal{D} \neq \emptyset\}.$$

Then $\mathcal{D}$ can be expressed as $\rho_A(\mathcal{C})$, $\rho_{B,v}(\mathcal{C})$ and $\rho_{C,v}(\mathcal{C})$ for some $v \in K^n$ according as F_0 is of Type A, B and C respectively.

Theorem (Theorems 9,24,25)**.** Let $\mathcal{D}$ be a self-orthogonal (resp. doubly-even) binary code of length $4n$ with a frame of Type A or B (resp. Type C). Then $\mathrm{Aut}(\mathcal{D})$ is transitive on the set of all frames of the same type if we assume $4n > 16$ (resp. $4n > 32$) for Type B (resp. Type C).

Combining above two theorems, we have

Theorem. For $U = A$, B or C, a mapping $\mathcal{C} \to \rho_{U,\mathbf{0}}(\mathcal{C})$ gives a one to one correspondence from the set of all isomorphism classes of self-orthogonal (resp. even) Kleinian codes of length n to the set of all isomorphims classes of self-orthogonal (resp. doubly-even) binary codes of length $4n$ with a frame of Type U if it is assumed that $4n > 16$ (resp. $4n > 32$) for $U = B$ (resp. $U = C$).

These are analogues of the following theorems.

Theorem (Kitazume, Kondo, Miyamoto [4]). Let L be an n-dimensional even lattice with a frame $F_0 = \{\pm e_1, \ldots, \pm e_n\}$. Let $\mathcal{C}$ be a code defined as follows:

$$\mathcal{C} = \{X \subset \{1, \ldots, n\} \mid (\Lambda + \frac{1}{2} e_X) \cap L \neq \emptyset\}.$$

Then replacing some e_i by $-e_i$ if necessary, L can be expressed as $L_A(\mathcal{C})$, $L_B(\mathcal{C})$ and $L_C^\delta(\mathcal{C})$ ($\delta = 0$ or 1 and $\delta \equiv n/8 \bmod 2$) according as F_0 is of Type A, B and C respectively.

Theorem (Kitazume, Kondo, Miyamoto [4]). Let L be an n-dimensional even lattice with a frame. Then $\mathrm{Aut}(L)$ is transitive on the set of all frames of the same type if we assume $n > 16$ (resp. $n > 32$) for Type B (resp. Type C).

Theorem (Kitazume, Kondo, Miyamoto [4]). For $U = A$, B or C, a mapping $\mathcal{C} \to L_U(\mathcal{C})$ gives a one to one correspondence from the set of all isomorphism classes of doubly even codes of length n to the set of all isomorphims classes of n-dimensional even lattices with a frame of Type U if it is assumed that $n > 16$ (resp. $n > 32$) for $U = B$ (resp. $U = C$).

In Section 5, we give some examples to show that the assumption: n is sufficiently large, in our main theorem is necessary.

2 Construction of binary codes from Kleinian codes, and frames of binary codes

Let $K = \{0, a, b, c\} \cong \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ be the Kleinian four group, where 0 is the neutral element. A code $\mathcal{C}$ over K of length n is a subset of K^n, and a code $\mathcal{C}$ is called linear if $\mathcal{C}$ is a subgroup of K^n. The weight $\mathrm{wt}(x)$ of $x = (x_1, \ldots, x_n) \in K^n$ is the number of nonzero x_i. A code $\mathcal{C}$ is called even if $\mathrm{wt}(x)$ is even for all $x \in \mathcal{C}$. The scalar product $(\cdot, \cdot)$: $K^n \times K^n \to \boldsymbol{F}_2$ is defined as $(x, y) = \sum_{i=1}^n x_i \cdot y_i$, where $a \cdot b = b \cdot a = a \cdot c = c \cdot a = b \cdot c = c \cdot b = 1$ and zero otherwise.

The dual code $\mathcal{C}^\perp$ is defined by

$$\mathcal{C}^\perp = \{x \in K^n \mid (x, y) = 0 \text{ for all } y \in \mathcal{C}\}.$$

We call $\mathcal{C}$ self-orthogonal if $\mathcal{C} \subset \mathcal{C}^\perp$ and self-dual if $\mathcal{C}^\perp = \mathcal{C}$.

A binary code of length n is a subset of $\boldsymbol{F}_2^n$, and a binary code $\mathcal{D}$ is called linear if $\mathcal{D}$ is a subgroup of $\boldsymbol{F}_2^n$. A code $\mathcal{D}$ is called doubly-even if $\mathrm{wt}(x)$ is divisible by 4 for all $x \in \mathcal{D}$. We define the scalar product on $\boldsymbol{F}_2^n$ by $x \cdot y = \sum_{i=1}^n x_i y_i$ for $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \boldsymbol{F}_2^n$.

The dual code $\mathcal{D}^\perp$ is defined by

$$\mathcal{D}^\perp = \{x \in \boldsymbol{F}_2^n \mid x \cdot y = 0 \text{ for all } y \in \mathcal{D}\}.$$

We call $\mathcal{D}$ self-orthogonal if $\mathcal{D} \subset \mathcal{D}^\perp$ and self-dual if $\mathcal{D}^\perp = \mathcal{D}$.

We assume that all codes in this paper are linear.

x	$\iota(x,0)$	$\iota(x,a)$	$\iota(x,b)$	$\iota(x,c)$
0	0000	0000	0000	0000
a	0011	0011	1100	1100
b	0101	1010	0101	1010
c	0110	1001	1001	0110

Table 1:

The automorphisms of $\boldsymbol{F}_2^n$ consist of the permutation of the positions and the automorphisms of K^n consist of the permutation of the positions together with a permutation of the symbols a, b and c at each position.

For $X \subset \{1, \dots, 4n\}$, define $e_X \in \boldsymbol{F}_2^{4n}$ by

$$(e_X)_i = \begin{cases} 1 & \text{if } i \in X, \\ 0 & \text{if } i \notin X. \end{cases}$$

We denote $e_{\{x\}}$ by e_x and $e_{\{1,\dots,4n\}}$ by $\mathbf{1}$.

Let $v \in K^n$. We define maps ρ_A, $\rho_{B,v}$, $\rho_{C,v}$ from Kleinian codes of length n to binary codes of length $4n$, where $\rho_{C,v}$ is defined only for even n. The maps ρ_A and $\rho_{C,v}$ appear in [3] as ρ_A and ρ_B. For analogies to [4], we use $\rho_{C,v}$ and define a new map $\rho_{B,v}$.

Definition 1. Let $d_4^n = \{(0000), (1111)\}^n$ and $(d_4^n)_0 = \{x \in d_4^n \mid \mathrm{wt}(x) \equiv 0 \pmod 8\}$, $(d_4^n)_1 = d_4 \setminus (d_4^n)_0$.

$$\begin{aligned} \rho_A(\mathcal{C}) &:= \iota(\mathcal{C}, \mathbf{0}) + d_4^n, \\ \rho_{B,v}(\mathcal{C}) &:= \iota(\mathcal{C}, v) + (d_4^n)_0, \\ \rho_{C,v}(\mathcal{C}) &:= (\iota(\mathcal{C}, v) + (d_4^n)_0) \cup (\iota(\mathcal{C}, v) + (d_4^n)_{\delta_{n \bmod 4,2}} + \kappa(v)), \end{aligned}$$

where $\kappa : K^n \to \boldsymbol{F}_2^{4n}$ is the map induced from $\kappa : K \to \boldsymbol{F}_2^4$, $0 \mapsto (1000)$, $a \mapsto (0100)$, $b \mapsto (0010)$, $c \mapsto (0001)$, and $\iota : K^n \times K^n \to \boldsymbol{F}_2^{4n}$ is the map induced from $\iota : K \times K \to \boldsymbol{F}_2^4$, $\iota(x,v) = \kappa(0) + \kappa(x) + ((\kappa(0) + \kappa(x)) \cdot \kappa(v))\mathbf{1}$.

Note that $\rho_{B,v}(\mathcal{C})$ (resp. $\rho_{C,v}(\mathcal{C})$) is equivalent to $\rho_{B,\mathbf{0}}(\mathcal{C})$ (resp. $\rho_{C,\mathbf{0}}(\mathcal{C})$).

The following is a slightly refined version of [3, Lemma 2].

Lemma 2. If $\mathcal{C}$ is a self-orthogonal (resp. even) Kleinian code, then $\rho_U(\mathcal{C})$ $(U = A, B, C)$ is a self-orthogonal (resp. doubly-even) binary code. If $\mathcal{C}$ is self-dual, then $\rho_A(\mathcal{C})$ and $\rho_C(\mathcal{C})$ are self-dual.

Definition 3. Let $\mathcal{D}$ be a self-orthogonal binary code of length $4n$. A set $\{f_1, \dots, f_n\} \subset \boldsymbol{F}_2^{4n}$ is called a frame of $\mathcal{D}$ if all the following conditions are satisfied:

- $f_i + f_j \in \mathcal{D}$ for any $i, j \in \{1, \dots, n\}$.
- $\mathrm{wt}(f_i) = 4$ for any $i \in \{1, \dots, n\}$.

- $\mathrm{supp}(f_i) \cap \mathrm{supp}(f_j) = \emptyset$ for any distinct $i, j \in \{1, \ldots, n\}$.

Definition 4. Let F be a frame of $\mathcal{D}$. We say that F is of

- Type A: if $F \subset \mathcal{D}$,
- Type B: if $F \not\subset \mathcal{D}$ and $F \subset \mathcal{D}^\perp$,
- Type C: if $F \not\subset \mathcal{D}^\perp$.

Let $F_0 = \{e_{I_1}, \ldots, e_{I_n}\}$ where $I_i = \{4i-3, 4i-2, 4i-1, 4i\}$.

Note that $d_4^n = \sum_{f \in F_0} \boldsymbol{F}_2 f$. It is not difficult to see that $\rho_U(\mathcal{C})$ has a frame F_0 of Type U ($U = A, B, C$) for any self-orthogonal Kleinian code $\mathcal{C}$.

Theorem 5. Let $\mathcal{D}$ be a self-orthogonal binary code containing d_4^n. Let $\mathcal{C}$ be a Kleinian code defined as $\mathcal{C} = \{x \in K^n \mid (d_4^n + \iota(x, \mathbf{0})) \cap \mathcal{D} \neq \emptyset\}$. Then $\mathcal{D} = \rho_A(\mathcal{C})$.

Theorem 6. Let $\mathcal{D}$ be a self-orthogonal binary code of length $4n$ with a frame F_0 of Type U ($U = B, C$). We assume $\mathcal{D}$ is doubly-even when $U = C$. Let $\mathcal{C}$ be a Kleinian code defined as $\mathcal{C} = \{x \in K^n \mid (d_4^n + \iota(x, \mathbf{0})) \cap \mathcal{D} \neq \emptyset\}$. Then $\mathcal{D} = \rho_{U,v}(\mathcal{C})$ for some $v \in K^n$.

