《科学研究費補助金（総合研究Ａ）研究集会報告集》

第12回代数的組合せ論シンポジウム 報告集

1995年7月29日～7月31日

於 東京大学駒場キャンパス

まえがき

この報告集は，１９９５年7月２９日（土）から7月３１日（月）にわたって，東京大学駒場キャンパスで行われた「第１２回代数的組合せ論シンポジウム」の講演記録です。

例年にない猛暑の中でしたが，１００人を超える出席者を得て盛会でした。この集会の計画に当たっては，同年２月に近藤武先生が還暦を迎えられたことを記念する意味で先生にゆかりの東京大学を会場に選ばせていただくとともに，プログラムの一部を任せていただきました。こうした計画を受けてくださった他の研究代表者に，この場を借りて感謝いたします。

この集会に関わる講演者の旅費，並びに，この報告集の作成にあたっては，科学研究費総合（A）（研究代表者：川中宣明 大阪大・理・教授）の援助をいただきました。また，会場の手配・運営にあたっては，東京大学・五味健作先生にご協力いただきました。ここに記して感謝いたします。

なお，私の連絡ミス等もあって報告集の発行が遅れたこと，にもかかわらず，すべての講演記録を収録できなかったことをお詫びいたします。

1996 年 1 月

北詰 正顕

「第１２回代数的組合せ論シンポジウム」

北詰正顕（千葉大・理）
坂内英一（九大・数理）
吉田知行（北大・理　）

日　時: １９９５年7月２９日（土）～7月３１日（月）
場　所: 東京大学駒場キャンパス（１３号館１３１３番教室）

プログラム

7月２９日（土）

10:00～10:50　江川嘉美（東理大・理）
日本のグラフ理論

11:00～11:50　川中宣明（阪大・理）
非結晶的な有限 Coxeter 群について

13:30～14:00　小須田雅（東大・数理）
Rational Brauer algebra の表現

14:05～14:35　Tayuan Huang(黃大原)(国立交通大学 (台湾)・九大・数理)
Spectral characterizations of some specialized odd graphs

14:40～15:10　Jack Koolen(Eindhoven 工科大・九大・数理)
On distance-regular graphs which are locally strongly regular

15:25～15:55　野村和正（東医歯大・教養）
Spin models and almost bipartite 2-homogeneous graphs

16:00～16:30　郭海涛 (九大・数理・上海交通大)
Classification of spin models with at most 10 vertices

16:40～17:30　宮本雅彦（愛媛大・理）
Tensor product of vertex operator algebra and modular forms

7月30日（日）

10:00〜10:50 鈴木通夫 (イリノイ大)
群とグラフ

11:00〜11:50 小関道夫（山形大・理）
符号理論と unitary reflection groups の不変式環との関連について

13:30〜14:00 坂内悦子 (九大・数理)
ある種の有限群の不変式環の生成元

14:05〜14:35 奥山哲郎 (北教大・旭川分校) －花木章秀 (山梨大・工)
Self Dual 群についての２，３の話題

14:40〜15:10 山田裕史（都立大・理）
基本表現のウエイトベクトルと Schur 函数

15:15〜15:45 宇佐美 (榎本) 陽子 (お茶大・理)
可換不足群を持つ惰性剰余群が位数８の二面体群である主ブロックのパーフェクトアイソメトリーについて

15:55〜16:45 近藤武（東女大・文理）
６次式のある族とそのガロア群

7月31日（月）

10:00〜10:50 原田耕一郎 (オハイオ州立大)
Vertex operator algebras について

11:00〜11:50 小池正夫（九大・数理）
Thompson series の合同式

13:30〜14:00 北詰正顕（千葉大・理）
The Leech lattice and the Niemeier lattices

14:05〜14:35 穴井宏和－横山和弘（富士通惰報研）
ガロア群計算の最新状況

14:40〜15:10 千吉良直紀 (熊大・自然科学)
A set of orders of abelian subgroups in finite groups

15:20〜16:10 吉田知行（北大・理）
有限群論と数理物理学における高次元カテゴリー論

目次

Extremal Set Theory in Japan

東京理科大学理学部応用数学科　　江川　嘉美

本稿では，Frankl-Ota-Tokushigeによる最近の一連の論文([4], [5], [6])を紹介する。

本稿を通じて，n, k, tは$n > k \geq t \geq 2$であるような整数を表し，Xは大きさnの集合を表すものとする。さらに，$\mathcal{F}$はX上のk一様な集合族である，つまり，$\mathcal{F} \subseteq \binom{X}{k}$であるとする(ここで，$\binom{X}{k} = \{F \subseteq X \mid |F| = k\}$である)。

まず，いくつか定義を述べる。$\mathcal{F}$が交差的であるとは，すべての$F, G \in \mathcal{F}$に対して$F \cap G \neq \emptyset$であることをいう。すべての$F \in \mathcal{F}$に対して$T \cap F \neq \emptyset$であるようなXの部分集合Tを，$\mathcal{F}$のtransversalとよぶ。

$$\mathcal{T}(\mathcal{F}) = \{T \mid T \text{は} \mathcal{F} \text{のtransversal}\}$$

$$\mathcal{T}(\mathcal{F}; t) = \{T \in \mathcal{T}(\mathcal{F}) \mid |T| = t\}$$

とおく。$\mathcal{F}$のtransversal number $\tau(\mathcal{F})$を，

$$\tau(\mathcal{F}) = \min\{|T| \mid T \in \mathcal{T}(\mathcal{F})\}$$

により定義する。明らかに，

$$\tau(\mathcal{F}) = \min\{\Delta \mid \mathcal{T}(\mathcal{F}; \Delta) \neq \emptyset\}$$

である.

次の定理は，極値集合論における古典的な定理である.

定理1 (Erdös-Ko-Rado [1]). $n \geq 2k$ とし，$\mathcal{F}$ は交差的であると仮定する。すると，次が成立する.

(i) $|\mathcal{F}| \leq \binom{n-1}{k-1}$.

(ii) $n > 2k$ とし，(i) において等号が成立していると仮定する. すると，ある $a \in X$ が存在して，

$$\mathcal{F} = \{F \in \binom{X}{k} \mid a \in F\}$$

となる.

定理1の(i)において等号が成立するのは，(ii)により，$t(\mathcal{F}) = 1$ の場合に限るわけであるが，$t(\mathcal{F}) = 1$ であれば $\mathcal{F}$ が交差的であるのは明らかであるから，$t(\mathcal{F}) = 1$ であるような集合族 $\mathcal{F}$ は，交差的な集合族の中ではつまらないものと言える。そこで，$t(\mathcal{F}) \geq t$ という仮定を付け加えるとどういう結論が導かれるかということを考える。$2 \leq t \leq 4$ の場合については，次の定理が証明されている（これらの定理において等号が成立する場合についても，定理1(ii) におけるように，$\mathcal{F}$ の形が決まることが証明されているが，そのことについての詳細は省略する；また，定理3,4に出てくる $M(n, k; t)$

の定義は，本稿の最後に述べる）．

定理2 (Hilton-Milner[1], Frankl-Füredi[3]). $n \geq 2k$ とし，$\mathcal{F}$ は交差的で，$\tau(\mathcal{F}) \geq 2$ であると仮定する．すると，$|\mathcal{F}| \leq \binom{n-1}{k-1} - \binom{n-k-1}{k-1} + 1$．

定理3 (Frankl[2]). n は k に比べて十分大きいとし，$\mathcal{F}$ は交差的で，$\tau(\mathcal{F}) \geq 3$ であると仮定する．すると，$|\mathcal{F}| \leq |\mathcal{A}(n, k; 3)|$．

定理4 ([5]). $k \geq 9$，n は k に比べて十分大きいとし，$\mathcal{F}$ は交差的で，$\tau(\mathcal{F}) \geq 4$ であると仮定する．すると，$|\mathcal{F}| \leq |\mathcal{A}(n, k; 4)|$．

$t \geq 5$ の場合については，定理2〜4におけるような正確な結果は知られていない．$t \geq 5$ の場合について述べるために，次の定義をする．

$$p(k, t) = \max\{|\mathcal{F}(\mathcal{F}; t)| \mid \mathcal{F} \text{は交差的で} \tau(\mathcal{F}) = t\}$$

（この定義においてmaxをとる際には，n も動かすものとする；あるいは，この定義に限り，X を無限集合とすることにしてもよい）

とおく。一般的に，次の定理が成立する．

定理5 ([2]). k, tを固定し，kはtに比べて十分大きいとする．このとき，各nに対して

$$f(n) = \max\{|\mathcal{F}| \mid \mathcal{F}\text{は交差的で}\tau(\mathcal{F}) \geq t\}$$

とおくと，$n \to \infty$のとき，

$$f(n) = p(k, t-1)\binom{n}{k-t} + O(n^{k-t-1}).$$

そこで，$p(k, t)$を調べることが重要になるわけであるが，次の予想がなされている．

予想6 ([4]). tを固定し，$k \to \infty$とすると，

$$p(k, t) = k^t - \frac{t(t-1)}{2}k^{t-1} + \frac{t}{4}\left[\frac{(t+1)(t^2-4t+7)}{2}\right]k^{t-2} + O(k^{t-3}).$$

この予想について，次の定理が証明されている．

定理7 ([2]). $p(k, 2) = k^2 - k + 1$.

定理8 ([4], [5]). $k = 3$または$k \geq 9$とすると，
$p(k, 3) = k^3 - 3k^2 + 6k - 4$.

定理9 ([6]). $k \to \infty$ のとき, $p(k,4) = k^4 - 6k^3 + O(k^2)$, $p(k,5) = k^5 - 10k^4 + O(k^3)$.

定理10 ([6]). t を固定し, $k \to \infty$ とすると,

$$p(k,t) \leq k^t - \frac{1}{\sqrt{2}}\left[\frac{t-1}{2}\right]^{\frac{3}{2}} k^{t-1} + O(k^{t-2}).$$

以下, 例について述べる. D を有向グラフとする. D の点集合は $V(D)$ で表し, 辺集合は $E(D)$ で表す. $x \in V(D)$ に対し, $N^+(x)$, $\deg^+(x)$ を,

$$N^+(x) = \{y \in V(D) \mid xy \in V(D)\},$$
$$\deg^+(x) = |N^+(x)|$$

により定義する. D がトーナメントであるとは, 各 $x, y \in V(D)$ $(x \neq y)$ に対し, xy, yx のうちのちょうど1つが $E(D)$ に属することをいう.

さて, D を, $\{1, 2, \cdots, t\}$ を点集合とするトーナメントとする. 各 $1 \leq i \leq t$ に対し, X_i を大きさ $k - \deg^+(i)$ の集合とし,

$$X = X_1 \dot{\cup} \cdots \dot{\cup} X_t \quad \text{(disjoint union)}$$

とする. さらに,

$$\mathcal{C}_i = \left\{F \in \binom{X}{k} \;\middle|\; F \supseteq X_i, \text{ かつ, すべての } j \in N^+(i) \text{ 対して } |F \cap X_j| = 1\right\},$$

$$\mathcal{C} = \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_t$$

とおく．すると，$\mathcal{C}$はt交差的かつ$\tau(\mathcal{C}) = t$であって，

$$\begin{aligned} &|\mathcal{T}(\mathcal{C}; t)| \\ &\geq \left|\left\{T \in \binom{X}{t} \;\middle|\; \text{すべての } 1 \leq i \leq t \text{ に対して } |T \cap X_i| = 1\right\}\right| \\ &= \Pi_{1 \leq i \leq t} (k - \deg^+(i)) \end{aligned}$$

となるが，$k \to \infty$のとき$\Pi_{1 \leq i \leq t} (k - \deg^+(i)) = k^t - \frac{n(n-1)}{2} k^{t-1} + O(k^{t-2})$であるから，この例は，予想6において$k^{t-1}$の係数を達成する例になっている．しかし，この方法では，Dとしてどのようなトーナメントをもってきても，k^{t-2}の係数を達成する例は得られない．以下，そのような例を構成するが，要点は，Dとして特別なトーナメントをとったうえで，$\mathcal{C}_i$の定め方を工夫することにある（以下では，上の例での$\mathcal{C}_i$に対応する集合族は$\mathcal{B}_i$で表してある）．

まず，tが奇数（$= 2s+1$）の場合を考える．$k = k - s$とおく．各$\alpha \in \mathbb{Z}$に対し

$$Y_{2\alpha} = \{(2\alpha, 2\beta) \mid 0 \leq \beta \leq k-1\},$$

$$Y_{2\alpha+1} = \{(2\alpha+1, 2\beta+1) \mid 0 \leq \beta \leq k-1\}$$

とおき，

$$W = \dot{\bigcup}_{i \in \mathbb{Z}} Y_i$$

とおく．Wにおける同値関係$\sim$を，

$$(i_1, j_1) \sim (i_2, j_2)$$

$\Longleftrightarrow$

$i_2 - i_1$ が t で割り切れ，

かつ，

$$\begin{cases} \dfrac{i_2 - i_1}{t} \text{ が偶数かつ } j_1 = j_2 \text{，または，} \\ \dfrac{i_2 - i_1}{t} \text{ が奇数かつ } j_1 + j_2 = 2k - 1 \end{cases}$$

により定め，

$$Y = W/\sim$$

とおく。Y の元は，その（$\sim$ に関する）代表元を用いて，(i, j) などの記号で表すことにする。各 $1 \leq i \leq t$ に対し，

$$j_0 = j_{i,0} = \begin{cases} k & (k+i \text{ が偶数のとき}) \\ k-1 & (k+i \text{ が奇数のとき}) \end{cases}$$

として，

$$\begin{aligned} &\mathcal{Q}_i \\ &= \Big\{ \{(i, j_0), (i+1, j_1), (i+2, j_2), \cdots, (i+\Delta, j_\Delta)\} \Big| \\ &\qquad \text{各 } r \ (1 \leq r \leq \Delta) \text{ に対し，} j_r - j_{r-1} \in \{1, -1\} \Big\}, \\ &\mathcal{B}_i = \{Y_i \cup Q \mid Q \in \mathcal{Q}_i\} \end{aligned}$$

とおき，

$$\mathcal{B} = \mathcal{B}(k, t) = \bigcup_{1 \leq i \leq t} \mathcal{B}_i$$

とおく。すると，$\mathcal{B}$ は t 交差的かつ $\tau(\mathcal{B}) = t$ であって，

$$\begin{aligned} &|T(\mathcal{B})| \\ &\geq \left| \left\{ T \in \binom{Y}{t} \right| \text{ すべての } 1 \leq i \leq t \text{ に対して } |T \cap Y_i| = 1 \right\}| \end{aligned}$$

$$+\sum_{1\le i\le t}\left|\left\{T\in\binom{Y}{t}\right|\right.$$

$$\left.(i+1,\ j_{i,0}+1),\ (i+1,\ j_{i,0}-1)\in T,\ \text{かつ},\right.$$

$$\left.\text{すべての } r\ (2\le r\le t-1) \text{ に対して } |T\cap Y_{i+r}|=1\right\}|$$

$$=\left(k-\frac{t-1}{2}\right)^t+t\left(k-\frac{t-1}{2}\right)^{t-2}$$

となるが，$k\to\infty$ のとき $\left(k-\frac{t-1}{2}\right)^t+t\left(k-\frac{t-1}{2}\right)^{t-2}=k^t-\frac{t(t-1)}{2}k^{t-1}+\frac{t(t+1)(t^2-4t+7)}{8}k^{t-2}+O(k^{t-3})$ であるから，この例は，予想6において k^{t-1}，k^{t-2} の係数を達成する例になっている。

次に，t が偶数 $(=2\Delta)$ の場合を考える。$k=k-\Delta$ とおく。各 $\alpha\in\mathbb{Z}$ に対し，

$$Y_{2\alpha}=\begin{cases}\{(2\alpha,2\beta)\mid 0\le\beta\le k\}\\ \qquad(0\le 2\alpha\le\Delta-1 \pmod t \text{ のとき})\\ \{(2\alpha,2\beta)\mid 1\le\beta\le k\}\\ \qquad(\Delta\le 2\alpha\le 2\Delta-1 \pmod t \text{ のとき}),\end{cases}$$

$$Y_{2\alpha+1}=\begin{cases}\{(2\alpha+1,2\beta+1)\mid 0\le\beta\le k\}\\ \qquad(0\le 2\alpha+1\le\Delta-1 \pmod t \text{ のとき})\\ \{(2\alpha+1,2\beta+1)\mid 0\le\beta\le k-1\}\\ \qquad(\Delta\le 2\alpha+1\le 2\Delta-1 \pmod t \text{ のとき})\end{cases}$$

とおき，

$$W=\dot{\bigcup}_{i\in\mathbb{Z}}Y_i$$

とおく。W における同値関係を，

$(i_1, j_1) \sim (i_2, j_2)$

$\Longleftrightarrow$

$i_2 - i_1$ が t で割りきれ，かつ，$j_1 = j_2$

により定め，

$Y = W/\sim$

とおく。各 $0 \leq i \leq t-1$ に対し，

$$j_0 = \begin{cases} k & (k+i \text{ が偶数のとき}) \\ k+1 & (k+i \text{ が奇数のとき}) \end{cases}$$

として，$0 \leq i \leq \Delta - 1$ のときは

$$\mathcal{Q}_i = \left\{ \{(i, j_0), (i+1, j_1), (i+2, j_2), \cdots, (i+\Delta-1, j_{\Delta-1})\} \,\middle|\, \text{各 } r \ (1 \leq r \leq \Delta-1) \text{ に対し，} j_r - j_{r-1} \in \{1, -1\} \right\},$$

$\Delta \leq i \leq t-1$ のときは

$$\mathcal{Q}_i = \left\{ \{(i, j_0), (i+1, j_1), (i+2, j_2), \cdots, (i+\Delta, j_\Delta)\} \,\middle|\, \text{各 } r \ (1 \leq r \leq \Delta) \text{ に対し，} j_r - j_{r-1} \in \{1, -1\} \right\}$$

とおき，さらに，

$$\mathcal{B}_i = \{Y_i \cup Q \mid Q \in \mathcal{Q}_i\}$$

とおく。

$$\mathcal{B} = \mathcal{B}(k, t) = \bigcup_{0 \leq i \leq t-1} \mathcal{B}_i$$

とおく。すると，$\mathcal{B}$ は t 交差的かつ $\tau(\mathcal{B}) = t$ であって，予想

Gにおいてk^{t-1}, k^{t-2}の係数を達成する例になっていることが, tが奇数の場合と同様の計算により, 確かめられる.

さて, $\mathcal{G} = \mathcal{B}(k, t-1)$とおき, Yは$\mathcal{B}(k, t-1)$の定義における通りであるとする. つまり, $Y = \bigcup_{G \in \mathcal{G}} G$である. nは十分大きいとし, $Y \subseteq X$とする. $a \in X - Y$を固定し,

$$\mathcal{A} = \mathcal{A}(n; k, t)$$
$$= \mathcal{G} \cup \{\{a\} \cup T \mid T \in \mathcal{T}(\mathcal{G}; k-1),\ a \notin T\}$$

とおく. すると, $\mathcal{A}$は交差的かつ$\tau(\mathcal{A}) = t$となる. これについて次の予想がなされているが, 解決には程遠いようである.

予想11 ([4]). nはk, tに比べて十分大きいとし, $\mathcal{F}$は交差的で, $\tau(\mathcal{F}) \geq t$であると仮定する. すると, $|\mathcal{F}| \leq |\mathcal{A}(n; k, t)|$.

REFERENCES

1. P. ERDÖS, C. KO AND R. RADO, Intersection theorems for systems of finite sets, Quart. J. Math. Oxford (2) 12 (1961), 313-320.
2. P. FRANKL, On intersecting families of finite sets, Bull. Austral. Math. Soc. 21 (1980), 363-372.
3. P. FRANKL AND Z. FÜREDI, Nontrivial intersecting families, J. Combin. Theory Ser. A 41 (1986), 150-153.
4. P. FRANKL, K. OTA AND N. TOKUSHIGE, Covers in uniform intersecting families and a counterexample to a conjecture of Lovász, preprint.
5. P. FRANKL, K. OTA AND N. TOKUSHIGE, Uniform intersecting families with covering number four, preprint.
6. P. FRANKL, K. OTA AND N. TOKUSHIGE, Uniform intersecting families with covering number restrictions, preprint.
7. A. J. W. HILTON AND E. C. MILNER, Some intersection theorems for systems of finite sets, Quart. J. Math. Oxford (2) 18 (1967), 369-384.

非結晶型の有限 Coxeter 群について

大阪大学理学研究科　　川中宣明

有限 Coxeter 群とは、つぎの形の presentation をもつ有限群 G のことである。

$$G = < r_1, r_2, \cdots, r_t \mid (r_i r_j)^{m(i,j)} = 1 >$$

ただし　$m(i,i) = 1$　　, $1 \leq i \leq t$
$m(i,j) = 2,3,4,\cdots$, $i \neq j$

($\{ r_1, r_2, \cdots, r_t \}$ を G の、Coxeter 群としての生成系という。)

よく知られているように、G は有限鏡映群と考えることもできる。 このとき、G は実直交群 $O(V) = O_n(R)$ の部分群で、$r_1, \cdots, r_t$ は $V = R^n$ の超平面に関する鏡映である。

G が V のある lattice $L = Ze_1 + Ze_2 + \cdots + Ze_n$ ($e_1, \cdots, e_n$ は V の R 基底) を保つとき、G は結晶型であるといい、そのような lattice がないとき、非結晶型であるという。

結晶型の有限 Coxeter 群は、半単純 Lie 群や Lie 環の Weyl 群として重要な役割を果たすが、非結晶型のほうは、今のところそれほど重要なものとは見なされていないように思う。 非結晶型の有限 Coxeter 群に対しても、結晶型の場合と同じ位の重要な役割を見つけだしたい、というのが、筆者の以前からの願望である。 この講演では、とてもそこまで行けないが、その方向のひとつの試みについて述べる。 もとになっているのは矢野環氏 [8] のアイデアである。

有限 Coxeter 群 G の生成系 $S = \{ r_1, r_2, \cdots, r_t \}$ の分割

(1)　　$S = \coprod S_\lambda$　　($\lambda \in \Lambda$)

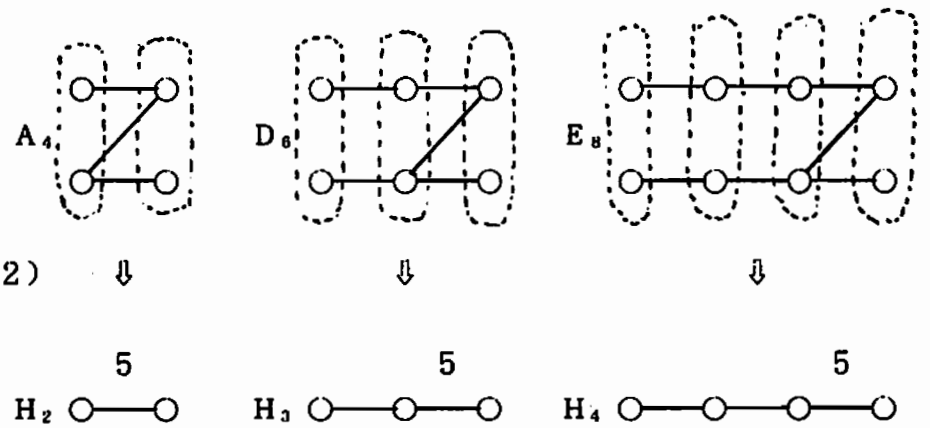
を考え、各 λ に対し、s_λ を G の部分群 $< S_\lambda >$ の（S_λ に関し）長さ最大の元とする。G の部分群

$$H = < s_\lambda >$$

が $\{ s_\lambda \mid \lambda \in \Lambda \}$ を生成系とする Coxeter 群になっているとき、H は G の、分割（1）に関する、「折り畳み（folding)」であるという（[8]）。

よく知られているのは、G が結晶型で、分割（1）が G の Dynkin 図形の自己同型 σ の生成する群 $< \sigma >$ の軌道分解に一致する場合で、[4] [5] [6] [7] など多くの文献がある。この場合を proper な折り畳みということにする。proper な折り畳みは、対応する Lie 環の折り畳みにまで延長できるので、その理論的意味は明確である。

proper な折り畳みのときには、結晶型の群から結晶型の群しか生じないのだが、矢野氏は、つぎのような exceptional な折り畳みを考えれば、結晶型の群から非結晶型の群が得られることを指摘した。



（既約な非結晶型有限 Coxeter 群は これら H_n 系列に属するものと位数 $2n$ （$n \geq 7$）の2面体群とで尽くされる。2面体群の方もやはり A 型の Coxeter 群の折り畳みとして得られるが、以下では H_n 系列だけに注意を集中する。）

これらの場合にも、proper な折り畳みのときの σ に相当するものが自然に定義できることを示すのが、本稿の主な目的である。

<u>定理</u> G を A_4, D_6 または E_8 型の有限 Coxeter 群、V を G の有限鏡映群としての実表現空間、Σ ($\subset V$) を G の（通常の意味での、すなわち crystallographic condition を満たす） root 系とする。 また、H を（2）で与えられる exceptional な折り畳みにより、G から得られる群とする。 このとき、次が成り立つ。

（i） H 加群 V の部分加群 U で、H の U への作用が H の鏡映群としての表現に一致するものが、ただ1つ存在する。

（ii） V の U への直交射影を π とする。 π の Σ への制限は1対1写像である。

（iii） Σ は

$$\Sigma = \Sigma_A \amalg \Sigma_B$$

と分割できる。 ここで、$\pi(\Sigma_A)$、$\pi(\Sigma_B)$ の元の長さはそれぞれ一定で

$$\pi(\Sigma_B) = \tau \cdot \pi(\Sigma_A) = \{ \tau \cdot \pi(\alpha) \mid \alpha \in \Sigma_A \}$$

である。 ただし、 $\tau = (1+\sqrt{5}))/2$ とする。

（iv） $\pi(\Sigma_A)$ （ または $\pi(\Sigma_B)$ ） は ［2］、［8］の意味で H の root系である。

（v） $\pi(\Sigma)$ で生成される Z 加群は、H 加群である。

（vi） GL（V）の元 T で

$$T(\alpha) = \beta$$

ただし $\alpha \in \Sigma_A$ かつ $\pi(\beta) = \tau \cdot \pi(\alpha)$

を満たすものが、ただ1つ存在する。 T は 対称変換で

$$T^2 = T + 1$$

を満たす。

（vii） 任意の $\alpha \in \Sigma_0$ に対し

$$\alpha \perp T\alpha$$

が成り立つ。

（viii） $U = \{ v \in V \mid Tv = \tau v \}$ である。

（ix） $H = \{ g \in G \mid Tg = gT \}$ である。また、H に含まれる鏡映は

$$r_\alpha \quad (r_{r\alpha}) \qquad , \ \alpha \in \Sigma_0$$

とかける。ただし r_α は α に直交する超平面（$\subset V$）に関する鏡映である。

（x） 任意の $\alpha \in \Sigma$ に対し

$$(T r_\alpha)^3 = (r_\alpha T)^3$$

が成り立つ。 $S_\alpha = r_\alpha T r_\alpha$ とおくと、上の式は

$$S_\alpha T S_\alpha = T S_\alpha T$$

とかくことができる。 また $v_\alpha = r_\alpha T r_\alpha T r_\alpha$ とおけば

$$T v_\alpha = v_\alpha T$$

とかくこともできる。

（xi） （群 $<G, T>$ の構造についてはまだよくわからないが）群 $<G, T>$ の T 不変部分群 $<G, T>^\tau$ については、次のことが分かる。

$$<G, T>^\tau = < v_\alpha \mid \alpha \in \Sigma >$$

$$= GL_m(Z[\tau])$$

$$m = \dim V / 2 = \dim U$$

上の定理の（viii）や（ix）は、T が proper な折り畳みのときの σ と似た役割を果たすことを示している。 一方、（xi）は proper な場合とは、かなり違う面もあることを示している。

古典的な結晶群の理論によれば、2次元または3次元ユークリッド空間内の与えられた lattice を保存する直交変換のなす群は位数 5 の元を含まない。 これは自然界に見られる結晶が決して位数 5 の回転対称性をもたないことを意味する。 ところが、1984年に Shechtman 等が位数 5 の回転対称性をもつ、としか思えないような「結晶」を発見して結晶学上の常識を覆した。 以後、このようなタイプの物質の状態は、「準結晶（ quasi-crystal ）」と呼ばれるようになり、現在も理論、実験の両面から活発に研究されている。 準結晶の数学的モデルとしては Penrose のタイル貼りが有名である。 この稿で報告したことは Penrose のタイル貼りやそれに類似のパターンと関連が深いように思われるが、まだよくはわからない。
（［1］、［3］を見よ。）

文献

[1] H.S.M. Coxeter : Cyclotomic integers, nondiscrete tessellations and quasicrystals, Indagonationes Mthematicae, New Series, 4 (1993),1-7.

