第20回代数的組合せ論シンポジウム報告集

2003年7月7日～9日

於　北海道大学学術交流会館

平成15年度科学研究費基盤研究(B)

(課題番号 13440001 研究代表者 吉田 知行)

まえがき

この報告集は，２００３年７月７日から７月９日の３日間，北海道大学学術交流会館小講堂において行われた「第20回代数的組合せ論シンポジウム」の講演記録である．遠隔地にもかかわらず１００名近い参加者で盛会でした．

この集会に係わる講演者の旅費，およびこの報告集の作成にあたっては，科学研究費基盤研究（A）「群論とカテゴリー論から見た母関数の研究」(課題番号13440001，研究代表者 吉田知行) の援助を受けています．

最後に，研究集会の参加者，特に講演者とプログラム作成に協力してくださった方々に感謝申し上げます．また，事務手続きや会場関係でお世話になった北海道大学の関係者にお礼申し上げます．

２００３年１２月
吉田 知行

「第20回代数的組合せ論シンポジウム」

日時：平成15年7月7日(月)〜9日(水)
場所：北海道大学学術交流会館小講堂 (北大正門入ってすぐの左手)
世話人：吉田知行 (北大) yoshidat@math.sci.hokudai.ac.jp

この研究集会は，科学研究費 (基盤研究 (1)B) 13440001「群論とカテゴリー論から見た母関数の理論」(代表吉田知行) の援助を受けています.

7月7日 (月)

10:00–11:00 宮本 雅彦 (筑波大学)
E_8-diagram, McKay's observation and vertex operator algebras

11:15–12:15 原田 昌晃 (山形大)–北詰 正顕 (千葉大)
On Some Self-Dual Codes and Unimodular Lattices in Dimension 48

14:00–15:00 岡田 聡一 (名大)–難波 正幸 (名大)
Bruhat 順序の MacNeille completion と alternating sign matrix

15:15–15:45 安部 利之 (東大学振)
頂点作用素代数 V_L^+ の有理性について

15:45–16:15 田辺 顕一朗 (筑波大)
頂点作用素代数の有限位数の自己同型群と Intertwining operator について

16:30–17:00 奥山 京 (鳥羽商専)
Mixed Basic Subgroups

7月8日 (火)

09:30–10:30 川中 宣明 (阪大)
代数的ゲーム理論の現状—「完全可解ゲームの生成」を中心として

10:45–11:45 坂内 英一 (九大)–坂内 悦子 (九大)
ユークリッド空間における種々のデザインの概念と tight デザインの分類

13:30–14:30 岡村 修志 (阪大 D1)
一般化された標準ヤング盤の総数公式の確率論的証明

14:45–15:15 土井 幸雄 (岡山大学)
群環的代数 — 群環の一般化について —

15:15–15:45 中川 暢夫 (近大)
平面関数と有限体上の単項多項式について

16:00–16:30 篠原 雅史 (九大 D1)
Classification of 3-distance sets in 2-dimensional Euclidean space

16:30–17:00 鈴木 寛 (国際基督教大学) On completely regular codes and related topics

7月9日 (水)

09:30–10:00 谷口 浩朗 (詫間電波高専)
A family of dual hyperovals over GF(q), q even

10:00–10:30 平峰 豊 (熊本大)–伊藤 昇
非可解群における (2n,2,2n,n) 差集合について

10:45–11:45 浅井 恒信 (近大)–竹ヶ原 裕元 (室蘭工大)–庭崎 隆 (愛媛大)
On conjectures of crossed homomorphisms, I.

13:00–13:30 浅井 恒信 (近大)–竹ヶ原 裕元 (室蘭工大)–庭崎 隆 (愛媛大)
On conjectures of crossed homomorphisms, II.

13:30–14:00 和田 倶幸 (東京農工大)
Eigenvalues and elementary divisors of Cartan matrices of tame and cyclic blocks

14:00–14:30 小田 文仁 (富山高専)
Crossed Burnside rings for a family of subgroups of a finite group

14:30–15:30 予備

目　次

E_8-diagram, McKay's observation and VOA

宮本雅彦（筑波大学・数学系）

２００３年７月７日（札幌にて）

1　序文

この講演では、最近 C.H.Lam と山田裕理、山内博氏達によって進展している $\sqrt{2}E_8$ 格子の頂点作用素代数 $V_{\sqrt{2}E_8}$ にまつわる結果を有限群論の立場から解説したいと思います。

まず、問題の説明から始めましょう。

モンスター単純群 $\mathbb{M}$ のなかに、位数２の元の共役類は２つあり、$2A, 2B$ と名付けられています。ここで、最初の数字は元の位数を表しており、A, B などの記号は単に中心化群の位数 $|C_{\mathbb{M}}(g)|$ の大きさの順に付けられています。

モンスター単純群の興味ある性質の一つとして、**6-transposition** という性質があります。これは位数２の元のある共役類（今の場合 $2A$ ）の任意の２元 e, f に対して

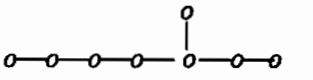
$$|ef| \leq 6$$

ということです。例えば、対称群 S_n の互換 (a, b) の共役類は 3-transposition であり、交代群 A_n の $(a_1, a_2)(a_3, a_4)$ 型の位数２の元の共役類は 6-transposition です。その意味で、6-transposition 群は単純群らしい条件です。

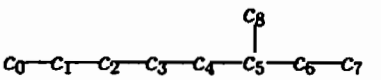
モンスター単純群の場合には、単なる 6-transposition というだけではなく、２つの $2A$ 元 e, f の積 ef の共役類は

$$1A, 2A, 3A, 4A, 5A, 6A, 4B, 2B, 3C$$

の９種類となっているわけですが、この数字と重複度を見て、McKay は E_8-型の単純リー環のルートラティス（E_8 で表す）の最大ウエイトの元です。extended E_8-ルートラティスで考えると長さが 0 の元をルートの和で表示するときの係数になっていることに気づきましたわけです。ここで、E_8-型のディンキンダイアグラムとは、



E_8



Extended E_8

の形のものです。このディンキンダイアグラムから、E_8-型のルートラティス

$$E_8 = \mathbb{Z}c_2 + \mathbb{Z}c_3 + \cdots + \mathbb{Z}c_9$$

に内積

$$\langle c_i, c_i \rangle = 2, \quad \langle c_i, c_j \rangle = \begin{cases} 0 & \text{if no line } c_i\ c_j \\ -1 & c_i \text{---} c_j \end{cases}$$

を入れると、良く知られているように正定値内積を持つ偶格子が出来ます。この時、$t = 2c_1 + 3c_2 + 4c_3 + 5c_4 + 6c_5 + 4c_6 + 2c_7 + 3c_8$ もルート $< t, t >= 2$ となります。これを extended E_8-格子 $\mathbb{Z}c_0 + \mathbb{Z}c_1 + \mathbb{Z}c_2 + \cdots + \mathbb{Z}c_8$ で考えると、これも偶格子で半正定値となり、内部に長さがゼロの（他のものとも直交している）元達は一次元空間

$$\mathbb{Z}1c_0 + 2c_1 + 3c_2 + 4c_3 + 5c_4 + 6c_5 + 4c_6 + 2c_7 + 3c_8)$$

を構成しています。この係数が $2A$ 達の積の共役類の数と一致しているというのが McKay の observation です。

当然、(1) これらを線で結ぶ理由も不明
(2) 数字を並べる理由も A, B, C を付ける理由も不明

です。モンスターにまつわることは偶然で片づけられないという雰囲気もあったのですが、この observation はあまりにも離れており、偶然の一致だろうというのが大半の印象でした。はっきり言って、どうやってこれを示せるのか皆目見当が付かなかったのです。

モンスター単純群 M は Griess によって構成された 196883 次元の Monstrous Griess algebra $\mathcal{B}$（非退化な内積を持つ可換非結合代数）の自己同型群として実現されています。この代数の少し簡単な構成を与えた Conway の論文の中で、彼は

$$2A\text{-involution } g \Rightarrow \text{軸 (ベキ等元) } e_g \in \mathcal{B}$$

を定義し、この対応に注目しています。これは $(C_{\mathrm{M}}(g)$ によって固定されている元達よりなる部分代数のベキ等元（ある意味で単位元）として与えています。この軸の注目すべき性質は、、２つの 2A 元 g, h に対し, 積 gh の共役類が同じなら、内積 $< e_g, e_h >$ も同じだということです。即ち、$2A$ 元達 g_1, h_1, g_2, h_2 があって、g_1h_1 と g_2h_2 の共役類が同じなら、$< e_{g_1}, e_{h_1} >=< e_{g_2}, e_{h_2} >$ なのです。この内積の値を表に書くと、

	$< e, f >$		$< e, f >$		$< e, f >$
$1A$	$256/2^{10}$	$2A$	$32/2^{10}$	$3A$	$13/2^{10}$
$4A$	$8/2^{10}$	$5A$	$6/2^{10}$	$6A$	$5/2^{10}$
$4B$	$4/2^{10}$	$3C$	$4/2^{10}$	$2B$	0

です。気づいて欲しいのは、E_8-ディンキンダイアグラムの点の配置の順番（左の $1A$ からの距離で、$3C$ と $2B$ は同じ距離にある）と内積の大きさが逆順していることです。

モンスター単純群を研究する楽しさの一つは、このような一致に対して、「単なる偶然」と考えない方が良いことに出会えるということです。ここで、大きな問題（将来の夢）を

2つ提起できます。(これが E_8-diagram に対する McKay's observation の本当の意味でしょう。)

(=>) E_8 の構造とモンスターの $2A$-involutions と関係あるか？　より正確には、E_8 の maximal weight のルートに出てくる係数と $2A$-involutions の積の位数との間に関係はあるか？ 簡単に言うと、上のように並べる理由を述べよ。
(<=) モンスターの $2A$ の積の共役類が E_8-diagram しかないこと（もう少し弱く 6-transposition であること）を説明できる方法があるのか？

今回の話では、最初の問題に出てくる数字の関係が頂点作用素代数を使うと上手く説明できることを紹介します。これは、最近 C.H.Lam, 山田裕理, 山内博達によって進展している頂点作用素代数に関する研究です。結果の一部は C.H.Lam によって昨年の京都(12月)での研究集会で報告されていますが、論文はまだ書かれていませんし、[1]内容の多くが頂点作用素代数に関する結果なので、群の部分に的を絞って、群論的な立場から推測できる証明を紹介したいと思います。

これにより、E_8-diagram に対する McKay's observation が単なる偶然ではないことが分かります。特に、最初の問題に関しては、興味深い結果が出てきているということを説明したいと思います。ただ、McKay's observation から想像される世界を考えると、今回の結果はその小さな一部分にすぎないと思いますが、決して偶然の話しではなく、面白いものが隠れているのではないかと期待できます。また問題2に関しては、まったく分かっていません。

2　準備

頂点作用素代数を使って、McKay's observation を説明しますので、少し頂点作用素代数(VOA)の理解が必要です。これからの話しの為（有限群の研究の為）に頂点作用素代数を勉強してもらえるとうれしいのですが、今回はその暇がありませんので、少し事実だけを覚えてもらいます。特に、一般論は使いませんが、頂点作用素代数の特別な元から定義される Miyamoto involution と呼ばれる自己同型が中心的な役割を果たしますので、それに関係した点を中心に説明していきます。

頂点作用素代数（略して VOA）は有限次元の斉次空間 V_i の直和

$$V = \mathbb{C}1 \oplus V_1 \oplus V_2 \oplus V_3 \oplus \ldots$$

の上に無限個の積を持つ代数ですが、ここでは、有限次元空間上の1つか2つの演算を持つ代数だけを扱います。V_i の元をウエイト i の元と呼びます。

(I) 格子から構成される頂点作用素代数

[1]この報告書を書き上げている段階で、プレプリントが出来てきています。

(偶正定値) 格子 L があれば、V_L で表記される格子頂点作用素代数と呼ばれる頂点作用素代数があります。この構造は今回重要なので、これを少し詳しく説明します。

$$L_i = \{a \in L \mid < a, a >= 2i\}$$

とおきます。V_L に出てくる記号は　形式的な $a(-i)$ $(i \in \mathbb{Z})$ と e^a 達です。この形には意味があり、a を変数と思い、微分形式の立場で見ると、$a(-i)$ は $a^{i+1}\frac{d}{da}$ を表していて、e^a は $\exp(a)$ に対応しています。そうすると、 $\exp(a)$ の形の式を高次微分 $\frac{d^n}{da^n}$ したものは、

$$(a^{i_1-1}\frac{d}{da})\cdots(a^{i_k-1}\frac{d}{da})e^a$$

の線形和になりますので、

$$a(-i_1)\cdots a(-i_k)e^a \qquad (i_1 \geq \cdots \geq i_k > 0)$$

の線形和全体の空間を $M(1)e^a$ で表します。一次元格子 $\mathbb{Z}a$ の頂点作用素代数の空間は

$$V_{\mathbb{Z}a} = \oplus_{n\in\mathbb{Z}} M(1)e^{na}$$

です。また、高次元の格子に対しては、

$$V_{\mathbb{Z}a_1+\mathbb{Z}a_2+\ldots+\mathbb{Z}a_n} = \otimes_{i=1}^n V_{\mathbb{Z}a_i}$$

で定義します。一般の格子 $L \subseteq \mathbb{Z}a_1 + \mathbb{Z}a_2 + \ldots + \mathbb{Z}a_n$ に対しては

$$V_L = \oplus_{a\in L} M(1)^{\otimes n} e^a$$

で定義します。これらの元に対して、次数は $\mathrm{wt}(a(-i)) = i$, $\mathrm{wt}(e^a) = \frac{<a,a>}{2}$ で定義します。そうすると、

(I-1) ウエイト 1 の空間 $(V_L)_1$ (リー代数部分)
$\mathbb{C}L$ の基底を $a_1, \ldots, a_k$ とすると

$$(V_L)_1 = (\sum_{i=1}^k \mathbb{C}a_i(-1)1) \oplus \sum_{a\in L_2} \mathbb{C}e^a$$

です。これは内積を持つリー代数となります。今回は内積を使わないので略しますが、リー積は

$$\begin{aligned}
&[a(-1), b(-1)] = 0\\
&[b(-1), e^a] = \langle b, a\rangle e^a\\
&[e^a, e^b] = < a, b > e^{a+b} \text{ if } a+b \in L_2\\
&[e^a, e^{-a}] = a(-1)1
\end{aligned}$$

で与えられています。簡単に述べると、$(V_L)_1$ の左部分 $a_i(-1)1$ 達がカルタン部分代数であり、e^a 部分がルート空間になっています。カルタン部分 $(\sum_{i=1}^k \mathbb{C}a_i(-1)1 \cong \{a(-1)1 \mid$

$a \in \mathbb{C}L\}$ は内積空間として $\mathbb{C}L$ と同型です。

例　L を A_1-型のリー代数 $sl_2(\mathbb{C})$ のルートラティスとすると、$L = \mathbb{Z}a, < a,a >= 2$ となります。この時、ウエイト１の空間は

$$(V_L)_1 = \mathbb{C}a(-1)1 \oplus \mathbb{C}e^a \oplus \mathbb{C}e^{-a}$$

となり、ちょうど、$\mathbb{C}a(-1)1$ の部分がカルタン代数、$\mathbb{C}e^a, \mathbb{C}e^{-a}$ が正と負のルート空間になっており、リー代数としては $sl_2(\mathbb{C})$ と同型です。

また、今回使う格子 L が満たす条件として、$L_1 = \emptyset$ を仮定します。この時、$(V_L)_1 \cong \mathbb{C}L$ です。例えば、任意のルート格子 H に対して、$L = \sqrt{2}H$ （内積を２倍）とすると、この条件を満たしています。

(1-2) ウエイト２の空間 $(V_L)_2$（グライス代数部分＋少し）は

$$\sum_{i \le j} \mathbb{C}a_i(-1)a_j(-1)1 \oplus \sum_{<a,a>=4} \mathbb{C}e^a + \sum_i \mathbb{C}a_i(-1)1$$

です。これも $\times_3$ 積と $\times_1$ 積によって、不変内積を持つ代数となります。

(II) 中心電荷 1/2 の共形元

$< a,a >= 4$ となる元 $a \in L$ があると、２つのウエイト２の元

$$e^{\pm}(a) = \frac{1}{16}a(-1)^2 1 \pm \frac{1}{4}(e^a + e^{-a})$$

が定義できるわけですが、これらは両方とも中心電荷 1/2 の共形元[2]となります。
(II-1) 共形元 e とはグライス代数の中で考えるとベキ等元 $e/2$ を２倍したものと考えて良いことが分かります。また、中心電荷 c は $< e/2, e/2 > \times 8$ と一致しています。

(III) $2A$-involution

$c = 1/2$ の有理共形元[3] e があれば、
(III-1) 自己同型 τ_e （位数高々２）が定義できる。
(III-2) $\tau_e = 1$ なら、$\sigma_e \in \mathrm{Aut}(V)$ （位数高々２）が定義できる。（σ 自己同型同士の積の位数は高々３であり、鏡映とおなじような性質を満たす。）
(III-3) $\sigma_e = 1$ なら、e は他のウエイト２の元やウエイト１の元と直交する。特に、頂点

[2]共形元とは、ウエイト２の元 e であって、それの n 番目の積 $\tilde{L}(n-1) = e \times_n$ 全体を考えると、$[\tilde{L}(n), \tilde{L}(m)] = (n-m)\tilde{L}(n+m) + \frac{n^3-n}{12}c$ というヴィラソロ代数の関係式を満たす元のことである。c を中心電荷と呼ぶ。

[3]有理共形元とは、e から作用素 $\tilde{L}(m)$ 達を作用させて生成されるヴィラソロ頂点作用素部分代数が単純であり、その加群がすべて既約加群の直和になることです。

作用素代数としてテンソル積に分解する。

ムーンシャインVOA		モンスター単純群
e: $c=1/2$ の共形元	$\leftrightarrow$	2A-involution τ_e
$=$ 軸	1 : 1 対応	

(IV) 共形元

H を A_n, D_n, E_n 型などのルート格子とする。$L=\sqrt{2}H$ の格子頂点作用素代数 $V_{\sqrt{2}H}$ において、各ルート $a\in H$ に対して、中心電荷 $1/2$ の有理共形元

$$e^{\pm}(\sqrt{2}a)=\frac{1}{8}a(-1)^2\mathbf{1}\pm\frac{1}{4}(e^{\sqrt{2}a}+e^{-\sqrt{2}a})$$

が2つ定義できる。

(IV-1) $\sqrt{2}H$ 型の格子から構成された頂点作用素代数の場合には、上の様にして構成した共形元によって定義される τ-involutions はすべて自明です。
グライス代数の内部では、これらの共形元の積は

$$4e^-(\sqrt{2}a)e^-(\sqrt{2}b)=\begin{cases}0 & \text{if } <a,b>=0\\ e^-(\sqrt{2}a)+e^-(\sqrt{2}b)-e^-(\sqrt{2}(a+b)) & \text{if } <a,b>=-1\\ e^-(\sqrt{2}a)+e^-(\sqrt{2}b)-e^-(\sqrt{2}(a-b)) & \text{if } <a,b>=1\end{cases}$$

となっています。結論を述べると、

$$R(H)=<e^-(\sqrt{2}a):a\in H_2>$$

は単位元 (idempotent) $\omega^H/2=\frac{2}{h+2}\sum_{a\in H_2^+}e^-(\sqrt{2}a)$ を持つ部分代数となっています。ここで h はコクスター数 (=ルートの数/次元) です。グライス代数全体は、単位元

$$\omega/2=\frac{1}{h}\sum_{a\in H_2^+}(e^+(\sqrt{2}a)+e^-(\sqrt{2}a))$$

を持っているので、

$$\tilde{\omega}=\omega-\omega^H$$

は中心電荷 $\frac{2k}{h+2}$ の共形元 (last 共形元) となります。
下に last 共形元の中心電荷の例を書いておきます。

A_1	$1/2$	A_2	$4/5$	A_3	1	A_4	$8/7$
A_5	$5/4$	A_6	$4/3$	A_7	$7/5$	A_8	$16/11$
E_6	$6/7$	E_7	$7/10$	E_8	$1/2$		

注目して欲しいのは、$H=E_8$ とすると、last 共形元の中心電荷が $c=\frac{2\times 8}{30+2}=\frac{1}{2}$ となることです。

(V) リー群の自己同型

説明したように、V_1 空間はリー代数であり、しかも $a \in V_1$ に対して、ゼロ積 $a\times_0 = a(0)$ を使って、$exp(a(0))$ を考えると、これは V_L の自己同型となります。特に、$a = a(-1)1 \in \mathbb{C}L$ とすると、

$$a(0)e^b =< a, b > e^b \qquad \exp(2\pi i a(0))e^b = e^{2\pi i<a,b>}e^b$$

であり、

$$< a, b >\in \mathbb{Z} \Rightarrow \exp(2\pi i a(0)) = 1 \text{ on } M(1)^{\otimes n}e^b$$
$$< a, b >= k/p \quad ((k, p) = 1) \Rightarrow \exp(2\pi i a(0)) \text{ の位数は } p \text{ です。}$$

(V-1) $K \subseteq L$ を部分格子として、$a \in \mathbb{Q}L$ で、

$$< a, K >\subseteq \mathbb{Z}, \quad < L, a >\subseteq \mathbb{Z}/p \quad (p \text{ 自然数})$$

とすると、$exp(a(0))$ は 部分頂点作用素 V_K の上で自明な位数 p の自己同型となります。

3 VOA の部分VOAの構成とその意味

説明を始めましょう。元々は、私が２つの共形元 e, f で

$$< \tau_e, \tau_f >\cong S_3$$

となる場合を分類したのが最初です。$|\tau_e\tau_f| = 3$ となる場合には、不思議なことにモンスター単純群に現れる状況と同じ@3A@型と@3C@型の２つの場合しかなく、
$3A$ 型だと、内積は $\frac{13}{2^{10}}$ で $VOA < e, f >$ のヴィラソロ元（単位元）ω は２つの共形元 (idempotents) w^1, w^2 の直交和に分かれ、それぞれ、中心電荷 $\mathbf{4/5 + 6/7}$ となり、
$3C$ 型だと、内積は $4/2^{10}$ で中心電荷 $1/2$ の共形元以外の共形元はみつからず、全体の中心電荷は $16/11$ となっている
ことが分かったわけです。僕自身は、これはバイモンスターの２６点 nodes やモンスター単純群の３元体上のアフィン平面における９点と１２線の関係に結びつけるつもりだったので、@3A@の方を強調した形の論文です。

この結果を見て、山内君（筑波大 D3)が「$3A$ 型 $VOA(e, f)$ と $3C$ 型 $VOA(e, f)$ を $V_{\sqrt{2}E_8}$ の中で実現できないか」と C.H.Lam に持ちかけたのがきっかけで、Lam が調べはじめ、上の中心電荷の和が $A_2 + E_6$, A_8 の last 共形元の中心電荷と一致することに気づいたわけです。そう考えると、$2A : A_1 + E_7$, $1A : E_8$, $2B : D_8$ 達が（自明ですが）同じことになっているわけです。@4B@ は島倉君（東大学振)の結果を使って分かります。この段階で、昨年の１２月に Lam が京都で発表しました。それで、C.H.Lam と山田さんと山内君達が他の $5A, 6A, 4B$ などの個々のケースごとに、$V_{\sqrt{2}E_8}$ の中に、$VOA(e, f)$ で、$\tau_e\tau_f$ が位数 p であり、ヴィラソロ元が上のような extended E_8-lattice の１点を除いたルート系の last 共形元の形になるものを構成していったわけです。あとで説明しますが、p が奇数の場合には成功するのですが、p が偶数の場合には 位数 $p/2$ のものが見つかってきました。

4 統一的な構成

(1) $V_{\sqrt{2}E_8}$ の形
ウエイト1の空間は8次元で、可換なリー代数 E_8 のすべてのルート a に対して、$e^{\pm}(a)$ という中心電荷 1/2 の共形元が決まります。これらの自己同型はすべて σ-involutions です。E_8-型なので、last 共形元 ω^1 の中心電荷は 1/2 であり、これは τ-involution $\tau(\omega^1)$ を与えていることが分かります。特に、簡単な計算から、ウエイト1の空間に -1 倍として作用していることが分かります。

(2) E_8-ルート格子構造
extended E_8-ディンキンダイアグラムの中から1点を取り除いたルート系の次元は8なので、それは E_8-lattice の同じランクの部分格子 L となります。しかも、指数は p (の巡回群) です ($p = 1, 2, 3, 4, 5, 6$)。

(2-1) 自己同型
この部分格子 L と $< a, L > \subseteq \mathbb{Z}$ となる元 a を使って、exponential 型の自己同型 $\rho = exp(a(0))$ で位数 p のものが定義できます。τ_{ω^1} はウエイト1の空間に -1 倍として作用しているので、$\theta = \tau_{\omega^1}$ は ρ を逆元に移します。即ち、$\theta(\rho)\theta^{-1} = (\rho)^{-1}$ です。

(3) 共役な別の共形元
$\omega^2 = \rho(\omega^1)$ とおくと、これは、中心電荷 1/2 の共形元で次を満たします。

$$\tau_{\omega^1}\tau_{\omega^2} = \rho^2$$

(4) 直交しているものの集まり
ω^1 は $e^-(\sqrt{2}a) : a \in (E_8)_2$ 達と直交しています。定義から、ρ は $e^-(\sqrt{2}a) : a \in L_2$ を固定し、それらの σ-involutions 達と可換なので、ω^2 は $e^-(\sqrt{2}a) : a \in L_2$ 達と直交していることが分かります。即ち、

$$VOA(e, f) \otimes < e^-(\sqrt{2}a) : a \in L_2 > \subseteq V_{\sqrt{2}E_8}$$

です。これにより、$VOA(e, f)$ のヴィラソロ元は L の last 共形元（達の和）となります。

(5) ウエイト1の空間が残らないこと
(5-1) Extended E_8-diagram から1点の除いたルート系 L を考えていますので、全体で8次元です。また、ワイル群の中にはカルタン部分代数に固定点（自明な0は除く）を持たないものがあります。
(5-2) $e^-(\sqrt{2}a)$ 型の共形元から生成される σ-involutions は reflections と同じものです.

この構成だと、$\tau_{\omega^1}\tau_{\omega^2} = \rho^2$ なので、ρ の位数 p が奇数の場合には、$\tau_{\omega^1}\tau_{\omega^2}$ の位数は希望通り p となりますが、p が偶数の場合には $\tau_{\omega^1}\tau_{\omega^2}$ の位数は $p/2$ となってしまい、希望とは異なります。しかし、これは当然のことなのです。ある頂点作用素代数の上で $\tau_{\omega^1}\tau_{\omega^2}$

の位数が偶数 p の場合には、$\phi = (\tau_{\omega^1}\tau_{\omega^2})^{p/2}$ は Dihedral 群 $< \tau_{\omega^1}, \tau_{\omega^2} >$ の中心に入りますので、ω^1, ω^2 を固定することが起きても不思議ありません。(実際に、ムーンシャイン頂点作用素代数においては τ-involutions と 共形元が 1:1 対応していますので、この現象が起きています。) それ故、ϕ の固定空間だけを考えると、共形元 ω^1, ω^2 が含まれており、$\tau_{\omega^1}\tau_{\omega^2}$ の位数は $VOA(\omega^1, \omega^2)$ においては $p/2$ なのです。では今回の場合、実際により大きな頂点作用素代数の上で位数 p となっていることを示しましょう。よく知られているように、リーチ格子 Λ は

$$\sqrt{2}E_8 \oplus \sqrt{2}E_8 \oplus \sqrt{2}E_8 \subseteq \Lambda$$

を満たしています。この埋め込みを考えると、

$$V_{\sqrt{2}E_8} \otimes V_{\sqrt{2}E_8} \otimes V_{\sqrt{2}E_8} \subseteq V_\Lambda$$

が成り立ち、V_Λ の中で考えると、ρ の位数は $2p$ となっており、$\tau_{\omega^1}\tau_{\omega^2}$ の位数が p となっていることが分かります。

(6) $\mathbb{Z}_p$-orbifold construction

リーチラティス Λ の頂点作用素代数 V_Λ に対して、ウエイト 1 の空間 ($\mathbb{C}\Lambda$ と同型) に固定点を持たない自己同型 ρ がある時、固定点の空間 $(V_\Lambda)^\rho$ はウエイト 1 の元を持ちません。これから $V^\natural$ が構成できるだろうと言われています。現在分かっているのは Λ 上で $\rho = -1$ の場合だけです。

$p = 3$ が出来たと言っている方もおられますが、何年も preprint レベルの論文もありません。

$p \leq 8$ の場合に正しいとすると、上で構成した $VOA(e, f)$ および、V_Λ の中への埋め込みはすべて $V^\natural$ の中に埋め込むことができます。

この $V_{\sqrt{2}E_8}$ だけに関する埋め込み問題は $\mathbb{Z}_p$-construction より簡単なことだと思われますので、考察すべき対象だと思っています。(いくつかは出来ています。)

On Some Self-Dual Codes and Unimodular Lattices in Dimension 48

原田昌晃 (山形大)・北詰正顕 (千葉大)

平成16年1月9日

1 序文

この原稿は, 講演者2名と宗政昭弘氏と Boris Venkov 氏との共同研究の結果 ([6]) について, 講演をした部分を中心にまとめたものである. 残念ながら割愛した部分もあるので, 細かな部分については原論文 [6] を参照していただければと思う.

今回登場するのは長さ 48 の code と 48 次元の lattice であるので, 特に注意しない限り code も lattice もそのように考えていただきたい.

長さ n の doubly-even self-dual code と次元 n の even unimodular lattice の minimum weight d と minimum norm μ については

$$d \leq 4\left[\frac{n}{24}\right] + 4,\ \mu \leq 2\left[\frac{n}{24}\right] + 2$$

であることが知られている. minimum weight d と minimum norm μ の bound が上がるところが 24 の倍数であり, 24 の次にきれいな状況になっているのは 48 次元ではないかと思われるのである. 24 次元は Steiner system $S(5,8,24)$, Golay $[24,12,8]$ code G_{24}, Mathieu 群 M_{24}, Leech lattice, Conway 群とあらゆる役者が勢揃いであるが, Leech lattice と Golay code しかないとも言えるわけで, 48 次元では比較的多くの研究対象が存在し, 有限群論からは離れるが, 興味深いものであると言えると思う.

ここでは, extremal singly-even self-dual code と extremal odd unimodular lattice について考える. doubly-even self-dual code や even unimodular lattice については, 多くの研究があり, 例えば, extremal doubly-even

self-dual [48, 24, 12] code の一意性が, ごく最近になって示されている [7]. 我々は shadow という概念と neighbor という関係を通じて, doubly-even self-dual code, even unimodular lattice と singly-even self-dual code, odd unimodular lattice についての情報を得ようと考えたのである.

2 Code と lattice からの準備

まず幾つか言葉の説明から始めることにする. C を (binary) self-dual code とする, つまり C は $C = C^{\perp}$ を満たす code である, ここで $C^{\perp}$ は C の通常の内積に関する dual code を表す. self-dual code は二つのクラスに分かれ, 全ての weight が 4 の倍数の場合 *doubly-even* とよばれ weight $\equiv 2 \pmod 4$ の codeword を含む場合 *singly-even* とよばれる.

C を singly-even self-dual code とし, C_0 で weight $\equiv 0 \pmod 4$ である codeword からなる subcode を表すことにする. ここで C_0 は指数 2 の subcode になる. C の *shadow* S は $C_0^{\perp} \setminus C$ で定義される. このとき C_0 の coset C_1, C_2, C_3 で $C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$ なるものが存在する, ここで $C = C_0 \cup C_2$, $S = C_1 \cup C_3$.

二つの長さ n の self-dual code C, C' が $\dim C \cap C' = n/2 - 1$ であるとき C, C' は *neighbor* であるという. もし C が singly-even self-dual code でその長さが 8 の倍数であれば C は丁度二つの doubly-even self-dual neighbor $C_0 \cup C_1$ と $C_0 \cup C_3$ をもつ.

Extremal singly-even [48, 24, 10] code の weight enumerator の可能性は二通り $(W_{48,1}, W_{48,2})$ であることが知られている [2]. ここでは code とその shadow の weight enumerator を挙げておく:

$$\begin{cases} W_{48,1} &= 1 + 704y^{10} + 8976y^{12} + 56896y^{14} + \cdots, \\ S_{48,1} &= y^4 + 44y^8 + 17021y^{12} + \cdots, \end{cases}$$

$$\begin{cases} W_{48,2} &= 1 + 768y^{10} + 8592y^{12} + 57600y^{14} + \cdots, \\ S_{48,2} &= 54y^8 + 16976y^{12} + \cdots. \end{cases}$$

次に lattice の方の準備をする. L を unimodular lattice とする, つまり L は $L = L^*$ を満たす lattice である, ここで L^* は L の通常の内積 (x, y) に関する dual lattice を表す. unimodular lattice は二つのクラスに分かれる. 全ての norm が偶数の場合 *even* とよばれ奇数の norm を含む場合 *odd* とよばれる.

L を odd unimodular lattice とし L_0 で全ての norm が偶数である vector だけの sublattice を表すことにする. code のときと同様に L_0 は指数 2 の sublattice になることが分かっている [3]. L の *shadow* S は $L_0^* \setminus L$ で定義される. このとき L_0 の coset L_1, L_2, L_3 で $L_0^* = L_0 \cup L_1 \cup L_2 \cup L_3$ なるものが存在する, ただしここで $L = L_0 \cup L_2$, $S = L_1 \cup L_3$.

二つの lattice L, L' が *neighbor* であるとは共に指数 2 の同じ sublattice を含む場合のことをいう. 次元が 8 の倍数の場合, L が odd unimodular lattice ならば丁度二つの even unimodular neighbor $L_0 \cup L_1$, $L_0 \cup L_3$ が存在する.

Conway–Slaone [3] の Section 1 に与えられている結果によって 48 次元の extremal odd unimodular lattice とその shadow の theta series の可能性が次の 2 種類に決められることが簡単な計算によって分かる:

$$\begin{cases} \theta_{L_{48,1}} = 1 + 385024q^5 + 26398208q^6 + \cdots, \\ \theta_{S_{48,1}} = 2q^2 + 2256q^4 + 52318616q^6 + \cdots, \end{cases}$$

$$\begin{cases} \theta_{L_{48,2}} = 1 + 393216q^5 + 26201600q^6 + \cdots, \\ \theta_{S_{48,2}} = 2400q^4 + 52313600q^6 + \cdots. \end{cases}$$

3 Code についての結果

次の結果は [1] で与えられている結果であるが証明が簡単なことと lattice の結果との関連を明白にするためにここでも証明を与えることにする.

命題 3.1. C を extremal doubly-even self-dual $[48, 24, 12]$ code とする. C は必ず weight enumerator $W_{48,1}$ をもつ extremal singly-even self-dual $[48, 24, 10]$ code を neighbor としてもつ.

(証明) w を weight 4 の vector とする. すると

$$N = (C \cap \langle w \rangle^\perp) \cup \{u + w \mid u \in C \setminus \langle w \rangle^\perp\}$$

が C の singly-even neighbor になることが分かる. $(C \cap \langle w \rangle^\perp)$ の部分は minimum weight は 12 以上であることがすぐに分かるので, 残りの部分の minimum weight がどのようになるかを考えればよい. ここで w と u の交わりは 1 か 3 であるので $w + u$ という形の vector の weight は 10 以上であることが分かる. したがって minimum weight は 10 になる. また, w が shadow の vector であることから weight enumerator は $W_{48,1}$ になる. □

ここではこの逆が成り立つことを示す.

定理 3.2. C を extremal singly-even self-dual $[48, 24, 10]$ code とする. このとき C は weight enumerator として $W_{48,1}$ をもつ. すると $C_0 \cup C_1$ または $C_0 \cup C_3$ は extremal doubly-even self-dual $[48, 24, 12]$ code になる.

(証明) まず D を doubly-even self-dual $[48, 24]$ code とし, その weight enumerator を $W_D = \sum_{i=0}^{12} a_{4i} y^{4i}$ で表すことにする. このとき $a_4 = 1$ であれば $a_8 \geq 44$ と $a_8 \equiv 2 \pmod 6$ が成り立つことが示される. この結果はこの定理の証明の本質的な部分になっているが講演でも証明には言及しなかったので, この原稿でも触れないことにする. なお, 興味のある方は原論文を見ていていただきたい.

次に C_1 が shadow に唯一つだけある weight 4 の vector を含むと仮定しても一般性は失わない. Shadow の weight enumerator $S_{48,1}$ から C_1 の weight 8 の vector は多くても 44 個である. ここで $C_0 \cup C_1$ は doubly-even self-dual neighbor になるが上の結果より shadow の weight 8 の vector を全て含むことになる. その結果, shadow の weight 8 以下の vector は全て C_1 に含まれることになるので, 別の doubly-even self-dual neighbor $C_0 \cup C_3$ の minimum weight は 12 になる. □

次に [9] で与えられた方法を用いて長さ 48 の extended quadratic residue code QR_{48} の全ての extremal singly-even self-dual $[48, 24, 10]$ neighbor を決定したので, その結果を述べる. この部分の計算は MAGMA を用いて行なわれた.

命題 3.3. QR_{48} は丁度 74 個の非同値な extremal singly-even self-dual $[48, 24, 10]$ neighbor を持つ.

この neighbor の分類結果の詳細は原論文を見ていただくことにして割愛するが, 74 個の内 10 個は weight enumerator として $W_{48,1}$ を持つことを注意しておく.

次に Houghten, Lam, Thiel and Parker [7] の最近の結果を述べることにする.

定理 3.4 (Houghten et al. [7]). 全ての extremal doubly-even self-dual $[48, 24, 12]$ code は QR_{48} に同値である.

この結果と, 上で述べた neighbor の分類と定理 3.2 より次が得られる.

命題 3.5. $W_{48,1}$ を weight enumerator とする extremal singly-even self-dual $[48,24,10]$ code は（同値を除いて）丁度 10 個存在する.

上の 10 個の code は命題 3.1 の証明中に与えられた構成方法にて得られるので, shadow の weight 4 の vector w を与えれば十分である. w の support を以下に書く:

$$\{1,2,3,4\},\{1,2,3,5\},\{1,2,4,5\},\{1,2,3,6\},\{1,2,4,6\},$$
$$\{1,2,3,7\},\{1,2,4,7\},\{1,3,4,7\},\{1,3,6,7\},\{1,4,6,7\}.$$

ただし, 座標を固定した QR_{48} を次の生成多項式をもつ巡回符号の extended code として定義することにする:

$$x^{23}+x^{19}+x^{18}+x^{14}+x^{13}+x^{12}+x^{10}$$
$$+x^9+x^7+x^6+x^5+x^3+x^2+x+1,$$

ここで生成多項式からの生成行列の与え方については [8, pp. 190–191] を参照することにする, また拡大された座標は最後にとることにする.

次に $W_{48,2}$ を weight enumerator とする extremal singly-even self-dual $[48,24,10]$ code について考える. QR_{48} の neighbor として 64 個存在することが分かっているがそれで全てだろうか.

N_{48} を $QR_{48}\cap\langle x,y\rangle^{\perp}$ と $\langle x,y\rangle$ で生成される singly-even self-dual code とする, ただし

$$x=(000000100000010101000000111000100100000000000100),$$
$$y=(000000000000011101000001011000101110011000100110),$$

でさらに QR_{48} は上で定義したものとする. このとき N_{48} は extremal singly-even self-dual $[48,24,10]$ code でその weight enumerator は $W_{48,2}$ となる. N_{48} の二つの doubly-even self-dual neighbor $D_{48,1}, D_{48,2}$ は次のような weight enumerator をもつ:

$$W_{D_{48,1}}=1+24y^8+17104y^{12}+\cdots,\ W_{D_{48,2}}=1+30y^8+17056y^{12}+\cdots.$$

したがって次を得る.

命題 3.6. Weight enumerator $W_{48,2}$ については二つの doubly-even neighbor がともに extremal にならないものが存在する.

以上より $W_{48,1}$ を weight enumerator としてもつ extremal singly-even self-dual code は neighbor を介して extremal doubly-even self-dual code と完全に結びつけることが出来るが $W_{48,2}$ の方は同じような状況ではないことが分かった. 分類を含めて特徴付けが出来るかどうかは今後の課題であると思われる.

さらに注意を一つ述べる. $W_{48,1}$ を weight enumerator としてもつ extremal singly-even code の場合は, その shadow の weight enumerator は一意的に C_1, C_3 の weight enumerator W_{C_1}, W_{C_3} に分けられる. つまり code C の選び方によらず

$$W_{C_1} = y^4 + 44y^8 + 8701y^{12} + \cdots, \ W_{C_3} = 8320y^{12} + \cdots$$

となる. しかしながら $W_{48,2}$ を weight enumerator としてもつ場合は W_{C_1}, W_{C_3} への分解は一意的ではないことが上の命題から分かる. つまり shadow の weight 8 の 54 個の vector の C_1 と C_3 への分解は $0+54$ や $24+30$ の場合の例を実際に構成した訳である. 我々は, この分解の全ての可能性を決定したかったのではあるが, 現時点ではまだ得られていない.

4 Lattice についての結果

上で述べた code の場合の結果と同じような結果が lattice についても得られている.

命題 4.1. L を extremal even unimodular lattice とする. このとき L は必ず theta series が $\theta_{L_{48,1}}$ である extremal odd unimodular neighbor をもつ.

(証明) w を norm 2 のベクトルで, $2w \in L$ をみたすものとする. L が extremal であることから, その theta series は一意に決まり, その 8 次の係数が 0 でないことから, L は norm 8 のベクトルを必ず含むので, その 1/2 倍を w とすればよい. すると, $w \notin L$ であるから, $(w, y) \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$ をみたす $y \in L$ が存在する. このとき

$$N = (L \cap \langle w \rangle^*) \cup \{u + y + w \mid u \in L \setminus \langle w \rangle^*\}$$

が L の odd neighbor になることが分かる. $(L \cap \langle w \rangle^*)$ の部分は minimum norm は 6 以上であることがすぐに分かるので, 残りの部分の minimum

norm がどのようになるかを考えればよい. ここで $a = u + y + w \in y + w + (L \setminus \langle w \rangle^*)$ とおくと, w と a の内積は 0 でない半整数であるので, 一般性を失わずに $(a, w) \leq -\frac{1}{2}$ としてよい. すると, $a + w$ が L に含まれることに注意すると,

$$6 \leq (a + w, a + w) \leq (a, a) + 1$$

より $(a, a) \geq 5$ を得る. したがって N の minimum norm は 5 になる. また, w が shadow の vector であることから theta series は $\theta_{L_{48,1}}$ になる. □

注意 4.2. 講演の際には, この証明は (長さは変わらないものの) もう少し tricky なものになっていた. 講演の直後に証明を整理して, 上のような簡単な形にしたら, だんだん自明なことに思えてきたので「定理」から「命題」に格下げしたのである.

Code の場合と同様に, この逆が成り立つことが示される. ここで述べる証明は Harmonic thata series を用いるもので, 言ってみれば, Venkov 氏の得意の手法を用いるものである.

定理 4.3. L を theta series が $\theta_{L_{48,1}}$ である extremal odd unimodular lattice とすると L は必ず extremal even unimodular neighbor をもつ.

(証明) まず, $L_0 \cup L_1, L_0 \cup L_3$ を L の 2 つの even neighbor とする. L_1 が shadow に唯一つだけある norm 2 の vector を含むと仮定してよい. これを α と表す. $\theta_{S_{48,1}}$ の 4 次の係数から, $L_1 \cup L_3$ の norm 4 の vector の総数は 2256 である.

ここで, 次の補題を証明なしに用いることにする.

補題 4.4. 一般に, Λ を 48 次元の even unimodular lattice, $\alpha \in \mathbb{R}^{48}$ とするとき, harmonic theta series

$$\vartheta_\Lambda(q) = \sum_{x \in \Lambda} \left((\alpha, x)^2 - \frac{1}{48}(\alpha, \alpha)(x, x) \right) q^{(x,x)/2}$$

は weight 26 の cusp form である. 特に, ある定数 c に対して

$$\vartheta_\Lambda(q) = c(q - 48q^2 + \cdots)$$

と表される. □

$N = L_0 \cup L_1$ とおいて, この補題を適用すると, $\vartheta_N(q) = c(q - 48q^2 + \cdots)$ の 1 次の係数を -48 倍したものが 2 次の係数になるから, N の norm k のベクトル全体の集合を $N(k)$ と書くことにすれば,

$$\sum_{\lambda \in N(4)} \left((\alpha, \lambda)^2 - \frac{1}{6} \right) = -48 \sum_{\lambda \in N(2)} \left((\alpha, \lambda)^2 - \frac{1}{12} \right)$$

となるが, $N(2) = \{\pm\alpha\}$ であるから左辺は $-\frac{47 \cdot 48}{6}$ に等しいことが容易にわかる.

ここで, $(\alpha, \lambda) = 0$ が任意の $\lambda \in N(4)$ について成り立つことを示す. 実際, $\alpha, \lambda \notin L_0$ より $\alpha \pm \lambda \in L_0$ となり,

$$(\alpha \pm \lambda, \alpha \pm \lambda) = 6 \pm 2(\alpha, \lambda) \geq 6$$

から主張を得る.

これを用いると, 右辺は $-\frac{1}{6}|N(4)|$ となるから, 合わせて, $|L_1(4)| = 47 \cdot 48 = 2256$ となり $L_3(4) = \emptyset$ を得る. すなわち, $L_0 \cup L_3$ には norm 4 の vector は含まれず, minimum norm は 6 になる. □

48 次元の extremal even unimodular lattice は P_{48p}, P_{48q}, P_{48n} という記号で表される 3 つが知られているだけで, 分類は完成していない. 従って, code の場合のような分類 (命題 3.5) のような結果は得られない. 仮に lattice をひとつ固定したとしても, その extremal odd unimodular neighbor を全て求めるのは難しいと思う.

次に, theta series が $\theta_{L_{48,2}}$ であるような extremal odd unimodular lattice について考えよう. 結論から言うと, code の場合と同様に extremal even unimodular lattice を neighbor に持つものも, 持たないものも存在する.

定理 4.5. Theta series が $\theta_{L_{48,2}}$ である extremal odd unimodular lattice については, 一つの extremal even unimodular lattice P_{48q} の neighbor となっているものも存在し, 二つの even neighbor ともが extremal でないものも存在する.

前者の lattice は次のように構成された. 知られている 3 つの extremal even unimodular lattice のうちの P_{48p} と P_{48q} については Construction A によってある Type II $\mathbb{Z}_6$-code から構成されることが分かっている [5].

まず $C_{48q}^{(6)} = (B_{48q}, T_{48q})$ を [5] で与えられている $A_6(C_{48q}^{(6)}) = P_{48q}$ なる code とする. ここで Type II (Type I) $\mathbb{Z}_6$-code は binary doubly-even (singly-even) self-dual code B と ternary self-dual code T のペア (B,T) とみなせることに注意. B_{48q} は doubly-even self-dual code d_{48}^+ に同値である (d_{48}^+ の定義は [10, Section 11] を参照). B_{48q} の singly-even self-dual neighbor のなかから $A_6(C'^{(6)}_{48q}(= (B'_{48q}, T_{48q})))$ が extremal odd unimodular lattice で kissing number 393216 となる B'_{48q} が見付かった. このとき (B_{48q}, T_{48q}) と (B'_{48q}, T_{48q}) が指数 2 の subcode を共通に含むので $A_6((B'_{48q}, T_{48q}))$ は $A_6((B_{48q}, T_{48q}))$ の neighbor になることが分かる. したがって $A_6((B'_{48q}, T_{48q}))$ が求める extremal odd unimodular lattice になる.

後者の (extremal even unimodular lattice の neighbor にならない) lattice の構成について述べる. 条件設定とは裏腹に, extremal even unimodular lattice を用いて存在が示されるところが面白いと思う. 以下では, 48 次元の色々な (binary 以外の) code や lattice が登場するが, 要は, 新しい lattice を作るのに知られている code と lattice の性質を使うということである.

まず, 長さ 48 の ternary extremal self-dual code から始める. これは次の 2 つ

(1) $C_3^{(q)} = QR_{48}$: Quadratic residue code

(2) $C_3^{(p)} = PS_{48}$: Pless symmetry code

が知られている (分類はされていない) . ここで用いた記号は, 本稿独自のものと理解されたい. 簡単のため, この 2 つを $C_3^{(*)}, (* = p, q)$ と表すことにする.

これに対して, Construction A により odd unimodular lattice

$$L^{(*)} = A_3(C_3^{(*)}) := \left\{ \frac{1}{\sqrt{3}}(x_1, \ldots, x_{48}) \mid x_i \in \mathbb{Z}, (x_i \pmod 3) \in C_3^{(*)} \right\}$$

を考える. ここで,

$$w = \frac{1}{2\sqrt{3}}(1, 1, \ldots, 1) \in \frac{1}{2}L^{(*)} \setminus L^{(*)}, L_0^{(*)} = L^{(*)} \cap \langle w \rangle^*$$

とおくと（命題 4.1 のときと同様に）$(w,y) \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$ をみたす $y \in L^{(*)}$ が存在し，$L_0^{(*)}$ を含む 3 つの unimodular lattice は，$L^{(*)}$ と

$$N_1^{(*)} = \langle L_0^{(*)}, w \rangle, \quad N_2^{(*)} = \langle L_0^{(*)}, w+y \rangle$$

の 2 つになる．このとき，次が知られている．

定理 4.6. $N_2^{(*)}$ は extremal even unimodular lattice である:

$$N_2^{(q)} \cong P_{48q}, \quad N_2^{(p)} \cong P_{48p}.$$

ここでは，extremal でない方の $N_1^{(*)}$ について考える．実は，次のことが成り立っている．

補題 4.7. $N_1^{(*)}$ は，ある extremal Type II $\mathbb{Z}_4$-code $C_4^{(*)}$ から Construction A によって得られる．すなわち，

$$N_1^{(*)} = A_4(C_4^{(*)}) := \left\{ \frac{1}{2}(x_1, \ldots, x_{48}) \;\middle|\; x_i \in \mathbb{Z}, (x_i \pmod 4) \in C_4^{(*)} \right\}.$$

この補題は $N_1^{(*)}$ が丁度 48×2 個の norm 4 のベクトル $\pm f_1, \ldots, \pm f_{48}$ を含んでいて，それらが互いに直交する $((f_i, f_j) = 4\delta_{ij})$ という事実による．上記のような $A_4(C_4^{(*)})$ としての記述（成分表示）は，$\frac{1}{2}f_1, \ldots, \frac{1}{2}f_{48}$ を（正規直交）基底にして表示したものである．だから，このときの座標系は，$L^{(*)} = A_3(C_3^{(*)})$ と書いたときの座標系とは異なっていることに注意されたい．

以下，簡単のため $(*)$ を省略して $L' := N_1^{(*)}$ とおく．今，$* = p, q$ をどちらかに固定して考えると，3 つの lattice が得られている．$L^{(*)}$ を出発点に，$N_1^{(*)}$, $N_2^{(*)}$ を作ったのである．今度は，これを $L' = N_1^{(*)}$ を中心に記述し直してみるのである．

まず，w' を $L^{(*)} \setminus N_1^{(*)}$ の元として，norm 3 のベクトルを取り，

$$L_0' = L' \cap \langle w' \rangle^*$$

とおく．すると，任意に $y' \in L' \setminus L_0'$ を取れば，L_0' を含む L' 以外の unimodular lattice は，

$$N_1' := \langle L_0', w' \rangle, \quad N_2' := \langle L_0', w'+y' \rangle$$

として得られ, それぞれ $L^{(*)}$, $N_2^{(*)}$ になる. 実際, w' の取り方から $L^{(*)} = \langle L_0', w' \rangle$ であり, 従って,

$$L_0' = L' \cap N_1' = N_1^{(*)} \cap L^{(*)} = L_0^{(*)}$$

となるから, $L_0^{(*)}$ を含むもう一つの neighbor として $N_2' = N_2^{(*)}$ とならざるを得ない.