Proof. Let $\mathcal{C}_0 = \{x \in K^n \mid ((d_4^n)_0 + \iota(x, \mathbf{0})) \cap \mathcal{D} \neq \emptyset\}$, and $\mathcal{C}_+ = \{x \in K^n \mid (d_4^n + \kappa(x)) \cap \mathcal{D} \neq \emptyset\}$. If F_0 is of Type B, we have $\mathcal{D} = \rho_{B,v}(\mathcal{C})$ for any $v \in \mathcal{C}_0^\perp \setminus \mathcal{C}^\perp$ (resp. $v \in \mathcal{C}_0^\perp$) when $\mathcal{C}_0 \neq \mathcal{C}$ (resp. $\mathcal{C}_0 = \mathcal{C}$). If F_0 is of Type C, we have $\mathcal{D} = \rho_{C,v}(\mathcal{C})$ for any $v \in \mathcal{C}_+$. □

Lemma 7. Let $\mathcal{D}$ be a self-orthogonal binary code. Assume there exists a weight 4 codeword $e_{\{i,j,k,\ell\}} \in \mathcal{D}$, then $(i, j)(k, \ell) \in \mathrm{Aut}(\mathcal{D})$.

3 Proof of the main theorem: Type A

Lemma 8. Let $\mathcal{D}$ be a self-orthogonal binary code. Assume F_0 is a frame of $\mathcal{D}$ of Type A. If F is another frame of $\mathcal{D}$ of Type A, then there exists $\sigma \in \mathrm{Aut}(\mathcal{D})$ satisfying $|F \cap F_0| < |\sigma(F) \cap F_0|$.

Proof. Let $f \in F \setminus (F_0 \cap F)$. Then $f = e_{X_i} + e_{X_j}$, for some $X_k \subset I_k$, $|X_k| = 2$ ($k = i, j$) with $i \neq j$. Let $\{s, t\} = X_i, \{u, r\} = I_j \setminus X_j$ and set $\sigma = (s, u)(t, r)$. Then $|F \cap F_0| < |\sigma(F) \cap F_0|$. □

By induction, we have the following.

Theorem 9. Let $\mathcal{D}$ be a self-orthogonal binary code of length $4n$ with a frame of Type A. Then $\mathrm{Aut}(\mathcal{D})$ is transitive on the set of all frames of $\mathcal{D}$ of Type A.

For frames of Type B or C, we have a similar result as Lemma 8 if two frames have a common element.

Lemma 10. Let $\mathcal{D}$ be a self-orthogonal binary code of length $4n$ with a frame F_0. If F is another frame of $\mathcal{D}$ such that $F \cap F_0 \neq \emptyset$, then there exists $\sigma \in \mathrm{Aut}(\mathcal{D})$ satisfying $|F \cap F_0| < |\sigma(F) \cap F_0|$.

In the following sections, we consider the case $F \cap F_0 = \emptyset$.

4 Proof of the main theorem: Type B,C

Definition 11. Let F, F' be frames. We call F is orthogonal to F' if $f \cdot f' = 0$ for any $f \in F$ and $f' \in F'$.

If F is orthogonal to F_0 and $F \cap F_0 = \emptyset$, then any $f \in F$ is of the form

$$f = e_{X_i} + e_{X_j},$$

for some $X_k \subset I_k$, $|X_k| = 2$ $(k = i, j)$ with $i \neq j$.

In this section, let $\mathcal{D}$ be a self-orthogonal binary code of length $4n$ with a frame F_0. If F is another frame of $\mathcal{D}$ such that F is orthogonal to F_0 and $F \cap F_0 = \emptyset$, then for any $f, f' \in F$ with $f \neq f'$, one of the following holds.

(i) $|\{i \in \{1, \ldots, n\} \mid \mathrm{supp}(f + f') \cap I_i \neq \emptyset\}| = 2$

(ii) $|\{i \in \{1, \ldots, n\} \mid \mathrm{supp}(f + f') \cap I_i \neq \emptyset\}| = 3$

(iii) $|\{i \in \{1, \ldots, n\} \mid \mathrm{supp}(f + f') \cap I_i \neq \emptyset\}| = 4$

Let $N(F) = \{\{f, f'\} \subset F \mid f \text{ and } f' \text{ satisfy (i)}\}$. Note that $|N(F)| \leq n/2$.

Lemma 12. Let F be a frame orthogonal to F_0 of $\mathcal{D}$ such that $F \cap F_0 = \emptyset$. If $|N(F)| < n/2$ then there exists $\sigma \in \mathrm{Aut}(\mathcal{D})$ such that

- $\sigma(F) \cap F_0 \neq \emptyset$ or
- $\sigma(F) \cap F_0 = \emptyset$, $\sigma(F)$ is orthogonal to F_0 and $|N(F)| + 1 \leq |N(\sigma(F))|$.

By induction, we have the following.

Lemma 13. Let F be a frame orthogonal to F_0 of $\mathcal{D}$. Then there exists $\tau \in \mathrm{Aut}(\mathcal{D})$ satisfying

- $\tau(F) \cap F_0 \neq \emptyset$ or
- $\tau(F) \cap F_0 = \emptyset$, $\tau(F)$ is orthogonal to F_0 and $|N(\tau(F))| = n/2$.

In the above lemma, $|N(\tau(F))| = n/2$ occurs only when n is even. Let $n = 2k$.

Definition 14. Let $v \in \boldsymbol{F}_2^8$. For $0 \leq i \leq k-1$, define $v^{(i)} \in \boldsymbol{F}_2^{8k}$ by $(v^{(i)})_j = \delta_{i,j} v$. Let

$$F_1 = \bigcup_{i=0}^{k-1} \{e_{\{1,2,5,6\}}{}^{(i)}, e_{\{3,4,7,8\}}{}^{(i)}\}.$$

Let $d_1 = (11000000)$, $d_2 = (00110000)$, $d_3 = (00001100)$, $d_4 = (00000011)$, $d_5 = (10101010)$ and set $D = \langle d_1, d_2, d_3, d_4, d_5 \rangle$.

A self-orthogonal code of length $8k$ with frames F_0 and F_1 of Type B is contained in D^k.

Definition 15. For $0 \le i \le k-1$ and $x \in K$, define $\varphi_{i,x} \in S_{8k}$ by

$$\begin{aligned}
\varphi_{i,0} &= (8i+1, 8i+7)(8i+2, 8i+8),\\
\varphi_{i,a} &= (8i+1, 8i+8)(8i+2, 8i+7),\\
\varphi_{i,b} &= (8i+3, 8i+5)(8i+4, 8i+6),\\
\varphi_{i,c} &= (8i+3, 8i+6)(8i+4, 8i+5),
\end{aligned}$$

and let

$$\begin{aligned}
\pi_i &= \varphi_{i,0}\varphi_{i,a}\varphi_{i,b}\varphi_{i,c},\\
\Phi_i &= \{\varphi_{i,x} \mid x \in K\} \cup \{\pi_i\varphi_{i,x} \mid x \in K\},\\
\Phi &= \{\phi_0 \dots \phi_{k-1} \mid \phi_i \in \Phi_i, 0 \le i \le k-1\}.
\end{aligned}$$

Lemma 16. $g(F_1) = F_0$ for any $g \in \Phi$.

Let $d_6 = (00001010)$ and $d_7 = (10001000)$.

Lemma 17. For each $c \in D + d_6 + d_7$, there exists a unique $\phi \in \Phi_0$ such that $\phi(d_6) \in \langle d_1 + d_4, d_2 + d_3\rangle + c + d_6$.

By above lemma, we can define $\psi_0 : D + d_6 + d_7 \to \Phi_0$ by

$$\psi_0(c) = \phi \text{ if } \phi(d_6) \in \langle d_1 + d_4, d_2 + d_3\rangle + c + d_6.$$

We extend ψ_0 to $\psi : D^k + (d_6 + d_7)^k \to \Phi$.

Lemma 18. Let $\mathcal{D}$ be a self-orthogonal binary code of length $8k$ with frames F_0 and F_1. If one of the following holds:

(i) $\mathcal{D} \subset \langle D^k, (d_6 + d_7)^k\rangle$ and $x \in \mathcal{D}^\perp \cap (D^k + (d_6 + d_7)^k)$,

(ii) $x \in \mathcal{D} \cap (D^k + (d_6 + d_7)^k)$ and $\mathrm{wt}(x) \equiv 0 \pmod 4$,

then $\psi(x) \in \mathrm{Aut}(\mathcal{D})$.

By above lemma, we have the following.

Lemma 19. Let $\mathcal{D}$ be a self-orthogonal (resp. doubly-even) binary code of length $8k$ with frames F_0 and F_1 of Type B (resp. Type C). Then there exists $g \in \mathrm{Aut}(\mathcal{D})$ satisfying $g(F_1) = F_0$.

Lemma 20. Let F be a frame orthogonal to F_0 of $\mathcal{D}$ such that $F \cap F_0 = \emptyset$ and $|N(F)| = k$. Then there exists $\nu \in S_{4n}$ satisfying $\nu(F) = F_1$ and $\nu(F_0) = F_0$.

By Lemmas 10, 13, 19, 20, and by induction, we have the following.

Lemma 21. Let $\mathcal{D}$ be a self-orthogonal (resp. doubly-even) binary code of length $4n$. Assume F_0 is a frame of $\mathcal{D}$ of Type B (resp. Type C). If F is another frame of $\mathcal{D}$ of Type B (resp. Type C) such that F is orthogonal to F_0, then there exists $\sigma \in \mathrm{Aut}(\mathcal{D})$ satisfying $\sigma(F) = F_0$.

Lemma 22. Let $n > 4$. Let $\mathcal{D}$ be a self-orthogonal binary code of length $4n$. Assume F_0 is a frame of $\mathcal{D}$ of Type B. If F is another frame of $\mathcal{D}$ of Type B then F is orthogonal to F_0.

Proof. Let $f \in F$. It suffices to show $f \cdot e_{I_i} = 0$ for any i satisfying $\mathrm{supp}(f) \cap I_i \neq \emptyset$. Since $|\{f \in F \mid \mathrm{supp}(f) \cap I_i \neq \emptyset\}| \leq 4 < |F|$, there exists $f' \in F$ such that $\mathrm{supp}(f') \cap I_i = \emptyset$. As $f + f' \in \mathcal{D} \subset (d_4^n)^\perp$, we have $f \cdot e_{I_i} = (f + f') \cdot e_{I_i} = 0$. □

Lemma 23. Let $n > 8$ be even. Let $\mathcal{D}$ be a doubly-even binary code of length $4n$. Assume F_0 is a frame of $\mathcal{D}$. If F is another frame of $\mathcal{D}$ then F is orthogonal to F_0.