[2] V.V. Deodhar : On the root systems of a Coxeter group, Comm. Alg. 10 (1982), 611-630.

[3] R.V. Moody and J. Patera : Quasicrystals and icosians, J. Phys. A : Math. Gen. 26 (1993), 2829-2853.

[4] P. Slodowy : Simple singularities and simple algebraic groups, Lecture Notes in Math. 815(1980), Springer.

[5] R. Steinberg : Lectures on Chevalley Groups, §11, Yale Univ.

[6] T. Tanisaki : Foldings of root systems and Gabrie's theorem, Tsukuba J. Math. 4 (1980), 89-97.

[7] 谷崎俊之 : 半単純代数群の諸性質の folding による遺伝について、箱根シンポジウム(群論)報告集、1979.

[8] 矢野環 : Root 系 、Coxeter 系の folding と free deformation の flat coordinate 系 、同上報告集.

A型量子群の混合テンソル表現の中心化環（rational Brauer algebra）の表現について

東京大学　数理科学研究科　小須田　雅

1．はじめに

A型量子群Uq=U_q(gl(r,C))と一般線形群GL(r,C)の混合テンソル表現の中心化環の既約表現について述べる．U_qは，次の生成元と関係式で定義されるC(q)上のalgebraである．

生成元　　$q^{\pm \varepsilon_i}$, X_i, Y_i $(1 \leqq i \leqq r)$

関係式

$$q^{\varepsilon_i} q^{-\varepsilon_i} = q^{-\varepsilon_i} q^{\varepsilon_i} = 1, \quad q^{\varepsilon_i} q^{\varepsilon_j} = q^{\varepsilon_j} q^{\varepsilon_i},$$

$$q^{\varepsilon_i} X_j q^{-\varepsilon_i} = qX_j \ (\text{if } j = i), \quad q^{-1} X_j \ (\text{if } j = i-1), \quad X_j \ (\text{otherwise}),$$

$$q^{\varepsilon_i} Y_j q^{-\varepsilon_i} = q^{-1} Y_j \ (\text{if } j = i), \quad qY_j \ (\text{if } j = i-1), \quad Y_j \ (\text{otherwise}),$$

$$[X_i, Y_j] = \delta_{ij} (q^{\varepsilon_i - \varepsilon_{i+1}} - q^{-\varepsilon_i + \varepsilon_{i+1}}) / (q - q^{-1}),$$

$$X_i X_j = X_j X_i, \quad Y_i Y_j = Y_j Y_i \quad (|i-j| \geqq 2),$$

$$X_i^2 X_{i\pm1} - (q+q^{-1}) X_i X_{i\pm1} X_i + X_{i\pm1} X_i^2 = 0 \quad (1 \leqq i, i\pm1 \leqq r-1),$$

$$Y_i^2 Y_{i\pm1} - (q+q^{-1}) Y_i Y_{i\pm1} Y_i + Y_{i\pm1} Y_i^2 = 0 \quad (1 \leqq i, i\pm1 \leqq r-1).$$

Uqのベクトル表現ϕを次で定義する．

$$\phi : X_i \to E_{i,i+1}, \quad Y_i \to E_{i+1,i}, \quad q^{\varepsilon_i} \to q^{E_{i,i}}.$$

また，Uqには，次のようなcoproductΔとantipode aが存在する．

$$\Delta^{(m)}(q^{\pm \varepsilon_i}) = q^{\pm \varepsilon_i} \otimes \cdots \otimes q^{\pm \varepsilon_i},$$

$$\Delta^{(m)}(X_i) = \Sigma q^{H_i} \otimes \cdots \otimes q^{H_i} \otimes X_i \otimes 1 \otimes \cdots \otimes 1,$$

$$\Delta^{(m)}(Y_i) = \Sigma 1 \otimes \cdots \otimes 1 \otimes Y_i \otimes q^{-H_i} \otimes \cdots \otimes q^{-H_i},$$

$$a(X_i) = -q^{-H_i} X_i, \quad a(Y_i) = -Y_i q^{H_i}, \quad a(q^{\varepsilon_i}) = q^{-\varepsilon_i}.$$

ここで，$q^{H_i} = q^{\varepsilon_i - \varepsilon_{i+1}}$である．

これらを使うと，混合テンソルV⊗…⊗V⊗V^*⊗…⊗V^*上に，表現を定めることができる．詳しくは，[KM]を参照されたい．こうしてできる表現を混合テンソル表現（Φ, $V^{(m,n)}$）と呼ぶことにする．一般線形群の場合もテンソル積表現と双対表現を組み合わせて，混合テンソル表現が定義できる．今回は，一般線形群GLr(C)の混合テンソル表現

が，どのような有理既約に分解するのかを調べ，それを利用した中心可環の既約表現の構成法について述べる．この構成は，A型量子群の混合テンソル表現（φ，$V^{(m,n)}$）に於いても，全く同様にできる．

始めに生成元と関係式による(q-)rational Brauer algebra を定義し，この既約表現の構成法を中心に述べる．次に，これらの algebra がそれぞれ混合テンソル表現の中心化環に同型に移されることを見る．

2．rational Brauer algebra の定義

次の生成元と関係式で定義されるC上のalgebraが，一般線形群 GLr(C) の混合テンソル積表現の中心化環と同型であることを示す．以下では，r≧m+nを仮定しておく．

生成元　$s_{m-1}, \cdots, s_2, s_1, e, s^*_1, s^*_2, \cdots, s^*_{n-1}$

関係式

$$s_i^2 = 1 \qquad (1 \le i \le m-1),$$

$$s_i s_j = s_j s_i \qquad (|i-j| \ge 2,\ 1 \le i, j \le m-1),$$

$$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \qquad (1 \le i \le m-2),$$

$$s^{*2}_i = 1 \qquad (1 \le i \le n-1),$$

$$s^*_i s^*_j = s^*_j s^*_i \qquad (|i-j| \ge 2,\ 1 \le i, j \le n-1),$$

$$s^*_i s^*_{i+1} s^*_i = s^*_{i+1} s^*_i s^*_{i+1} \qquad (1 \le i \le n-2),$$

$$e^2 = re,$$

$$s_i s^*_j = s^*_j s_i \qquad (1 \le i \le m-1,\ 1 \le j \le n-1),$$

$$s_i e = e s_i \qquad (2 \le i \le m-1),$$

$$s^*_i e = e s^*_i \qquad (2 \le i \le n-1),$$

$$e s_1 e = e, \quad e s^*_1 e = e,$$

$$e s_1 s^*_1 e (s_1 - s^*_1) = 0, \quad (s_1 - s^*_1) e s_1 s^*_1 e = 0.$$

生成元と関係式から，このalgebraの単項 式の個数は，（係数を１にしておくと）高々(m+n)!個であり，したがって，次元は，(m+n)!で抑えられることがわかる．

3．q-rational Brauer algebra の定義

今，rational Brauer algebra の定義を少し変えて，qを不定元とする有理関数体C(q)上のalgebraを次の生成元と関係式で定義する．やはり，r≧m+nを仮定する．

生成元　$T_{m-1}, \cdots, T_2, T_1, E, T^*_1, T^*_2, \cdots, T^*_{n-1}$.

関係式

$$(T_i - q)(T_i + q^{-1}) = 0 \qquad (1 \le i \le m-1),$$

$$T_i T_j = T_j T_i \qquad (|i-j| \ge 2,\ 1 \le i, j \le n-1),$$

$$T_iT_{i+1}T_i = T_{i+1}T_iT_{i+1} \qquad (1\leq i\leq m-2),$$

$$(T^*_i - q)(T^*_i + q^{-1}) = 0 \qquad (1\leq i\leq n-1),$$

$$T^*_iT^*_j = T^*_jT^*_i \qquad (|i-j|\geq 2,\ 1\leq i, j\leq n-1),$$

$$T^*_iT^*_{i+1}T^*_i = T^*_{i+1}T^*_iT^*_{i+1} \qquad (1\leq i\leq n-2),$$

$$E^2 = [r]E,$$

$$T_iT^*_j = T^*_jT_i \qquad (1\leq i\leq m-1,\ 1\leq j\leq n-1),$$

$$T_iE = ET_i \quad (2\leq i\leq m-1), \qquad T^*_iE = ET^*_i \quad (2\leq i\leq n-1),$$

$$ET_1E = q^rE, \quad ET^*_1E = q^rE,$$

$$ET_1^{-1}T^*_1E(T_1-T^*_1) = 0, \quad (T_1-T^*_1)ET_1^{-1}T^*_1E = 0.$$

ここで，$[r] = q^{r-1}+q^{r-3}+\cdots+q^{1-r}$ である．この algebra をq-rational Brauer algebraと呼ぶことにする．q=1とおくと，rational Brauer algebra の生成元と関係式が得られることに注意する．

4．GL(r,C)の混合テンソル表現の分解

GL(r,C)の既約表現の同値類とその中心化環の既約表現の同値類は，1対1に対応していることが，表現論の一般論よりわかるので，まずGL(r,C)の混合テンソル表現が，どのように既約有理表現に分解するのかを考えてみる．簡単のために，対角行列 $g = \mathrm{diag}(x_1,x_2,\dots,x_r)$ の分解の様子についてのみ考える（Stembridge[Ste]参照）．双対空間への表現の対角和は，$(x_1^{-1}+x_2^{-1}+\dots+x_r^{-1})$となることに注意すると，混合テンソル表現の対角和は，

$$(x_1+x_2+\dots+x_r)^m\,(x_1^{-1}+x_2^{-1}+\dots+x_r^{-1})^n = \Sigma c_\gamma s_\gamma \qquad (4.1)$$

となる．右辺は，既約分解に従って項をまとめたもので，s_γ は既約表現での対角和，c_γ はその重複度をあらわす．右辺の添え字のγは，整数の減少列（$\gamma_1\geq\gamma_2\geq\cdots\geq\gamma_r$）で表わされる．重複度が0でない$\gamma$が，右辺のm,nの増加に従い，どのように移っていくかをもう少し，詳しくみてみる．s_γ は$x_1,x_2,\dots,x_r$の関数で，次のように表わされることが，知られている[Ste].

$$s_\gamma(x_1,x_2,\dots,x_r) = a_{\gamma+\delta}(x_1,x_2,\dots,x_r)/\,a_\delta(x_1,x_2,\dots,x_r). \qquad (4.2)$$

ここで，$\delta = (r-1, r-2, \dots, 0)$，$a_\gamma(x_1,x_2,\dots,x_r) = \det[x_i^{\gamma_j}]$である．$s_\gamma$ は，Schur多項式の拡張になっている．

(4.1)の右辺のm,nが増加したときにs_γの分岐の様子を見れば，既約表現の分岐の様子がわかる．ここで，

$$(x_1+x_2+\cdots+x_r)a_{\gamma+\delta} = \Sigma_i\, a_{\gamma+\delta+\varepsilon_i},$$

$$(x_1^{-1}+x_2^{-1}+\cdots+x_r^{-1})a_{\gamma+\delta} = \Sigma_i\, a_{\gamma+\delta-\varepsilon_i},$$

$\varepsilon_i=(0,\cdots,0,1,0,\cdots,0)$

となることから，γは，$(\gamma_1,\gamma_2,\ldots,\gamma_r)$のどれか1つの成分を1増やす（減らす）ことによって得られる減少列に，分岐する．例えば，$r=6$，$\gamma=(2,1,1,0,0,-1)$で表わされる表現，V_γに双対空間V^*をテンソルして得られる空間は，次のように分岐する．

$$V_\gamma\otimes V^* \cong V_{(1,1,1,0,0,-1)}\oplus V_{(2,1,0,0,0,-1)}\oplus V_{(2,1,1,0,-1,-1)}\oplus V_{(2,1,1,0,0,-2)}.$$

これを図で表わすと下の図のようになる．

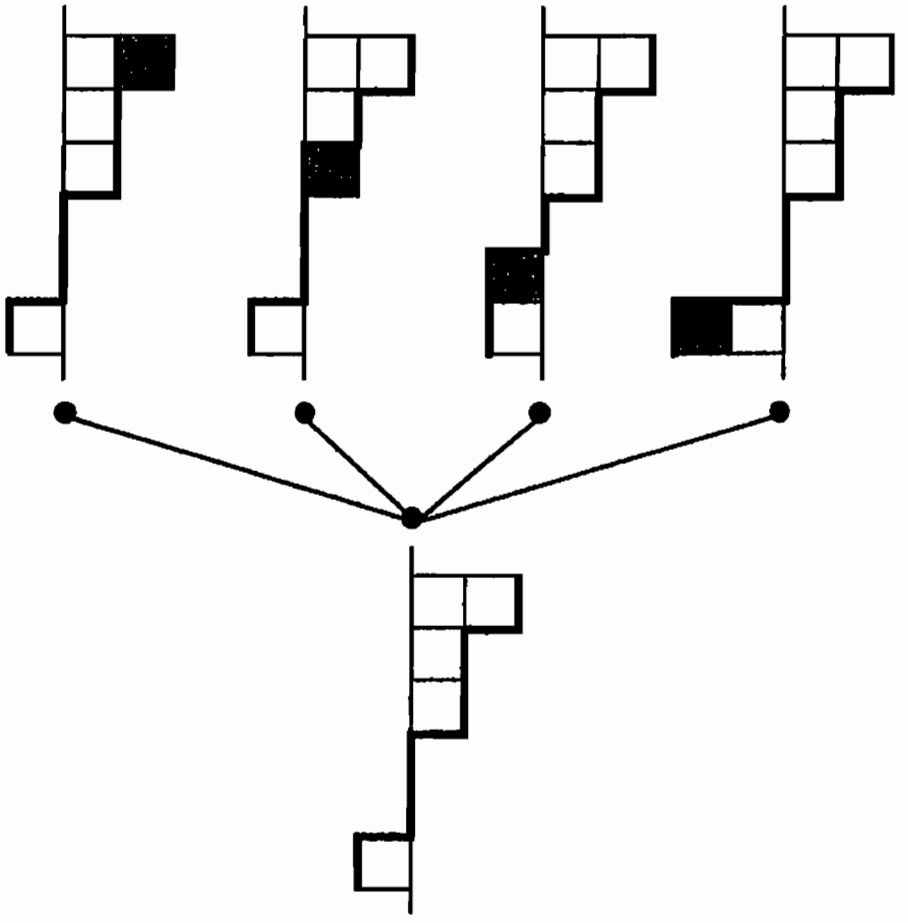


図4－3　$V_\gamma\otimes V^*$の分岐（その1）

τについては，正の部分と負の部分に分けて，分割の組で表わす方法がある．負の数は，必ず右端にまとまって現われるので，これを右側から絶対値の大きい順に表わす．この表わし方で，上記の分岐を表わすと図４－４のようになる．

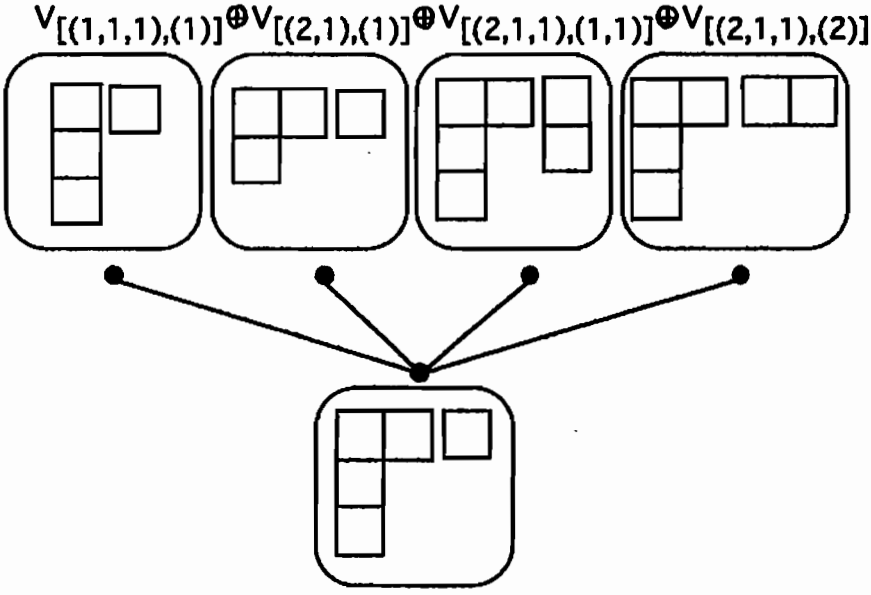
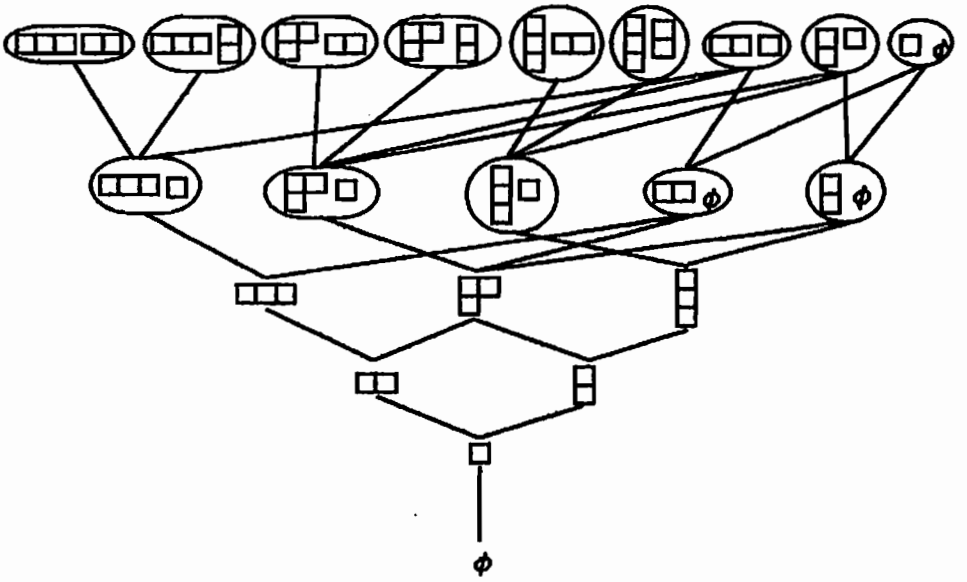


図４－４　$V_\tau \otimes V^*$の分岐（その２）

このようにして，$1 = 1 \cdot s_\tau$（$\tau = (0,0,\ldots,0)$）から始めてVをm回，V^*をn回テンソルさせたときに，s_τの分岐をグラフで表わすことができる．下の図は，m=3，n=2でrが十分に大きい場合である．



5．既約表現の構成

4．で作ったグラフは，Bratteli Digram と呼ばれ，これは，求める中心化環の（テンソルの回数の増加に伴う）増大列のTowerを表わしていると考えることができる[GHJ]. Bratteli Diagram の m+n 番目に出来る分割の組で表わされる頂点$\gamma=\gamma^{(m+n)}$を固定し，$\gamma^{(0)}=(0, 0, \ldots, 0)$で表わされる最初の頂点から$\gamma$へ至る，m+n本の辺からなる道達をbasisとする空間V_γを考え，q-rational Brauer algebra をV_γに表現する．（正確には，$C(q)\otimes V_\gamma$上の線形変換を定める．）V_γの標準基を定める道を１つ固定し，$t=t_\gamma$とおく．

T_{m-i}の定める線形変換

t_γのi-1 番目，i 番目，i+1番目の頂点に注目する．これらの頂点には，それぞれ分割ν，μ，λが与えられているとする．λは，νにboxを２つ付け加えて，得ることができる．i番目とi+1番目のboxの座標を（行列の成分のように）それぞれ，(r_i, c_i)，(r_{i+1}, c_{i+1})とするとき，$d=d(t,i)=(c_{i+1}-r_{i+1})-(c_i-r_i)$とおく．下の図の様にi番目とi+1番目のboxを鉤状に繋いだbox達をまとめてフックと呼ぶことにする．このbox達の数（両端を含める）をフックの長さとして，hとおく．i番目のboxが，i+1番目のboxの左側にあるとき，d=h-1，i番目のboxが，i+1番目のboxの上側にあるとき，d=1-hとなる．

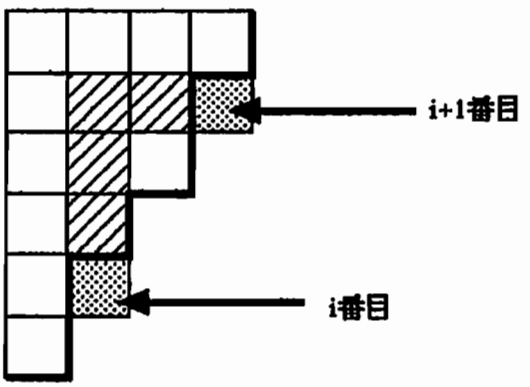


図５－１

（|d|≠1のとき）

このときi番目とi+1番目のboxを つける順序を入れ替えてできる道をt'とおく．d(t',i) = -dとなる．t，t' の定めるベクトルをそれぞれ v_t，$v_{t'}$とおき，T_{m-1}による線形変換を次のように定義する．

$$T_{m-i}v_t = (q^d/[d])v_t + ([d-1]/[d])v_{t'},$$

（d=1のとき）　$T_{m-i}v_t = qv_t$　と定める．

(d= -1のとき)　$T_{m-i}v_t = -q^{-1}v_t$　と定める.