ここで, $L^{(*)}$ に含まれている norm 3 のベクトルは, $L' = N_1^{(*)} = A_4(C_4^{(*)})$ の座標系の下では, $w' = \frac{1}{4}(1, 1, \ldots, 1)$ という形で表される以外ないことがわかる. (ただし, $C_4^{(*)}$ の成分を必要に応じて ± 1 倍している.) なぜなら, N_2' の minimum norm が 6 であることから, L' の基底である norm 4 のベクトルは L_0' には含まれないから, w' の norm が 3 であることに注意すると, 上記のような形しかあり得ないのである. このとき, $y' = \frac{1}{4}(-8, 0, \ldots, 0)(\in N_1')$ (これは, 先ほどの記号では $-f_1$ である) と取ることが出来て $w' + y' = \frac{1}{4}(-7, 1, \ldots, 1)(\in N_2')$ である.

以上の準備の下に, 目的の lattice を作る. $L'' := N_1^{(*)}$ (L' と同じ) として, w', y' の取り方を少しだけ変えて新しい lattice を作るのである. まず,

$$w'' = \frac{1}{4}(-3, -3, 1, \ldots, 1) = w' - f_1 - f_2$$

として,

$$L_0'' = L'' \cap \langle w'' \rangle^*$$

とおく. $y'' \in L'' \setminus L_0''$ は, $y'' = \frac{1}{4}(8, 0, \ldots, 0)$, $w'' + y'' = \frac{1}{4}(5, -3, 1, \ldots, 1)$, と取ることができて, L_0'' を含む L'' 以外の unimodular lattice

$$N_1'' := \langle L_0'', w'' \rangle, \quad N_2'' := \langle L_0'', w'' + y'' \rangle$$

となる. このとき, $\min(N_1'') = 4, \min(N_2'') = 5$ が示されるので, N_2'' の even neighbor の minimum norm が共に 4 であることから, N_2'' が目的の lattice となって, 定理の証明が終わる. 実際, $\min(N_1'') = 4$ はほぼ自明である. 問題の $\min(N_2'') = 5$ は $\min(N_2') = 6$ を用いて, 次のように示される.

$\min(N_2'') < 5$ と仮定する. すると, $\min(N_2'') = 3$ となるが, norm 3 のベクトル $v'' \in N_2''$ は,

$$v'' = \frac{1}{4}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{48}), \quad (\forall \varepsilon_i = \pm 1)$$

という形にならざるを得ない. そこで,

$$v' = v'' - \frac{\varepsilon_1}{2} f_1 - \frac{\varepsilon_2}{2} f_2 = \frac{1}{4}(-3\varepsilon_1, -3\varepsilon_2, \ldots, \varepsilon_{48})$$

とおく. このとき $(v', v') = 4$ と

$$v' - (w' + y') = v'' - (w'' + y'') - \frac{\varepsilon_1 - 3}{2} f_1 - \frac{\varepsilon_2 + 1}{2} f_2 \in L'' = L'$$

が容易にわかる. よって, $(v' - (w' + y'), w') \in \mathbb{Z}$ が言えれば, $v' - (w' + y') \in L_0' \subset N_2'$ が言え, $w' + y' \in N_2'$ より $v' \in N_2'$ となって $\min(N_2') = 6$ に矛盾して証明が完了する.

この内積の値は直接成分計算をすれば,

$$(v' - (w' + y'), w') = \frac{1}{16}(-3\varepsilon_1 - 3\varepsilon_2 + \varepsilon_3 + \cdots + \varepsilon_{48} + 40)$$

が得られる. 一方 v'' と $w'' + y''$ が N_2'' に含まれているから,

$$(v'', w'' + y'') = \frac{1}{16}(5\varepsilon_1 - 3\varepsilon_2 + \varepsilon_3 + \cdots + \varepsilon_{48})$$

は整数であり, 従って,

$$(v' - (w' + y'), w') = (v'', w'' + y'') + \frac{1}{2}(\varepsilon_1 + 5) \in \mathbb{Z}$$

が得られる. □

ここで, 以上の過程で得られた副産物について触れておく. 上記の構成では $* = p, q$ に応じて lattice は 2 つ出来る. 実は, この 2 つは非同型である. このことは, 何から示されるかというと, $C_4^{(p)}$ と $C_4^{(q)}$ が非同値であることによる. これは, この 2 つの mod 2 での像がそれぞれ $G_{24} \oplus G_{24}$ と QR_{48} であることから分かる. ところが, 長さ 48 の extremal Type II $\mathbb{Z}_4$-code はひとつしか知られていなかったのである. ということは, 少なくとも一方は新しい code だということになる. 事実は, $C_4^{(q)}$ は extended quadratic residue $\mathbb{Z}_4$-code として知られているもので, $C_4^{(p)}$ が新しい code であった.

既に触れたように, binary extremal doubly-even self-dual $[48, 24, 12]$ code の一意性が, ごく最近になって示された ([7]) わけであるが, ternary code や $\mathbb{Z}_4$-code については分類は未解決問題である. 実際, 長さ 24 でさえ ternary extremal self-dual code の分類が完成している (位数 24 の

Hadamard 行列の分類に帰着出来る）だけで, ternary self-dual code 全体や $\mathbb{Z}_4$-code については分類にはまだ遠い. まだまだ研究する余地はあるようである.

最後に一言付け加えておこう. 2つの extremal even unimodular lattice P_{48p}, P_{48q} の自己同型群は,

$$\begin{aligned} \mathrm{Aut}(P_{48q}) &\cong 2^2 \cdot PSL(2,47). \\ \mathrm{Aut}(P_{48p}) &\cong 2 \cdot PSL(2,23) \times S_3. \end{aligned}$$

となることが知られているが, バイブル [4] を見ると Thompson からの personal commnication によるとある. 散在型単純群発見の時代に調べてみたが残念なことに新しい群にはならなかったという経緯なのだろう. この2つについては, すでに述べたように code との関連もあって, ある程度よくわかっていると言えると思うが, もう一つ知られている P_{48n} については（少なくとも筆者達には）その実体がつかめていない. 今後の研究課題であると思っている.

参考文献

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

[2] 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** (1990), 1319–1333.

[3] J.H. Conway and N.J.A. Sloane, A note on optimal unimodular lattices, *J. Number Theory* **72** (1998), 357–362.

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

[5] M. Harada, M. Kitazume and M. Ozeki, Ternary code construction of unimodular lattices and self-dual codes over $\mathbb{Z}_6$, *J. Alg. Combin.* **16** (2002), 209–223.

[6] M. Harada, M. Kitazume, A. Munemasa and B. Venkov, On some self-dual codes and unimodular lattices in dimension 48, (submitted).

[7] S.K. Houghten, C.W.H. Lam, L.H. Thiel and J.A. Parker, The extended quadratic residue code is the only $(48, 24, 12)$ self-dual doubly-even code, *IEEE Trans. Inform. Theory* **49** (2003), 53–59.

[8] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[9] A. Munemasa, On the enumeration of binary self-dual codes, (preprint).

[10] E. Rains and N.J.A. Sloane, Self-dual codes, in *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 177–294.

Bruhat 順序の MacNeille completion と alternating sign matrix

岡田　聡一 (名古屋大学多元数理科学研究科)
難波　正幸 (名古屋大学多元数理科学研究科)

概 要

本報告では，A 型 Coxeter 群，B 型 Coxeter 群上の Bruhat order の組合せ論的な記述と，それらを部分半順序集合として含む最小の complete lattice (Bruhat order の MacNeille completion) の組合せ論的な記述について述べる．これらの組合せ論的な記述に用いられるのが，alternating sign matrix と呼ばれる行列 (あるいは monotone triangle) である．alternating sign matrix はその定義により，置換行列の拡張となっているが，それが Bruhat order の MacNeille completion として現れる点で興味深い．

1 Introduction

この節では，本報告のキーワードである Coxeter 系，Coxeter 群上の Bruhat order，半順序集合の MacNeille completion について簡単に説明する．(Coxeter 系については [2], [7] を，半順序集合 (lattice) については [1] を参照されたい.)

まず，Coxeter 系とその上の Bruhat order を定義する．

Definition 1.1. 群 W が，S によって生成され，次の (1), (2) を基本関係としてもつとき，(W,S) は **Coxeter 系**であるという．

(1) 任意の $s \in S$ に対して，$s^2 = e$.

(2) 相異なる S の 2 元 $s, s' \in S$ に対して，$m(s,s') \in \{1,2,\cdots\} \cup \{\infty\}$ が存在して，

$$(ss')^{m(s,s')} = e.$$

ただし，$m(s,s')=\infty$ は，積 ss' を何乗しても単位元にならないことを意味する．

Definition 1.2. (W,S) を Coxeter 系とする．W 上の半順序 $\leq$ を，

$$w_1 \leq w_2 \overset{def}{\iff} w_2 \text{ のある reduced expression } w_1 = s_1 \cdots s_r \text{ に対し，} w_1 = s_{i_1} \cdots s_{i_t}\ (1 \leq i_1 < \cdots < i_t \leq r) \text{ と表される}$$

によって定義する．この W 上の半順序を **Bruhat order** と呼ぶ．

次に，半順序集合の MacNeille completion を定義する．

Definition 1.3. $(P,\leq)$ を半順序集合とする．

(a) P が次の 2 条件を満足するとき，**lattice** であるという．

(1) 任意の $x,y \in P$ に対して，$z \in P$ で，$z \leq x$，$z \leq y$ となるもののうち最大のものがただ一つ存在する．

(2) 任意の $x,y \in P$ に対して，$z' \in P$ で，$z' \geq x$，$z' \geq y$ となるもののうち最小のものがただ一つ存在する．

このとき，(1) を満たす最大の z を x と y の meet と呼び，$x \wedge y$ と表す．また，(2) を満たす最小の z' を x と y の join と呼び，$x \vee y$ と表す．

(b) P が次の 2 条件を満足するとき，**complete lattice** であるという．

(1) 任意の $S \subseteq P$ に対して，$z \in P$ で，任意の $x \in S$ に対して $z \leq x$ となるもののうち，最大のものがただ一つ存在する．

(2) 任意の $S \subseteq P$ に対して，$z' \in P$ で，任意の $x \in S$ に対して $z' \geq x$ となるもののうち，最小のものがただ一つ存在する．

このとき，(1) を満たす最大の z を S の meet と呼び，$\wedge S$ と表す．また，(2) を満たす最小の z' を S の join と呼び，$\vee S$ と表す．

一般の半順序集合 $(P,\leq)$ に対して，P を部分半順序集合として含むような最小の complete lattice (MacNeille completion) が次のようにして構成できる．

$(P,\leq)$ を半順序集合とし，最小元 $\hat{0}$ をもつと仮定する．(ただし，最小元が存在しないときは新たに最小元を付け加えればよい．) P の部分集合 X に対して，

$$G(X)=\{y\in P\mid y\geq x\ (\forall x\in X)\},$$
$$L(X)=\{y\in P\mid y\leq x\ (\forall x\in X)\}$$

とおき，$\overline{X}\subseteq P$ を

$$\overline{X}=L(G(X))$$

により定義する．そして，

$$L(P)=\{X\subseteq P\mid \overline{X}=X,\ X\neq\emptyset\}$$

とおき，P の部分集合としての包含関係に関して $L(P)$ を半順序集合とみる．このとき，

Fact 1.4. $(L(P),\subseteq)$ は，complete lattice である．また，その lattice 構造は，

$$X\wedge Y=X\cap Y,\quad X\vee Y=\overline{X\cup Y}$$

により与えられる．

Definition 1.5. この半順序集合 $(L(P),\subseteq)$ を P の **MacNeille completion** という．

$x\in P$ に対して，

$$\overline{\{x\}}=I_x=\{y\in P\mid y\leq x\}$$

であり，この部分集合 I_x は，x によって生成される principal order ideal と呼ばれる．

Fact 1.6. 半順序集合 $(P,\leq)$ は最小元 $\hat{0}$ と最大元 $\hat{1}$ をもつと仮定する．$(P,\leq)$ の MacNeille completion を $(L(P),\subseteq)$ とする．このとき，

(1) 写像 $P\ni x\longmapsto\overline{\{x\}}\in L(P)$ は，単射であり，順序を保つ．この写像によって P を $L(P)$ の部分半順序集合とみなす．

(2) L が complete lattice であるとき，順序を保つ単射写像 $P\hookrightarrow L$ は順序を保つ単射写像 $L(P)\hookrightarrow L$ に拡張される． □

この Fact により，P の MacNeille completion $L(P)$ は

$$L(P)=\{I_{x_1}\wedge I_{x_2}\wedge\cdots\wedge I_{x_r}\mid x_1,x_2,\cdots,x_r\in P,\ r=0,1,2,\cdots\}$$

と書いても良いことが分かる．

2 $\mathfrak{S}_n$ 上の Bruhat order と alternating sign matrix

この節では，対称群 $\mathfrak{S}_n$ 上の Bruhat order の組合せ論的な記述と，その MacNeille completion を考える．ここで，組合せ論的な対象として用いられるのが monotone triangle と alternating sign matrix である．(alternating sign matrix については，[3] を参照されたい．)

2.1 $\mathfrak{S}_n$ の Bruhat order の組合せ論的記述

$W = \mathfrak{S}_n$ を n 次対称群とし，$S = \{s_1, \cdots, s_{n-1}\}$ $(s_i = (i, i+1))$ とおくと，$(\mathfrak{S}_n, S)$ は A_{n-1} 型 Coxeter 系をなす．

$\mathfrak{S}_n$ 上の Bruhat order は，monotone triangle を用いることにより，組合せ論的に記述できることが知られている．

Definition 2.1. (a) 正整数を成分とする n 次の triangle

$$T = (t_{i,j})_{1 \le j \le i \le n} = \begin{array}{ccccccccc} & & & & t_{1,1} & & & & \\ & & & t_{2,1} & & t_{2,2} & & & \\ & & \iddots & & & & \ddots & & \\ & \iddots & & & & & & \ddots & \\ t_{n,1} & & t_{n,2} & & \cdots & & t_{n,n-1} & & t_{n,n} \end{array}$$

が条件

$$t_{i+1,j} \le t_{i,j} \le t_{i+1,j+1}, \qquad t_{i,j} < t_{i,j+1}$$

を満たすとき，n 次の **monotone triangle** であるという．

(b) 最下行が $1, 2, \cdots, n$ である n 次の monotone triangle 全体のなす集合を $\mathcal{M}_n$ と表す：

$$\mathcal{M}_n = \{\text{最下行が } 1, 2, \cdots, n \text{ からなる } n \text{ 次 monotone triangle}\}.$$

(c) 2 つの monotone triangle $T = (t_{i,j})$, $T' = (t'_{i,j})$ に対して，半順序 $\preceq$ を，

$$T \preceq T' \overset{def}{\iff} t_{i,j} \le t'_{i,j} \ (1 \le j \le i \le n)$$

によって定義する．

置換 $w=[w(1),\cdots,w(n)]\in\mathfrak{S}_n$ に対して，n 次の triangle $T_w=(t_{i,j})$ を

$$\{t_{i,1},t_{i,2},\cdots,t_{i,i}\}=\{k\mid w(k)\leq i\ (1\leq k\leq n)\}$$

となるように定める．このとき，$T_w\in\mathcal{M}_n$ である．この monotone triangle を用いることによって，$\mathfrak{S}_n$ 上の Bruhat order は次のように組合せ論的に記述される：

Theorem 2.2. (Ehresmann [5], Proctor [10], etc...) $w_1,w_2\in\mathfrak{S}_n$ に対して，$T_{w_1},T_{w_2}\in\mathcal{M}_n$ をそれぞれに対応する n 次 monotone triangle とする．このとき，

$$w_1\leq w_2\iff T_{w_1}\preceq T_{w_2}$$

が成立する． □

例えば，$\mathfrak{S}_4$ において，

$$w_1=[2,3,1,4],\quad w_2=[3,2,1,4],\quad w_3=[2,1,4,3]$$

を考える．このとき，対応する monotone triangle は，

$$T_{w_1}=\begin{array}{ccccccc}&&&3&&&\\&&1&&3&&\\&1&&2&&3&\\1&&2&&3&&4\end{array},\quad T_{w_2}=\begin{array}{ccccccc}&&&3&&&\\&&2&&3&&\\&1&&2&&3&\\1&&2&&3&&4\end{array},\quad T_{w_3}=\begin{array}{ccccccc}&&&2&&&\\&&1&&1&&\\&1&&2&&4&\\1&&2&&3&&4\end{array}$$

である．よって，Theorem 2.2 を用いると，

$$T_{w_1}\prec T_{w_2}\text{ より }w_1<w_2,\qquad T_{w_2}\not\preceq T_{w_3}\text{ より }w_2\not\leq w_3$$

となることが分かる．

また，$\mathfrak{S}_4$ 上の Bruhat order の Hasse 図は図 1 のようになる．

2.2 $\mathfrak{S}_n$ の MacNeille completion

最下行が $1,2,\cdots,n$ である monotone triangle 全体 $\mathcal{M}_n$ は，Definition 2.1 で与えた半順序に関して complete lattice をなし，その lattice 構造は，

$$T\wedge T'=(\min(t_{i,j},t'_{i,j})),\quad T\vee T'=(\max(t_{i,j},t'_{i,j}))$$

により与えられる．ここで，$T=(t_{i,j}),T'=(t'_{i,j})$ である．よって，Theorem 2.2 により，$\mathcal{M}_n$ は，Bruhat order に関する半順序集合 $\mathfrak{S}_n$ を部分半

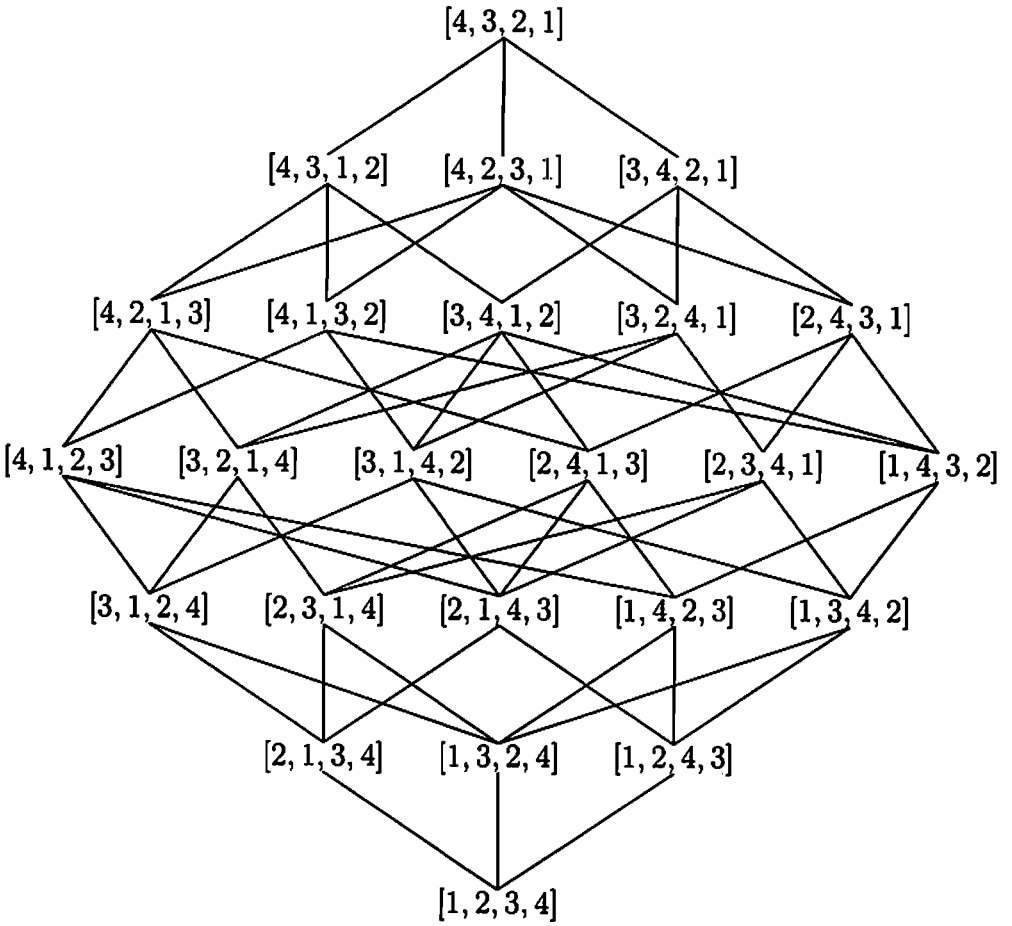


図 1: $\mathfrak{S}_4$ 上の Bruhat order

順序集合として含む complete lattice であることが分かる．従って，Fact 1.6 より，順序を保つ単射 $L(\mathfrak{S}_n) \hookrightarrow \mathcal{M}_n$ が存在する．実はこの単射が，半順序集合としての同型写像となっている．

Theorem 2.3. (Lascoux–Schützenberger [8]) 半順序集合として，

$$L(\mathfrak{S}_n) \cong \mathcal{M}_n$$

である．ここで，$L(\mathfrak{S}_n)$ は，Bruhat order に関する半順序集合 $\mathfrak{S}_n$ の MacNeille completion である． □

2.3 Alternating sign matrix

最下行が $1, 2, \cdots, n$ である monotone triangle は，置換行列の拡張である alternating sign matrix と 1 対 1 に対応している．

Definition 2.4. (a) n 次正方行列 $A = (a_{i,j})_{1 \le i,j \le n}$ は，次の 3 条件を満たすとき，**alternating sign matrix** (以下 ASM と略す) であるという：

(1) $a_{i,j} \in \{0, 1, -1\}$.

(2) A の各列，各行の成分の和は 1 である．

(3) A の各行，各列の 0 でない成分は，1 で始まり，1 と -1 が交互に現れる．

(b) n 次 ASM 全体のなす集合を $\mathcal{A}_n$ と表す：

$$\mathcal{A}_n = \{n \text{ 次 ASM 全体}\}.$$

Example 2.5. (1) $w \in \mathfrak{S}_n$ に対応する置換行列 $P_w = (\delta_{i,w(j)})_{1 \le i,j \le n}$ は，n 次 ASM である．ここで，$\delta_{i,j}$ はクロネッカーのデルタである．(以下，n 次置換行列全体のなす集合も $\mathfrak{S}_n$ で表すことにする．)

(2) $\mathcal{A}_3 = \mathfrak{S}_3 \cup \left\{ \begin{pmatrix} 0 & 1 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \right\}$ である．

(3) n 次置換行列は，-1 を成分に持たない n 次 ASM として特徴付けられる．

Remark 2.6. n 次 ASM の個数 $\sharp\mathcal{A}_n$ は,

$$\sharp\mathcal{A}_n = \prod_{k=0}^{n-1} \frac{(3k+1)!}{(n+k)!}$$

で与えられる. □

n 次 ASM は，最下行が $1, 2, \cdots, n$ である n 次 monotone triangle と次のように 1 対 1 に対応している．$A = (a_{i,j})_{1 \le i,j \le n} \in \mathcal{A}_n$ を n 次 ASM とする.

(1) まず，n 次正方行列 $\overline{A} = (\overline{a}_{i,j})_{1 \le i,j \le n}$ を,

$$\overline{a}_{i,j} = \sum_{p=1}^{i} a_{p,j} \quad (1 \le i, j \le n)$$

によって定義する．このとき，ASM の定義により，$\overline{a}_{i,j} \in \{0, 1\}$ となっている.

(2) 次に，この $\overline{A}$ を用いて，monotone triangle $T_A = (t_{i,j})_{1 \le j \le i \le n}$ を,

$$\{t_{i,1}, t_{i,2}, \cdots, t_{i,i}\} = \{k \mid \overline{a}_{i,k} = 1\}$$

となるように定める．すると，$T_A \in \mathcal{M}_n$ となることが容易に確認できる.

この作り方は逆にたどることができるので，次の命題が成立する.

Proposition 2.7. 対応 $\mathcal{A}_n \ni A \longmapsto T_A \in \mathcal{M}_n$ は全単射である.

Example 2.8. 例えば,

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

に対して,

$$\overline{A} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$$

であるから，

$$T_A = \begin{array}{ccccccc} & & & 3 & & & \\ & & 1 & & 3 & & \\ & 1 & & 2 & & 4 & \\ 1 & & 2 & & 3 & & 4 \end{array}$$

となる．

Remark 2.9. (a) $A \in \mathcal{A}_n$ とし，対応する monotone triangle を $T_A = (t_{i,j})$ とする．このとき，

$$A \in \mathfrak{S}_n \iff A \text{は} -1 \text{を成分に持たない．}$$
$$\iff t_{i+1,j} \leq t_{i,j} \leq t_{i+1,j+1} \text{となる} i, j \text{は存在しない}$$

(b) 置換行列 $P_w \in \mathfrak{S}_n$ に対して，$T_{P_w} = T_w$ である．ここで，T_w は，Theorem 2.2 の前に述べた $w \in \mathfrak{S}_n$ に対応する monotone triangle である．

2.4 $\mathcal{M}_n$ の lattice 構造 — join-irreducible な元 —

この小節では，complete lattice $\mathcal{M}_n$ のより詳しい lattice 構造を見ることにする．

Definition 2.10. $(P, \leq)$ を半順序集合とする．

(a) $x, y \in P$ とする．$y \lneq x$ であり，$y \leq z \leq x$ となる元 $z \in P$ が存在しないとき，x は y を **cover する**という．

(b) $x \in P$ に対して，x が cover する元全体のなす集合を $C(x)$ と表す：

$$C(x) = \{y \in P \mid x \text{は} y \text{を cover する}\}$$

(c) P が lattice であるとし，$x \in P$ とする．$\sharp C(x) = 1$，すなわち，x が cover する元が 1 つだけ存在するとき，x は **join-irreducible** であるという．

(d) P が lattice であるとき，

$$j(P) = \{P \text{の join-irreducible な元}\}$$

とおく．

(e) P が lattice であり，さらに，任意の $x, y, z \in P$ に対して

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z), \quad x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

が成り立つとき，P は **distributive lattice** であるという．

一般に，(finite) distributive lattice L の構造はその join-irreducible な元全体のなす部分半順序集合 $j(L)$ の構造から一意的に定まる．$\mathcal{M}_n$ は distributive lattice であり，$j(\mathcal{M}_n)$ の構造は次の定理で与えられる．

Theorem 2.11. $0 \leq r < s < t \leq n$ に対して，

$$w_{r,s,t} = [1, 2, \cdots, r, (s+1), (s+2), \cdots, t, (r+1), (r+2), \cdots, s, (t+1), \cdots, n]$$

とおき，対応する monotone triangle を $T_{r,s,t} = T_{w_{r,s,t}}$ とする．このとき，$j(\mathcal{M}_n)$ について，

(1)
$$j(\mathcal{M}_n) = \{T_{r,s,t} \mid 0 \leq r < s < t \leq n\}$$
である．特に，その個数 $\sharp j(\mathcal{M}_n)$ は，
$$\sharp j(\mathcal{M}_n) = \frac{n(n+1)(n-1)}{3}$$
により与えられる．

(2) $T_{r,s,t}, T_{r',s',t'} \in j(\mathcal{M}_n)$ に対して，
$$T_{r,s,t} \preceq T_{r',s',t'} \Longleftrightarrow r \geq r',\ t \leq t',\ s - r \leq s' - r',\ t - s \leq t' - s'.$$

(3) $j(\mathcal{M}_n)$ は，
$$j(\mathcal{M}_n) = P_1 \cup \cdots \cup P_{n-1}, \quad P_k = \{T_{r,s,t} \mid t - r = k - 1\}$$
なる graded poset の構造をもち，
$$\sharp P_k = k(n-k) \quad (1 \leq k \leq n-1)$$
となっている． □

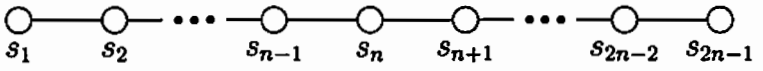
Remark 2.12. この Theorem の $j(\mathcal{M}_n)$ は，Geck-Kim [6] の与えた $\mathfrak{S}_n$ の base に一致している．

3 B_n 型 Coxeter 群と Half-turn symmetric ASM

この節では，B_n 型 Coxeter 群を $2n$ 次対称群 $\mathfrak{S}_{2n}$ の部分群として実現することによって，その上の Bruhat 順序の組合せ論的な記述と MacNeille completion について考える．このときに現れる組合せ論対象が half-turn symmetric ASM (180° 回転によって不変な ASM) である．

3.1 B_n 型 Coxeter 群とその上の Bruhat order

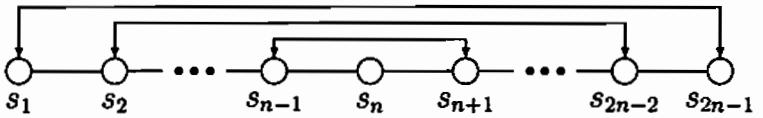
A_{2n-1} 型 Coxeter 系 $(\mathfrak{S}_{2n}, S)$ は，次の Coxeter 図形を持つ：



この Coxeter 図形の自己同型 $\sigma : S \to S$ を，

$$\sigma(s_i) = s_{2n-i} \quad (1 \leq i \leq 2n-1)$$

によって定義する．すなわち，σ は，上の Coxeter 図形において



となるものである．このとき，この S 上の全単射 σ は，

$$\sigma(s^{(1)}s^{(2)}\cdots s^{(r)}) = \sigma(s^{(1)})\sigma(s^{(2)})\cdots\sigma(s^{(r)}) \quad (s^{(i)} \in S)$$

によって，$\mathfrak{S}_{2n}$ 上の自己同型写像 (同じシンボル σ を用いて表すことにする) に拡張される．そして，$\mathfrak{S}_{2n}$ の自己同型写像 σ により固定される元の全体のなす $\mathfrak{S}_{2n}$ の部分群を $W(B_n)$ とする：

$$W(B_n) = \{w \in \mathfrak{S}_{2n} \mid \sigma(w) = w\}.$$

すると，

$$W(B_n) = \{w \in \mathfrak{S}_{2n} \mid w(i) + w(2n+1-i) = 2n+1 \ (1 \leq i \leq n)\}$$

とも表される．このとき，Coxeter 系の一般論から，次の定理が得られる．

Theorem 3.1. (1) (R. Steinberg [11]) $W(B_n)$ は B_n 型 Coxeter 群である.

(2) (M. Nanba [9]) $W(B_n)$ 上の Bruhat order は, $\mathfrak{S}_{2n}$ 上の Bruhat order の $W(B_n)$ への制限に一致する. すなわち, $\leq$ を $\mathfrak{S}_{2n}$ 上の Bruhat order とし, $\leq_B$ を $W(B_n)$ 上の Bruhat order とするとき, $w_1, w_2 \in W(B_n)$ に対して,

$$w_1 \leq_B w_2 \iff w_1 \leq w_2$$

である. □

この定理により, B_n 型 Coxeter 群は $\mathfrak{S}_{2n}$ の部分群 $W(B_n)$ として実現され, その Bruhat order は埋め込み $W(B_n) \hookrightarrow \mathfrak{S}_{2n}$ により得られることがわかる. 従って, $\mathfrak{S}_{2n}$ 上の Bruhat order の組合せ論的な記述 (Theorem 2.2) を用いることにより, B_n 型 Coxeter 群上の Bruhat order の組合せ論的な記述が得られる. (Theorem 3.7 を見よ.)

3.2 Half-turn symmetric ASM

この小節では, 前小節で述べた A_{2n-1} 型 Coxeter 系の Coxeter 図形の自己同型 σ に相当する $\mathcal{A}_{2n}$ 上の全単射を考え, その固定点 (half-turn symmetric ASM) と対応する monotone triangle を考える.

ASM $A \in \mathcal{A}_N$ に, A を 180° 回転させたできる ASM $\sigma(A)$ を対応させることによって, 全単射 $\sigma : \mathcal{A}_N \to \mathcal{A}_N$ を定義する. すなわち,

$$A = \begin{pmatrix} a_{11} & a_{22} & \cdots & a_{1N} \\ a_{21} & a_{22} & \cdots & a_{2N} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \cdots & a_{NN} \end{pmatrix}$$

に対して,

$$\sigma(A) = \begin{pmatrix} a_{NN} & a_{NN-1} & \cdots & a_{N1} \\ a_{N-1N} & a_{N-1N-1} & \cdots & a_{N-11} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1N} & a_{1N-1} & \cdots & a_{11} \end{pmatrix}$$

である.

Definition 3.2. N 次 ASM A は，$\sigma(A) = A$ を満たすとき，half-turn symmetric ASM (以下 HTSASM と略す) であるという．N 次 HTSASM 全体のなす集合を $\mathcal{HA}_N$ と表す：

$$\mathcal{HA}_N = \{N \text{ 次 HTSASM}\}.$$

例えば，$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ は，HTSASM である．また，$2n$ 次の置換 $w \in \mathfrak{S}_{2n}$ に対して，それに対応する置換行列を $P_w = (\delta_{i,w(j)})$ とする．このとき，

$$\begin{aligned} P_w \text{ が HTSASM} &\iff w(i) + w(2n+1-i) = 2n+1 \ (1 \le i \le 2n) \\ &\iff w \in W(B_n) \end{aligned}$$

また，HTSASM の定義により，次のことが容易にわかる．

Proposition 3.3. $A \in \mathcal{A}_{2n}$ が HTSASM であるための必要十分条件は，

$$\overline{a}_{ni} = 1 \iff \overline{a}_{n2n+1-i} = 0 \ (1 \le \forall i \le 2n)$$

が成り立つことである．ここで，$\overline{a}_{ni} = \sum_{p=1}^{n} a_{pi}$ である．

Definition 3.4. (a) n 次の monotone triangle $T = (t_{ij})_{1 \le j \le i \le n}$ は，次の 2 条件を満足するとき，**B_n 型 monotone triangle** であるという：

(1) $t_{ij} \in \{1, 2, \cdots, 2n\}$.

(2) $k \in \{t_{n1}, \cdots, t_{nn}\} \iff 2n+1-k \notin \{t_{n1}, \cdots, t_{nn}\}$.

(b) B_n 型 monotone triangle 全体のなす集合を $\mathcal{M}_n^B$ と表す：

$$\mathcal{M}_n^B = \{B_n \text{ 型 monotone triangle 全体}\}.$$

(c) $2n$ 次 monotone triangle $T \in \mathcal{M}_{2n}$ に対して，T の上から n 行のなす n 次 monotone triangle を $T^{(n)}$ と表す．

$2n$ 次 HTSASM A に対して，Proposition 3.3 から，$T_A^{(n)} \in \mathcal{M}_n^B$ となる．逆に，$T \in \mathcal{M}_n^B$ が与えられたとき，monotone triangle から ASM を復元する操作と同様にして，$0, 1, -1$ を成分とする $n \times 2n$ 行列 $\widetilde{A}$ が得られる．そして，この $\widetilde{A}$ を 180° 回転させ，$\widetilde{A}$ の $n+1$ 行目以下に加えることにより，$2n$ 次の HTSASM A が得られる．よって，次の命題が得られる．

Proposition 3.5. 対応 $\mathcal{HA}_{2n} \ni A \longmapsto T_A^{(n)} \in \mathcal{M}_n^B$ は全単射である． □

Example 3.6. Proposition 2.7 により，

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 0 & 1 & -1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \longleftrightarrow \quad T_A = \begin{array}{ccccccc} & & & 2 & & & \\ & & 1 & & 3 & & \\ & 1 & & 2 & & 3 & \\ 1 & & 2 & & 3 & & 4 \end{array}$$

であるから，

$$T_A^{(2)} = \begin{array}{ccc} & 2 & \\ 1 & & 3 \end{array}$$

である．

逆に，上の $T_A^{(2)}$ が与えられたとき，$0, 1$ を成分とする行列から monotone triangle を作る操作を逆に行うことによって，$0, 1$ を成分に持つ行列

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

が得られる．よって，Proposition 3.3 の条件を満足する行列

$$\widetilde{A} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \end{pmatrix}$$

が得られる．この行列を 180° 回転させ，$\widetilde{A}$ の 3 行目以下に加えることにより得られる行列は，上の HTSASM A である．

Theorem 3.1 (2) により，$W(B_n)$ 上の Bruhat order は $\mathfrak{S}_{2n}$ 上の Bruhat order の $W(B_n)$ への制限である．したがって，Proposition 2.7，Proposition 3.5，Thoerem 2.2 により次の定理を得る．

Theorem 3.7. $W(B_n)$ 上の Bruhat order を $\leq_B$ と表す．このとき，w_1, $w_2 \in W(B_n)$ に対して，

$$\begin{aligned} w_1 \leq_B w_2 &\iff T_{w_1} \preceq T_{w_2} \quad \text{in} \quad \mathcal{M}_{2n} \\ &\iff T_{w_1}^{(n)} \preceq T_{w_2}^{(n)} \quad \text{in} \quad \mathcal{M}_n^B \end{aligned}$$

が成り立つ． □

この定理により，$\mathcal{M}_n^B$ は，Bruhat order に関する B_n 型 Coxeer 群 $W(B_n)$ を部分半順序集合として含むことがわかる．そこで，半順序集合 $\mathcal{M}_n^B$ の半順序構造について考えることにする．

全単射 $\mathcal{A}_{2n} \ni A \mapsto T_A \in \mathcal{M}_{2n}$ を通して，行列を 180° 回転させる全単射 $\sigma : \mathcal{A}_{2n} \to \mathcal{A}_{2n}$ から，

$$\sigma(T_A) = T_{\sigma(A)} \quad (A \in \mathcal{A}_{2n})$$

となる全単射 $\sigma : \mathcal{M}_{2n} \to \mathcal{M}_{2n}$ が定まる．また，この σ による固定点全体のなす部分半順序集合を $\mathcal{M}_{2n}^{\sigma}$ とおく：

$$\mathcal{M}_{2n}^{\sigma} = \{T \in \mathcal{M}_{2n} \mid \sigma(T) = T\}.$$

このとき，$T \in \mathcal{M}_{2n}$ と $A \in \mathcal{A}_{2n}$ が対応している (つまり，$T = T_A$) とすると，

$$T \in \mathcal{M}_{2n}^{\sigma} \iff T^{(n)} \in \mathcal{M}_n^B \iff A \in \mathcal{HA}_n$$

であり，対応 $\mathcal{M}_{2n}^{\sigma} \ni T \mapsto T^{(n)} \in \mathcal{M}_n^B$ は半順序集合としての同型写像である．さらに，lattice の一般論により，$\mathcal{M}_{2n}^{\sigma}$ は complete lattice をなすから，上の同型により，$\mathcal{M}_n^B$ も complete lattice をなすことが分かる．

以上のことから，次の疑問が出てくる：

「$\mathcal{M}_n^B$ は，$W(B_n)$ の MacNeille completion であるか？」

この問に対する答えは，

(1) $n = 2$ のとき，$\mathcal{M}_2^B$ は $W(B_2)$ の MacNeille completion である．

(2) しかし，$n \geq 3$ のときは，$\mathcal{M}_n^B$ は $W(B_n)$ の MacNeille completion より大きい．

Example 3.8. (1) $n = 2$ のとき，$W(B_2)$ の Bruhat order に関する Hasse 図，$W(B_2)$ の MacNeille completion の Hasse 図はそれぞれ図 2，図 3 のようになる．

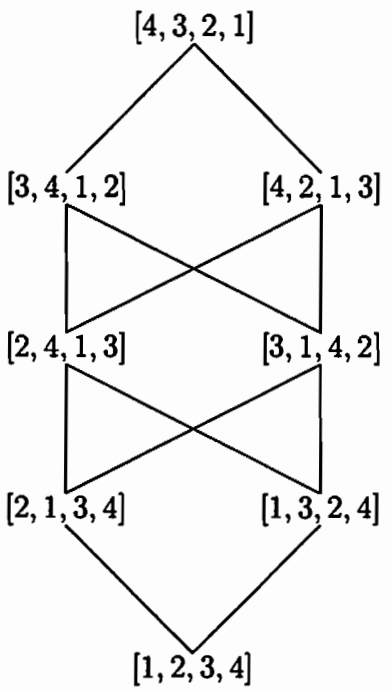


図 2: $W(B_2)$ の Bruhat order の Hasse 図

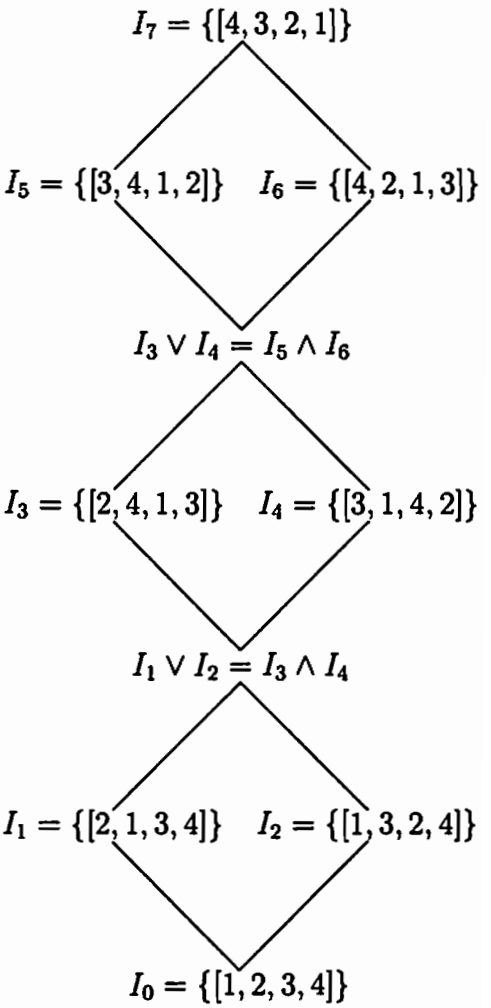


図 3: $W(B_2)$ の Mac Neille completion の Hasse 図

(2) $n=3$ のとき，次の 8 つの B_3 型 monotone triangle は $W(B_3)$ の MacNeille completion に属さない．

$$\begin{array}{ccccccc} & & 3 & & & & \\ & 3 & & 4 & & & \\ 1 & & 3 & & 5 & & \end{array} \qquad \begin{array}{ccccccc} & & 4 & & & & \\ & 3 & & 4 & & & \\ 1 & & 3 & & 5 & & \end{array} \qquad \begin{array}{ccccccc} & & 4 & & & & \\ & 3 & & 4 & & & \\ 2 & & 4 & & 6 & & \end{array} \qquad \begin{array}{ccccccc} & & 4 & & & & \\ & 3 & & 4 & & & \\ 2 & & 4 & & 6 & & \end{array}$$

$$\begin{array}{ccccccc} & & 3 & & & & \\ & 3 & & 4 & & & \\ 1 & & 4 & & 5 & & \end{array} \qquad \begin{array}{ccccccc} & & 3 & & & & \\ & 3 & & 4 & & & \\ 2 & & 3 & & 6 & & \end{array} \qquad \begin{array}{ccccccc} & & 3 & & & & \\ & 3 & & 4 & & & \\ 2 & & 4 & & 6 & & \end{array} \qquad \begin{array}{ccccccc} & & 4 & & & & \\ & 3 & & 4 & & & \\ 1 & & 4 & & 5 & & \end{array}$$

$n \geq 3$ のとき，$\mathcal{M}_n^B$ は $W(B_n)$ の MacNeille completion より大きいが，Fact 1.6 により，$\mathcal{M}_n^B$ の部分半順序集合として $W(B_n)$ の MacNeille completion を実現することができる．これからの問題として，$W(B_n)$ の MacNeille completion を $\mathcal{M}_n^B$ の部分半順序集合として組合せ論的に記述すること，あるいは，$\mathcal{M}_n^B$ の構造を Bruhat order を用いて記述すること，などが残されている．

3.3 $\mathcal{M}_n^B$ の lattice 構造 — Join-irreducible な元 —

この小節では，$\mathcal{M}_n$ のときと同様，complete lattice $\mathcal{M}_n^B$ の join irreducible な元全体のなす半順序集合 $j(\mathcal{M}_n^B)$ について考える．

そのために，次の一般論を用いる．

Lemma 3.9. L を distributive lattice とし，$\sigma : L \to L$ を L の lattice としての自己同型とする．このとき，

(1) σ による固定点全体のなす L の部分半順序集合 L^σ も distributive lattice である．

(2) L の join-irreducible な元全体のなす集合を $j(L)$ とするとき，L^σ の join-irreducible な元全体は，

$$j(L^\sigma) = \{\vee X \mid X \text{ は } j(L) \text{ における } \langle\sigma\rangle \text{ 軌道}\}$$

で与えられる．

この一般論を $\mathcal{M}_{2n}$ とその上の自己同型 σ に対して適用し，半順序集合の同型 $\mathcal{M}_{2n}^\sigma \cong \mathcal{M}_n^B$ を用いることによって，$j(\mathcal{M}_n^B)$ の構造がわかる．$j(\mathcal{M}_{2n})$ 上の σ の作用が

$$\sigma(T_{r,s,t}) = T_{2n-t,2n-s,2n-r} \quad (0 \leq r < s < t \leq 2n)$$

で与えられることに注意すると，次の定理が得られる．

Theorem 3.10. $j(\mathcal{M}_n^B)$ について，

(1) $j(\mathcal{M}_n^B)$ は

$$j(\mathcal{M}_n^B) = \{(T_{r,s,t} \vee T_{2n-t,2n-s,2n-r})^{(n)} \mid 0 \leq r < s < t \leq 2n\}$$

で与えられる．特に，その個数 $\sharp j(\mathcal{M}_n^B)$ は，

$$\sharp j(\mathcal{M}_n^\sigma) = \frac{n(2n^2+1)}{3}$$

となる．

(2) $j(\mathcal{M}_n^B)$ は

$$j(\mathcal{M}_n^B) = P_1 \cup \cdots \cup P_{2n-1}$$

と分解される graded poset であり，

$$\sharp P_k = \begin{cases} \dfrac{k(2n-k)}{2} & (k : \text{even}) \\ \dfrac{k(2n-k)+1}{2} & (k : \text{odd}) \end{cases}$$

で与えられる． □

Remark 3.11. (1) $j(\mathcal{M}_n^B)$ に含まれる元の個数は，Geck-Kim [6] が求めた Bruhat order に関する半順序集合 $W(B_n)$ の base の個数と一致している．

(2) $\mathcal{M}_n$ の場合とは異なり，$j(\mathcal{M}_n^B)$ の元がすべて $W(B_n)$ の元と対応しているわけではない．実際，$n = 3$ のとき，

$$T = \begin{array}{ccccc} & & 3 & & \\ & 3 & & 4 & \\ 1 & & 3 & & 5 \end{array} \in j(\mathcal{M}_3^B)$$

は $W(B_3)$ の元とは対応しないが，

$$S = \begin{array}{ccccccc} & & & 3 & & & \\ & & 3 & & 4 & & \\ & 1 & & 3 & & 4 & \\ 1 & & 2 & & 3 & & 4 \\ & 1 & & 2 & & 3 & & 4 & & 5 \\ 1 & & 2 & & 3 & & 4 & & 5 & & 6 \end{array}, \qquad \sigma(S) = \begin{array}{ccccccc} & & & 1 & & & \\ & & 1 & & 2 & & \\ & 1 & & 2 & & 5 & \\ 1 & & 2 & & 5 & & 6 \\ & 1 & & 2 & & 3 & & 5 & & 6 \\ 1 & & 2 & & 3 & & 4 & & 5 & & 6 \end{array}$$

の 2 つの monotone triangle の join の上から 3 行を取り出したものである．

参考文献

[1] G. Birkhoff, "Lattice theory", A. M. S. Colloq. Pub., Vol.25, A. M. S., Providence, RI, 1967.

[2] N. Bourbaki, "Groupes et algèbres de Lie, Chapitres 4, 5 et 6", Hermann, Paris, 1968.

[3] D. M. Bressoud, "Proofs and Confirmations : The Story of the Alternating Sign Matrix Conjecture", Cambridge University Press, 1999.

[4] V. V. Deodhar, Some characterization of Bruhat ordering on a Coxeter group and determination of the relative Möbius Function, Invent. Math. **39** (1977), 187–198.

[5] C. Ehresmann, Sur la topologie de certains espaces homogènes, Ann. Math. **35** (1934), 396–443.

[6] M. Geck and S. Kim, Bases for the Bruhat–Chevalley order on all finite Coxeter groups, Journal of Algebra **197** (1997), 278–310.

[7] J. E. Humphreys, "Reflection Groups and Coxeter Groups", Cambridge University Press, 1990.

[8] A. Lascoux and M.-P. Schützenberger, Treillis et bases des groupes de Coxeter, Electronic Journal of Combinatorics **3** no.2 (1996), ♯R27.

[9] M. Nanba, Bruhat order on the fixed-point subgroup by a Coxeter graph automorphism, preprint.

[10] R. A. Proctor, Classical Bruhat orders and lexicographic shellability, Journal of Algebra **77** (1982), 104–126.

[11] R. Steinberg, "Endmorphisms of Linear Algebraic Groups", Memoirs of American Mathmatical Society No.80, 1968.