Proof. Let $f \in F$. It suffices to show $f \cdot e_{I_i} = 0$ for any i satisfying $\mathrm{supp}(f) \cap I_i \neq \emptyset$. Since $|\{e_{I_j} \in F_0 \mid \mathrm{supp}(f) \cap I_j \neq \emptyset\}| \leq 4 < |F_0|$, there exists $I_j \in F$ such that $\mathrm{supp}(f) \cap I_j = \emptyset$. And since $|\{f' \in F \mid \mathrm{supp}(f') \cap (I_i \cup I_j) \neq \emptyset\}| \leq 8 < |F|$, there exists $f' \in F$ such that $\mathrm{supp}(f') \cap (I_i \cup I_j) = \emptyset$. As $f + f', e_{I_i} + e_{I_j} \in \mathcal{D}$, we have $f \cdot e_{I_i} = (f + f') \cdot (e_{I_i} + e_{I_j}) = 0$. □

Now we have the following.

Theorem 24. Let $n > 4$. Let $\mathcal{D}$ be a self-orthogonal binary code of length $4n$ with a frame of Type B. Then $\mathrm{Aut}(\mathcal{D})$ is transitive on the set $\mathcal{F}$ of all frames of $\mathcal{D}$ of Type B.

Proof. Without loss of generality, we can assume F_0 is a frame of $\mathcal{D}$ of Type B. By Lemme 22, any $F \in \mathcal{F}$ is orthogonal to F_0. Thus by Lemma 21, $\mathrm{Aut}(\mathcal{D})$ is transitive on $\mathcal{F}$. □

Theorem 25. Let $n > 8$ be even. Let $\mathcal{D}$ be a doubly-even binary code of length $4n$ with a frame of Type C. Then $\mathrm{Aut}(\mathcal{D})$ is transitive on the set of all frames of $\mathcal{D}$ of Type C.

Proof. Without loss of generality, we can assume F_0 is a frame of $\mathcal{D}$ of Type C. By Lemme 23, any $F \in \mathcal{F}$ is orthogonal to F_0. Thus by Lemma 21, $\mathrm{Aut}(\mathcal{D})$ is transitive on $\mathcal{F}$. □

5 Exceptions

If a self-orthogonal (resp. doubly-even) binary code $\mathcal{D}$ of length $4n$ has frames F_0, F of Type B (resp. Type C), then by Lemma 21, F is not orthogonal to F_0 and thus $n \leq 4$ (resp. $n \leq 8$) by Lemma 22 (resp. Lemma 23). With the help of MAGMA [5], we give all codes up to equivalence such that no automorphism of $\mathcal{D}$ maps F to F_0.

5.1 Type B

$n = 4$, $F = \{e_{\{i,i+4,i+8,i+12\}} : 1 \le i \le 4\}$, a generator matrix of $\mathcal{D}$ is

$$\begin{bmatrix} 1100110000000000 \\ 0110011000000000 \\ 0011001100000000 \\ 0000111111110000 \\ 0000000011001100 \\ 0000000001100110 \\ 0000000000110011 \end{bmatrix}.$$

5.2 Type C

(i) $n = 6$, $F = \{e_{\{1,2,3,8\}}, e_{\{4,5,6,7\}}\} \cup \{e_{\{i,i+4,i+8,i+12\}} : 9 \le i \le 12\}$.

- The $[24, 12]$-code $\mathcal{D}_1$ generated by $F_0 + F_0$, $F + F$ and

$$\begin{bmatrix} 110011000000000000000000 \\ 011001100000000000000000 \\ 000000001100110000000000 \\ 000000000110011000000000 \end{bmatrix}$$

  which is equivalent to C_{24} in [6].
- Two $[24, 11]$-codes $\mathcal{D}_2 = \mathcal{D}_1 \cap e^{\perp}_{\{1,2\}}$ and $\mathcal{D}_3 = \mathcal{D}_1 \cap e^{\perp}_{\{1,8,12,14,20,22\}}$.
- Three $[24, 10]$-codes $\mathcal{D}_4 = \mathcal{D}_2 \cap \mathcal{D}_3$, $\mathcal{D}_5 = \mathcal{D}_2 \cap e^{\perp}_{\{2,3\}}$ and $\mathcal{D}_6 = \mathcal{D}_3 \cap e^{\perp}_{\{1,2,15,16,23,24\}}$.

(ii) $n = 8$, $F = \{e_{\{i,i+4,i+8,i+12\}} : i \in \{1, 2, 3, 4, 17, 18, 19, 20\}\}$.

- The $[32, 16]$-code $\mathcal{D}_7$ generated by $F_0 + F_0$, $F + F$ and

$$\begin{bmatrix} 11001100000000000000000000000000 \\ 01100110000000000000000000000000 \\ 00000000000000001100110000000000 \\ 00000000000000000110011000000000 \end{bmatrix},$$

  which is equivalent to the 29th code in [1].
- Two $[32, 15]$-codes $\mathcal{D}_8 = \mathcal{D}_7 \cap e^{\perp}_{\{1,2,9,10\}}$ and $\mathcal{D}_9 = \mathcal{D}_7 \cap e^{\perp}_{\{1,3,9,11,17,18,25,26\}}$.
- Three $[32, 14]$-codes $\mathcal{D}_{10} = \mathcal{D}_8 \cap \mathcal{D}_9$, $\mathcal{D}_{11} = \mathcal{D}_8 \cap e^{\perp}_{\{2,3,10,11\}}$ and $\mathcal{D}_{12} = \mathcal{D}_9 \cap e^{\perp}_{\{1,2,9,10,17,19,25,27\}}$.

References

[1] J. H. Conway and V. Pless, On the enumeration of self-dual codes, J. Combin. Theory Ser. A **28** (1980), 26–53.

[2] J. H. Conway and N. J. A. Sloane, "Sphere Packing, Lattices and Groups," 3rd ed., Springer-Verlag, New York, 1999.

[3] G. Höhn, Self-dual codes over the Kleinian four group, *Math. Ann.* **327** (2003), 227–255

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

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

[6] V. Pless and N. J. A. Sloane, Binary self-dual codes of length 24, Bull. Amer. Math. Soc. **80** (1974), 1173–1178.

[7] H. Shimakura, On isomorphism problems for vertex operator algebras associated with even lattices, Proc. Amer. Math. Soc., in press.

[8] N. J. A. Sloane, Self-dual codes and lattices, Proc. Sympos. Pure Math. **34** (1979), 273–308.

On a class of wreath products of hypergroups and association schemes

田中 利恵

ここに紹介する結果は Paul-Hermann Zieschang (University of Texas at Brownsville) との共同研究により得られたものである。証明などの詳細は [6] をご覧頂きたい。

1 Hypergroups

Hypergroup という用語は F. Marty により 1930 年代に導入され [4]、これまで活発に研究されてきた。研究者により定義の仕方が様々であったり、hypergroup と同義の概念が異なる用語で表現されたりすることもある。Hypergroup や関連する事項については、[1]、 [2]、 [3] などを参照されたい。

初めに hypergroup を定義するが、ここで採用する定義は Zieschang によるもので Marty の定義がわずかに一般化されている [8]:

Let S be a set, and let μ be a map from $S \times S$ to the power set of S. For any two elements p and q of S, we write pq instead of $\mu(p, q)$ and assume that pq is not empty.

For any two non-empty subsets P and Q of S, we define the *complex product* PQ to be the union of the sets pq with $p \in P$ and $q \in Q$. If one of the two factors in a complex product consists of a single element, say s, we write s instead of $\{s\}$ in that product.

We call S a *hypergroup* (with respect to μ) if the following three conditions hold.

H1 For any three elements p, q, and r in S, we have $p(qr) = (pq)r$.

H2 The set S possesses an element e such that $se = \{s\}$ for each element s in S.

H3 For each element s in S, there exists an element s^* in S such that $p \in rq^*$ and $q \in p^*r$ for any three elements p, q, and r in S satisfying $r \in pq$.

Association scheme は complex product に関して上記の 3 条件 H1、H2、H3 を満たす; cf. [7]。 従って hypergroup は association scheme の一般化であり、特に、群の一般化になっている。群に相当する hypergroup S は S の任意の 2 元 p, q について $|pq| = 1$ が成立するもので、これを thin hypergroup と呼ぶことにする。ここでは、条件を少し緩めて、$p \neq q^*$ を満たす任意の 2 元 p, q に対して $|pq| = 1$ が成り立つような hypergroup について考える。

2 Wreath products of hypergroups

主結果を述べるために必要な用語をいくつか定義する：

Let S be a finite hypergroup. A non-empty subset T of S is said to be *closed* if $pq^* \subseteq T$ for any $p, q \in T$. The intersection of closed subsets is also closed. For a non-empty subset U of S, $< U >$ is the intersection of all closed subsets containing U.

Let s be an element in S different from e. We say s is an *involution* if $< s >= \{e, s\}$. We say s is an *idempotent* if $ss = \{s\}$ and $< s >= \{e, s, s^*\}$.

Let T be a closed subset of S. For $s \in S$, we write $s^T := TsT$ and define $S//T := \{s^T : s \in S\}$. Then $S//T$ gives a partition of S. Define $\mu_T : S//T \times S//T \to \mathcal{P}(S//T)$ by

$$\mu_T(p^T, q^T) := \{r^T : r \in pTq\}.$$

We can verify that $S//T$ is a hypergroup with respect to μ_T.

Hypergroups S_1 and S_2 are said to be *isomorphic* if there is a bijection f from S_1 to S_2 which satisfies $f(pq) = f(p)f(q)$.

A hypergroup S is called a *wreath product* of hypergroups S_1 and S_2 if it has a closed subset T such that

$$T \cong S_1, \quad S//T \cong S_2$$

and $st = \{s\}$ for any $t \in T$ and $s \in S \setminus T$. We write $S = S_1 \wr S_2$.