T^*_iの定める線形変換

t_γのm+i-1 番目，m+i 番目，m+i+1番目の頂点に注目する．これらの頂点には，それぞれ整数の減少列α，β，γが与えられているとする．これらを図５－２のように表わすと，γは，αからboxを２つを取り除いて，得ることができる．m+i番目とm+i+1番目に取り除かれるboxの作るフックの長さ（取り除かれる２つのboxを含めたboxの数）をhとおく．m+iの番目操作で取り除かれるboxが，m+i+1の番目操作で取り除かれるboxより，上または右側にあるとき，d = h-1とおき，下または左側にあるとき，d = 1-h とおく．

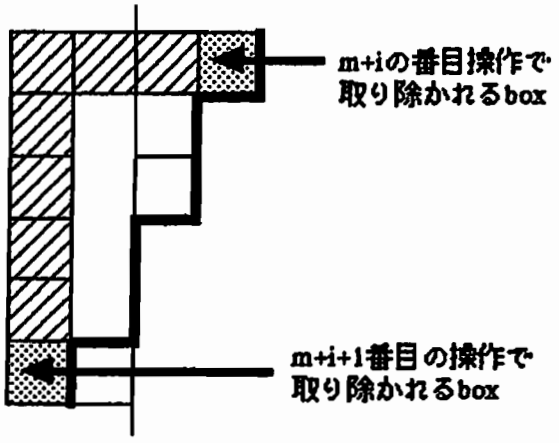


図５－２

(|d|≠1のとき)

このときm+i番目とm+i+1番目 の操作で取り除かれるboxの順序を入れ替えてできる道をt'とおく．d(t',i) = -dとなる．t，t' の定めるベクトルをそれぞれ v_t，v_t，とおき，T^*_iによる線形変換を次のように定義する.

$$T^*_i v_t = (q^d/[d])v_t + ([d+1]/[d])v_t,$$

(d =1のとき)　$T^*_i v_t = qv_t$　と定める.

(d = -1のとき)　$T^*_i v_t = -q^{-1}v_t$　と定める.

Eの定める線形変換

t_γのm-1番目，m番目，m+1番目の頂点に注目する.

(m-1番目とm+1番目に与えられた分割νが等しいとき)

νにboxを１つ付け加えてできるboxをλ_1，λ_2，…，λ_kとおく．t_γとm番目においてのみ異なる道をm番目の頂点に対応してt_1，t_2，…，t_kとする．これらの表わすベク

トルをv_{t1}, v_{t2}, …, v_{tk}とする. Eの定める線形変換を次のように, 定義する.

$Ev_t = \Sigma(w(\lambda_i)/w(\nu))v_{ti}$, ここで, $w(\lambda) = s_\lambda(q^{1-r}, q^{3-r}, \ldots, q^{r-1})$ である.

(そうでないとき) $Ev_t = 0$ とする.

以上のようにして定めた線形変換は, q-rational Brauer algebra の既約表現を定める. また, 上記の定義において, $q = 1$ を代入し, T_i, T^*_i, Eをs_i, s^*_i, eで置き換えたものは, rational Brauer algebra の既約表現を定める.

このようにして定めた既約表現について以下のことがわかる[KM].

- ●インデックスが異なると互いに非同値
- ●Bratteli Diagramは, 表現の完全代表系を与える
- ●(q-)rational algebra の次元は, (m+n)!である

6. 中心化環への表現

q-rational Brauer algebra の生成元を次の様に$V\otimes\cdots\otimes V\otimes V^*\otimes\cdots\otimes V^*$に表現すると, これらは, 1. で定めた$U_q$の作用と可環になることがわかる.

$T_i \to 1\otimes\cdots\otimes 1\otimes T\otimes 1\otimes\cdots\otimes 1 \quad (1\leq i\leq m-1)$,

ここで, $T = q\Sigma_j E_{j,j}\otimes E_{j,j} + \Sigma_{j\neq k} E_{j,k}\otimes E_{k,j} + (q-q^{-1})\Sigma_{j<k} E_{j,j}\otimes E_{k,k}$.

$T^*_i \to 1\otimes\cdots\otimes 1\otimes T^*\otimes 1\otimes\cdots\otimes 1 \quad (1\leq i\leq n-1)$,

ここで, $T^* = q\Sigma_j E_{j,j}\otimes E_{j,j} + \Sigma_{j\neq k} E_{j,k}\otimes E_{k,j} + (q-q^{-1})\Sigma_{j>k} E_{j,j}\otimes E_{k,k}$.

$E \to 1\otimes\cdots\otimes 1\otimes(\Sigma_{j,k} q^{-r+2k-1} E_{j,k}\otimes E_{j,k})\otimes 1\otimes\cdots\otimes 1$

この表現は, $r\geq m+n$のとき, injective になるので, 5. で定めた表現が, U_qの混合テンソル表現の中心化環の既約表現を定めることがわかる.

GL(r,C)の混合テンソルの中心化環も同様で, 上の定義でq=1と置き, T_i, T^*_i, Eをそれぞれ, s_i, s^*_i, eで置き換えたものは, rational Brauer algebra の表現を定め, $r\geq m+n$のとき, injectiveとなる. 従って, 5. で定めた表現が, GL(r,C)の混合テンソル表現の中心化環の既約表現を定めることがわかる.

文献

[GHJ] F.M.Goodman, P de la Harpe and V.F.R.Jones: "Coxeter Graphs and towers of Algebras", Springer-Verlag, New York, 1989.

[KM] M.Kosuda and J.Murakami: Centralizer Algebras of the Mixed Tensor

Representations of Quantum Group $U_q(gl(n,C))$, Osaka J.Math. 30 (1993), 475-507.

[Ste] J.R.Stembridge: Rational tableaus and the tensor algebra of gl_n, J.Combinatorial Theory A46(1987), 79-102.

Spectral Characterizations of Some Generalized Odd Graphs

Tayuan Huang*
Department of Mathematics
Kyushu University
and
Chao-Rong Liu
Institute of Mathematics
Academia Sinica
Taipei, Taiwan

September 12, 1995

Abstract

Suppose that G is a connected, k-regular graph such that $Spec(G) = Spec(\Gamma)$ where Γ is a distance-regular graph with parameters $a_1 = a_2 = \cdots = a_{d-1} = 0$ and $a_d > 0$; *i.e.*, a generalized odd graph, we show that G must be distance-regular with the same intersection array as that of Γ in terms of the notion of Hoffman polynomials. Furthermore, G is isomorphic to Γ if Γ is one of the odd polygons C_{2d+1}, the odd graphs O_{d+1}, the folded $(2d+1)$-cube, the coset graph of the binary Golay code, the Hoffman-Singleton graph, the Gewirtz graph, the Higman-Sims graph, or the second subconstituent of the Higman-Sims graph.

1 Introduction

We shall consider only finite undirected graphs without loops and multiple edges. Let $G = (V(G), E(G))$ be a connected, k-regular graph and A an adjacency matrix of G, which is

*On leave from Department of Applied Mathematics, National Chiao-Tung University, Hsinchu, Taiwan
e-mail: thuang@math.nctu.edu.tw

row-indexed, as well as column-indexed by the vertices of G; also let A^i be the usual matrix product of i copies of A, and $A^i(x,y)$ be the entry of A at row x and column y. Suppose λ is an eigenvalue of A, then, since A is symmetric, λ is real, and the multiplicity of λ as a root of the characteristic equation $det(\lambda I - A) = 0$ is equal to the dimension of the eigen space corresponding to λ. The spectrum of A is called the *spectrum* of the graph G, denoted by

$$Spec(G) = (k^{m_0}, {\theta_1}^{m_1}, \cdots, {\theta_{s-1}}^{m_{s-1}})$$

where $k > \theta_1 > \cdots > \theta_{s-1}$ are distinct eigenvalues together with their multiplicities $m_0 = 1$, $m_1, \cdots$, and m_{s-1} respectively; refer to [3] for more details.

Now assume Γ is a connected graph with diameter d, let $\Gamma_i(x) = \{y | y \in V(\Gamma)$ and $d(x,y) = i\}$, where $V(\Gamma)$ is the vertex set of Γ and $d(x,y)$ is the distance between vertices x and y. Γ is called *distance-regular* if the parameters $c_i = |\Gamma_{i-1}(x) \cap \Gamma_1(y)|$, $a_i = |\Gamma_i(x) \cap \Gamma_1(y)|$ and $b_i = |\Gamma_{i+1}(x) \cap \Gamma_1(y)|$ depend not on particular vertices x and y we choose, but only on the distance $i = d(x,y)$ between them. It is clear that $c_0 = b_d = 0$, $c_1 = 1$, $b_0 = |\Gamma_1(x)|$ for each $x \in V(\Gamma)$, and $a_i = b_0 - b_i - c_i$. The following array

$$\begin{bmatrix} c_0 & c_1 & c_2 & c_3 & \cdots & c_{d-1} & c_d \\ a_0 & a_1 & a_2 & a_3 & \cdots & a_{d-1} & a_d \\ b_0 & b_1 & b_2 & b_3 & \cdots & b_{d-1} & b_d \end{bmatrix}$$

or $\{b_0, b_1, \ldots, b_{d-1}; c_1, c_2, \ldots, c_d\}$ is called *the intersection array of* Γ. *Generalized odd graphs* of diameter d are distance regular graphs of diameter d with parameters $a_1 = a_2 = \cdots = a_{d-1} = 0$, and $a_d > 0$. The odd polygons C_{2d+1}, the odd graphs O_{d+1}, the folded $(2d+1)$-cube (both defined in section 2), the coset graph of binary Golay code, the coset graph of the truncated binary Golay code, the Hoffman-Singleton graph, the Gewirtz graph, the Higman-Sims graph, and the second subconstituent of the Higman-Sims graph are examples of generalized odd graphs, refer to [5] as shown in the table in section 2 for further details.

One can see from the spectrum of a graph whether it is regular and connected, strongly regular, or whether it is bipartite distance-regular of diameter 3, but one can not tell its distance-regularity directly [5, p.263]. However, it is known that a connected, regular graph with diameter d has at least $d+1$ distinct eigenvalues and that distance regular graphs of diameter d have exactly $d+1$ distinct eigenvalues. It seems interesting to study the distance-regularity of those graphs of diameter d with exactly $d+1$ distinct eigenvalues. The distance-regularity of graphs with the same spectra of some distance-regular graphs have been studied under some additional properties, for example: with large girth [6], with diameter 3 and $\mu = 1$ [10], with diameter 4 and prescribed λ, k_2 [8]. All graphs with spectra of distance-regular graphs with at most 30 vertices can be found in [11]. Following the

work in [13], the relationship between distance-regularity and spectrum of connected regular graphs will be further studied in this paper.

One of the significant links between spectra and connectedness, regularity of graphs is the so called *Hoffman Polynomial*. For a connected, k-regular graph G with $Spec(G) = (k, \theta - 1^{m-1}, \cdots, \theta_{s-1}{}^{m_{s-1}})$, let $q(x) = \prod_{i=1}^{s-1}(x - \theta_i)$, then $p(x) = \frac{|V(G)|}{q(k)}q(x)$ is called the *Hoffman Polynomial* of G. It is the polynomial of the smallest degree such that $p(A) = J$, where A is an adjacency matrix of G and J is the all-one matrix of order $|V(G)|$, and plays a critcal role in the proof of the main theorem. Some common properties, for example their common minimal polynomials and their *Hoffman polynomials*, of connected regular graphs with the same spectrum as that of generalized graphs are given is section 2. Based on these informations, together with some known characterizations in terms of their intersection arrays among distance-regular graphs, the main result of this paper is proved in Section 3, this provides an affirmative answer to the question mentioned by Cvetković [7, p.36] that whether the Odd graphs can be characterized by their spectra among connected regular graphs.

Main Theorem *If G is a connected regular graph which has the same spectrum as that of a generalized odd graph Γ of diameter d, then G is distance regular with the same intersection array as that of Γ. Furthermore, if Γ is one of the following : the odd polygons C_{2d+1}, the odd graph O_{d+1}, the folded $(2d+1)$-cube, the coset graph of the binary Golay code, the Hoffman-Singleton graph, the Gewirtz graph, the Higman-Sims graph, or the second subconstituent of the Higman-Sims graph, then G is isomorphic to Γ.*

The following corollary follows immediately from a theorem of Tutte [16].

Corollary : *If G is a connected regular graph which has the same deck of 1-vertex-deleted subgraphs as that of a Generalized Odd graph Γ, then G is a distance regular graph with the same intersection array as that of Γ.*

2 Hoffman Polynomials of Generalized Odd Graphs

Throughout the rest of this paper, we assume that G is a connected k-regular graph with $Spec(G) = Spec(\Gamma) = (\theta_0^{m_0}, \theta_1^{m_1}, \theta_2^{m_2}, \cdots, \theta_d^{m_d})$ with $\theta_0 = k$, and $m_0 = 1$, where Γ is a generalized odd graph of diameter d with intersection array

$$\begin{bmatrix} c_0 & c_1 & c_2 & c_3 & \cdots & c_{d-1} & c_d \\ 0 & 0 & 0 & 0 & \cdots & 0 & a_d \\ b_0 & b_1 & b_2 & b_3 & \cdots & b_{d-1} & b_d \end{bmatrix}.$$

Furthermore, let A be an adjacency matrix of G. The common *Hoffman polynomial* for the graphs Γ and G in terms of their common spectrum is given in this section, which provides a way to show the distance-regularity of G in the next section.

Clearly, odd polygons C_{2d+1} are generalized odd graphs of diameter d with intersection array $\{2, 1, \cdots, 1; 1, 1, \cdots, 1\}$. We now recall some examples, families or sparadic, of generalized odd graphs.

1. Let k be an integer with $k \geq 2$,the Odd graph O_k of characteristic k has the $(k-1)$-subsets of $\{1,2, \cdots, 2k-1\}$ as vertices, and two vertices are adjacent if and only if their corresponding subsets are disjoint. The small odd graphs are the triangle $K_3(k = 2)$, and the Petersen graph $(k = 3)$. In general, the odd graph O_k are distance-regular graphs of diameter $k-1$ with intersection array

   (a)

$$\begin{bmatrix} 0 & 1 & 1 & 2 & 2 & \cdots & d-1 & d-1 & d \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & d \\ 2d & 2d-1 & 2d-1 & 2d-2 & 2d-2 & \cdots & d+1 & d+1 & 0 \end{bmatrix}$$

   for the case $k = 2d$, and

   (b)

$$\begin{bmatrix} 0 & 1 & 1 & 2 & 2 & \cdots & d & d \\ 0 & 0 & 0 & 0 & 0 & \cdots & 0 & d+1 \\ 2d+1 & 2d & 2d & 2d-1 & 2d-1 & \cdots & d+1 & 0 \end{bmatrix}$$

   for the case $k = 2d+1$.

   The eigenvalues of O_k are the integers $\theta_i = (-1)^i(k-i)$ with multiplicities $m_i = \binom{2k-1}{i} - \binom{2k-1}{i-1}$ respectively for $0 \leq i \leq k-1$. The Odd graphs are uniquely determined by their intersection arrays by Moon [14], or refer to [5, p.260] among distance-regular graphs.

2. Folded $(2d+1)$-cube is the graph defined on the partitions of an $(2d+1)$-set into two subsets, and two partitions being adjacent when their common refinement contains a set of size one. The intersection array is given by

$$\begin{bmatrix} 0 & 1 & 2 & 3 & \cdots & d-1 & d \\ 0 & 0 & 0 & 0 & \cdots & 0 & d+1 \\ 2d+1 & 2d & 2d-1 & 2d-2 & \cdots & d+2 & 0 \end{bmatrix},$$

and its eigenvalues and multiplicities are $\theta_j = 2d+1-4j$ with $m_j = \binom{2d+1}{2j}$, $j \leq d$. The folded $(2d+1)$-cubes is also uniquely determined by its intersection array [5, p.264].

In addition to these two families, Moore graphs, *i.e.*, distance-regular graphs with diameter d and with the intersection array

$$\begin{bmatrix} 0 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & k-1 \\ k & k-1 & k-1 & k-1 & \cdots & k-1 & 0 \end{bmatrix}$$

provide another family of generalized odd graphs, refer to [3] for more details. It is known that the intersection array for a Moore graph with valency $k \geq 3$, and girth $g \geq 5$ is feasible if and only if $g = 5$ and $k \in \{3, 7, 57\}$. The case k = 3, 7 are realized by the Petersen graph and the Hoffman-Singleton graph respectively. The existence of a Moore graph with k = 57 remains open, which can not be distance transitive if it exists. Some other sporadic generalized odd graphs are given in the following table, whether these graphs are uniquely determined by their intersection arrays are indicated too.

diameter	intersection array	examples	uniqueness	remarks
d=2	{3,2;1,1}	O_3	Yes	Moore graph
	{7,6;1,1}	Hoffman-Singleton graph	Yes	Moore graph [5, p.391]
	{57,56;1,1}	?		
	{5,4;1,2}	complement of Clebsch graph	Yes	folded 5-cubes [5, p.104]
	{10,9;1,2}	Gewirtz graph	Yes	[5, p.372]
	{16,15;1,4}	the second subconstituent of the Higman-Sims graph	Yes	[5, p.394]
	{22,21;1,6}	the Higman-Sims graph	Yes	[9, p.933]
d=3	{7,6,6;1,1,2}	?		[5, p.148]
	{23,22,21;1,2,3}	the coset graph of the binary Golay code	Yes	[5, p.361]
	{22,21,20;1,2,6}	the coset graph of the truncated binary Golay code	?	[5, p.362]

For $x, y \in V(G)$ at distance i, let

$$|G_j(x) \cap G_1(y)| = \begin{cases} c_i(x,y) & if \ \ j = i-1, \\ a_i(x,y) & if \ \ j = i, \\ b_i(x,y) & if \ \ j = i+1. \end{cases}$$

To show the distance-regularity of G is equivalent to show that all $c_i(x,y)$, $a_i(x,y)$ and $b_i(x,y)$ are functions of $i = d(x,y)$ only, independent of the choice of x and y for all i with $0 \leq i \leq d$. We achieve this by showing that some systems of linear equations related to the *Hoffman polynomial* have their unique solutions.

We now turn to the explicit expression of the common *Hoffman polynomial* for G and Γ. Since $A^{j+1}(x,y) = (A^jA)(x,y) = \sum_{z \in G_1(y)} A^j(x,z)$, and $G_j(x) \cap G_1(y)$ is empty if $j \neq i-1$, i or $i+1$ whenever $x, y \in V(G)$ are at distance i. Lemma 2.1 is obvious, which is included here for later reference.

Lemma 2.1 *If $d(x,y) = i$, then*

$$A^{j+1}(x,y) = \sum_{z \in G_1(y) \cap G_{i-1}(x)} A^j(x,z) + \sum_{z \in G_1(y) \cap G_i(x)} A^j(x,z) + \sum_{z \in G_1(y) \cap G_{i+1}(x)} A^j(x,z).$$

In particular,

$$A^i(x,y) = \sum_{z \in G_1(y) \cap G_{i-1}(x)} A^{i-1}(x,z).$$

The spectrum of G shall shed some light on the structure of G via that of Γ. Since $A^i(x,y)$ indicates the number of walks of length i in G joining x and y, it follows that the number of closed walks in G of length $2i+1$ is $Tr(A^{2i+1}) = \sum_{j=0}^{d} m_i {\theta_j}^{2i+1}$. On the other hand, $a_i = 0 (i \leq d-1)$ for generalized odd graphs, they have no odd cycles of length up to $2d-1$, it follows that $\sum_{j=0}^{d} m_j {\theta_j}^{2j+1} = 0$, and hence $A^{2i+1}(x,x) = 0$. These observations are summarized in the following.

Lemma 2.2 *1.* $A^{2i+1}(x,x) = 0$ *for* $i \leq d-1$,

2. $A^{2i+1-j}(x,y) = 0$ *for* $y \in G_j(x)$ *and* $1 \leq j \leq i$, *and*

3. $a_i(x,y) = 0$ *for all* $y \in G_i(x)$ *and* $i \leq d-1$.

Furthermore, the common minimal polynomial $m(x)$ of Γ, and hence of G, is given by

$m(x) = \det(xI - B) = (x-\theta_0)(x-\theta_1)(x-\theta_2)\cdots(x-\theta_d)$, where

$$B = \begin{bmatrix} 0 & c_1 & & & & 0 \\ b_0 & 0 & c_2 & & & \\ & b_1 & 0 & c_3 & & \\ & & \cdots & \cdots & & \\ & & & \cdots & \cdots & \\ & & & b_{d-2} & 0 & c_d \\ 0 & & & & b_{d-1} & a_d \end{bmatrix}_{(d+1)\times(d+1)}$$

is the intersection matrix of Γ. Let

$$\begin{aligned} q(x) &= m(x)/(x-\theta_0) \\ &= (x-\theta_1)(x-\theta_2)\cdots(x-\theta_d) \\ &= x^d + q_{d-1}x^{d-1} + q_{d-2}x^{d-2} + \cdots + q_2x^2 + q_1x^1 + q_0. \end{aligned} \tag{1}$$

Based on the property that $a_1 = \cdots = a_{d-1} = 0$, the coefficients of $q(x)$ can be expressed systematically in terms of the parameters b_i and c_i of Γ.

In general, let $\lambda = \lfloor d/2 \rfloor$, $\mu = \lceil d/2 \rceil$, and let

$$P_s^l = (-1)^{(l-s+1)/2} c_s c_{s+1} \cdots c_{l-1} c_l$$

whenever $l - s$ is positive and odd. The explicit expressions for the polynomials $m(x)$ and $q(x)$ and hence for the coefficients $q_i, 0 \le i \le d-1$, of $q(x)$ are given in the following. Note that $a_d \neq 0$ occurs in terms of the second half of $m(x)$ and c_d occurs in each term of the second half of $q(x)$ which play a critical role in the proof of the main theorem. For convenience, let $i_0 = -2$.

$$\begin{aligned} m(x) &= x^{d+1} \\ &+ \sum_{t=1}^{\mu} (-1)^t \left(\sum_{i_1=0}^{d-(2t-1)} b_{i_1} c_{i_1+1} \left(\sum_{i_2=i_1+2}^{d-(2t-3)} b_{i_2} c_{i_2+1} \left(\cdots \left(\sum_{i_{t-1}=i_{t-2}+2}^{d-3} b_{i_{t-1}} c_{i_{t-1}+1} \left(\sum_{i_t=i_{t-1}+2}^{d-1} b_{i_t} c_{i_t+1} \right) \right) \cdots \right) \right) \right) x^{d-2t+1} \\ &- a_d x^d \\ &+ a_d \sum_{s=1}^{\lambda} (-1)^{s+1} \left(\sum_{i_1=0}^{d-2s} b_{i_1} c_{i_1+1} \left(\sum_{i_2=i_1+2}^{d-(2s-2)} b_{i_2} c_{i_2+1} \left(\cdots \left(\sum_{i_{s-1}=i_{s-2}+2}^{d-2} b_{i_{s-1}} c_{i_{s-1}+1} \left(\sum_{i_s=i_{s-1}+2}^{d-2} b_{i_s} c_{i_s+1} \right) \right) \cdots \right) \right) \right) x^{d-2s} \end{aligned}$$

and

$$q(x) = x^d$$

$$+\sum_{t=1}^{\lambda}(-1)^t\left(P^d_{d-2t+1}+\sum_{i_1=0}^{d-2t}b_{i_1}c_{i_1+1}\left(P^d_{d-2t+3}+\sum_{i_2=i_1+2}^{d-2t+2}b_{i_2}c_{i_2+1}\left(\cdots\right.\right.\right.$$

$$\left.\left.\left.\cdots\left(P^d_{d-3}+\sum_{i_{t-1}=i_{t-2}+2}^{d-4}b_{i_{t-1}}c_{i_{t-1}+1}\left(P^d_{d-1}+\sum_{i_t=i_{t-1}+2}^{d-2}b_{i_t}c_{i_t+1}\right)\right)\cdots\right)\right)\right)x^{d-2t}$$

$$+c_dx^{d-1}$$

$$+c_d\sum_{s=1}^{\mu-1}(-1)^s\left(P^{d-1}_{d-2s}+\sum_{i_1=0}^{d-2s-1}b_{i_1}c_{i_1+1}\left(P^{d-1}_{d-2s+2}+\sum_{i_2=i_1+2}^{d-2s+1}b_{i_2}c_{i_2+1}\left(\cdots\right.\right.\right.$$

$$\left.\left.\left.\cdots\left(P^{d-1}_{d-4}+\sum_{i_{s-1}=i_{s-2}+2}^{d-5}b_{i_{s-1}}c_{i_{s-1}+1}\left(P^{d-1}_{d-2}+\sum_{i_s=i_{s-1}+2}^{d-3}b_{i_s}c_{i_s+1}\right)\right)\cdots\right)\right)\right)x^{d-2s-1}.$$

We conclude the above observations in the following lemma.

Lemma 2.3 *Let* $q(x)=x^d+c_dx^{d-1}+\sum_{i=0}^{d-2}q_ix^i$ *as given in (1), then the coefficients are*

$$q_{d-2t}$$

$$=\quad(-1)^t\left(P^d_{d-2t+1}+\sum_{i_1=0}^{d-2t}b_{i_1}c_{i_1+1}\left(P^d_{d-2t+3}+\sum_{i_2=i_1+2}^{d-2t+2}b_{i_2}c_{i_2+1}\left(\cdots\left(P^d_{d-1}+\sum_{i_t=i_{t-1}+2}^{d-2}b_{i_t}c_{i_t+1}\right)\cdots\right)\right)\right)$$

for $1\le t\le\lfloor d/2\rfloor$, and

$$q_{d-2s-1}$$

$$=\quad c_d(-1)^s\left(P^{d-1}_{d-2s}+\sum_{i_1=0}^{d-2s-1}b_{i_1}c_{i_1+1}\left(P^{d-1}_{d-2s+2}+\sum_{i_2=i_1+2}^{d-2s+1}b_{i_2}c_{i_2+1}\left(\cdots\left(P^{d-1}_{d-2}+\sum_{i_s=i_{s-1}+2}^{d-3}b_{i_s}c_{i_s+1}\right)\cdots\right)\right)\right)$$

for $1\le s\le\lceil d/2\rceil-1$.