頂点作用素代数 V_L^+ の有理性について

安部利之
東京大学大学院数理科学研究科
(日本学術振興会特別研究員 PD)
abe@ms.u-tokyo.ac.jp

1 序

正定値非退化双線形偶形式を持つ格子 L に付随して，頂点作用素代数 V_L が構成される．その頂点作用素代数は L の -1-等長変換から誘導される位数 2 の自己同型写像を持ち，その写像による固定点全体 V_L^+ は再び頂点作用素代数の構造を持つ．本報告集では，格子 L の階数が 1 のときに，頂点作用素代数 V_L^+ の下に有界な $\mathbb{Z}$ の次数付けを持つ V-加群は完全可約となること，すなわち有理的であること，を証明したので，そのことについて報告する．また格子 L の階数が 1 である時，V_L や V_L^+ は中心電荷 1 の頂点作用素代数であり，有理性と C_2 有限性と呼ばれる性質をあわせもつ．有理性と C_2 有限性を満たす頂点作用素代数は指標がモジュラー不変性を持つことなど有理的共形場理論と対応していると考えられている．そこで V_L の有限自己同型群の固定点として得られる頂点作用素代数と物理の分野で知られている $c=1$ 有理的共形場理論との関係についても説明する．

2 準備

ここでは頂点作用素代数の表現論におけるいくつかの概念の定義を述べる．まず，頂点作用素代数の定義を述べる．定義より得られる結果などは例えば [K] または [MN] を参照．

頂点作用素代数 V とは，可算無限個の二項演算

$$V \times V \to V, \quad (a,b) \to a(n)b \quad (n \in \mathbb{Z}),$$

を備えた $\mathbb{C}$ 上の $\mathbb{Z}$-graded ベクトル空間 $V = \bigoplus_{n\in\mathbb{Z}} V(n)$ で，**真空ベクトル** $1 \in V_0$ と **Virasoro 元** $\omega \in V_2$ を持ち次の公理を満たすものである:

(1) 任意の $a,b \in V$ に対し，n が十分大きな整数ならば $a(n)b = 0$.

(2) (Borchards 恒等式) 任意の $a,b,c \in V$ および $p,q,r \in \mathbb{Z}$ に対し

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

(3) 任意の $a \in V$ に対し，$1(n)a = \delta_{n,-1}a\,(n \in \mathbb{Z})$, $a(-1)1 = a$ および $a(n)1 = 0\,(n \geq 0)$ が成立する．

(4) $L(n) := \omega(n+1)$ と定義するとある複素数 $c_V \in V$ が存在して中心電荷 c_V の Virasoro 代数の交換関係が成り立つ:

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

(5) 任意の $n \in \mathbb{Z}$ に対し，各 $V(n)$ は $L(0)$ に関する固有値 n の有限次元固有空間であり，十分小さな整数 n に対し $V(n) = 0$ である．

(6) 任意の $a \in V$, $n \in \mathbb{Z}$ に対し，$(L(-1)a)(n) = -na(n-1)$ が成立する．

頂点作用素代数の**自己同型写像** g とは，V 上の線形同型写像であって，任意の $a \in V$ と $n \in \mathbb{Z}$ に対し $g \circ a(n) \circ g^{-1} = (g(a))(n)$ および，$g(\omega) = \omega$ を満たすものである．この時，$g(1) = 1$ が成り立つ．自己同型写像全体のなす群を $\mathrm{Aut}(V)$ で表すと，任意の $\mathrm{Aut}(V)$ の有限部分群 G に対し，その固定点のなす V の部分空間 V^G は自然に頂点作用素代数の構造を持つ．このようにして得られた頂点作用素代数はオービフォールド模型と呼ばれている．

次に C_2-有限性の定義について述べる．今 $C_2(V) = \mathrm{span}\{a(-1)b \,|\, a, b \in V\}$ とおく．この時，頂点作用素代数 V が **C_2-有限**もしくは**C_2-有限性を満たす**とは，商空間 $V/C_2(V)$ が有限次元となることである．この性質は頂点作用素代数の表現論において多くの現象を証明するのに必要とされる性質で，表現論を展開する上で非常に有用な概念である．しかし具体的な例に対し，その証明を実行するのは一般に困難である．

次に加群の定義をする．頂点作用素代数には次数付けや有限性の条件によりいくつかの加群の概念が使い分けられている．まず次数付けのない一番 “弱い” 加群の定義を述べる．

頂点作用素代数 V に対し，**弱 V-加群**とは，可算無限個の線形写像

$$V \times M \to M, \quad (a, u) = a(n)u \quad (n \in \mathbb{Z}),$$

を持つベクトル空間 M で，次を満たすものである:

(1) 任意の $a \in V$, $u \in V$ に対し，n が十分大きな整数ならば $a(n)u = 0$.

(2) 任意の $a, b \in V$, $u \in M$ および $p, q, r \in \mathbb{Z}$ に対し

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

(3) 任意の $u \in M$, $n \in \mathbb{Z}$ に対し，$\mathbf{1}(n)u = \delta_{n,-1}u$ が成立する．

頂点作用素代数 V の元 a に対し，その弱加群への可算無限個の作用 $a(n)$ を母関数の形で一度にあらわした作用素 $\sum_{n\in\mathbb{Z}} a(n)z^{-n-1}$ を a に付随する頂点作用素といい $Y(a,z)$ と表す．

弱 V-加群 M が整数の次数付け $M = \bigoplus_{n\in\mathbb{Z}} M(n)$ を持ち，任意の $a \in V(k)\,(k \in \mathbb{Z})$ および $m,n \in \mathbb{Z}$ に対し $a(m)M(n) \subset M(m+n-k-1)$ が成立し，さらに十分小さな n に対し $M(n) = 0$ となるとき，M は **$\mathbb{Z}$-graded 弱 V-加群**であるという．

定義 2.1. 頂点作用素代数 V が**有理的**であるとは，任意の $\mathbb{Z}$-graded 弱 V-加群が完全可約となることをいう．

弱 V-加群 M の $\mathbb{Z}$-graded 弱 V-部分加群の構成法のひとつとして $L(0) = \omega(1)$ の固有空間をとる方法がある．任意の $r \in \mathbb{C}$ に対し $M(r)$ を $L(0)$ に関する固有値 r の固有空間とする．この時，$a \in V(k)$ に対し $[L(0), a(m)] = (m+k-1)a(m)$ が任意の $m \in \mathbb{Z}$ について成立するので $\bigoplus_{n\in\mathbb{Z}} M(r+n)$ は M の弱 V-部分加群となる．もし $M(r+n)$ が十分小さな n に対し成り立てば，これが $\mathbb{Z}$-graded 弱加群を与える．特に $M = \bigoplus_{r\in\mathbb{C}/\mathbb{Z}} \bigoplus_{n\in\mathbb{Z}} M(r+n)$ が成り立ち，各弱部分加群 $\bigoplus_{n\in\mathbb{Z}} M(r+n)$ の次数付けが下に有界で，更に各固有空間が有限次元であるときこの $\mathbb{Z}$-graded 弱 V-加群 M を **V-加群**という．定義より頂点作用素代数は随伴表現に関し V-加群となることがわかる．

頂点作用素代数 V が有理的または C_2-有限である時，既約 $\mathbb{Z}$-graded 弱 V-加群は常に V-加群となり，同型を除き有限個しか存在しないことが知られている ([Z], [DLM1])．

最後に V-加群に付随する跡関数のモジュラー不変性ついて述べる．$M = \bigoplus_{n=0}^{\infty} M(r+n)$ を V-加群とする (ここで r は最低固有値に取り替える)．この時，$a \in V(k)$ で $L(n)a = 0\,(n \geq 1)$ を満たすような元に対し (このような性質を持つベクトルを特異ベクトルという)，q-跡 $F_M(a,q)$

$$\begin{aligned} F_M(a,q) &= \mathrm{tr}\,|_M a(k-1) q^{L_0 - \frac{c_V}{24}} \\ &= \sum_{n=0}^{\infty} (\mathrm{tr}\,|_{M_n} a(k-1)) q^{r-\frac{c_V}{24}+n} \in q^{r-\frac{c_V}{24}}\mathbb{C}[[q]] \end{aligned}$$

で定義する．特に $\mathrm{ch}_M(q) = F_M(1,q)$ を加群 M の**指標**という．

定理 2.2. ([Z]) V を C_2-有限な頂点作用素代数とし，$M = \bigoplus_{n=0}^{\infty} M(r+n)$ を V-加群とする．この時，任意の特異ベクトル $a \in V$ に対し，その q-跡 $F_M(a,q)$ は，領域 $\{q \in \mathbb{C} | |q| < 1\}$ で収束し，その極限 $\tilde{F}_M(a,q)$ は，ある $\{|q| < 1\}$ 上定義された正則関数 $f(q)$ に対し，

$$\tilde{F}_M(a,q) = q^{r-c_V/24} f(q)$$

と表される.

従って, 任意の特異ベクトル $a \in V$ に対し,

$$S_M(a,\tau) = \tilde{F}_M(a, e^{2\pi i\tau})$$

と定義すると, 定理 2.2 より $S_M(a,\tau)$ は上半平面 $H = \{z \in \mathbb{C} | \mathrm{Im} z > 0\}$ で正則関数となることがわかる. この正則関数を, $a \in V$ に付随する M の**跡関数**という.

跡関数へのモジュラー群 $SL_2(\mathbb{Z})$ の作用を次のように定義する: 行列 $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z})$ に対し,

$$S|_A(a,\tau) = (\gamma\tau + \delta)^{-k} S\left(a, \frac{\alpha\tau+\beta}{\gamma\tau+\delta}\right)$$

$(a \in V(k))$. この時, 次の定理が成立する.

定理 2.3. ([Z]) V を C_2-有限で有理的な頂点作用素代数とする. また $M^1, \ldots, M^d$ を同型を除いた既約 V-加群の完全なリストとする. この時, 任意の $1 \le i,j \le d$ と $A \in SL_2(\mathbb{Z})$ に対しある定数 $c_{i,j}(A) \in \mathbb{C}$ が一意的に存在して, 任意の特異ベクトル $a \in V$ に対し,

$$S_{M^i}|_A(a,\tau) = \sum_{j=1}^{d} c_{j,i}(A) S_{M^j}(a,\tau)$$

が成立する.

3 格子頂点作用素代数

ここでは正定値 $\mathbb{Z}$ 双線形写像 $(\cdot,\cdot)$ をもつ偶格子 L に付随する頂点作用素代数の構成について簡単に説明する (詳しくは [FLM] を参照). しかし本報告集では階数 1 の格子のみを扱うので, 階数 1 の場合に限定して解説する.

$\mathfrak{h} = \mathbb{C}h$ を $(h,h) = 1$ で定義された対称双線形形式を持つ C 上の 1 次元ベクトル空間とする. ベクトル空間 $\mathfrak{h}$ を可換 Lie 代数とみなしそのアファイン化 $\hat{\mathfrak{h}} := \mathfrak{h} \otimes \mathbb{C}[t,t^{-1}] \oplus \mathbb{C}K$ を考える. Lie 代数 $\hat{\mathfrak{h}}$ の交換関係は

$$[h \otimes t^m, h \otimes t^n] = n\delta_{m+n,0}K, \quad [\hat{\mathfrak{h}}, K] = 0, \quad (m,n \in \mathbb{Z})$$

で与えられる. この時, $\lambda \in \mathfrak{h}$ に対し, $\hat{\mathfrak{h}}$ の可換部分 Lie 代数 $\mathfrak{h} \otimes \mathbb{C}[t]$ の 1 次元加群 $\mathbb{C}e^\lambda$ を次で定義する:

$$(h \otimes t^n).e^\lambda = \delta_{n,0}(\lambda,h)e^\lambda \ (n \ge 0), \quad K.e^\lambda = e^\lambda.$$

この既約 $\mathfrak{h}\otimes\mathbb{C}[t]$-加群から誘導される誘導 $\hat{\mathfrak{h}}$-加群 $U(\hat{\mathfrak{h}})\otimes_{U(\mathfrak{h}\otimes\mathbb{C}[t])}\mathbb{C}e^{\lambda}$ を $M(1,\lambda)$ とする．この時 $\hat{\mathfrak{h}}$-加群 $M(1)=M(1)^0$ には中心電荷 1 の頂点作用素代数の構造が入り，各 $\lambda\in\mathfrak{h}$ に対して $M(1,\lambda)$ が既約な $M(1)$-加群となる．今 $\hat{\mathfrak{h}}$-加群上の $h\otimes t^n\,(n\in\mathbb{Z})$ の作用を $h(n)$ とあらわすことにすると真空ベクトルは $1=1\otimes e^0$, Virasoro 元は $\omega=(1/2)h(-1)^2 1$ で与えられる．また $h(-1)1$ に付随する頂点作用素 $Y(h(-1)\mathbf{1},z)$ は

$$Y(h(-1)\mathbf{1},z)=h(z)=\sum_{n\in\mathbb{Z}}h(n)z^{-n-1}$$

となり任意の元に付随する頂点作用素は $h(z)$ の微分と正規積を用いて定義される．

任意の自然数 k に対し，$\mathfrak{h}$ の元 $\alpha=\sqrt{2k}h$ を考えると，正定値偶格子 $L=\mathbb{Z}\alpha$ が得られる．また $L^\circ=\{h\in\mathfrak{h}\,|\,(h,L)\subset\mathbb{Z}\}$ は L の双対格子である．この時，任意の $\lambda\in L^\circ$ に対して

$$V_{\lambda+L}:=\bigoplus_{m\in\mathbb{Z}}M(1,\lambda+m\alpha)\tag{3.1}$$

とおくと，V_L が頂点作用素代数の構造を持ち，各 $\lambda\in L^\circ$ に対して $V_{\lambda+L}$ が既約な V_L-加群となる．真空ベクトルや Virasoro 元は $M(1)(\subset V_L)$ と同じもの (従って V_L の中心電荷も 1) であり，分解 (3.1) は 既約 $M(1)$-加群への分解を与える．また $1\otimes e^{m\alpha}\in V_L$ (以下 $e^{m\alpha}$ と表す) に対する頂点作用素 $Y(e^{m\alpha},z)$ は

$$Y(e^{m\alpha},z):=\exp\left(\sum_{n=1}^{\infty}\frac{m\alpha(-n)}{n}z^n\right)\exp\left(-\sum_{n=1}^{\infty}\frac{m\alpha(n)}{n}z^{-n}\right)z^{m\alpha}P_{m\alpha}$$

で定義される，ここで $z^{m\alpha}$ や $P_{m\alpha}$ は

$$z^{m\alpha}(u\otimes e^{\mu})=z^{m(\alpha,\mu)}u\otimes e^{\mu},\quad P_{m\alpha}(u\otimes e^{\mu})=u\otimes e^{\mu+m\alpha}$$

$(u\in U(\hat{\mathfrak{h}}),\mu\in\lambda+L)$ で定義される $V_{\lambda+L}$ 上の作用素である．

定理 3.1. ([D], [DLM2]) L を階数 1 の正定値偶格子とする．

(1) この時頂点作用素代数 V_L は C_2-有限かつ有理的である．

(2) 任意の既約 V_L-加群はある $\lambda\in L^\circ$ が存在し $V_{\lambda+L}$ に同値である．また $V_{\lambda+L}$ と $V_{\mu+L}$ が同値となる必要十分条件は $\lambda-\mu\in L$ となることである．

注意 3.2. 定理 3.1 は一般階数の格子 L に対しても成立する．

4 V_L の自己同型群とオービフォールド模型

ここでは階数 1 の格子頂点作用素代数の自己同型群とその有限部分群によるオービフォールド模型について述べる．その中で格子 L の -1-等長変換を持ち上げて得られる位数 2 の自己同型写像 θ によるオービフォールドが有理的であることも述べる．

一般階数の格子頂点作用素代数の自己同型群については [DN] においてその形が決定されている．しかし階数が 1 の時にはその構造を具体的に見ることができる．

今 $L = \mathbb{Z}\alpha$ とおく．この時，線形写像 $\theta : V_L \to V_L$ を各 $m \in \mathbb{Z}$ と $n_i \in \mathbb{Z}_{>0}$ に対し，

$$\theta(h(-n_1)\cdots h(-n_r)e^{m\alpha}) = (-1)^r h(-n_1)\cdots h(-n_r)e^{-m\alpha}$$

で定義すると，この線形写像は V_L の位数 2 の自己同型写像を与える．また任意の $c \in \mathbb{C}^\times$ に対し，

$$t_c(h(-n_1)\cdots h(-n_r)e^{m\alpha}) = c^m h(-n_1)\cdots h(-n_r)e^{-m\alpha}$$

と定義すると，t_c も V_L の自己同型写像を与える．この自己同型写像達は，$t_c \circ t_{c'} = t_{cc'}$ および $\theta \circ t_c \circ \theta = t_{c^{-1}}$ を満たしていることがわかる．

今 $L = \mathbb{Z}\alpha$ で $(\alpha, \alpha) \geq 4$ と仮定する．この時，V_L の自己同型群は

$$\mathrm{Aut}\,(V_L) = \langle \theta, t_c \rangle \cong \mathbb{Z}_2 \ltimes \mathbb{C}^\times$$

となる．実際 $V_L(1)$ は 1 次元でありそれは $h(-1)1$ を基底に持つので，$g \in \mathrm{Aut}\,(V_L)$ に対し，ある $\kappa \in \mathbb{C}^\times$ が存在して $g(h(-1)1) = \kappa h(-1)1$ が成り立つ．Virasoro 元 $\omega = 1/2h(-1)^2 1$ は g で固定されるので $\kappa = \pm 1$ を得る．必要ならば g を $\theta \circ g$ に置き換えることにより $g(h(-1)1) = h(-1)1$ を仮定してよい．これは g の作用が $h(n)\,(n \in \mathbb{Z})$ の作用と可換であることを表し $g : V_L \to V_L$ は $\hat{\mathfrak{h}}$-加群の同型写像であることがわかる．特に $g(e^{m\alpha}) = c_m e^{m\alpha}$ となる $c_m \in \mathbb{C}^\times$ が各 $m \in \mathbb{Z}$ に対して存在し，$e^{(m+1)\alpha} = e^{m\alpha}(-m(\alpha,\alpha) - 1)e^{\alpha}$ が成り立つことに注意すると，この両辺に g を作用させることによって帰納的に $c_m = c_1^m\,(m \in \mathbb{Z})$ が導かれる．このことから $g = t_{c_1} \in \langle \theta, t_c \rangle$ が得られる．

このように $\mathrm{Aut}\,(V_L)$ の有限部分群は共役を除き，巡回群 $C_n = \langle t_{\rho_n} \rangle$, $\rho_n = e^{\frac{2\pi i}{n}}$ もしくは 2 面体群 $D_n = \langle t_{\rho_n}, \theta \rangle$ に同型であり，対応するオービフォールド模型は

$$(V_{\mathbb{Z}\alpha})^{C_n} = V_{\mathbb{Z}n\alpha}, \quad (V_{\mathbb{Z}\alpha})^{D_n} = (V_{\mathbb{Z}n\alpha})^{\langle\theta\rangle} \tag{4.1}$$

となることがわかる．以下 $V_L^+ = V_L{}^{\langle\theta\rangle}$ と定義する．

前節で V_L が C_2-有限かつ有理的であることを述べた．別の言い方をすれば，任意の自然数 n に対し V_L の有限自己同型群 C_n に対するオービフォールド模型は常に C_2-有限で有理的であるということである．群 D_n に対しては，$V_L^{D_n}$ が C_2-有限性が成り立つことを Yamskulna が [Yam] において証明した．そこで講演者は $V_L^{D_n}$ の有理性について考察し，実際に有理的であることを証明した ([A])．まとめると，

定理 4.1. 偶格子 $L = \mathbb{Z}\alpha$, $(\alpha,\alpha) \geq 4$ に対し，V_L^+ は C_2-有限かつ有理的である．

頂点作用素代数 V_L^+ の自己同型群については [DG] において具体的に構成され，決定されている．それは以下のようになる．

$$\mathrm{Aut}\,(V_{\mathbb{Z}\alpha}^+) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & (\alpha,\alpha) = 4,6 \text{ または } (\alpha,\alpha) > 8, \\ S_3, & k = 8. \end{cases}$$

$(\alpha,\alpha) \neq 8$ の場合，$(V_{\mathbb{Z}\alpha}^+)^{\mathbb{Z}/2\mathbb{Z}}$ は $V_{\mathbb{Z}(2\alpha)}^+$ と同型となる．一方 $(\alpha,\alpha) = 8$ の場合には，S_3 の部分群は共役を除いて $1, C_2, C_3$ および S_3 に同型である．対応するオービフォールド模型は $(V_{\mathbb{Z}\alpha}^+)^{C_2} \cong V_{\mathbb{Z}(2\alpha)}^+$ であるが，$(V_{\mathbb{Z}\alpha}^+)^{C_3}$ と $(V_{\mathbb{Z}\alpha}^+)^{S_3}$ はどちらも V_L や V_L^+ と同型とならない．これらのオービフォールド模型は次で述べる $V_{\mathbb{Z}(\sqrt{2}h)}$ のあるオービフォールド模型で与えられる．

L が A_1 型のルート格子，すなわち $(\alpha,\alpha) = 2$ の時には話は複雑になる．記号の濫用であるが，$L = A_1$ と書くことにする．この場合 V_{A_1} は $V_{A_1}(1) \cong sl_2(\mathbb{C})$ で生成されており，その自己同型群は $e^{a(0)}$ $(a \in sl_2(\mathbb{C}))$ で生成される．従って V_{A_1} には Lie 群 $SL_2(\mathbb{C})$ が作用しているが，その作用は忠実ではなく実際にはその中心で割った $PSL_2(\mathbb{C})$ が自己同型群として作用している．よく知られているように $PSL_2(\mathbb{C})$ の有限自己同型群は共役を除いて，巡回群 C_n $(n \geq 1)$，二面体群 D_n $(n \geq 2)$ そして Alt_4, S_4 または Alt_5 に同型である．

自己同型群 $\mathrm{Aut}\,(V_{A_1})$ の部分群として C_n, D_n はそれぞれ $C_n \cong \langle t_{\rho_n} \rangle$ および $D_n \cong \langle t_{\rho_n}, \theta \rangle$ と実現されており，従って対応するオービフォールド模型は (4.1) によって与えられる．$V_{A_1}^+$ の有理性や C_2-有限性，自己同型群についてはまだ説明してないが $\langle\theta\rangle$ が巡回群 C_2 に共役なので $V_{A_1}^+ \cong V_{A_1}^{C_2} \cong V_{2A_1}$ であることから導かれる．すなわち定理 4.1 は任意の正定値偶格子に対し成立する．

残りの有限自己同型群 Alt_4, S_4 または Alt_5 に関するオービフォールド模型に関しては [DGR] による自己同型群に関する研究を除いて現在まであまり研究されていない．[DGR] において，Dong, Griess および Ryba は $V_{A_1}^{Alt_4}$ $V_{A_1}^{S_4}$, $V_{A_1}^{Alt_5}$ の自己同型群を完全に決定した．その結果は以下のようになる．

$$\mathrm{Aut}\,(V_L^{Alt_4}) \cong \mathbb{Z}/2\mathbb{Z}, \quad \mathrm{Aut}\,(V_L^{S_4}) \cong 1, \quad \mathrm{Aut}\,(V_L^{Alt_5}) \cong 1$$

また $V_{A_1}^{Alt_4}$ の自己同型群 $\mathbb{Z}/2\mathbb{Z}$ によるオービフォールド模型が $V_{A_1}^{S_4}$ に同型となる.

最後に $V_{\mathbb{Z}\alpha}^+$, $(\alpha,\alpha)=8$ のオービフォールド模型との関係について述べる. 定義から V_{A_1} は $V_{\mathbb{Z}\alpha}^+$ を部分頂点作用素代数として含んでおり, V_{A_1} は $V_{\mathbb{Z}\alpha}^+$-加群として $V_{\mathbb{Z}\alpha}^+$ を含む 4 つの互いに非同値な既約加群の直和に分解する. この時 $V_{\mathbb{Z}\alpha}^+$ 上には 1 としてそれ 以外の既約加群のいずれか 2 つの上に -1 として作用する写像で生成される正 2 面体群 $\mathfrak{a}$ が S_4 の位数 4 の正規部分群として実現される. すなわち $V_\alpha^+ \cong V_{A_1}^{\mathfrak{a}}$ であり, $S_4/\mathfrak{a} \cong S_3$ が $\mathrm{Aut}\,(V_{\mathbb{Z}\alpha}^+)$ を誘導するのである. このように $V_{\mathbb{Z}\alpha}^+$ のオービフォールド模型は V_{A_1} の S_4 の $\mathfrak{a}$ を含む部分群, つまり共役を除いて $\mathfrak{a}$, Alt_4 および S_4 のオービフォールド模型として得られる. 従って同一視 $(V_{\mathbb{Z}\alpha}^+)^{C_3} \cong (V_{A_1}^+)^{Alt_4}$ と $(V_{\mathbb{Z}\alpha}^+)^{S_3} \cong (V_{A_1}^+)^{S_4}$ が得られる.

以上の議論により次の結果を得る:

定理 4.2. ([DG], [DGR]) 集合

$$\{V_L,\ V_L^+,\ V_{A_1}^{Alt_4},\ V_{A_1}^{S_4},\ V_{A_1}^{Alt_5} \mid L \text{ は階数 1 正定値偶格子 }\}$$

は同型を除き, この集合の頂点作用素代数をとりその有限自己同型群でオービフォールド模型をとるという操作で閉じている.

5 $c=1$ 有理的頂点作用素代数の分類について

この節では Ginsparg により提唱された $c=1$ 有理的共形場理論の分類 (ここでは超対称性を持つ模型については述べない) について簡単に述べる ([G] または [川上–梁] を参照). Ginsparg は [G] においてガウス模型と呼ばれる $c=1$ 有理的共形場理論 (これが格子頂点作用素代数に対応している), およびその部分模型について, その分配関数を調べそれらがモジュラー不変性を持つものの表を構成した. その結果, それらの間には巻き付き数と呼ばれるパラメータを持つ 2 方向の系列と例外的な 3 つの模型があることが見出され, 2 方向には同じ分配関数を持つ模型が現れることを見出した.

Ginsparg の分類の提示のあと, [Kir] において Kiritsis は中心電荷が 1 の分配関数を分類することにより, $c=1$ 有理的共形場理論に現れる分配関数は Ginsparg の提示した模型のものでなければならないことを示し, $c=1$ 有理的共形場理論の分配関数を完全に決定した.

これらの模型はこれまでわれわれが前節まで考察してきた格子頂点作用素代数のオービフォールド模型として得られており, それぞれの共形場理論の分配関数は指標に対応している. Ginsparg の分類により得られる模型は定理 4.2 のいずれかに同型であり, さらに同じ分配関数を持つモデルは頂点作用素代数としても同型となることがわかる.

ここで注意するのは，Ginsparg の分類について対応する頂点作用素代数が存在し，その指標として分配関数が得られるということであり，逆に分配関数が等しい模型は Ginsparg により与えられた模型のいずれかで与えられるかという問題はまだ未解決であるということである．つまり定理 4.2 の頂点作用素代数の指標と等しい $c = 1$ 頂点作用素代数は互いに同型かという問題はまだ未解決である．

モジュラー不変性に関して，定理 2.3 との関連について述べる．定理 2.3 により C_2-有限かつ有理的な頂点作用素代数の既約関数に付随する跡関数の張る空間はモジュラー群の作用で不変である．特にモジュラー群の部分群で既約加群の跡関数に自明に作用する部分群が合同部分群を含めばその指標は特にモジュラー不変性を持つ．この核に関する研究は Bantay ([Ban]) によりされており，係数 $\{c_{i,j}(A)\}$ に関しいくつかの条件[1]が満たされれば，実際にある自然数 N が存在し合同部分群 $\Gamma(N)$ に関し不変になることが知られている．従って階数 1 の偶格子 L に対し V_L, V_L^+ の指標のモジュラー不変性は Zhu の定理（定理 2.3）からの帰結であるとも考えられる．このように例外型の $c = 1$ 頂点作用素代数 $V_{A_1}^{Alt_4}$, $V_{A_1}^{S_4}$, $V_{A_1}^{Alt_5}$ の指標のモジュラー不変性もまた，これらの頂点作用素代数が C_2-有限性と有理性を持つことからの示されるのではないかと推測でき，したがってこれらの模型の C_2-有限性，有理性および既約加群の分類，フュージョン則の決定などがこれからの研究の目的である．

References

[A] T. Abe, Rationality of the vertex operator algebra V_L^+ associated to a even positive definite lattice L, 準備中.

[Ban] P. Bantay, The kernel of the modular representation and the Galois action in RCFT, *Commun. Math. Phys.* **233** (2003), 423–438.

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

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

[DGR] C. Dong, R. L. Griess and A Ryba, Rank one lattice type vertex operator algebras and their automorphism groups II. E-series, *J. Algebra* **17** (1999), 701–710.

[DLM1] C. Dong, H.-S. Li and G. Mason, Twisted representations of vertex operator algebras, *Math. Ann.* **310** (1998), 571–600.

[1]既約加群の最低固有値が有理数であり，フュージョン則と S-行列に対する係数 $\{c_{i,j}(S)\}$ を結ぶ等式である Verlinde 公式が成立するならば成り立つ．V_L や V_L^+ に関してはこれらの条件は成立していることが知られている．

[DLM2] C. Dong, H.-S. Li and G. Mason, Modular-invariance of trace functions in orbifold theory and generalized moonshine, *Commun. Math. Phys* **214** (2000), 1–56.

[DN] C. Dong and K. Nagatomo, Automorphism groups and twisted modules for lattice vertex operator algebras, Contemp. Math., **248**, Amer. Math. Soc., Providence, RI, (1999) 117–133.

[FLM] I. Frenkel, J. Lepowsky and A. Meurman, "Vertex Operator Algebras and the Monster", Pure and Appl. Math., Vol. 134, Academic Press, Boston, 1988.

[G] P. Ginsparg, Curiosities at $c = 1$, *Nucl. Phys. B* **295** (1988), 153–170.

[K] V. Kac, *Vertex algebras for beginners*, Second ed., University Lecture Series **10**, Amer. Math. Soc. 1998

[川上–梁] 川上則雄, 梁 成吉, 共形場理論と 1 次元量子系, 新物理選書, 岩波書店, (1997).

[Kir] E. Kiritsis, Proof of the completeness of the classification of rational conformal field theories with $c = 1$, *Phys. Lett.* B **217** (1989), 427–430.

[MN] A. Matsuo and K. Nagatomo, *Axioms for a Vertex Algebra and the Locality of Quantum Fields*, MSJ Memoirs No.4, Mathematical Society of Japan, 1999.

[Yam] G. Yamskulna, C_2-cofiniteness of the vertex operator algebra V_L^+ when L is a rank one lattice, math.QA/0202056.

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

頂点作用素代数の有限位数の自己同型群とIntertwining operatorについて

田辺顕一朗
筑波大学数学系

Vを頂点作用素代数とし、Gをその有限位数の自己同型群とする。Gによって固定されるVの元の全体V^Gはまた頂点作用素代数になることが知られている。

Vの表現論とGの情報を用いてV^Gの表現論を記述せよという問題が[1]で出されている。その後、色々な設定の下での取り組みが成されている。

今回、既約V加群を分解して得られる既約V^G加群達の間のfusion ruleに関してVのfusion ruleとGの情報を用いた一つの下限を得ることが出来たので報告する。

頂点作用素代数やその加群の定義、基本的な性質は[5]や[6]を参照して下さい。以下Vは単純な頂点作用素代数で、Gはその有限位数の自己同型群とする。

1 準備.

1.1 既約V加群を分解して得られる既約V^G加群.

今回取り扱う既約V^G加群を紹介するために、しばらく色々なものを準備する必要がある。

V加群(L, Y_L)と$g \in G$が与えられたとき、V加群$(L\circ g, Y_{L\circ g})$を$L\circ g := L$かつ

$$Y_{L\circ g}(u,z) := Y_L(gu,z),\ {}^\forall u \in V.$$

で定義する。$\mathcal{S}$を互いに非同型な既約V加群からなる空でない有限集合とする。さらに$\mathcal{S}$はG安定であるとする。$\mathcal{S}$がG安定とは、任意の$L \in \mathcal{S}$

と任意の $g \in G$ に対して、ある $M \in \mathcal{S}$ が存在して V 加群としての同型 $M \circ g \simeq L$ が成り立つことをいう。

$M \circ g \simeq L$ のとき線型同型写像 $\phi(g, L) : L \to M$ で

$$\phi(g, L)Y_L(u, z) = Y_M(gu, z)\phi(g, L), \ {}^{\forall}u \in V.$$

となるものが存在するが、以下各 $g \in G$ と $L \in \mathcal{S}$ に対してそのような写像 $\phi(g, L)$ を一つずつ固定しておく。またこの場合、$M \in \mathcal{S}$ を Lg^{-1} と表すことにする。$L \in \mathcal{S}$ で $a, b \in G$ とする。L の既約性から、$\alpha_L(a, b) \in \mathbb{C}^\times$ で

$$\phi(a, Lb^{-1})\phi(b, L) = \alpha_L(a, b)\phi(ab, L).$$

となるものが存在する。記号 $e(M)$ $(M \in \mathcal{S})$ を準備し、$\{e(M) \mid M \in \mathcal{S}\}$ を基底とする $\mathbb{C}$ 上のベクトル空間 $\mathbb{C}\mathcal{S} = \bigoplus_{M \in \mathcal{S}} \mathbb{C}e(M)$ を考える。$\mathbb{C}\mathcal{S}$ 上に可換な積 $e(L)e(M) := \delta_{L,M}e(M)$ を定義しておく。群環 $\mathbb{C}G$ と $\mathbb{C}\mathcal{S}$ とのテンソル積 $\mathcal{A}_\alpha(G, \mathcal{S}) := \mathbb{C}G \otimes_{\mathbb{C}} \mathbb{C}\mathcal{S}$ 上に積を $(a \otimes e(L))(b \otimes e(M)) := \alpha_M(a, b)ab \otimes e(Lb^{-1})e(M)$ で定義する。$\mathcal{A}_\alpha(G, \mathcal{S})$ は $\mathbb{C}$ 上の有限次元半単純結合代数となることが知られている [4]. $\mathcal{A}_\alpha(G, \mathcal{S})$ の V 加群 $\mathcal{L} := \bigoplus_{L \in \mathcal{S}} L$ への作用を、$a \otimes e(M) \in \mathcal{A}_\alpha(G, \mathcal{S})$ と $u \in L$ に対して $a \otimes e(M) \cdot u := \delta_{M,L}\phi(a, L)u$ で定義する。

V^G は V の部分代数なので自然に $\mathcal{L}$ に作用しているが、V^G と $\mathcal{A}_\alpha(G, \mathcal{S})$ の $\mathcal{L}$ への作用は可換であることが分かる。$V^G \otimes_{\mathbb{C}} \mathcal{A}_\alpha(G, \mathcal{S})$ 加群として $\mathcal{L}$ は

$$\mathcal{L} = \bigoplus_{\lambda \in \Lambda} M_\lambda \otimes Q_\lambda.$$

- $\{Q_\lambda\}_{\lambda \in \Lambda}$: 既約 $\mathcal{A}_\alpha(G, \mathcal{S})$ 加群の完全代表系
- $M_\lambda := \mathrm{Hom}_{\mathcal{A}_\alpha(G,\mathcal{S})}(Q_\lambda, \mathcal{L})$. ($V^G$ 加群としての構造を自然に持つ).

と分解できる。以上の設定の下で Dong と Yamskulna は次を示した:

定理 1. ([4] Theorem 6.14)

1. 各 M_λ は零でない既約 V^G 加群である。
2. V^G 加群としての同型 $M_\lambda \simeq M_\mu$ が成り立つためには $\lambda = \mu$ が必要十分である。

以下、定理 1 を用いて得られた既約 V^G 加群のみを取り扱う。上で表れた結合代数 $\mathcal{A}_\alpha(G, \mathcal{S})$ やその既約加群 Q_λ 達は今回の主結果でも登場し、重要である。

1.2 頂点作用素代数の intertwining operator と fusion rule.

頂点作用素代数の intertwining operator と fusion rule の定義を思い出しておく。

定義 1. L_1, L_2, L_3 を V 加群とする。線型写像

$$\begin{aligned} I(\cdot,x): \quad L_1 &\to \mathrm{Hom}_{\mathbb{C}}(L_2, L_3)\{x\} \\ u &\mapsto I(u,x)=\sum_{\alpha\in\mathbb{C}} u_\alpha x^{-\alpha-1}. \end{aligned}$$

が次の条件を満たしたとき、$I(\cdot,x)$ は $\binom{L_3}{L_1\ L_2}$ 型の intertwining operator であるという:

1. $u\in L_1, v\in L_2, \alpha\in\mathbb{C}$ に対して、整数 n が十分大きければ、$u_{\alpha+n}v=0$ が成り立つ。
2. $u\in L_1$ に対して、$I(L(-1)u,x)=\dfrac{d}{dx}I(u,x)$ が成り立つ。
3. $a\in V, u\in L_1, v\in L_2$ に対して、

$$\begin{aligned} &x_0^{-1}\delta\Big(\frac{x_1-x_2}{x_0}\Big)Y_{L_3}(a,x_1)I(u,x_2)v - x_0^{-1}\delta\Big(\frac{-x_2+x_1}{x_0}\Big)I(u,x_2)Y_{L_2}(a,x_1)v \\ &\quad = x_2^{-1}\delta\Big(\frac{x_1-x_0}{x_2}\Big)I(Y_{L_1}(a,x_0)u,x_2)v. \end{aligned}$$

が成り立つ。

$\binom{L_3}{L_1\ L_2}$ 型の intertwining operator 全体の成すベクトル空間を $I_V\binom{L_3}{L_1\ L_2}$ で表す。その次元 $\dim_{\mathbb{C}} I_V\binom{L_3}{L_1\ L_2}$ を $\binom{L_3}{L_1\ L_2}$ 型の fusion rule と呼ぶ。

2 主結果.

Dong–Yamskulna の定理で得られた既約 V^G 加群達の、intertwining operator の成す線型空間を調べたい。intertwining operator の定義には加群が 3 つ必要なので Dong–Yamskulna の定理に表れたもの達を 3 つずつ用意する必要がある。

S_i $(i=1,2,3)$ を互いに非同型な既約 V 加群からなる空でない G 安定な有限集合とする。$L_i\in S_i$ と $g\in G$ に対して、L_i から L_ig^{-1} への線型同型写像を、$\phi_i(g,L_i): L_i\to L_ig^{-1}$ と表すことにする。

$L_i \in \mathcal{S}_i$ $(i=1,2,3)$ とする。$g \in G$ と $f \in I_V\binom{L_3}{L_1\ L_2}$ に対して ${}_gf \in I_V\binom{L_3g^{-1}}{L_1g^{-1}\ L_2g^{-1}}$ を次で定義する: $u \in L_1$ に対して

$$ {}_gf(u,x) := \phi_3(g,L_3)f(\phi_1(g,L_1)^{-1}u,x)\phi_2(g,L_2)^{-1}. $$

各 $i=1,2,3$ に対して $\mathcal{L}_i := \bigoplus_{L_i \in \mathcal{S}_i} L_i$ とおいて、Dong-Yamskulna の定理で得られた既約 $V^G \otimes \mathcal{A}_{\alpha_i}(G,\mathcal{S}_i)$ 加群への分解を考える:

$$ \mathcal{L}_i = \bigoplus_{\lambda_i \in \Lambda_i} M^i_{\lambda_i} \otimes Q^i_{\lambda_i}. \quad M^i_{\lambda_i}: \text{既約 } V^G \text{ 加群},\ Q^i_{\lambda_i}: \text{既約 } \mathcal{A}_{\alpha_i}(G,\mathcal{S}_i) \text{ 加群}. $$

線型空間

$$ \mathcal{I} := \bigoplus_{(L_1,L_2,L_3)\in \mathcal{S}_1\times\mathcal{S}_2\times\mathcal{S}_3} I_V\binom{L_3}{L_1\ L_2} \otimes L_1 \otimes L_2 $$

を考える。$\mathcal{I}$ には $\mathcal{A}_{\alpha_3}(G,\mathcal{S}_3)$ が次のように作用している: $g \otimes e(M) \in \mathcal{A}_{\alpha_3}(G,\mathcal{S}_3)$, $f \in I_V\binom{L_3}{L_1\ L_2}$, $u \in L_1$, $v \in L_2$ に対して

$$ (g\otimes e(M))\cdot(f\otimes u\otimes v) := \delta_{M,L_3}\cdot {}_gf \otimes \phi_1(g,L_1)u \otimes \phi_2(g,L_2)v. $$

$(\lambda_1,\lambda_2) \in \Lambda_1\times\Lambda_2$ に対して $\mathcal{J}_{\lambda_1,\lambda_2} := \mathrm{Span}_{\mathbb{C}}\{f\otimes u\otimes v \in \mathcal{I} \mid u \in Q^1_{\lambda_1},\ v \in Q^2_{\lambda_2}\}$ とおく。$\mathcal{J}_{\lambda_1,\lambda_2}$ は $\mathcal{I}$ の部分 $\mathcal{A}_{\alpha_3}(G,\mathcal{S}_3)$ 加群になっている。以上の準備の下で主定理を述べる:

定理 2. 各 $(\lambda_1,\lambda_2,\lambda_3) \in \Lambda_1\times\Lambda_2\times\Lambda_3$ に対して

$$ \dim_{\mathbb{C}} I_{V^G}\binom{M^3_{\lambda_3}}{M^1_{\lambda_1}\ M^2_{\lambda_2}} \geq \dim_{\mathbb{C}} \mathrm{Hom}_{\mathcal{A}_{\alpha_3}(G,\mathcal{S}_3)}(Q^3_{\lambda_3}, \mathcal{J}_{\lambda_1,\lambda_2}). $$

が成り立つ。

証明は、まず具体的に $\mathrm{Hom}_{\mathcal{A}_{\alpha_3}(G,\mathcal{S}_3)}(Q^3_{\lambda_3},\mathcal{J}_{\lambda_1,\lambda_2})$ から $I_{V^G}\binom{M^3_{\lambda_3}}{M^1_{\lambda_1}\ M^2_{\lambda_2}}$ への線型写像を構成する。構成法はきちんと述べると長くなるので省略する。構成した写像が単射であることは、Dong-Yamskulna の定理と以下で紹介する二つの補題を用いて示すことが出来るので定理の主張は従う。。

補題 3. $\mathcal{S}_i = \{L^j_i\}_{j\in H_i}$ と元を表示しておく。各 $i \in H_1, j \in H_2$ に対してそれぞれいくつかの一次独立な元 $v^{i1},\dots,v^{ip_i} \in L^i_1, w^{j1},\dots,w^{jq_j} \in L^j_2$ が与えられたとする。また各 $i \in H_1, j \in H_2, k \in H_3$ に対していくつかの一次独立な元 $f^{ijk}_1,\dots,f^{ijk}_{m_{ijk}} \in I_V\binom{L^k_3}{L^i_1\ L^j_2}$ が与えられたとする。

この時 $\{f^{ijk}_r(v^{is},x)w^{jt} \in \mathcal{L}_3\{x\}\}_{i,j,k,r,s,t}$ は一次独立である。

$R_1 \subset L_1$, $R_2 \subset L_2$ をそれぞれ斉次有限次元部分空間とする。P を $\mathrm{Span}_{\mathbb{C}}\{f \otimes u \otimes v \in \mathcal{I} \mid u \in R_1,\ v \in R_2\}$ の有限次元部分空間とする。各 $n \in \mathbb{Z}$ に対して線型写像

$$\begin{array}{rccc} \psi_n : & P & \to & \mathcal{L}_3 \\ & f \otimes u \otimes v & \mapsto & \displaystyle\sum_{i \geq n} f(u)_i v. \end{array}$$

を定義する。$Z_n := \mathrm{Im}\psi_n$ とおく。

$$\begin{array}{rccc} \phi_n : & Z_n & \to & Z_{n+1} \\ & \displaystyle\sum_{i \geq n} f(u)_i v & \mapsto & \displaystyle\sum_{i \geq n+1} f(u)_i v. \end{array}$$

とおく。各 n に対して ϕ_n は well-defined である。ϕ_n を使うと、次の補題を示すことが出来る。

補題 4. $n \ll 0$ に対して線型空間としての同型 $P \overset{\psi_n}{\simeq} Z_n$ が成り立つ。

補題 3. と 4. は [3] の手法を intertwining operator の場合に拡張することによって証明できる。

3 応用.

最近我々は、モンスター単純群の $3B$ 元に関連していると期待されるある具体的な頂点作用素代数の表現論を調べた [2]。その頂点作用素代数はある単純な頂点作用素代数 V の、位数 3 のある自己同型群 $G = \langle g \rangle$ によって固定される部分頂点作用素代数 V^G になっている。現在その fusion rule の計算をしているのであるが、一次独立な intertwining operator を期待される数だけうまく構成できないかと考えたのが今回の研究の動機である。

その頂点作用素代数 V には次の条件を満たす非同型な既約 V 加群 M_0, M_1, M_2 が存在する。

- $M_j \circ g \simeq M_{j+1}$ が成り立っている。添え字は (mod 3) で考えることにする。
- 準備 1.1 に表れたスカラー $\alpha_{M_i}(a,b)$ は全て 1 に取り直すことが出来る。

•

$$\dim_{\mathbb{C}} I_V\binom{M_{2+j}}{M_{0+j}\ M_{1+j}} = \dim_{\mathbb{C}} I_V\binom{M_{2+j}}{M_{1+j}\ M_{0+j}} = 1.\ (j=0,1,2).$$

が成り立っている。M_0, M_1, M_2 を成分とする他の型の fusion rule は 0 である。

Dong-Yamskulna の定理から各 M_j は V^G 加群として同型かつ既約となることが分かる。V^G 加群としては M_j を M で表すことにする。定理2を用いて $\binom{M}{M\ M}$ 型の fusion rule の下限を求めてみる。

$\mathcal{S}_i := \{M_0, M_1, M_2\}$ $(i=1,2,3)$ とおくと、$\mathcal{S}_i$ は G 安定である。$\mathcal{A} := \mathcal{A}_{\alpha_i}(G, \mathcal{S}_i) = \bigoplus_{j,a=0}^{2} \mathbb{C}(g^j \otimes e(M_a))$ となり、

$$(g^j \otimes e(M_a)) \cdot (g^k \otimes e(M_b)) = \delta_{a+k,b} g^{j+k} \otimes e(M_b).$$

が成り立つ。$\mathcal{A}$ は3次正方行列の全体からなる行列環と同型である。次の3次元既約 $\mathcal{A}$ 加群 $W := \oplus_{i=0}^{2} \mathbb{C} q_i$ を定義する: $g^j \otimes e(M_a) \in \mathcal{A}$ と $q_b \in W$ に対して

$$(g^j \otimes e(M_a)) \cdot q_b := \delta_{a,b} q_{b+j}.$$

すると

$$\begin{aligned} \mathcal{L}_i &= M_0 \oplus M_1 \oplus M_2 \simeq M \otimes W.\ (i=1,2,3) \\ &\quad (V^G \otimes \mathcal{A} \text{ 加群としての同型}) \end{aligned}$$

が成り立つ。

$$\begin{aligned} \mathcal{I} &= (\bigoplus_{j=0}^{2} I_V\binom{M_{2+j}}{M_{0+j}\ M_{1+j}} \otimes M_{0+j} \otimes M_{1+j}) \\ &\quad \oplus (\bigoplus_{j=0}^{2} I_V\binom{M_{2+j}}{M_{1+j}\ M_{0+j}} \otimes M_{1+j} \otimes M_{0+j}). \end{aligned}$$

となり、$\mathcal{J}_{MM}$ は $\mathcal{A}$ 加群としては

- $\mathcal{J}' := \mathrm{Span}_{\mathbb{C}}\{(a,b,c) \mid a,b,c \in \{0,1,2\} \text{ は相異なる}\}$.
- $g^j \otimes e(M_d) \in \mathcal{A}$ と $(a,b,c) \in J'$ に対して

$$(g^j \otimes e(M_d)) \cdot (a,b,c) := \delta_{d,a}(a+j, b+j, c+j).$$

で定義される A 加群 $\mathcal{J}'$ と同型となる。$\mathcal{J}'$ は A 加群として

$$\begin{aligned}\mathcal{J}' &= \mathrm{Span}_{\mathbb{C}}\{(0,1,2),(1,2,0),(2,0,1)\}\\ &\quad \oplus \mathrm{Span}_{\mathbb{C}}\{(1,0,2),(2,1,0),(0,2,1)\}\end{aligned}$$

と既約加群に分解することが簡単に分かるので定理2を用いると、

$$\dim I_{V^G}\binom{M}{M\ M} \geq 2.$$

が分かる。

実は $\dim I_{V^G}\binom{M}{M\ M} = 2$ となっていることが、さらにZhu加群の理論や計算機を用いることによって示すことが出来る(計算機は、加群の元の間に成立する関係式を大量に見付けるのに必要である)他の加群の場合も等号が成立している。

参考文献

[1] R. Dijkgraaf, C. Vafa, E. Verlinde, and H. Verlinde, The operator algebra of orbifold models, Comm. Math. Phys. **123** (1989), 485–526.

[2] C. Dong, C.H. Lam, K. Tanabe, H. Yamada, K. Yokoyama, $\mathbb{Z}_3$ symmetry and W_3 algebra in lattice vertex operator algebras, preprint(math.QA/0302314).

[3] C. Dong and G. Mason, On quantum Galois theory, Duke Math. J. **86** (1997), 305-321.

[4] C. Dong and G. Yamskulna, Vertex operator algebras, generalized doubles and dual pairs, *Math. Z.* **241** (2002), 397–423.

[5] I. Frenkel, Y. Huang, and J. Lepowsky, On axiomatic approaches to vertex operator algebras and modules, Mem. Amer. Math. Soc. **104** (1993).

[6] I. Frenkel, J. Lepowsky, and A. Meurman, Vertex operator algebras and the Monster, Pure and Applied Mathematics, **134**, Academic Press, Inc., Boston, MA, 1988.

MIXED BASIC SUBGROUPS IN ABELIAN GROUP THEORY

TAKASHI OKUYAMA

ABSTRACT. In general, primary groups have basic subgroups. It is well-known that all basic subgroups are isomorphic. First we extend the concept of basic subgroups from primary groups to mixed groups. We call the basic subgroups *mixed basic subgroups*. Next we present an example of a mixed group in which not all mixed basic subgroups are isomorphic.

1. NOTATION AND BASICS

Throughout this note, $\mathbf{Z}$ denotes a set of integers, $\mathbf{P}$ a set of all prime integers, and p is a prime.

1.1. Maximal Torsion Subgroups. Let G be a group. If every element of G is of finite order, then G is a *torsion group*, while G is torsion–free if all its elements, except for 0, are of infinite order. Mixed groups contain both nonzero elements of finite order and elements of infinite order. A primary group or p–group is defined to be a group the order of whose elements are power of a fixed prime p.

Proposition 1.1. [2, Theorem 1.1] *The set T of all elements of finite order in a group G is a subgroup of G. Then T is a torsion group and the quotient group G/T is torsion–free. Hence T is the maximal torsion subgroup of G.*

Proof. Since $0 \in T$, T is not empty. If $a, b \in T$, i.e., $ma = 0$ and $nb = 0$ for some $m, n \in \mathbf{Z}$, then $mn(a - b) = 0$, and so $a - b \in T$. Hence T is a subgroup of G. We show that G/T is torsion–free. Suppose that $c + T \in G/T$ such that $l(c + T) \in T$ for some $l \in \mathbf{Z}$. Then $lc \in T$ and $c \in T$. Hence $c + T = T$ is the zero of G/T. By the previous argument, it is easy to see that T is the maximal torsion subgroup of G. □

1.2. Socle. Let G be a group and

$$G[p] = \{g \in G \mid pg = 0\}.$$

1991 *Mathematics Subject Classification.* 20K21, 20K27.