注）群を hypergroup とみなしたとき、ここで定義した hypergroup の wreath product と群の wreath product とは必ずしも一致しない。（しかし、群の wreath product の作用から得られる association scheme のレベルで考えるとある種の対応関係がある。）

3 Main result

Theorem 3.1 *Let S be a finite hypergroup. Then the following are equivalent.*

(a) *For any $p, q \in S$ with $p \neq q^*$, $|pq| = 1$.*

(b) *S is a wreath product of hypergroups all of which are thin, generated by an involution, or generated by an idempotent.*

この定理は可換 association scheme における筆者の結果 [5] の一般化となっている。Association scheme に付随して Terwilliger 代数という非可換半単純 $\mathbb{C}$ 代数が得られるが、論文 [5] では、Terwilliger 代数が almost commutative という面白い性質をみたす association scheme の分類と特徴づけが行われている。Association scheme の可換性を仮定しないと付随する Terwilliger 代数は一般には almost commutative にはならないが、それでもまだ面白い性質をもつ。今回の hypergroup に関する結果の系として、[5] の一般の（可換とは限らない） association scheme への拡張が得られた（用語の定義は [6] を参照のこと）：

Theorem 3.2 *Let (X, S) be an association scheme. The following are equivalent:*

(a) *For each non-primary irreducible $\mathcal{T}$-module W, $|Supp(W)| = 1$.*

(b) *For any $p, q \in S$ with $p \neq q^*$, $|pq| = 1$.*

(c) *(X, S) is a wreath product of association schemes all of which are group schemes, or one-class schemes.*

Association scheme は集合 X と X 上の二項関係の集合 S のペアであり、hypergroup の枠組みで捉えるというのは、集合 X を無視して、S のみに注目するということである。条件 (b) を満たす association scheme を分類するには hypergroup の枠組みで捉えるのが自然であることがわかった。

参考文献

[1] Blau, H.: Table algebras, *European J. Combin.* **30**, 1426–1455 (2009)

[2] Blau, H. and Zieschang, P.-H.: Sylow theory for table algebras, fusion rule algebras, and hypergroups, *J. Algebra* **273**, 551–570 (2004)

[3] Bloom, W. and Heyer, H.: *Harmonic Analysis of Probablity Measures on Hypergroups*. Walter de Gruyter, Berlin New York (1995)

[4] Marty, F.: Sur une généralisation de la notion de groupe, in Huitième Congres des Mathématiciens, Stockholm 1934, 45–59

[5] Tanaka, R.: Classification of commutative association schemes with almost commutative Terwilliger algebras, *J. Algebraic Combin.* **33**, 1–10 (2011)

[6] Tanaka, R. and Zieschang, P.-H.: On a class of wreath products of hypergroups and association schemes, *J. Algebraic Combin.* doi 10.1007/s10801-012-0376-y (2012)

[7] Zieschang, P.-H.: *Theory of Association Schemes*. Springer Monographs in Mathematics, Berlin Heidelberg New York (2005)

[8] Zieschang, P.-H.: *Hypergroups*. Preprint (Max-Planck-Institut für Mathematik Preprint Series 2010 (97))

Buratti-Del Fra DHO および deformation of Veronesean DHO の簡単な表示

香川高専　谷口浩朗 (Hiroaki Taniguchi)*

1　はじめに

この稿では高次元双対超卵形 (dimensional dual hyperoval) を DHO と表すことにする．Buratti-Del Fra's DHO [1],[2] や Veronesean DHO の変形である DHO [5] は表示が煩雑であり，研究をためらわせるところがあった.（ともすれば存在自体が疑いの眼で見られることもあったのでは無いかと想像する.）今回それらの DHO の簡単な（計算に乗りやすい）表示が発見できたのでそれを報告したい．まず，2 元体上の DHO の定義を与える．射影空間 $PG(m,2)$ 内の DHO は C. Huybrechts と A. Pasini [4] により以下のように定義された.

定義 1 ($GF(2)$ 上の DHO)**.** m-次元射影空間 $PG(m,2)$ における d-次元部分空間の集合 S が, $PG(m,2)$ における d-次元双対超卵形であるとは，以下のことが成り立つことである:
(1) S に属するどの 2 個の d-部分空間も 1 点で交わり,
(2) S に属するどの異なる 3 個の d-部分空間も共通点を持たず,
(3) S に属する d-部分空間達は $PG(m,2)$ を生成し,
(4) S は 2^{d+1} 個の d-部分空間から成る.

以下 $d \geq 3$ とする. $GF(2)$ 上の d-次元の双対超卵形が生成する射影空間の次元 n については，$2d \leq n \leq d(d+3)/2$ であろうと予想されている．その最大の次元と考えられる $PG(d(d+3)/2, 2)$ には，現在
（1）Huybrechts' DHO [3],
（2）Buratti-Del Fra's DHO [1],[2],
（3）Veronesean DHO [6], [7],
（4）Veronesean DHO の変形 [5],

*E-mail address: taniguchi@dg.kagawa-nct.ac.jp

の 4 種類の（同型でない）双対超卵形が構成されている．（2）および（4）の簡単な表示を与えることが本稿の目的である。

2 Buratti-Del Fra's DHO と Deformation of Veronesean DHO

$n \geq d+1 \geq 3$ とし，H を $d+1$ 次元ベクトル空間とする．以下のことが分かっている．

命題 1. $s,t \in H$ にたいし $a(s,t) \in H \oplus (H \wedge H)$ を次を満たすように定める．
(a1) $a(s,s) = (0,0)$,
(a2) $a(s,t) = a(t,s)$,
(a3) $a(s,t) \neq (0,0)$,
(a4) $a(s,t) = a(s',t')$ *if and only if* $\{s,t\} = \{s',t'\}$,
(a5) $\{a(s,t) \mid t \in H\} \cup \{(0,0)\}$ *is a vector space over* $GF(2)$.
このとき，$X(s) := \{a(s,t) \mid t \in H \backslash \{0\}\}$ は $PG(H \oplus (H \wedge H))$ の d-次元部分空間であり $S = \{X(s) \mid s \in H\}$ は d-次元双対超卵形となることが分かる．

以下 H の基底 $\{e_0, e_1, \ldots, e_d\}$ を固定する．$t = e_{i_1} + \cdots + e_{i_l} \in H$ と基底で表すとき，$Supp(t) := \{e_{i_1}, \cdots, e_{i_l}\}$ と定める．また，$J(t) := Supp(t)$ ($|Supp(t)|$ が奇数の場合)，$J(t) := \{0\} \cup Supp(t)$ ($|Supp(t)|$ が偶数の場合) と定める．$t = \alpha_0 e_0 + \alpha_1 e_1 + \cdots + \alpha_d e_d \in H$ $(\alpha_i \in GF(2), \forall i)$ のとき $\bar{t} := \alpha_1 e_1 + \cdots + \alpha_d e_d$ と定める．また ξ を集合 $H \backslash \{0, e_0\}$ の特性関数とする．

例 1. *Buratti Del Fra's DHO* は以下の $a(s,t)$ で定められる．

$$\begin{aligned} a(s,t) &= (s+t, s \wedge t) \\ &+ x_{\bar{s},\bar{t}} \sum_{w \in J(\bar{s})} (e_0, e_0 \wedge w) + \sum_{w \in J(\bar{t})} x_{w,\bar{s}} (e_0, e_0 \wedge w) \end{aligned}$$

ここに $x_{s,t} := \xi(s+t) + \sum_{w \in J(t)} \xi(s+w) \in GF(2)$ とする．

さて，$GF(2)$-ベクトル空間 $H \otimes H$ の部分空間 $\wedge^2(H)$ を $\wedge^2(H) = \langle x \otimes y + y \otimes x \mid x,y \in H \rangle$ と定義し，$S^2(H) := (H \otimes H)/\wedge^2(H)$ における $x \otimes y$ の像をまた $x \otimes y$ と記すことにする．

命題 2. $s,t \in H$ にたいし $b(s,t) \in S^2(H)$ を次を満たすように定める．
(b1) $b(s,s) = s \otimes s$,

(b2) $b(s,t) = b(t,s)$,
(b3) $b(s,t) \neq 0$,
(b4) $b(s,t) = b(s',t')$ *iff* $\{s,t\} = \{s',t'\}$,
(b5) $\{b(s,t) \mid t \in H\backslash\{0\}\} \cup \{(0,0)\}$ *is a vector space over* $GF(2)$.
このとき，$X(s) := \{b(s,t) \mid t \in H\backslash\{0\}\}$ および $X(\infty) := \{b(s,s) \mid t \in H\backslash\{0\}\}$ は $PG(S^2(H))$ の d-次元部分空間であり $S := \{X(s)|s \in H\backslash\{0\}\} \cup \{X(\infty)\}$ は d-次元双対超卵形となる.

例 2. *Deformation of Veronesean DHO* は以下の $b(s,t)$ で定められる.

$$b(s,t) = s \otimes t \quad + \quad x_{s,t} \sum_{w \in Supp(s)} w \otimes (w + e_0) \\ + \quad \sum_{w \in Supp(t)} x_{w,s} w \otimes (w + e_0).$$

ここに $x_{s,t} := \xi(s+t) + \sum_{w \in Supp(t)} \xi(s+w) \in GF(2)$ とする.

例 3. *Buratti Del Fra's DHO* について以下の和公式が成り立つ.

$$a(s,t_1) + a(s,t_2) = a(s, s + t_1 + t_2 + \alpha\{s,t_1,t_2\}e_0),$$

ここに $\alpha\{s,t_1,t_2\} := \xi(s+t_1) + \xi(s+t_2) + \xi(t_1+t_2) \in GF(2)$，$\xi(t)$ は集合 $H\backslash\{0,e_0\}$ の特性関数である.

例 4. *Deformation of Veronesean DHO* について以下の和公式が成り立つ.

$$b(s,t_1) + b(s,t_2) = b(s, t_1 + t_2 + \alpha\{s,t_1,t_2\}(s+e_0)),$$

ここに $\alpha\{s,t_1,t_2\} := \xi(t_1)\xi(s+t_1) + \xi(t_2)\xi(s+t_2) + \xi(s+t_1+t_2)\xi(t_1+t_2) \in GF(2)$，$\xi(t)$ は集合 $H\backslash\{0,e_0\}$ の特性関数である.

H の元 $s := \sum_{i=0}^{d} x_i e_i$, $t := \sum_{i=0}^{d} y_i e_i$ (ここに $x_i, y_i \in GF(2)$) に対して $s \cap t := \sum_{i=0}^{d} x_i y_i e_i$ および $s \cup t := s + t + s \cap t$ とする．また，$\epsilon(s,t) := \xi(s)\xi(t)\xi(s+t)$ と定める．本稿の目的は次の 2 つの定理を証明することである.

定理 1. $s,t \in H$ に対し $\hat{a}(s,t) \in H \oplus (H \wedge H)$ を以下のように定める.

$$\hat{a}(s,t) := (s+t, s \wedge t) + \xi(s+t)(e_0, e_0 \wedge (s \cap t)).$$

このとき $\{\hat{a}(s,t)\}$ は *Buratti-Del Fra DHO* と同型の *DHO* を定義する.