The expressions for those coefficients of the polynomial $q(x)$ are used in the next section. Let $v=\frac{q(\theta_0)}{|V(G)|}$, then $q(A)=vJ$ where J is the all one matrix of order $|V(G)|$ [12]. Multiplying A^i on both sides of the equation $q(A)=vJ$, and since $AJ=\theta_0J$, we have $A^iq(A)=\theta_0{}^ivJ$, $0\le i\le d-1$. The information contained in this system of matrix equations can be translated into a set of systems of linear equations in variables $A^i(x,y)$ and with the coefficients of $q(x)$ as its coefficients. Further details will be worked in the next section.

3 Proof of the Main Theorem

Following the same notations used in section 2, we shall show that $c_i(x,y)$, $a_i(x,y)$ and $b_i(x,y)$ are functions of $i=d(x,y)$ only, independent of the choice of x and y, $0\le i\le d$, by

showing that each system mentioned in the end of section 2 has a unique solution. Indeed, the distance structure of the generalized odd graph Γ provides nontrivial solutions for these systems. We shall show in this section that each of their coefficient matrices has nonzero determinants, which shows the uniqueness of their solutions.

Clearly, $a_i = a_i(x,y) = 0$ whenever x, y are at distance i at most $d-1$ as shown in Lemma 2.2. To determine $c_i(x,y)$, $b_i(x,y) = b_0 - c_i(x,y) - a_i(x,y)$ whenever $x, y \in V(G)$ at distance i, $0 \leq i \leq d-1$, we shall show the uniqueness of $A^i(x,y)$ with $d(x,y) = i$, $2 \leq i \leq d-1$ by solving the following system of linear equations obtained from $q(A) = vJ$,

$$\begin{cases} A^{d-1-i}q(A) &= v{\theta_0}^{d-1-i}J \\ A^{d-2-i}q(A) &= v{\theta_0}^{d-2-i}J \\ \vdots & \\ A^2q(A) &= v{\theta_0}^2J \\ A^1q(A) &= v{\theta_0}^1J \\ A^0q(A) &= v{\theta_0}^0J \end{cases}$$

at entries (x,y) for vertices x and y at distance i, $2 \leq i \leq d-1$.

Indeed, for vertices x, y at distance i, $2 \leq i \leq d-1$, clearly $A^i(x,y) = 0$ if $i < d(x,y)$ or if $i + d(x,y) \leq 2d-1$ is odd by Lemma 2.2, the others $A^l(x,y)$ can be regarded as variables. More precisely, for vertices x and y at distance 2, $A(x,y) = A^3(x,y) = A^5(x,y) = \cdots = A^{2d-3}(x,y) = 0$, the above system can be simplified into

$$\begin{bmatrix} q_{d-1} & q_{d-3} & q_{d-5} & \cdots & q_5 & q_3 & q_1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & q_{d-2} & q_{d-4} & \cdots & q_6 & q_4 & q_2 & q_0 & 0 & 0 & \cdots & 0 & 0 \\ \hline 0 & q_{d-1} & q_{d-3} & \cdots & q_7 & q_5 & q_3 & q_1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & q_{d-2} & \cdots & q_8 & q_6 & q_4 & q_2 & q_0 & 0 & \cdots & 0 & 0 \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \hline 0 & 0 & 0 & \cdots & 0 & q_{d-1} & q_{d-3} & q_{d-5} & q_{d-7} & q_{d-9} & \cdots & q_3 & q_1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & q_{d-2} & q_{d-4} & q_{d-6} & q_{d-8} & \cdots & q_4 & q_2 \end{bmatrix} \begin{bmatrix} A^{2d-4}(x,y) \\ A^{2d-6}(x,y) \\ A^{2d-8}(x,y) \\ A^{2d-10}(x,y) \\ \vdots \\ A^4(x,y) \\ A^2(x,y) \end{bmatrix} = v \begin{bmatrix} k^{d-3} \\ k^{d-4} \\ k^{d-5} \\ k^{d-6} \\ \vdots \\ k^1 \\ k^0 \end{bmatrix}$$

whenever d is even; or

$$\left[\begin{array}{cccccccccccc}
q_{d-1} & q_{d-3} & q_{d-5} & \cdots & q_6 & q_4 & q_2 & q_0 & 0 & 0 & \cdots & 0 & 0 \\
1 & q_{d-2} & q_{d-4} & \cdots & q_7 & q_5 & q_3 & q_1 & 0 & 0 & \cdots & 0 & 0 \\
\hline
0 & q_{d-1} & q_{d-3} & \cdots & q_8 & q_6 & q_4 & q_2 & q_0 & 0 & \cdots & 0 & 0 \\
0 & 1 & q_{d-2} & \cdots & q_9 & q_7 & q_5 & q_3 & q_1 & 0 & \cdots & 0 & 0 \\
\hline
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\hline
0 & 0 & 0 & \cdots & 0 & q_{d-1} & q_{d-3} & q_{d-5} & q_{d-7} & q_{d-9} & \cdots & q_2 & q_0 \\
0 & 0 & 0 & \cdots & 0 & 1 & q_{d-2} & q_{d-4} & q_{d-6} & q_{d-8} & \cdots & q_3 & q_1 \\
\hline
0 & 0 & 0 & \cdots & 0 & 0 & q_{d-1} & q_{d-3} & q_{d-5} & q_{d-7} & \cdots & q_4 & q_2
\end{array}\right]
\left[\begin{array}{c}
A^{2d-4}(x,y) \\
A^{2d-6}(x,y) \\
\hline
A^{2d-8}(x,y) \\
A^{2d-10}(x,y) \\
\hline
\vdots \\
\hline
A^6(x,y) \\
A^4(x,y) \\
\hline
A^2(x,y)
\end{array}\right]
= v
\left[\begin{array}{c}
k^{d-3} \\
k^{d-4} \\
\hline
k^{d-5} \\
k^{d-6} \\
\hline
\vdots \\
\hline
k^2 \\
k^1 \\
\hline
k^0
\end{array}\right]$$

whenever d is odd.

Similarly for vertices x, y at distance 3, substituting $A(x,y) = A^2(x,y) = A^4(x,y) = A^6(x,y) = \cdots = A^{2d-4}(x,y) = 0$, the above system can also be simplified into

$$\left[\begin{array}{cccccccccccc}
q_{d-1} & q_{d-3} & q_{d-5} & \cdots & q_5 & q_3 & q_1 & 0 & 0 & 0 & \cdots & 0 \\
1 & q_{d-2} & q_{d-4} & \cdots & q_6 & q_4 & q_2 & q_0 & 0 & 0 & \cdots & 0 \\
\hline
0 & q_{d-1} & q_{d-3} & \cdots & q_7 & q_5 & q_3 & q_1 & 0 & 0 & \cdots & 0 \\
0 & 1 & q_{d-2} & \cdots & q_8 & q_6 & q_4 & q_2 & q_0 & 0 & \cdots & 0 \\
\hline
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\hline
0 & 0 & 0 & \cdots & 0 & q_{d-1} & q_{d-3} & q_{d-5} & q_{d-7} & q_{d-9} & \cdots & q_3
\end{array}\right]
\left[\begin{array}{c}
A^{2d-5}(x,y) \\
A^{2d-7}(x,y) \\
\hline
A^{2d-9}(x,y) \\
A^{2d-11}(x,y) \\
\hline
\vdots \\
\hline
A^3(x,y)
\end{array}\right]
= v
\left[\begin{array}{c}
k^{d-4} \\
k^{d-5} \\
\hline
k^{d-6} \\
k^{d-7} \\
\hline
\vdots \\
\hline
k^0
\end{array}\right]$$

whenever d is even; or

$$\left[\begin{array}{cccccccccccc}
q_{d-1} & q_{d-3} & q_{d-5} & \cdots & q_6 & q_4 & q_2 & q_0 & 0 & 0 & \cdots & 0 \\
1 & q_{d-2} & q_{d-4} & \cdots & q_7 & q_5 & q_3 & q_1 & 0 & 0 & \cdots & 0 \\
\hline
0 & q_{d-1} & q_{d-3} & \cdots & q_8 & q_6 & q_4 & q_2 & q_0 & 0 & \cdots & 0 \\
0 & 1 & q_{d-2} & \cdots & q_9 & q_7 & q_5 & q_3 & q_1 & 0 & \cdots & 0 \\
\hline
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
\hline
0 & 0 & 0 & \cdots & 0 & q_{d-1} & q_{d-3} & q_{d-5} & q_{d-7} & q_{d-9} & \cdots & q_2 \\
0 & 0 & 0 & \cdots & 0 & 1 & q_{d-2} & q_{d-4} & q_{d-6} & q_{d-8} & \cdots & q_3
\end{array}\right]
\left[\begin{array}{c}
A^{2d-5}(x,y) \\
A^{2d-7}(x,y) \\
\hline
A^{2d-9}(x,y) \\
A^{2d-11}(x,y) \\
\hline
\vdots \\
\hline
A^5(x,y) \\
A^3(x,y)
\end{array}\right]
= v
\left[\begin{array}{c}
k^{d-4} \\
k^{d-5} \\
\hline
k^{d-6} \\
k^{d-7} \\
\hline
\vdots \\
\hline
k^1 \\
k^0
\end{array}\right]$$

whenever d is odd.

We shall show later in Lemma 3.1 that the coefficient matrices in both cases can be transformed into upper triangular matrices with entries 1 along their main diagonal, it follows that $A^2(x,y) = c_2(x,y)$ is a constant, say c_2, whenever $x, y \in V(G)$ at distance 2, and $A^3(x,y)$ is also a constant whenever $x, y \in V(G)$ at distance 3. Note that these coefficients

matrices for the case i = 2 were arranged so that rows $2r+1, 2r+2$ can be obtained from previous two rows by moving one entry to right for $1 \le r \le \lfloor d/2 \rfloor - 2$, except the final row in case of odd d. Those processes can be performed successively for all $2 \le i \le d-1$.

Let $\mathbf{E_{d,0}}$ be the coefficient matrix given in the case $i = 2$, and $\mathbf{E_{d,i-2}}$ be the submatrix obtained from $\mathbf{E_{d,0}}$ by deleting the last $i-2$ rows as well as the last $i-2$ columns. So we only need to prove $\det \mathbf{E_{d,0}} \neq 0$, it follows that that $\det \mathbf{E_{d,i-2}} \neq 0$. The system (2) can be simplified into a system of linear equations

$$\mathbf{E_{d,i-2}} \begin{bmatrix} A^{2d-2-i}(x,y) \\ A^{2d-4-i}(x,y) \\ A^{2d-6-i}(x,y) \\ \vdots \\ A^{i+4}(x,y) \\ A^{i+2}(x,y) \\ A^{i}(x,y) \end{bmatrix} = v \begin{bmatrix} k^{d-1-i} \\ k^{d-2-i} \\ k^{d-3-i} \\ \vdots \\ k^{2} \\ k^{1} \\ k^{0} \end{bmatrix}$$

Clearly, these systems have nontrivial solutions through the distance regularity of the given generalized odd graph Γ. The uniqueness of $A^i(x,y)$ with $x, y \in V(G)$ at distance i follows from the fact that $\det \mathbf{E_{d,0}} \neq 0$ and that $\det(\mathbf{E_{d,i-2}}) \neq 0$ for $2 \le i \le d-1$ as given in Lemma 3.1, which will be proved later.

Lemma 3.1 $\det(\mathbf{E_{d,0}}) \neq 0$, $\det(\mathbf{E_{d,i-2}}) \neq 0$, *for* $2 \le i \le d-1$.

The following corollary follows easily.

Corollary 3.2 *$A^i(x,y)$ is a constant for $x, y \in V(G)$ at distance i, $2 \le i \le d-1$. Moreover, $A^d(x,y) = v$ whenever $x, y \in V(G)$ at distance d.*

For vertices x, y and z in $V(G)$ with $d(x,y) = i$ and $d(z,x) = i-1$, both $A^i(x,y)$ and $A^{i-1}(x,z)$ are constants respectively as shown in Corollary 3.2. By Lemma 2.1,

$$A^i(x,y) = \sum_{w \in G_1(y) \cap G_{i-1}(x)} A^{i-1}(x,w) = c_i(x,y) A^{i-1}(x,z),$$

it follows that both $c_i(x,y)$ and $b_i(x,y) = b_0 - c_i(x,y) - a_i(x,y)$ are constants. For vertices x, $y \in V(G)$ at distance d, $A^d(x,y) = v$ is equal to $c_d(x,y)$ multiplied by an absolute constant, hence $c_d(x,y)$ is a constant too, say c_d.

Lemma 3.3 *$c_i(x,y)$, $b_i(x,y)$ are constants, say c_i, b_i, respectively whenever x, $y \in V(G)$ at distance $i \leq d-1$. Moreover, $c_d(x,y)$ and hence $a_d(x,y)$ are constants, say c_d, a_d respectively, whenever $d(x,y) = d$.*

Up to this point, combining Lemmas 2.2 and 3.3 we may conclude that G is a distance regular graph of diameter d with the same intersection array as that of Γ, this proves the first half of the Main Theorem. Those graphs mentioned in the Main Theorem are all generalized odd graphs which are uniquelly determined by their intersection array as we mentioned in section 2. Hence the second half of the Main Theorem follows immediately.

In the rest of this paper, we shall prove Lemma 3.1 in an algorithmic way. Since c_d is a common factor for all entries on the odd rows of $\mathbf{E_{d,0}}$ as shown in Lemma 2.3, let M_1 be the matrix obtained from $\mathbf{E_{d,0}}$ by factoring out c_d for all entries along the odd rows and others remained unchanged. Based on the expressions of the coefficients of the polynomial $q(x)$ given in Lemma 2.3, in order to deal with these matrices in a convenient way, let $S_{0,j} = F_{0,j} = 1$ for convenience, and let

$$
\begin{aligned}
&F_{m,i} \\
&= (-1)^m \Bigg(P^{d-2i+1}_{d-2i-(2m-2)} + \sum_{i_1=0}^{d-2i-(2m-1)} b_{i_1} c_{i_1+1} \Bigg(P^{d-2i+1}_{d-2i-(2m-4)} + \sum_{i_2=i_1+2}^{d-2i-(2m-3)} b_{i_2} c_{i_2+1} \Bigg(\cdots \\
&\qquad \cdots \Bigg(P^{d-2i+1}_{d-2i-2} + \sum_{i_{m-1}=i_{m-2}+2}^{d-2i-3} b_{i_{m-1}} c_{i_{m-1}+1} \Bigg(P^{d-2i+1}_{d-2i} + \sum_{i_m=i_{m-1}+2}^{d-2i-1} b_{i_m} c_{i_m+1} \Bigg) \Bigg) \cdots \Bigg) \Bigg) \Bigg)
\end{aligned}
$$

and

$$
\begin{aligned}
&S_{m,i} \\
&= (-1)^m \Bigg(P^{d-2i+2}_{d-2i-(2m-3)} + \sum_{i_1=0}^{d-2i-(2m-2)} b_{i_1} c_{i_1+1} \Bigg(P^{d-2i+2}_{d-2i-(2m-5)} + \sum_{i_2=i_1+2}^{d-2i-(2m-4)} b_{i_2} c_{i_2+1} \Bigg(\cdots \\
&\qquad \cdots \Bigg(P^{d-2i+2}_{d-2i-1} + \sum_{i_{m-1}=i_{m-2}+2}^{d-2i-2} b_{i_{m-1}} c_{i_{m-1}+1} \Bigg(P^{d-2i+2}_{d-2i+1} + \sum_{i_m=i_{m-1}+2}^{d-2i} b_{i_m} c_{i_m+1} \Bigg) \Bigg) \cdots \Bigg) \Bigg) \Bigg)
\end{aligned}
$$

Note that $c_d F_{m,1} = q_{d-2m-1}$ and $S_{m,1} = q_{d-2m}$ and $q_i = 0$ if $i < 0$. Hence, the matrix M_1 can

be expressed as

$$M_1 = \begin{matrix} M_{1,1} \\ M_{1,2} \\ M_{1,3} \\ M_{1,4} \\ \vdots \end{matrix} \begin{bmatrix} 1 & F_{1,1} & F_{2,1} & F_{3,1} & \cdots & F_{d-3,1} \\ 1 & S_{1,1} & S_{2,1} & S_{3,1} & \cdots & S_{d-3,1} \\ 0 & 1 & F_{1,1} & F_{2,1} & \cdots & F_{d-4,1} \\ 0 & 1 & S_{1,1} & S_{2,1} & \cdots & S_{d-4,1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix}_{(d-2)\times(d-2).}$$

Before we transform matrices related M_1 into triangular matrices by applying some row-operations over them, the following lemmas are given for computional purpose, which can be proved straightfoward.

Lemma 3.4 *1.* $S_{m,1} - F_{m,1} = (-c_{d-1}a_d)S_{m-1,2}$ *for* $1 \le m \le d-3$, *and*

2. $F_{m,1} - S_{m,2} = (-c_{d-2}b_{d-1})F_{m-1,2}$ *for* $1 \le m \le d-4$.

Lemma 3.5 *let* $2 \le j \le \lceil (d-3)/2 \rceil$,

1. $S_{m,j} - F_{m,j} = (-c_{d-2j+1}b_{d-2j+2})S_{m-1,j+1}$ *for* $1 \le m \le (d-2j-1)$, *and*

2. $F_{m,j} - S_{m,j+1} = (-c_{d-2j}b_{d-2j+1})F_{m-1,j+1}$ *for* $1 \le m \le (d-2j-2)$.

It is worth mentioning here that $c_{d-1}a_d$, $c_{d-2j+1}b_{d-2j+2}$, $c_{d-2j}b_{d-2j+1}$ are common factors of $S_{m,1} - F_{m,1}$, $S_{m,j} - F_{m,j}$, and $F_{m,j} - S_{m,j+1}$ respectively. Moreover the condition $a_d \neq 0$ plays a critical role in this argument, as shown in Lemma 3.4 and then next in Step 1.

The purpose of the following steps is to transform M_1 into an upper triangular matrix in terms of row operations. In particular, M_1 is already [1] if $d = 3$, and steps 1, 2 are enough to reduced M_1 into an upper triangular matrix in case $d = 4,5$.

Step 1. to get M_2 from M_1 with rows $M_{1,1}$, $M_{1,2}$, ..., $M_{1,d-2}$:

1. since $c_{d-1}a_d$ is a common factor for each entries of the row $-M_{1,1} + M_{1,2}$ by Lemma 3.4, replace

$$\begin{matrix} M_{1,1} \\ M_{1,2} \end{matrix} \begin{bmatrix} 1 & F_{1,1} & F_{2,1} & F_{3,1} & \ldots & F_{d-3,1} \\ 1 & S_{1,1} & S_{2,1} & S_{3,1} & \ldots & S_{d-3,1} \end{bmatrix}$$

by

$$\begin{matrix} M_{2,1} \\ M_{2,2} \end{matrix} \begin{bmatrix} 1 & F_{1,1} & F_{2,1} & F_{3,1} & \ldots & F_{d-3,1} \\ 0 & 1 & S_{1,2} & S_{2,2} & \ldots & S_{d-4,2} \end{bmatrix},$$

where $M_{2,1} = M_{1,1}$, and $M_{2,2} = (-1/c_{d-1}a_d)(-M_{1,1} + M_{1,2})$;

2. similar for pairs of rows $M_{1,2i-1}$ and $M_{1,2i}$, which are obtained from rows $M_{1,2i-3}$ and $M_{1,2i-2}$ by shifting right one entry for $i = 2, 3, \ldots, \lceil (d-3)/2 \rceil$;

3. if d is odd, then the final row $M_{1,d-2}$ remains unchanged, say $M_{2,d-2}$;

4. let M_2 be the resulting matrix with rows $M_{2,1}, M_{2,2}, \ldots, M_{2,d-2}$.

Step 2. to get M_3 from M_2 with rows $M_{2,1}, M_{2,2}, \ldots, M_{2,d-2}$:

1. let $M_{3,1} = M_{2,1}$ which remain unchanged;

2. starting from the second row of M_2, since $c_{d-2}b_{d-1}$ is a common factor of the row $-M_{2,2} + M_{2,3}$ by Lemma 3.4, replace

$$\begin{matrix} M_{2,2} \\ M_{2,3} \end{matrix} \begin{bmatrix} 0 & 1 & S_{1,2} & S_{2,2} & \ldots & S_{d-4,2} \\ 0 & 1 & F_{1,1} & F_{2,1} & \ldots & F_{d-4,1} \end{bmatrix}$$

by

$$\begin{matrix} M_{3,2} \\ M_{3,3} \end{matrix} \begin{bmatrix} 0 & 1 & S_{1,2} & S_{1,2} & \ldots & S_{d-4,2} \\ 0 & 0 & 1 & F_{1,2} & \ldots & F_{d-5,2} \end{bmatrix},$$

where $M_{3,2} = M_{2,2}$, and $M_{3,3} = (-1/c_{d-2}b_{d-1})(-M_{2,2} + M_{2,3})$;

3. similar for pairs of rows $M_{2,2i}$ and $M_{2,2i+1}$ where $i = 2, 3, \ldots, \lfloor (d-3)/2 \rfloor$;

4. if d is even, then the final row $M_{2,d-2}$ remains unchanged, say $M_{3,d-2}$;

5. let M_3 be the resulting matrix with rows $M_{3,1}, M_{3,2}, \ldots, M_{3,(d-2)}$.

The above two steps can be done in pairs recursively as follows for $\dot{2} \leq j \leq \lceil \frac{d-3}{2} \rceil$, but step $d-2$ is skipped in case d is even.

Step 2j-1. to get M_{2j} from M_{2j-1} with rows $M_{2j-1,1}, M_{2j-1,2}, \ldots, M_{2j-1,d-2}$:

1. let $M_{2j,i} = M_{2j-1,i}$, for $1 \leq i \leq 2j-2$ remain unchanged;

2. starting from the $(2j-1)$-th row, since $c_{d-2j+1}b_{d-2j+2}$ is a common factor for each entries of the row $-M_{2j-1,2j-1} + M_{2j-1,2j}$ by Lemma 3.5, replace

$$\begin{matrix} M_{2j-1,2j-1} \\ M_{2j-1,2j} \end{matrix} \begin{bmatrix} 0 & \ldots & 0 & 1 & F_{1,j} & F_{2,j} & F_{3,j} & \ldots & F_{d-2j-1,j} \\ 0 & \ldots & 0 & 1 & S_{1,j} & S_{2,j} & S_{3,j} & \ldots & S_{d-2j-1,j} \end{bmatrix}$$

by

$$\begin{matrix} M_{2j,2j-1} \\ M_{2j,2j} \end{matrix} \begin{bmatrix} 0 & \dots & 0 & 1 & F_{1,j} & F_{2,j} & F_{3,j} & \dots & F_{d-2j-1,j} \\ 0 & \dots & 0 & 0 & 1 & S_{1,j+1} & S_{2,j+1} & \dots & S_{d-2j-2,j+1} \end{bmatrix},$$

where

$$\begin{aligned} M_{2j,2j-1} &= M_{2j-1,2j-1} \text{ and} \\ M_{2j,2j} &= (-1/c_{d-2j+1}b_{d-2j+2})(-M_{2j-1,2j-1} + M_{2j-1,2j}). \end{aligned}$$

Note that the first $2j-2$ columns consists of entries 0 only;

3. similar for pairs of rows $M_{2j-1,2i-1}$, and $M_{2j-1,2i}$ for $j+1 \le i \le \lceil (d-3)/2 \rceil$;

4. if d is odd then the final row $M_{2j-1,d-2}$ remains unchanged, say $M_{2j,d-2}$;

5. let M_{2j} be the resulting matrix with rows $M_{2j,1}$, $M_{2j,2}$, ..., $M_{2j,d-2}$.

Step 2j. to get M_{2j+1} from M_{2j} with rows $M_{2j,1}$, $M_{2j,2}$, ..., $M_{2j,d-2}$:

1. let $M_{2j+1,i} = M_{2j,i}$ for $1 \le i \le 2j-1$ remain unchanged;

2. starting from the $2j$-th row, since $c_{d-2j}b_{d-2j+1}$ is a common factor for each entries of the row $-M_{2j,2j} + M_{2j,2j+1}$ by Lemma 3.5, replace

$$\begin{matrix} M_{2j,2j} \\ M_{2j,2j+1} \end{matrix} \begin{bmatrix} 0 & \dots & 0 & 1 & S_{1,j+1} & S_{2,j+1} & S_{3,j+1} & \dots & S_{d-2j-2,j+1} \\ 0 & \dots & 0 & 1 & F_{1,j} & F_{2,j} & F_{3,j} & \dots & F_{d-2j-2,j} \end{bmatrix}$$

by

$$\begin{matrix} M_{2j+1,2j} \\ M_{2j+1,2j+1} \end{matrix} \begin{bmatrix} 0 & \dots & 0 & 1 & S_{1,j+1} & S_{2,j+1} & S_{3,j+1} & \dots & S_{d-2j-2,j+1} \\ 0 & \dots & 0 & 0 & 1 & F_{1,j+1} & F_{2,j+1} & \dots & F_{d-2j-3,j+1} \end{bmatrix}$$

where

$$\begin{aligned} M_{2j+1,2j} &= M_{2j,2j} \text{ and} \\ M_{2j+1,2j+1} &= (-1/c_{d-2j}b_{d-2j+1})(-M_{2j,2j} + M_{2j,2j+1}) \end{aligned}$$

Note that the first $2j-1$ columns consist of entries 0 only;

3. similar for pairs of rows $M_{2j,2i}$, and $M_{2j,2i+1}$ for $j \le i \le \lfloor (d-3)/2 \rfloor$;

4. if d is even, then the final row $M_{2j,d-2}$ remains unchanged, say $M_{2j+1,d-2}$;

5. let M_{2j+1} be the resulting matrix with rows $M_{2j+1,1}$, $M_{2j+1,2}$, ..., $M_{2j+1,d-2}$.