$G[p]$ is called a *p-socle* of G. This is an elementary group in the sense that every element has a square-free order.

1.3. **p-height.** Let G be a group and $g \in G$. The greatest nonnegative integer r for which $p^r x = g$ is solvable for some $x \in G$, is called the p-height $h_p(g)$ of g. If $p^r x = g$ is solvable whatever r is, g is of *infinite p-height*, $h_p^G(g) = \infty$.

1.4. **Pure subgroup.**

Definition 1.2. *A subgroup A of a group G is said to be p-pure in G if, for all nonnegative integer n,*

$$A \cap p^n G = p^n A.$$

If A is p-pure in G for every $p \in \mathbf{P}$, then A is called a pure subgroup of G.

If A is a pure subgroup of G, then $h_p^G(a) = h_p^A(a)$ for all $p \in \mathbf{P}$ and every $a \in A$.

1.5. **N-high subgroups.**

Definition 1.3. *Let G be a group and let A and N be subgroups of G. If A is maximal with respect to the property of being disjoint from N, then A is called an N-high subgroup of G.*

The existence of N-high subgroups is guaranteed by Zorn's lemma. Combining the results in [3] and [1], we obtain the following characterization of N-high subgroups.

Proposition 1.4. *Let N be a subgroup of a group G. Then a subgroup A of G is N-high in G if and only if*

1. $A \cap N = 0$,
2. *A is neat in G,*
3. $G[p] = A[p] \oplus N[p]$ *for every* $p \in \mathbf{P}$, *and*
4. $G/(A \oplus N)$ *is torsion.*

Corollary 1.5. *Let A be a torsion-free subgroup of a group G. Then A is T-high in G if and only if*

1. *A is neat in G,*
2. $G/(A \oplus N)$ *is torsion.*

2. p–INDEPENDENT SYSTEM AND p–BASIC SUBGROUPS

Definition 2.1. *Let G be a group. A system $\{g_i\}_{i\in \mathbf{I}}$ of elements of G, not containing 0, is called p–independent in G, if for every finite subsystem $\{g_1, g_2, \ldots, g_k\}$ and for any positive integer r,*

$$\sum_{i=1}^{k} n_i g_i \in p^r G, \quad n_i g_i \neq 0, \quad n_i \in \mathbf{Z}$$

implies $p^r | n_i$ for $1 \leqq i \leqq k$.

Thus, by definition, p–independence is of finite character. Hence, every p–independent system of G can be expanded to a maximal one.

Lemma 2.2. *Every independent system is necessarily independent.*

Proof. Suppose that $\sum_{i=1}^{k} n_i g_i = 0, n_i g_i \neq 0$, and $n_i \in \mathbf{Z}$. Then $\sum_{i=1}^{k} n_i g_i \in p^r G$. By hypothesis, $p^r | n_i$ for all $r \geqq 1$. Hence $n_i = 0$. This is a contradiction. Therefore $n_i g_i = 0$ for $1 \leqq i \leqq k$ and the assertion is confirmed. □

Lemma 2.3. *A p–independent system contains only elements of infinite order and of orders which are powers of the given prime p.*

Proof. Suppose that g is of order m in a p–independent system and p^s is the highest power of p dividing m. Let $m = p^s t$ with $t \in \mathbf{Z}$. Suppose that $t \neq 1$. Then $(t, p) = 1$ and $p^r x + ty = 1$ for some $x, y \in \mathbf{Z}$. Since $p^s g = p^r x p^s g + typ^s g = p^r x p^s g + ymg = p^r x p^s g \in p^r G$, $p^r | p^s$ for all $r \geqq 1$. This is a contradiction. Hence $p^s g = 0$. □

Lemma 2.4. *The following holds.*

1. *A subgroup generated by a p–independent system in a group G is p–pure in G.*
2. *If an independent system containing but elements of p–power and infinite order generates a p–pure subgroup, then it is p–independent.*

Proof. (1) Let C be the subgroup generated by a p–independent system $\{g_i\}_{i\in \mathbf{I}}$. Let $c \in C \cap p^r G$. Then $c = \sum_{i=1}^{k} n_i g_i \in p^r G$ where $n_i \in \mathbf{Z}$ and $n_i g_i \neq 0$ for $1 \leqq i \leqq k$. By p–independence, there exist $m_i \in \mathbf{Z}$ for $1 \leqq i \leqq k$ such that $n_i = p^r m_i$. Thus $c = p^r \sum_{i=1}^{k} m_i g_i \in p^r C$ and C is p–pure in G.

(2) Let $\{x_i\}_{i\in \mathbf{I}}$ be an independent system in G such that $o(x_i)$ is ∞ or a power of the given p. Set

$$C = \langle x_i \mid i \in \mathbf{I} \rangle = \oplus_{i\in \mathbf{I}} \langle x_i \rangle$$

which is assumed to be p–pure in G. Suppose that $\sum_{i=1}^{l} s_i x_i \in p^r G$ where $s_i \in \mathbf{Z}$ and $s_i g_i \neq 0$ for $1 \leqq i \leqq l$. By the purity of C,

$\sum_{i=1}^{l} s_i x_i = p^r(\sum_{i=1}^{l} t_i x_i)$ for some integers $t_i (1 \leqq i \leqq l)$. Since $\{x_i\}_{i \in I}$ is independent in G, $s_i x_i = p^r t_i x_i$ for $1 \leqq i \leqq l$. If $o(x_i) = \infty$, then $s_i = p^r t_i$. Suppose that $o(x_i) = p^{u_i}$. If $u_i \leqq r$, then $s_i x_i = p^r t_i x_i = 0$. This contradicts the choice of $s_i x_i$. If $u_i > r$, then $p^{u_i} | (s_i - p^r t_i)$ and so $p^r | s_i$. □

Definition 2.5. *Let G be a group. A subgroup B of G is said to be a p-basic subgroup if the subgroup B satisfies the following three conditions:*

1. *B is a direct sum of cyclic p-groups and infinite cyclic groups;*
2. *B is p-pure in G;*
3. *$G/B = p(G/B)$.*

Let

$$B = \oplus_{i \in I} \langle b_i \rangle.$$

The system $\{b_i\}_{i \in I}$ is called a p-basis of G.

If a group G is equipped with the p-adic topology, then the conditions (1),(2),(3) imply that B is Hausdolff in its p-adic topology, which is the same as the one induced by the p-adic topology of G, and B is dense in G.

Evidently, G is a p-basic subgroup of itself if and only if (1) holds for G. Further, 0 is a p-basic subgroup if and only if G is p-divisible.

We present a few examples of p-basic subgroups.

Example 2.6. *Let B_n be a direct sum of cyclic groups of the same order p^n, and A the torsion part of the direct product of the $B_n (n = 1, 2, \dots)$. Then the direct sum $B = \oplus_{n=1}^{\infty} B_n$ is a basic subgroup.*

Proof. A consists of all vectors $a = (b_1, \dots, b_n, \dots)$ with $b_n \in B_n$ such that there is an integer k with $p^k b_n = 0$ for every n, while B consists of all $a \in A$ with almost all $b_n = 0$. Conditions (1) and (2) are clearly satisfied, so it suffices to prove that every $a \in A$ is divisible by p mod B. Since $p^k b_n = 0, a - (b_1 + \cdots + b_n) = (0, \dots, 0, b_{k+1}, b_{k+2}, \dots)$ is certainly divisible by p, because $p \mid b_{k+i}$ in $B_{k+i} (i = 1, 2, \dots)$. □

Example 2.7. *Let $\mathbf{Q}_p^*$ be the ring of p-adic integers and $\mathbf{J_p}$ the additive group of $\mathbf{Q}_p^*$. Then $\mathbf{Z}$ is a p-basic subgroup of $\mathbf{J_p}$.*

Example 2.8. *Let $p_1, p_2, \dots, p_i, \dots$ be different primes, and define*

$$T = \oplus_{i=1}^{\infty} \langle b_i \rangle \quad \textit{with} \quad o(b_i) = p_i.$$

Then T is the torsion part of $\Pi_{i=1}^{\infty} \langle b_i \rangle$. Consider $a_0 = (b_1, \dots, b_i, \dots) \in \Pi_{i=1}^{\infty} \langle b_i \rangle$. For $i \neq j$, the equation $p_j x = b_i$ is uniquely solvable in $\langle b_i \rangle$, thus $\Pi_{i=1}^{\infty} \langle b_i \rangle$ contains unique elements $a_i (i = 1, 2, \dots)$ such that a_i has

0 *for its ith coordinate and satisfies*

$$p_i a_i = (b_1, \dots, b_{i-1}, 0, b_{i+1}, \dots) = a_0 - b_i.$$

Let $G = \langle T, a_i \mid i \geqq 1 \rangle$ *and* $G_i = \langle a_0, a_i \rangle$. *Then* $G_i = \langle a_i \rangle \oplus \langle b_i \rangle$ *and* $G/\langle a_0 \rangle = \oplus_{i=1}^{\infty} G_i/\langle a_0 \rangle \cong \oplus_{i=1}^{\infty} \mathbf{Z}(p_i^2)$. *Hence* G_i *is a* p_i*-basic subgroup of* G.

Lemma 2.9. $\{b_i\}_{i \in \mathbf{I}}$ *is a* p*-basis of a group* G *if and only if* $\{b_i\}_{i \in \mathbf{I}}$ *is a maximal* p*-independent system.*

Proof. ($\Rightarrow$) Suppose that $\{b_i\}_{i \in \mathbf{I}}$ is a p-basis of a group G. Let $B = \oplus_{i \in \mathbf{I}} \langle b_i \rangle$. By Definition 2.5(1), $\{b_i\}_{i \in \mathbf{I}}$ is independent. Further, by Lemma 2.4(2) and Definition 2.5(1)(2), $\{b_i\}_{i \in \mathbf{I}}$ is p-independent in G. Let $0 \neq g \in G$. By Definition 2.5(3), $g + B = pg' + B$ for some $g' \in G$. Hence there exists a relation of the form $g + \sum_{i=1}^{k} b_i \in pG$. Therefore, if we enlarge the system $\{b_i\}_{i \in \mathbf{I}}$ by adjoining g to $\{b_i\}_{i \in \mathbf{I}}$, the arising system is no longer p-independent. Hence $\{b_i\}_{i \in \mathbf{I}}$ is a maximal p-independent system of G.

($\Leftarrow$) Let $\{a_i\}_{i \in \mathbf{I}}$ be a maximal p-independent system of G. By Lemma 2.2, $\{a_i\}_{i \in \mathbf{I}}$ is independent. Thus

$$A = \langle a_i \mid i \in \mathbf{I} \rangle = \oplus_{i \in \mathbf{I}} \langle a_i \rangle.$$

Hence A satisfies the condition (1) of Definition 2.5.

By Lemma 2.4(1), A is p-pure in G. Therefore A satisfies the condition (2) of Definition 2.5.

Let $0 \neq g \in G$. By maximality of $\{a_i\}_{i \in \mathbf{I}}$, there is some relation

$$\alpha_0 g + \sum_{i=1}^{s} \alpha_i a_i \in p^r G, \quad \alpha_i \in \mathbf{Z}, \quad \alpha_0 g \neq 0, \quad \alpha_i a_i \neq 0 \tag{2.10}$$

$$\text{for} \quad 1 \leqq i \leqq s, \quad \text{and} \quad p^r \nmid \alpha_j \quad \text{for some} \quad j (0 \leqq j \leqq s).$$

By the p-independence of the a_i, we have certainly

$$p^r \nmid \alpha_0. \tag{2.11}$$

First we let g be a torsion element and use induction on $o(g)$. Suppose that $o(g) = p$. By (2.10), $\alpha_0 g + A \in p(G/A)$. Further, by (2.10), $\alpha_0 g \neq 0$ and by (2.11), $(p; \alpha_0) = 1$. Hence $g + A \in p(G/A)$.

Suppose by induction that $g + A \in p(G/A)$ for all g with $o(g) < p^r$. Assume $o(g) = p^r$. By (2.11), we can write $\alpha_0 = p^t \beta_0$ with $0 \leqq t < r$, and $(\beta_0, p) = 1$. Now (2.10) becomes $\sum_{i=1}^{s} \alpha_i a_i \in p^t G$. Hence $\alpha_i = p^t \beta_i$ for some integers $\beta_i (1 \leqq i \leqq s)$ and

$$p^t (\beta_0 g + \sum_{i=1}^{s} \beta_i a_i) = p^r b$$

for some $b \in G$. Note that $o(\beta_0 g + \sum_{i=1}^{s} \beta_i a_i - p^{r-t} b) \leqq p^t$. By induction hypothesis,

$$\beta_0 g + \sum_{i=1}^{s} \beta_i a_i - p^{r-t} b + A = pg' + A$$

for some $g' \in G$. Since $r > t$, $\beta_0 g + A \in p(G/A)$. Since $(\beta_0, p) = 1$, $g + A \in p(G/A)$.

Suppose that there is some relation

$$\alpha_0' g + \sum_{i=1}^{s'} \alpha_i' a_i \in p^{r'} G, \quad \alpha_i' \in \mathbf{Z}, \quad \alpha_0' g \neq 0, \quad \alpha_i' a_i \neq 0 \tag{2.12}$$

$$\text{for} \quad 1 \leqq i \leqq s', \quad \text{and} \quad p^{r'} \nmid \alpha_j \quad \text{for some} \quad j (0 \leqq j \leqq s').$$

If $r' < r$, then, by the same argument, we show that $g + A \in p(G/A)$.

Suppose that $r' > r$. Similarly, by the same argument proving (2.11), we can write $\alpha_0' = p^{t'} \beta_0'$ with $0 \leqq t' < r'$, $(\beta_0', p) = 1$ and (2.10) becomes $\sum_{i=1}^{s} \alpha_i' a_i \in p^{t'} G$. Hence $\alpha_i' = p^{t'} \beta_i'$ for some integers $\beta_i' (1 \leqq i \leqq s)$ and

$$p^{t'} (\beta_0' g + \sum_{i=1}^{s} \beta_i' a_i) = p^{r'} b'$$

for some $b' \in G$. Then $t' < r$, because $p^{t'} \beta_0' g = \alpha_0' g \neq 0$ and $o(g) = p^r$. Therefore $o(\beta_0' g + \sum_{i=1}^{s} \beta_i' a_i - p^{r'-t'} b') \leqq p^{t'} < p^{r'}$. By the same argument, we show that $g + A \in p(G/A)$.

Next $o(g) = \infty$. We already showed that if $o(g)$ is of finite, then $g + A \in p(G/A)$. Using this assertion, by the same argument, we show that $g + A \in p(G/A)$.

□

Theorem 2.13. [2, Theorem 32.3] *Every group contains p–basic subgroups for every $p \in \mathbf{P}$.*

Proof. There exists a maximal p–independent system in the group. By Lemma 2.9, it generates a p–basic subgroup. □

Theorem 2.14. [2, Theorem 35.2] *For a given prime p, all p–basic subgroups of a group G are isomorphic.*

3. Basic subgroups of p–groups

We now focus our attention on p–groups where p–basic subgroups are particularly important. If G is a p–group and q is a prime $\neq p$, then evidently G has only one q–basic subgroup, namely 0. Therefore, in p–groups we may refer to the p–basic subgroups simply as *basic subgroups*, without danger of confusion.

Definition 3.1. *Let G be a p-group. A subgroup B of G is said to be a basic subgroup if the subgroup B satisfies the following three conditions:*

1. *B is a direct sum of cyclic p-groups;*
2. *B is pure in G;*
3. *$G/B = p(G/B)$.*

Example 3.2. *Let*

$$B = \oplus_{n=1}^{\infty}\langle x_n\rangle$$

with $o(x) = p^n$ for all $n \geqq 1$. For every $n \geqq 1$, let

$$y_n = x_n - px_{n+1}.$$

Then the following holds.

1. *$\{y_n\}$ is p-independent system in B.*
2. *Let $B' = \langle y_n \mid n \geqq 1\rangle$. Then*

$$B' = \oplus_{n=1}^{\infty}\langle y_n\rangle$$

   is pure in B.
3. *$x_n \notin B'$ for all $n \geqq 0$.*
4. *B/B' is divisible. Hence B' is a proper basic subgroup of B.*

Proof. (1) Suppose that

$$y = \sum_{i=1}^{k} n_i y_i \in p^r B, \quad n_i y_i \neq 0, \quad n_i \in \mathbf{Z} \tag{3.3}$$

for any positive integer r. Then

$$n_1 x_1 + \sum_{i=2}^{k}(n_i - pn_{i-1})x_i - pn_k x_{k+1} \in p^r B.$$

By definition of B, $n_1 x_1 \in p^r\langle x_1\rangle$ and $r \geqq 1$. Hence $p|n_1$ and so $n_1 y_1 = 0$. This contradicts $n_1 y_1 \neq 0$. Inductively, (3.3) becomes

$$y = \sum_{i=r+1}^{k} n_i y_i \in p^r G, \quad n_i y_i \neq 0 \quad \text{for} \quad r+1 \leqq i \leqq k.$$

Hence

$$y = n_{r+1}x_{r+1} + \sum_{i=r+2}^{k}(n_i - pn_{i-1})x_i - pn_k x_{k+1} \in p^r B.$$

By definition of B,

$$n_{r+1}x_{r+1} \in p^r\langle x_{r+1}\rangle, (n_i - pn_{i-1})x_i \in p^r\langle x_i\rangle \quad \text{for} \quad r+2 \leqq i \leqq k.$$

Hence $p^r|n_i$ for $r+1 \leqq i \leqq k$. The assertion is verified.
(2) By Lemma 2.2 and (1), $\{y_n\}$ is independent. Thus

$$B' = \oplus_{n=1}^{\infty}\langle y_n\rangle.$$

By Lemma 2.4(1) and (1), B' is p–pure in B. Since B is a p–group, B' is pure in B.
(3) Suppose that $x_1 \in B'$. Then

$$\begin{aligned} x_1 &\in \sum_{i=1}^{s}\gamma_i y_i \\ &= \gamma_1 x_1 + \sum_{i=2}^{s}(\gamma_i - p\gamma_{i-1})x_i - p\gamma_s x_{s+1} \end{aligned}$$

where $\gamma_i \in \mathbf{Z}$ for $1 \leqq i \leqq s$. Since $\{x_n\}$ is independent in B, we have $p^i|\gamma_i$ for $1 \leqq i \leqq s$. Hence $x_1 = 0$ and this is a contradiction. Therefore $x_1 \notin B'$. By induction and definition, we have $x_n \notin B'$ for all $n \geqq 1$.
(4) By definition, for all $n \geqq 1$, $y_n = x_n - px_{n+1}$ and hence $x_n + B' = px_{n+1} + B'$. Therefore B/B' is divisible. Further, by (2) and (3), B' is a proper basic subgroup of B. □

Occasionally it is useful to speak of a basic subgroup of a torsion group G, too. Thereby, we mean the direct sum $\oplus_p B_p$ of the basic subgroups B_p of the p–components of G. Thus a basic subgroup B of a torsion group G is defined by the conditions:

1. B is a direct sum of cyclic groups of prime power orders;
2. B is pure in G;
3. $G/B = p(G/B)$ for all $p \in \mathbf{P}$.

4. Mixed Basic Subgroups

It is well-known that there exist basic subgroups for all torsion groups. In this section, we consider extending the concept of basic subgroups from torsion groups to arbitrary abelian groups.

Proposition 4.1. *Let G be a group and A a T–high subgroup of G. Then there exists a subgroup L containing A such that*

$$G/T(L) = L/T(L) \oplus T/T(L) \tag{4.2}$$

and $T(L)$ is a basic subgroup of T.

Proof. If T is a direct sum of cyclic groups, then let $L = G$. Suppose that G_p is not a direct sum of cyclic groups for some $p \in \mathbf{P}$. Then G_p is unbounded. By [2, Lemma 35.1], there exists a proper basic subgroup B of T. Since T/B is divisible, T/B is an absolute direct summand

of G/B. Since $(A+B)/B \cap T/B = 0$, there exists a subgroup L of G containing A such that

$$G/B = L/B \oplus T/B.$$

Since L/B is torsion-free, $B = T(L)$. □

Conversely, a subgroup L of G satisfying (4.2) has the following three properties:

1. $T(L)$ is a direct sum of cyclic groups;
2. L is pure in G;
3. G/L is torsion divisible.

It is well-known that, if G is torsion, then a subgroup L of G having the above three properties is a basic subgroup of G. Moreover, L has the property (4.2). In general, we show that, for any group G, the same assertion is verified.

Theorem 4.3. *Let L be a subgroup of a group G. Then L satisfies the following three conditions:*

1. *$T(L)$ is a direct sum of cyclic groups;*
2. *L is pure in G;*
3. *G/L is torsion divisible,*

if and only if

$$G/T(L) = L/T(L) \oplus T/T(L)$$

and $T(L)$ is a basic subgroup of T.

Proof. It suffices to show necessity. First we prove that $G = T + L$. Let $g \in G$. By (3) and (2), $mg \in L \cap mG = mL$ for some integer m. Then we have $mg = mx$ for some $x \in L$. Since $g - x \in T$, $g \in T + L$. Hence $G = T + L$ and so $G/T(L) = L/T(L) \oplus T/T(L)$.

By (3), $T/T(L)$ is divisible. Hence, by (1), $T(L)$ is a basic subgroup of T. □

Proposition 4.1 and Theorem 4.3 provide the existence of mixed basic subgroups of arbitrary abelian groups.

Definition 4.4. *A subgroup L of a group G is said to be a mixed basic subgroup of G if L has the following three conditions:*

1. *$T(L)$ is a direct sum of cyclic groups;*
2. *L is pure in G;*
3. *G/L is torsion divisible.*

By Proposition 4.1 and [2, Lemma 35.1], we immediately state the following.

Corollary 4.5. *Let G be a group. If G_p is unbounded for some $p \in \mathbf{P}$, then we obtain an infinite properly decreasing chain*

$$L_1 \supset L_2 \supset \cdots \supset L_n \supset \ldots$$

where every subgroup L_i is a basic subgroup of G for $i \geqq 1$ such that $T(L_i)$ are all isomorphic.

Proposition 4.1 and Theorem 4.3 combined lead the following useful property.

Corollary 4.6. *Let G be a group. Let A be any subgroup such that $A \cap T = 0$ and B any basic subgroup of T. Then there exists a mixed basic subgroup L containing A such that $B = T(L)$.*

5. An Example

In this section, we present an example of a mixed group in which not all mixed basic subgroups are isomorphic.

Example 5.1. *Let $G = A \oplus B$ where $A = \langle \frac{1}{p^n} \mid n \geqq 0 \rangle$ and $B = \oplus_{n=1}^{\infty} \langle x_n \rangle$ with $o(x) = p^n$. Let $a \in A$ and $a = p^n a_n$ such that $a_n \in A$ and $pa_{n+1} = a_n$ for every $n \geqq 1$. Define*

$$L = \langle a_n + x_n \mid n \geqq 1 \rangle.$$

Then we have the following properties. First, by Definition 4.4, we have the following.

Property 5.2. *G is a mixed basic subgroup of G.*

We will show that L is a mixed basic subgroup of G by verifying the conditions of Definition 4.4.

Property 5.3. *For every $n \geqq 1$, let $y_n = x_n - px_{n+1}$. Then the following holds.*

1. *$y_n \in L$ for all $n \geqq 1$.*
2. *Let $B' = \langle y_n \mid n \geqq 1 \rangle$. Then*

$$B' = \oplus_{n=1}^{\infty} \langle y_n \rangle$$

is pure in B and the maximal torsion subgroup of L, i.e. $B' = T(L)$.

Proof. (1) By definition, $a_n - pa_{n+1} = 0$. Hence

$$\begin{aligned} y_n &= x_n - px_{n+1} \\ &= (a_n + x_n) - p(a_{n+1} + x_{n+1}) - (a_n - pa_{n+1}) \\ &= (a_n + x_n) - p(a_{n+1} + x_{n+1}) \end{aligned}$$

and so $y_n \in L$.
(2) First we show $L[p] = B'[p]$. Let $x \in L[p]$. Then

$$x = \sum_{i=1}^{k} \beta_i(a_i + x_i) \quad \text{and} \quad px = 0 \tag{5.4}$$

where $\beta_i \in \mathbf{Z}$ for $1 \leqq i \leqq k$. Since $px = 0$, we have

$$-\sum_{i=1}^{k} \beta_i p a_i = \sum_{i=1}^{k} \beta_i p x_i \in A \cap B = 0.$$

Since $\{x_i\}$ is independent in B, we have $\beta_i = p^{i-1}\beta_i'$ for some integer β_i'. Since $x \in B$, by (5.4),

$$\sum_{i=1}^{k} \beta_i' p^{i-1} a_i = x - \sum_{i=1}^{k} \beta_i' p^{i-1} x_i \in A \cap B = 0. \tag{5.5}$$

Note that, by definition, $p^{i-1}a_i = a_1$. By (5.5),

$$\sum_{i=1}^{k} \beta_i' = 0. \tag{5.6}$$

and

$$\begin{aligned}
x &= \sum_{i=1}^{k-1} \beta_i' p^{i-1} x_i \\
&= \beta_1'(x_1 - px_2) + (\beta_1' + \beta_2')px_2 + \sum_{i=3}^{k} \beta_i' p^{i-1} x_i \\
&= \beta_1'(x_1 - px_2) + (\beta_1' + \beta_2')p(x_2 - px_3) \\
&+ (\beta_1' + \beta_2' + \beta_3')p^2 x_3 + \sum_{i=4}^{k} \beta_i p^{i-1} x_i \\
&= \cdots \\
&= \beta_1'(x_1 - px_2) + (\beta_1' + \beta_2')p(x_2 - px_3) \\
&+ (\beta_1' + \beta_2' + \beta_3')p^2(x_3 - px_4) + \ldots \\
&+ (\beta_1' + \beta_2' + \cdots + \beta_{k-1}')p^{k-2}(x_{k-1} - px_k) \\
&+ (\sum_{i=1}^{k} \beta_i')p^{k-1} x_k.
\end{aligned}$$

By (5.6), $(\sum_{i=1}^{k} \beta_i')p^{k-1}x_k = 0$. Then

$$x = \sum_{i=1}^{k-1}(\sum_{j=1}^{i} \beta_j')p^{i-1}y_i \in B'[p].$$

Hence

$$L[p] = B'[p]. \tag{5.7}$$

Next we prove that $T(L) = B'$. Note that $B' \subseteq T(L) \subseteq B$. Suppose that $pz \in B'$ with $z \in T(L)$. Since

$$pB' \subseteq B' \cap p(T(L)) \subseteq B' \cap pB \overset{=}{(3.2)}(2)pB',$$

we have $B' \cap p(T(L)) = pB'$. Therefore $pz \in pB'$ and $pz = pb$ for some $b \in B'$. Since $z - b \in L[p]$, by (5.7), $z - b \in B'$ and $z \in B'$. Hence $B' = T(L)$. □

Property 5.8. *L is a proper mixed basic subgroup of G.*

Proof. By definition, $G = L + B$. By Property 5.3(2), $G/B' = L/B' \oplus B/B'$ and $B' = T(L)$. Further, by Example 3.2(3), $B' = T(L)$ is a proper basic subgroup of B. Hence, by Theorem 4.3, L is a proper mixed basic subgroup of L. □

Property 5.9. *$L \ncong G$.*

Proof. Suppose that $L \cong G$. Then $L = F \oplus B'$ where $F \cong A$. Note that F is the maximal p–divisible subgroup of L. Since $L \subseteq G$, $F \subseteq A$ and hence $F = A$. This contradicts $x_1 \notin L$. Hence $L \ncong G$. □

REFERENCES

[1] K. Benabdallah and J. Irwin. On N–High Subgroups of Abelian Groups, *Bull. Soc. Math. France*, 96:337–346, 1968.

[2] L. Fuchs. *Infinite Abelian Groups, Vol. I, II.* Academic Press, 1970 and 1973.

[3] J. Irwin and E. A. Walker. On N–High Subgroups of Abelian Groups, *Pacific J. Math.*, 11(4):1363–1374, 1961.

DEPARTMENT OF MATHEMATICS, TOBA NATIONAL COLLEGE OF MARITIME TECHNOLOGY, 1–1, IKEGAMI–CHO, TOBA–SHI, MIE–KEN, 517–8501, JAPAN
E-mail address: okuyamat@toba-cmt.ac.jp

代数的ゲーム理論の現状

川中　宣明　(大阪大学・情報科学研究科)

2003年10月28日

1　典型的なゲーム

ここでは次の３つを「典型的なゲーム」と考える。

（1）「中山 正のゲーム」（非確率的１人ゲーム）([5])

ヤング図形 Y と自然数 r が与えられたとき、Y から r フックを次々に「抜いて」いく。（正確に言うと「フックを抜いて（もし、必要なら）詰める」だが、わずらわしいので、単に「抜く」と表現する。）ただし、r フックとは、r の倍数個の「箱」からなるフックのことである。r フックが抜けなくなったら、ゲームは終了する。このゲームは、対称群のモジュラー表現と関係が深い。（詳しくは [3] を参照して下さい。）指定した r をはっきりさせたいときは「中山の r フック ゲーム」と呼ぶことにする。

（2）「佐藤幹夫のゲーム」（非確率的２人ゲーム）([9])

中山の r フック ゲームを、二人のプレイヤーが交互にプレイする「２人ゲーム」に改造したものを「佐藤の r フック ゲーム」と呼び、$r=1$ の場合は単に「佐藤のゲーム」と呼ぶ。自分の番なのにプレイするべき「手」がない、という状態になった人が「負け」である。

（3）「Greene-Nijenhuis-Wilf のゲーム」（確率的１人ゲーム）([2])

与えられたヤング図形の上を、hook walk のルールに従って移動していくゲームである。詳細については、岡村修志氏の修士論文 [6], およびこの報告集の中の岡村氏の稿を参照して下さい。

以上の３つのゲームの、どれにもヤング図形とフックが登場する。その意味で、これらのゲームの間に表面的な類似性があるのは明らかである。しかし、後で述べるフック公式（定理２および定理３）は、より深い内的関連性の存在を暗示する。この関連性の追及が、現在の「代数的ゲーム理論」における中心的問題のひとつである。([10] において、佐藤幹夫氏は、佐藤のゲームと対称群の表現論の類似性を追及する問題を提唱し、それが「良い数学の種になるだろう。」と述べている。）

2　代数系としての「ゲーム」

一般的な立場からゲームを研究するには「ゲームの定義」が必要である。われわれは次の定義を採用する。

定義　S を空でない集合とし、$\varphi : S \longrightarrow 2^S$ を S から S の部分集合の空間 2^S への写像とする。組 (S,φ) が「ゲーム」であるとは、次の２条件を満たすこととして定義される。
①　任意の $s \in S$ に対し、$|\varphi(s)| < \infty$,
②　S の元の列 $s_0.s_1, s_2, ..., s_i, s_{i+1}, ...$ で、$s_{i+1} \in \varphi(s_i), i = 0, 1, 2, ...$ を満たすものは必ず有限列である。言い換えれば、ある i に対して $\varphi(s_i) = \emptyset$ である。

ゲーム (S,φ) が与えられたとき、S の元をそのゲームの「局面 (position)」という。また、局面 s に付随する集合 $\varphi(s)$ を局面 s における「選択肢 (option)」という。選択肢が存在しない、すなわち $\varphi(s) = \emptyset$ であるような局面 s のことを「終局面 (ending position)」という。
ゲーム (S,φ) を「１人ゲーム」のモデルとみなすときは、プレイヤーはある（前もって与えられた）局面 s から出発して、次々と選択肢の中の元を選んでいき、終局面に達したらゲームは終了、と考える。とくに、各々の選択肢 $\varphi(s)$ に前もって確率測度を入れておき、その確率測度に従って、選択肢の中の元を選んでいくと考えれば「確率的１人ゲーム」のモデルとなる。「２人ゲーム」のモデルとみなすときは、２人のプレイヤーが交互に選択肢の中の元を選んでいき、終局面を先に選んだプレイヤーを勝ちと判定する。

「ゲーム」の数学的定式化としては、既に von Neumann-Morgenstern によるものや Conway [1] によるものがある。しかし、第１節で考えた「典型的ゲーム」（１）～（３）（および、それらの一般化）の関連を研究するためには、（確率的または非確率的）１人ゲームと２人ゲームを並行的に取り扱う必要がある。これが、われわれが上の（新しい）定式化を必要とする理由である。この目的のため、われわれは、少なくとも今のところは、研究の対象を「２人のプレイヤーの選択肢が一致している」タイプの２人ゲームに限定することにした。日常的なゲーム（囲碁、将棋、オセロなど）には「自分の石（或いは駒）」という概念があり、２人のプレイヤーの選択肢は明確に区別されている。（相手の駒を動かしたり、相手の石を置いたりすることは禁止されている。）Conway の理論では、このタイプの２人ゲームに重点が置かれているが、われわれはその種の２人ゲームは扱わない。ゲーム概念を純粋数学の一部として取り込むためには、現時点では、そのほうがより適切と考えるからである。

ゲーム (S,φ) は単項演算 φ をもつ代数系と考えることができる。(ただし、この演算 φ の値は一意には定まらないし、値が「空」になることすらある。)そのように考えると、ゲームの同型写像や準同型写像の概念が自然に定義され、部分ゲームの概念も定義される。ここでは「部分ゲーム」と「ゲームの和」の定義だけを書いておく。

定義　(S,φ) をゲームとする。S の空でない部分集合 S' に対し

$$\varphi'(s') = \varphi(s') \cap S'$$

と置くと (S',φ') はゲームである。これを部分ゲームという。とくに任意の $s \in S$ に対し

$$\varphi^{(1)}(s) = \varphi(s), \varphi^{(k)}(s) = \{\varphi(t) | \, t \in \varphi^{(k-1)}(s)\} \ (k = 2,3,...),$$

$$< s >= \{s\} \cup \varphi^{(1)}(s) \cup \varphi^{(2)}(s) \cup ...$$

とおいたとき、部分ゲーム $< s >$ を s で生成された部分ゲームという。

定義　2つのゲーム (S_1,φ_1) と (S_2,φ_2) の和 $S_1 + S_2$ とは、次で定義されるゲーム (S,φ) のことである。

$$S = S_1 \times S_2,$$

$$\varphi(s_1,s_2) = (\varphi(s_1) \times \{s_2\}) \cup (\{s_1\} \times \varphi(s_2)), \quad s_1 \in S_1, s_2 \in S_2.$$

これは「グラフの積」と呼ばれている概念と実質的に同じものだが、ゲーム理論では伝統的に「和」と呼ばれているので、ここでも「和」と呼んでおく。S_1 に対応するゲーム盤と S_2 に対応するゲーム盤を並べて置き（手番のたびに）どちらか一方を選んでプレイする、というゲームのことである。

3　ダイアグラムとフック

第1節で述べた3つのゲームでは「ヤング図形」と「フック」の概念が主要な役割を演じているという意味で「特殊なゲーム」のように見える。この節では、ダイアグラム（図形）もフックも一般のゲームで定義できる概念であることを説明する。

定義　(S,φ) をゲームとする。局面 $s \in S$ のダイアグラム $D(s)$ とは、s における選択肢 $\varphi(s)$ に「*フック構造 H^*」を入れたもののことである。

$$D(s) = \varphi(s), \quad H^*(s') = \{s'' \in D(s) | \, s' \in \varphi(s'')\}, \ s' \in D(s)$$

$H^*(s')$ を $s' \in D(s)$ における *フックといい、$H(s') = H^*(s') \cup \{s'\}$ を s' におけるフックという。ダイアグラム $D(s)$ の2元 s_1, s_2 に対し

$$s_1 < s_2 \Longleftarrow s_1 \in H^*(s_2)$$

とすると、$<$ は $D(s)$ 上の半順序を生成する。

局面 s のダイアグラム $(D(s), H^*)$ は、それ自体、ひとつのゲームである。これを corner-hook-walk ゲームと呼ぶ。corner-hook-walk ゲームで終局面 t に達したら、$(D(s), H^*)$ の部分ゲーム $D(s) \setminus \{t\}$ に移行し、以下、同様に繰り返してダイアグラムが空になるまで続けるのが hook-walk ゲームである。(これらについては、岡村修志氏の稿を見ていただきたい。)

4 ルート系とゲーム

代数的ゲーム理論の中心的テーマのひとつは「良いゲーム」を構成することである。「良い」の基準としては、第1節であげた典型的ゲームと類似の性質をもつこと、と解釈しておくことにする。不思議なことに、かなり多くの数学分野で「良い対象」はルート系と結びついている。ゲームも例外ではない、ということを示すのが、この節の目的である。
まず、記号の説明を兼ねて、 Kac-Moody Lie 代数のルート系とワイル群についての一般的事項を復習する。詳細については、[4] を参照して下さい。

$A = (a_{ij})_{1 \le i,j \le n}$ を generalized Cartan matrix とする。すなわち、A は次の条件を満たす整数行列である。

$$(1)\ a_{ii} = 2,\ 1 \le i \le n, \quad (2)\ a_{ij} \le 0,\ i \ne j, \quad (3)\ a_{ij} < 0 \Leftrightarrow a_{ji} < 0$$

V を有限次元実ベクトル空間とし、$\check{V}$ をその双対ベクトル空間とする。$\alpha_1, ..., \alpha_n$ を V の、$\check{\alpha}_1, ..., \check{\alpha}_n$ を $\check{V}$ の一次独立な元とし

$$< \alpha_i, \check{\alpha}_j >= a_{ij}, \quad 1 \le i, j \le n$$

を満たしているとする。$\Pi = \{\alpha_1, ..., \alpha_n\}$ の元を simple root という。V の線形変換 $r_i = r_{\alpha_i}$ と $\check{V}$ の線形変換 $\check{r}_i$ を

$$r_i(v) = v - < v, \check{\alpha}_i > \alpha_i, \qquad \check{r}_i(\check{v}) = \check{v} - < \alpha_i, \check{v} > \check{\alpha}_i$$

で定義する。これらは $r_i^2 = 1, \check{r}_i{}^2 = 1$ を満たすから、それぞれ $GL(V), GL(\check{V})$ の元である。$W = W_\Pi$ を $\{r_i |\ 1 \le i \le n\}$ で生成された $GL(V)$ の部分群とし、$\check{W}$ を $\{\check{r}_i |\ 1 \le i \le n\}$ で生成された $GL(\check{V})$ の部分群とする。対応 $r_i \longrightarrow \check{r}_i$ によって $W \cong \check{W}$ なので、以下では $r_i = \check{r}_i$, $W = \check{W}$ と同一視す

る。このとき

$$< v, \check{v} > = < w(v), w(\check{v}) > \quad v \in V, \check{v} \in \check{V}, w \in W$$

が成り立つ。$w(\alpha_i)(w \in W, 1 \leq i \leq n)$ の形の V の元を real root という。real root の全体を Δ とかく。Δ の元 α は

$$\alpha = \sum_i c_i \alpha_i, \quad c_i \in \mathbf{Z}$$

と一意的にかくことができる。すべての $c_i \geq 0$ なら正の root、すべての $c_i \leq 0$ なら負の root という。正の root の全体を Δ^+、負の root の全体を Δ^- とおくと

$$\Delta = \Delta^+ \cup \Delta^-$$

が成り立つ。同様にして、$\check{\Delta}$、$\check{\Delta}^{\pm}$ も定義される。Δ と $\check{\Delta}$ の間には

$$(w\alpha)\check{} = w(\check{\alpha})$$

を満たすような一対一対応

$$\alpha \longleftrightarrow \check{\alpha}$$

がある。$\alpha = \sum_i c_i \alpha_i \in \Delta^+$ に対し、その height を

$$ht(\alpha) = \sum_i c_i$$

で定義する。また

$$r_\alpha(v) = v - < v, \check{\alpha} > \alpha, \quad v \in V$$

によって $r_\alpha \in GL(V)$ を定義する。$\alpha = w\alpha_i$ $(w \in W)$ なら

$$r_\alpha = w r_i w^{-1}$$

である。

以下、simple root $\alpha_* \in \Pi$ を固定し、$r_{\alpha_*} = r_*$ とおく。$\alpha \in \Delta^+$ が（α_* に関し）1-increasing root であるとは

$$\alpha = r_{i_k} \cdots r_{i_1} \alpha_*, \quad ht(r_{i_t} \cdots r_{i_1} \alpha_*) = t + 1 \ (1 \leq t \leq k), \quad r_{i_1}, \ldots, r_{i_k} \neq r_*$$

とかけることをいう。このことと $w = r_{i_k} \cdots r_{i_1}$ が $W_{\Pi \setminus \{\alpha_*\}}$ の (dominant) minuscule element (D. Peterson の意味、[7] [11] 参照、Peterson 自身の論文は未発表）とは同値である。この事実を用いると minuscule element の分類 [8] [11] が非常に簡単化される。

S を (α_* に関する) 1-increasing roots 全体の集合とし、$\alpha \in S$ に対し

$$\mathcal{H}(\alpha) = \{\beta \in \Delta^+ | \ < \alpha, \check{\beta} >= 1\}$$

とおく。また $\varphi : S \longrightarrow 2^S$ を

$$\varphi(\alpha) = \{r_\beta \alpha | \ \beta \in \mathcal{H}(\alpha)\}, \quad \alpha \in S$$

で定義する。(右辺は S の部分集合である。) (S, φ) がゲームであることは容易にわかる。

注意　multiply-laced な Dynkin 図形から生じるゲームはすべてある simply-laced なディンキン図形から生じるゲームに同型であることがわかる。このゲームとしての同型は Stembridge [11] による類似の結果 (poset としての同型) より強い主張である。

定理 1　t を自然数とする。$\varphi_t : S \longrightarrow 2^S$ を

$$\varphi_t(\alpha) = \{r_\beta \alpha | \ \beta \in \Delta^+, < \alpha, \check{\beta} >= 1, ht(\beta) \text{ is a multiple of } t\}$$

で定義する。$\alpha \in S$ で生成される (S, φ_t) の部分ゲームを $< \alpha >_t$ とかく。このとき、次が成り立つ。
(i) $< \alpha >_t$ の ending position は α から一意的に決まる。
(ii) $< \alpha >_t \cong < \alpha_1 > + < \alpha_2 > + ... + < \alpha_k >$ となる $\alpha_1, \alpha_2, ... \alpha_k \in S$ が存在する。ただし、$< \alpha_i >$ は　α_i で生成された (S, φ) の部分ゲームを意味する。

上の定理は、ヤング図形における t-core と t-quotient の理論 ([3]) の一般化である。ヤング図形の場合はA型のルート系にひとつ別の simple root α_* を付け加えてできる (ディンキン図形が Y の字型の) ルート系に対応する。この場合に第3節で述べた一般論に従ってダイアグラムとフックを定義すれば、ヤング図形とそのフックが復元され、r_β の作用が「フックを抜く」という操作に対応するのである。

定理 2 (岡村 [6]) $\alpha \in S$ とする。ダイアグラム $D(\alpha)$ における hook-walk ゲームにより $D(\alpha)$ の線形化が等確率

$$\prod_\beta ht(\beta)/n!, \quad (\beta \in \mathcal{H}(\alpha))$$

で生成される ($n = |D(\alpha)|$)。とくに、$D(\alpha)$ の線形化の個数 $N(D(\alpha))$ はフック公式

$$N(D(\alpha)) = n! / \prod_\beta ht(\beta), \quad (\beta \in \mathcal{H}(\alpha))$$

で与えられる。

上の定理は Greene-Nijenhuis-Wilf [2] の結果の一般化である。詳細については、岡村氏の稿を参照して下さい。

次の結果を述べるためには、$\mathbf{Z}$ における (標準とは異なる) 和 $\oplus$ が必要である。$a,b,c \in \mathbf{Z}$ の 2 進展開を

$$a = \ldots a_3 a_2 a_1 a_0, \quad b = \ldots b_3 b_2 b_1 b_0, \quad c = \ldots c_3 c_2 c_1 c_0$$

とする。$a \oplus b = c$ であるとは

$$a_i + b_i \equiv c_i \quad (\mod 2), \quad i = 0,1,2,3,\ldots$$

であることと定義する。これは人工的な定義に見えるかもしれないが、次のように考えると、ある意味で非常に自然な和であることがわかる。$a,b \in \mathbf{Z}_{\geq 0}$ とし、$a = b = 0$ から始めて、順に、$a \oplus b$ の値を次のルール①～③に従って決めていくのである。

① 当然ながら加法の法則（可換則、結合則、0 元の性質）は全て満たさなければならない。
② これも当然ながら、$\mathbf{Z}_{\geq 0}$ のどの 2 元も全て相異なるとする。
③ 上の 2 つのルールに違反しない限り、$a \oplus b$ の値としては（その時点で）可能な限り、最も小さい値とする。

たとえば、ルール①により $0 \oplus 0 = 0,\ 0 \oplus 1 = 1 \oplus 0 = 1$ である。次に $1 \oplus 1$ を考えるが、ルール③を適用すると $1 \oplus 1 = 0$ となる。再びルール①により、$2 \oplus 0 = 0 \oplus 2 = 2$ である。次は $2 \oplus 1$ と $1 \oplus 2$ だが、この値を 0 としても、或いは 1 または 2 としても、ルール①②と既に決まっている $1 \oplus 1 = 0$ に矛盾することがわかる。従って、ルール③により $2 \oplus 1 = 1 \oplus 2 = 3$ となる。以下同様にして、順に下から決めていくと、上で 2 進法を用いて定義したのと一致する和 $\oplus$ が生成される。($\mathbf{Z}$ 全体での $\oplus$ についても同様である。) 情報科学（符号理論、暗号理論など）では、和 $\oplus$ は「排他的論理和 (exclusive or)」と呼ばれ、常用されている。

定理 3 ([12]) ゲーム (S,φ) は、定理 1，2 と同じく、上でルート系を用いて定義されたゲームとする。$E : S \longrightarrow \mathbf{Z}_{\geq 0}$ をフック公式

$$E(\alpha) = \sum_{\beta} \mathrm{Norm}(E(\beta)), \quad (\beta \in \mathcal{H}(\alpha))$$

で定義する。(ただし、$\mathrm{Norm}(x) = x \oplus (x-1),\ x \in \mathbf{Z}$, とする。) このとき、2 人ゲーム $< \alpha >$ が後手必勝であるための必要十分条件は

$$E(\alpha) = 0$$

で与えられる。

上の定理は佐藤 [9] の結果の一般化である。講演では、この結果の k-version についても述べた。これは Norm を

$$\mathrm{Norm}_k(x) = x \oplus (x - 2^k), \quad k = 0, 1, 2, ...$$

に置き換えて（もちろん、それに応じてゲーム自体も変形して）できる定理３の一般化である。残念ながら k-version については、定理１と定理２の類似は存在しないように見える。

定理１～３のうち、証明がほぼ満足できる形で得られているのは、定理１だけである。他の定理の証明には、1-increasing roots の分類＝ minuscule 元の分類 [8] が使われ、今のところ本質的に case-by-case でのチェックが必要になってしまう。

参考文献

[1] J. H. Conway : On Numbers and Games, Academic Press, 1976.

[2] C. Greene, A. Nijenhuis, and H.S. Wilf : A probabilistic proof of a formula for the number of Young tableaux of a given shape, Advances in Math., 31, 104-109 (1979).

[3] G.D. James and A. Kerber : The representation theory of symmetric groups. Encyclopaedia of Mathematics and Its Applications, Vol. 16, Addison-Wesley, Reading, Massachusetts, 1981.

[4] V. G. Kac : Infinite-dimensional Lie Algebras, Birkhauser, Boston, 1983.

[5] T. Nakayama : On some modular properties of irreducible representations of a symmetric group I, II, Jap. J. Math., 17, 165-184, 411-423 (1940).

[6] 岡村修志：一般化された標準ヤング盤を等確率でランダムに生成するアルゴリズム、大阪大学大学院修士論文 (2003 年 3 月).

[7] R. A. Proctor : Minuscule elements of Weyl groups, the numbers game, and d-complete posets, Journal of Algebra, 213, 272-303 (1999).

[8] R. A. Proctor : Dynkin diagram classification of λ-minuscule Bruhat lattices and of d-complete posets, J. Algebraic Combinatorics, 9, 61-94 (1999).

[9] 佐藤幹夫（榎本彦衛記）： Maya game について、数学のあゆみ、15-1（佐藤幹夫特集号)、73-84、 1970.

[10] 佐藤幹夫（梅田 亨記）：佐藤幹夫講義録（1984/85、ソリトン理論)、数理解析研究所、1989.

[11] J. R. Stembridge : Minuscule elements of Weyl groups, Journal of Algebra 235, 722-743 (2001).

[12] N. Kawanaka : Sato-Welter games and Kac-Moody Lie algebras, 数理解析研究所講究録「表現論的組合せ論」、2001.

ユークリッド空間における種々のデザインの概念と tight デザインの分類

坂内英一（Eiichi Bannai）・ 坂内悦子（Etsuko Bannai）

九大・数理（Graduate School of Mathematics Kyushu University）

この原稿は上記タイトルで行った第 20 回代数的組合せ論シンポジウム（北大学術交流会館）の講演の OHP シートをかなり忠実に再現したものである.

t-デザインおよび tight t-デザインについて次の様ないろいろな立場から考察することができる.

Approximation Theory :
- Cubature formula (quadrature fomula)
- Orthogonal polynomials
- etc.

Combinatorics :
- t-(v, k, λ) design
- t-designs in Q-polynomial association schemes
- spherical t-designs and generalizations
- etc.

Statistics
- rotatable designs
- optimal designs
- experimental designs
- etc.

Representation theory, Geometry
- designs on projective space
- designs on Grassmannian spaces
- designs on symmetric spaces
- etc.

この講演では t-デザインなどに関する上記の様なアプローチの簡単な解説とともに、次の 3 つの新しい結果について述べる.

(1) Tight Euclidean 4-designs with constant weight の分類. ([2] 参照.)

(2) Tight Gaussian 4-designs with constant weight あるいは Tight Gaussian 4-designs on 2 concentric spheres の分類. ([3] 参照.)

(3) Tight optimal 4-designs on 2 concentric spheres の分類. ([4] 参照.)

講演では時間の関係もあって上記（2）の証明の概略のみを与えた．上記（3）は講演の時点では完全には完成していなかったが、その後完成した.

1 Approximation theory からのアプローチ

定義. 区間 t-デザイン
区間 $[a,b](\subset \mathbf{R}^1)$ の有限部分集合 $X=\{x_1,\ x_2,\ldots,x_m\}$ は次の条件を満たす時に区間デザインと呼ばれる.

$$\frac{1}{b-a}\int_a^b f(x)dx=\frac{1}{|X|}\sum_{x\in X}f(x)$$

が高々 t 次の全ての多項式に対して成り立つ.

定義. cubature fomula of strength t (=ウエイト関数 $\omega(x)$ を持つ t-デザイン)
区間 $[a,b]$ の有限部分集合 X は次の条件を満たす時に strength t の cubature fomula と言う.

$$\frac{1}{b-a}\int_a^b f(x)dx=\sum_{x\in X}\omega(x)f(x)$$

が高々 t 次の全ての多項式に対して成り立つ．ここで $\omega: X\to \mathbf{R}_{>0}$ はウェイト関数と呼ばれ $\sum_{x\in X}\omega(x)=1$ を満たす.