定理 2. $s,t \in H\backslash\{0\}$ に対し $\hat{b}(s,t) \in S^2(H)$ を以下のように定める.

$$\hat{b}(s,t) := s \otimes t + \epsilon(s,t)((s \cup t) \otimes (s \cup t + e_0)).$$

このとき $\{\hat{b}(s,t)\}$ は *Deformation of Veronesean DHO* と同型の *DHO* を定義する.

証明においては、次の命題を用いる.

命題 3.
- $PG(d(d+3)/2,2)$ を生成する d-次元 *DHO* $S := \{X(t) \mid t \in H\}$ において $a(s,t) := X(s) \cap X(t)$ が例 *3* の和公式を満たすならば，S は *Buratti Del Fra's DHO* と同型である.
- $PG(d(d+3)/2,2)$ を生成する d-次元 *DHO* $S := \{X(t) \mid t \in H\backslash\{0\}\} \cup \{X(\infty)\}$ において $b(s,t) := X(s) \cap X(t)$ および $b(s,s) := X(s) \cap X(\infty)$ が例 *4* の和公式を満たすならば，S は *Deformation of Veronesean DHO* と同型である.

3 定理１の証明

補題 1. 定理 *1* の $\hat{a}(s,t)$ に関して，以下の和公式が成り立つ.

$$\hat{a}(s,t_1) + \hat{a}(s,t_2) = \hat{a}(s, s + t_1 + t_2 + \alpha\{s,t_1,t_2\}e_0).$$

ここに $\alpha\{s,t_1,t_2\} := \xi(s+t_1) + \xi(s+t_2) + \xi(t_1+t_2)$ とする.

証明. $\{\xi(s+t_1), \xi(s+t_2), \xi(t_1+t_2)\}$ の値による場合分けで確かめていく. (これらの値のうち，2 個が 0 ならば 3 個とも 0 になることに注意をして下さい.)

(1) $\xi(s+t_1) = 1$, $\xi(s+t_2) = 1$, $\xi(t_1+t_2) = 1$ の場合

$$\begin{aligned}
\hat{a}(s,t_1) + \hat{a}(s,t_2) &= (s+t_1, s \wedge t_1) + (e_0, e_0 \wedge (s \cap t_1)) \\
&+ (s+t_2, s \wedge t_2) + (e_0, e_0 \wedge (s \cap t_2)) \\
&= (t_1+t_2, s \wedge (t_1+t_2)) \\
&+ (0, e_0 \wedge (s \cap (t_1+t_2))) \\
&= \hat{a}(s, s+t_1+t_2+e_0).
\end{aligned}$$

(2) $\xi(s+t_1) = 0$, $\xi(s+t_2) = 1$, $\xi(t_1+t_2) = 1$ の場合

$$\begin{aligned}
\hat{a}(s,t_1) + \hat{a}(s,t_2) &= (s+t_1, s \wedge t_1) \\
&+ (s+t_2, s \wedge t_2) + (e_0, e_0 \wedge (s \cap t_2)) \\
&= (t_1+t_2, s \wedge (t_1+t_2)) \\
&+ (e_0, e_0 \wedge (s \cap t_2)) \\
&= \hat{a}(s, s+t_1+t_2).
\end{aligned}$$

(3) If $\xi(s+t_1)=1$, $\xi(s+t_2)=1$, $\xi(t_1+t_2)=0$ の場合

$$\begin{aligned}\hat{a}(s,t_1)+\hat{a}(s,t_2) &= (s+t_1, s\wedge t_1)+(e_0, e_0\wedge(s\cap t_1))\\ &+ (s+t_2, s\wedge t_2)+(e_0, e_0\wedge(s\cap t_2))\\ &= (t_1+t_2, s\wedge(t_1+t_2))\\ &+ (0, e_0\wedge(s\cap(t_1+t_2)))\\ &= \hat{a}(s, s+t_1+t_2).\end{aligned}$$

(4) $\xi(s+t_1)=0, \xi(s+t_2)=0$, $\xi(t_1+t_2)=0$ の場合
$(s+t_1, s\wedge t_1)+(s+t_2, s\wedge t_2)=(s+(s+t_1+t_2), s\wedge(s+t_1+t_2))$ なので

$$\hat{a}(s,t_1)+\hat{a}(s,t_2)=\hat{a}(s, s+t_1+t_2).$$

以上より，補題の成立が確かめられた. □

定理 *1* の証明. $\{0, e_0, \ldots, e_d\}$ の元を例 1 の $a(s,t)$ および定理 1 の $\hat{a}(s,t)$ に代入してみると

$$\begin{aligned}\hat{a}(e_i,e_j)=(e_i+e_j+e_0, e_i\wedge e_j) \quad &\text{および} \quad a(e_i,e_j)=(e_i+e_j, e_i\wedge e_j),\\ \hat{a}(0,e_j)=(e_j+e_0, 0) \quad &\text{および} \quad a(0,e_j)=(e_j, 0),\\ \hat{a}(0,e_0)=(e_0,0) \quad &\text{および} \quad a(0,e_0)=(e_0,0) \text{ となる.}\end{aligned}$$

このことより $\{a(e_i,e_j), a(0,e_j), a(0,e_0) \mid 0\le i<j\le d\}$, および $\{\hat{a}(e_i,e_j), \hat{a}(0,e_j), \hat{a}(0,e_0) \mid 0\le i<j\le d\}$ がともに $H\oplus(H\wedge H)$ の基底であることが分かる. さて, 線形同型写像

$$\pi : H\oplus(H\wedge H)\cong H\oplus(H\wedge H)$$

を基底の上ですべての $0\le i<j\le d$ に対して $\pi(\hat{a}(e_i,e_j))=a(e_i,e_j)$, またすべての $0\le i\le d$ に対して $\pi(\hat{a}(0,e_i))=a(0,e_i)$ となるように定める. このとき補題 1 より, $a(s,t)$ および $\hat{a}(s,t)$ の和公式が同じであるので，s,t を基底で表したときの長さによる帰納法により，すべての $s,t\in H$ に対して $\pi(\hat{a}(s,t))=a(s,t)$ が成り立つことが分かる. よって $\{\hat{a}(s,t)\}$ はもとの Buratti-Del Fra DHO と同型な DHO を定めることが分かる. □

4 定理２の証明

補題 2. 以下の和公式が成り立つ.

$$\hat{b}(s,t_1)+\hat{b}(s,t_2)=\hat{b}(s,t_1+t_2+\alpha\{s,t_1,t_2\}(s+e_0)).$$

ここに $\alpha\{s,t_1,t_2\} := \xi(t_1)\xi(s+t_1)+\xi(t_2)\xi(s+t_2)+\xi(s+t_!+t_2)\xi(t_1+t_2) \in GF(2)$ とする.

証明. $\{\epsilon(s,t_1),\epsilon(s,t_2),\epsilon(s,t_1+t_2)\}$ の値による場合分けで確かめていく. (注意:$\epsilon(s,t_1+t_2)=\epsilon(s,t_1+t_2+s+e_0)$ であること, また $\{\epsilon(s,t_1),\epsilon(s,t_2),\epsilon(s,t_1+t_2)\}$ のうち 2 個の値が 0 と一致すれば 3 個とも 0 となることに注意する.)

(1) $\epsilon(s,t_1)=1$, $\epsilon(s,t_2)=1$ $\epsilon(s,t_1+t_2)=1$ の場合

$$\begin{aligned}\hat{b}(s,t_1)+\hat{b}(s,t_2) &= s\otimes(t_1+t_2)+(t_1+t_2)\otimes(t_1+t_2+e_0)\\ &+ (s\cap(t_1+t_2))\otimes(s\cap(t_1+t_2)+e_0)\\ &= \hat{b}(s,t_1+t_2+(s+e_0)).\end{aligned}$$

(2) $\epsilon(s,t_1)=0$, $\epsilon(s,t_2)=1$, $\epsilon(s,t_1+t_2)=1$ の場合
($t_1=e_0$ or $t_1=s$ or $t_1=s+e_0$ なので)

$$\begin{aligned}\hat{b}(s,t_1)+\hat{b}(s,t_2) &= s\otimes(t_1+t_2)+t_2\otimes(t_2+e_0)\\ &+ (s\cap t_2)\otimes(s\cap t_2+e_0)+s\otimes(s+e_0)\\ &= \hat{b}(s,t_1+t_2).\end{aligned}$$

(3) $\epsilon(s,t_1)=1$, $\epsilon(s,t_2)=1$, $\epsilon(s,t_1+t_2)=0$ の場合
($t_1+t_2=0, e_0$,$t_1+t_2=s$, or $t_1+t_2=s+e_0$ なので)

$$\begin{aligned}\hat{b}(s,t_1)+\hat{b}(s,t_2) &= s\otimes(t_1+t_2)+(t_1+t_2)\otimes(t_1+t_2+e_0)\\ &+ (s\cap(t_1+t_2))\otimes(s\cap(t_1+t_2)+e_0)\\ &= \hat{b}(s,t_1+t_2).\end{aligned}$$

(4) $\epsilon(s,t_1)=0$, $\epsilon(s,t_2)=0$, $\epsilon(s,t_1+t_2)=0$ の場合

$$\hat{b}(s,t_1)+\hat{b}(s,t_2)=s\otimes t_1+s\otimes t_2=s\otimes(t_1+t_2)=\hat{b}(s,t_1+t_2).$$

$\alpha\{s,t_1,t_2\} := \xi(t_1)\xi(s+t_1)+\xi(t_2)\xi(s+t_2)+\xi(s+t_1+t_2)\xi(t_1+t_2)$ と定めれば, $\xi(s)\alpha\{s,t_1,t_2\} := \epsilon(s,t_1)+\epsilon(s,t_2)+\epsilon(s,s+t_1+t_2)$ なので, $\{\hat{b}(s,t)\}$ は補題 2 の和公式を満たすことが分かる. □

定理 *2* の証明. $\{e_0,\ldots,e_d\}$ の元を例 2 の $b(s,t)$ および定理 2 の $\hat{b}(s,t)$ に代入してみると

$$\begin{aligned}\hat{b}(e_i,e_j) &= e_i\otimes e_j+\epsilon(e_i,e_j)((e_i+e_j)\otimes(e_i+e_j+e_0)),\\ b(e_i,e_j) &= e_i\otimes e_j \text{ となる.}\end{aligned}$$

このことより $\{b(e_i, e_j) \mid 0 \leq i \leq j \leq d\}$, および $\{\hat{b}(e_i, e_j) \mid 0 \leq i \leq j \leq d\}$ がともに $S^2(H) = (H \otimes H)/\wedge^2(H)$ の基底であることが分かる. さて, 線形同型写像 $\pi : S^2(H) \cong S^2(H)$ を基底の上ですべての $0 \leq i < j \leq d$ に対し $\pi(\hat{b}(e_i, e_j)) = b(e_i, e_j)$ となるように定める. このとき補題 2 より, $b(s,t)$ および $\hat{b}(s,t)$ の和公式が同じであるので, s,t を基底で表したときの長さによる帰納法により, すべての $s,t \in H\backslash\{0\}$ に対して $\pi(\hat{b}(s,t)) = b(s,t)$ が成り立つことが分かる. よって $\{\hat{b}(s,t)\}$ はもとの Deformation of Veronesean DHO と同型な DHO を定めることが分かる. □

References

[1] M. Buratti and A. Del Fra, Semi-Boolean quadruple systems and dimensional dual hyperovals, Advances in Geometry. 3 (2003), 245–253.