After steps 1, 2, $\cdots$, $d-3$, an upper triangular matrix with 1 along its main diagonal is obtained, hence $\det M_1$, $\det \mathbf{E}_{d,0}$, and hence $\det \mathbf{E}_{d,i}$ are all non-zero. This completes the proof of Lemma 3.1 and hence the main theorem.

Remark: The above argument does not work for bipartite distance-regular graphs of diameter $d \geq 4$. Since $a_d = 0$, $S_{m,1} = F_{m,1}$ for all $m \leq d-3$ by Lemma 3.4, it follows that M_1, and hence $\mathbf{E_{d,0}}$, $\mathbf{E_{d,i}}$ for all $i \leq d-3$ are singular.

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I: Association Schemes*, Lecture Note Series 58, Benjamin-Cummmings, Menlo Park, California, 1984.

[2] N. Biggs, Some Odd Graph Theory, *Proc. Second Internat. Conf. on Comb.Math. Annals of the New York Academy of Science,* vol. 319(1979), pp. 71-81.

[3] N. Biggs, *Algebraic Graph Theory*, 2nd edition, Cambridge Univ. Press, Cambridge, 1993.

[4] R. C. Bose and B. Laskar, Eigenvalues of the Adjacency Matrix of Cubic Lattice Graphs, *Pacific J. of Math.* vol. 29, No. 3, pp. 623–629, 1969.

[5] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance Regular Graphs.* Springer-verlag, Berlin, 1989.

[6] A. E. Brouwer and W. H. Haemers, The Gewirtz Graph: An Exercise in the Theory of Graph Spectra, *Europ. J. Combinatorics* (1993)14, 397-407.

[7] D. Cvetkovic, M. Doob, I. Gutman, A. Torgasev, *Recent results in the theory of graphs spectra*, Annals of Discrete Mathematics 36, North-Holland, 1988.

[8] E. R. van Dam and W. H. Haemers, *A Characterization of Distance-Regular Graphs with Diameter three*, preprint.

[9] A. Gewirtz, Graphs with maximal even girth, *Canad. J. Math.* 21 (1969), pp. 915-934.

[10] W. H. Haemer, Distance-Regularity and the Spectrum of Graphs, *Linear Alg. Appl* (to appear).

[11] W. H. Haemers and E. Spence, Graphs Cospectral with Distance-Regular Graphs, *Linear and Multilinear Algebra* (to appear).

[12] A. J. Hoffman, On the polynomial of a graph, *Amer. Math. Monthly* 70 (1963) pp. 30–36.

[13] T. Huang, Spectral Characterization of Odd graphs O_k, $k \leq 6$, *Graphs and Combinatorics* (1994) 10, pp. 235–240.

[14] A. Moon, Characterization of the Odd Graphs O_k by Parameters, *Discrete Mathematics* 42 (1982), pp. 91–97.

[15] A. J. Schwenk and B. J. Wilson, *Selected Topics in Graph Theory*, L. W. Beineke and R. J. Wilson(eds), Academic P., (1981), pp. 307–336.

[16] W. T. Tutte, All the king horses, *Graph Theory and Related topics* (J.A. Bondy, U.S.A. Murty, eds.), Academic Press, 1979, pp. 15-33.

On distance-regular graphs which are locally strongly regular

J.H. Koolen*
FSP Mathematisierung,
University of Bielefeld,
P.O. Box 10 01 31,
33501, Bielefeld,
Germany.

January 8, 1996

Abstract

In this note we will give an inequality for distance-regular graphs. If equality occurs in this inequality then the distance-regular graph is locally strongly regular. We investigate the situation in which equality occur. This is joint work with A. Jurišić and P. Terwilliger.

1 Introduction

In this note we will give an inequality for distance-regular graphs. If equality occurs in this inequality then the distance-regular graph is locally strongly regular. We investigate the situation in which equality occur. This is joint work with A. Jurišić and P. Terwilliger.

Let Γ be a graph. Define $\Gamma_i(x) = \{y \in V\Gamma \mid d(x,y) = i\}$ for a vertex x of Γ. We write $\Gamma(x)$ for $\Gamma_1(x)$. A connected graph Γ is *distance-regular* if there are constants a_i, b_i, c_i, $i = 1, \ldots,$ diam(Γ) such that for vertices x, y we have $|\Gamma_{i+1}(y) \cup \Gamma(x)| = b_i$, $|\Gamma_i(y) \cup \Gamma(x)| = a_i$, and $|\Gamma_{i-1}(y) \cup \Gamma(x)| = c_i$ if $d(x,y) = i$. In particular a distance-regular graph Γ is regular with valency b_0.

*This note was written while the author was supported by a fellowship from the European Union's "Algebraic Combinatorics" project.

The *adjacency matrix* of a graph Γ is a $(0,1)$-matrix A where the columns and rows are indexed by the vertices of Γ such $A_{x,y} = 1$ if and only if x and y are adjacent, i.e. $d(x,y) = 1$. By the eigenvalues of a graph Γ we mean the eigenvalues of its adjacency matrix.

In the next section we give the inequation and gives some examples when equality holds.

2 An inequality

Let Γ be a distance-regular graph. Then define for $\theta \in \mathbf{R} \setminus \{-1\}$ the number $b(\theta) := -1 - \frac{b_1}{1+\theta}$. Define for a vertex x the graph $\Delta(x)$ as the subgraph of Γ induced on $\Gamma(x)$. Terwilliger showed the following proposition using standard representations.

Proposition 1 (cf. [4, Proposition 7.10]) *Let Γ be a distance-regular graph with eigenvalues $k = \theta_0 > \theta_1 > \cdots > \theta_d$. Let x be a vertex of Γ and let $\eta_1 \geq \eta_2 \geq \cdots \geq \eta_k$ be the eigenvalues of $\Delta(x)$. Then $b(\theta_d) \geq \eta_i \geq b(\theta_1)$ for $i \neq 1$.*

We need the following proposition be fore we can show the inequality.

Proposition 2 *Let $a, b, \alpha_1, \ldots, \alpha_n$ be reals with $a \leq \alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_n \leq b$ and $a \neq b$. Let*

$$s = \sum_{i=1}^{n} \alpha_i.$$

Let $\gamma = \frac{bn-s}{b-a}$ and $\delta = \frac{an-s}{a-b}$. Then

$$\sum_{i=1}^{n} \alpha_i^2 \leq \gamma a^2 + \delta b^2,$$

and equality holds if and only if γ and δ are integers and $\alpha_\gamma = a$ and $\alpha_{\gamma+1} = b$.

Using Propositions 1 and 2 it is not difficult to show the following proposition.

Proposition 3 *Let Γ be a distance-regular graph with eigenvalues $k = \theta_0 > \theta_1 > \cdots > \theta_d$ and let x be a vertex of Γ. Then*

$$k \leq \frac{b_1 \theta_1 \theta_d}{b_1 + (1+\theta_1)(1+\theta_d)} \tag{1}$$

and equality holds if and only if $\Delta(x)$ is a graph with eigenvalues $\lambda, b(\theta_1), b(\theta_d)$ or Γ is bipartite.

Proof. Let $\eta_1 \geq \eta_2 \geq \ldots \geq \eta_k$ be the eigenvalues of $\Delta(x)$. Then

$$\sum_{i=1}^{k} \eta_i = 0 \text{ and } \sum_{i=1}^{k} \eta_i^2 = ka_1.$$

Now this proposition follows directly from Propositions 1 and 2. □

Examples of distance-regular graphs where equality holds in the previous proposition are the Johnson graphs $J(2n,n)$, the halved $2n$-cubes, the Taylor graphs, i.e. distance-regular graphs with $k_3 = 1$, and the Patterson graph, associated to the Suzuki group, with intersection diagram $\{280,243,144,10;1,8,90,280\}$, cf. [1, Section 13.7].

For diameter three we have the following theorem.

Theorem 4 *Let Γ be a non-bipartite distance-regualar graph with diameter 3 and equality in (1). Then Γ is a Taylor graph.*

We have the following conjecture.

Conjecture 5 *Let Γ be a non-bipartite distance-regular graph of diameter at least 5 and with equality in 1. Then Γ is a Johnson graph $J(2n,n)$ or a halved $2n$-cube.*

Remark. Let Δ be a strongly regular graph with intersection array $\{(q(pq+p+q),(p+1)(q-1)(q+1);1,q(p+q)\}$. An antipodal distance-regular r-cover of Δ has equality in (1). There are four such covers known. One of them is antipodal 3-cover of the Kneser graph $K(7,2)$, the complement of the Johnson graph $J(7,2)$. This graph is locally the Petersen graph. They are all 3-covers. It is not known if that such a cover must be a 3-cover. The 2-covers are P- and Q-polynomial. More information about this family is in the theses by Jurišić [3, Section 4.5] and Dickie [2, Chapter 2].

References

[1] A.E. Brouwer, A.M. Cohen and A. Neumaier, *Distance-regular graphs*, Ergebnisse der Mathematik 3.18, Springer, Heidelberg (1989).

[2] Garth A. Dickie, *Q-Polynomial structures for association schemes and distance-regular graphs*, Ph.D. thesis, University of Wisconsin, Madison (1995)

[3] Aleksander Jurišić, *Antipodal covers*, Ph.D. thesis, University of Waterloo, Waterloo (1995)

[4] J.H. Koolen, *Euclidean representations and substructures of distance-regular graphs*, Ph.D. thesis, Eindhoven University of Technology, Eindhoven (1994)

SPIN MODELS AND ALMOST BIPARTITE 2-HOMOGENEOUS GRAPHS

Kazumasa Nomura
Tokyo Ikashika University

1 Introduction

A spin model is one of the statistical mechanical models which were introduced by Vaughan Jones to construct invariants of knots and links [12]. A spin model is defined as a complex-valued symmetric function w on $X \times X$, where X is a finite set of "spins", satisfying several axioms. Each spin model S gives a corresponding link invariant through its partition function. Three examples of spin models are mentioned in Jones' paper [12]; Potts models, cyclic models and square models. It must be remarked that the Jones polynomial can be obtained from the partition function of the Potts models.

A connection between spin models and distance-regular graphs was found by Francois Jaeger [9] by constructing a new spin model on the Higman-Sims graph, a distance-regular graph of diameter $d = 2$ with $n = 100$ vertices, which was discovered by D. Higman and C. Sims [8], where we say that a spin model $S = (X, w)$ is constructed on a connected graph $\Gamma = (X, E)$ if $w(x, y)$ depends only on the distance $\partial(x, y)$ in the graph Γ. Jaeger [9] proved that the corresponding link invariant of the Higman-Sims model becomes a specialization of the Kauffman polynomial [14]. After Jaeger's discovery, a new infinite family of spin models were constructed on Hadamard graphs by the author [14]. The corresponding link invariants of the Hadamard models were determined

by Jaeger [10,11], and then Jones [13] gave a pair of two links which can be detected by this invariant but not by Jones polynomial.

These examples of spin models can be constructed on almost bipartite distance-regular graphs. Moreover these graphs have extra regularity which we call 2-homogeneity; an almost bipartite distance-regular graph $\Gamma = (X, E)$ is 2-homogeneous if and only if $|\Gamma_{i-1}(u) \cap \Gamma_1(x) \cap \Gamma_1(y)|$ is a constant for all u, x, $y \in X$ with $\partial(u,x) = \partial(u,y) = i$, $\partial(x,y) = 2$ ($i = 1, \ldots d$, where d denotes the diameter of Γ). In fact it was shown [21] that if a triangle-free connected graph affords a spin model with certain weights then the graph must be distance-regular and almost bipartite.

This paper contains two main results (Theorem 4.3 and Theorem 5.1) without proof. A complete version will be appear in Advanced Study in Pure Mathematics with the same title.

In Section 2, some preliminaries on spin models and distance-regular graphs are given. In Section 3, two necessary and sufficient conditions (H1), (H2) for 2-homogeneity of almost bipartite distance-regular graphs are given. Then we slightly generalize of Yamazaki's sufficient condition for 2-homogeneity [22]. In Section 4 and Section5, our main results are given.

There are two generalizations of Jones' spin models by Kawagoe-Munemasa-Watatani [15] and Bannai-Bannai [1] (see also [2, 3, 16]). In this paper we restrict our interest to the original spin models defined in [12].

2 Spin Models and Distance-Regular Graphs

2.1 Definition and examples of spin models

A *spin model* is a pair $S = (X, w)$ of a finite set of size $|X| = n > 0$ and a complex-valued function w on $X \times X$ such that (for all a, b, c in X)

(S1) $w(a,b) = w(b,a) \neq 0$,

(S2) $\Sigma_{x \in X}\, w(a,x)w(b,x)^{-1} = n\delta_{a,b}$,

(S3) $\Sigma_{x \in X}\, w(a,x)w(b,x)w(c,x)^{-1} = \sqrt{n}\, w(a,b)w(a,c)^{-1}w(b,c)^{-1}$.

The equation (S3) is called the "star-triangle" relation. The elements of X is called the *spins*, and the function w is called the *(Boltzmann) weight*. Putting $a = c$ in (S3), we have

$$\sum_{x \in X} w(b,x) = \sqrt{n}\, w(a,a)^{-1},$$

so that $w(a,a) = \alpha$ is a constant, called the *modulus* of S, which is independent of the choice of a in X.

The *weight matrix* of a spin model $S = (X, w)$, $|X| = n$, is a $n \times n$ matrix W, indexed by $X \times X$, whose (x,y)-entry is $W_{x,y} = w(x,y)$. For b, c in X, we consider a vector $\mathbf{u}_{bc}$ in the n-space $V = \mathbf{C}^n$, where the entries of the vectors are indexed by X, whose x-entry is given by

$$(\mathbf{u}_{bc})_x = \frac{w(b,x)}{w(c,x)}, \qquad (x \in X).$$

Then the condition (S3) can be written as

$$W\mathbf{u}_{bc} = \sqrt{n}\, w(b,c)^{-1}\mathbf{u}_{bc}.$$

This means the vector $\mathbf{u}_{bc}$ is an eigenvector of W for the eigenvalue $\sqrt{n}\, w(b,c)^{-1}$. It can be easily shown from (S2) that, for a fixed $b \in X$,

the vectors $\mathbf{u}_{bc}$, $c \in X$ are linearly independent and hence form a basis of V. Therefore the values $\sqrt{n}\, w(b,c)^{-1}$, $c \in X$ give all the eigenvalues of W, where multiplicities are counted. This means that the multiplicity of an eigenvalue $\sqrt{n}\,\lambda^{-1}$ agrees with the number of $x \in X$ such that $w(b,x) = \lambda$ (thus this number does not depend on the choice of b). The vector $\mathbf{u}_{bb}$ becomes the all one vector $\mathbf{j}$, and it is an eigenvector of W corresponding the eigenvalue $\sqrt{n}\,\alpha^{-1}$ (α is the modulus). From condition (S2), the other vectors $\mathbf{u}_{bc}$, $b \neq c$ are orthogonal to $\mathbf{j}$.

Now we give three basic examples of spin models.

Potts model. Let X be a finite set with $n > 1$ elements. Let β be a solution of $\beta^2 + \beta^{-2} + \sqrt{n} = 0$ and put $\alpha = -\beta^{-3}$. Define a function w on $X \times X$ by

$$w(x,y) = \begin{matrix} \alpha & x = y, \\ \beta & \text{otherwise.} \end{matrix}$$

Then (X, w) is a spin model called the *Potts model* [12]. Potts model with $n = 2$ is also called the *Ising model*.

Cyclic model. Let $X = \{0, 1, \ldots, n-1\}$, and let θ be a primitive n-root of unity when n is odd, or a primitive $2n$-root of unity when n is even. Define a function w on $X \times X$ by

$$w(x,y) = \alpha\theta^{(x-y)^2},$$

where

$$\alpha^2 = \frac{\sqrt{n}}{\sum_{i=0}^{n-1} \theta^{i^2}}.$$

Then (X, w) becomes a spin model, called the *cyclic model* [2,6,12].

Square model. Let $X = \{1, 2, 3, 4\}$ and let α be an arbitrary non-zero complex number. Let us consider the following matrix:

$$\begin{pmatrix} \alpha & \alpha^{-1} & -\alpha & \alpha^{-1} \\ \alpha^{-1} & \alpha & \alpha^{-1} & -\alpha \\ -\alpha & \alpha^{-1} & \alpha & \alpha^{-1} \\ \alpha^{-1} & -\alpha & \alpha^{-1} & \alpha \end{pmatrix}$$

and define a function w on $X \times X$ by $w(x, y) = W_{x,y}$. Then (X, w) becomes a spin model, called the *square model* [7,12].

2.2 Preliminaries for distance-regular graphs

Let $\Gamma = (X, E)$ be a connected (undirected simple) graph of diameter d with the vertex set X and the edge set E with the usual metric ∂ on X. For vertices u, v and for integers r, s, define

$$\Gamma_r(u) = \{x \in X \mid \partial(u, x) = r\},$$

$$\mathrm{D}_s^r(u, v) = \Gamma_r(u) \cap \Gamma_s(v).$$

Γ is said to be *distance-regular* if there are integers b_r, c_r such that for any two vertices u, x at distance $r = \partial(u, x)$, there are precisely c_r neighbours of x in $\Gamma_{r-1}(u)$ and b_r neighbours of x in $\Gamma_{r+1}(u)$. In particular Γ is regular of valency $k = b_0$, and there are $a_r = k - c_r - b_r$ neighbours of x in $\Gamma_r(u)$. The parameters c_r, b_r, a_r $(r = 0, \ldots, d)$ satisfy (see [5] Proposition 4.1.6)

$$1 = c_1 \leq c_2 \leq \cdots \leq c_{d-1} \leq c_d,$$

$$k = b_0 \geq b_1 \geq \cdots \geq b_{d-1} \geq b_d = 0.$$

The array

$$\begin{Bmatrix} 0 & c_1 & c_2 & \cdots & c_{d-1} & c_d \\ 0 & a_1 & a_2 & \cdots & a_{d-1} & a_d \\ k & b_1 & b_2 & \cdots & b_{d-1} & 0 \end{Bmatrix}$$

is called the *intersection array* of Γ.

It is known (see [5] Section 4.1) that the parameters

$$p^t_{r,s} = |\mathrm{D}^r_s(u,v)|, \qquad (t = \partial(u,v))$$

are well-defined, i.e. these parameters depends only on r, s and $t = \partial(u,v)$, rather than on the individual vertices u, v with $t = \partial(u,v)$. The parameters $p^t_{r,s}$ are called the *intersection numbers* of Γ. Clearly $c_r = p^r_{r-1,1}$, $a_r = p^r_{r,1}$ and $b_r = p^r_{r+1,1}$ hold.

Let A_i $(i = 0, 1, \ldots, d)$ denote the i-th adjacency matrix of Γ, i.e. A_i is the $n \times n$ matrix, indexed by $X \times X$, whose (x,y)-entry is

$$(A_i)_{x,y} = \begin{cases} 1 & \partial(x,y) = i, \\ 0 & \text{otherwise.} \end{cases}$$

In particular, $A_0 = I$ the identity matrix of size n and $A_1 = A$ the usual adjacency matrix of Γ. The matrices A_0, A_1, ..., A_d satisfy

$$A_i A_j = A_j A_i = \sum_{\ell=0}^{d} p^\ell_{ij} A_\ell.$$

In particular,

$$AA_i = b_{i-1}A_{i-1} + a_i A_i + c_{i+1}A_{i+1}$$

holds. Using this relation recursively, A_i can be written as a polynomial in A, i.e. there are polynomials $v_i(x)$ of degree i such that $A_i = v_i(A)$ holds for $i = 0, 1, \ldots, d$.

It is known that the adjacency matrix A has distinct eigenvalues $\theta_0 = k$, θ_1, ..., θ_d, and the corresponding eigenspaces V_0, V_1, ..., V_d in $V = \mathbf{C}^n$ $(n = |X|)$ are mutually orthogonal (see [5] Section 4.1):

$$V = V_0 \oplus V_1 \oplus \cdots \oplus V_d \quad \text{(orthogonal sum)}.$$

Remark that V_0 is the 1-dimensional subspace spanned by $\mathbf{j}$.

More precise descriptions about distance-regular graphs can be found in [4,5].

2.3 Spin models on distance-regular graphs

Let $\Gamma = (X, E)$ be a connected graph of diameter d with the usual metric ∂ on X. Let R_i $(i = 0, 1, \ldots, d)$ be the set of pairs (x, y) in $X \times X$ such that $\partial(x, y) = i$. Then $X \times X$ is partitioned into $d + 1$ relations:

$$X \times X = R_0 \cup R_1 \cup \cdots \cup R_d.$$

We consider spin models $S = (X, w)$ such that w takes a constant value t_i on R_i $(i = 0, 1, \ldots, d)$, i.e. $w(x, y) = t_i$ holds for all x, y in X at distance $\partial(x, y) = i$. In this case we say that the spin model $S = (X, w)$ is constructed on the graph $\Gamma = (X, E)$. We are particularly interested in spin models which are constructed on distance-regular graphs.

For three vertices x, y, z and for integers i, j, ℓ, define

$$P_{i,j,\ell}(x, y, z) = |\Gamma_i(x) \cap \Gamma_j(y) \cap \Gamma_\ell(z)|.$$

Lemma 2.1 *Let $\Gamma = (X, E)$ be a distance-regular graph of diameter d with the intersection numbers $p^\ell_{i,j}$, and let $t_0, \ldots, t_d$ be non-zero complex numbers. Define a function w on $X \times X$ by $w(x, y) = t_{\partial(x,y)}$. Then $S = (X, w)$ is a spin model if and only if the following conditions hold:*

(S2') For $\ell = 1, \ldots, d$,

$$\sum_{i=0}^{d} \sum_{j=0}^{d} p^\ell_{i,j} t_i t_j^{-1} = 0,$$

(S3') For all x, y, z in X,

$$\sum_{i=0}^{d} \sum_{j=0}^{d} \sum_{\ell=0}^{d} P_{i,j,\ell}(x, y, z) t_i t_j t_\ell^{-1} = \sqrt{n}\, t_{\partial(x,y)} t_{\partial(x,z)}^{-1} t_{\partial(y,z)}^{-1}.$$

Now we give two examples which are constructed on distance-regular graphs.

Jaeger's Higman-Sims model. The Higman-Sims graph, which was discovered by D. Higman and C. Sims [8], is the unique distance-regular graph $\Gamma = (X, E)$ of diameter $d = 2$ with the following intersection array:

$$\begin{Bmatrix} 0 & 1 & 6 \\ 0 & 0 & 16 \\ 22 & 21 & 0 \end{Bmatrix}.$$

Γ has $|X| = 100$ vertices.

A spin model was constructed on the Higman-Sims graph by F. Jaeger [9] (see also [7]). Let $\tau = (1+\sqrt{5})/2$ and put

$$t_0 = (5\tau + 3)\sqrt{-1}, \quad t_1 = \tau\sqrt{-1}, \quad t_2 = (-\tau + 1)\sqrt{-1}.$$

Define a function w on $X \times X$ by $w(x, y) = t_{\partial(x,y)}$ for x, $y \in X$. Then $S = (X, w)$ becomes a spin model. The corresponding link invariant becomes a specialization of the Kauffman polynomial [7].

Hadamard model. Hadamard graphs are distance-regular graphs of diameter $d = 4$ with the following intersection array:

$$\begin{Bmatrix} 0 & 1 & 2m & 4m-1 & 4m \\ 0 & 0 & 0 & 0 & 0 \\ 4m & 4m-1 & 2m & 1 & 0 \end{Bmatrix},$$

where m is a positive integer. There is a natural correspondence between Hadamard graphs of valency $4m$ and Hadamard matrices of size $4m$ (see [5] Theorem 1.8.1). Let s, t_0, t_1 be complex numbers such that

$$s^2 + 2(2m-1)s + 1 = 0, \quad t_0^2 = \frac{2\sqrt{m}}{(4m-1)s+1}, \quad t_1^4 = 1,$$

and put

$$t_2 = st_0, \quad t_3 = -t_1, \quad t_4 = t_1.$$

Define a function w on $X \times X$ by $w(x, y) = t_{\partial(x,y)}$ for x, $y \in X$. Then $S = (X, w)$ is a spin model [17]. The corresponding link invariants of these models were determined by Jaeger [10,11].

3 2-homogeneous Distance-Regular Graphs

3.1 Definition of 2-homogeneity

Let $\Gamma = (X, E)$ be a distance-regular graph of diameter d. For a vertex x in X and for a subset A of X, let $e(x, A)$ denote the number of edges from x into A; $e(x, A) = |\Gamma_1(x) \cap A|$. Γ is said to be *t-homogeneous* (where t is an non-negative integer) if the following condition holds for all integers r, s, i, j and for all vertices u, v, u', v' with $\partial(u, v) = \partial(u', v') = t$:

$$x \in \mathrm{D}_s^r(u, v),\ x' \in \mathrm{D}_s^r(u', v') \Longrightarrow e(x,\ \mathrm{D}_j^i(u, v)) = e(x', \mathrm{D}_j^i(u', v')).$$

This means that, for two vertices u, v at distance t and for x in $\mathrm{D}_s^r(u, v)$, the number of edges from x into $\mathrm{D}_j^i(u, v)$ depends only on r, s, i, j rather than on the individual vertices u, v, x with $\partial(u, v) = t$ and $x \in \mathrm{D}_s^r(u, v)$.