次に $k(x)$ を区間 $[a,b]$ 上で定義された正の実数値をとる重み関数とする．ここでは簡単のために連続性を仮定しておく.

定義. 重み関数を持った cubature fomula of strength t
(=重み関数 $k(x)$ とウエイト関数 $\omega(x)$ を持つ t-デザイン)
区間 $[a,b]$ の有限部分集合 X は次の条件を満たす時に strength t の cubature fomula と言う.

$$\frac{1}{\int_a^b k(x)d(x)}\int_a^b f(x)k(x)dx=\sum_{x\in X}\omega(x)f(x)$$

が高々 t 次の全ての多項式に対して成り立つ．ここで $\omega: X\to \mathbf{R}_{>0}$ はウェイト関数と呼ばれ $\sum_{x\in X}\omega(x)=1$ を満たす.

この時次のことがよく知られている.

Gauss-Jacobi quadrature formula
任意の与えられた重み関数 $k(x)$ に対して，有限集合 $X=\{x_1,\ x_2,\ \ldots,x_{e+1}\}$ $(\subset[a,b])$ および正の実数の組 $\{\lambda_1,\ \lambda_2,\ \ldots,\lambda_{e+1}\}$ が存在して次の条件を満たす．

$$\omega(x_i)=\lambda_i,\ i=1,\ldots,e+1,$$

かつ

$$\frac{1}{\int_a^b k(x)dx}\int_a^b f(x)k(x)dx=\sum_{x\in X}\omega(x)f(x)$$

が高々 $2e+1$ 次の全ての多項式に対して成り立つ．

上の Gauss-Jacobi quadrature formula の詳細については Szegö の本（[20]47 頁付近）を参照されたい（あるいは [14], [16], [11] 参照）．ここで $p_0(x),\ p_1(x),\ \ldots,p_{e+1}(x),\ \ldots$ は重さ関数 $k(x)$ に関する直交多項式とする，即ち

$$\frac{1}{\int_a^b k(x)dx}\int_a^b p_i(x)p_j(x)k(x)dx=\delta_{i,j}$$

が成り立っているとすると $x_1,\ x_2,\ \ldots,x_{e+1}$ は多項式 $p_{e+1}(x)$ の零点であり $\omega(x_i)=\lambda_i$ は Chrietoffel numbers と呼ばれ次の式で与えられる．

$$\begin{aligned}\lambda_i=&\quad\frac{1}{p_0(x_i)^2+p_1(x_i)^2+\cdots+p_{e+1}(x_i)^2}\\=&\quad\frac{1}{K_{e+1}(x_i,x_i)}\end{aligned}$$

さて，Cubature formula (quadrature formula) の高次元版はどうなるであろうか？　特に Gauss-Jacobi quadrarure formula の高次元版はどれぐらい可能であろうか？Dunkl-Xu の本 [11] はこの問題意識で書かれており非常に興味深い．具体的には次の問題を主に考えたい．

Ω を $\mathbf{R}^n$ の領域とし Ω 上の重み関数を $k:\Omega\to\mathbf{R}_{>0}$ とする．X を Ω の有限部分集合とする．この時次の状況を考える．

$$\frac{1}{\int_\Omega k(x)dx}\int_\Omega f(x)k(x)dx=\sum_{x\in X}\omega(x)f(x)$$

が任意の高々 t 次の n 変数多項式 $f(x)=f(x_1,\ldots,x_n)$ に対して成り立っている．

Q.1 この時 $|X|$ の自然な下界（lower bound）は？
Q.2 $|X|$ がその下界と一致する時（その様な X を tight t-デザインと呼ぶ）その様な X の分類は可能か？

例.　球面上のデザイン
$\Omega=S^{n-1}$（単位球面）$\subset\mathbf{R}^n$ において次の

cubature formula for strength t （イ）
spherical t-designs ($\omega(x)$ =constant となる cubature formula of strength t) （ロ）

の二つが考えられる. (ここで $k(x) \equiv 1$ とする.)

(イ), (ロ) のいずれにおいても

$$|X| \geq \begin{cases} \binom{n-1+e}{e} + \binom{n-1+e-1}{e-1}, & \text{if } t = 2e \\ 2\binom{n-1+e}{e}, & \text{if } t = 2e+1 \end{cases}$$

が成り立つことが知られている.

上の不等式は、(ロ) の場合は Delsarete-Goethals-Seidel [9] による球面デザインについての良く知られている結果であるが, より一般の (イ) の場合に同じ不等式が Approximation theory においてその前からすでに知られていたとも言える. ただし, (ロ) の場合を特に考えることにより, 組合せ論の立場からの研究が活発になったと言える. なお, (イ) の状況で $|X|$ が上の不等式において等号を満たせば, 実は $\omega(x)$ は定数であり, 従って (ロ) の場合になる, 即ち球面デザインになることが示される. したがって, 球面上の tight デザインを考えている限りでは, (イ) と (ロ) のどちらで考えても構わないということになる. 後でみるように, 一般のユークリッド空間上のデザインに関しては (イ) と (ロ) の間で大きな差異が現れる.

一般に $\mathrm{Pol}_e(\mathbf{R}^n)$ を高々 e 次の n 変数多項式全体の作るベクトル空間とする. $\Omega \subset \mathbf{R}^n$ に対して $\mathrm{Pol}_e(\mathbf{R}^n)$ の定義域を Ω に制限したものを $\mathrm{Pol}_e(\Omega) = \mathrm{Pol}_e(\mathbf{R}^n)|_\Omega$ と置く. この時 $\mathrm{Pol}_e(\Omega) \cong \mathrm{Pol}_e(\mathbf{R}^n)$ が成り立つ時 (あるいは Ω が開集合を含む時) 次の条件 :

$$\frac{1}{\int_\Omega k(x)dx} \int_\Omega f(x)k(x)dx = \sum_{x \in X} \omega(x) f(x)$$

が任意の高々 $2e$ 次の n 変数多項式 $f(x) = f(x_1, \ldots, x_n)$ に対して成り立っている,
が成り立つならば

$$|X| \geq \binom{n+e}{e}$$

が成り立つ.

上の不等式において等号が成立している場合に X を $k(x)$, $\omega(x)$ に関する Ω の tight $2e$-デザインと呼ぶ. (このデザインは $2e+1$- デザインに成る可能性もあることにも注意されたい.

Gauss-Jacobi quadrature の高次元版を考えることは, これが $2e+1$-デザインになる場合をかんがえることになる (Dunkl-Xu [11] 参照) .

我々の問題意識は $2e$-デザインの場合を考えることにある. $2e+1$ を考えるのと $2e$ で考えるのはかなりの違いがある.

2 新しい結果 (Gaussian デザイン について)

定義. Gaussian デザイン
$X \subset \mathbf{R}^n$, $|X| < \infty$, $\alpha > 0$ とする.

$$\frac{1}{\int_{\mathbf{R}^n} e^{-\alpha\|x\|^2} dx} \int_{\mathbf{R}^n} f(x) e^{-\alpha\|x\|^2} dx = \sum_{x \in X} \omega(x) f(x) \tag{2-1}$$

が任意の高々 $2e$ 次の n 変数多項式 $f(x) = f(x_1, \ldots, x_n)$ に対して成り立っている時に X を $\mathbf{R}^n$ の Gaussian $2e$-デザインと呼ぶ.

X が $\mathbf{R}^n$ の Gaussian $2e$-デザインであれば $|X| \geq \binom{n+e}{e}$ が成り立つことは容易に分かる.

上記の不等式において等号が成り立つ時に X を Gaussian tight $2e$-デザインであると言う.

一般のウェイト $\omega(x)$ に関する Gaussian tight $2e$-デザインについて次の定理が成り立つ. 定理に使う記号をまず説明する. $\{\|x\| \mid x \in X\} = \{r_1, r_2, \ldots r_p\}$ とする. X は原点 0 を含む場合もありうる. S_i を原点を中心とする半径 r_i の球面とする. $r_i = 0$ の時は $S_i = \{0\}$ とする. $X_i = X \cap S_i$ と置く.

定理 1.
X を Gaussian tight $2e$-デザインとすると次の条件 (1), (2) および (3) が成り立つ.

(1) $p \geq [\frac{e}{2}] + 1$.

(2) $\omega(x)$ は各 X_i 上で一定の値をとる.

(3) 各 X_i は高々 e-距離集合である. 即ち $|\{\|u - v\| \mid u, v \in X_i,\ u \neq v\}| \leq e$.

定理 2.
X を tight Gaussian 4-デザインとすると次の条件 (1), (2), (3), および (4) が成り立つ.

(1) $0 \in X$ の時 X が $\mathbf{R}^n$ の tight Gaussian 4-デザインであることと $X - \{0\}$ が半径 $\sqrt{\frac{n+2}{2\alpha}}$ 上の tight 4-デザイン (従って $p = 2$) であることは同値である. この時 weight $\omega(x)$ は次の式で与えられる.

$$\omega(x) = \begin{cases} \frac{2}{n+2}, & x = 0 \text{ の時}, \\ \frac{2}{(n+3)(n+2)}, & \|x\| = \sqrt{\frac{n+2}{2\alpha}} \text{ の時}, \end{cases}$$

(2) $0 \notin X$ かつ $p = 2$ の時, $n = 2$ となり X は直交変換により次の 6 点集合に移る.

$$\{r_1(\cos\frac{2l\pi}{3}, \sin\frac{2l\pi}{3}),\ -r_2(\cos\frac{2l\pi}{3}, \sin\frac{2l\pi}{3}) \mid l = 0,\ 1,\ 2\}.$$

ここで $r_1 = \frac{\sqrt{5}+1}{\sqrt{2\alpha}}$, $r_2 = \frac{\sqrt{5}-1}{\sqrt{2\alpha}}$ であり, ウエイト関数 $\omega(x)$ は次の式で与えられる.

$$\omega(u) = \begin{cases} \omega_1 = \frac{1}{6} - \frac{\sqrt{5}}{15} & \text{for } u \in X_1 \\ \omega_2 = \frac{1}{6} + \frac{\sqrt{5}}{15} & \text{for } u \in X_2. \end{cases}$$

(Note that $\frac{\omega_1}{\omega_2} = (\frac{r_2}{r_1})^3$ holds.)

(3) $\omega(x)$ が X 上で定数である時, Gaussian tight 4-デザインは存在しない.

(4) ウエイトが $\omega(x) = e^{-\alpha\|x\|^2}$ である Gaussian tight 4-デザインは存在しない.

注意:
(i) 上の定理2 (3) では仮定から $p \leq 2$ を示すことができるので定理2 (2) を用いることにより証明できる.
(ii) 一般のウェイト $\omega(x)$ を持ち, $p \geq 3$ である様な Gaussian tight 4-デザインの分類はまだ未解決問題である.

3 統計におけるデザインとの関連

以下 $\Omega \subset \mathbf{R}^n$ とし通常 Ω は直交群 $O(n)$ により不変であることを仮定する. Ω 上の正規化された測度 ξ ($\xi(\Omega) = 1$) を Ω 上のデザインと呼ぶ. $\dim(\mathrm{Pol}_e(\Omega)) = m$ とし $\mathrm{Pol}_e(\Omega)$ の基底 $e_1, e_2, \ldots, e_m$ を一組固定する. 各 ξ に対して $\mathrm{Pol}_e(\Omega)$ の内積を $\langle f, g\rangle_\xi = \int_\Omega f(x)g(x)d\xi(x)$ で定義する. この時行列

$$M_\xi = \left(\langle e_i, e_j\rangle_\xi\right)_{\substack{1\leq i\leq m,\\ 1\leq j\leq m}}$$

を Ω 上のデザイン ξ の information 行列と言う. 行列 M_ξ が正則である時にデザイン ξ の次数は e であると言う. 以下 [8], [15], [16], [18], [19], [10] などを参照.

注意:
(i) 球面 S^{n-1} 上の spherical $2e$-デザイン X は $\Omega = S^{n-1}$ 上の次数 e のデザインであるが, $\Omega = \mathbf{R}^n$ 上で考えると次数 e とはなり得ない.
(ii) Ω 上のデザイン ξ および $\gamma \in O(n)$ に対して $\xi \circ \gamma$ は Ω 上のデザインとなる.

定義
Ω 上のデザイン ξ おいて,

$$\int_\Omega f(x)d\xi = \int_\Omega f(x)d(\xi \circ \gamma)$$

が任意の $\gamma \in O(n)$ および次数が高々 t の任意の多項式 $f(x)$ にたいして満される時にデザイン ξ は strength t を持つと言う. (厳密に言うと統計のデザインにおいて strength が t であるとは上記の等式が高々 t 次の多項式まで満たされて $t+1$ については満たされていないことを言うが, ここではこだわらないことにする.)

注意:
上記の定義には多くの言い換えがある. (Noimaier-Seidel [18], [19], Delsarte-Seidel [10] 参

照.)

定義 (Rotatable デザイン, Euclidean デザイン)
Ω 上のデザイン ξ は次数 e かつ strength $2e$ の時に rotatable デザインであると言う.
次数 e の rotatable デザインが有限なサポート $X = \mathrm{suppt}(\xi)$ を持つ時 X を Euclidean $2e$-デザインと呼ぶことにする. さらに $|X| = \binom{n+e}{e}$ の時に tight であると言う.

さて, ベクトル空間 $\mathrm{Pol}_e(\Omega)$ に正定値な内積 $\langle -, - \rangle$ を一つ固定しておく. 各デザイン ξ に対して

$$V_e(\xi) = \{f \in \mathrm{Pol}_e(\Omega) \mid \langle f, f \rangle_\xi \leq 1\}$$

とし上記で固定した内積空間 $(\mathrm{Pol}_e(\Omega), \langle -, - \rangle)$ における $V_e(\xi)$ の体積を $\mathrm{Vol}(V_e(\xi))$ とする.
(Ω 上のデザイン ξ が次数 e であることと $\mathrm{Vol}(V_e(\xi)) < \infty$ であることは同値である.)

定義 (Optimal デザイン)
Ω 上の次数 e のデザイン ξ について

$$\mathrm{Vol}(V_e(\xi)) \leq \mathrm{Vol}(V_e(\eta))$$

が Ω 上の任意のデザイン η にたいして成り立つ時に ξ を optimal であると言う.

注意 :
Ω 上の optimal デザイン ξ について information 行列の行列式 $\det(M_\xi)$ は

$$\{\det(M_\eta) \mid \eta \text{ は } \Omega \text{ 上のデザイン}\}$$

の中での最大値を与えている.

事実 :
(i) 次数 e の optimal デザインは次数 e の rotatable デザインである.
(ii) $\mathbf{R}^n$ の Gaussian $2e$- デザインは $\mathbf{R}^n$ の 次数 e の rotatable デザインである.

定理 (まとめ)

(I) Tight Euclidean 4-デザインでウェイトが定数であるものは次のように分類される (2002 年 12 月の数理研研究集会の報告集参照) : すなわち, そのようなものは

$$X = \{0\} \cup (\text{tight spherical 4-design })$$

につきる. ここでは spherical design は単位球面だけでなく任意の半径についても考える.

(II) $\mathbf{R}^n$ の二つの同心球面にのっている tight Gaussian 4-デザインは分類される (定理 2 (1), (2) 参照). ウェイトが定数である tight Gaussian 4-デザインは存在しない (定理 2 (3) 参照).

(III) $\mathbf{R}^n$ の二つの同心球面にのっている tight optimal 4-デザインの分類はウェイトが定数である Euclidean tight 4-デザインの分類に帰着される.

注意：
(i) spherical tight 4-デザインの存在・非存在に関してはいろいろなことが知られている ([9], [5] ,[6], [1], [7] 参照) .

(ii) 上記 (I),(II),(III) の証明はほぼ共通の手法を用いた．この講演では (II) について簡単に述べた．ここではそれについて次の節で解説する．

(iii) 上記定理の (I), (II), および (III) を全て含む「Master Theorem」としてウェイト ω が定数でない場合の $\mathbf{R}^n$ の Euclidean tight 4-デザインの分類定理が強く望まれる．もしそれができれば (I), (II), (III) はその中に含まれる．

(iv) (I), (II), (III) の tight $2e$-デザイン ($e \geq 3$) の分類も非常に望まれる．

4 Tight Gaussian 4-デザイン

この節では (II), 即ち定理 1 および定理 2 の証明の概略を述べる．n 変数の調和多項式全体の作るベクトル空間を $\mathrm{Harm}(\mathbf{R}^n)$ とする．また n 変数の l 次同次多項式全体の作るベクトル空間を $\mathrm{Hom}_l(\mathbf{R}^n)$ とし，$\mathrm{Harm}_l(\mathbf{R}^n) = \mathrm{Hom}_l(\mathbf{R}^n) \cap \mathrm{Harm}(\mathbf{R}^n)$ とする．次に球面上の Haar 測度 σ を一つ固定する．そして $\mathrm{Harm}(\mathbf{R}^n)$ の正定値内積

$$\langle f, g \rangle_\sigma = \frac{1}{\int_{S^{n-1}} d\sigma(x)} \int_{S^{n-1}} f(x)g(x)d\sigma(x)$$

に関する $\mathrm{Harm}_l(\mathbf{R}^n)$ の正規直交基底 $\{\varphi_{l,i}(x) \mid 1 \leq i \leq N_l\}$ を考える．ここで $N_l = \dim(\mathrm{Harm}_l(\mathbf{R}^n))$ とする．次に $\mathrm{Pol}_e(\mathbf{R}^n)$ の正定値内積

$$\langle f, g \rangle = \frac{1}{\int_{\mathbf{R}^n} e^{-\alpha\|x\|^2} dx} \int_{\mathbf{R}^n} f(x)g(x)e^{-\alpha\|x\|^2} dx$$

を考える．この時各 l に対して一変数多項式の組 $\{g_{l,j}(R)\}$ で次の条件を満たすものが存在する．即ち $g_{l,j}(R)$ の次数は j かつ集合 $\mathcal{H}_l = \{g_{l,j}(\|x\|^2)\varphi_{l,i}(x) \mid 0 \leq j \leq [\frac{e-l}{2}],\ 1 \leq i \leq N_l\}$ は $\mathrm{Hom}_l(\mathbf{R}^n)$ の正規直交基底になっている．この時 $\mathcal{H} = \sum_{l=0}^{e} \mathcal{H}_l$ は $\mathrm{Pol}_e(\mathbf{R}^n)$ の正規直交基底になっている．この時 $|\mathcal{H}| = \dim(\mathrm{Pol}_e(\mathbf{R}^n)) = \binom{n+e}{e}$ である．

次に $\mathbf{R}^n$ の有限部分集合 X と $\mathcal{H}$ で添字付けられた行列 M を考える．M の $(x, g_{l,j}\varphi_{l,i})$ 成分を $\sqrt{\omega(x)}g_{l,j}(\|x\|^2)\varphi_{l,i}(u)$ としておく．そうすると X が $\mathbf{R}^n$ のウェイトが $\omega(x)$ の Gaussian $2e$-デザインであるならば ${}^tM\,M = I$ が成立する．(従って $|X| \geq \binom{n+e}{e}$ が成り立つ.) さらに X が tight であれば (即ち $|X| = \binom{n+e}{e}$ であれば) M は正則な正方行列となり $M\,{}^tM = I$ を得る．以下 X を tight Gaussian $2e$-デザインであると仮定して式 $M\,{}^tM = I$ を解釈する．

(u,u)-成分

$r_i \neq 0$ とし $R_i = r_i^2$ と置く．$u \in X_i$ とする．この時対角成分 $(M\,{}^tM)(u,u)$ は調和多項式

の正規直交基底を使った Gegenbauer 多項式 $Q_l(y)$, $(0 \le l \le e)$ の和公式により

$$\omega(u) \sum_{l+2j \le e} {R_i}^l \, g_{l,j}({R_i})^2 Q_l(1) = 1 \tag{4-1}$$

となる．左辺の $\omega(u)$ 以外の項は n, e, R_i にのみ依存して定まる．したがって $\omega(u)$ は X_i 上で定数となる（定理１（２））．

(u,v)-成分
$R_i(={r_i}^2) \neq 0$ とすると u, $v \in X_i$, $u \neq v$, に対して

$$\sum_{l+2j \le e} {R_i}^l \, g_{l,j}({R_i})^2 Q_l(\frac{(u,v)}{R_i}) = 0 \tag{4-2}$$

となる．従って u, v の内積 (u,v) は高々 e 次の多項式のゼロ点になっている．即ち各 X_i は高々 e-距離集合である（定理１（３））．

上記の行列 M は正則である．従って 単項式の集合 $\{||x||^{2j} \mid 0 \le j \le [\frac{e}{2}]\}$ は X 上で一時独立でなければならない．したがって $p \ge [\frac{e}{2}] + 1$ を得る（定理１（１））．これで定理１の証明は完了する．

以下 X は $\mathbf{R}^n$ の tight Gaussian 4-デザインとする．もし $0 \in X$ であれば $p \ge 3$ とすると $X - \{0\}$ は少なくとも原点を中心とする少なくとも２つの同心球面と交わっておりかつ $X - \{0\}$ は少なくとも２つの同心球面上にのっている Euclidean 4-デザインである．そうすると，Delsarte-Seidel [10] の定理により $|X - \{0\}| \ge \binom{n+2}{2} = |X|$ が成り立つことになって矛盾を引き起こす．従って $p = 2$ となる．この時 $X - \{0\}$ は一つの球面上にのっており spherical 4-デザインである．この時ウェイト関数 $w(x)$ の値は Gaussian デザインの定義式 (2-1) を単項式 $||x||^2$ と $||x||^4$ に応用することによって定理２（１）で与えた値になることが計算できる（定理２（１）の証明完了）．

次に $0 \notin X$ かつ $p = 2$ とする．また以下の証明では $n \ge 7$ の場合について述べる．$n \le 6$ の場合はそれぞれ特別な考察によって証明することができるが，ここでは詳細は述べないことにする．([12], [13] 参照.) 各 X_i 上での $\omega(x)$ の値を ω_i とする．この時 ω_i は Gaussian デザインの定義式 (2-1) を単項式 $||x||^2$ と $||x||^4$ に応用することによって n, α, R_1 $(={r_1}^2)$, R_2 $(={r_2}^2)$, $|X_1|$, $|X_2|$ により一意的に与えられることが分かる（実は $|X_2| = \binom{n+2}{2} - |X_1|$）．得られた ω_1 と ω_2 を ${}^tMM + I$ の対角成分から得られた式 (4-1) に代入すると各 X_i に対して次の等式が得られる．

$$4(|X_i| - n)\alpha^2 {R_i}^2 - 4|X_i| n R_i \alpha - n^2 + n^2|X_i| + 2|X_i| n - 2n = 0. \tag{4-3}$$

次に u, $v \in X_i$, $u \neq v$ に対して $A_i = ||u - v||^2$ と置くと ${}^tMM + I$ の非対角成分から得られた式 (4-2) より A_i に関する２次の多項式が得られる．もし $|X_i| \le n$ とすると A_i の満たす２次式方程式が実根を持たなくなることが示せる．従って $|X_i| > n$, $i = 1, 2$ を得る．今 $|X_1| \ge |X_2|$ としておくと

$$\frac{1}{2}\binom{n+2}{2} \le |X_1| \le \binom{n+2}{2} - (n+1) = \frac{n(n+1)}{2}$$

が成り立つ．n が小さくないと言う仮定より上記の不等式から常に X_1 は2-距離集合になっている．2-距離集合については次の定理が知られている．

Larman-Rogers-Seidel の定理 ([17])
$\mathbf{R}^n$ の 2-距離集合 X の距離の 2 乗を a, b $(b>a)$ とする．$|X|>2n+3$ であれば次の条件を満たす自然数 k が存在する．即ち

$$2\leq k\leq \sqrt{\frac{n}{2}}+\frac{1}{2},\quad \frac{a}{b}=\frac{k-1}{k}.$$

さて X_1 の異なる 2 点間の距離の 2 乗 A_1 の満たす 2 次式の 2 根を a, b とする．$\frac{a}{b}=\frac{k-1}{k}$ で k を定義すると

$$\left(\frac{a+b}{a-b}\right)^2=(2k-1)^2$$

が成り立つ．一方 a, b を今述べた 2 次式を使って具体的に計算すると

$$\left(\frac{a+b}{a-b}\right)^2=\frac{(1+2\alpha R_1)^2}{4\alpha R_1-n-1}$$

が得られる．右辺の関数を R_1 の関数として考えて $G(R_1)$ と置く．式 (4-3) より $G(R_1)$ は $|X_1|$, n, α の関数となるが，n と α を固定すると $|X_1|$ に関する単調減少関数となることが証明できる．これは初等的な微積分を使った沢山の計算を必要とする．このことから $n\geq 7$ の時に

$$n+3<G(R_1)<n+6$$

を得る．従って $G(R_1)+n+4$ または $n+5$ でなければならない．このことから $n+4=(2k-1)^2$ または $n+5=(2k-1)^2$ でなければならないがいずれの場合も矛盾が得られる（定理２（２）の証明完了）．

この定理の証明では 2-距離集合に関する Larman-Rogers- Seidel の定理を本質的に使ったが彼等の定理の 3-距離集合あるいは e-距離集合 $(e\geq 3)$ への拡張が強く望まれる．

References

[1] E. Bannai and E. Bannai, *Algebraic Combinatorics on Spheres* (in Japanese) Springer Tokyo 1999.

[2] E. Bannai and E. Bannai, *On Euclidean tight 4-designs* , preprint.

[3] E. Bannai and E. Bannai, *On Gaussian tight 4-designs* , preprint.

[4] E. Bannai and E. Bannai, *On Optimal Tight 4-Designs on 2 Concentric Spheres*, preprint.

[5] E. Bannai and R. M. Damerell, *Tight spherical designs I*, J. Math. Soc. Japan 31 (1979) 199-207.

[6] E. Bannai and R. M. Damerell, *Tight spherical designs II*, J. London Math. Soc. 21 (1980) 13-30.

[7] E. Bannai, A. Munemasa and B. Venkov, *The nonexistence of certain tight spherical designs*, preprint.

[8] G. E. P. Box and J. S. Hunter, *Multi-factor experimental designs for exploring response surfaces*, Ann. Math. Statist. 28, (1957)195–241

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

[10] P. Delsarte and J. J. Seidel, *Fisher type inequalities for Euclidean t-designs*, Lin. Algebra and its Appl. 114-115 (1989) 213-230.

[11] C. F. Dunkl and Y. Xu, Orthogonal polynomials of several variables. Encyclopedia of Mathematics and its Applications, 81. Cambridge University Press, Cambridge, 2001. xvi+390 pp.

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

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

[14] A. Erdélyi et al. *Higher transcendental Functions, Vol II, (Bateman Manuscript Project)*, MacGraw-Hill (1953).

[15] S. Karlin and W. J. Studden, *Tchebycheff Systems with Application in Analysis and Statistics*, Interscience, 1966.

[16] J. Kiefer, *Optimum designs V, with applications to systematic and rotatable designs*, Proc. 4th Berkeley Sympos. 1, (1960) 381–405.

[17] D. G. Larman, C. A. Rogers and J. J. Seidel, *On two-distance sets in Euclidean space*, Bull London Math. Soc. 9 (1977) 261-267.

[18] A. Neumaier and J. J. Seidel, *Discrete measures for spherical designs, eutactic stars and lattices*, Nederl. Akad. Wetensch. Proc. Ser. A 91=Indag. Math. 50 (1988) 321-334.

[19] A. Neumaier and J. J. Seidel, *Measures of strength 2e and optimal designs of degree e*, Sankya 54 (1991) 299-309.

[20] G. Szegö, Orthogonal polynomials. Fourth edition. American Mathematical Society, Colloquium Publications, Vol. XXIII. American Mathematical Society, Providence, R.I., 1975. xiii+432 pp.

一般化された標準ヤング盤の総数公式の確率論的証明

大阪大学大学院情報科学研究科　岡村修志

1　はじめに

Kac-Moody Lie 環の Weyl 群の dominant minuscule 元 (5 節参照) に対して、その最短表示の総数公式を与える定理 (Peterson) がある。この定理の完全な証明は Peterson と Proctor によって準備中と言われているが、2003 年 7 月現在、論文またはプレプリントの形で発表されていない。この定理は Proctor[P1][P2] と Stembridge[St2] によって、d-complete poset と呼ばれる図形の標準盤の総数を与える hook 公式 (4 節参照) と同値であることが示された。d-complete poset は Young 図形や Shifted Young 図形を特殊な場合に含む拡張された図形であり、(simply-laced な場合の)dominant minuscule 元を特徴付けるものとして Proctor[P1][P2] によって導入された (2 節・5 節参照)。本稿において d-complete poset の定義 (2 節)、及びその hook の定義 (3 節) を与え、d-complete poset に対する hook 公式及び、その証明方針を概説し (4 節)、Peterson の定理と hook 公式との同値性について簡単に説明する (5 節)。

Young 図形に対する hook 公式は、歴史的には Frame-Robinson-Thrall[FRT] によって最初に与えられ、様々な証明が知られているが、その中で確率論的証明が Greene-Nijenhuis-Wilf[GNW] により与えられた。hook 公式は hook 自体が分からなくても、hook length さえ分かれば適用できる公式である (従って hook length 公式とも呼ばれる) がこの確率論的証明においては hook 自体が大きな役割を演じる。正確には、hook walk algorithm と言う hook が本質的な役割を果たす確率的アルゴリズムを構成し、そのアルゴリズムが与えられた形の d-complete poset の任意の標準盤を等確率生成するアルゴリズムであることを示すことで hook 公式が証明される (4 節参照)。同様の方法を用いて Sagan[Sa] により Shifted Young 図形の場合が証明された。一般の d-complete poset の場合について、その hook の定義は Kawanaka[K] により与えられた (3 節参照)。その hook を適用することで一般の場合にも hook walk algorithm が構成でき、従って Greene-Nijenhuis-Wilf の方法が拡張できる。d-complete poset の hook 公式の hook walk algorithm による確率論的証明は本稿では概説に留められるが、詳細については [O] において記述さ

れている。

2 d-complete poset

以下、有限順序集合の事を poset と呼ぶ (連結とは限らない)。poset を図にした時は常に上、又は左に向かうほど大きくなるように表す。

Proctor によって定義された d-complete poset は Young 図形をその特殊なケースとして含む拡張された概念になっている。本節では基本的な言葉の準備と d-complete poset の定義を与え、d-complete poset の簡単な性質を説明する。この節の内容は基本的に Proctor[P2] に従う。

正方形を左端と右端が揃うように配置した図形の事を Young 図形と言う。Young 図形は各正方形を点として見て、隣り合う点同士を線で結んだ図形と見直すことができる。この図形を集合として各点を要素に持つと考え、上や左に向かうほど大きくなるように順序が入っていると考えると poset になる。この poset を Young 図形の poset 表示と呼ぶ。以下、ヤング図形は常にこの poset 表示を意味するとする。

P を任意の poset とする。$x,y \in P$ に対して x が y を cover する時、$x \gtrdot y$ と表す。P と P' が順序同型であるとき、$P \simeq P'$ と表す。P の極小元を P の **corner** と呼ぶ。P の順序が全順序である時 P は **chain** であると言う。$a,b \in P, a < b$ に対して $[a,b] := \{c \in P | a \leq c \leq b\}$ とする。P の部分 poset P' が任意の $x \in P'$ に対して「$y \geq x \ in \ P \Longrightarrow y \in P'$」なる条件を満たす時、$P'$ を P の **filter** と言う。

$k \geq 3$ に対して順序集合 $d_k(1)$ を次のように定める。

$$
\begin{gathered}
d_k(1) := \{w_1, w_2, \cdots, w_{k-2}, x, y, z_1, z_2, \cdots, z_{k-2}\} \\
w_1 < w_2 < \cdots < w_{k-2} \\
w_{k-2} < x < z_1 \\
w_{k-2} < y < z_1 \\
z_1 < z_2 < \cdots < z_{k-2}
\end{gathered}
$$

$d_k(1)$ の比較不能元 x,y を $d_k(1)$ の **side** と言う。又、$d_k^-(1) := d_k(1) - \{z_{k-2}\}$ とする。

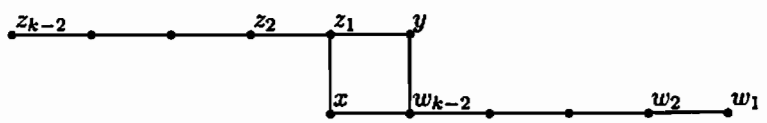


図 1: $d_k(1)$

$w,x,y,z \in P$ に対して

$$z \succ x,y \qquad x,y \succ w \ in P$$

なる条件が成り立つ時、$\{w,x,y,z\}$ を P 上の **diamond** と言う。

$a,b \in P$ に対して $[a,b] \simeq d_k(1)$ なる時、$[a,b]$ は P の d_k**-interval** であると言う。その時、b は P 上 d_k-interval の **neck** であると言い、a は P 上 d_k-interval の **tail** であると言う。又、a は b を neck に持つと言い、b は a を tail に持つと言う。$b \in P$ がある k に対して P 上 d_k-interval の neck である時、単に b を P 上の neck と呼ぶ。

$a,b \in P$ とする。$k \geq 4$ について $[a,b] \simeq d_k^-(1)$ の時 $[a,b]$ を P の d_k^--interval と呼ぶ。$w,x,y \in P$ に対して $x,y \succ w$ なる時、$\{w,x,y\}$ を d_3^--interval と呼ぶ。$k \geq 3$ について d_k-interval から最大元を除いたものは d_k^--interval である。

$k \geq 4, x,y \in P, [x,y] : d_k^-$-interval に対して

$$\exists z \in P \ s.t. \ y \prec z, [x,z] : d_k\text{-interval}$$

の時、$[x,y]$ を **complete** d_k^-**-interval** と呼ぶ。同様に $k=3$, $w,x,y \in P$, $\{w,x,y\} : d_3^-$-interval に対して

$$\exists z \in P \ s.t. \ \{w,x,y,z\} : d_3\text{-interval}$$

の時、$\{w,x,y\}$ を **complete** d_3^-**-interval** と呼ぶ。d_k^--interval であるが、complete d_k^--interval でないものを **incomplete** d_k^-**-interval** と呼ぶ。

$x,y,w,w' \in P, w \neq w'$ とする。$k \geq 4$ に対して

$$\begin{gathered} w \prec x, w' \prec x, \\ [x,y] : d_{k-1}\text{-interval}, \\ [w,y], [w',y] : d_k^-\text{-interval} \end{gathered}$$

のとき d_k^--interval $[w,y]$ と $[w',y]$ は **overlap** するという。又、

$$\begin{gathered} w \prec x, w \prec y, \\ w' \prec x, w' \prec y, \\ \{w,x,y\}, \{w',x,y\} : d_3^-\text{-interval} \end{gathered}$$

のとき d_3^--interval $\{w,x,y\}$ と $\{w',x,y\}$ は overlap するという。

P が次の条件を満たす時 P を d_3**-complete** と呼ぶ。

(1) incomplete d_3^--interval は存在しない。

(2) $\{w,x,y,z\}$:diamond ,z:最大元ならば $|\{v \in P | v \prec z\}| = 2$

(3) overlap する d_3^--interval は存在しない。

$k \geq 4$ に対して、P が次の条件を満たす時 P を **d_k-complete** と呼ぶ。
(1) incomplete d_k^--interval は存在しない。
(2) $[x,y]$:d_k-interval ならば $|\{v \in P | v \lessdot y\}| = 1$
(3) overlap する d_k^--interval は存在しない。

全ての $k \geq 3$ に対して d_k-complete である poset を **d-complete poset** と呼ぶ。

Young 図形 は d-complete poset である。又、後で説明するように Young 図形 の hook 公式と同様の公式が d-complete poset に対しても成り立つ。従って d-complete poset は Young 図形 のある種の自然な拡張になっていると言える。

任意の d-complete poset は'slant 既約' な成分の'slant 和' として分解され、各'slant 既約' 成分は 15 種類に分類されることが Proctor によって示された。従って任意の d-complete poset は完全に視覚的に把握できる。以下、その説明をする。

命題 2.1 d-complete poset の filter は d-complete poset である。

命題 2.2 連結な d-complete poset には最大元が存在する。

連結な poset T が次の条件を満たす時、T を **rooted tree** と呼ぶ。

$$\forall v \in T \text{ に対して } \{v' \in T | v' \geq v\} \text{ は } chain$$

又、いくつか (1 つでも良い) の rooted tree の (非連結) 和集合を **forest** と呼ぶ。forest、特に rooted tree は明らかに d-complete poset である。

以下 S を一般の d-complete poset とする。S の filter の内で、forest の形をした最大のものを S の **top tree** と言う。S の top tree の元で特に S 上の neck になっていないものを S の **acyclic element** と呼ぶ。

命題 2.3 d-complete poset S_1,S_2(S_2 は連結) と S_1 の acyclic element a,S_2 の最大元 b に対して、集合 $S_0 = S_1 \cup S_2$ に S_1, S_2 のもとの順序関係と新たな順序関係 $a > b$ によって生成される順序を入れると S_0 も d-complete poset である。

命題 2.3 によって構成された d-complete poset S_0 を d-complete poset S_1,S_2 の **slant 和** と呼び $S_1{}^a\backslash_b S_2$ と表す。d-complete poset が連結であり、2 つ以上の d-complete poset の slant 和 で表せない時 **slant 既約** であると言う。特に 1 つの点のみから成る集合 (ドットと呼ぶ) は slant 既約 d-complete poset

である。ドット以外の slant 既約 d-complete poset は全て少なくとも一つの diamond を含む。

命題 2.4 任意の 連結 d-complete poset は slant 既約 d-complete poset の slant 和 として一意的に表される。

連結 d-complete poset S が slant 既約 d-complete poset $S_1, S_2, \cdots, S_l$ の slant 和 で表せる時、$S_1, S_2, \cdots, S_l$ を S の **slant 既約成分**と呼ぶ。

定理 2.5 (slant 既約 d-complete poset の分類定理)(Proctor)
slant 既約 d-complete poset は 15 種類に分類される。

15 種類の slant 既約 d-complete poset の一覧はここでは与えない。その一覧は [P2] 及び [O] において記載されている。

3 hook

この節以降も特に注意が無ければ S は一般の d-complete poset を表すとする。hook とは S の各元に対応して定まるある条件を満たす S の部分集合である。Young 図形 の hook は広く知られているが d-complete poset への hook の定義の拡張は Kawanaka[K] により与えられた。本節ではこの hook の定義を与える。

S の filter S' $(S' \neq S)$ と $v \in S \backslash S'$ について $S' \cup \{v\}$ が S の filter なら v を S' の (S における)**outside corner** と呼ぶ。d-complete poset に hook を定義するためにいくつかのステップを踏む (図 5-8 において例示されている)。

(STEP1) 任意の d-complete poset S に対してその top tree を T と表す。$k := |T|$ とする。T の各元に 1〜k の値を重複無く割り当てる (どのように割り当てても良い)。この時、次のようにして S の全ての元に対して 1〜k を割り当てることができる。
(1) $S' := T$
(2-a) $S \backslash S' = \emptyset$ ならアルゴリズム終了
(2-b) $S \backslash S' \neq \emptyset$ なら S'の outside corner v を一つ取ってくる。(どのように取っても良い)
(3) v をtailに持つような S 上の neck v'が一意に存在し、それは S'の元である。この v'にラベルされている値を v にラベルする。
(4) $S' := S' \cup \{v\}$ として(2-a)へ

この対応付けによって $l : S \to \{1, 2, \cdots, k\}$ が定まる。

(STEP2) $\{1, 2, \cdots k\}$ で添え字付けられた不定元の集合 $A := \{\alpha_1, \alpha_2, \cdots, \alpha_k\}$ に対して $\mathbf{Z}(A) := \{z_1\alpha_1 + \cdots z_k\alpha_k | z_i \in \mathbf{Z}\ (1 \leq i \leq k)\}$ として $\mathbf{Z}$-線形空間を定め、$\forall i \in \{1, \cdots, k\}$ に対して $\mathbf{Z}(A)$ への $\mathbf{Z}$-線形写像 s_i を次の関係式から生成されるものとして定める。

$$s_i(\alpha_i) = -\alpha_i$$
$$s_i(\alpha_j) = \alpha_i + \alpha_j \quad (T \text{ 上で } i \text{ と } j \text{ が隣接している時})$$
$$s_i(\alpha_j) = \alpha_j \quad (T \text{ 上で } i \text{ と } j \text{ が隣接してない時})$$

$v_1, v_2, \cdots, v_n$ を $S = \{v_1, v_2, \cdots, v_n\}$ で $v_i > v_j \Rightarrow i < j$ なるように取る。$i_k := l(v_k)\ (1 \leq k \leq n)$ とする。各 s_{i_k} は $\mathbf{Z}(A)$ 上の $\mathbf{Z}$-線形写像である。以上の準備の下、S の hook の定義をする。

(STEP3) (d-complete poset における hook の定義)
$\forall v \in S$ に対し v の S 上の hook $H_S(v)$ を次のように定義する。S が明らかな時は単に H_v とも表す。
(1) $H_S(v) := \emptyset$
(2) k を $v = v_k$ なる k として定める。(一意に定まる)
(3) $\alpha := \alpha_{i_k}$
(4) $\alpha_{new} := s_{i_k}(\alpha)$
(5) $\alpha_{new} \neq \alpha$ なら $H_S(v) := H_S(v) \cup \{v_k\}$
(6) $\alpha := \alpha_{new}$
(7-a) k<n なら k:=k+1 として (4) へ
(7-b) k=n なら アルゴリズム終了

一見この定義が well-defined であることは自明ではないが実際には well-defined である。以下、hook に関していくつかの性質を述べる。

命題 3.1
(i) v' が v の hook に含まれる $\Longrightarrow v \geq v'$
(ii) $\forall v \in S$ に対して v 及び、v に cover される元は v の hook に入る。

系 v が S の *corner* $\Longleftrightarrow h_S(v) = 1$

命題 3.2 S の任意の filter S' 及び $v \in S'$ に対して

$$H_{S'}(v) = H_S(v) \cap S'$$

命題 3.3 v が S において neck でないなら $H_S(v) = \{v' \in S | v' \leq v\}$ である。

命題 3.2 の結果と合わせて、次の系が得られる。

系 1 $w < v$ *in* S に対して v が $[w,v]$ において neck でないなら $[w,v] \subset H_S(v)$ である。

また、(本当は少し説明が必要だが) 次の系も得られる。

系 2 $w < v$ *in* S に対して v と w が S の異なる slant 既約成分 S_1, S_2 に属するなら $S_2 \subset H_S(v)$ である。

従ってこの系により、slant 既約 d-complete poset の hook が分かっていれば、直ちに一般の d-complete poset の hook も導くことができることが分かる。

$\forall v \in S$ に対して $h_S(v) := |H_S(v)|$ を v の S 上の **hook length** と呼ぶ。S が明らかな時は単に h_v とも表す。

命題 3.4 $b \in S$ に対して
(i) b が S 上の neck でない時、

$$h_b = |\{v \in S | b \geq v\}|$$

(ii) b が S 上の neck である時、$[a,b]$ が d_k-interval となるような $a \in S$ が一意に存在するが、この時 x, y を $[a,b]$ の side とすると次の式が成り立つ。

$$h_b = h_x + h_y - h_a$$

(ii) は自明ではないが、(i) は命題 3.3 により明らか。命題 3.4 により、任意の d-complete poset に対して、その hook の形を構成しなくても帰納的に hook length だけを計算することができる。歴史的には d-complete poset に対しては hook よりも hook length が先に定義された (5 節参照)。

4 d-complete poset の hook 公式

本節において hook 公式 及び、任意の d-complete poset に対してその標準盤を等確率生成するアルゴリズムの説明をし、等確率性の証明を与えるために何を示すべきかを明らかにする。

以下、$n := |S|$ とする。全単射 $\sigma : S \to \{1, 2, \cdots, n\}$ が次の条件を満たす時、σ を S の標準盤と呼ぶ。

$$v, v' \in S \text{について} v \geq v' \Rightarrow \sigma(v) \leq \sigma(v')$$

この時、f_S を S の標準盤の総数とする。

定理 4.1 (hook 公式) 任意の d-complete poset S に対して次の式が成り立つ。

$$f_S = \frac{n!}{\prod_{v \in S} h_v} \qquad (n = |S|) \tag{1}$$

この定理の証明のために hook walk algorithm を定義する。このアルゴリズムが d-complete poset の標準盤を等確率で生成するアルゴリズムであることが後の定理から分かる。

定義 (hook walk algorithm)
(1) $i := 1$
(2) S の任意の元を $\frac{1}{n-i+1}$ の確率で取り出し、それを v_1 と表す。
(3) $j := 1$
(4-a) v_j が S の corner なら (5) へ
(4-b) v_j が S の corner でないなら、v_{j+1} を $H_{v_j} \backslash \{v_j\}$ の中から $\frac{1}{h_{v_j}-1}$ の確率で取り出す。$j := j + 1$ として (4-a) へ
(5) v_j に $n - i + 1$ をラベルする。$S := S \backslash \{v_j\}$
(6-a) $S = \emptyset$ ならアルゴリズム終了
(6-b) $S \neq \emptyset$ なら $i := i + 1$ として (2) へ

hook の定義により、このアルゴリズムは必ず有限試行で停止する。このアルゴリズムによって S の一つの標準盤を得る。S の任意の標準盤 σ に対して hook walk algorithm によって σ が選ばれる確率を $Prob_S(\sigma)$ で表す。

上のアルゴリズムの (1)-(5) の部分は S の一つの corner を選ぶ単独のアルゴリズムと見ることができる。このアルゴリズムを corner hook walk algorithm と呼ぶ。S の任意の corner ω に対して corner hook walk algorithm によって ω が選ばれる確率を $prob_S(\omega)$ と表す。

定理 4.2 S の任意の標準盤 σ に対して $Prob_S(\sigma)$ は σ に依存せず一様に次の式で与えられる。

$$Prob_S(\sigma) = \frac{\prod_{v \in S} h_v}{n!}$$

明らかにこの定理から定理 4.1 が導かれる。従って、定理 4.2 を示すことを考える。S の corner ω に対し $W_S(\omega)$ を

$$W_S(\omega) := \{v \in S | \omega \in H_S(v), v \neq \omega\}$$

と定め、S が明らかな時は W_ω とも表す。

定理 4.3 S の任意の filter S' とその任意の corner ω に対して次の式が成り立つ。

$$prob_{S'}(\omega) = \frac{1}{|S'|} \prod_{v \in W_{S'}(\omega)} (1 + \frac{1}{h_v - 1})$$

本稿では示さないが、比較的容易に次の主張が成り立つ。

主張 4.4 S に対して定理 4.3 が成り立つなら定理 4.2 も成り立つ。

従って、定理 4.3 を示せば S について hook 公式を示せたことになるが全ての d-complete poset に対して hook 公式を示したいので定理 4.3 を次のように修正する。

定理 4.3' 任意の d-complete poset S とその任意の corner ω に対して次の式が成り立つ。

$$prob_S(\omega) = \frac{1}{n} \prod_{v \in W_S(\omega)} (1 + \frac{1}{h_v - 1}) \tag{2}$$

これが言えれば全ての d-complete poset に対して hook 公式が言えたことになる。この (2) を S の corner ω における **corner hook 公式**と呼ぶ。又は単に (S, ω) の corner hook 公式と呼ぶ。

注意 S の任意の corner に対して corner hook 公式が示せても S の hook 公式が示せるわけではない。S の hook 公式を示すためには S の任意の filter S' の任意の corner に対して corner hook 公式を示さねばならない。

5 Peterson の定理

本節では d-complete poset に対応する概念である (simply-laced な)Weyl 群の dominant minuscule 元を定義し、d-complete poset の標準盤の総数が hook 公式 で与えられると言う定理と同値な Peterson の定理を紹介する。本節では d-complete poset を P で表す。

任意の Dynkin 図形 Γ を固定する。Γ に対応する Kac-Moody Lie 環を考える。以下、real root を単に root と呼ぶ。root α の height を $ht(\alpha)$ と表す。$\{\alpha_1, \cdots, \alpha_l\}$ を対応する simple system とし、$1 \leq i \leq l$ で s_i を α_i に対応する simple reflection とする。Φ^+ を positive root system、Φ^- を negative root system とし、$w \in W$ に対して $\Phi(w) := \Phi \cap w\Phi^-$ とする。よく知られるように w の最短表示の長さ $l(w) = |\Phi(w)|$ であり、$w = s_{i_n} s_{i_{n-1}} \cdots s_{i_1}$(最

短表示) に対して

$$\Phi(w) = \{s_{i_n} \cdots s_{i_{k+1}} \alpha_{i_k} | 1 \leq k \leq n\}$$

である。$\beta_k := s_{i_n} \cdots s_{i_{k+1}} \alpha_{i_k}$ とする。

$w = s_{i_n} s_{i_{n-1}} \cdots s_{i_1} \in W$ を最短表示とする。integral weight λ に対して

$$p = 1, 2, \cdots n \text{ で } < s_{i_{p-1}} \cdots s_{i_2} s_{i_1}(\lambda), \alpha_{i_p}^{\vee} >= 1$$

なる条件が成り立つ時、w を **λ-minuscule** と呼ぶ。この時 λ に対して $s_{i_1}, s_{i_2}, \cdots s_{i_n}$ の順に作用させていくと

$$\lambda \mapsto \lambda - \alpha_{i_1} \mapsto \lambda - \alpha_{i_1} - \alpha_{i_2} \mapsto \cdots \mapsto \lambda - \alpha_{i_1} - \alpha_{i_2} - \cdots - \alpha_{i_n}$$

である。$w \in W$ がある λ で λ-minuscule である時、w を **minuscule** と言い、特に、λ が dominant である時、dominant minuscule という。$w \in W$ に対して w の最短表示は一意的ではない。w の λ-minuscule 性は w の最短表示の仕方に依存する性質に見えるが実は $w = s_{i_1} \cdots s_{i_n} = s_{j_1} \cdots s_{j_n}$ に対して一方の表示に対して λ-minuscule ならもう一方の表示についても λ-minuscule である (cf.[St2],Prop.2.1)。

以上の準備の下、次の定理を紹介する。

定理 5.1 (Peterson) 任意の dominant minuscule 元 $w \in W$ に対して、$r(w)$ を w の最短表示の総数とすると次の式が成り立つ。

$$r(w) = \frac{l(w)!}{\prod_{\beta \in \Phi(w)} ht(\beta)}$$

Peterson の定理は 1989 年頃 Peterson によって証明されたと言われており、[St3] において引用されている。この定理は Proctor[P1][P2] と Stembridge[St2] の結果により、d-complete poset の hook 公式 と同値であることが言える。以下、それをおおまかに説明する。

任意の (simply-laced とは限らない) dominant minuscule 元 w に対して、$w = s_{i_n} \cdots s_{i_1}$ を最短表示とする。$P := \{v_1, v_2, \cdots, v_n\}$ に対して、P 上の順序 $\preceq$ を次のようにして定める。$v_p, v_q \in P$ が、$p < q$ かつ ($s_{i_p} s_{i_q} \neq s_{i_q} s_{i_p}$ 又は $i_p = i_q$) の時 $v_p \succ v_q$ とし、その transitive closure として関係 $\preceq$ を定めると、これは順序関係として well-defined である。この方法で得られる (ラベル付き)poset $(P, \preceq)$ を w の heap と呼ぶ (cf.[St2],sec.3)。この poset $(P, \preceq)$ は d-complete poset になる。この時、次のような対応関係が成り立つ。

$$\begin{aligned} l(w) &= |S| \\ r(w) &= f_S \\ \{ht(\beta)\}_{\beta \in \Phi(w)} &= \{h_S(v)\}_{v \in S} \end{aligned}$$

但し、最後の等式はβとνの間に上手く対応を付けると、一致するという意味である。これらの事から d-complete poset と hook 公式の同値性を導くことができる。

参考文献

[FRT] J.S.Frame, G. de B.Robinson, and R.M.Thrall, The hook graphs of the symmetric group, Canad.J.Math.6 (1954), 316-325.