[2] A. Del Fra and S. Yoshiara, Dimensional dual hyperovals associated with Steiner systems, European Journal of Combinatorics. 26 (2005), 173–194.

[3] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AC^*$ geometries, Discrete Mathematics. 255 (2002), 503–532.

[4] C. Huybrechts and A. Pasini, Frag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40. (1999), 503–532.

[5] H. Taniguchi, A new family of dual hyperovals in $PG(d(d+3)/2, 2)$ with $d \geq 3$, Discrete Mathematics, 309(2009), 418–429.

[6] J. Thas and H. van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, The Quarterly Journal of Mathematics, Oxford. 55 (2004), 99–113.

[7] S. Yoshiara, Ambient spaces of dimensional dual arcs, Journal of Algebraic Combinatorics. 19 (2004), 5–23.

[8] S. Yoshiara, Notes on Taniguchi's dimensional dual hyperovals, European J.Combin. 28 (2007), 674–684.

Permutation Pattern と Lehmer Code から定まる半順序集合の構造について

冨江　雅也

盛岡大学　(e-mail: tomie@morioka-u.ac.jp)

1 Introduction

本稿では Permutation Pattern の基本的な事柄を概観した後、転倒数を用いた重み付き和として現れる q-類似および $q=-1$ の特殊化について紹介する。また置換から定まる Lehmer code の半順序集合の構造に関して、先行研究および筆者により得られた結果を紹介する。Permutation Pattern の数え上げにおける基本的な定理として Knuth による、どのような S_3 の元 σ に対しても σ avoiding permutation の個数が Catalan 数で数え上げられるという事実がある [12] [13]。Catalan 数とは二項係数を用いて $C_n=\dfrac{1}{n+1}\binom{2n}{n}$ と表される数であり、組合せ的対象の数え上げにおいて頻繁に現れる。たとえば Stanley の教科書において多くの Catalan 数で数え上げられる対象が演習問題として挙げられている [16]。中でも最も有名な例として Dyck Path が知られている。$\sigma\in S_3$ avoiding permutation から Dyck path への全単射がいくつも提案されており [7]、さらにいくつかの S_4 の元 τ に対して τ avoiding permutation の数え上げには Dyck path の親類にあたる Schröder path が現れる [11]。また Claesson により提案された generalized permutation pattern においては自然に Motzkin path が出てきたりもする [6]。このように Permutation Pattern と Lattice Path の間には密接なつながりがある。また Permutation Pattern と Lattice Path の間の全単射においては多くの結果が知られており、特に Claesson と Kitaev は [7] に於いて、全単射の良さを表す一つの指標として、”対応によってどのくらいの（どのような）対象間の重みが保たれるか”を提案し、過去に得られた多くの対応の良さに関して論じている。一方自然数をパラメーターに持つ k-Catalan 数、Coxeter 群の degree を用いて一般化された Coxeter Catalan 数, さらにこれらを含む Fuss–Catalan 数などへの一般化も研究されている [1]。

本稿においては、Permutation Pattern の数え上げについていくつかの古典的な結果を概観する。次に Lattice Path との関連、特に一対一対応について簡単に述べた後、Permutation Pattern の数え上げにおける q-類似（の一つ）を紹介する。特に $q=1$ とすれば元の数が復元されるが、$q=-1$ となる場合について、いくつかの先行研究及び筆者が得た計算結果を述べる。最後に置換から定まる Lehmer code の半順序構造について、Denoncourt の先行研究及び筆者が最近得た結果を紹介する。

2 Permutation Patternについて

初めにPermutation Patternを議論する際に基本的となる用語を定義する。詳細はKitaevの教科書を参照のこと [9]

Definition 2.1. $\pi \in S_n$および$\sigma \in S_k$に対してπがσ-patternを含むとは、$1 \leq i_1 < i_2 < \cdots < i_k \leq n$に対し$\pi(i_1)\pi(i_2)\cdots\pi(i_k)$の大小関係が$\sigma(1)\sigma(2)\cdots\sigma(k)$と一致するときをいう。

特に$st(\pi(i_1)\pi(i_2)\cdots\pi(i_k))$は$\pi(i_1)\pi(i_2)\cdots\pi(i_k)$において大小関係を保ちつつ$S_k$の元として表したものとする。たとえば462513においては**462**513において$st(425) = 213$となるので213-patternを含む。次にPattern Avoidingを定義する。

Definition 2.2. $\pi \in S_n$ σ-pattern avoiding permutationであるとは$1 \leq \forall i_1 < \forall i_2 < \cdots < \forall i_k \leq n$に対して$st(\pi(i_1)\pi(i_2)\cdots\pi(i_k)) \neq \sigma(1)\sigma(2)\cdots\sigma(k)$が成り立つ時をいう。

S_nにおいてσ-avoiding permutationとなるものの集合を$S_n(\sigma)$と置く。特に
$S_3(321) = \{123, 132, 213, 231, 312\}$である。

Theorem 2.1. [12] [13]
$\sharp S_n(123) = \sharp S_n(132) = \sharp S_n(213) = \sharp S_n(231) = \sharp S_n(312) = \sharp S_n(321) = \frac{1}{n+1}\binom{2n}{n}$

いくつかの置換をavoidする場合についてもSchmidtとSimionによって考えられている。置換の集合Bに対してBに属するpatternを持たないS_nの部分集合を$S_n(\mathrm{B})$とおく、このとき

Theorem 2.2. [14]
$\sharp\mathrm{B} = 2$ならば$S_n(\mathrm{B})$の個数は以下のいずれかとなる

1. $\sharp S_n(132, 123) = \sharp S_n(132, 213) = \sharp S_n(132, 231) = \sharp S_n(132, 312) = 2^{n-1}$
2. $\sharp S_n(132, 321) = \binom{n}{2} + 1$
3. $\sharp S_n(123, 321) = 1, 2, 4, 4, 0, 0, 0, \cdots$

Theorem 2.3. [14]
$\sharp\mathrm{B} = 3$ならば$S_n(\mathrm{B})$の個数は以下のいずれかとなる

1. $\sharp S_n(123, 132, 213) = F_{n+1}$, F_n: Fibonacci number, $F_0 = 0, F_1 = 1$
2. $\sharp S_n(123, 132, 231) = \sharp S_n(132, 213, 231) = \sharp S_n(123, 132, 312) = \sharp S_n(123, 231, 312) = n$

BがS_3の元からなる場合はすべて知られており、$\sharp B = 2$で、S_3およびS_4の元からなる場合の数え上げもすでに計算されている。特に$\sharp B = 2$であり双方ともS_4の元からなる場合はいくつかを除いて数え上げは済んでいる。いくつかの場合はSchröder pathとかかわりが指摘されており興味深い [11]。

3　転倒数を用いた重み付き和

3.1　定義といくつかの結果

本節では特に置換の転倒数に注目する。詳細は Kitaev の教科書を参照のこと [9]

Definition 3.1. B を置換の集合として

$$F(n, \mathrm{B}, \mathrm{q}) := \sum_{\pi \in \mathrm{S_n(B)}} \mathrm{q}^{\sharp \mathrm{inv}\pi}$$

と定める。ただし invπ で π の転倒数のペアを表すものとする。

このとき $F(n, \mathrm{B}, \mathrm{q})$ に関して知られている結果をいくつか挙げる。

Example 3.1.

1. $F(n, \phi, q) = \prod_{i=1}^{n-1}(1 + q + q^2 + \cdots + q^i)$
2. $F(n, \{213, 312\}, q) = \prod_{i=1}^{n-1}(1 + q^i)$ [14]
3. $F(n, \{321, 231\}, q) = (1 + q)^{n-1}$ [14]
4. $F(n, \{132, 312\}, q) = \sum_{k=0}^{n-1} q^k F(k, \{132, 213\}, q)$ [14]
5. $S_n(312)$ と Dyck path への Inversion と Path が囲む面積が一致する全単射 [2]
6. $S(321)$ において $\sum_{\pi \in S(321)} x^{n(\pi)} s^{a(\pi)} q^{\mathrm{inv}(\pi)}$ の母関数を用いた表示 $n(\pi)$ は π の次数、$a(\pi)$ は *generating tree* における次数 [3]

特に最後に挙げた Barcucci, Luogo, Pergola, Pinzani は次の定理を示している。

Theorem 3.1. [3]
$S_n(321)$ の置換に対して Inversion の平均は

$$\frac{\sqrt{\pi}}{4} n^{\frac{3}{2}} + o(n)$$

3.2　Even Odd Sum

転倒数を用いた重み付き和において $q = -1$ としたときの値について述べる。つまりは $F(n, \mathrm{B}, -1))$ の値、Permutation Pattern によって制限された置換集合における偶置換と奇置換の差について考える。このような特殊化は極めて自然な発想であり、また以下に述べるように面白い現象が観察されているゆえにすでに知られており、研究が進んでいる可能性も十分にあるが、現時点で Baxter の論文 [4]、Klazar の論文 [10]、Simion Scumidt の論文 [14] およびその参照論文以外に文献は見つからなかった。さらには、今回述べた転倒数以外にも置換から定まる重みとして、descent, peak, valley など様々な物が知られており、それらの $q = -1$ 特殊化についても面白い話があるのではないかと考えている。それらを含めてもしご存知の方があればご教示下さい。初めに基本的な事柄として次の定理を挙げる。

Theorem 3.2. [14]

1. $F(n,\{123\},-1) = F(n,\{231\},-1) = F(n,\{312\},-1) = (-1)^{\binom{n}{2}} C_{(n-1)/2}$
2. $F(n,\{321\},-1) = F(n,\{213\},-1) = F(n,\{132\},-1) = C_{(n-1)/2}$

ただし n が偶数のときは $C_{(n-1)/2} = 0$ と定める。

とくに n が偶数の場合においては Noncrossing Partition における Kreweras Complement から直ちに従う。次の定理は簡単であるが非常に有用である。