It was shown [18] that, for a distance-regular graph Γ of diameter d in which $\mathrm{D}_1^1(u, v)$ is a (non-empty) clique for every edge uv, Γ is 1-homogeneous if and only if Γ is isomorphic to a regular near $2d$-gon (see [5] Section 6.4 for the definition).

Now we restrict our interest to the case $t = 2$. Let us consider the following conditions for a distance-regular graph Γ of diameter d:

(H1) There are integers $\delta_2, \ldots, \delta_d$ such that, for every pair of vertices u, v at distance $\partial(u, v) = 2$, and for every x in $\Gamma_r(u) \cap \Gamma_r(v)$, there are precisely δ_r neighbours of x in $\Gamma_{r-1}(u) \cap \Gamma_{r-1}(v)$ $(r = 2, \ldots, d)$.

(H2) There are integers $\gamma_1, \ldots, \gamma_d$ such that, for every vertex x and for every u, v in $\Gamma_r(x)$ with $\partial(u, v) = 2$, there are precisely γ_r common neighbours of u and v in $\Gamma_{r-1}(x)$ $(r = 1, \ldots, d)$.

Lemma 3.1 *Let $\Gamma = (X, E)$ be a distance-regular graph of diameter d. Then (H1) is equivalent to (H2).*

A connected graph Γ is said to be *bipartite* if there is no cycle of odd length, and *almost bipartite* if there is no cycle of odd length ℓ with $\ell < 2d+1$ (where d is the diameter of Γ). Let Γ be a distance-regular graph of diameter d with intersection numbers c_r, a_r, b_r $(r = 0, \ldots, d)$. Clearly Γ is bipartite if and only if $a_r = 0$ for $r = 0, \ldots, d$, and Γ is almost bipartite if and only if $a_r = 0$ for $r = 0, \ldots, d-1$.

Lemma 3.2 *Let Γ be an almost bipartite distance-regular graph of diameter d. Then Γ is 2-homogeneous if and only if Γ satisfies (H1).*

3.2 A sufficient condition for 2-homogeneity

Yamazaki [22] proved that every bipartite distance-regular graph with an eigenvalue of multiplicity k (k is the valency) satisfies condition (H1). Here we give a slight generalization.

Proposition 3.3 *Let Γ be an almost bipartite distance-regular graph of valency k. If the adjacency matrix A of Γ has an eigenvalue θ of multiplicity f with $1 < f \leq k$, then Γ is 2-homogeneous.*

4 Graphs with spin model structure

4.1 An observation

Here we observe that the examples of spin models given in Section 2 can be constructed on distance-regular graphs. Jaeger's Higman-Sims model and the Hadamard models are constructed on distance-regular

graphs with the intersection arrays:

$$\begin{Bmatrix} 0 & 1 & 6 \\ 0 & 0 & 16 \\ 22 & 21 & 0 \end{Bmatrix},$$

and

$$\begin{Bmatrix} 0 & 1 & 2m & 4m-1 & 4m \\ 0 & 0 & 0 & 0 & 0 \\ 4m & 4m-1 & 2m & 1 & 0 \end{Bmatrix}.$$

The Potts models with n spins is constructed on a complete graph K_n, which is a distance-regular graph of diameter $d = 1$ with the intersection array

$$\begin{Bmatrix} 0 & 1 \\ 0 & k-1 \\ k & 0 \end{Bmatrix}, \qquad k = n-1.$$

The weights are given by $t_0 = \alpha$, $t_1 = \beta$, where $\beta^2 + \beta^{-2} + \sqrt{n} = 0$ and $\alpha = -\beta^{-3}$

The cyclic model with n spins is constructed on the n-cycle C_n which is a distance-regular graph of diameter d with the intersection array:

$$\begin{Bmatrix} 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 2 & 1 & 1 & \cdots & 1 & 0 \end{Bmatrix} \quad \text{when } n = 2d+1,$$

or

$$\begin{Bmatrix} 0 & 1 & 1 & \cdots & 1 & 2 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 2 & 1 & 1 & \cdots & 1 & 0 \end{Bmatrix} \quad \text{when } n = 2d.$$

The weights are given by $t_i = \alpha\theta^{i^2}$ $(i = 0, \ldots, d)$, where θ is a primitive n-root of unity if $n = 2d+1$, a primitive $2n$-root of unity if $n = 2d$, and $\alpha = \sqrt{n}/(\sum_{i=0}^{n-1} \theta^{i^2})$.

The square model is constructed on the 4-cycle C_4 with $t_0 = \alpha$, $t_1 = \alpha^{-1}$, $t_2 = -\alpha$, where α is a non-zero complex number.

Observe that all the above distance-regular graphs are almost bipartite. Moreover, as easily observed, each successive three terms t_{i-1}, t_i, t_{i+1} are distinct $(0 < i < d)$ in each of the above spin models except the square model with $\alpha = \pm 1$.

Motivated by the above observation, the author obtained the following result [21].

Theorem 4.1 *Let $\Gamma = (X, E)$ be a connected graph of diameter d which has no 3-cycle. Let $t_0, \ldots, t_d$ be non-zero complex numbers such that $t_1 \neq t_i$ and $t_{i-2} \neq t_i \neq t_{i-1}$ for $i = 2, \ldots, d$. Define a function w on $X \times X$ by $w(x, y) = t_{\partial(x,y)}$ for $x, y \in X$. If $S = (X, w)$ is a spin model, then Γ is an almost bipartite distance-regular graph.*

proclaim

This was obtained by "localizing" the star-triangle relation (S3). This technique of localization was introduced in [19].

4.2 2-homogeneity

Lemma 4.2 *Let $\Gamma = (X, E)$ be a distance-regular graph of diameter $d > 1$ and valency k, and let $t_0, \ldots, t_d$ be non-zero complex numbers such that $t_i \neq t_1$ for $i = 2, \ldots, d$. Assume $S = (X, w)$ is a spin model, where w is a function on $X \times X$ defined by $w(x, y) = t_{\partial(x,y)}$ for $x, y \in X$. Then the adjacency matrix A of Γ has an eigenvalue θ of multiplicity f with $1 < f \leq k$.*

Lemma 4.2 and Proposition 3.3 imply:

Theorem 4.3 *Let $\Gamma = (X, E)$ be an almost bipartite distance-regular graph of diameter d, and let $t_0, t_1, \ldots, t_d$ be non-zero complex numbers*

such that $t_1 \neq t_i$ *for* $i = 2, \ldots, d$. *If* $S = (X, w)$ *is a spin model with the weight* w *defined by* $w(x, y) = t_{\partial(x,y)}$, $x, y \in X$, *then* Γ *is 2-homogeneous.*

Theorem 4.1 and Theorem 4.3 imply:

Corollary 4. 4 *Let* $\Gamma = (X, E)$ *be a triangle-free connected graph of diameter* d, *and let* $t_0, \ldots, t_d$ *be non-zero complex numbers such that* $t_1 \neq t_i$ *and* $t_{i-2} \neq t_i \neq t_{i-1}$ *for* $i = 2, \ldots, d$. *If* $S = (X, w)$ *is a spin model with the weight* w *defined by* $w(x, y) = t_{\partial(x,y)}$, $x, y \in X$, *then* Γ *is an almost bipartite 2-homogeneous distance-regular graph.*

Remark. The assumption 'triangle-free' in Corollary 4.4 is essential. Actually there exists a distance-regular graph Γ (with triangles) such that Γ affords a spin model structure with weights $t_0, \ldots, t_d$ satisfying the same conditions but Γ is not 2-homogeneous. Also remark that every connected graph can have a spin model structure with the weights $t_1 = \cdots = t_d$ (Potts model), and so we need some conditions on the weights $t_0, \ldots, t_d$ in Corollary 4.4.

5 Classification of almost bipartite 2-homogeneous graphs

Theorem 5. 1 *Let* Γ *be an almost bipartite 2-homogeneous distance-regular graph of diameter* $d > 0$ *and valency* k. *Then* Γ *has one of the following intersection arrays:*

(1) $\left\{ \begin{array}{ccc} 0 & 1 \\ 0 & k-1 \\ k & 0 \end{array} \right\}$, $k > 0$,

(2) $\left\{ \begin{array}{ccc} 0 & 1 & k \\ 0 & 0 & 0 \\ k & k-1 & 0 \end{array} \right\}$, $k > 1$,

$$(3)\quad \left\{\begin{matrix} 0 & 1 & c \\ 0 & 0 & k-c \\ k & k-1 & 0 \end{matrix}\right\},\quad \begin{matrix} k=\gamma(\gamma^2+3\gamma+1), \\ c=\gamma(\gamma+1),\ \gamma>0, \end{matrix}$$

$$(4)\quad \left\{\begin{matrix} 0 & 1 & k-1 & k \\ 0 & 0 & 0 & 0 \\ k & k-1 & 1 & 0 \end{matrix}\right\},\quad k>1,$$

$$(5)\quad \left\{\begin{matrix} 0 & 1 & 2\gamma & 4\gamma-1 & 4\gamma \\ 0 & 0 & 0 & 0 & 0 \\ 4\gamma & 4\gamma-1 & 2\gamma & 1 & 0 \end{matrix}\right\},\quad \gamma>0,$$

$$(6)\quad \left\{\begin{matrix} 0 & 1 & c & k-c & k-1 & k \\ 0 & 0 & 0 & 0 & 0 & 0 \\ k & k-1 & k-c & c & 1 & 0 \end{matrix}\right\},\quad \begin{matrix} k=\gamma(\gamma^2+3\gamma+1), \\ c=\gamma(\gamma+1),\ \gamma>0, \end{matrix}$$

$$(7)\quad \left\{\begin{matrix} 0 & 1 & \cdots & 1 & 2 \\ 0 & 0 & \cdots & 0 & 0 \\ 2 & 1 & \cdots & 1 & 0 \end{matrix}\right\},\quad d>1,$$

$$(8)\quad \left\{\begin{matrix} 0 & 1 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 \\ 2 & 1 & \cdots & 1 & 0 \end{matrix}\right\},\quad d>1,$$

$$(9)\quad \left\{\begin{matrix} 0 & 1 & 2 & 3 & \cdots & k-1 & k \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 \\ k & k-1 & k-2 & k-3 & \cdots & 1 & 0 \end{matrix}\right\},\quad k=d,$$

$$(10)\quad \left\{\begin{matrix} 0 & 1 & 2 & 3 & \cdots & d-1 & d \\ 0 & 0 & 0 & 0 & \cdots & 0 & d+1 \\ 2d+1 & 2d & 2d-1 & 2d-2 & \cdots & d+2 & 0 \end{matrix}\right\}\quad d>1.$$

Remark. The intersection arrays in the above list are realized by the following graphs:

(1) complete graph K_{k+1},

(2) complete bipartite graph $K_{k,k}$,

(3) antipodal quotient of 5-dimensional hypercube when $\gamma=1$, Higman-Sims graph when $\gamma=2$, the existence of graphs is unknown when $\gamma>2$,

60

(4) complement of $2 \times (k+1)$-grid,

(5) Hadamard graph of valency $k = 4\gamma$,

(6) antipodal double cover of (3),

(7) cycle C_{2d+1} of length $2d+1$,

(8) cycle C_{2d} of length $2d$,

(9) d-dimensional hypercube,

(10) antipodal quotient of $(2d+1)$-dimensional hypercube.

References

[1] E. Bannai and Et. Bannai, Generalized generalized spin models (four-weight spin models), *Pac. J. Math.*, to appear.

[2] E. Bannai and Et. Bannai, Spin models on finite cyclic groups, *J. Algebraic Combinatorics*, **3** (1994), 243–259.

[3] E. Bannai, Et. Bannai and F. Jaeger, On spin models, modular invariance, and duality, submitted.

[4] Ei. Bannai and T. Ito, "Algebraic Combinatorics I," Benjamin/Cummings, Menlo Park, Calif., 1984.

[5] A.E. Brouwer, A.M. Cohen and A. Neumaier, "Distance-reguar graphs," Springer-Verlag, Berlin, Heidelberg, 1989.

[6] D.M. Goldschmidt and V. Jones, Metaplectic link invariants, *Geom. Dedicata* **31** (1989), 165–191.

[7] P. de la Harpe, Spin models for link polynomials, strongly regular graphs and Jaeger's Higman-Sims model, *Pac. J. Math* **162** (1994), 57–96.

[8] D. Higman and C. Sims, A simple group of order 44,352,000, *Math. Z.* **105** (1968), 110–113.

[9] F. Jaeger, Strongly regular graphs and spin models for the Kauffman polynomial, *Geom. Dedicata* **44** (1992), 23–52.

[10] F. Jaeger, On spin models, triply regular association schemes, and duality, *J. Algebraic Combinatorics*, to appear.

[11] F. Jaeger, New constructions of models for link invariants, *Pac. J. Math.*, to appear.

[12] V. Jones, On knot invariants related to some statistical mechanical models, *Pac. J. Math.* **137** (1989), 311–336.

[13] V. Jones, private communication.

[14] L.H. Kauffman, An invariant of regular isotopy, *Trans. AMS* **318** (1990), 417–471.

[15] K. Kawagoe, A. Munemasa and Y. Watatani, Generalized spin models, *J. of Knot Theory and its Ramifications*, to appear.

[16] V.G. Kac and M. Wakimoto, A construction of generalized spin models, preprint.

[17] K. Nomura, Spin models constructed from Hadamard matrices, *J. Combin. Theory Ser. A* **68** (1994), 251–261.

[18] K. Nomura, Homogeneous graphs and regular near polygons, *J. Combin. Theory Ser. B* **60** (1994), 63–71.

[19] K. Nomura, Spin models with an eigenvalue of small multiplicity, *J. Combin. Theory Ser. A*, to appear.

[20] K. Nomura, Spin models on bipartite distance-regular graphs, *J. Combin. Theory Ser. B*, to appear.

[21] K. Nomura, Spin models on triangle-free connected graphs, submitted.

[22] N. Yamazaki, Bipartite distance-regular graphs with an eigenvalue of multiplicity k, *J. Combin. Theory Ser. B*, to appear.

Classification of Spin Models with at most 10 Vertices

Haitao Guo
Department of Mathematics
Kyushu University

1 Introduction

In this paper, we classify spin models (X, W_+, W_-) with $5 \leq |X| \leq 10$ vertices in terms of commutative self-dual association schemes. This classcification is crucially based on the work about relation between spin models and association schemes by Jaeger and Nomura and the classification of association schemes with at most 10 vertices by Nomiyama. The notion of spin model is one of the statistical mechanical models introduced by V.F.R. Jones [12]. The importance of spin models comes from the fact that every spin model gives an invariant of knots and links through its partition function. Kawagoe, Munemasa and Watatani [13] generalized it by dropping the symmetric condition and gave the following definition.

Definition 1.1 *Let X be a finite set, $|X| = n = D^2$, w_+ and w_- be complex valued functions on $X \times X$. The tripe (X, w_+, w_-) is called a (generalized) spin model if the following conditions are satisfied for all α, β, and γ in X.*

(1) $w_+(\alpha,\beta)w_-(\beta,\alpha) = 1$,

(2) $\sum_{x\in X} w_-(\alpha,x)w_+(x,\beta) = n\delta_{\alpha,\beta}$,

(3) (star-triangle relation) $\sum_{x\in X} w_+(\alpha,x)w_+(x,\beta)w_-(x,\gamma) = Dw_+(\alpha,\beta)w_-(\beta,\gamma)w_-(\alpha,\gamma)$.

A spin model is called symmetric if the following additional condition

$$w_+(\alpha,\beta) = w_+(\beta,\alpha),\ w_-(\alpha,\beta) = w_-(\beta,\alpha)$$

is satisfied for any α and β in X .

Bannai and Bannai [2] made a further gengeralization and defined generalized generalized (4-weight) spin models as follows.

Definition 1.2 *Let X be a finite set and w_i, $i = 1, 2, 3, 4$, be complex valued functions on $X \times X$. The 5-tuple (X, w_1, w_2, w_3, w_4) is called a generalized generalized (4-weight) spin model if the following conditions are satisfied, where $|X| = n = D^2$.*

(4) $w_1(\alpha,\beta)w_3(\beta,\alpha) = 1$, $w_2(\alpha,\beta)w_4(\beta,\alpha) = 1$ *for any* α *and* β *in* X,

(5) $\sum_{x\in X} w_1(\alpha,x)w_3(x,\beta) = n\delta_{\alpha,\beta}$, $\sum_{x\in X} w_2(\alpha,x)w_4(x,\beta) = n\delta_{\alpha,\beta}$ *for any* α *and* β *in* X,

(6a) $\sum_{x\in X} w_1(\alpha,x)w_1(x,\beta)w_4(x,\gamma) = Dw_1(\alpha,\beta)w_4(\beta,\gamma)w_4(\alpha,\gamma)$ *for all* α, β *and* γ *in* X,

(6b) $\sum_{x\in X} w_1(x,\alpha)w_1(\beta,x)w_4(\gamma,x) = Dw_1(\beta,\alpha)w_4(\gamma,\beta)w_4(\gamma,\alpha)$ *for any* α *and* β *in* X.

Let $M(X)$ be the vector space of all matrices with rows and cloumns indexed by X and with complex entries, W_+ and W_- be the matrices in $M(X)$ defined by $W_+ = (w_+(\alpha,\beta))_{\alpha,\beta\in X}$ and $W_- = (w_-(\alpha,\beta))_{\alpha,\beta\in X}$. Let I be the identity matrix and J be the all-one matrix. Let $\circ$ denote the Hadamard product of two square matrices of the same size. Then those conditions given in Definition 1.1 can be restated as following:

(7) ${}^tW_+ \circ W_- = J$,

(8) $W_+W_- = nI$,

(9) ${}^tW_+({}^tW_-\circ(W_+M)) = D{}^tW_-\circ(W_+(W_-\circ M))$ for all M in $M(X)$.

A spin model is also denoted by (X, W_+, W_-).

Let $(X_i,(W_i)_+,(W_i)_-)$, for $i = 1,2$, be two spin models, then it is easy to see that $(X_1\times X_2, (W_1)_+\otimes(W_2)_+, (W_1)_-\otimes(W_2)_-)$ is also a spin model, which is called the tensor product of the previous models. Many examples of spin models can be found in the Bose-Mesner algebras of some association schemes

Example 1.3 *([7,9,12]) Let X be a finite set of cardinality n. Let* $R_0 = \{(x,x) \mid x \in X\}$ *and* $R_1 = \{(x,y) \mid x,y \in X$ *are distinct* $\}$*.Then(X,* $\{R_0, R_1\}$*) is a symmetric association scheme with 1 class. Suppose* A_0 *and* A_1 *are the adjacency matrices of* R_0 *and* R_1 *respectively, i.e.,* $A_0 = I$ *and* $A_1 = J - I$. *Let* $W_+ = t_0A_0 + t_1A_1$ *(and hence* $W_- = t_0^{-1}A_0 + t_1^{-1}A_1$*), where* t_0 *and* t_1 *satisfying*

$$\begin{cases} t_1^2 + t_1^{-2} + D = 0 \\ t_0 = -(t_1)^{-3}, \end{cases}$$

then (X, W_+, W_-) *is a spin model, called* **Potts model.**

A family of spin models from cyclic group association schemes and their symmetrizations is constructed by Bannai and Bannai [1,3]. Let $\mathcal{X}(G_n) = (G_n, \{R_i\}_{0\le i\le n-1})$ be a group association scheme on the cyclic group G_n. Note that the adjacency matrices of $\mathcal{X}(G_n)$ are given by

$$A_1 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}, \text{ and } A_i = (A_1)^i \text{ for } i = 0, 1, \dots n-1.$$

Furthermore, the eigenmatrix P of $\mathcal{X}(G_n)$ is given by

$$P = (\zeta_n^{ij}) \qquad 0 \leq \text{i,j} \leq \text{n-1}$$

where ζ_n is a primitive n-th root of unity.

Theorem 1.4 *([1]) With the above notation, let* $W_+ = \sum_{i=0}^{n-1} t_i A_i$ *and* $W_- = \sum_{i=0}^{n-1} t_{i'}^{-1} A_i$, *where* $i' = n - i$, *and*

$$t_i = \eta^{i(i+2s)} t_0 \qquad \text{for } 0 \leq i \leq n-1,$$
$$t_0^2 = D\eta^{s^2} / \textstyle\sum_{l=0}^{n-1} \eta^{l^2} \qquad \text{for } 0 \leq s \leq n-1,$$

with $\eta = \zeta_n^{\frac{n-1}{2}}$ *when n is odd, and* $\eta^2 = \zeta_n^{-1}$ *when n is even. Then* (G_n, W_+, W_-) *is a spin model, called* **cyclic model on** $\mathcal{X}(G_n)$.

Let $\widetilde{R_i} = R_i \cup R_{i'}$, for $i = 0, 1, \dots, [\frac{n}{2}]$, and $\widetilde{\mathcal{X}}(G_n) = (G_n, \{\widetilde{R_i}\}_{0 \leq i \leq [\frac{n}{2}]})$ a symmetrization association scheme. Let $\tilde{A}_i = A_i + A_{i'}$ for $i \neq i'$, and $\tilde{A}_i = A_i$ for $i = i'$ with $0 \leq \text{i} \leq [\frac{n}{2}]$. Then $\tilde{A}_i$ is an adjacency matrix with respect to $\widetilde{R_i}$ for all $0 \leq \text{i} \leq [\frac{n}{2}]$.

Theorem 1.5 *([3]) With the above notation, let* $W_+ = \sum_{i=0}^{[\frac{n}{2}]} t_i \tilde{A}_i$ *and* $W_- = \sum_{i=0}^{[\frac{n}{2}]} t_i^{-1} \tilde{A}_i$, *where*

(i) in case $n \neq 4$,

$$t_i = \eta^{i^2} t_0 \qquad \text{for } 0 \leq i \leq [\tfrac{n}{2}]$$
$$t_0^2 = D / \textstyle\sum_{l=0}^{\frac{n+1}{2}} \eta^{l^2}$$

with $\eta = \zeta^{\frac{n+1}{2}}$ *or* $\zeta^{\frac{n-1}{2}}$ *when n is odd, and* $\eta^2 = \zeta$ *or* ζ^{-1} *when n is even;*

(ii) in case $n = 4$,

$$t_1 = \eta t_0 \quad t_2 = -t_0 \text{ and } t_0^2 = D\eta^{-1}/2$$

with any nonzero complex number η.
Then (G_n, W_+, W_-) *is a symmetric spin model, called* **cyclic model on** $\widetilde{\mathcal{X}}(G_n)$

Bannai, Bannai and Jaeger [4] gave a classification for spin models on abelian group schemes. The classification of the symmetric spin models with n = 5, 6,and 7 has been completed by Bannai, Jaeger and Sali [6]. Also, generalized spin models with n $\leq$ 5 has been classified in [6]. Ikuta [8] classified the generalized spin models for n = 6 and 8. In this paper, the spin models with 5 $\leq$ n $\leq$ 10 vertices are classified in the following theorem.

Theorem 1.6 *Let (X, W_+, W_-) be a spin model with $5 \leq n \leq 10$ vertices,*
Case 1 *If n = 5, 6, 7 and 10, then it is one of the following*
(i) Potts model;
(ii) Cyclic model on $\mathcal{X}(G_n)$ or $\widetilde{\mathcal{X}}(G_n)$;
Case 2 *If n = 8, then it is one of the following*
(i) Potts model;
(ii) Cyclic model on $\mathcal{X}(G_8)$ or $\widetilde{\mathcal{X}}(G_8)$;
(iii) Spin model on Abelian group scheme on $Z_2 \times Z_4$ or $Z_2 \times Z_2 \times Z_2$;
(iv) Spin model (X, W_+, W_-) with the following

$$W_- = \begin{pmatrix} W' & -W' & W & W \\ -W' & W' & W & W \\ W & W & W' & -W' \\ W & W & -W' & W' \end{pmatrix}$$

where

$$W' = t_0 \begin{pmatrix} 1 & k \\ k & 1 \end{pmatrix} \text{ and } W = \tfrac{1+k}{\sqrt{2}} t_0^{-1} \begin{pmatrix} 1 & -k \\ -k & 1 \end{pmatrix}$$

with $k^2 = -1$ and t_0 any non-zero complex number;
Case 3 *If n = 9, then it is one of the following*
(i) Potts model;
(ii) Cyclic model on $\mathcal{X}(G_9)$ or $\widetilde{\mathcal{X}}(G_9)$;
(iii) Tensor product of two spin models, which are cyclic models on $\mathcal{X}(G_3)$ or Potts models, or one is cyclic model on $\mathcal{X}(G_3)$ and the other is Potts model.

2 Preliminaries

Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme, A_i be the adjacency matrix of $\mathcal{X}$ w.r.t.R_i and $\mathcal{U}$ be the subpace of $M(X)$ spanned by matrices A_i, $i = 0, 1, \ldots, d$. Then $\mathcal{U}$ is an associative commutative algebra with unit J under Hadamard product and $\mathcal{U}$ is also an associative commutative algebra with unit I under ordinary matrix product. The subspace $\mathcal{U}$ of $M(X)$ endowed with two algebra structure is called the Bose-Mesner algebra of the association scheme. Let $E_0, \ldots, E_d$ be the basis of minimal idempotents of $\mathcal{U}$. The eigenmatrices $P = (P_{ij})_{n \times n}$ and $Q = (Q_{ij})_{n \times n}$ of $\mathcal{U}$ related to the two basis of idempotents are as follows

$$A_j = \sum_{i=0}^{n} P_{ij} E_i,$$
$$E_j = \frac{1}{n} \sum_{i=0}^{n} Q_{ij} A_i.$$

Thus

$$PQ = nI$$

An association scheme $\mathcal{X}$ is said to be self-dual if $P = \bar{Q}$, i.e., $P\bar{P} = nI$ (See [5] on association schemes). The modular invariance property played a significant role in the construction of spin models from association schemes.