[GNW] C.Greene, A.Nijenhuis, and H.S.Wilf, A probabilistic proof of a formula for the number of Young Tableaux of a given shape, Adv.in Math.31 (1979), 104-109.

[K] N.Kawanaka, Sato-Welter game and Kac-Moody Lie algebras, 数里解析研究所講究録 1190 (2001), 95-106.

[O] S.Okamura, 一般化された標準ヤング盤を等確率でランダムに生成するアルゴリズム, 大阪大学大学院理学研究科修士論文 (2003)

[P1] R.A.Proctor, Minuscule elements of Weyl groups, the numbers game, and d-complete posets, J.Algebra 213 (1999), 272-303.

[P2] R.A.Proctor, Dynkin diagram classification of λ-minuscule Bruhat lattices and of d-complete posets, J.Algebraic Combin.9 (1999), 61-94.

[Sa] B.E.Sagan, On selecting a random shifted Young tableau, J.Algorithms 1 (1980), 213-234.

[St1] J.R.Stembridge, On the fully commutative elements of Coxeter groups, J.Algebraic Combin.5 (1996), 353-385.

[St2] J.R.Stembridge, Minuscule Elements of Weyl Groups, J.Algebra 235 (2001), 722-743.

[St3] J.R.Stembridge, Quasi-Minuscule Quotients and Reduced Words for Reflections, J.Algebraic Combin.9 (2001), 275-293.

群環的代数
–群環の一般化について–

土井　幸雄
岡山大学・教育学部

1996年，フィンランドの数学者 Koppinen は一つの有限次元ベクトル空間に同時に2種類のフロベニウス代数構造を入れた概念 double Frobenius algebra を導入しました [K]．代数的組合せ論へのホップ代数的アプローチとしてはたぶん最初の論文だったのではないでしょうか．面白い発想ですが，その複雑さ・難解さからいまだに後継者が現れておりません．本人だけがその後5編ほど communication in algebra に関連論文を発表し現在に至っています．一方3年前，私は竹内氏と共同で bi-Frobenius algebra なる概念を導入しました [DT]．有限次元ホップ代数の自然な一般化で，ある対応により Koppinen の double Frbenius algebra とほぼ一致しています．そして最近この中に group-like algebra ＜日本語で群環的代数＞と私が呼んでいる面白いクラスが見つかりました [D3]．有限群の群環の一般化で，Kawada's character algebra の非可換バージョンのようなものです．本報告では，このような概念を考えるに到った経緯を中心に，北大での講演に沿った解説を行います．時間の関係で講演中省いた部分の解説も加えてあります．

はじめに　G を有限群，k を一般の体とする．k 上の群環 kG は次の性質をもつ：
線形写像 $\phi : kG \to k$ を $\phi(g) = \delta_{1,g}$ で定義すると

$$\sum_{g \in G} \phi(gx)g = x^{-1}$$

が任意の元 $x \in G$ に対して成り立つ．この性質に注目して群環的代数の概念が得られる．

定義1　A を体 k 上の有限次元 (結合的) 代数とし，基礎体 k への代数射 $\varepsilon : A \to k$ と A の k 基底 $\mathbf{B} = \{b_0 = 1, b_1, \ldots, b_d\}$ および involution $S : \mathbf{B} \to \mathbf{B}, b_i \mapsto b_{i^*}$ $(i^{**} = i)$ が与えられているとする．次の3条件をみたすとき，4つ組 $(A, \varepsilon, \mathbf{B}, S)$ を**群環的代数** (group-like algebra) と呼ぶ．
(G1) $\varepsilon(b_{i^*}) = \varepsilon(b_i) \neq 0$, $\forall i$,
(G2) $p_{ij}^k = p_{j^*i^*}^{k^*}$, $\forall i, j, k$, ここで p_{ij}^k は $\mathbf{B}$ に関する構造定数を表す．
(G3) $p_{ij}^0 = \delta_{ij^*}\varepsilon(b_i)$, $\forall i, j$.

注意 1　上の S を A から A への線形写像に拡張したとき，条件 (G2) は

$$S(xy) = S(y)S(x), \quad (x,\ y \in A)$$

を意味する．よって $S = \mathrm{id}$ なら（この場合 A は**対称的**であるという），A の積は可換になる．

また条件 (G3) は

$$\sum_{i=0}^{d} \frac{1}{\varepsilon(b_i)} \phi(b_i x) b_i = S(x), \quad (x \in A)$$

と同値であることが容易に確かめられる，ただし線形写像 $\phi : A \to k$ は群環をまねて $\phi(b_i) = \delta_{0,i}$ で定義する．この観察より，群環 kG は

$$\varepsilon(g) = 1,\ S(g) = g^{-1},\ (g \in G),\ \mathbf{B} = G$$

として群環的代数になる．群環でない群環的代数の例はあとで述べる．

注意 2　群環的代数 $(A, \varepsilon, \mathbf{B}, S)$ には

$$\Delta(b_i) = \frac{1}{\varepsilon(b_i)} b_i \otimes b_i \quad (i = 0, 1, \ldots, d)$$

と定義して余代数になる．余単位射はすでに与えられた ε を用いる．しかし 余積 $\Delta : A \to A \otimes A$ が乗法的とは限らないのでホップ代数にはならない．また写像 $S : A \to A$ もアンチポード条件をみたしていない．しかしながら

$$t := b_0 + b_1 + \cdots + b_d$$

とおくと，条件 (G3) は

$$(*) \qquad \sum \phi(t_{(1)}x) t_{(2)} = S(x), \quad (x \in A)$$

と表され，次で定義するバイフロベニウス代数の仲間に入ることがわかる．

定義 2　H を体 k 上の有限次元代数かつ余代数とし，余積を $\Delta : H \to H \otimes H$, 余単位射を $\varepsilon : H \to k$ で表す．双対空間 $H^* = \mathrm{Hom}(H, k)$ の元 ϕ と H の元 t に対し，写像 S を上の $(*)$ で定義する．次の6条件をみたすとき，4つ組 (H, ϕ, t, S) は**バイフロベニウス代数** (bi-Frobenius algebra) であると呼ぶ．

(BF1) $\varepsilon(hh') = \varepsilon(h)\varepsilon(h')$, $(\forall h, h' \in H)$ and $\varepsilon(1) = 1$.
(BF2) $\Delta(1) = 1 \otimes 1$.
(BF3) $\{\phi \leftharpoonup h \mid h \in H\} = H^*$, where $(\phi \leftharpoonup h)(h') := \phi(hh')$.
(BF4) $\{t \leftharpoonup f \mid f \in H^*\} = H$, where $t \leftharpoonup f := \sum f(t_{(1)}) t_{(2)}$.
(BF5) $S(hh') = S(h')S(h)$, $S(1) = 1$.
(BF6) $\Delta(S(h)) = \sum S(h_{(2)}) \otimes S(h_{(1)})$, $\varepsilon(S(h)) = \varepsilon(h)$.

注意 3　H^* は次の作用 $\rightharpoonup$, $\leftharpoonup$ で両側 H 加群になる：

$$(h \rightharpoonup f)(x) = f(xh),\ (f \leftharpoonup h)(x) = f(hx)$$

条件 (BF3) は右 H 加群射

$$\theta : H \to H^*,\ \theta(h) = \phi \leftharpoonup h$$

が全射，したがって全単射であることをいっている（同次元だから）．つまり (BF3) は (H, ϕ) がフロベニウス代数という条件である．線形代数より

$$\theta' : H \to H^*,\ \theta'(h) = h \rightharpoonup \phi$$

は左 H 加群同型射となる．同型射のずれ $\theta'^{-1} \circ \theta$ がいわゆる中山自己同型と呼ばれるものである．

条件 (BF4) は (BF3) の双対的条件である．H^* は H の余代数構造から引き起こされる代数の構造をもつ．そして H は次の作用で両側 H^* 加群になる：

$$f \rightharpoonup h = \sum h_{(1)} f(h_{(2)}),\ h \leftharpoonup f = \sum f(h_{(1)}) h_{(2)}$$

条件 (BF4) は

$$\kappa : H^* \to H,\ \kappa(f) = t \leftharpoonup f$$

が右 H^* 加群同型射ということ．このとき，組 (H, t) がフロベニウス余代数であるという．

$$\kappa' : H^* \to H,\ \kappa'(f) = f \rightharpoonup t$$

は左 H^* 加群同型射となる．このように H と H^* の間には**フーリエ変換**とでも呼ぶべき 4 種類の対応がある．

代数 H^* の積をフーリエ変換 θ で H 上に引き戻すことにより，新しい積 $\star$ が入り具体的には次のように表せる．

$$x \star y = \sum \phi(y_{(1)} \overline{S}(x)) y_{(2)}$$

アダマール積と呼ぶ．この積のもと，組 (H, ε) はフロベニウス代数で，t が単位元となる．古い積との間に次の関係がなりたつ．

$$\varepsilon(S\mathcal{N}(x) \star y) = \phi(xy), \quad \forall x,\ y \in H$$

Koppinen の double Frobenius algebra はこの等式から出発したものである．群環的代数の場合，アダマール積は

$$b_j \star b_i = \delta_{ij} b_i$$

となり，従来のものと一致する．

結果 1　$S = \kappa \circ \theta'$ がなりたつ．実際，

$$\begin{aligned}(\kappa \circ \theta')(h) &= \kappa(h \rightharpoonup \phi) \\ &= t \leftharpoonup (h \rightharpoonup \phi) \\ &= \sum (h \rightharpoonup \phi)(t_{(1)}) t_{(2)} \\ &= \sum \phi(t_{(1)} h) t_{(2)} = S(h).\end{aligned}$$

とくに S は全単射となる．逆写像を $\overline{S}$ で表すと，S の定義から

$$h = \sum \overline{S}(t_{(2)})\phi(t_{(1)}h)$$

を得る．つまり $\{\overline{S}(t_{(2)}), t_{(1)}\}$ がフロベニウス代数 (H, ϕ) の2重基底を与える．よってフロベニウス代数のスタンダードな議論 (cf. [D2]) から

$$\sum h\overline{S}(t_{(2)}) \otimes t_{(1)} = \sum \overline{S}(t_{(2)}) \otimes t_{(1)}h$$

が任意の $h \in H$ でなりたつ．よって，次の元

$$v := \sum \overline{S}(t_{(2)})t_{(1)}$$

は H の中心に属す．v が可逆元なら，$\sum v^{-1}\overline{S}(t_{(2)}) \otimes t_{(1)}$ はいわゆる $H \otimes H$ の separable idempotent となるから，H は分離的代数で，とくに半単純である（マシュケの定理の一般化）．さらに $S^2 = id$ かつ k 代数閉体のとき，次の内積のもとで H の既約指標についての直交関係が成立する：

$$(**) \qquad (f|g) = \sum f(v^{-1}S(t_{(2)}))g(t_{(1)}),\ f,\ g \in H^*$$

結果2　等式 $S = \kappa \circ \theta'$ から，S が全単射なら κ, θ' も全単射になる．よってバイフロベニウス代数の定義の2条件 (BF3),(BF4) は条件 "S **が全単射**" に置き換えられる．これは候補の代数がバイフロベニウスかどうかの判定に有効に働く．例えば群環的代数 $(A, \varepsilon, \mathbf{B}, S)$ の S は全単射だから，注意1の ϕ と $t = b_0 + b_1 + \cdots + b_d$ でバイフロベニウスになる（(BF3,4) のチェックは不要）．この場合 $S^2 = id$ だから $\overline{S} = S$ で，中心元 v は

$$v = 1 + \frac{1}{\varepsilon(b_1)}b_{1^*}b_1 + \cdots + \frac{1}{\varepsilon(b_d)}b_{d^*}b_d$$

となる．内積 $(**)$ は

$$(f|g) = \sum_{i=0}^{d} \frac{1}{\varepsilon(b_i)} f(v^{-1}b_{i^*})g(b_i)$$

となる．

バイフロベニウスの例　有限次元ホップ代数 H はバイフロベニウスである．実際，H^* の右積分 ϕ と H の右積分 t の対で $\phi(t) = 1$ となるものを選ぶ．このとき，H のアンチポード S に対し以前の $(*)$ がなりたつことが証明できる．よく知られているように S は全単射で (BF5,6) をみたす．よって上の判定からバイフロベニウスになる．ホップ代数でもなく群環的代数でもない例として次がある．

1変数多項式環 $k[X]$ のイデアル (X^4) を考え，$H = k[X]/(X^4)$ とおく．H に次の余代数構造を入れる：
$\Delta(1) = 1 \otimes 1$, $\Delta(x) = 1 \otimes x + x \otimes 1$,
$\Delta(x^2) = 1 \otimes x^2 + x \otimes x + x^2 \otimes 1$,
$\Delta(x^3) = 1 \otimes x^3 + x \otimes x^2 + x^2 \otimes x + x^3 \otimes 1$,

$\varepsilon(1)=1,\ \varepsilon(x)=\varepsilon(x^2)=\varepsilon(x^3)=0.$
このとき，$\phi(x^m)=\delta_{m,3},\ t:=x^3,\ S=id$ でバイフロベニウス．

結果 3　(H,ϕ,t,S) を一般のバイフロベニウス代数とする．等式 $S(h)=\sum\phi(t_{(1)}h)t_{(2)}$ に ε をほどこして

$$\varepsilon(h)=\phi(th),\ \forall h\in H$$

を得る．フーリエ変換 θ を用いてこれを H 内に引き戻すと

$$th=t\varepsilon(h),\ \forall h\in H$$

を得る．つまり，元 t は右積分となる．バイフロベニウス代数の最も重要な性質である．一般に左積分条件

$$ht=\varepsilon(h)t,\ \forall h\in H$$

はみたさない．しかし，例えば群環的代数のように $S(t)=t$ なら，条件 (BF5) から左積分にもなる．群環的代数において $t=b_0+b_1+\cdots+b_d$ が右積分かつ左積分であることを構造定数を用いて表現すれば

$$(G4)\qquad p_{0i}^k+p_{1i}^k+\cdots+p_{di}^k=\varepsilon(b_i),$$

$$(G4')\qquad p_{i0}^k+p_{i1}^k+\cdots+p_{id}^k=\varepsilon(b_i).$$

双対的議論から ϕ は

$$\sum\phi(h_{(1)})h_{(2)}=\phi(h)1,\ \forall h\in H$$

なる性質，すなわち H^* の右積分となる．群環的代数の場合この性質は自明となる．

群環的代数の例　2 次元群環的代数のは乗積表は次の形に限る．理由は積分条件 (G4) からただち．

$A_q(2)$	1	b
1	1	b
b	b	$q+(q-1)b$

$\varepsilon(b)=q(\neq 0)\in k$ で $S=id$. $v:=v(A_q(2))=2+\frac{q-1}{q}b$ である．$\varepsilon(t)=1+q\neq 0$ なら v は可逆 $(v^{-1}=\frac{(q^2+1)-(q-1)b}{(q+1)^2})$ で半単純．$q=-1$ なら半単純でない．$A_1(2)$ は位数 2 の巡回群の群環である．

$\phi((b_ib_j)b_k)$ と $\phi(b_i(b_jb_k))$ を別々に計算して両辺を比較し (G2) を加味することで次の等式を得る．

$$(G5)\qquad p_{ij}^k\varepsilon(b_k)=p_{kj^*}^i\varepsilon(b_i)$$

これが 3 次元群環的代数の決定に有効に働く．

3 次元非対称 $(S\neq id)$ の場合は次の形 (ただし $\mathrm{char}(k)\neq 2$ とする)：

$A_q(3)$	1	b_1	b_2
1	1	b_1	b_2
b_1	b_1	$\frac{q-1}{2}b_1+\frac{q+1}{2}b_2$	$q+\frac{q-1}{2}(b_1+b_2)$
b_2	b_2	$q+\frac{q-1}{2}(b_1+b_2)$	$\frac{q+1}{2}b_1+\frac{q-1}{2}b_2$

ただし，$S(b_1)=b_2$ and $q:=\varepsilon(b_1)=\varepsilon(b_2)\neq 0$. $v=v(A_q(3))=3+\frac{q-1}{q}(b_1+b_2)$.
もし $\varepsilon(t)=2q+1\neq 0$ なら v は可逆で

$$v^{-1}=\frac{2q^2+1+(1-q)(b_1+b_2)}{(2q+1)^2}.$$

Proof. $S\neq id$ だから $S(b_1)=b_2$ である．(G1), (G3) より

$$q:=\varepsilon(b_1)=\varepsilon(b_2)\neq 0,\ p_{11}^0=p_{22}^0=0,\ p_{12}^0=p_{21}^0=q$$

また (G2) より

$$p_{11}^1=p_{22}^2,\ p_{12}^1=p_{12}^2,\ p_{21}^1=p_{21}^2,\ p_{22}^1=p_{11}^2$$

さらに (G5) より

$$p_{12}^2=p_{21}^1,\ p_{11}^1=p_{12}^1$$

したがって積は可換で，乗積表は次の形：

	1	b_1	b_2
1	1	b_1	b_2
b_1	b_1	$\alpha b_1+\beta b_2$	$q+\alpha(b_1+b_2)$
b_2	b_2	$q+\alpha(b_1+b_2)$	$\beta b_1+\alpha b_2$

次に積分条件 (G4) から $q=1+2\alpha=\alpha+\beta$. よって $\mathrm{char}(k)\neq 2$ なら $\alpha=\frac{q-1}{2}$, $\beta=\frac{q+1}{2}$, $\mathrm{char}(k)=2$ なら $q=1$, $\beta=1+\alpha$ となり上の表を得る．$(b_1b_1)b_2=b_1(b_1b_2)$, $(b_1b_2)b_2=b_1(b_2b_2)$ は直接計算で確かめられる．他のケースは可換性より明らか．したがってこの積は結合律をみたす． □

3 次元対称群環的代数は次の形に限る：

$A_{p,q}^{\beta}(3)$	1	b_1	b_2
1	1	b_1	b_2
b_1	b_1	$p+(p-1-\beta q)b_1+\beta p b_2$	$\beta q b_1+(p-\beta p)b_2$
b_2	b_2	$\beta q b_1+(p-\beta p)b_2$	$q+(q-\beta q)b_1+(q-1-p+\beta p)b_2$

ただし，$\varepsilon(b_1)=p$ and $\varepsilon(b_2)=q$ and $\beta\in k$. $v(A_{p,q}^{\beta}(3))$ は

$$1+\frac{b_1b_1}{p}+\frac{b_2b_2}{q}=3+\frac{2p-1-\beta(p+q)}{p}b_1+\frac{q-p-1+\beta(p+q)}{q}b_2.$$

これが可逆元なる条件は次の値が 0 でないこと：

$$\frac{(p+q+1)^2}{pq}\cdot\{(\beta^2-\beta)(p+q)^2+\beta(q+1)^2+(1-\beta)(p+1)^2\}$$

例　正 6 角形の頂点の集合をその距離で 4 分類してできるアソシエーション・スキームを考える．距離が最長の頂点対を b_1, 中間距離の

頂点対を b_2, 隣同士の頂点対を b_3 とすると，その隣接代数の乗積表は次の通り．

	1	b_1	b_2	b_3
1	1	b_1	b_2	b_3
b_1	b_1	1	b_3	b_2
b_2	b_2	b_3	$2+b_2$	$2b_1+b_3$
b_3	b_3	b_2	$2b_1+b_3$	$2+b_2$

これは $A_1(2)$ と $A_2(2)$ のテンサー積と一致する．また**立方体**の頂点の集合をやはりその距離で 4 分類してできるアソシエーション・スキームがある．その隣接代数は $A_1(2)$ と $A_3(2)$ のテンサー積である．Petersen **グラフ**の 10 個の頂点をその距離で 3 分類（長さ 2 以上は一まとめにする）してできるアソシエーション・スキームの隣接代数は 3 次元対称群環的代数 $A_{3,6}^{1/3}(3)$ である．Shrikhande **グラフ**から同様にして作られたアソシエーション・スキームの隣接代数は $A_{6,9}^{1/3}(3)$ である．

注意　4 次元の構造は完全な決定まで到ってない．しかし可換なものしかないことはわかっている．5 次元については，$S=(14)(23)$ タイプは可換になる．$S=(14)$ タイプについては可換なものしかないかどうか不明．

次の例は 6 次元非可換な例である．

例　$\mathrm{char}(k)\neq 2$, $q\neq 0\in k$ とする．

	1	b_1	b_2	b_3	b_4	b_5
1	1	b_1	b_2	b_3	b_4	b_5
b_1	b_1	$\frac{q-1}{2}b_1+\frac{q+1}{2}b_2$	$q+\frac{q-1}{2}(b_1+b_2)$	b_5	$qb_3+\frac{q-1}{2}(b_4+b_5)$	$\frac{q+1}{2}b_4+\frac{q-1}{2}b_5$
b_2	b_2	$q+\frac{q-1}{2}(b_1+b_2)$	$\frac{q+1}{2}b_1+\frac{q-1}{2}b_2$	b_4	$\frac{q-1}{2}b_4+\frac{q+1}{2}b_5$	$qb_3+\frac{q-1}{2}(b_4+b_5)$
b_3	b_3	b_4	b_5	1	b_1	b_2
b_4	b_4	$\frac{q-1}{2}b_4+\frac{q+1}{2}b_5$	$qb_3+\frac{q-1}{2}(b_4+b_5)$	b_2	$q+\frac{q-1}{2}(b_1+b_2)$	$\frac{q+1}{2}b_1+\frac{q-1}{2}b_2$
b_5	b_5	$qb_3+\frac{q-1}{2}(b_4+b_5)$	$\frac{q+1}{2}b_4+\frac{q-1}{2}b_5$	b_1	$\frac{q-1}{2}b_1+\frac{q+1}{2}b_2$	$q+\frac{q-1}{2}(b_1+b_2)$

ただし，$S(b_1)=b_2$, $S(b_i)=b_i$ $(i=3,4,5)$, $\varepsilon(b_j)=q$ $(j=1,2,4,5)$, $\varepsilon(b_3)=1$.

$$\varepsilon(t)=4q+2,\ v=6+\frac{2q-2}{q}(b_1+b_2)$$

であり，$4q+2\neq 0$ なら v は可逆で

$$v^{-1}=\frac{1}{2(2q+1)^2}\{(2q^2+1)-(q-1)(b_1+b_2)\}$$

中心 Z は群環的代数で $A_{2q,2q+1}^{0}(3)$ と一致する．

$q=1$ のとき，3 次対称群 S_3 の群環になる．($b_1=(123)$, $b_2=(132)$, $b_3=(23)$, $b_4=(13)$, $b_5=(12)$ とせよ．)

参考文献

[BI] E. Bannai and T. Ito, "Algebraic Combinatorics I: Association Schemes", Benjamin-Cummings, Menlo Park CA, 1984.

[D1] Y. Doi, *Substructures of bi-Frobenius algebras*, J. Algebra 256 (2002), 568-582.

[D2] Y. Doi, *Group-like algebras*, Proceedings of the 35th Symposium on Ring Theory and Representation Theory (Okayama, Japan), 53-58.

[D3] Y. Doi, *Bi-Frobenius algebras and group-like algebras*, preprint.

[DT] Y. Doi and M. Takeuchi, *BiFrobenius algebras*, Contemporary Mathematics 267 (2000) "New trends in Hopf algebra theory", 67-97.

[K] M. Koppinen, *On algebras with two multiplications, including Hopf algebras and Bose-Mesner algebras*, J. Algebra 182 (1996), 256-273.

[Z] P.-H. Zieschang, "An Algebraic Approach to Association Schemes", (Lecture Notes in Mathematics; 1628), Springer, 1996.

平面関数と有限体上の単項式について

近畿大学・理工学部・理学科
中川 暢夫

1. 平面関数

「**Definition 1**」 G と H を位数 n の有限群とし、f を G から H への関数とする。各 $u \in G$ に対し、$f_u(x) = f(ux)f(x)^{-1}$ $(x \in G)$ と定義する。$u \neq 1$ なる任意の u に対して、f_u が bijection であるとき、f を G から H への次数 n の平面関数 (planar function) という。
G から H への次数 n の平面関数 f より、群 $G \times H$ が全点の集合上に正則に作用するような、位数 n のアファイン平面が構成される。

「**Theorem 1**」(Dembowski and Ostrom)
G から H への次数 n の平面関数 f があれば、n は奇数である。

「**Theorem 2**」(Blokuis,Jungnickel and Schmidt)
可換群 G から可換群 H への次数 n の平面関数 f があれば、n は素数巾である。

この **Theorem 2** は次の「条件付き有限射影平面の素数巾予想」の解決に関わる定理の系として得られる。

「**Theorem 3**」(Blokuis,Jungnickel,Schmidt and Ganley)
位数 n の射影平面が、位数 n^2 の可換な自己同型群をもつならば、n は素数巾である。
(n が偶数の時は Ganley により、n が奇数の時は Blokuis,Jungnickel,Schmidt により証明された。)
n が奇数のときのこの定理の証明は、群環をつくり、その中で差集合からでる式を巧妙に評価して、n が奇数で素数巾でないという仮定から矛盾を導く。

「**Theorem 4**」(Hiramine,Gluck, Ronayi and Szonyi)
次数が奇素数 p の平面関数は有限素体 $\mathbf{F}_p$ 上の 2 次式 $f(x) = ax^2 + bx + c$ $(a \neq 0)$ である。

「Theorem 5」(Nakagawa)
G と H を位数 p^n の可換 p 群とし、G から H への平面関数 f が存在すると仮定せよ。このとき、n が奇数ならば、$exp(H) \leq p^{\frac{n+1}{2}}$ となり、また n が偶数ならば、$exp(H) \leq p^{\frac{n}{2}}$ となる。更に、n が 2 以上ならば、G は巡回群ではない。

今までに知られている平面関数の例は全て、G と H が基本可換 p 群の場合である。

例 1

$$\mathbf{F}_{p^n} \longrightarrow \mathbf{F}_{p^n} : \quad x \longmapsto x^2$$

(この平面関数にはデザルグ平面が対応する。)

例 2

$$\mathbf{F}_{3^n} \longrightarrow \mathbf{F}_{3^n} : \quad x \longmapsto x^{\frac{3^a+1}{2}} \quad ((a, 2n) = 1)$$

($1 < a < 2n$ のとき、この平面関数には non-translation planes が対応する。)

例 3

$$\mathbf{F}_{3^4} \longrightarrow \mathbf{F}_{3^4} : \quad x \longmapsto a(x^6 + x^{30} + x^{54}) - x^{10} - x^{18} \quad (a^2 = -1)$$

(この平面関数にはデザルグでない semi-field planes が対応する。)

2. 有限体上の単項式である平面関数

基本可換群型の平面関数は有限体上の多項式になることが示されるが、このなかで特に単項式の場合を考えていく。

「Conjecture 1」
$p \geq 5$ とする。$\mathbf{F}_{p^n}$ 上の単項式 $f(x) = x^d$ が平面関数ならば、$d = 2p^i \ (0 \leq i \leq n-1)$ である。
($p = 3$ の場合は上記の例 2 がこの予想の形をはずれる平面関数である。)

「Theorem 6」(Nakagawa)
$\mathbf{F}_{p^2}$ 上の単項式 $f(x)=x^d$ が平面関数ならば、

$$(1)\quad d=(p-1)\ell+2\ \ (\ell=1,2,\cdots,p-1)$$

$$(2)\quad (d,p^2-1)=2$$

「Theorem 7」(Nakagawa)
$d=ip+j\ \ (0\leq i,j\leq p-1)$ とおく。$d>\frac{p^2-1}{2}$, $0\leq i\leq\frac{p-1}{2}$ 且つ $0\leq j\leq\frac{p-1}{2}$ ならば、$\mathbf{F}_{p^2}$ 上の単項式 $f(x)=x^d$ は平面関数でない。
(この定理より、とりうる全ての d の値のうち、$\frac{1}{4}$ 程度の d に対して $f(x)=x^d$ は平面関数になり得ない事が解る。)

「Definition 2」$\omega=e^{\frac{2\pi i}{p}}$ とおく。

$$\mathbf{F}_p^n\longrightarrow\mathbf{F}_p,\quad x\longmapsto f(x)$$

に対し、$F(x)=\omega^{f(x)}$ とする。このとき、

$$\hat{F}(a)=\sum_{x\in\mathbf{F}_p^n}F(x)\omega^{(a,x)}\qquad(a\in\mathbf{F}_p^n)$$

を F のフーリエ係数とよぶ。(ここで、(a,x) は a と x の内積を表す。)
さて、任意の $a\in\mathbf{F}_p^n$ に対し、$|\hat{F}(a)|$ =(定数) となるとき、f を **bent function** とよぶ。

例 4 $\mathbf{F}_p$ 上の非退化2次形式は **bent function** である。

「Theorem 8」(Nakagawa) $p\neq 2$ とする。

$$\mathbf{F}_p^n\longrightarrow\mathbf{F}_p^n,\quad x\longmapsto f(x)=(f_1(x),f_2(x),\cdots,f_n(x))$$

が平面関数となる必要十分条件は任意の $a_1,a_2,\cdots,a_n\ \ ((a_1,a_2,\cdots,a_n)\neq(0.0,\cdots,0))$ に対し、

$$a_1f_1+a_2f_2+\cdots+a_nf_n$$

が **bent function** になることである。

ここで、次の問題を考えてみたい。

「**Problem 1**」 どのような m に対し、$\mathbf{F}_p$ 上の m 次形式が **bent function** になるか。2 変数の m 次形式について次のような結果を得た。

「**Theorem 9**」(Nakagawa)

$$f(x,y) = a_0x^m + a_1x^{m-1}y + a_2x^{m-2}y^2 + \cdots + a_my^m$$

を $\mathbf{F}_p$ $(p \neq 2)$ 上の m 次形式とする。

$$\phi_f(t) = a_0 + a_1t + \cdots + a_mt^m$$

とおく。$|\{\, t \mid \phi_f(t) = 0\}| \neq 1$, $|\{\, t \mid \phi_f(t) = 0\}| \neq 2$、且つ $(m, p-1) \neq 2$ とする。このとき、f は **bent function** ではない。特に、2 変数 3 次形式は **bent function** でない。2 次形式でない **bent function** として、次のような例がある。

例 5 $(p-1,3) = 1$, $b \neq 0$ とする。$\mathbf{F}_p$ 上の 4 次形式

$$f(x,y) = ax^4 + bx^3y$$

は **bent function** である。

3. 有限体上の単項式からくる差方程式の解の個数の挙動

有限体 $\mathbf{F}_{p^n}$ 上の方程式 $(x+1)^d - x^d = b$ を考える。

$$N_d(b) = |\{\, x \mid (x+1)^d - x^d = b \,\}|$$

とし、$N_d = \max_{b \in \mathbf{F}_{p^n}} \mathrm{N_d(b)}$ とおく。$f(x) = x^d$ が $\mathbf{F}_{p^n}$ 上の平面関数になることの必要十分条件が $N_d = 1$ であることは見やすい。N_d が $1, 2, 3$ などと小さい値をとる関数 $f(x) = x^d$ をみつけることは暗号理論の観点からも意味のあることらしい。(参考文献 [5] 参照。)
そこで、b が $\mathbf{F}_{p^n}$ の元を走る時、特殊な d について、方程式 $(x+1)^d - x^d = b$ の解の挙動に関するいくつかの結果をかいてみる。

例 6(Kasami power functions)

$$\mathbf{F}_{2^n} \longrightarrow \mathbf{F}_{2^n}, \quad x \longmapsto x^{2^{2k}-2^k+1} \quad (k,n) = 1$$

において、$d = 2^{2k} - 2^k + 1$ とすると、$x \longmapsto (x+1)^d - x^d$ は $\mathbf{F}_{2^n}$ 上 2 : 1 写像である。特に $N_d = 2$.

「**Theorem 10**」(Nakagawa)
χ を $\mathbf{F}_{p^n}$ 上の位数 2 の指標とする。また、$d = \frac{p^n-1}{2} + 1$ とする。$\mathbf{F}_{p^n}$ の関数 $f(x) = x^d$ において、
(1):$p^n \equiv 3 \pmod 4$ の場合、

$$N_d(1) = n_d(-1) = \frac{p^n+1}{4},$$

$$N_d(b) = 1 \text{ if } \chi(\frac{-1-b}{2}) = 1 \text{ and } \chi(\frac{1-b}{2}) = 1,$$

$$N_d(b) = 1 \text{ if } \chi(\frac{1+b}{2}) = 1 \text{ and } \chi(\frac{b-1}{2}) = -1,$$

$$N_d(b) = 0 \text{ for other } b \in \mathbf{F}_{p^n}.$$

(2):$p^n \equiv 1 \pmod 4$ の場合、

$$N_d(1) = \frac{p^n+3}{4}, \text{ and } N_d(-1) = \frac{p^n-1}{4},$$

$$N_d(b) = 2 \text{ if } \chi(\frac{1+b}{2}) = 1 \text{ or } \chi(\frac{1-b}{2}) = 1,$$

$$N_d(b) = 0 \text{ for other } b \in \mathbf{F}_{p^n}.$$

「**Theorem 11**」(Hellseth and Sundberg)
$d = \frac{p^n-1}{2} + 2$ とする。$\mathbf{F}_{p^n}$ の関数 $f(x) = x^d$ において、

$$N_d = 1 \text{ if } p = 3 \text{ and } n \text{ is even},$$

$$N_d = 3 \text{ if } p \neq 3 \text{ and } p^n \equiv \mod 4,$$

$$N_d = 4 \text{ otherwise.}$$

最後に **Theorem 11** での証明で必要となる **Weil sum** についての深い結果を述べて終わりにしたい。

「**Theorem 12**」(Weil)
$\phi \in \mathrm{Char}(\mathbf{F}_{p^n}^*)$, $|\phi| = m > 1$ とする。$f(x)$ を $\mathbf{F}_{p^n}$ 上の次数 1 以上の monic な多項式で、

どの多項式の m 乗でもないとする。$\mathbf{F}_{p^n}$ の十分大きな拡大体の中で、$f(x)=0$ の異なる解の個数は丁度 d とする。このとき、

$$\sum_{\gamma\in\mathbf{F}_{p^n}}\phi(f(\gamma))=-(\omega_1+\omega_2+\cdots+\omega_{d-1})$$

となる。ここで、$|\omega_i|=p^{\frac{n}{2}}\ (1\leq i\leq d-1)$.

Theorem 12 は指標 ϕ に対し、k 個の、1 の p^n-1 乗根 $\zeta_1,\zeta_2,\cdots,\zeta_k$ と k 個の、$\mathbf{F}_{p^n}$ の元 $a_1,a_2,\cdots,a_k$ を与える時、k の値が p^n の値に比べて、比較的小さいならば、

$$\phi(x+a_i)=\zeta_i\quad(1\leq i\leq k)$$

となる元 x の存在を保証する。

参考文献

(1) A.Blokhus,D.Jungnickel and B.Schmidt, Proof of the prime power conjecture for projective planes of order n with abelian collineation groups, to appear in Proc. AMS.

(2) P.Dembowski and T.G.Ostrom, Planes of order n with collineation groups of order n^2 , Math. Zeitschrift 99(1967),53-75.

(3) M.J.Ganley, On a paper of Dembowski and Ostrom, Arch.Math. 27(1976),93-98.

(4) D.Gluck, A note of permutation polynomials and finite geometries, Discrete Math. 80(1990),97-100.

(5) T.Helleseth and D.Sandberg, Some Power Mappings with Low Differential Uniformity, Applicable Algebra in Engineering, Communication and Computing 8(1997),363-370.

(6) Y.Hiramine, A conjecture on affine planes of prime order, J .Combin. Theory Ser. A 52(1989),44-50.

(7) Y.Hiramine, Factor sets associated with regular collineation groups, J. Algebra 142(1991),414-423.

(8) H.Hiramine, Planar functions and related group algebra, J.Algebra 152(1992),135-145.

(9) N.Nakagawa, The non-existence of right cyclic planar functions of degree p^n for $n \leq 2$, J.Combin. Theory Ser. A 63(1993), 55-64.

(10) N.Nakagawa, Left Cyclic Planar Functions Of Degree p^n, Utilitas Math. 51(1997), 89-96.

(11) N.Nakagawa, On Polynomial Families in n Indeterminates over Finite Prime Fields Coming from Planar Functions, Finite Fields with Applications to Coding Theory,Cryptography and Related Areas, Springer (2002),251-262.

(12) L.Ronayi and T.Szonyi, Planar functions over finite fields, Combinatorica 9(1989),315-320.

(13) U.Ott, Endliche zyklische Ebenen, Math. Zeitschrift 144(1975), 195-215.

On Completely Regular Codes and Related Topics

Hiroshi SUZUKI*†
Department of Mathematics
International Christian University

August 13, 2003

1 Introduction

This is an article to introduce completely regular codes from a view point of Terwilliger algebra associated with a set of vertices defined by the author in [9]. Completely regular codes were defined by P. Delsarte in [3] in connection with perfect codes in 1973, but there are not many articles on this subject. We refer the readers to [2, Chapter 11] for results prior to 1989, and [4, 5, 6, 7, 8].

We first review terminologies and notation we use in this article. We mainly follow [1]. See also [2].

Graph:

- $\Gamma = (X, R)$: a connected graph, where
  X: a finite set, $R \subset \binom{X}{2}$, i.e., R is a subset of the set of 2-element subsets of X.
- For $x, y \in X$, $x \sim y \Leftrightarrow (x, y) \in R$.
- $\partial(x, y) =$ the length of a shortest path between x and y.

*Electric mail : hsuzuki@icu.ac.jp
†This research was partially supported by the Grant-in-Aid for Scientific Research (No.12640039), Japan Society of the Promotion of Science.

- $D = \max\{\partial(x,y) \mid x,y \in X\}$: diameter of Γ.
- $C \subset X$ is called a code of Γ, and is also called a subgraph of Γ when the induced subgraph structure on C is considered.
- $C_i = \Gamma_i(C) = \{x \in X \mid \partial(x,C) = i\}$ is called the i-th subconstituent with respect to C, where $\partial(x,C) = \min\{\partial(x,y) \mid y \in C\}$. When $C = \{x\}$, we write $\Gamma_i(x)$ for $\Gamma_i(\{x\})$.
- $t = t(C) = \max\{i \mid C_i \neq \emptyset\}$ is called the covering radius of C. We have $C = C_0$ and

$$X = C_0 \cup C_1 \cup \cdots \cup C_t \quad \text{(disjoint union)}.$$

- $w = w(C) = \max\{\partial(x,y) \mid x,y \in C\}$ is called the width of C.
- $\delta = \delta(C) = \min\{\partial(x,y) \mid x,y \in C,\ x \neq y\}$ is called the minimum distance of C.
- $V = \boldsymbol{C}^X = \mathrm{Span}(\hat{x} \mid x \in X)$ is a vector space over the complex number field consisting of the set of column vectors with rows indexed by the elements of X, and $\hat{x}$ denotes the unit vector whose x-entry is 1 and 0 otherwise.
- The adjacency matrix $A \in \mathrm{Mat}_X(\boldsymbol{C})$ of Γ is defined as follows.

$$A_{x,y} = \begin{cases} 1, & \text{if } x \sim y \\ 0, & \text{otherwise} \end{cases}.$$

- For $i \in \{0,1,\ldots,t\}$, $E_i^* = E_i^*(C) \in \mathrm{Mat}_X(\boldsymbol{C})$ are defined as follows.

$$(E_i^*)_{x,y} = \begin{cases} 1, & \text{if } x = y \text{ and } x \in C_i \\ 0, & \text{otherwise} \end{cases}.$$

Then E_i^* is the projection onto the subspace $E_i^*V = \mathrm{Span}(\hat{x} \mid x \in C_i)$.

Definition 1.1 The Terwilliger algebra $\mathcal{T} = \mathcal{T}(C)$ of a graph $\Gamma = (X,R)$ associated with a subset C of X is a matrix subalgebra over $\boldsymbol{C}$ of $\mathrm{Mat}_X(\boldsymbol{C})$ generated by A together with $E_0^*, E_1^*, \ldots, E_t^*$, where $t = t(C)$. A $\mathcal{T}$-module W is a $\mathcal{T}$-invariant linear subspace of V. A nonzero $\mathcal{T}$-module W is said to be irreducible if W does not contain proper nonzero $\mathcal{T}$-modules. An irreducible $\mathcal{T}$-module W is said to be thin if $\dim E_i^*W \leq 1$ for every $i = 0,1,\ldots,t$.

Note that $\mathcal{T}$ is always semisimple as it is generated by symmetric matrices.

Thin irreducible modules: Let W be a thin irreducible $\mathcal{T}$-module. Write

$$W = E_0^* W \oplus E_1^* W \oplus \cdots \oplus E_t^* W.$$

Since $E_i^* W \subset E_i^* V = \mathrm{Span}(\hat{x} \mid x \in C_i)$, we have

$$AE_i^* W \subset E_{i-1}^* W + E_i^* W + E_{i+1}^* W.$$

Using this fact and the irreducibility of W, it is not difficult to show that there exist indices e and $e+d$ with $0 \le e \le e+d \le D$ such that

$$E_i^* W \neq 0 \text{ if and only if } e \le i \le e+d.$$

The index e is called the endpoint and d the diameter of W. Let v_i be a nonzero vector in $E_{e+i}^* W$. Then

$$\begin{aligned} W &= E_e^* W \oplus E_{e+1}^* W \oplus \cdots \oplus E_{e+d}^* W \\ &= \mathrm{Span}(v_0, v_1, \ldots, v_d). \end{aligned}$$

Hence there exist constants β_{i-1}, α_i, and γ_{i+1} satisfying

$$Av_i = \beta_{i-1} v_{i-1} + \alpha_i v_i + \gamma_{i+1} v_{i+1},$$

with $i = 0, 1, \ldots, d$, $\beta_{-1} = 0$, $\gamma_{d+1} = 1$, and $v_j = 0$ for $j < 0$ or $j > d$. By irreducibility of W, we have $\beta_i \gamma_{i+1} \neq 0$ for $i = 0, 1, \ldots, d-1$. Thus if we define polynomials $g_i(x) \in C[x]$ by $g_{-1}(x) = 0$, $g_0(x) = 1$, and

$$x \cdot g_i(x) = \beta_{i-1} g_{i-1}(x) + \alpha_i g_i(x) + \gamma_{i+1} g_{i+1}(x),$$

for $i = 0, 1, \ldots, d$, then $v_i = g_i(A) v_0$ and $g_{d+1}(A) W = 0$. It is known that these polynomials form a system of orthogonal polynomials with respect to a certain weight function. Moreover, if $E_0, E_1, \ldots, E_m$ are primitive idempotents of $C[A]$, then

$$\begin{aligned} W &= C[A] v_0 \\ &= E_0 W \oplus E_1 W \oplus \cdots \oplus E_m W, \end{aligned}$$

and $E_i W = Span(E_i v_0)$. In particular, $\dim E_i W \le 1$.

Summary: If a thin irreducible $\mathcal{T}$-module W exists, then we have the following.

- W weakly represents some combinatorial structure, especially when the vector v_0 is given as a simple sum of vectors $\hat{y}$ with $y \in C$.
- A system of orthogonal polynomials are associated to the module.
- Every eigenvalue of A on W is of multiplicity 1.

2 Completely Regular Codes

Definition 2.1 Let $\Gamma = (X, R)$ be a connected graph, and C a nonempty subset of X. Let $\mathbf{1}_C = \sum_{x \in C} \hat{x} \in V = \boldsymbol{C}^X$. Then C is said to be a completely regular code if $\mathcal{T}(C)\mathbf{1}_C$ is a thin irreducible $\mathcal{T}(C)$-module.

Questions:

Q1. Are graphs with many completely regular codes 'good'?

Q2. Is there any characteristic of completely regular codes in a 'good' graph?

Q3. Are there some 'good' classes of completely regular codes?

For simplicity, assume that $\Gamma = (X, R)$ is a regular connected graph of diameter D. Then $C[A]$ contains the all 1's matrix $J \in \mathrm{Mat}_X(\boldsymbol{C})$. We consider the case when $\{x\}$ is a completely regular code for every $x \in X$. Let $\mathbf{1}$ be the all 1's vector in V and $\mathbf{1}_i = E_i^* \mathbf{1}$. Then $\mathbf{1}_0 = \mathbf{1}_C$ and

$$\mathbf{1}_i = \sum_{x \in C_i} \hat{x}, \text{ where } C_i = \Gamma_i(x).$$

Let $x \in X$, and $W = \mathcal{T}\hat{x}$. Since $J \in C[A] \subset \mathcal{T}$, $\mathbf{1} = J\hat{x} \in \mathcal{T}\hat{x} = W$, and $\mathbf{1}_i = E_i^* \mathbf{1} \in E_i^* W$. Thus we have the following.

$$\begin{aligned} & W \text{ is thin} \\ \Leftrightarrow\ & W = \mathrm{Span}(\mathbf{1}_0, \mathbf{1}_1, \ldots, \mathbf{1}_D) \\ \Leftrightarrow\ & E_{i-1}^* A \mathbf{1}_i = c_i \mathbf{1}_{i-1},\ E_i^* A \mathbf{1}_i = a_i \mathbf{1}_i, \text{ and} \\ & E_{i+1}^* A \mathbf{1}_i = b_i \mathbf{1}_{i+1}, \text{ for some constants } c_i, a_i, b_i. \end{aligned}$$

Now it is not difficult to show that Γ is a distance-regular graph and we reached the following well-known result.

Proposition 2.1 *Let $\Gamma = (X, R)$ be a connected regular graph*. Then the following are equivalent.*

(i) *For every $x \in X$, $\{x\}$ is a completely regular code.*

(ii) *Γ is a distance-regular graph.*

At our seminar, R. Hosoya presented the following result.

*If Γ is not regular, (i) is equivalent to Γ being a distance-biregular graph.

Proposition 2.2 *Let $\Gamma = (X, R)$ be a connected graph of diameter D. Then the following are equivalent.*

(i) *For every $\{x, y\} \in R$, $\{x, y\}$ is a completely regular code with the same parameter set*[†].

(ii) *Γ is a distance-regular graph with $a_{D-1} = 0$.*

In order to state problems, let us introduce several terminologies. Let $\Gamma = (X, R)$ be a connected graph. For $C \subset X$, let $w(C) = \max\{\partial(x, y) \mid x, y \in C\}$. $w(C)$ is called the width of C. For $x \in X$, let $x^{\perp} = \{y \in X \mid \partial(x, y) \leq 1\}$. For $\{x, y\} \in R$,

$$\langle x, y \rangle = \bigcap_{z \in x^{\perp} \cap y^{\perp}} z^{\perp}$$

is called a singular line through x and y. Note that $x, y \in \langle x, y \rangle$ and $w(\langle x, y \rangle) = 1$.

Problem 2.1 Characterize a connected graph (or a distance-regular graph) such that $\langle x, y \rangle$ is a completely regular code for every $\{x, y\} \in R$.

Problem 2.2 Characterize a connected graph (or a distance-regular graph) such that for every $x, y \in X$ with $\partial(x, y) = i$, there is a completely regular code C with $i = w(C)$ containing x, and y.

3 Thin Irreducible Modules

Let $\Gamma = (X, R)$ be a distance-regular graph of valency k and diameter D. For each $i = 0, 1, \ldots, D$, let $A_i \in \mathrm{Mat}_X(C)$ be the i-th adjacency matrix defined by

$$(A_i)_{x,y} = \begin{cases} 1 & \partial(x, y) = i \\ 0 & \text{otherwise} \end{cases}.$$

Then there is a polynomial $v_i(x) \in C[x]$ of degree exactly i such that $v_i(A) = A_i$. Let $k_i = v_i(k)$. Then $k_i = |\Gamma_i(x)|$ for every $x \in X$. Let $\theta_0 > \theta_1 > \cdots > \theta_D$ be distinct eigenvalues of A and let $E_0, E_1, \ldots, E_D$ be the primitive idempotents of $C[A]$ corresponding to each of the distinct eigenvalues. Then each column of E_i is an eigenvector of the same eigenvalue θ_i of A, and $AE_i = \theta_i E_i$. Let $m(\theta_i) = \mathrm{tr}(E_i)$. Then $m(\theta_i)$ is the multiplicity of θ_i as an eigenvalue of A. Set $\Theta = \{\theta_0, \theta_1, \ldots, \theta_D\}$.

[†]The parameter set consists of $\alpha_i, \beta_i, \gamma_i$ according to the basis $\mathbf{1}_i = E_i^* \mathbf{1}$.

Let C be a nonempty subset of X and $T = T(C)$. We consider an irreducible module W such that $E_0^* W \neq 0$, i.e., a module of endpoint 0. We remark a couple of things. First if W is an irreducible $T(C)$-module of endpoint e, then W can be viewed as an irreducible $T(C_e)$-module of endpoint 0 with $C_e = \Gamma_e(C)$. Secondly as far as we are studying completely regular codes, the module we first look at is $T(C)1_C$ of endpoint 0.

Proposition 3.1 *Let $\Gamma = (X, R)$ be a distance-regular graph. Let u be a eigenvector of A in $V = C^X$ such that $Au = \theta u$. Let $v_i = E_i^* u$ for $i = 0, 1, \ldots, t$. Suppose $v_0 \neq 0$. If $E_i^* A_i v_0$, $E_i^* A_{i+1} v_0 \in \mathrm{Span}(v_i)$, then $W = Tv_0 = Tu$ is a thin irreducible module.*

Applying the previous proposition to $u = \mathbf{1}$, we have the following corollary proved in [8].

Corollary 3.2 *Let $\Gamma = (X, R)$ be a distance-regular graph and let C be a nonempty subset of X. For each i, suppose*

$$\mu_i = |\{y \in C \mid \partial(x, y) = i\}|, \ \lambda_{i+1} = |\{y \in C \mid \partial(x, y)\}|$$

are independent of the choice of $x \in C_i$, then C is a completely regular code.