Theorem 3.3. [4]
$\sigma = \sigma(1)\sigma(2)\sigma(3)\cdots\sigma(k), \sigma' = \sigma(2)\sigma(1)\sigma(3)\cdots\sigma(k)$ としたとき $F(n,\{\sigma,\sigma'\},-1) = 0$ となる。

特に Corollary として次を得る。

Corollary 3.1. [4]
$F(n,\{3412,3421\},-1) = 0$, $F(n,\{1423,1432\},-1) = 0$, $F(n,\{1234,1243\},-1) = 0 \quad \cdots$

とくに B として S_4 の偶置換および奇置換を 2 つ取ってきたとき常に $F(n,B,-1) = 0$ となるとは限らない。例えば

Proposition 3.1. [4]
$F(n,\{1234,1324\},-1) = -1$ となる。特に $S_7(1234,1324)$ における偶置換の個数は 918、奇置換は 919

Baxter は次の予想を提示した。

Conjecture 3.1. [4]

1. $F(n,\{4231,213\},-1) = 1$
2. $F(n,\{123,1432\},-1) = \pm F_{n-2}$, F_n: Fibonacci number
3. $F(n,\{4312,4213\},-1) = 0$

筆者は次の計算結果を得た。

Proposition 3.2 (Tomie)**.**

1. $F(n,\{4231,213\},-1) = 1$
2. $F(n,\{123,1432\},-1) = (-1)^n F_{n-2}$, F_n: Fibonacci number

$F(n,\{4312,4213\},-1) = 0$ が成立するか否かについては現在のところ分かっていないが Baxter は $n \leq 22$ については成立すると述べている。

4 Permutation Pattern と Weak Bruhat Order

S_n の元 σ, τ に関して $\mathrm{inv}(\sigma) \subset \mathrm{inv}(\tau)$ $\subset$ を満たすとき $\sigma \leq \tau$ と定める。このような半順序集合は Weak Bruhat Order と呼ばれ単位元 e を最小元、最長元 ω を最大元とする束となる。半順序集合に関する基本的な量として Möbius 関数が定義される。Weak Bruhat order に関する性質などは Björner と Brenti の教科書 [5]、半順序集合に関する事柄に関しては Stanley の教科書 [15] を参照のこと。

Definition 4.1. 半順序集合 P 及び $x \leq y \in \mathrm{P}$ に対して Möbius 関数 $\mu([x,y])$ を関係式 $\sum_{x \leq z \leq y} \mu([x,y]) = \delta_{xz}$ を満たす唯一の値として定める。特に P が最大元 $\widehat{1}$ と最小元 $\widehat{0}$ を持つとき $\mu([\widehat{0},\widehat{1}])$ を Möbius 数といい、$\mu(\mathrm{P})$ で表す

特に $S_n(321,312,231)$ および $S_n(321)$ に Weak Bruhat Order を入れ最大元を付け加えた半順序集合 $\widehat{S_n}(321,312,231)$ および $\widehat{S_n}(321)$ を考える。

Theorem 4.1. [17]
$\widehat{S_n}(321,312,231)$ および $\widehat{S_n}(321)$ の Möbius 数は共に $F_{n-2}(-1)$ となる。
ただし $F_n(q)$ は、$F_1(q) = F_2(q) = 1, \quad F_{k+2}(q) = F_{k+1}(q) + qF_k(q)$ て定まる *q-Fibonacci* 数。

Fact 4.1. $S_n(132), S_n(213), S_n(231)$ および $S_n(312)$ に Weak Bruhat Order を入れると Tamari Lattice を得る。とくに Möbius 数は $(-1)^n$

5 Permutation Pattern と Lehmer Code

対称群 S_n の元 σ に対して $c_i(\sigma) := \sharp\{j | i < j,\ \sigma(i) > \sigma(j)\}$ と定め $\mathbf{c}(\sigma) = (c_1(\sigma), c_2(\sigma), \ldots, c_n(\sigma)) \in \mathbb{N}^n$ と置く。この時 $\Lambda_\omega = \{\sigma | \sigma \leq \omega \text{ in weak Bruhat order}\}$ を用いて、$\mathbf{c}(\Lambda_\sigma) \subset \mathbb{N}^n$ を定め、自然数の直積順序でもって半順序構造を入れる。$\mathbf{c}(\Lambda_\sigma)$ は驚くべきことに分配束の構造を持つ [8]。

Theorem 5.1. [8]
$\sigma \in S_n$ に対して $\mathbf{c}(\Lambda_\sigma)$ は分配束

分配束は join irreducible な元からなる部分半順序集合の order ideal 全体に包含関係を入れた順序として実現される。特にこのような部分半順序集合を base poset と呼ぶ。特に $\mathbf{c}(\Lambda_\sigma)$ の base poset を M_σ と置く。

Theorem 5.2. [8]
$c_i(\sigma) \neq 0,\ x \in [c_i(\sigma)]$ に対して $m_{i,x} \in \mathbb{N}^n$ における j 成分を

1. $0 \cdots (j \leq i-1)$
2. $x \cdots (j = i)$
3. $0 \cdots (j \geq i+1 \text{ and } \sigma(i) > \sigma(j))$
4. $\max\{0, x - \sharp\{k | i < k < j,\ \sigma(i) > \sigma(k)\}\}$ $(j \geq i+1 \text{ and } \sigma(i) < \sigma(j))$

と定める。このとき $M_\sigma = \{m_{i,x}(\sigma)|c_i(\sigma) \neq 0,\ x \in [c_i(\sigma)]\}$ となる。

M_σ の構造に関して次の事がすぐにわかる。

Proposition 5.1. [18]
231-avoiding permutation σ に対して M_σ は chain の disjoint union 。また逆は成立しない。たとえば M_{2341} は 231-*pattern* を持っているが長さ *2* の *chain* となる。

次に Permutation Pattern と類似した概念を半順序集合において考える。

Definition 5.1.
半順序集合 P と Q に対して P は Q と同型な部分半順序集合を含まない時 P が Q-free という

例えば $2 \oplus 2$ かつ $3 \oplus 1$ free となる n 点からなる半順序集合の個数は Catalan 数で数え上げられることが知られている [16]。

Theorem 5.3. [18]
$\omega \in S_n(3412, 3421)$ であることと M_ω が B_2-free であることは同値。但し B_2 はランク 2 の Boolean algebra

REFERENCE

[1] D. Armstrong, Generalized noncrossing partitions and combinatorics of Coxeter groups, Mem. Amer. Math. Soc. 202 (2009), no.949.

[2] J. Bandlow and K. Killpatrick, An Area-to-Inv Bijection Between Dyck Path and 312-avoiding Permutations. Electron. J. Combin. 8 (2001), no.1, Research Paper 40, 16pp. (electronic)

[3] E. Barcucci, A. Del Lungo, E. Pergola and R. Pinzani, Some permutations with forbidden subsequences and their inversion number, Discrete Mathematics, 234 (1-3) (2001) 1-15.

[4] A. Baxter, Refining enumeration schemes to count according to inversion number, Pure Mathematics and Applications (Special issue for the proceedings of Permutation Patterns 2009). Volume 21. Issue No. 2. (2010). 137-160.

[5] A. Björner, F. Brenti, Combinatorics of Coxeter groups, Springer-Verlag, New York, 2005.

[6] A. Claesson, Generalized pattern avoidance, European Journal of Combinatorics, [22, 961-971, 2001.

[7] A. Claesson and S. Kitaev, Classification of bijections between 321- and 132-avoiding permutations. Sem. Lothar. Combin. 60 (2008), Art. B60d, 30pp.

[8] H. Denoncourt, A refinement of weak order intervals into distributive lattices, arXiv:1102.2689.

[9] S. Kitaev, Patterns in permutations and words, Springer Verlag (EATCS monographs in Theoretical Computer Science book series) 2011.

[10] M. Klazar, Counting even and odd partitions, Amer. Math. Monthly 110,6(2003), 527-532.

[11] D. Kremer, Permutations with forbidden subsequences and a generalized Schröder number. Discrete Math, 218, 270, 333-344.

[12] D. Knuth, The art of computer programming, I: Fundamental algorithms. Addison-Wesley, Publishing Co, Reading, Mass-London-Don Mills, Ont, 1969

[13] D. Knuth, The art of computer programming, III: Sorting and searching, Addison-Wesley, Reading, MA, 1973.

[14] R.Simion and F. W. Schmidt, Restricted permutations, European Journal of Combinatorics 6(4), 383-406, 1985.

[15] R.P. Stanley, Enumerative Combinatorics, vol. 1, Wadsworth Brooks/Cole, Pacific Grove, CA, 1986; second printing, Cambridge University Press, Cambridge, 1997.

[16] R. P. Stanley, Enumerative Combinatorics, vol. 2, Cambridge University Press, Cambridge, 1999.

[17] M. Tomie, NBB bases of some pattern avoiding lattices, arXiv:0912.4560.

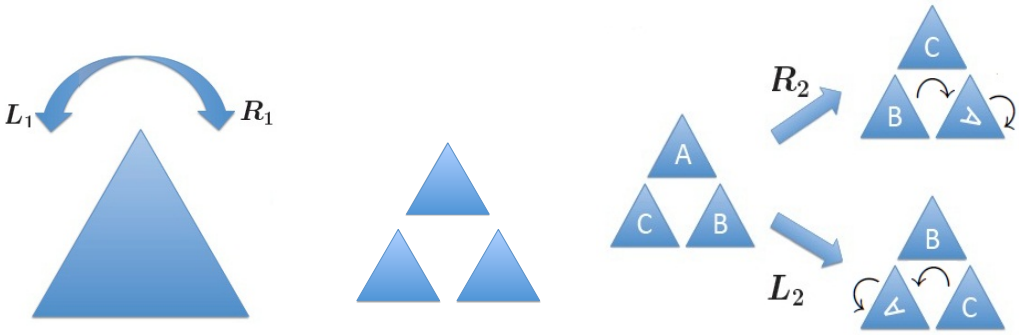
[18] M. Tomie, A relation between the shape of a permutation and the shape of the base poset derived from the Lehmer codes, arXiv:1111.3094.