Definition 2.1 *Let $\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$ be a commutative self-dual association scheme and P be the eigenmatrix of $\mathcal{X}$, $|X| = n = D^2$. Then $\mathcal{X}$ is said to have the modular invariance property if there exists an invertible diagonal matrix $T = diag(t_0, t_1, \ldots, t_d)$ such that $(PT)^3 = t_0 D^3 I$.*

With the above notation, Bannai, Bannai and Jaeger gave constructions of certain spin models from some self-dual association scheme.

Theorem 2.2 *([4]) Let $\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$ be a self-dual association scheme with eigenmatrix P, and an invertible diagonal matrix $T = diag(t_0, t_1, \ldots, t_d)$ satisfies $(PT)^3 = t_0 D^3 I$. Then $W_+ = D\sum_{i=0}^{d} t_i E_i$ and $W_- = D\sum_{i=0}^{d} t_i A_i$ satisfy*

(1') $W_+ \circ W_- = J$,

(2') $W_+ W_- = nI$,

(3') ${}^tW_+({}^tW_- \circ (W_+ M)) = D\,{}^tW_- \circ (W_+ (W_- \circ M))$ for all M in $\mathcal{U}$.

Remark : If we replace the condition 'for all M in $\mathcal{U}$' in condition (3') by the condition that 'for all M in $M(X)$', we will get condition(9). So (X, W_+, W_-) is called a spin model at the algebraic level in $\mathcal{U}$.

Indeed, association schemes and their Bose-Mesner algebras provide a convenient and natural framework for the study of spin models (see [9]). Several subsequent works ([1,3,4,8,10]) observed that the matrices W_+ and W_- of a spin model belong to the Bose-Mesner algebra of some self-dual association schemes and can be obtained by solving certain modular invariance equations. This observation was confirmed in the following theorem.

Theorem 2.3 *([10,11,15]) Every spin model is given by a solution of the modular invariance equations for some commutative self-dual association schemes.*

Due to above theorems and the classification of association schemes with at most 10 vertices by Nomiyama [14], spin models with at most 10 vertices can be classified in the following way:

Step 1 *Determine whether the commutative association schemes given in [14] are self-dual, i.e., to check whether $P\bar{P} = nI$ for the (suitably indexed) eigenmatrices P of the scheme;*

Step 2 *For each case remained in Step 1, to find a diagonal matrix $T = diag(t_0, \ldots, t_d)$ with nonzero t_0 satisfying $(PT)^3 = t_0 D^3 I$. Since $P\bar{P} = nI$, i.e., $P^{-1} = \frac{1}{n}\bar{P}$, we have $TPT = \frac{t_0}{D}\bar{P}T^{-1}\bar{P}$. A family of modular invariance equations is obtained by comparing the corresponding entries of both sides and then to find out all solutions of these equations;*

Step 3 *Check whether (X, W_+, W_-), as constructed in Theorem 2.2, is an actural spin model or not, i.e., to check star-triangle condition in Definition 1.1.*

3 Classification

In this section, we give the proof of our result. Here we use the same notation of classification of association schemes given in [14]. For example, $6C_3$ means the third commutative association scheme with $n = 6$ in the list given in [14] and $6S_6$ the sixth sysmetric association scheme with $n = 6$ in the list.

Remark : Since Example1.3 implies that there exists a Potts model from an association scheme of class d=1 for any n, we will consider assocition scheme of classes $d > 1$.

3.1 The case of n = 5

Since there are exactly two association schemes of d (> 1) calsses for n=5, i.e., $\mathcal{X}(G_5)$ and $\tilde{\mathcal{X}}(G_5)$,it is clear that those spin models with n = 5 are Potts model or cyclic model on $\mathcal{X}(G_5)$ or $\tilde{\mathcal{X}}(G_5)$ respectively.

3.2 The case of n = 6

Among the six commutative association schemes of d (> 1) calsses for n=6, four of them, namely $6C_3$, $6C_4$, $6S_6$ and $6S_7$, are not self-dual, their eigenmatrices P are repectively as follows.

$$P_{6C_3} = \begin{pmatrix} 1 & 3 & 1 & 1 \\ 1 & -3 & 1 & 1 \\ 1 & 0 & \zeta_3 & \zeta_3^2 \\ 1 & 0 & \zeta_3^2 & \zeta_3 \end{pmatrix} \qquad P_{6C_4} = \begin{pmatrix} 1 & 2 & 2 & 1 \\ 1 & 0 & 0 & -1 \\ 1 & \alpha & \beta & 1 \\ 1 & \beta & \alpha & 1 \end{pmatrix}$$

where α and β are the roots of $t^2 + 2t + 4 = 0$, and

$$P_{6S_6} = \begin{pmatrix} 1 & 4 & 1 \\ 1 & 0 & -1 \\ 1 & -2 & 1 \end{pmatrix} \qquad P_{6S_7} = \begin{pmatrix} 1 & 3 & 2 \\ 1 & 0 & -1 \\ 1 & -3 & 2 \end{pmatrix}.$$

It is easy to check that these matrices do not satisfy $P\bar{P} = 6I$ for any arbitrary ordering of $\{A_i\}$. The other two schemes are $\mathcal{X}(G_6)$ and $\tilde{\mathcal{X}}(G_6)$. Therefore, as in the case of n = 5, the spin models with n = 6 are Potts model, cyclic models on $\mathcal{X}(G_6)$ or $\tilde{\mathcal{X}}(G_6)$ respectively.

3.3 The case of n = 7

In addition to $\mathcal{X}(G_7)$ and $\tilde{\mathcal{X}}(G_7)$, there is another commutative association scheme of d (> 1) classes for n = 7, namely $7C_3$.

Lemma 3.1 *The association scheme $7C_3$ is self-dual and has modular invariance property with $T = diag(t_0, t_1, t_2)$, where $t_0^2 = \frac{\sqrt{7}\alpha}{\alpha-3}$, t_1 and t_2 are the roots of $t^2 + \frac{\bar{\alpha}}{2}t_0 t - \sqrt{7}\frac{\alpha+1}{\alpha-3} = 0$.*

Proof : First the eigenmatrix P of $7C_3$ is

$$P_{7C_3} = \begin{pmatrix} 1 & 3 & 3 \\ 1 & \alpha & \bar{\alpha} \\ 1 & \bar{\alpha} & \alpha \end{pmatrix}$$

where α is a root of $t^2 + t + 2 = 0$. It is clear that $P\bar{P} = 7I$, so it is self-dual. To find $T = (t_0, t_1, t_2)$ satisfying $(P_{7C_3}T)^3 = t_0 7^{\frac{3}{2}} I$, as considered in Step 2, we have a family of equations as follows

(3.3.1) $t_0^2 = \frac{t_0}{\sqrt{7}}(t_0^{-1} + 3t_1^{-1} + 3t_2^{-1})$

(3.3.2) $\alpha t_1^2 = \frac{t_0}{\sqrt{7}}(3t_0^{-1} + \bar{\alpha}^2 t_1^{-1} + \alpha^2 t_2^{-1})$

(3.3.3) $\alpha t_2^2 = \frac{t_0}{\sqrt{7}}(3t_0^{-1} + \alpha^2 t_1^{-1} + \bar{\alpha}^2 t_2^{-1})$

(3.3.4) $t_0 t_1 = \frac{t_0}{\sqrt{7}}(t_0^{-1} + \bar{\alpha} t_1^{-1} + \alpha t_2^{-1})$

(3.3.5) $t_0 t_2 = \frac{t_0}{\sqrt{7}}(t_0^{-1} + \alpha t_1^{-1} + \bar{\alpha} t_2^{-1})$

(3.3.6) $\bar{\alpha} t_1 t_2 = \frac{t_0}{\sqrt{7}}(3t_0^{-1} + 2t_1^{-1} + 2t_2^{-1})$

Equations (3.3.2) through (3.3.5) give $(t_1 - t_2)(t_0 + \alpha(t_1 + t_2)) = 0$. Suppose $t_1 - t_2 = 0$, let $\frac{t_0}{t_1} = s$, then $s^2 + 5s + 1 = 0$ by (3.3.1) (3.3.5) and hence $s = \frac{3(1+2\alpha)}{3-\alpha}$ by (3.3.4) (3.3.6). Hence $s = \frac{3(1+2\alpha)}{3-\alpha}$ is not a root of $s^2 + 5s + 1 = 0$, it follows that $t_0 + \alpha(t_1 + t_2) = 0$, i.e., $t_1 + t_2 = -\frac{\bar{\alpha}}{t_0}$. By (3.3.2) and (3.3.3), we obtain

(3.3.7) $t_0(t_1 + t_2) = \frac{t_0}{\sqrt{7}}(2t_0^{-1} - t_1^{-1} - t_2^{-1})$

Hence, $t_0^2 = \frac{\sqrt{7}\alpha}{\alpha-3}$ by (3.3.7) and (3.3.1) and $t_1 t_2 = -\frac{\sqrt{7}(\alpha+1)}{\alpha-3}$ by (3.3.7) and (3.3.6). The lemma follows immediately.

Remark : Straightforward computation shows that (X, W_+, W_-), as constructed in Theorem 2.2, is not necessarily an actural spin model, because the star-triangle condition fails when $(\alpha, \beta, \gamma) = (1, 2, 7)$.

Hence, the spin models with n = 7 are Potts model or cyclic models on $\mathcal{X}(G_7)$ or $\tilde{\mathcal{X}}(G_7)$ respectively.

3.4 The case of n = 8

Lemma 3.2 *There are exactly eight self-dual schemes among those 17 commutative association schemes with d(> 1) classes for n = 8, namely* $8C_3$, $8C_4$, $8S_5$, $8C_6$, $8S_9$, $8S_{10}$, $8S_{16}$ *and* $8S_{17}$.

B Proof: Since $8C_3$, $8C_{10}$, $8C_4$ and $8S_5$ are $\mathcal{X}(G_8)$ and $\tilde{\mathcal{X}}(G_8)$ or association schemes on abelian groups $Z_2 \times Z_4$, $Z_2 \times Z_2 \times Z_2$ respectively, clearly they are self-dual. Furthermore, the eigenmatrices P of $8C_6, 8S_9, 8S_{16}$ and $8S_{17}$ are as follows

$$P_{8C_6} = \begin{pmatrix} 1 & 2 & 1 & 2 & 1 & 1 \\ 1 & 0 & i & 0 & -1 & -i \\ 1 & -2i & -1 & 2i & 1 & -1 \\ 1 & 0 & -i & 0 & -1 & i \\ 1 & -2 & 1 & -2 & 1 & 1 \\ 1 & 2i & -1 & -2i & 1 & -1 \end{pmatrix} \qquad P_{8S_9} = \begin{pmatrix} 1 & 2 & 1 & 1 & 2 & 1 \\ 1 & 0 & -1 & 1 & 0 & -1 \\ 1 & -2 & 1 & 1 & -2 & 1 \\ 1 & 2 & 1 & -1 & -2 & -1 \\ 1 & 0 & -1 & -1 & 0 & 1 \\ 1 & -2 & 1 & -1 & 2 & -1 \end{pmatrix}$$

$$P_{8S_{16}} = \begin{pmatrix} 1 & 2 & 1 & 4 \\ 1 & -2 & 1 & 0 \\ 1 & 2 & 1 & -4 \\ 1 & 0 & -1 & 0 \end{pmatrix} \qquad P_{8S_{17}} = \begin{pmatrix} 1 & 3 & 1 & 3 \\ 1 & -1 & 1 & -1 \\ 1 & 3 & -1 & -3 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

It can be shown that $P\bar{P} = 8I$ for these matrices. For the remaining 9 schemes, the corresponding matrices are given as follows:

$$P_{8C_7} = \begin{pmatrix} 1 & 2 & 1 & 2 & 1 & 1 \\ 1 & -2 & 1 & -2 & 1 & 1 \\ 1 & 2 & 1 & -2 & -1 & -1 \\ 1 & -2 & 1 & 2 & -1 & -1 \\ 1 & 0 & -1 & 0 & i & -i \\ 1 & 0 & -1 & -0 & -i & i \end{pmatrix}$$

$$P_{8C_8} = \begin{pmatrix} 1 & 2 & 2 & 1 & 1 & 1 \\ 1 & -2 & -2 & 1 & 1 & 1 \\ 1 & 0 & 0 & -1 & -1 & 1 \\ 1 & 0 & 0 & 1 & -1 & -1 \\ 1 & 2i & -2i & -1 & 1 & -1 \\ 1 & -2i & 2i & -1 & 1 & -1 \end{pmatrix} \qquad P_{8C_{11}} = \begin{pmatrix} 1 & 2 & 2 & 1 & 2 \\ 1 & -2 & 2 & 1 & -2 \\ 1 & 0 & -2 & 1 & 0 \\ 1 & \sqrt{2}i & 0 & -1 & -\sqrt{2}i \\ 1 & -\sqrt{2}i & 0 & -1 & \sqrt{2}i \end{pmatrix}$$

$$P_{8C_{12}} = \begin{pmatrix} 1 & 4 & 1 & 1 & 1 \\ 1 & -4 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ 1 & 0 & -1 & i & -i \\ 1 & 0 & -1 & -i & i \end{pmatrix} \qquad P_{8C_{13}} = \begin{pmatrix} 1 & 2 & 2 & 2 & 1 \\ 1 & -2 & -2 & 2 & 1 \\ 1 & 2i & -2i & -2 & 1 \\ 1 & -2i & 2i & -2 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$P_{8S_{14}} = \begin{pmatrix} 1 & 2 & 1 & 2 & 2 \\ 1 & 2 & 1 & -2 & -2 \\ 1 & -2 & 1 & 2 & -2 \\ 1 & -2 & 1 & -2 & 2 \\ 1 & 0 & -1 & 0 & 0 \end{pmatrix} \qquad P_{8S_{15}} = \begin{pmatrix} 1 & 4 & 1 & 1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ 1 & 0 & -1 & 1 & -1 \\ 1 & 0 & -1 & -1 & 1 \\ 1 & -4 & 1 & 1 & 1 \end{pmatrix}$$

$$P_{8S_{18}} = \begin{pmatrix} 1 & 3 & 4 \\ 1 & 3 & -4 \\ 1 & -1 & 0 \end{pmatrix} \qquad P_{8S_{19}} = \begin{pmatrix} 1 & 6 & 1 \\ 1 & -2 & 1 \\ 1 & 0 & -1 \end{pmatrix}$$

Straightforward computations show that they do not satisfy $P\bar{P} = 8I$ for any arbitrary ordering of $\{A_i\}$, and hence the corresponding association schemes are not self-dual.

We now check the modular invariance property for $8C_6, 8S_9, 8S_{16}$ and $8S_{17}$.

Lemma 3.3 *$8C_6$ does not satisfy the modular invariance property.*

Proof: Suppose there is a diagonal matrix $T = diag(t_0, \ldots, t_5)$ with nonzero t_0 satisfying $(P_{8C_6}T)^3 = t_0 8^{\frac{3}{2}} I$, then we have some modular invariance equtions as follows,

$$\begin{gathered} t_0^{-1} + t_2^{-1} + t_4^{-1} + t_5^{-1} = 0, \\ t_0^{-1} + t_2^{-1} + t_4^{-1} - t_5^{-1} = 0, \\ t_0^2 = -t_2^2. \end{gathered}$$

So $t_0 + t_4 = t_2 + t_5 = 0$ and $t_2 = kt_0$ where $k^2 = -1$. We have further modular invariance equations,

$$\begin{aligned} t_1 &= \tfrac{1}{\sqrt{2}}(t_0^{-1} - it_2^{-1}), \\ t_3 &= \tfrac{1}{\sqrt{2}}(t_0^{-1} + it_2^{-1}), \end{aligned}$$

then $t_1 t_3 = \frac{1}{2}(t_0^{-2} + t_2^{-2}) = 0$, which is impossible since T is invertible.

Lemma 3.4 *$8S_9$ has the modular invariance property with*

$$T = diag(t_0, \tfrac{1-k}{\sqrt{2}}t_0^{-1}, -t_0, kt_0, \tfrac{1+k}{\sqrt{2}}t_0^{-1}, -kt_0)$$

where $k^2 = -1$ *and* t_0 *any non-zero complex number.*

Proof: Suppose $T = diag(t_0, \ldots, t_5)$ with nonzero t_0 satisfies $(P_{8C_9}T)^3 = t_0 8^{\frac{3}{2}} I$, As before, we have

$$\begin{gathered} t_0^{-1} + t_2^{-1} + t_3^{-1} + t_5^{-1} = 0, \\ t_0^{-1} + t_2^{-1} - t_3^{-1} - t_5^{-1} = 0, \\ t_0^2 = -t_3^2. \end{gathered}$$

So $t_0 + t_2 = t_3 + t_5 = 0$ and $t_3 = kt_0$ with $k^2 = -1$. Furthermore,

$$\begin{aligned} t_1 &= \tfrac{1}{\sqrt{2}}(t_0^{-1} + t_3^{-1}) = \tfrac{1-k}{\sqrt{2}}t_0^{-1}, \\ t_4 &= \tfrac{1}{\sqrt{2}}(t_0^{-1} - t_4^{-1}) = \tfrac{1+k}{\sqrt{2}}t_0^{-1}. \end{aligned}$$

The lemma follows immediately.

Lemma 3.5 $8C_{16}$ *does not satisfy the modular invariance property.*

Proof: Suppose there is a diagonal matrix $T = diag(t_0, \ldots, t_5)$ with nonzero t_0 satisfying $(P_{8C_6}T)^3 = t_0 8^{\frac{3}{2}} I$, then we have

$$\begin{gathered} t_0 = t_2, \\ t_0^2 = \tfrac{t_0}{\sqrt{8}}(2t_0^{-1} + 2t_1^{-1} + 4t_3^{-1}), \text{ and} \\ t_0 t_2 = \tfrac{t_0}{\sqrt{8}}(2t_0^{-1} + 2t_1^{-1} - 4t_3^{-1}). \end{gathered}$$

It implies $t_3 = 0$, which is impossible. Then the lemma is proved.

Lemma 3.6 $8S_{17}$ *has the modular invariance property with* $T = diag(t_0, -t_0, kt_0, -kt_0)$, *where* $t_0^2 = \frac{k-1}{\sqrt{2}}$ *and* $k^2 = -1$.

Proof; Suppose $T = diag(t_0, \ldots, t_3)$ with nonzero t_0 satisfies $(P_{8C_{17}}T)^3 = t_0 8^{\frac{3}{2}} I$, then we have

$$\begin{aligned} t_0^2 = -t_2^2 &= \tfrac{t_0}{\sqrt{8}}(t_0^{-1} + 3t_1^{-1} + t_2^{-1} + 3t_3^{-1}), \\ t_1^2 = -t_3^2 &= \tfrac{t_0}{\sqrt{8}}(3t_0^{-1} + t_1^{-1} + 3t_2^{-1} + t_3^{-1}), \\ t_0 t_3 = t_1 t_2 &= \tfrac{t_0}{\sqrt{8}}(t_0^{-1} - t_1^{-1} - t_2^{-1} + t_3^{-1}), \\ t_0 t_2 &= \tfrac{t_0}{\sqrt{8}}(t_0^{-1} + 3t_1^{-1} - t_2^{-1} - 3t_3^{-1}), \\ t_0 t_1 &= \tfrac{t_0}{\sqrt{8}}(t_0^{-1} - t_1^{-1} + t_2^{-1} - t_3^{-1}). \end{aligned}$$

So $t_0 = kt_2$, $t_3 = kt_1$ and

$$t_0^2 + t_0 t_2 = \frac{t_0}{\sqrt{2}}(t_0^{-1} + 3t_1^{-1}),$$
$$t_1 t_2 + t_0 t_1 = \frac{t_0}{\sqrt{2}}(t_0^{-1} - t_1^{-1}).$$

Therefore $t_0 = -t_1$ and $t_1^2 = \frac{k-1}{\sqrt{2}}$. The lemma is proved.

Theorem 3.7 *Any spin model (X, W_+, W_-) with $|X|$ =8 is one of the following:*

(i) Potts model;

(ii) Cyclic model on $\mathcal{X}(G_8)$ or $\tilde{\mathcal{X}}(G_8)$;

(iii) Spin model on Abelian group scheme on $Z_2 \times Z_4$ or $Z_2 \times Z_2 \times Z_2$;

(iv) Spin model (X, W_+, W_-), where W_- is given in Theorem 1.6.

Proof: In addition to $8C_3$,$8C_4$, $8S_5$ and $8S_{10}$, Lemmas 3.2 through 3.6*showthat*8S$_9$ and $8S_{17}$ have the modular invariant property. The spin models constructed from association schemes $8C_4$ and $8S_5$ on cyclic group and schemes $8C_3$ and $8S_{10}$ on Abelian group $Z_2 \times Z_4$ and $Z_2 \times Z_2 \times Z_2$ are known in [1,3,4]. For $8S_9$, routine computation confirms that the spin model (X, W_+, W_-) constructed by Theorem 2.2 is an actural model where W_- is

$$W_- = \begin{pmatrix} W' & -W' & W & W \\ -W' & W' & W & W \\ W & W & W' & -W' \\ W & W & -W' & W' \end{pmatrix}$$

with

$$W' = t_0 \begin{pmatrix} 1 & k \\ k & 1 \end{pmatrix} \text{ and } W = \frac{1+k}{\sqrt{2}} t_0^{-1} \begin{pmatrix} 1 & -k \\ -k & 1 \end{pmatrix}$$

$k^2 = -1$. When $t_0^2 = \frac{k-1}{2}$, the spin model is identical with the spin model constructed from association scheme $8S_{17}$. Therefore we have the theorem.

Remark : The spin model of case (iv) is missed in Ikuta's result [8]. By Lemma 5 in [16], one can obtain a 4-weight spin model with $n = 2$ from it.

3.5 The case of n = 9

Lemma 3.8 *There are eight self-dual schemes among 11 commutative association schemes with d (> 1) classes for n = 9, which are $9C_1$, $9C_2$, $9C_3$, $9S_4$, $9S_5$, $9S_7$, $9S_{10}$ $9S_{11}$. The other are not self-dual.*

Proof: Obviously, $9C_1$, $9C_2$ and $9S_5$, which are association schemes on abelian group $Z_3 \times Z_3$, $\mathcal{X}(G_9)$ and $\tilde{\mathcal{X}}(G_9)$ respectively, are self-dual. The eigenmatrices P of $9C_3$, $9S_4$,$9S_7$, $9S_{10}$, and $9S_{11}$ are as follows

$$P_{9C_3} = \begin{pmatrix} 1 & 2 & 1 & 2 & 1 & 2 \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 2 & \zeta_3^2 & 2\zeta_3^2 & \zeta_3 & 2\zeta_3 \\ 1 & -1 & \zeta_3^2 & -\zeta_3^2 & \zeta_3 & -\zeta_3 \\ 1 & 2 & \zeta_3 & 2\zeta_3 & \zeta_3^2 & 2\zeta_3^2 \\ 1 & -1 & \zeta_3 & -\zeta_3 & \zeta_3^2 & -\zeta_3^2 \end{pmatrix}$$

$$P_{9S_4} = \begin{pmatrix} 1 & 2 & 2 & 2 & 2 \\ 1 & 2 & -1 & -1 & -1 \\ 1 & -1 & 2 & -1 & -1 \\ 1 & -1 & -1 & 2 & -i \\ 1 & -1 & -1 & -1 & 2 \end{pmatrix} \qquad P_{9C_7} = \begin{pmatrix} 1 & 2 & 2 & 4 \\ 1 & -1 & 2 & -2 \\ 1 & 2 & -1 & -2 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$P_{9C_{10}} = \begin{pmatrix} 1 & 4 & 4 \\ 1 & 1 & -2 \\ 1 & -2 & 1 \end{pmatrix} \qquad P_{9C_{11}} = \begin{pmatrix} 1 & 2 & 6 \\ 1 & 2 & -3 \\ 1 & -1 & 0 \end{pmatrix}$$

It can be seen that $P\bar{P} = 9I$ for these matrices. For the remaining three schemes, the related matrices are given as follows

$$P_{9C_6} = \begin{pmatrix} 1 & 3 & 3 & 1 & 1 \\ 1 & \alpha & \bar{\alpha} & 1 & 1 \\ 1 & \bar{\alpha} & \alpha & 1 & 1 \\ 1 & 0 & 0 & \zeta_3 & \zeta_3^2 \\ 1 & 0 & 0 & \zeta_3^2 & \zeta_3 \end{pmatrix}$$

$$P_{9C_8} = \begin{pmatrix} 1 & 6 & 1 & 1 \\ 1 & -3 & 1 & 1 \\ 1 & 0 & \zeta_3 & \zeta_3^2 \\ 1 & 0 & \zeta_3^2 & \zeta_3 \end{pmatrix} \text{ and } P_{9C_9} = \begin{pmatrix} 1 & 3 & 3 & 2 \\ 1 & 0 & 0 & -1 \\ 1 & \alpha & \bar{\alpha} & 2 \\ 1 & \bar{\alpha} & \alpha & 2 \end{pmatrix}$$

where α is a root of $t^2 + 3t + 9 = 0$. These matrices do not satisfy $P\bar{P} = 9I$ for arbitrary ordering of $\{A_i\}$, therefore the corresponding association schemes are not self-dual.