Proof. Since $E_i^* A_i \mathbf{1}_0 = \mu_i \mathbf{1}_i$ and $E_i^* A_{i+1} \mathbf{1}_0 = \lambda_{i+1} \mathbf{1}_i$, the assertion follows from Proposition 3.1. ∎

Let $v = E_0^* v$ be a nonzero vector. Set

$$\rho_v(x) = \frac{1}{|X|} \sum_{i=0}^{D} \frac{\overline{{}^t v} A_i v}{\|v\|^2} \frac{v_i(x)}{k_i} \in R[x].$$

The following is called the inner distribution of the vector v.

$$a(v) = \left(\frac{\overline{{}^t v} A_0 v}{\|v\|^2}, \ldots, \frac{\overline{{}^t v} A_i v}{\|v\|^2}, \ldots, \frac{\overline{{}^t v} A_D v}{\|v\|^2} \right).$$

By definition, if $w = w(C)$ is the width of C, then the degree of $\rho_v(x)$ is at most w. On the other hand by direct computation we have

$$\frac{\|E_i v\|^2}{\|v\|^2} = \rho_v(\theta_i) m(\theta_i).$$

Since $C[A]v = \mathrm{Span}(E_0 v, E_1 v, \ldots, E_D v)$, we have

$$\begin{aligned} \dim C[A]v &\geq D + 1 - (\#\text{ of roots of } \rho_v(x) \text{ in } \Theta) \\ &\geq D + 1 - \deg \rho_v \\ &\geq D + 1 - w(C). \end{aligned}$$

Set $r = r(v) = \dim C[A]v - 1$. $r(v)$ is said to be the dual degree of v. Now we have the following.

Theorem 3.3 ([9]) *Let $\Gamma = (X, R)$ be a distance-regular graph of diameter D, and C a nonempty subset of X. Let $v = E_0^* v$ be a nonzero vector. Then the following hold.*

(1) $\dim C[A]v + w(C) \geq D + 1$.

(2) *If $\dim C[A]v + w(C) = D + 1$, then $T(C)v$ is a thin irreducible $T(C)$-module.*

The nonzero vector $v \in E_0^* V$ satisfying the condition in Theorem 3.3 (2) is called a tight vector. When $E_0^* V$ is spanned by tight vectors, we call C a tight code.

When $v = \mathbf{1}_0$, $|X|E_0\mathbf{1}_0 = J\mathbf{1}_0 = |C|\mathbf{1} \neq \mathbf{0}$. Hence

$$r = |\{i \mid E_i\mathbf{1}_0 \neq \mathbf{0},\ i = 1, 2, \ldots, D\}|.$$

The dual degree is customarily defined for a code using this definition. Hence ours is a bit generalized usage of the term.

Corollary 3.4 *Let $\Gamma = (X, R)$ be a distance-regular graph of diameter D, and C a nonempty subset of X. If $r + w(C) = D$, then C is a completely regular code. Moreover, we have $t = r$ in this case.*

Note that the condition in the corollary can be checked if we have $a(C)$ together with the set of eigenvalues of A.

4 Perfect Codes

Let $\delta = \delta(C)$ be the minimal distance, $t = t(C)$ the covering radius, and r the dual degree. It is clear that $\delta \leq 2t+1$. Moreover, $t \leq r$ in general. When $\delta = 2t + 1$, C is called a perfect code.

Proposition 4.1 ([3]) *The following are equivalent.*

(i) $\delta = 2t + 1$, *i.e., the code C is perfect.*

(ii) $\delta = 2r + 1$.

Moreover, in this case C is a completely regular code.

This is another result for a code to become completely regular by a condition imposed on $a(\mathbf{1}_0)$.

Problem 4.1 Find a generalization of Proposition 4.1 such that Tv becomes completely regular by a condition imposed on $a(v_0)$.

5 Codes in a Distance-Regular Graph

Example 5.1 Let $Q = \{1, 2, \ldots, q\}$ be a q-set, and $X = Q^D$. For $x = (x_1, \ldots, x_D)$, $y = (y_1, \ldots, y_D) \in X$,

$$(x, y) \in R \Leftrightarrow |\{i \mid x_i \neq y_i\}| = 1.$$

The graph $\Gamma = (X, R)$ is called the Hamming graph $H(D, q)$.

Completely regular codes have been studied in the context of perfect codes or codes which are very close to perfect, for example, uniformly packed codes. Hamming codes, extended Hamming codes, binary Golay codes, ternary Golay codes, etc. On the other hand, it is easy to see that if $C = \{x, y\}$ is a completely regular code with two vertices in $H(D, 2)$ then either $\partial(x, y) = D$ or 1[‡]. The first is the case when C is a (trivial) perfect code and it represents codes with large minimum distance, while the latter is the case when C is a tight code and it represents codes with rich substructures.

A systematic search of completely regular codes was first made in [4] assuming the group action. But not a satisfactory result is known for their classification.

Problem 5.1 Classify tight codes in known distance-regular graphs.

Problem 5.2 Classify all completely regular codes with minimal distance $\delta(C) \geq 7$.

6 Strongly Closed Property of a Code

Definition 6.1 Let $\Gamma = (X, R)$ be a distance-regular graph and Y a nonempty subset of X. Y is said to be strongly closed in Γ if for every $x, y \in Y$,

$$\{z \mid \partial(x, z) + \partial(z, y) \leq \partial(x, y) + 1\} \subset Y.$$

The following result was proved by Y. Enta and the author.

Proposition 6.1 *Let $\Gamma = (X, R)$ be a distance-regular graph of valency k, and $\emptyset \neq C \subset Y \subset X$. Suppose C is a completely regular code and Y is strongly closed such that $\max\{|\Gamma(y) \cap Y| \mid y \in Y\} < k$. Then C is strongly closed.*

Problem 6.1 Classify distance-regular graphs with a (or many) strongly closed completely regular code(s) of width at least 2.

Hamming graphs $H(D, q)$ and dual polar graphs have strongly closed completely regular codes of arbitrary width.

[‡]This is also obtained by an application of Proposition 6.1

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin/Cummings, California, 1984.

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

[3] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Research Reports Supplements 1973, No.10.

[4] M. Giudice and C. E. Praeger, Completely transitive codes in Hamming graphs, European J. Combin. 20 (1999), 647-661.

[5] M. A. Fiol and E. Garriga, On the algebraic theory of pseudo-distance-regularity around a set, Linear Algebra Appl. 298 (1999), 115-141.

[6] M. A. Fiol and E. Garriga, An algebraic characterization of completely regular codes in distance-regular graphs, SIAM J. Discrete Math. 15 (2001/02), 1-13.

[7] W. J. Martin, Completely regular designs, J. Combin. Des. 6 (1998), 261-273.

[8] A. Neumaier, Completely regular codes, Discrete Math., 106/107 (1992), 353-360.

[9] H. Suzuki, The Terwilliger algebra associated with a set of vertices in a distance-regular graph, preprint.

A family of dual hyperovals over $GF(q)$ with q even

谷口浩朗

詫間電波高専
香川県三豊郡大字香田５５１

1 Introduction

Let $GF(q)$ be a finite field consisting of q elements, and $PG(n,q)$ an n-dimensional projective space over the field $GF(q)$.

A d-dimensional dual hyperoval S is a family of d-dimensional subspaces of $PG(n,q)$ which satisfy the following conditions: see [2]

(1) For every distinct member X and Y of S, $X \cap Y$ is a projective point.

(2) For any three distinct members X_1, X_2 and X_3 of S, the intersection $X_1 \cap X_2 \cap X_3 = \emptyset$.

(3) Let $X \in S$. Then the set of projective points $\{X \cap Y \mid Y \in S,\ X \neq Y\}$ span X.

(4) The members of S span $PG(n,q)$.

(5) The cardinality $|S|$ is $q^d + q^{d-1} + \cdots + q + 2$.

Thas and Van Maldeghem [1] constructed a d-dimensional dual arc $\mathcal{AV}_d$ of size $q^d + q^{d-1} + \cdots + q + 1$ over $GF(q)$ using Veronesean. Yoshiara [3] extended the dual arc $\mathcal{AV}_d$ to a dual hyperoval $\mathcal{HV}_d$ in case q is even, and constructed d-dimensional dual hyperovals in $PG(n,q)$ with q even for $4d-2 \leq n \leq d(d+3)/2$ using quotients of $\mathcal{HV}_d$.

In this paper, we construct a new family of dual hyperovals over $GF(q)$ with q even.

For any $GF(q)$-vector space V of finite dimension, we denote by rank V the dimension of V over the field $GF(q)$.

We define the equivalence relation $s \sim t$ for $s,\ t \in V - \{0\}$ if and only if there exists a non-zero $k \in GF(q)$ such that $s = kt$. Then, we are able

to regard $V-\{0\}/\sim$ as a projective space over $GF(q)$. From now on, we denote by $PG(V)$ the projective space $V-\{0\}/\sim$, and we denote by $[\alpha]$ the equivalence class of α in $PG(V)$ for any element $\alpha \in V-\{0\}$.

We also denote the multiplicative group $GF(q)-\{0\}$(resp. $GF(q^n)-\{0\}$) by $GF(q)^*$(resp. $GF(q^n)^*$), and the Galois group of $GF(q^n)$ over $GF(q)$ by $Gal(GF(q^n)/GF(q))$.

2 The construction

Lemma . *Let m and n be integers with $q := 2^m \geq 2$ and $n \geq 2$, and assume that $q-1$ and n are mutually coprime. Let σ be a generator of the Galois group $Gal(GF(q^n)/GF(q))$. Then the mapping*

$$\sigma - 1 : GF(q^n)^* \ni x \mapsto x^{\sigma-1} = x^\sigma / x \in GF(q^n)^*$$

induces an isomorphism from $GF(q^n)^*/GF(q)^*$ onto $GF(q^n)^*/GF(q)^*$.

Proof. It is clear that $\sigma - 1$ is a group homomorphism from $GF(q^n)^*$ into $GF(q^n)^*$. It is also clear that $x^{\sigma-1} = 1 \in GF(q)^*$ for any $x \in GF(q)^*$. Conversely, let $x \in GF(q^n)^*$ such that $x^{\sigma-1} = \alpha \in GF(q)^*$. Then we have $x^\sigma = \alpha x$, which implies $x = x^{\sigma^n} = \alpha^n x$. Since the cardinality $|GF(q)^*| = q-1$, and since $q-1$ and n are mutually coprime by the assumption, we conclude that $\alpha = 1$. Hence we see that $x^\sigma = x$, which implies that $x \in GF(q)^*$. □

Theorem 1. *Let m, n and d be positive integers with $q := 2^m$ and $d+1 \leq n$. We assume that $q-1$ and n are mutually coprime integers. We choose a $GF(q)$ vector subspace V of rank $d+1$ in $GF(q^n)$, and denote by $PG(V)$ the projective space $V-\{0\}/\sim$. We regard $GF(q^n) \times GF(q^n)$ as a $GF(q)$ vectorspace, and denote by $PG(GF(q^n) \times GF(q^n))$ the projective space $GF(q^n) \times GF(q^n) - \{0\}/\sim$.*

Let σ be a generator of $Gal(GF(q^n)/GF(q))$.

For $[\alpha] \in PG(V)$, we define a d-dimensional projective subspace $X_{[\alpha]}$ in $PG(GF(q^n) \times GF(q^n))$ as follows:

$$X_{[\alpha]} = \{\ [(x\alpha, x^\sigma\alpha + x\alpha^\sigma)] \mid [x] \in PG(V)\ \}.$$

We also define a d-dimensional projective subspace X_∞ in $PG(GF(q^n) \times GF(q^n))$ as follows:

$$X_\infty = \{[(x^2, 0)] \mid [x] \in PG(V)\}.$$

Then $S := \{\ X_{[\alpha]} \mid [\alpha] \in PG(V)\} \cup \{X_\infty\}$ is a dual hyperoval.

Proof. It is clear that $X_{[\alpha]}$ and X_∞ are d-dimensional projective subspaces in $PG(GF(q^n) \times GF(q^n))$. Let $[\alpha], [\beta] \in PG(V)$ with $[\alpha] \neq [\beta]$. For any point t in $X_{[\alpha]} \cap X_{[\beta]}$, there exists $[x], [y] \in PG(V)$ such that t is expressed in $PG(GF(q^n) \times GF(q^n))$ as follows:

$$t = [(x\alpha, x^\sigma\alpha + x\alpha^\sigma)] = [(y\beta, y^\sigma\beta + y\beta^\sigma)].$$

That is, there exists $k \in GF(q)^*$ such that a member of the equivalence class of t is expressed in $GF(q^n) \times GF(q^n)$ as follows:

$$(x\alpha, x^\sigma\alpha + x\alpha^\sigma) = k(y\beta, y^\sigma\beta + y\beta^\sigma).$$

From this equation, we have

$$x\alpha = ky\beta, \tag{2.1}$$

$$(x\alpha)^\sigma = k(y\beta)^\sigma, \tag{2.2}$$

$$x^\sigma\alpha + x\alpha^\sigma = ky^\sigma\beta + ky\beta^\sigma. \tag{2.3}$$

If we multiply (2.3) by $\beta\beta^\sigma$, we have

$$x^\sigma\alpha\beta\beta^\sigma + x\alpha^\sigma\beta\beta^\sigma = ky^\sigma\beta^2\beta^\sigma + ky\beta(\beta^\sigma)^2.$$

From (2.1), (2.2), we have

$$x^\sigma\alpha\beta\beta^\sigma + x\alpha^\sigma\beta\beta^\sigma = x^\sigma\alpha^\sigma\beta^2 + x\alpha(\beta^\sigma)^2.$$

Hence we obtain

$$(x\beta^\sigma - x^\sigma\beta)(\alpha^\sigma\beta - \alpha\beta^\sigma) = 0.$$

Since $[\alpha]$ and $[\beta]$ are different members of $PG(V) \subset GF(q^n)^*/GF(q)^*$, and since $\sigma-1$ is an isomorphism from $GF(q^n)^*/GF(q)^*$ onto $GF(q^n)^*/GF(q)^*$ by Lemma , we have $\alpha^{\sigma-1} \neq \beta^{\sigma-1}$, hence $\alpha^\sigma\beta - \alpha\beta^\sigma \neq 0$. Thus, we obtain $x\beta^\sigma - x^\sigma\beta = 0$, which implies that $x^{\sigma-1} = \beta^{\sigma-1}$. By Lemma , we have $[x] = [\beta] \in PG(V) \subset GF(q^n)^*/GF(q)^*$, and similarly we have $[y] = [\alpha] \in PG(V)$. That is, $t = X_{[\alpha]} \cap X_{[\beta]} = [(\alpha\beta, \alpha^\sigma\beta + \alpha\beta^\sigma)]$.

Therefore, we see that $X_{[\alpha]} \cap X_{[\beta]}$ is a projective point. Moreover, for mutually distinct members $[\alpha]$, $[\beta]$ and $[\gamma] \in PG(V)$, we see that $X_{[\alpha]} \cap X_{[\beta]} \cap X_{[\gamma]} = \emptyset$.

Similarly, we have $X_{[\alpha]} \cap X_\infty = [(\alpha^2, 0)] \in PG(GF(q^n) \times GF(q^n))$. Hence we see that $X_\infty \cap X_{[\alpha]}$ is a projective point. Moreover, for $[\alpha] \neq [\beta]$, we see that $X_\infty \cap X_{[\alpha]} \cap X_{[\beta]} = \emptyset$.

Since the cardnality $|PG(V)| = q^d + q^{d+1} + \cdots + 1$, we have $|S| = q^d + q^{d+1} + \cdots + 2$, and therefore we conclude that S is a dual hyperoval. □

Let q be a prime power, $n \geq 2$ and σ a generator of the Galois group $Gal(GF(q^n)/GF(q))$. In the Lemma , Lemma and Corollary 1 which follow, we denote by Tr the trace function from $GF(q^n)$ to $GF(q)$.

Lemma (Additive form of Hilbert's Theorem 90). *Let a be an element of $GF(q^n)$. Then the equation $x^\sigma - x = a$ has a solution x in $GF(q^n)$ if and only if $Tr(a) = 0$.*

Lemma . *Let a and t be non-zero elements in $GF(q^n)$. Then, the equation $x^\sigma t - xt^\sigma = a$ has a solution x in $GF(q^n)$ if and only if $Tr((1/t^{\sigma+1})a) = 0$.*

Proof. We see that $x^\sigma t - xt^\sigma = a$ has a solution x in $GF(q^n)$ if and only if $(x/t)^\sigma - x/t = a/t^{\sigma+1}$ has a solution x/t in $GF(q^n)$. This means, by Lemma , that $Tr((1/t^{\sigma+1})a) = 0$. □

The following lemma is well known. So, we omit the proof.

Lemma . *Let q be prime power, $n \geq 2$ and regard $GF(q^n)$ as a vector space of rank n over $GF(q)$. Then, any vector subspace H of rank $n-1$ can be expressed as $H = \{z \in GF(q^n) \mid Tr(\alpha z) = 0\}$ for some non-zero $\alpha \in GF(q^n)$. Let $H_1 := \{z \in GF(q^n) \mid Tr(\alpha_1 z) = 0\}$ and $H_2 := \{z \in GF(q^n) \mid Tr(\alpha_2 z) = 0\}$ be two vector subspaces of rank $n-1$. Then $H_1 \neq H_2$ if and only if α_1 and α_2 are linearly independent over $GF(q)$.*

Corollary 1. *Let d and m be positive integers with $d \geq 2$ and set $q := 2^m$. We assume that $q-1$ and $d+1$ are mutually coprime integers. Then there exists a d-dimensional dual hyperoval in $PG(2d+1, q)$.*

Proof. We choose $n = d+1$ and $V = GF(2^{d+1})$ in Theorem 1. We have to show that the dual hyperoval S span $PG(2d+1, q)$. As a vector space, we have to show that the members of S span $GF(q^{d+1}) \times GF(q^{d+1})$ over $GF(q)$. Since X_∞ span $\{(x, 0) | x \in GF(q^{d+1})\}$, we have to show that $\{x^\sigma y + xy^\sigma\}$ span $GF(q^{d+1})$ as a $GF(q)$-vector space. Since $\{x^\sigma + x | x \in GF(q^{d+1})\} = \{s \in GF(q^{d+1}) | Tr(s) = 0\}$ is a rank d $GF(q)$-vector subspace H in $GF(q^{d+1})$, we only have to show, by Lemma , that there exists a rank d $GF(q)$-vector subspace $H_1 := \{a \in GF(q^{d+1}) | Tr(a/t^{\sigma+1}) = 0\}$ such that $H \neq H_1$. Therefore, we only have to show that there exists $t \in GF(q^{d+1})$ such that $t^{\sigma+1} \notin GF(q)$ by Lemma . If $t^{\sigma+1} \in GF(q)$, then $t^\sigma = a/t$ for some $a \in GF(q)$, hence $t^{\sigma^2} = a/(a/t) = 1$. Since $d+1 \geq 3$, there exists t such that $t^{\sigma^2} \neq t$, that is, there exists t such that $t^{\sigma+1} \notin GF(q)$. Thus we have proved this colloraly. □

Corollary 2. *Let d and m be positive integers with $m \geq 2$ and set $q := 2^m$. Then there exists a d-dimensional dual hyperoval in $PG(d(d+3)/2, q)$.*

Proof. We choose n sufficient large such that n is coprime with $d+1$, and choose a $GF(q)$-vector subspace V of $GF(q^n)$ such that a basis $\{e_0, e_1, \ldots, e_d\}$ of V satisfies that $\{e_i e_j\}$ for $i \leq j$ are also linearly independent over $GF(q)$. Then, since $(e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma)$ spans the ambient space of S, the dimension of the ambient space is greater than or equal to $d(d+3)/2$.But since the dimension of the ambient space is less than or equal to $d(d+3)/2$ by S. Yosiara[3], we conclude that S is a dual hyperoval in $PG(d(d+3)/2, q)$. □

Proposition 1. *Let V be as in Theorem 1 and $[\alpha]$, $[\beta]$ and $[\gamma]$ collinear points in $PG(V)$ such that $[\beta] \neq [\gamma]$. Then $X_{[\alpha]} \subset \langle X_{[\beta]}, X_{[\gamma]} \rangle$.*

Proof. Since there exist s and t in $GF(q)$ such that $\alpha = s\beta + t\gamma$, we have

$$(x\alpha, x^\sigma \alpha + x\alpha^\sigma) = s(x\beta, x^\sigma \beta + x\beta^\sigma) + t(x\gamma, x^\sigma \gamma + x\gamma^\sigma)$$

for any $x \in V$, which implies that $X_{[\alpha]} \subset \langle X_{[\beta]}, X_{[\gamma]} \rangle$.

□

References

[1] J. A. Thas and Van Maldegem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, *preprint.*

[2] S. Yoshiara, A family of d-dmensional dual hyperovals in $PG(2d+1, 2)$, Europ. J. Combinatrics, **20**(1999), 589-603.

[3] S. Yoshiara, Ambient spaces of dimensional dual arcs, *to appear in Journal of Algebraic Combinatrics.*

On (2n,2,2n,n)relative difference sets in non-solvable groups

Yutaka Hiramine
Department of Mathematics, Faculty of Education, Kumamoto University
Kurokami, Kumamoto, Japan
E-mail: hiramine@gpo.kumamoto-u.ac.jp

Noboru Ito
Hachimae 2-1612, San Royal 301,Nagoya,Meito 465-0018, Japan
E-mail: fn48@tcp-ip.or.jp

1 Introduction

Let G be a group of order $4n$. For a subset X of G, we set $X^{(-1)} = \{x^{-1} \mid x \in X\}$ and we identify a subset X of G with a group ring element $\widehat{X} = \sum_{x \in X} x \in \mathbb{C}[G]$. The set of G-conjugates of an element $x(\in G)$ is denoted by x^G.

A $2n$-subset R of G is called *a left Hadamard transversal* of G with respect to a subgroup $\langle t \rangle$ of order 2 if $G = R\langle t \rangle$ and $\widehat{R}\widehat{R^{-1}} = n\widehat{S}_1 + 2n\widehat{S}_2$ for some subsets S_1 and S_2 of G ([3]). Therefore $|R \cap Rx| = 0, n, or\ 2n$ for $x \in G$ according as $x \notin S_1 \cup S_2$, $x \in S_1$ or $x \in S_2$, respectively. A *right Hadamard transversal* of G is defined similarly.

Let R be a left Hadamard transversal of G with respect to $\langle t \rangle \simeq \mathbb{Z}_2$. If we assume that

$$(*) \quad R \neq xR \ \ \forall x \in G \setminus \{1\},$$

then, by a result of [3] some left translate of R, say R_0, satisfies that $G = \langle t \rangle R_0 = R_0\langle t \rangle$ and $R_0 R_0^{(-1)} = 2n + n(G - \langle t \rangle)$ for an element t_0 of order 2 (Result 3.1). Therefore R_0 is a $(2n, 2, 2n, n)$ relative difference set (RDS). Here, a $2n$-subset D of G is called a $(2n, 2, 2n, n)$ relative difference set (RDS) relative to a subgroup $\langle s \rangle \simeq \mathbb{Z}_2$ if $DD^{(-1)} = 2n + n(G - \langle s \rangle)$. From a left Hadamard transversal satisfying $(*)$ one can construct a Hadamard matrix of order $2n$ (see [3] and Result 3.1).

In this article we show that :

Theorem 3.5 *Assume that a group G of order $4n$ contains a left Hadamard transversal R with respect to $\langle t \rangle$ satisfying $R \neq xR$ $\forall x \in G \setminus \{1\}$. Then R is a $(2n, 2, 2n, n)RDS$ relative to $\langle t \rangle$. If G has a subgroup H satisfying $G = [G, G]H$, $t \in H$ and $t^G \not\subset H$, then there exists a $v \times v$ integral matrix $B = (b_{i,j})$ such that $BB^T = B^TB = \frac{n}{2}I_v$, where $v = \frac{|G:H|(|t^G| - |t^G \cap H|)}{2|t^G|}$ and $|b_{i,j}| \leq \frac{1}{2}|H|$.*

Proposition 3.6 *Let (G, Ω) be a transitive permutation group of degree $r(> 4)$ and t an involution of G. Suppose that $[G, G]$ is transitive on Ω. If t fixes $r - 4$ points and the square free part of $|G|$ has a prime divisor p such that $p \equiv 3 \pmod 4$, then G has no left Hadamard transversal w.r.t.$\langle t \rangle$ satisfying $R \neq xR$ $\forall x \in G \setminus \{1\}$.*

As a corollary we have :

Corollary 3.8 *There is no left Hadamard transversal R satisfying $R \neq xR$ $\forall x \in G \setminus \{1\}$ in $A_5, S_5, A_7, S_7, PSL(2, 7)$ and $PGL(2, 7)$.*

The terminologies in this article are taken from [1] and [4].

2 Preliminaries

We list some preliminary results to prove our theorem.

Result 2.1 *(N. Ito and P. S. Kim [3]) Let G be a group of order $4n$ containing an involution b. Suppose that R is a left Hadamard transversal of G with respect to $\langle b \rangle$. Then the following are equivalent.*

(a) $xR \neq R$ *for any* $x \in G \setminus \{1\}$.

(b) *G contains a $2n$-subset S such that $|s_1R \cap s_2R| = n$ for any two distinct elements s_1, s_2 of S.*

(c) *R is a right Hadamard transversal of G with respect to $\langle c \rangle$, where c is the element of G such that $cR \cap R = \phi$, and G conains a $2n$-subset S' such that $|Rs_1 \cap Rs_2| = n$, for any $s_1, s_2 \in S', s_1 \neq s_2$. Therefore $Rx \neq R$ for any $x \in G \setminus \{1\}$.*

Result 2.2 *(N. Ito and P. S. Kim [3]) Suppose that a group G has a left and right transversal R with respect to $\langle b \rangle$ and $\langle c \rangle$, respectively. If one of the equivalent conditions stated in Result 2.1 holds, then b and c are conjugate.*

3 Proof of Theorem 3.5

First of all, we show the following:

Result 3.1 *(N. Ito and P. S. Kim [3]) Let R be a a left Hadamard transversal in a group G of order $4n$ satisfying $R \neq xR \ \ \forall x \in G \setminus \{1\}$. Then a left translate $R_0(= Rg)$ of R is a $(2n, 2, 2n, n)$relative difference set in G relative to $\langle t_0 \rangle$ for an involution $t_0 \in G$ satisfying $R_0 R_0^{(-1)} = R_0^{(-1)} R_0 = 2n + n(G - \langle t_0 \rangle)$.*

Proof. By Result 2.1, R is also a right Hadamard transversal of G with respect to $\langle s \rangle$ for an involution s of G.

$$R^{(-1)}R = 2n + n(\langle s \rangle).$$

Moreover, by Result 2.2,

$$RR^{(-1)} = 2n + n(\langle g^{-1}sg \rangle).$$

for an element g of G. Set $R_0 = gR$ and $t_0 = s$. Then we have the lemma.

Throughout this article we assume the following.

Hypothesis 3.2 *Let R be a left Hadamard transversal in a group G of order $4n$ w.r.t $\langle t \rangle \simeq \mathbb{Z}_2$ satisfying $R \neq xR \ \ \forall x \in G \setminus \{1\}$. Assume that there is a subgroup H containing t such that $G = [G, G]H$ and $t^G \not\subset H$.*

By Lemma 3.1, we may asuume that

$$(**) \qquad RR^{(-1)} = R^{(-1)}R = 2n + n(G - 1 - t).$$

Let (G, Ω) be a transitive permutation group on a set Ω such that $G_\alpha = H$. Set $r = [G : H]$ and $h = [H : \langle t \rangle]$. Then $|G| = 2hr$. Let K be the kernel of the permutation representation. Then $K = \cap_{x \in G} x^{-1}Hx$. By assumption, $t \in H \setminus K$, for otherwise, $t \in K$ and so $t^G \subset K \subset H$ as $G \rhd K$. This is contrary to Hypothesis 3.2.

Let V be the permutation module for G over $\mathbb{C}$ with the natural basis Ω. Let φ be the representation of G over $\mathbb{C}$ corresponding to the G-module V. Then $\varphi(g)$ is a permutation matrix of degree r for each $g \in G$. We note that if $\alpha_i g = \alpha_j$ then i-th row of $\varphi(g)$ is e_j, where $e_1 = (1, 0, \cdots, 0), \cdots, e_r = (0, \cdots, 0, 1)$. Set $T_0 = \varphi(t)$. We may assume that $\mathrm{Fix}(t) = \{\alpha_1, \cdots, \alpha_f\}$

and $\alpha_{f+1}t = \alpha_{f+2}, \alpha_{f+3}t = \alpha_{f+4}, \cdots, \alpha_{f+w-1}t = \alpha_{f+w}$, where $r = f + w$ and $1 \leq f \leq r-2$ as $t \in H \setminus K$. Then we have

$$T_0 = \begin{bmatrix} I_f & & & \\ & D & & \\ & & \ddots & \\ & & & D \end{bmatrix}$$

where I_f is a unit matrix of degree f and $D = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. We note that w is even.

Lemma 3.3 *Set $A = \varphi(R) = (a_{ij})$ and denote by A^T the transposed matrix of A. Then the following hold :*

(i) $AA^T = A^TA = nI_r + 2nhJ_{r,r} - nT_0$, *where $J_{u,v}$ is the $u \times v$ all one matrix,*

(ii) *if $i \leq f$ or $j \leq f$, then $a_{i,j} = h$, and*

(iii) $AT_0 = T_0A$ *and* $A + AT_0 = 2hJ_{r,r}$.

Proof. By Theorem 4.3.4 of [1], $(1_G, 1_H^G) = 1$, where 1_G is the trivial character of G. Let χ be any linear character of G distinct from 1_G. As $G = [G,G]H$ and $\chi \neq 1_G$, $(1_H, \chi|_H)_H = 0$. Hence, by Frobenius reciprocity theorem, $(1_H^G, \chi) = (1_H, \chi|_H)_H = 0$. Thus 1_G is the only linear constituent of 1_H^G.

We note that $r > 2$ as $t^G \notin H$. Set $L = \varphi(G)$ and let $v \in V$. Then $(vL)\varphi(g) = v(\varphi(Gg)) = vL$ for all $g \in G$. By what we have shown in the last paragraph, $(\alpha_1 + \cdots + \alpha_r)\mathbb{C}$ is the only one dimensional G-submodule of V. Hence $vL \in (\alpha_1 + \cdots + \alpha_r)\mathbb{C}$. Therefore, as L has a constant row sum $4n(= |G|)$, we have $L = \frac{4n}{r}J = 2hJ$, where $J = J_{r,r}$.

Set $I = I_r$. Since $\varphi(g)$ is an orthogonal matrix for each $g \in G$, it follows that $\varphi(R^{(-1)}) = A^T$. Hence, by (**), we have $AA^T = A^TA = 2nI + n(L - I - T_0) = nI + 2nhJ - nT_0$. Thus (i) holds.

Set $\Gamma = \{\alpha_1, \cdots, \alpha_f\}$. Let $\alpha_j \in \Gamma$ and set $M = G_{\alpha_j}$. Let x_i be an element of G such that $\alpha_j x_i = \alpha_i$ for each i with $1 \leq i \leq r$. Then $G = Mx_1 \cup \cdots \cup Mx_r$ is a right coset decomposition of G by M. Let $M = \langle t \rangle y_1 \cup \cdots \cup \langle t \rangle y_h$ be a right coset decomposition of M by $\langle t \rangle$. As $\{y_ix_k \mid 1 \leq i \leq h,\ 1 \leq k \leq r\}$ is a complete set of right coset representatives of $G/\langle t \rangle$, $R = \sum_{i,k} t_{i,k}y_ix_k$ for some $t_{i,k} \in \langle t \rangle$. Since $\alpha_j(t_{i,k}y_ix_k) = \alpha_k$ for each i with $1 \leq i \leq h$, we have $a_{j,k} = h$ for any j with $1 \leq j \leq f$ and k with $1 \leq k \leq r$. Similarly, we can set

$R^{(-1)} = \sum_{i,k} s_{i,k}y_ix_k$, where $s_{i,k} \in \langle t \rangle$, as $R^{(-1)}$ is also a complete set of right coset representatives of $G/\langle t \rangle$ (see (**)). Then $\alpha_j g^{-1} = \alpha_k$ for any i with $1 \leq i \leq h$, where $g = (s_{i,k}y_ix_k)^{-1}$. As $g \in R$, this implies that the number of elements g of R satisfying $\alpha_k g = \alpha_j$ is equal to h for any k with $1 \leq k \leq r$ and j with $1 \leq j \leq f$. Therefore we have (ii). By (**), $G = \langle t \rangle R = R\langle t \rangle$. Hence $R + Rt = R + tR = G$ and so we have (iii).

Set $C = (c_{i,j})$, where $c_{i,j} = a_{f+i,f+j}$ with $1 \leq i, j \leq w$. By Lemma 3.3, we can set $A = \begin{bmatrix} hJ_{f,f} & hJ_{f,w} \\ hJ_{w,f} & C \end{bmatrix}$. Moreover, we define a 2×2 matrix $C_{i,j}$ by $C_{i,j} = \begin{bmatrix} c_{2i-1,2j-1} & c_{2i-1,2j} \\ c_{2i,2j-1} & c_{2i,2j} \end{bmatrix}$ for each $i, j \in \{1, 2, \cdots, \frac{w}{2}\}$. Then $C = (C_{i,j})$.

By definition, A has constant row and column sums $|R|(= 2n = rh)$. Applying Lemma 3.3(ii) C also has constant row and column sums $hw(= rh - fh)$.

Lemma 3.4 *Set $\alpha = h^2w$, $\beta = h^2w + n$ and $\gamma = h^2w - n$. Then the following hold :*

(i) $CC^T = C^TC = (B_{ij})$, *where* $B_{i,i} = \begin{bmatrix} \beta & \gamma \\ \gamma & \beta \end{bmatrix}$ $(1 \leq i \leq \frac{w}{2})$ *and* $B_{i,j} = \alpha J_{2,2}$ *for any* i, j *with* $1 \leq i, j \leq \frac{w}{2}, i \neq j$ *and*

(ii) Each $C_{i,j}$ *is of the form* $\begin{bmatrix} x & y \\ y & x \end{bmatrix}$, *where* $x + y = 2h$. *Here* x *and* y *are non-negative integers depending on* i *and* j.

Proof. By (i) and (ii) of Lemma 3.3, we have (i). Set $\tilde{D} = \mathrm{diag}(D, \cdots, D)$. Then, by Lemma 3.3(iii), $C\tilde{D} = \tilde{D}C$ and $C + C\tilde{D} = 2hJ_{w,w}$. Thus we can easily verify (ii).

Set $P = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$. Then P is an orthogonal matrix and $P^T = P^{-1} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$. Moreover, $P^{-1} \begin{bmatrix} x & y \\ y & x \end{bmatrix} P = \begin{bmatrix} x-y & 0 \\ 0 & x+y \end{bmatrix}$. We define a $w \times w$ orthoganal matrix $\tilde{P}$ by $\tilde{P} = \mathrm{diag}(P, P, \cdots, P)$. Then, by Lemma

3.4(ii), we have

$$\tilde{P}^{-1}C\tilde{P} = \begin{bmatrix} 2b_{1,1} & 0 & 2b_{1,2} & 0 & \cdots & 2b_{1,v} & 0 \\ 0 & 2h & 0 & 2h & \cdots & 0 & 2h \\ 2b_{2,1} & 0 & 2b_{2,2} & 0 & \cdots & \cdots & \vdots \\ 0 & 2h & 0 & 2h & \cdots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \cdots & \vdots \\ 2b_{v,1} & 0 & \cdots & \cdots & \cdots & 2b_{v,v} & 0 \\ 0 & 2h & \cdots & \cdots & \cdots & 0 & 2h \end{bmatrix},$$

where $v = \frac{w}{2}$ and each $b_{i,j}$ is an integer such that $|b_{i,j}| \leq h$. Furthermore,

$$(\tilde{P}^{-1}C\tilde{P})^T(\tilde{P}^{-1}C\tilde{P}) = \begin{bmatrix} 2n & 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 2h^2w & 0 & 2h^2w & \cdots & 0 & 2h^2w \\ 0 & 0 & 2n & 0 & \cdots & \cdots & \vdots \\ 0 & 2h^2w & 0 & 2h^2w & \cdots & \cdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \cdots & \vdots \\ 0 & 0 & \cdots & \cdots & \cdots & 0 & 0 \\ 0 & 2h^2w & \cdots & \cdots & \cdots & 0 & 2h^2w \end{bmatrix}.$$

We now define a $v \times v$ matrix B by $B = (b_{i,j})$. Then $(2B)(2B)^T = (2B)^T(2B) = 2nI_v$. On the other hand, by counting the cardinality of $\{(\alpha_1, t_1) | t_1 \in t^G,\ \alpha_1 \in Fix(t_1),\}$ in two ways, we have $[G : H]|t^G \cap H| = |t^G|f$ since $|Fix(x^{-1}tx) = |Fix(t)|$ for any $x \in G$. It follows that $f = \frac{[G:H]|t^G \cap H|}{|t^G|}$. Thus we have the following.

Theorem 3.5 *Assume that a group G of order $4n$ contains a left Hadamard transversal R with respect to $\langle t \rangle$ satisfying $R \neq xR\ \forall x \in G \setminus \{1\}$. Then R is a $(2n, 2, 2n, n)RDS$ relative to $\langle t \rangle$. If G has a subgroup H satisfying $G = [G, G]H$, $t \in H$ and $t^G \not\subset H$, then there exists a $v \times v$ integral matrix $B = (b_{i,j})$ such that $BB^T = B^TB = \frac{n}{2}I_v$, where $v = \frac{[G:H](|t^G| - |t^G \cap H|)}{2|t^G|}$ and $|b_{i,j}| \leq \frac{1}{2}|H|$.*

As corollaries we have :

Proposition 3.6

Let (G, Ω) be a transitive permutation group of degree $r(> 4)$ and t an involution of G. Suppose that $[G, G]$ is transitive on Ω. If t fixes $r - 4$ points and the square free part of $|G|$ has a prime divisor p such that $p \equiv 3 \pmod 4$, then G has no left Hadamard transversal w.r.t.$\langle t \rangle$ satisfying $R \neq xR\ \ \forall x \in G \setminus \{1\}$.

Proof. Put $|G| = 4n$. By Theorem 3.5, there exists a 2×2 integral matrix B such that $BB^T = \frac{1}{2}nI_2$. Hence a diophantine equation $x^2 + y^2 = \frac{1}{2}n$ has a solution (x, y). Applying a well known result on number theory we have the proposition.

Remark 3.7 *Assume that the square free part of $m!$ has a prime divisor p such that $p \equiv 3 \pmod 4$. By Proposition 3.6, A_m and S_m have no left Hadamard transversal R w.r.t $\langle t \rangle$ satisfying $R \neq xR$ $\forall x \in G \setminus \{1\}$ for any involution t of the form $(i, j)(k, \ell)$.*

By Proposition 3.2 of [2] and Proposition 3.6, we have the following.

Corollary 3.8 *There is no left Hadamard transversal R satisfying $R \neq xR$ $\forall x \in G \setminus \{1\}$ in $A_5, S_5, A_7, S_7, PSL(2,7)$ and $PGL(2,7)$.*

Remark 3.9 *In Theorem 3.5, if we put $H = \langle t \rangle$, then the resulting matrix B is a weighing matrix of weight $\frac{1}{2}n$ and order v unless $G \rhd \langle t \rangle$.*

Acknowledgment

The authors thank A. Watanabe and S. Yoshiara for several helpful comments and suggestions.

References

[1] D. Gorenstein, "Finite Groups," Harper & Row, New York, 1968.

[2] Y. Hiramine, On $(2n, 2, 2n, n)$ relative difference sets, *J. of Combinatorial Theory, Ser. A* **101** (2003), 281-284.

[3] N. Ito and P.S. Kim, On generalized Hadamard subsets, *J. of Algebra* **223** (2000), 601-609.

[4] A. Pott, "Finite Geometry and Character Theory," Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin (1995)

On conjectures of crossed homomorphisms

近畿大学・理工学部　浅井 恒信 (Tsunenobu Asai)
Department of Mathematics, Kinki University

室蘭工業大学　竹ヶ原 裕元 (Yugen Takegahara)
Muroran Institute of Technology

愛媛大学・理学部　庭崎 隆 (Takashi Niwasaki)
Department of Mathematics, Ehime University

1 Introduction

We study some congruences about the number of crossed homomorphisms between two finite groups. Let C, H be finite groups such that C acts on H, and denote by ${}^c h$ this action of $c \in C$ on $h \in H$. We denote $Z^1(C,H)$ for the set of crossed homomorphisms from C to H; i.e.

$$Z^1(C,H) := \{\lambda : C \to H \mid \lambda(cc') = \lambda(c) \cdot {}^c(\lambda(c')) \quad \text{for } c, c' \in C\}.$$

If the action is trivial, then $Z^1(C,H) = \mathrm{Hom}(C,H)$, the set of homomorphisms. Let D be a subgroup of C. For any $\mu \in Z^1(D,H)$, we denote $Z^1(C,H;D,\mu)$ for the set of crossed homomorphisms from C to H whose restriction to D is μ, and denote $\tilde{\mu}(D) := \{\mu(d)d \mid d \in D\}$ which is the subgroup of HC, the semidirect product of H by C, corresponding to μ.

In Asai and Yoshida [2], the following conjectures about the number of homomorphisms and crossed homomorphisms are introduced and their relations are studied.

Conjecture H. Let A and G be finite groups and B a subgroup of A. Then for any homomorphism μ from B to G,

$$|H(A,G;B,\mu)| \equiv 0 \mod \gcd\left(|A/A'B|, |C_G(\mu(B))|\right),$$

where $H(A,G;B,\mu) := \{\lambda \in \mathrm{Hom}(A,G) \mid \lambda_{|B} = \mu\}$ and A' is the commutator subgroup of A.

Conjecture I. Let p be a prime number. Let C be a finite abelian p-group and H a finite p-group such that C acts on H. Then

$$|Z^1(C,H)| \equiv 0 \mod \gcd(|C|, |H|).$$

Theorem 2.1(Asai-Yoshida [2]) *If Conjecture* I *is true, then so is Conjecture* H.

Here, we consider the following conjecture, which is a generalization of Conjecture H and Conjecture I, and prove the following theorem.

Conjecture C. Let C and H be finite groups such that C acts on H and D a subgroup of C. Then for any $\mu \in Z^1(D,H)$,

$$|Z^1(C,H;D,\mu)| \equiv 0 \mod \gcd\left(|C/C'D|, |C_H(\tilde{\mu}(D))|\right),$$

where $C_H(\tilde{\mu}(D)) = C_{HC}(\tilde{\mu}(D)) \cap H$.

Main Theorem: *Conjecture* C *and Conjecture* I *are equivalent.*

Conjecture I has not been proved yet in general, but it holds in several cases. We list some results concerning with Conjecture I, almost which are proved in Asai-Yoshida [2] and Asai-Takegahara [1].

Proposition 1.1 (i) *If C is a cyclic p-group, then Conjecture* I *is true.*
(ii) *If C is an elementary abelian p-group, then Conjecture* I *is true.*
(iii) *If C is a direct product of a cyclic p-group and an elementary abelian p-group, then Conjecture* I *is true.*
(iv) *If H is an abelian p-group, then Conjecture* I *is true.*
(v) *Suppose that the action C on H is defined by a homomorphism from C to H, that is, there exists some $f \in \mathrm{Hom}(C, H)$ such that ${}^c h := f(c)hf(c)^{-1}$. Then Conjecture* I *is true.*
(vi) *If C is a free abelian group, then*

$$|Z^1(C, H)| \equiv 0 \mod |H|.$$

Especially, if C is a free cyclic group, then $|Z^1(C, H)| = |H|$.

In section 2, we explain our counting methods. In section 3, we sketch the outline of the proof of Main Theorem. In Section 4, we apply our methods to prove the following group theoretic results.

Hall's Theorem([4]): *Let H be a finite group and L a subgroup of H. For any $y, z \in H$ and a natural number n,*

$$\#\{x \in LyL \mid x^n = z\} \equiv 0 \mod \gcd(n, |C_L(z)|).$$

Brauer's Lemma([3]): *Let G be a group. Let H be a normal subgroup of finite order n. For any $x \in G$ and $y \in H$, x^n and $(yx)^n$ are conjugate in H.*

2 On counting metods

Let C and H be groups such that C acts on H, D a subgroup of C, and $\mu \in Z^1(D, H)$. In this section, we assume that D is a normal subgroup of C and $|Z^1(C, H; D, \mu)| \neq 0$. First we define an action of C/D on $C_H(\tilde{\mu}(D)) = C_{HC}(\tilde{\mu}(D)) \cap H$.

Definition 2.1 Take any $\lambda \in Z^1(C, H; D, \mu)$ and fix. Then C/D acts on $C_H(\tilde{\mu}(D))$ by ${}^{cD}h := \lambda(c) \cdot {}^c h \cdot \lambda(c)^{-1}$ for $c \in C$ and $h \in C_H(\tilde{\mu}(D))$. For a subgroup K of $C_H(\tilde{\mu}(D))$, we denote $K_{\tilde{\lambda}(C)}$ for the maximal C/D-invariant subgroup of K with this action; i.e.

$$K_{\tilde{\lambda}(C)} := \bigcap_{c \in C} {}^{cD}K = \bigcap_{c \in C} \lambda(c) \cdot {}^c K \cdot \lambda(c)^{-1}.$$

Here C/D acts on $K_{\widetilde{\lambda(C)}}$, and we denote $Z^1_\lambda(C/D, K_{\widetilde{\lambda(C)}})$ for the set of crossed homomorphisms from C/D to $K_{\widetilde{\lambda(C)}}$ with this action; i.e.

$$\begin{aligned} &Z^1_\lambda(C/D, K_{\widetilde{\lambda(C)}}) \\ &\quad := \{\zeta : C/D \to K_{\widetilde{\lambda(C)}} \mid \zeta(c_1c_2D) = \zeta(c_1D) \cdot {}^{c_1D}(\zeta(c_2D)) \quad \text{for } c_1, c_2 \in C\}. \end{aligned}$$

Crossed homomorphisms have the following properties.

Proposition 2.2 *For any $\lambda, \eta \in Z^1(C, H; D, \mu)$, $\eta(c) \in C_H(\widetilde{\mu}(D))\lambda(c)$ for any $c \in C$.*

PROOF: For any $\lambda \in Z^1(C, H; D, \mu)$, we have that $\widetilde{\mu}(D) \trianglelefteq \widetilde{\lambda}(C)$ and so $\lambda(c)c \in N_{HC}(\widetilde{\mu}(D)) \cap Hc$ for any $c \in C$. Here $N_{HC}(\widetilde{\mu}(D)) \cap Hc = C_H(\widetilde{\mu}(D))\lambda(c)c$, so we have that $\eta(c) \in C_H(\widetilde{\mu}(D))\lambda(c)$ for any $c \in C$. □

Proposition 2.3 *Take any $\lambda \in Z^1(C, H; D, \mu)$ and fix. Then there is a one to one correspondence between $Z^1(C, H; D, \mu)$ and $Z^1_\lambda(C/D, C_H(\widetilde{\mu}(D)))$.*

PROOF: By Proposition 2.2, for any $\eta \in Z^1(C, H; D, \mu)$, there is some $\Delta\eta : C \to C_H(\widetilde{\mu}(D))$ such that $\eta(c) = \Delta\eta(c)\lambda(c)$. Then $\Delta\eta \in Z^1_\lambda(C/D, C_H(\widetilde{\mu}(D)))$. Conversely, for any $\zeta \in Z^1_\lambda(C/D, C_H(\widetilde{\mu}(D)))$, we define $\Delta^{-1}\zeta : C \to H$ by $\Delta^{-1}\zeta(c) := \zeta(cD)\lambda(c)$ for $c \in C$. Then $\Delta^{-1}\zeta \in Z^1(C, H; D, \mu)$. These relations give a one to one correspondence between the sets $Z^1(C, H; D, \mu)$ and $Z^1_\lambda(C/D, C_H(\widetilde{\mu}(D)))$. □

Next we define a conjugate action of $C_H(\widetilde{\mu}(D))$ on $Z^1(C, H; D, \mu)$ and two equivalence relations on the set $Z^1(C, H; D, \mu)$.

Definition 2.4 The group $C_H(\widetilde{\mu}(D))$ acts on $Z^1(C, H; D, \mu)$ by conjugation; i.e.

$$\begin{array}{ccccccc} C_H(\widetilde{\mu}(D)) \times Z^1(C, H; D, \mu) & \longrightarrow & Z^1(C, H; D, \mu) & & & & \\ (h, \lambda) & \longmapsto & {}^h\lambda & : & C & \to & H \\ & & & & c & \mapsto & h \cdot \lambda(c) \cdot {}^ch^{-1} = [h, \lambda(c)c] \cdot \lambda(c). \end{array}$$

Definition 2.5 Let K be a subgroup of $C_H(\widetilde{\mu}(D))$. For $\lambda, \eta \in Z^1(C, H; D, \mu)$, we define:

$$\eta \approx_K \lambda \quad \overset{\text{def}}{\Longleftrightarrow} \quad \eta(c) \in K\lambda(c) \quad \text{for all } c \in C$$

and

$$\eta \approxeq_K \lambda \quad \overset{\text{def}}{\Longleftrightarrow} \quad \eta \approx_K {}^k\lambda \quad \text{for some } k \in K.$$

Take any $\lambda \in Z^1(C, H; D, \mu)$ and fix, and we consider the equivalent classes $\{\eta \in Z^1(C, H; D, \mu) \mid \eta \approx_K \lambda\}$ and $\{\eta \in Z^1(C, H; D, \mu) \mid \eta \approxeq_K \lambda\}$.

Proposition 2.6 *Take any $\lambda \in Z^1(C, H; D, \mu)$ and fix. For a subgroup K of $C_H(\widetilde{\mu}(D))$, there is a one to one correspondence between the sets $\{\eta \in Z^1(C, H; D, \mu) \mid \eta \approx_K \lambda\}$ and $Z^1_\lambda(C/D, K_{\widetilde{\lambda(C)}})$.*

PROOF: For any $\eta \in Z^1(C,H;D,\mu)$ such that $\eta \approx_K \lambda$, there is some $\Delta\eta : C \to K$ such that $\eta(c) = \Delta\eta(c)\lambda(c)$. Then we may consider that $\Delta\eta \in Z^1_\lambda(C/D, K_{\tilde{\lambda}(C)})$. Conversely, for any $\zeta \in Z^1_\lambda(C/D, K_{\tilde{\lambda}(C)})$, we define $\Delta^{-1}\zeta : C \to H$ by $\Delta^{-1}\zeta(c) := \zeta(cD)\lambda(c)$ for $c \in C$. Then we have that $\Delta^{-1}\zeta \in Z^1(C,H;D,\mu)$, and $\Delta^{-1}\zeta \approx_K \lambda$. These relations give a one to one correspondence between the sets $\{\eta \in Z^1(C,H;D,\mu) \mid \eta \approx_K \lambda\}$ and $Z^1_\lambda(C/D, K_{\tilde{\lambda}(C)})$. □

Lemma 2.7 *Take any $\lambda \in Z^1(C,H;D,\mu)$ and fix. Let K be a subgroup of $C_H(\tilde{\mu}(D))$ and $k \in K$. Then ${}^k\lambda \approx_K \lambda$ if and only if $k \in K_{\tilde{\lambda}(C)}$.*

Lemma 2.8 *Take any $\lambda \in Z^1(C,H;D,\mu)$ and fix. Let K be a subgroup of $C_H(\tilde{\mu}(D))$. For any $k \in K$, there is a one to one correspondence between $Z^1_\lambda(C/D, K_{\tilde{\lambda}(C)})$ and $Z^1_{k_\lambda}(C/D, K_{\tilde{k_\lambda}(C)})$.*

By classifing the set $\{\eta \in Z^1(C,H;D,\mu) \mid \eta \approxeq_K \lambda\}$ by $\approx_K$, we have the following propoition.