多重三角形の置換群について

筑波大学数理物質科学研究科数学専攻博士前期課程
山口　正男

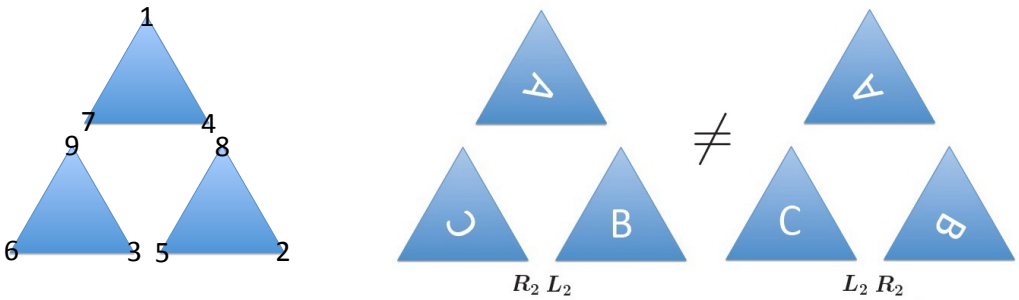
1　導入

まず、正三角形の頂点を回転させる二つ置換、右 120° 回転 R_1 と左 120° 回転 L_1 を考える。次に、この拡張として図のように三つの三角形を大きな三角形の頂点に配置し（これをここでは 2 重三角形とよぶ。）、その置換 R_2 と L_2 を次のように定める。



詳しく説明すると、まず 2 重三角形の上部の三角形 A を R_1 で回転させ、次に（三角形 A,B と C を頂点とする）大きな三角形を R_1 で回転させたものが R_2 である。L_2 は、2 重三角形の上部の三角形 A を L_1 で回転させ、次に大きな三角形を L_1 で回転させたものである。

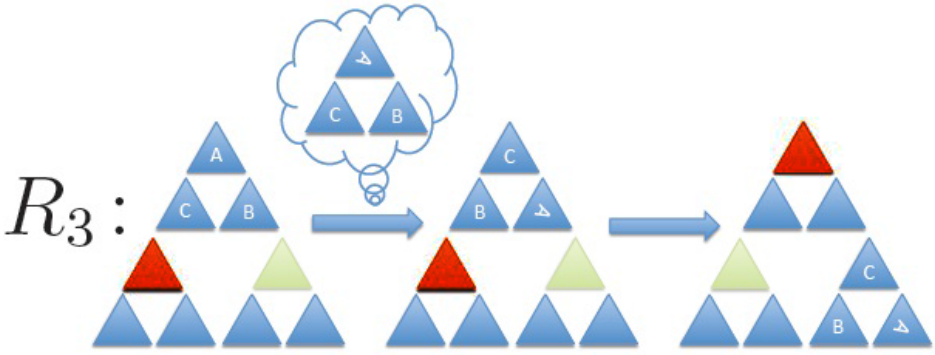
よって、R_2 と L_2 はこの三角形 A,B と C の頂点を合わせた九つの頂点の置換である。そして、下左図のように一番上の頂点は R_2 により順番に $(1,2,3,\cdots,9)$ と移動する。故に R_2 はこの 9 点上可移であり、L_2 も中心線で R_2 と対称であるため可移である。



しかし、R_2 と L_2 は非可換である。実際に上右図のように $R_2\ L_2$ と $L_2\ R_2$

は異なる。但し、積は右から作用するとして表示している。

さらに、これを拡張し上記の２重三角形（3個の三角形）をさらに大きな三角形の頂点に配置したもの（それを３重三角形とする。）の全頂点（２７点）上の置換を定める。先ほどと同様に二つの置換 R_3 と L_3 を考えるのだが、R_3 と L_3 は中心線に関して対称性があるため R_3 だけを説明する。やはり、この時も二つの置換は２７点上可移であり互いに非可換である。



2　置換群の定義

これから 3^n 点上の置換群 G_n を定義する。まず、$R_1 = \sigma_1 = (1,2,3)$ とし $L_1 = \sigma_1^{-1} = (3,2,1)$ とする。この時、$G_1 = \langle \sigma_1 \rangle$ とすると次のように R_2 と L_2 を定義でき $G_2 = \langle R_2, L_2 \rangle$ を定義する。

定義 1
$G_1 = \langle \sigma_1 \rangle$ とし、$G_1 \times G_1 \times G_1$ の成分の置換 $\sigma_2 = (1,2,3)$ を考えリース積 $G_1 \wr \langle \sigma_2 \rangle$ を考える。この時

$$R_2 = \sigma_1 \sigma_2$$
$$L_2 = {\sigma_1}^{-1} {\sigma_2}^{-1}$$

とおき、G_2 をこの R_2 と L_2 で生成された $G_1 \wr \langle \sigma_2 \rangle$ の部分群と定義する。つまり

$$G_2 = \langle R_2, L_2 \rangle \subseteq G_1 \wr \langle \sigma_2 \rangle$$

とする。ここで、右から作用しているとする。

同様に、$n \geq 3$ に対して帰納的に定義する。

定義 2
$G_{n-1} \times G_{n-1} \times G_{n-1}$ の成分の置換 $\sigma_n = (1,2,3)$ を考え

$$R_n = \sigma_1 \sigma_2 \cdots \sigma_n$$
$$L_n = {\sigma_1}^{-1} {\sigma_2}^{-1} \cdots {\sigma_n}^{-1}$$

とおき

$$G_n = \langle R_n, L_n \rangle$$

と定義する。

3　G_n の性質

GAP を使った計算により $n = 1,2,3,4,5,6$ に関して位数は次のようになる。

$$\left|G_1\right| = 3 \quad \left|G_2\right| = 3^3 \quad \left|G_3\right| = 3^8 \quad \left|G_4\right| = 3^{22} \quad \left|G_5\right| = 3^{63} \quad \left|G_6\right| = 3^{165}$$

G_2 の構造をみると

補題 1

$$\left|G_2\right| = 3^3$$

そして、3 つの三角形を回転させる位数 9 の基本アーベル 3 群があり、それ以外の元はすべて位数 9 の元である。

証明

$\langle R_2\rangle$、$\langle L_2\rangle$ と $\langle L_2^{-1}R_2L_2\rangle$ は全て異なる位数 9 の部分群であり、$\langle R_2^3, R_2L_2\rangle$ は位数 9 の基本アーベル群である。

□

予想

$$\left|G_n\right| = \left|G_{n-1}\right|^3 / 3^{n-2}\,(n \geq 2)$$

記号

$n \geq 1$ に対して

$$E_n^1 := \left\{g \in G_n \middle| g^3 = 1\right\}$$

とおく。

定理 1

$n > 1$ に対して

$$\begin{array}{rl} \phi_n \colon & \begin{array}{ccc} G_n & \to & G_{n-1} \\ \cup & & \cup \end{array} \\ & R_n \mapsto R_{n-1} \\ & L_n \mapsto L_{n-1} \end{array}$$

は全射準同型写像になる。

証明

n 重三角形の一番小さい三角形を点と見ることにより上の全射準同型写像が得られる。（ここで、n 重三角形とは $n-1$ 重三角形を大きな三角形の各頂点に配置したのとし、1 重三角形は単に正三角形とする。）

□

記号

$m \geq 1$ に対して

$$E_n^m := \left\{ g \in G_n \middle| g^{3^m} = 1 \right\}$$

とおく。

定理 2

(1) G_n は二元生成である。
(2) $\ker \phi_n$ は基本アーベル 3 群 となる。
(3) E_n^m は G_n の部分群であり、 $E_n^1 = \ker \phi_n \quad (m \geq 1)$
(4) $Z(G_n) = \left\{ 1, {R_n}^{3^{n-1}}, {L_n}^{3^{n-1}} \right\}$ 特に、$\left| Z(G_n) \right| = 3$

証明

(1) は定義より明らか。

$\ker \phi_n$ はすべての最小三角形の配置を固定しているので、各最小三角形の回転の群の直積の部分群である。故に、$\ker \phi_n$ は基本アーベル 3 群である。よって (2) が成り立つ。

(3) を示す。

R_1 と L_1 は正三角形の頂点の回転であるから次のように行列表示できる。

$$R_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, L_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

そして、$G_n \subseteq (G_{n-1} \times G_{n-1} \times G_{n-1}) \rtimes \langle \sigma_n \rangle$ であるから、帰納的に

$$R_n = \begin{bmatrix} 0 & R_{n-1} & 0 \\ 0 & 0 & I_{3^{n-1}} \\ I_{3^{n-1}} & 0 & 0 \end{bmatrix}, L_n = \begin{bmatrix} 0 & 0 & L_{n-1} \\ I_{3^{n-1}} & 0 & 0 \\ 0 & I_{3^{n-1}} & 0 \end{bmatrix} \quad (n \geq 2)$$

と行列表示ができる。

また

$$\begin{array}{ccc} G_n & \subseteq & (G_{n-1} \times G_{n-1} \times G_{n-1}) \rtimes \langle \sigma_n \rangle \\ \downarrow & \phi_n & \downarrow \\ G_{n-1} & \subseteq & (G_{n-2} \times G_{n-2} \times G_{n-2}) \rtimes \langle \sigma_{n-1} \rangle \\ & \vdots & \\ \downarrow & \phi_3 & \downarrow \\ G_2 & \subseteq & (G_1 \times G_1 \times G_1) \rtimes \langle \sigma_2 \rangle \end{array}$$

なので

$$\ker \phi_n \subseteq \ker \phi_{n-1} \times \ker \phi_{n-1} \times \ker \phi_{n-1}$$

である。そして

$$\phi_3 \cdots \phi_n \left(E_n^1\right) \subseteq E_2^1$$

なので、補題 1 より E_n^1 は $G_{n-1} \times G_{n-1} \times G_{n-1}$ の部分群である。
よって、$(E_{n-1}^{\ 1} \times E_{n-1}^{\ 1} \times E_{n-1}^{\ 1}) \cap G_n = \ker \phi_n$ より

$$E_n^1 = \ker \phi_n \quad (n \geq 2)$$

であり E_n^1 の各元は G_1 の元を対角成分とするブロック行列である。
また

$$E_n^m = (\phi_{n-m+1} \cdots \phi_n)^{-1} \left(E_{n-m+1}^{\ 1}\right)$$

なので (3) が成り立つ。特に、$E_n^n = G_n$ である。

次に、(4) について。再び帰納的に示す。補題 1 より $n = 2$ では成り立つ。ゆえに $n \geq 3$ に関して、$n-1$ 以下では (4) が成り立つとする。
いま、$g \in Z(G_n)$ とすると $\phi_n(g) \in Z(G_{n-1})$ より

$$g = \begin{bmatrix} g_1 & 0 & 0 \\ 0 & g_2 & 0 \\ 0 & 0 & g_3 \end{bmatrix} (g_1, g_2, g_3 \in Z(G_{n-1}))$$

である。この時、R_n による共役で g は不変であるが g_1, g_2, g_3 の巡回置換を引き起こす。故に、

$$g_1 = g_2 = g_3 \in Z(G_{n-1})$$

である。つまり、$g_1 = 1, R_{n-1}^{3^{n-2}}, L_{n-1}^{3^{n-2}}$ であるから

$$Z\left(G_n\right) = \left\{1, {R_n}^{3^{n-1}}, {L_n}^{3^{n-1}}\right\}$$

よって、(4) が成り立つ。

□