Proposition 2.9 *Take any $\lambda \in Z^1(C,H;D,\mu)$ and fix. For a subgroup K of $C_H(\tilde{\mu}(D))$,*

$$\#\{\eta \in Z^1(C,H;D,\mu) \mid \eta \approxeq_K \lambda\} = (K : K_{\tilde{\lambda}(C)}) \cdot |Z^1_\lambda(C/D, K_{\tilde{\lambda}(C)})|.$$

3 Proof of Main Theorem

Here we sketch the outline of the proof of Main Theorem. First we introduce Conjecture II, and show that Conjectures C and II are equivalent and Conjectures II and I are equivalent.

Conjecture II: Let C be an abelian p-group and H a finite group such that C acts on H. Then

$$|Z^1(C,H)| \equiv 0 \mod \gcd(|C|, |H|).$$

Step 1 *Conjecture* C *and* II *are equivalent.*

PROOF: We prove that if Conjecture II is true, then so is Conjecture C. We asuume that Conjecture II is true. If the statement

$$|Z^1(C,H;D,\mu)| \equiv 0 \mod \gcd(|C/C'D|_p, |C_H(\tilde{\mu}(D))|),$$

holds for any prime p, then Conjecture C holds. Let E be a subgroup of C such that $C'D \leq E \leq C$ and $(C : E) = (C : C'D)_p$. $C_H(\tilde{\mu}(D))$ acts on $Z^1(E,H;D,\mu)$ by conjugation, i.e.

$$\begin{array}{ccc} C_H(\tilde{\mu}(D)) \times Z^1(E,H;D,\mu) & \longrightarrow & Z^1(E,H;D,\mu) \\ (h,\eta) & \longmapsto & ({}^h\eta : e \mapsto h \cdot \eta(e) \cdot {}^eh^{-1}). \end{array}$$

Thus

$$\begin{aligned} |Z^1(C,H;D,\mu)| &= \sum_{\eta \in Z^1(E,H;D,\mu)} |Z^1(C,H;E,\eta)| \\ &= \sum_{\eta \in Z^1(E,H;D,\mu)/\sim_{C_H(\tilde{\mu}(D))}} (C_H(\tilde{\mu}(D)) : C_{C_H(\tilde{\mu}(D))}(\tilde{\eta}(E))) \cdot |Z^1(C,H;E,\eta)| \end{aligned}$$

Here E is a normal subgroup of C and C/E is an abelian p-group, so we have that

$$\begin{aligned}
&(C_H(\tilde{\mu}(D)) : C_{C_H(\tilde{\mu}(D))}(\tilde{\eta}(E))) \cdot |Z^1(C, H; E, \eta)| \\
&\quad \equiv 0 \bmod (C_H(\tilde{\mu}(D)) : C_{C_H(\tilde{\mu}(D))}(\tilde{\eta}(E))) \cdot \gcd(|C/E|, |C_H(\tilde{\eta}(E))|) \\
&\quad \equiv 0 \bmod \gcd(|C/C'D|_p, |C_H(\tilde{\mu}(D))|) .
\end{aligned}$$

□

Step 2 *Conjecture* II *and* I *are equivalent.*

PROOF: We asuume that Conjecture I is true. Let K be a Sylow p-subgroup of H. We classify $Z^1(C, H)$ by $\approx_K$, and each equivalence class satisfies that

$$\#\{\eta \in Z^1(C, H) \mid \eta \approx_K \lambda\} = (K : K_{\tilde{\lambda}(C)}) \cdot |Z^1_\lambda(C, K_{\tilde{\lambda}(C)})|.$$

Here $K_{\tilde{\lambda}(C)}$ is a p-group, so we have that

$$\begin{aligned}
\#\{\eta \in Z^1(C, H) \mid \eta \approx_K \lambda\} &\equiv 0 \bmod (K : K_{\tilde{\lambda}(C)}) \cdot |Z^1_\lambda(C, K_{\tilde{\lambda}(C)})| \\
&\equiv 0 \bmod (K : K_{\tilde{\lambda}(C)}) \cdot \gcd\left(|C|, |K_{\tilde{\lambda}(C)}|\right) \\
&\equiv 0 \bmod \gcd(|C|, |K|) \\
&\equiv 0 \bmod \gcd(|C|, |H|_p) \\
&\equiv 0 \bmod \gcd(|C|, |H|) .
\end{aligned}$$

Hence we have that

$$|Z^1(C, H)| \equiv 0 \qquad \bmod \gcd(|C|, |H|) .$$

□

4 Some applicatins

Hall's Theorem([4]): *Let H be a finite group and L a subgroup of H. For any $y, z \in H$ and a natural number n,*

$$\#\{x \in LyL \mid x^n = z\} \equiv 0 \mod \gcd(n, |C_L(z)|).$$

PROOF: Let $LyL = \bigcup_i C_L(z) y_i C_L(z)$ be a double coset decomposition, and we set $\mathcal{X} := \{x \in LyL \mid x^n = z\}$ and $\mathcal{X}_i := \{x \in C_L(z) y_i C_L(z) \mid x^n = z\}$. Then $\mathcal{X} = \bigcup_i \mathcal{X}_i$, and we show that each $|X_i|$ is congruent to 0 mod $\gcd(n, |C_L(z)|)$.

Let m be the order of z. Let $C = \langle c \rangle$ be a cyclic group of order mn, $D = \langle c^n \rangle$ be a subgroup of order m and $\mu \in \mathrm{Hom}(D, H)$ such that $\mu(c^n) = z$. Here note that $C_L(\mu(D)) = C_L(z)$ and we set $K := C_L(\mu(D))$.

We assume that $|X_i| \neq 0$, and take any $x \in X_i$. There exists $\lambda \in H(C, H; D, \mu)$ such taht $\lambda(c) = x$. Then the sets $\mathcal{X}_i$ and $\mathcal{Y} := \{\eta \in H(C, H; D, \mu) \mid \eta(c) \in K\lambda(c)K\}$ are bijective. Here note that $K\lambda(c)K = Ky_iK$. Then

$$\mathcal{Y} = \bigcup_{\lambda_i \in \mathcal{Y}/\approx_K} \{\eta \in H(C, H; D, \mu) \mid \eta \approx_K \lambda_i\}$$

and

$$\begin{aligned}\#\{\eta \in H(C,H;D,\mu) \mid \eta \approx_K \lambda_i\} &= (K : K_{\widetilde{\lambda_i(C)}}) \cdot |Z^1_{\lambda_i}(C/D, K_{\widetilde{\lambda_i(C)}})| \\ &\equiv 0 \mod (K : K_{\widetilde{\lambda_i(C)}}) \cdot \gcd(|C/D|, |K_{\widetilde{\lambda_i(C)}}|) \\ &\equiv 0 \mod \gcd(|C/D|, |K|)\end{aligned}$$

So we have that

$$|\mathcal{X}_i| = |\mathcal{Y}| \equiv 0 \mod \gcd(n, |C_L(z)|).$$

Brauer's Lemma([3]): *Let G be a group. Let H be a normal subgroup of finite order n. For any $x \in G$ and $y \in H$, x^n and $(yx)^n$ are conjugate in H.*

PROOF: We fix $x \in G$ and $y \in H$. Let $C = \langle c \rangle$ be a free cyclic group and $D = \langle c^n \rangle$ the subgroup of index n. We define an action of C on H by ${}^c h := xhx^{-1}$ for $h \in H$. Because C is a free cyclic group $|Z^1(C,H)| = |H|$.

$$\begin{aligned}|Z^1(C,H)| &= \sum_{\mu \in Z^1(D,H)} |Z^1(C,H;D,\mu)| \\ &= \sum_{\mu \in Z^1(D,H)/\sim_H} (H : C_H(\tilde{\mu}(D))) \cdot |Z^1(C,H;D,\mu)| \\ &\geq (H : C_H(D)) \cdot |Z^1(C,H;D,0_D)| \neq 0.\end{aligned}$$

where 0_D is a zero map from D to H. Because by Proposition 2.3 and C/D is cyclic, we have that

$$(H : C_H(D)) \cdot |Z^1(C,H;D,0_D)| \equiv 0 \mod \gcd(|C/D|, |H|)$$

So we have that

$$|Z^1(C,H)| = (H : C_H(D)) \cdot |Z^1(C,H;D,0_D)| = |H|$$

For any crossed homomorphism in $Z^1(C,H)$, whose restriction to D is conjugate to 0_D. We define

$$\begin{array}{rccc} \lambda : & C & \to & H \\ & c & \mapsto & y \end{array}$$

then $\lambda \in Z^1(C,H)$, and there exists some $h \in H$ such that $\lambda(c^n) = {}^h 0_D(c^n)$. Hence we have $\lambda(c^n)c^n = {}^h 0_D(c^n)c^n$, and so $(\lambda(c)c)^n = hc^n h^{-1}$ in HC. We define

$$\begin{array}{rccc} \varphi : & HC & \to & G \\ & yc^i & \mapsto & yx^i \end{array}$$

then φ is a group homomorphism. Consider the image of φ we have that $(yx)^n = hx^n h^{-1}$ in G.

References

[1] T. Asai and Y. Takegahara, On the number of crossed homomorphisms, *Hokkaido Math. J.* **28** (1999), 535–543.

[2] T. Asai and T. Yoshida, $|\mathrm{Hom}(A, G)|$, II, *J. Algebra* **160** (1993), 273–285.

[3] R. Brauer, On a theorem of Frobenius, *American Math. Monthly* **76** (1969), 12–15.

[4] P. Hall, On a theorem of Frobenius, *Proc. London Math. Soc.* (2) **40** (1935), 468–501.

Eigenvalues and elementary divisors of Cartan matrices of cyclic blocks and tame blocks

東京農工大学　工学部　和田倶幸　(Tomoyuki Wada)

1 Introduction

G を有限群, F を標数 $p>0$ の代数的閉体とし, B を FG の block でその defect group を D, 位数を $|D|=p^d$ とする. $l=l(B)$ を B に含まれる既約 Brauer (modular) 指標の個数とする. B のカルタン行列 $C_B=(c_{ij})$ とは, $l\times l$ 行列で, 各成分 c_{ij} は B に属する既約 $FG-$ 加群 S_j が i 番目の projective indecomposable $FG-$ 加群 P_i の中に組成因子として現れる重複度を表す. $\rho(B)$ を C_B の Frobenius-Perron 固有値 (i.e. 最大固有値) とする. $R=R_B$ を C_B の固有値の全体, 同様に $E=E_B$ を C_B の ($\mathbf{Z}-$) 単因子の全体の集合とする. カルタン行列の固有値, とくに Frobenius-Perron 固有値 $\rho(B)$ の性質に興味を持って調べてきた. $\rho(B)$ がどのようなときに整数になるかを考えると, 単因子との関係が現れてくる. [KW] や [KMW] ではいくつかの場合に $\rho(B)$ の整数性が他の固有値の整数性を支配していて, これは一般の群でも成り立つのではないかと思われた. またさらに具体的な群のカルタン行列の固有値を計算すると, C_B の固有値のある部分集合と C_B の単因子のある部分集合同志の間にうまく対応がつくのではないかと思われる. ここではこの新しい予想を述べ, それが $l\leq 5$ のときの cyclic block と tame block で成り立つことを報告した.

2 Questions and facts

$\rho(B)$ は一般には整数とは限らない. また $\rho(B)$ と $|D|$ の大小関係も一般にはどちらが大きいとは限らない. むしろ整数になるのは特別な意味があるように思われる. 一方単因子については良く知られている. 最大の単因子はちょうど $|D|$ に一致して, 他の単因子はそれより真に小さな p のべきである. [KW], [KMW] では次のような Question を得た.

Q1(KMW). $\rho(B)\in\mathbf{Z}\Longrightarrow\rho(B)=|D|$?

Q2(KMW). $\rho(B) = |D| \Longrightarrow R = E$?

Q1, Q2 については次の場合には正しいことが確かめられている.

Fact 1(KW, KMW). If D is a normal subgroup of G, then $\rho(B) = |D|$ and $R = E$.

Fact 2(KW, KMW). If D is cyclic, then Q1 and Q2 are true.

Fact 3(KW, KMW). If B is tame (i.e. $p = 2, D \simeq$ dihedral, semidihedral or generalized quaternion), then Q1 and Q2 are true.

Fact 2,3 ではさらに強く $\rho(B) \in \mathbf{Z}$ ならば B とその Brauer 対応子 b は Morita 同値になる. しかしこれは一般には成り立たない. 可解群で反例がある.

Fact 4(KMW). If G is p-solvable, then Q2 is true. If G is p-solvable and $l = 2$, then Q1 is true.

G が p-solvable のときは Q1 はまだ証明されていない. また単純群などでカルタン行列が知られていて, l が小さいときは実験した結果今のところ Q1, Q2 は正しいようである.

3 Conjectures

[KW] を書いたころ Q1 に関して, 清田はすでに次が成り立つのではないかと予想している.

Conjecture(Kiyota). $|D| \mid N(\rho(B))$, where $N(\rho(B))$ is the norm of $\rho(B)$ (i.e. the product of all algebraic conjugates of $\rho(B)$).

もしこの予想 (K) が正しいなら, Q1 は正しい. どうしてかというと, [KW] により一般に, C_B の固有値 ρ は代数的整数として $|D|$ を割る (i.e. ある代数的整数 λ があって $\rho \cdot \lambda = |D|$ をみたす). すると, もし $\rho(B)$ が整数ならば, $N(\rho(B)) = \rho(B)$ で上の注意より $\rho(B) \mid |D|$. そこで予想 (K) が正しいならば, 逆に $|D| \mid \rho(B)$ となって $\rho(B) = |D|$.

いろいろな例を調べるとさらに強い次のことが言えるのではないかと思われるようになった. これは C_B の固有値と単因子との間に, より explicit な関係が存在するこ

とを主張している.

Let $f_B(x)$ be the characteristic polynomial of C_B. Let $f_B = f_1 \cdot f_2 \cdots f_r$ be a Z-irreducible decomposition of $f_B(x)$. Let $R_i := \{\rho_{i1}, \cdots, \rho_{in_i}\}$, $1 \leq i \leq r$ be the set of all roots of $f_i(x)$. So we denote and write as $R = \{\rho_{11}, \cdots, \rho_{1n_1}\ ;\ \rho_{21}, \cdots, \rho_{2n_2}\ ;\ \cdots\ ;\ \rho_{r1}, \cdots, \rho_{rn_r}\}$. Then for each i, $N(\rho_{ij}) = \prod_{k=1}^{n_i} \rho_{ik} = |f_i(0)|$ for any $j = 1, 2, \cdots n_i$.

Conjecture. There is a decomposition $E = E_1 \sqcup \cdots \sqcup E_r$ such that the following three conditions are satisfied.

(i) $|R_i| = |E_i|$ for $1 \leq i \leq r$.

(ii) Let $E_i = \{e_{i1}, \cdots, e_{in_i}\}$, then $\prod_{k=1}^{n_i} e_{ik} = N(\rho_{ij})$.

(iii) Let $\rho(B) \in R_1$. Then $|D| \in E_1$. In particular, $|D| \mid N(\rho(B))$.

注1 (ii) が正しければ, もし固有値が整数ならば, それは単因子と一致する. (iii) が正しいとすると, $\rho(B)$ が整数ならば $\rho(B) = |D|$ である.

注2 発表したときは, $\rho(B) \in R_1$ ならば, $\deg f_1 \geq \deg f_i$ for all i も成り立つのではないかと主張した. もしこれがいえれば, Q2 がいえるので. しかしその後この主張には反例があることが判明した. それは, $G = SL(2,32)$ と $Sz(32), p = 2, B$: principal block の場合で, いずれも $l = 31$ で $f_B(x) = f_1(x) \cdot (f_2(x))^2$ となる. ここで $\deg f_1 = 7$ だが $\deg f_2 = 12$ となっている.

例1 $G = S_6, p = 3, B : principal, |D| = 9$

$$C_B = \begin{pmatrix} 4 & 2 & 1 & 1 & 2 \\ 2 & 4 & 2 & 2 & 1 \\ 1 & 2 & 4 & 1 & 2 \\ 1 & 2 & 1 & 3 & 2 \\ 2 & 1 & 2 & 2 & 4 \end{pmatrix}, \quad f_B(x) = (x^3 - 13x^2 + 29x - 9)(x-3)^2, \quad N(\rho(B)) = 9$$

$R = \{\rho(B) = \rho_{11}, \rho_{12}, \rho_{13}; 3; 3\}$

$E = \{9, 1, 1; 3; 3\}$

4 cyclic block with $l \leq 5$

ここでは cyclic defect group D をもつ block B で $l = l(B) \leq 5$ のときに予想が成り立つことの概略を示す. 予想を一般の cyclic block について証明することは難しく, $l \leq 5$ の場合をやっても今のところ見通しがたたない.

B を cyclic defect group D をもつ G の block とし, $T(B)$ を B の Brauer tree とする. $m \geq 1$ を $T(B)$ の exceptional vertex の multiplicity とする. $l = l(B)$ は $T(B)$ の辺の本数である. このとき $lm+1 = |D|$, $l \mid p-1$, また C_B の単因子は $|D|$ とそれ以外はすべて 1 (したがって $\det C_B = |D|$) であることが知られている.

Theorem 1. *Let B be a cyclic block of FG. If $l(B) \leq 5$, then Conjecture is true. Furthermore, if $\rho(B) \in R_1$, then $\deg f_1 \geq \deg f_i$ for all $1 \leq i \leq r$ under the above notation.*

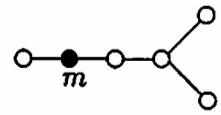
Sketch of proof. $l = 1$ のときは明らか. $l = 2$ のときは Fact 2 より明らか. したがって $l = 3,4,5$ のときに確かめればよい. また $p = 2$ ならば $l = 1$ より p は odd としてよい. 実は数式処理ソフト MAPLE で計算すると, parameter を 1 個含んでいても固有多項式や固有値の計算をしてくれる (単因子の計算はしてくれないが). 固有多項式の因子の既約性にやや疑問があるものの, 単因子が $|D|$ と 1 のみと分かっているので, これを信用してしまえば結論は出る. しかしそれではあまりにも見通しが無い. やはり大変でも手で計算することにした. 基本方針は次のようにする. なおこの方法は熊本大の渡辺アツミさんの示唆によるところが大きい.

(I) Z-基本変形を用いて特性行列 $C_B - xI$ を変形し, できるだけ 3 角行列に近い形にして $f_B(x)$ を特定し, 分解して, 単因子との関係も見る.
(II) 各因子 $f_i(x)$ が実際に Z-既約であることを証明する.

ここで Z-基本変形とは, (a) 2 つの行, 列の入れ替え, (b) ある行, 列を Z-多項式倍して他の行, 列に加える, (c) ある行, 列を ± 1 倍する の 3 種類の変形をいう. この変形でほとんどの場合, 3 角行列にまで変形できるが, だめな場合もあり, そのときは (c′) ある行, 列を 0 でない Z-倍する, ことを最後の手段として許す. ただしこのときは単因子が変形していないかどうかに注意する.

まず Brauer tree の形を exceptional vertex の位置を含めて分類する. (1) $l = 3$ のとき 4 通りの場合, (2) $l = 4$ のとき 8 通りの場合, (3) $l = 5$ のとき 2 0 通りの場合がある.

例として (3.2.4) のときをやってみる. Brauer tree は,



で, このときカルタン行列は $C_B = \begin{pmatrix} m+1 & m & 0 & 0 & 0 \\ m & m+1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 \end{pmatrix}$ となる.

(I) $C_B - xI = \begin{pmatrix} \alpha+m-1 & m & 0 & 0 & 0 \\ m & \alpha+m-1 & 1 & 0 & 0 \\ 0 & 1 & \alpha & 1 & 1 \\ 0 & 0 & 1 & \alpha & 1 \\ 0 & 0 & 1 & 1 & \alpha \end{pmatrix}$, $\alpha = 2 - x$.

特性行列 $C_B - xI$ を Z 基本変形で次の形にまで変形できる.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha+m-1 & m(\alpha-1) \\ 0 & 0 & 0 & -(\alpha-1)^2(\alpha+2) & (1-\alpha)(1-\alpha^3+4\alpha-2) \end{pmatrix}$$

ここで5行目を m 倍し, Z 基本変形を続けると,

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & m(\alpha-1) & \alpha+m-1 \\ 0 & 0 & 0 & 0 & -g_B(\alpha) \end{pmatrix}$$

となり, 最後に両辺の determinant を m で割ると $f_B(x) = g_B(x)(x-1), g_B(x) = x^4 - (2m+7)x^3 + (12m+14)x^2 - (17m+9)x + (5m+1)$ を得る. また左右からかけた変形行列の x に 0 を代入すれば, 単因子の一意性から (Z)-単因子をも得る.

(II) $g_B(x)$ の Z 既約性

(1) 1次式を因子にもたないことは, もし $g_B(x)$ が $\lambda = p^i$ を根にもつとして

(i) $i>0$ のとき　$\cdots f_B(p^i)=0$ の式の p^i の係数を見ると分かる.
(ii) $i=0$ のとき $g_B(1)=0$ から矛盾が出る.

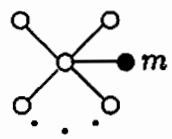
(2) 2次式 × 2次式にならないことは, もし分解するとして係数の関係から矛盾を出す.

結論 $f_B(x)=\{x^4-(2m+7)x^3+(12m+14)x^2-(17m+9)x+(5m+1)\}(x-1)$.
$R=\{\rho(B)=\rho_{11},\rho_{12},\rho_{13},\rho_{14};1\}$,　$N(\rho(B))=|D|$.
$E=\{|D|,1,1,1;1\}$.

なおこの議論で使うことは, (i) 固有値 $\rho\in\mathbf{Z}\Longrightarrow\rho=p^i$ for $1\leq i\leq d$, (ii) このとき $i=d\Longrightarrow R=E$ (Fact 2), 従ってこのときは特に 1 を固有値にもたねばならない, (iii) $l=5(\text{odd})\Longrightarrow m=\text{even}$ などである.

l が一般的な場合の結果として

(1) Brauer tree が



のときは　$C_B=\begin{pmatrix} 2 & 1 & \cdots & \cdots & \cdots & 1 \\ 1 & 2 & 1 & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & 1 & 2 & 1 \\ 1 & \cdots & \cdots & \cdots & 1 & m+1 \end{pmatrix}$　となる. すると

$C_B-xI=\begin{pmatrix} \alpha & 1 & \cdots & \cdots & \cdots & 1 \\ 1 & \alpha & 1 & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & 1 & \alpha & 1 \\ 1 & \cdots & \cdots & \cdots & 1 & \alpha+m-1 \end{pmatrix}$　よりこれを変形すると最終的に

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1-\alpha & 0 & 0 & & & \vdots \\ \vdots & 1-\alpha & 1-\alpha & 0 & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 1-\alpha & 1-\alpha & \cdots & 1-\alpha & 0 & 0 \\ 0 & 1-\alpha & 1-\alpha & \cdots & \cdots & 1-\alpha & m-1 \\ 0 & * & * & \cdots & * & 0 & (1-\alpha)(\alpha+l-1)-(m-1)(\alpha+l-2) \end{pmatrix}$$

より

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1-\alpha & 0 & 0 & & & \vdots \\ \vdots & 1-\alpha & 1-\alpha & 0 & \ddots & & \vdots \\ \vdots & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & 1-\alpha & 1-\alpha & \cdots & 1-\alpha & 0 & 0 \\ 0 & * & * & \cdots & * & (1-\alpha)(\alpha+l-1)-(m-1)(\alpha+l-2) & 0 \\ 0 & 1-\alpha & \cdots & \cdots & 1-\alpha & m-1 & 1-\alpha \end{pmatrix}$$

という3角行列を得る.

したがって $f_B(\alpha)=(1-\alpha)^{l-2}\{(1-\alpha)(\alpha+l-1)-(m-1)(\alpha+l-2)\}$ より

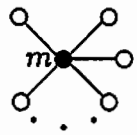
$f_B(x)=(x-1)^{l-2}\{x^2-(m+l+1)x+(ml+1)\}$ を得る.

Lemma. *If $m>1$, then $g_B(x)=x^2-(m+l+1)x+(ml+1)$ is $\mathbf{Z}$-irreducible. Then in this case, the set of eigenvalues of $C_B=\{\rho(B)=\rho_1,\rho_2;\ 1\ ;\ \cdots\ ;\ 1\}$ and the set of elementary divisors $=\{|D|,1;\ 1\ ;\ \cdots\ ;\ 1\}$.*

Proof. Let $m>1$. Suppose $g_B(x)$ is reducible. Then $g_B(x)$ decomposes into two factors of degree one. Therefore $\rho(B)$ must be an integer, and so another root of $g_B(x)$ must be 1. Then $g_B(x)=(x-1)(x-(ml+1))=x^2-(ml+2)x+(ml+1)$. Hence, $ml+2=l+m+1$. This implies $(l-1)(m-1)=0$. This contradicts $l>1$ and $m>1$.

If $m=1$, $g_B(x)=x^2-(p^d+1)x+p^d=(x-1)(x-p^d)$. In this case,

$f_B(x) = (x-1)^{l-1}(x-p^d)$.

(2) Brauer tree が 

のときは $f_B(x) = (x-1)^{l-1}(x-p^d)$ となり $R = E$ である [K-M-W].

注3 $l(B) = 6$ のときは Brauer tree の種類は 53 通りとなり, 手で確かめるのは容易でない.

5 Tame blocks

Theorem 2 *Let B be a tame block of FG with defect group D of order 2^n (i.e. $p = 2$ and D is isomorphic to dihedral, generalized quaternion or semidihedral). Then Conjecture is true. Furthermore, if $\rho(B) \in R_1$, then $\deg f_1 \geq \deg f_i$ for all $1 \leq i \leq r$ under the notation of §4.*

Skect of proof. tame のときは $l = l(B) = 1, 2, 3$ となるが, Fact 3 より $l = 3$ のときに確かめればよい. また Erdmann [E] により次の 1 2 の場合に確かめればよい.

(i) D : dihedral のとき $D(3A)_1, D(3B), D(3K)$
(ii) D : generalized quaternion のとき $Q(3A)_2, Q(3B), Q(3K)$
(iii) D : semidihedral のとき $SD(3A)_1, SD(3B)_1, S(3B)_2, SD(3C)_2, SD(3D), SD(3H)$

いずれも parameter を 1 個含むが, 3 次行列なので単因子の計算も楽である. cyclic block と違い単因子に 2 が現れる場合もある. $f_B(x)$ の因子の **Z**-既約性の証明も, cyclic の場合と同様である. いくつか結論だけ述べる.

Example. $D(3K)$ $\quad C_B = \begin{pmatrix} 2 & 1 & 1 \\ 1 & c+1 & c \\ 1 & c & c+1 \end{pmatrix}$, where $c = 2^{n-2} \geq 1$.

$f_B(x) = x^3 - (2c+4)x^2 + (6c+3)x - 4c = (x^2 - (2c+3)x + 4c)(x-1)$,
$N(\rho(B)) = |D|$.

(a) If $c = 1$, then $f_B(x) = (x-4)(x-1)^2$.
$R = E = \{|D|; 1; 1\}$.

(b) If $c > 1$, then $g_B(x) = x^2 - (2c+3)x + 4c$ is $\mathbf{Z}$-irreducible, and $N(\rho_B) = |D|$.
$R = \{\rho_B = \rho_1, \rho_2; 1\}$, where ρ_is are algebraically conjugate for $1 \leq i \leq 2$.
$E = \{|D|, 1; 1\}$.

Example. $SD(3A)_1$ $\quad C_B = \begin{pmatrix} 4k & 2k & 2k \\ 2k & k+1 & k \\ 2k & k & k+2 \end{pmatrix}$, where $k = 2^{n-2}, n \geq 4$.
$f_B(x) = x^3 - (6k+3)x^2 + (15k+2)x - 8k$.
$f_B(x)$ is $\mathbf{Z}$-irreducible, and $N(\rho_B) = 2|D|$.
$R = \{\rho_B = \rho_1, \rho_2, \rho_3\}$, where ρ_is are algebraically conjugate for $1 \leq i \leq 3$.
$E = \{|D|, 2, 1\}$.

Example. $Q(3B)$ $\quad C_B = \begin{pmatrix} 8 & 4 & 4 \\ 4 & s+2 & 2 \\ 4 & 2 & 4 \end{pmatrix}$, where $s = 2^{n-2} \geq 2$.
$f_B(x) = x^3 - (s+14)x^2 + (12s+20)x - 16s$.

(a) If $s = 2$, then $f_B(x) = (x^2 - 14x + 16)(x-2)$
$R = \{\rho_B = \rho_1, \rho_2; 2\}$, where ρ_is are algebraically conjugate for $1 \leq i \leq 2$ and $N(\rho_B) = 2|D|$.
$E = \{|D|, 2; 2\}$.

(b) If $s > 2$, then $f_B(x)$ is $\mathbf{Z}$-irreducible.
$R = \{\rho_B = \rho_1, \rho_2, \rho_3\}$, where ρ_is are algebraically conjugate for $1 \leq i \leq 3$ and $N(\rho_B) = 4|D|$.
$E = \{|D|, 2, 2\}$.

References

[E] K. Erdmann, "Blocks of Tame Representation Type and Related Algebras", Springer Lecture Notes, vol. 1428, Springer-Verlag, Berlin/New York, 1990.

[KMW] M. Kiyota, M. Murai and T. Wada, Rationalty of eigenvalues of Cartan matrices in finite groups, Jour. Algebra 249 (2002), 110-119.

[KW] M. Kiyota and T. Wada, Some remarks on eigenvalues of the Cartan matrix in finite groups, Comm. Algebra 21, vol.21 (1993), 3839-3860.

Crossed Burnside rings for some families of subgroups of a finite group

小田 文仁 (Fumihito Oda)
富山工業高等専門学校一般科目

1 はじめに

有限群の表現論における様々な誘導定理を公理論的に考察するための道具として研究された Mackey functor ([Bo97], [We00]) は，その射全体から構成される Mackey algebra [TW95] の上の加群とみなすことができる．Mackey algebra の中心の部分環にはこの理論でもっとも基本的な可換環である Burnside ring [Bo00] と Yoshida により導入された crossed Burnside ring [OY01] がある．Bouc は p-局所環上の crossed Burnside ring のべき等元公式を導き，さらにそれを応用し，Mackey algebra の中心のべき等元公式を導いた [Bo01]．本稿は Bouc の仕事を別の角度から導くことをめざすために始められた，ある条件をみたす部分群の族から構成される crossed Burnside ring に関する Yoshida との共同研究の入り口に関する報告である．Yosida による generalized Burnside ring の理論 [Yo90] が基礎になっている．

2 Crossed Burnside rings

(2.1) Category $(G,\mathcal{X})$-xset/S. 有限群 G の部分群の族 $\mathcal{X}$ は条件「$H \in \mathcal{X} \Rightarrow {}^gH \in \mathcal{X}$ for any $g \in G$」を満たすものとする．モノイド S は，以下の条件をみたす G の作用が存在するとき **G-monoid** と呼ぶ:

$$G \times S \longrightarrow S;\ (g,s) \longmapsto {}^gs,$$
$${}^{gh}s = {}^g({}^hs),\ {}^1s = s;\ {}^g(st) = {}^gs \cdot {}^gt,\ {}^g1 = 1 \quad \text{for } s,t \in S, g,h \in G.$$

本稿では S に有限性を仮定する．G 自身は共役の作用で G-monoid になるが，それを特に G^c で表す．有限 G-集合 X は G-map $\|\cdot\| : X \longrightarrow S; x \longmapsto \|x\|$. が存在するとき **crossed G-set** (over S) と呼ぶ．$\|\cdot\|$ を **weight function** と呼ぶ．$s \in S$ に対し $X[s] = \{s \in X \mid \|x\| = s\}$ を crossed G-set X の *s-component* と呼ぶ．$g \in G$ と $s \in S$ に対し $gX[s] = X[{}^gs]$ が成り立つ．特に $s \in S$ の stabilizer G_s は $X[s]$ に作用する．従って crossed G-set X は G 集合として S-次数付きの直和 $X = \coprod_{s \in S} X[s]$ に分解される．Crossed G-集合 X は，各元 $x \in X$ に対して安定化群 G_x がすべて $\mathcal{X}$ に含まれるとき **crossed $(G,\mathcal{X})$-集合**と呼ぶ．二つの crossed $(G,\mathcal{X})$-集合 X, Y の間の G-写像 $f : X \to Y$ は weight を保つとき，すなわち $\|f(x)\| = \|x\|$ for all $x \in X$ を満たすとき，**crossed $(G,\mathcal{X})$-map** と呼ぶ．X から Y への crossed G-maps 全体を $\mathrm{XMap}_{G,\mathcal{X}}(X,Y)$ で表す．有限 crossed $(G,\mathcal{X})$-集合と crossed G-maps 全体の圏を $(G,\mathcal{X})$-xset/S で表す．S 上の crossed $(G,\mathcal{X})$-集合 X, Y の **tensor product** は集合としては直積 $X \otimes Y = X \times Y$, weight function を $g(x,y) = (gx,gy)$, $\|(x,y)\| = \|x\| \cdot \|y\|$ $(g \in G, x \in X, y \in Y)$ として定義される．一般に $X \otimes Y$ は crossed $(G,\mathcal{X})$-set になるとは限らない．$\mathcal{X}$ が intersection に関して閉じているならば $X \otimes Y$ は crossed $(G,\mathcal{X})$-set になる．圏 $(G,\mathcal{X})$-xset/S の disojoint union に関する Grothendieck group を $X\Omega(G,\mathcal{X},S)$ で表す．部分群 $H \leq G$ に対して S における H の **centralizer** $C_S(H) := \{s \in S \mid {}^hs = s \quad \forall h \in H\}$ は，$WH := N_G(H)/H$ が monoid の自己同型として作用する S の submonoid である．部分群 $H \in \mathcal{X}$ による transitive G-集合 G/H は weight function を

$\|gH\| = {}^g s, (s \in C_S(H))$ と定めることにより，crossed $(G,\mathcal{X})$-set になるが，これを **transitive crossed** $(G,\mathcal{X})$**-set** と呼び $(G/H)_s$ と表す．すべての crossed $(G,\mathcal{X})$-sets は transitive crossed $(G,\mathcal{X})$-sets の直和に一意的に分解される ([OY01] (2.13)) ので，$X\Omega(G,\mathcal{X},S)$ は次のような free $\mathbb{Z}$-basis をもつ：$\{(G/D)_s | D \in C(\mathcal{X}),\ s \in [C_S(D)]_G\}$．$X\Omega(G,\mathcal{X},S)$ が crossed Burnside ring $X\Omega(G,S)$ の部分環になるための必要十分条件は $\mathcal{X}$ が intersection について閉じていて $G \in \mathcal{X}$ が成り立つことである．

(2.2) EXAMPLE. $G = S_3 = \langle t = (1,2),\ s = (1,2,3)\rangle$, $\mathcal{X} = \{1,\ C := \langle t\rangle,\ \langle st\rangle,\ \langle s^2t\rangle\}$ とするときすべての transitive crossed $(G,\mathcal{X})$-sets は同型を度外視して $(G/1)_1$, $(G/1)_t$, $(G/1)_s$, $(G/C)_1$, $(G/C)_t$ である． □

(2.3) Crossed ghost rings. Monoid S の semigroup algebra $\mathbb{Z}[S]$ は G-basis S の permutation G-module である．$\mathbb{Z}[C_S(H)]$ は S の中心 $Z[S]$ の WH の作用を持つ部分環である．G は直積の環 $\Xi(G,\mathcal{X}) := \prod_{H\in\mathcal{X}} \mathbb{Z}[C_S(H)]$ に環の自己同型として右から

$$\xi^g := \left(\sum_{s\in C_S(H)} \xi({}^gH, {}^gs)s\right)_H \quad \text{for} \quad \xi = \left(\sum_{s\in C_S(H)} \xi(H,s)s\right)_H \quad \text{and} \quad g \in G$$

により作用する．$\Xi(G,\mathcal{X})$ の G-固定点全体からなる部分環を **crossed ghost ring with respect to** $\mathcal{X}$ と呼び，$X\tilde{\Omega}(G,\mathcal{X},S)$ で表す．以下の等式が成り立つ．

$$X\tilde{\Omega}(G,\mathcal{X},S) \;=\; \left(\prod_{H\in\mathcal{X}} \mathbb{Z}[C_S(H)]\right)^G \cong \prod_{(H)\in C(\mathcal{X})} \mathbb{Z}[C_S(H)]^{WH}.$$

(2.4) EXAMPLE. (2.2) のもとで $\hat{s} = s + s^{-1}$, $\hat{t} = t + st + s^2t$ とおくとき，$X\tilde{\Omega}(G,\mathcal{X},S)$ の基底は以下のようになる：

P	1	C
CP	G	C
NP	G	C
$\dim K[CP]^{WP}$	3	2
basis	$1,\ \hat{t},\ \hat{s}$	$1,\ t$

□

(2.5) Burnside homomorphisms. 部分群 $H \in \mathcal{X}$ に対して φ_H を

$$\varphi_H : X\Omega(G,\mathcal{X},S) \longrightarrow \mathbb{Z}[C_S(H)]^{WH} : x \longmapsto \sum_{x\in X^H} \|x\| = \sum_{s\in C_S(H)} |X[s]^H| s$$

で定める．さらに **Burnside homomorphism with respect to** $\mathcal{X}$ を

$$\varphi : X\Omega(G,\mathcal{X},S) \longrightarrow X\tilde{\Omega}(G,\mathcal{X},S) : [X] \longmapsto (\varphi_H([X]))_{(H)}$$

で定める．

(2.6) EXAMPLE. (2.4) のもとで Burnside homomorphism with respect to $\mathcal{X}$ による $X\Omega(G,\mathcal{X},S)$ の各基底の像を行列表示すると以下のようになる．

$(G/P)_s$	1	$\hat{t}$	$\hat{s}$	1	t
$(G/1)_1$	6	0	0	0	0
$(G/1)_t$	0	2	0	0	0
$(G/1)_s$	0	0	3	0	0
$(G/C)_1$	3	0	0	1	0
$(G/C)_t$	0	1	0	0	1

(2.7) Condition $(C)_p$. 素数を p とする．部分群 $H \in \mathcal{X}$ に対し $\overline{H} = \cap\{K \in \mathcal{X} \mid H \subseteq K\}$ と定める．もし H を含む $K \in \mathcal{X}$ が存在しないときには $\overline{H} = G$ とする．条件 $(C)_p$ を次のように定める:

$$(C)_p \quad gH \in ((WH)_s)_p,\ s \in C_S(H),\ H \in \mathcal{X} \Longrightarrow \overline{\langle g \rangle H} \in \mathcal{X}.$$

ただし，$((WH)_s)_p$ は $(WH)_s$ の Sylow p-subgroup とする．$\mathbb{Z}_{(p)} = \{a/b | a \in \mathbb{Z},\ b \in \mathbb{Z} - p\mathbb{Z}\} \subseteq \mathbb{Q}$ とおくとき，

$$X\Omega(G,\mathcal{X},S)_{(p)} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} X\Omega(G,\mathcal{X},S), X\tilde{\Omega}(G,\mathcal{X},S)_{(p)} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} X\tilde{\Omega}(G,\mathcal{X},S).$$

と書く．

(2.8) Lemma. *Let $x \in X\Omega(G,\mathcal{X},S)$ and $H \leq G$ such that $\overline{H} \in \mathcal{X}$. Then $x(H) = x(\overline{H})$.*

(2.9) Cauchy-Frobenius homomorphisms. Obstruction groups with respect to $\mathcal{X}$ を

$$\mathrm{XObs}(G,\mathcal{X},S)_{(p)} = \prod_{[H,s]} (\mathbb{Z}/|(WH)_s|_p\mathbb{Z})$$

で定める．さらに **Cauchy-Frobenius homomorphism** を

$$\begin{aligned} \psi^{(p)}_{H,s} \ :\ & X\tilde{\Omega}(G,\mathcal{X},S) \longrightarrow \mathbb{Z}/|(WH)_s|_p\mathbb{Z} \\ :\ & \left(\sum_{t \in C_S(H)} \xi(H,t)t\right)_{(H)} \longmapsto \sum_{nH \in ((WH)_s)_p} \overline{\xi(\overline{\langle n \rangle H}, s)}. \end{aligned}$$

のように定める．すると **CFB-map with respect to $\mathcal{X}$** が次のように得られる:

$$\psi^{(p)} = (\psi^{(p)}_{H,s}) : X\tilde{\Omega}(G,\mathcal{X},S) \longrightarrow \mathrm{XObs}(G,\mathcal{X},S)_{(p)}.$$

(2.10) Theorem (Fundamental theorem). *Let p be a prime. Then under the condition $(C)_p$, the following sequence of abelian groups is exact:*

$$0 \longrightarrow X\Omega(G,\mathcal{X},S)_{(p)} \xrightarrow{\varphi^{(p)}} X\tilde{\Omega}(G,\mathcal{X},S)_{(p)} \xrightarrow{\psi^{(p)}} \mathrm{XObs}(G,\mathcal{X},S)_{(p)} \longrightarrow 0.$$

PROOF. Note that the free abelian groups $X\Omega(G,\mathcal{X},S)$ and $X\tilde{\Omega}(G,\mathcal{X},S)$ have a same rank by 2.3. By the definition of the crossed ghost ring with respect to $\mathcal{X}$ there is an isomorphism of abelian groups:

$$\begin{aligned} f \ :\ & X\tilde{\Omega}(G,\mathcal{X},S) \longrightarrow \prod_{[H,s]} \mathbb{Z} \\ :\ & \left(\sum_s \xi(H,s)s\right)_H \longmapsto (\xi(H,s))_{[H,s]} \end{aligned}$$

By [OY01] Lemma 2.13 (4), the $[H,s]$-component of $f \circ \varphi([X])$ is equal to

$$|X[s]^H| = \sharp\{x \in X^H \mid \|x\| = s\} = |\mathrm{XMap}_{G,\mathcal{X}}((G/H)_s, X)|.$$

Thus the linear map $f \circ \varphi$ is presented by the matrix

$$M := \left(|\mathrm{XMap}_{G,\mathcal{X}}((G/H)_s, (G/K)_t)|\right)_{[H,s],[K,t]} \tag{2.10.1}$$

indexed by isomorphism classes of transitive crossed $(G,\mathcal{X}$-sets. Since

$$\mathrm{XMap}_{G,\mathcal{X}}((G/H)_s,(G/K)_t)\neq\emptyset \quad\Longrightarrow\quad H\subseteq {}^gK \quad (\exists g\in G) \tag{2.10.2}$$

by [OY01] Lemma 2.13 (5), the matrix M is an upper triangular matrix with diagonal constituents $|(WH)_s|$'s after arranging $[H,s]$'s by the order of H's. Thus the Burnside homomorphisms $\varphi^{(p)}$ is injective and

$$\mathrm{Coker}(\varphi^{(p)})\cong \mathrm{XObs}(G,\mathcal{X},S). \tag{2.10.3}$$

Note that $\psi^{(p)}$ is surjective because the matrix corresponding to $\psi^{(p)}$ is conjugate to a triangular matrix. Thus by the universality of the cokernels, we know that it remains only to show that

$$\psi^{(p)}\circ\varphi^{(p)}=0. \tag{2.10.4}$$

Let $X\in X\Omega(G,\mathcal{X},S)$. Then for any $K\in\mathcal{X}$, $s\in C_S(K)$ and $gK\in((WK)_s)_p$,

$$X(\overline{\langle g\rangle K})=X(\langle g\rangle K) \tag{2.10.5}$$

by the condition $(\mathrm{C})_p$ and Lemma (2.8). For a crossed G-set X, the H-component of $\varphi(X)$ is given by

$$\varphi_H(X)=\sum_{x\in X^H}\|x\|=\sum_{s\in C_S(H)}|X[s]^H|s,$$

where $X[s]^H:=\{x\in X^H\mid \|x\|=s\}$ as before. Thus

$$\begin{aligned}
\psi^{(p)}_{H,s}\circ\varphi^{(p)}(X) &= \sum_{nH\in(WH_s)_p}\varphi^{(p)}(X)(\overline{\langle n\rangle H},s) \mod |(WH)_s|_p\\
&= \sum_{nH\in(WH_s)_p}X(\overline{\langle n\rangle H},s) \mod |(WH)_s|_p\\
&= \sum_{nH\in(WH_s)_p}X(\langle n\rangle H,s) \mod |(WH)_s|_p\\
&= \sum_{nH\in(WH_s)_p}|X[s]^{\langle n\rangle H}| \mod |(WH)_s|_p.
\end{aligned}$$

Applying the Cauchy-Frobenius lemma to the WH-set $X[s]$, we have

$$\begin{aligned}
\psi^{(p)}_{H,s}\circ\varphi^{(p)}(X) &= |(WH)_s|_p\cdot|((WH)_s)_p\backslash X[s]^H|\\
&\equiv 0 \mod |(WH)_s|_p,
\end{aligned}$$

proving (2.10.4). The theorem is proved. □

(2.11) Corollary. *Let $\mathbb{K}$ be a commutative ring in which $|G|\cdot 1_{\mathbb{K}}$ is invertible. Then*

$$\mathbb{K}\otimes_{\mathbb{Z}}X\Omega(G,\mathcal{X},S)\cong\prod_{(H)\in C(\mathcal{X})}\mathbb{K}[C_S(H)]^{WH}.$$

In particular, $X\Omega(G,\mathcal{X},S)$ is commutative if and only if $\mathbb{Z}[C_S(H)]^{WH}$ is commutative for any $H\in\mathcal{X}$.

(2.12) Theorem. *Under the condition* $(C)_p$, $X\Omega(G,\mathcal{X},S)_{(p)}$ *has a unique ring structure such that the Burnside homomorphism* $\varphi^{(p)}$ *is a ring homomorphism.*

PROOF. In order to prove that the existence of a ring structure on $X\Omega(G,\mathcal{X},S)_{(p)}$, it will suffice to show that $\mathrm{Im}\varphi^{(p)}$ is a subring of $X\tilde{\Omega}(G,\mathcal{X},S)$, because $\varphi^{(p)}$ is injective. Set $x=[X]$, $y=[Y]$, where X and Y are $(G,\mathcal{X})$-sets. Then by Lemma (2.8) for any subgroup H of G with $\overline{H}\in\mathcal{X}$,

$$\varphi(x)(H)=x(\overline{H})=\sum_{s\in C_S(H)}|X[s]^H|s.$$

Thus

$$\begin{aligned}
&\psi^{(p)}_{H,s}(\varphi^{(p)}(x)\cdot\varphi^{(p)}(y))_H\\
\equiv&\sum_{gH\in((WH)_s)_p}(\varphi^{(p)}(x)\cdot\varphi^{(p)}(y))(\overline{\langle g\rangle H},s)\\
\equiv&\sum_{gH\in((WH)_s)_p}\varphi^{(p)}(x)(\overline{\langle g\rangle H})\cdot\varphi^{(p)}(y)(\overline{\langle g\rangle H})\\
\equiv&\sum_{gH\in((WH)_s)_p}x(\langle g\rangle H)\cdot y(\langle g\rangle H)\\
\equiv&\sum_{gH\in((WH)_s)_p}|X^{\langle g\rangle H}|\cdot|Y^{\langle g\rangle H}|\\
\equiv&\sum_{gH\in((WH)_s)_p}|((X\times Y)^H)^{\langle g\rangle}|\\
\equiv&\ 0\mod|(WH)_s|_p.
\end{aligned}$$

The last congruence follows from the Cauchy-Frobenius lemma. This proves that $\varphi(x)\cdot\varphi(y)$ belongs to $\mathrm{Ker}\psi^{(p)}=\mathrm{Im}\phi^{(p)}$, that is, the image of $\varphi^{(p)}$ is closed under multiplication.

Next in order to prove the existence of an identity element, it will suffice to show that the identity element 1 of $X\tilde{\Omega}(G,\mathcal{X},S)$ belongs to the image of $\varphi^{(p)}$. But

$$\psi^{(p)}_{H,s}(1)_H=\sum_{gH\in((WH)_s)_p}1\equiv 0\bmod|(WH)_s|_p,$$

and so by the fundamental theorem, we conclude that the edentity element 1 of $X\tilde{\Omega}(G,\mathcal{X},S)$ is contained in $\mathrm{Im}\ \varphi^{(p)}=\mathrm{Ker}\ \psi^{(p)}$. Thus $X\Omega(G,\mathcal{X},S)$ has an identity element and $\varphi^{(p)}$ maps the identity element to 1. □

(2.13) Definition. Let R be a commutative ring. The R-module $R\otimes_{\mathbb{Z}}X\Omega(G,\mathcal{X},S)$ is called a **crossed Burnside ring with respect to** $\mathcal{X}$ provided it has a ring structure with identity element such that the Burnside homomorphism

$$1\otimes\varphi:R\otimes X\Omega(G,\mathcal{X},S)\longrightarrow R\otimes X\tilde{\Omega}(G,\mathcal{X},S)$$

is an injective ring homomorphism.

参考文献

[Bo97] S. BOUC, *Green functors and G-sets*, Lecture Notes in Mathematics, vol. 1671, Springer, 1997.

[Bo00] S. Bouc, Burnside rings, In *Handbook of Algebra*, Vol. 2, Elsevier Science B.V. (2000), 439–804.

[Bo01] S. Bouc, The p-blocks of the Mackey algebra, preprint 2001.

[OY01] F. Oda and T. Yoshida, Crossed Burnside Rings I. The Fundamental Theorem, *J. Algebra* **236**, 29–79.

[TW95] J. Thévenaz and P. Webb, The structure of Mackey functors, *Trans. Amer. Math. soc.* **347 (6)** (1995), 1865–1961.

[We00] P. Webb, A guide to Mackey functor, In *Handbook of Algebra* Vol. 2, Elsevier Science B.V. (2000), 805–836.

[Yo90] T. Yoshida, The generalized Burnside ring of a finite group, *Hokkaido Math. J.* **19** (1990), 509–574.