Lemma 3.9 *$9S_3$ has the modular invariance property with $T = diag(\zeta_3 s^2 f, \zeta_3 s^2 t^2 f, sf, st^2 f, f, t^2 f)$, where $t = \zeta_3$ or ζ_3^2, $s^3 = 1$ and $f^2 = \frac{1}{3}(1+2t)(\zeta_3 s^2 + \zeta_3^2 s + \zeta_3^2)$.*

Proof: Suppose $T = diag(t_0, \ldots, t_5)$ with nonzero t_0 satisfies $(P_{9C_3}T)^3 = t_0 9^{\frac{3}{2}} T$, then we have modular invariance equations as follows,

$$
\begin{aligned}
t_0^2 = \zeta_3^2 t_2 t_4 &= \tfrac{t_0}{3}(t_0^{-1} + 2t_1^{-1} + t_2^{-1} + 2t_3^{-1} + t_4^{-1} + 2t_5^{-1}),\\
t_0 t_1 = \zeta_3^2 t_2 t_5 = \zeta_3^2 t_3 t_4 &= \tfrac{t_0}{3}(t_0^{-1} - t_1^{-1} + t_2^{-1} + -t_3^{-1} + t_4^{-1} - t_5^{-1}),\\
t_0 t_2 &= \tfrac{t_0}{3}(t_0^{-1} + 2t_1^{-1} + \zeta_3^2 t_2^{-1} + 2\zeta_3^2 t_3^{-1} + \zeta_3 t_4^{-1} + 2\zeta_3 t_5^{-1}),\\
t_0 t_4 &= \tfrac{t_0}{3}(t_0^{-1} + 2t_1^{-1} + \zeta_3 t_2^{-1} + 2\zeta_3 t_3^{-1} + \zeta_3^2 t_4^{-1} + 2\zeta_3^2 t_5^{-1}),\\
t_0 t_3 &= \tfrac{t_0}{3}(t_0^{-1} - t_1^{-1} + \zeta_3^2 t_2^{-1} - \zeta_3^2 t_3^{-1} + \zeta_3 t_4^{-1} - \zeta_3 t_5^{-1}),\\
t_0 t_5 &= \tfrac{t_0}{3}(t_0^{-1} - t_1^{-1} + \zeta_3 t_2^{-1} - \zeta_3 t_3^{-1} + \zeta_3^2 t_4^{-1} - \zeta_3^2 t_5^{-1}).
\end{aligned}
$$

Hence

$$
\begin{aligned}
t_0^2 + t_0 t_2 + t_0 t_4 &= t_0(t_0^{-1} + 2t_1^{-1}),\\
t_0 t_1 + t_0 t_3 + t_0 t_5 &= t_0(t_0^{-1} - t_1^{-1}),
\end{aligned}
$$

and

$$
t_0/t_1 = t_2/t_3 = t_4/t_5 = t,
$$

then

$$
t = \tfrac{t_0+t_2+t_4}{t_1+t_3+t_5} = \tfrac{t_1+2t_0}{t_1-t_0} = \tfrac{1+2t}{1-t}.
$$

Therefore $t^2+t+1=0$ i.e., $t=\zeta_3$ or ζ_3^2. Furtherly $\zeta_3 t_2^2 = t_0 t_4$ and $\zeta_3 t_4^2 = t_0 t_2$, so $(t_2/t_4)^3 = 1$. Let $t_2 = s t_4$, where $s^3=1$, then

$$
\begin{aligned}
t_5 &= t^2 t_4,\\
t_3 = t^2 t_2 &= s t^2 t_4,\\
t_0 &= \zeta_3 s^2 t_4,
\end{aligned}
$$

and $t_1 = \zeta_3 s^2 t^2 t_4$. Since $t_0 = \frac{1}{3}(t_0^{-1}+2t_1^{-1}+t_2^{-1}+2t_3^{-1}+t_4^{-1}+2t_5^{-1})$, $t_4 = \frac{1}{3}(1+2t)(\zeta_3 s^2+\zeta_3^2 s+\zeta_3^2)$. The lemma is proved

Lemma 3.10 *$9S_4$ does not satisfy the modular invariance property.*

Proof: Suppose that $T = diag(t_0,\ldots,t_4)$ with nonzero t_0 satisfies $(P_{9S_4}T)^3 = t_0 9^{\frac{3}{2}} T$. As above proof, we have

$$
\begin{aligned}
t_0^2 &= \tfrac{t_0}{3}(t_0^{-1} + 2t_1^{-1} + 2t_2^{-1} + 2t_3^{-1} + 2t_4 - 1),\\
t_0 t_1 &= \tfrac{t_0}{3}(t_0^{-1} + 2t_1^{-1} - t_2^{-1} - t_3^{-1} - t_4 - 1),\\
2t_1^2 &= \tfrac{t_0}{3}(2t_0^{-1} + 4t_1^{-1} + t_2^{-1} + t_3^{-1} + t_4 - 1).
\end{aligned}
$$

So $t_0 = t_1 = \epsilon$ and $t_2^{-1} + t_3^{-1} + t_4^{-1} = 0$, where $\epsilon^2 = 1$. But we also have

$$t_2 = \frac{1}{3}(2t_2^{-1} - t_3^{-1} - t_4^{-1}),$$
$$t_3 = \frac{1}{3}(-t_2^{-1} + 2t_3^{-1} - t_4^{-1}),$$
$$t_4 = \frac{1}{3}(-t_2^{-1} - t_3^{-1} + 2t_4^{-1}),$$

then $t_2^2 = t_3^2 = t_4^2 = 1$ contradiction. The lemma is proved.

Lemma 3.11 *$9S_7$ has the modular invariance property with $T = diag(t_0, \alpha t_0, \beta t_0, \alpha\beta t_0)$, where $t_0^2 = 1$ when $\alpha = \beta = \zeta_3$ or ζ_3^2 , and $t_0^2 = -1$ when $(\alpha, \beta) = (\zeta_3, \zeta_3^2)$ or (ζ_3^2, ζ_3).*

Proof: Suppose $T = diag(t_0, \ldots, t_3)$ with nonzero t_0 satisfies $(P_{9S_7}T)^3 = t_0 9^{\frac{3}{2}} T$, then we have

$$t_0^2 = \frac{t_0}{3}(t_0^{-1} + 2t_1^{-1} + 2t_2^{-1} + 4t_3^{-1}),$$
$$t_0 t_1 = \frac{t_0}{3}(t_0^{-1} - t_1^{-1} + 2t_2^{-1} - 2t_3^{-1}),$$
$$t_0 t_2 = \frac{t_0}{3}(t_0^{-1} + 2t_1^{-1} - t_2^{-1} - 2t_3^{-1}),$$
$$t_0 t_3 = t_1 t_2 = \frac{t_0}{3}(t_0^{-1} - t_1^{-1} - t_2^{-1} + t_3^{-1}),$$
$$-t_1^2 = \frac{t_0}{3}(t_0^{-1} - t_1^{-1} - t_2^{-1} + t_3^{-1}).$$

Let $t_1/t_0 = t_3/t_2 = \alpha$,$t_2/t_0 = \beta$ and $t_3/t_0 = \gamma$, then

$$t_0^2 + 2t_0 t_1 = t_0 t_1 - t_1^2,$$
$$t_0^2 + 2t_0 t_2 = t_0 t_2 - t_2^2,$$
$$t_0^2 + 2t_0 t_3 = t_0(t_0^{-1} + 2t_3^{-1}),$$
$$t_3^2 + 2t_0 t_3 = t_0(2t_0^{-1} + t_3^{-1}),$$

we have

$$\alpha^2 + \alpha + 1 = 0,$$
$$\beta^2 + \beta + 1 = 0,$$
$$\gamma^3 = 1 \text{ and } \gamma = \alpha\beta,$$

and the lemma is proved.

The following lemma was proved in [9]

Lemma 3.12 *$9S_{10}$ has the modular invariance property, but $9S_{11}$ does not.*

Theorem 3.13 *Let (X, W_+, W_-) be a spin model with $n = 9$, then the spin model is one of the following*

(i) Potts model;

(ii) Cyclic model on $\mathcal{X}(G_9)$ or $\tilde{\mathcal{X}}(G_9)$;

(iii) The tensor products of two spin models, which are cyclic models on $\mathcal{X}(G_3)$, or Potts models, or one is cyclic models on $\mathcal{X}(G_3)$ and the other is Potts model.

Proof: The spin model from association scheme $9C_1$ on Abelian group $Z_3 \times Z_3$ is constructed in [4]. It is a tensor product of cyclic models on $\mathcal{X}(G_3)$. The spin model from $9S_{10}$, constructed in [9], is a tensor product of two Potts models. By calculating, the spin model from $9C_3$ constructed by theorem 2.2 is an actural model. The matrix W_- has the following form

$$W_- = \begin{pmatrix} a & b & b & c & d & d & f & g & g \\ b & a & b & d & c & d & g & f & g \\ b & b & a & d & d & c & g & g & f \\ f & g & g & a & b & b & c & d & d \\ g & f & g & b & a & b & d & c & d \\ g & g & f & b & b & a & d & d & c \\ c & d & d & f & g & g & a & b & b \\ d & c & d & g & f & g & b & a & b \\ d & d & c & g & g & f & b & b & a \end{pmatrix}$$

with $a = \zeta_3 s^2 f$, $b = \zeta_3 s^2 t^2 f$, $c = sf$, $d = st^2 f$, $g = t^2 f$, where $t = \zeta_3$ or ζ_3^2, $s^3 = 1$ and $f^2 = \frac{1}{3}(1+2t)(\zeta_3 s^2 + \zeta_3^2 s + \zeta_3^2)$. It is a tensor product of a cyclic model on $\mathcal{X}(G_3)$ and a Potts model. On the other hand, the spin models from $9S_7$ is identical with it when s=1. Therefore we have the theorem.

3.6 The case of n = 10

Lemma 3.14 *There are exactly three self-dual schemes among 11 commutative association schemes with d (> 1) classes for n = 10, namely $10C_1$, $10S_4$ and $10S_9$. The other are not self-dual.*

Proof: It is obvious that $10C_1$ and $10S_4$,i.e., $\mathcal{X}(G_{10})$ and $\tilde{\mathcal{X}}(G_{10})$ respectively, are self-dual. The eigenmatrix of $10S_9$ is

$$P_{10S_9} = \begin{pmatrix} 1 & 1 & 4 & 4 \\ 1 & -1 & 4 & 4 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

which satisfies $P\bar{P} = 10I$, and hence $10S_9$ is self-dual. For the other seven schemes, the corresponding matrices are given asfollows

$$P_{10C_3} = \begin{pmatrix} 1 & 2 & 2 & 2 & 2 & 1 \\ 1 & 0 & 0 & 0 & 0 & -1 \\ 1 & 2\zeta_5 & 2\zeta_5^4 & 2\zeta_5^2 & 2\zeta_5^3 & 1 \\ 1 & 2\zeta_5^2 & 2\zeta_5^3 & 2\zeta_5^4 & 2\zeta_5 & 1 \\ 1 & 2\zeta_5^3 & 2\zeta_5^2 & 2\zeta_5 & 2\zeta_5^4 & 1 \\ 1 & 2\zeta_5^4 & 2\zeta_5 & 2\zeta_5^3 & 2\zeta_5^2 & 1 \end{pmatrix} \qquad P_{10C_5} = \begin{pmatrix} 1 & 5 & 1 & 1 & 2 & 1 \\ 1 & -5 & 1 & 1 & 1 & 1 \\ 1 & 0 & \zeta_5^2 & \zeta_5^4 & \zeta_5^3 & \zeta_5 \\ 1 & 0 & \zeta_5^4 & \zeta_5^3 & \zeta_5 & \zeta_5^2 \\ 1 & 0 & \zeta_5 & \zeta_5^2 & \zeta_5^4 & \zeta_5^3 \\ 1 & 0 & \zeta_5^3 & \zeta_5 & \zeta_5^2 & \zeta_5^4 \end{pmatrix}$$

$$P_{10S_8} = \begin{pmatrix} 1 & 4 & 4 & 1 \\ 1 & -4 & 2 & 1 \\ 1 & 2 & -4 & 1 \\ 1 & 0 & 0 & -1 \end{pmatrix} \qquad P_{10S_{10}} = \begin{pmatrix} 1 & 2 & 2 & 5 \\ 1 & 2 & 2 & -5 \\ 1 & \alpha & \beta & 0 \\ 1 & \beta & \alpha & 0 \end{pmatrix}$$

where α and β are roots of $t^2 + t - 1 = 0$.

$$P_{10S_{11}} = \begin{pmatrix} 1 & 1 & 8 \\ 1 & 1 & -2 \\ 1 & -1 & 0 \end{pmatrix}$$

$$P_{10S_{12}} = \begin{pmatrix} 1 & 4 & 5 \\ 1 & 4 & -5 \\ 1 & -1 & 0 \end{pmatrix} \qquad P_{10S_{13}} = \begin{pmatrix} 1 & 3 & 6 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$$

These matrices do not satisfy $P\bar{P} = 10I$ for any arbitrarily ordering of $\{A_i\}$, and hence the corresponding schemes are not self-dual.

Remark : Since $10S_6$ is isomorphics to $10S_4$ via the permutation (2,9)(3,5,4,10,8,7) on their vertices, $10S_6$ is ignored in the list in [14].

Lemma 3.15 *$10S_9$ has the modular invariance property with $T = diag(t_0, kt_0, \alpha^{-1}t_0, k\alpha^{-1}t_0)$, where $k^2 = -1$, α is a root of $t^2 + 3t + 1 = 0$ and $t_0 = \frac{1-k}{\sqrt{10}}(1 + 4\alpha)$.*

Proof: Suppose $T = diag(t_0, \ldots, t_3)$ with nonzero t_0 satisfies $(P_{10S_9}T)^3 = t_0 10^{\frac{3}{2}} T$. Therefore we have

(3.6.1) $\quad t_0^2 = -t_1^2 = \frac{t_0}{\sqrt{10}}(t_0^{-1} + t_1^{-1} + 4t_2^{-1} + 4t_3^{-1}),$

(3.6.2) $\quad -t_2^2 = t_3^2 = \frac{t_0}{\sqrt{10}}(4t_0^{-1} + 4t_1^{-1} + t_2^{-1} + t_3^{-1}),$

(3.6.3) $\quad t_0 t_1 = \frac{t_0}{\sqrt{10}}(t_0^{-1} - t_1^{-1} + 4t_2^{-1} - 4t_3^{-1}),$ and

(3.6.4) $\quad t_0 t_2 = \frac{t_0}{\sqrt{10}}(t_0^{-1} + t_1^{-1} - t_2^{-1} - t_3^{-1}).$

By (3.6.1) and (3.6.2), $t_1 = k_1 t_0, t_3 = k_2 t_2$, where $k_1^2 = k_2^2 = -1$, then (3.6.1) and (3.6.3) become

$$t_0 = \frac{1}{\sqrt{10}}((1-k_1)t_0^{-1} + 4(1-k_2)t_2^{-1}),$$
$$k_1 t_0 = \frac{1}{\sqrt{10}}((1+k_1)t_0^{-1} + 4(1+k_2)t_2^{-1}).$$

Hence we have $k_1 = k_2 = k$, and (3.6.1), (3.6.4) become

$$t_0 = \frac{1-k}{\sqrt{10}}(t_0^{-1} + 4t_2^{-1}),$$
$$t_1 = \frac{1-k}{\sqrt{10}}(t_0^{-1} - t_2^{-1}),$$

let $t_0/t_1 = \alpha$, then α satisfys $t^2 + 3t + 1 = 0$.
By (3.6.1)

$$t_0^2 = \frac{1-k}{\sqrt{10}}(1 + 4\alpha).$$

The lemma is proved.

Remark : By calculation, we see that the spin model (X, W_+, W_-) as constructed in Theorem 2.2 is not an actural model because the star-triangle condition fails when $(\alpha, \beta, \gamma) = (1, 1, 2)$.

As above consideration, the spin model with n = 10 is a Potts model or a cyclic model on $\mathcal{X}(G_{10})$ or $\widetilde{\mathcal{X}}(G_{10})$ respectively.

Finally, combining the results in all subsections considered above, we have the classification of spin models with $5 \leq$ n ≤ 10 as described in Theorem1.6.

Acknowledgement The author would like to thank K. Nomura for suggesting the present form for W_- of (iv) in case $n = 8$ of Theorem 1.6 and pointing out a 4-weight spin model can be obtained from it.

References

[1] E. Bannai, E. Bannai, Spin models on finite cyclic groups, J. of Algebraic Combinatorics,3 (1994), 243-259.

[2] E. Bannai, E. Bannai, Generalized generalized spin models (four-weight spin models), Pacific J. of Math., to appear.

[3] Etsuko Bannai, Modular invariance property and spin models attached to cyclic group association schemes, to appear in Journal of Statistical Planning and Inference.

[4] E. Bannai, E. Bannai and F. Jaeger, On spin models, modular invariance and duality, to appear.

[5] E. Bannai and T. Ito, Algebraic Combinatorics I, Association Schemes, Benjuminl Cummings, Menlo Park C.A. 1984.

[6] E. Bannai, F. Jaeger and A. Sali, Classification of small spin models, Kyushu J. Math Vol XLVIII No.1, 1994.

[7] P.de.la. Harpe, Spin models for link polynomials, strongly regular graph and Jaeger's Higmann-Sims model, Pac. J. Math 162(1994) 57-96.

[8] T. Ikuta, On spin models attached to association schemes, Ph.D. thesis, Kyushu University 1994.

[9] F. Jaeger, Strogly regular graphs and spin models for the Kauffman polynomial, Geom. Dedicata 44(1992), 23-52.

[10] F. Jaeger, Towards a classification of spin models in terms of association schemes, preprint.

[11] F. Jaeger, M. Matsumoto and K. Nomura, Association schemes defined by type II matrices and spin models, preprint.

[12] V.F.R. Jones, On knot invariants related to some statistical mechanical models, Pac. J. Math 137(1989) 311-334.

[13] K. Kawagoe, A. Munemasa and Y. Watatani, Generalized spin models, to appear in Knot Theory and its Ramifications.

[14] E. Nomiyama, Classification of association schemes with at most ten vertices, Master's degree thesis, Kyushu Univ. 1994.

[15] K. Nomura, Twisted extensions of spin models, J. Algebraic Comb. 4 (1995), 173-182.

[16] K. Nomura, An algebra associated with a spin model, to appear.

頂点作用素代数のテンソル積構成

宮本雅彦
愛媛大学理学部

1 序文

頂点作用素代数の概念は Frenkel, Lepowsky, Meurman によるムーンシャイン加群の構成と Borcherds による頂点代数の導入から始まりました．頂点作用素代数は本質的に 2 次元共形場理論のカイラル代数と同一だと考えられています．頂点作用素代数の理論はこの数年で急速に発展し，ヴィラソロ代数やアフィンカッツムーディ代数の表現論に多くの新しい展望を与えています．この理論はまた，有限群や，モジュラー関数などに対しても多くの興味ある関係を提供しています．

もっとも注目される例はムーンシャイン加群

$$V^\natural = \sum_{i=0}^{\infty} V_i^\natural$$

であり，多くの興味ある性質を持っています．例えば，この頂点作用素代数の自己同型群は最大の散在型有限単純群であるモンスター単純群 M であり，$V^\natural$の指標

$$q^{-1}\sum_{n=0}\dim V_n^\natural q^n$$

は古典的モジュラー関数

$$J(z) = q^{-1} + 196884q + \ldots \qquad (q = e^{2\pi i z}),$$

となっています．しかも，モンスター単純群の各元 $g \in \mathbf{M}$ に対して，トレース指標

$$\sum_{n=0} \mathrm{tr}(g_{|V_n^\natural})e^{2\pi i(n-1)z},$$

もある合同群のモジュラー関数となっています．さらに，この頂点作用素代数は一般化されたカッツムーディ代数（ボーチャード代数）の一つであるモンスターリー代数を定義します．

このような性質は知られている頂点作用素代数すべてが類似したものをもっており，証明はされてはいませんが頂点作用素代数のもつ不思議な性質と考えられています．

しかしながら，問題はこのような頂点作用素代数の例が多くなく，また存在しているものも，その構成が決して簡単ではないということです．

この講演の最初の目的は頂点作用素代数の新しい構成法を紹介することです．著者は最近，偶2次コードから頂点作用素代数を構成する方法を発表しました．[M2]．それらはある頂点作用素超代数のテンソル積の部分代数として定義しました．ここでの目標は，その方法を発展させ，Mossberg [Mo] が導入した頂点作用素超代数の拡張した概念から群の拡大の部分を取り外した group-skew 頂点作用素代数を使って新しい頂点作用素代数と構成することです．この構成の利点は構成法が簡単なので，構成された頂点作用素代数の指標などの情報が分かりやすいことです．例えば応用として，

(1) 指標で，モジュラー関数などの多くの関数を得ることができ，
(2) 上の関数の間の恒等式
(3) Orbifold 構成と格子のツイスト構成との関係
(4) Broué Enguehard 写像の説明
が分かります．

(3) について説明すると，ムーンシャイン加群 $V^\natural$ はリーチ格子頂点作用素代数 V_Λ から orbifold 構成によって構成されています．Montague はこの方法を他のニイマイヤ格子にも適用して，幾つかの新しい頂点作用素代数を構成したのですが，その中の幾つかの頂点作用素代数は，他のニイマイヤ格子頂点作用素代数と一致していました．モンタギューはこの一致がコードから構成された格子のツイスト構成と一致している事に気付きました．例えば，D をゴーレイコードとすると，タイプ A_1^{24} のニイマイヤ格子が構成でき，頂点作用素代数 $V_{A_1^{24}}$ が構成できます．これを orbifold 構成すると丁度リーチ格子頂点作用素代数と同型となることが指標からわかりますが，A_1^{24} 型の格子のツイストでリーチ格子が構成できるのです．これがなぜ起こるのかを我々のテンソル積構成を通して明らかにすることができます．

(4) についは説明すると，[BE] の中で，Broué-Enguehard は self-dual doubly even 2次コードの weight enumerators からモジュラー形式の空間への写像を定義しました．self-dual doubly even 2次コードの weight enumerators の空間は $\mathbb{C}[x,y]^G$ に同型であることが知られています．ここで，G は$\sigma_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ と$\sigma_2 = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & 1 \end{pmatrix}$ によって生成された位数 192 の有限群です．$\mathbb{C}[x,y]$ への作用は$\sigma(x) = ax + by, \sigma(y) = cx + dy$ で与えます．

最近，小関氏 [O] は同じ写像が形式的 weight enumerators の空間 $\mathbb{C}[x,y]^H$ とモジュラー形式の空間 $\mathbb{C}[E_4, E_6]$ との間の代数同型を与えることを示しました．さらに，Jacobi-forms と Siegel modular forms に対しても類似した写像ができることが小関、坂内両氏によって示されています．[BO]．ここでは，少し変形した Broué-Enguehard の写像が頂点作用素代数の言葉で与えられることをしめし，さらに小関氏によって拡張された写像も group-skew 頂点作用素代数の言葉で説明できることを示します．

2 Group-skew 頂点作用素代数 の定義

通常は，頂点作用素代数とは幾つかの条件を満足する無限個の積をもった無限次数付きベクトル空間 $V=\sum_{n=0}^{\infty}V_n$ です．しかし，頂点作用素代数は色々な顔を持っており，ヴィラソロ代数を含む可換 (local) な元からなる代数とも言えます．この可換性は物理において locality とよばれ，数学における通常の可換とは異なっているものです．可換 (local) について少し説明しましょう．

結合代数 R にたいして，形式的巾級数
$a(z)=\sum a_n z^{-n-1}, b(z)=\sum b_n z^{-n-1}\in R[[z,z^{-1}]]$ を考えます．ここで $R[[z,z^{-1}]]$ は R に係数を持つ形式的巾級数全体のなす空間を表します．通常，可換とは

$$a(z)b(z)=b(z)a(z)$$

の事ですが，無限級数なので積さえも定義できません．形式的級数であることをつかって，２つの変数を考え，

$$\text{十分大きな n に対して}\qquad (z_1-z_2)^n a(z_1)b(z_2)=(z_2-z_1)^n b(z_2)a(z_1)$$

が成り立つとき，$a(z)$ と $b(z)$ を可換と呼び，$a(z)\sim b(z)$ で表すことにします．

頂点作用素代数の定義を与えましょう．ここでは，通常の公理と少し異なる方法で説明します．通常は Jacobi の恒等式をつかっています．これは非常に役に立つ恒等式であるが，証明しようとすると大変です．ここの目標は構成なので，それらの同値であることが Dong と Li によって証明された"可換"を使うことにします．

定義 1　　$V=\oplus_{n=0}^{\infty}V_n$ を（フォック空間と呼ばれる）自然数次数付きベクトル空間とし，各 $v\in V$ に対して，v の頂点作用と呼ばれる形式的巾級数

$$Y(v,z)=\sum v_n z^{-n-1}\in End\ V[[z,z^{-1}]]$$

が与えられており，次の条件を満たす
(1) $Y(v,z)$ は互いに可換，即ち，任意の v,v' に対して $Y(v,z)\sim Y(v',z)$ が成り立つ．
(2) ヴィラソロ元 $w\in V_2$ と呼ばれる特別な元があって，それの頂点作用素

$$w(z)=\sum w_n z^{-n-1}=\sum L(n)z^{-n-2}$$

の係数 $L(n9$ は次の $(a)\sim(c)$ を満たす．
(a) [ヴィラソロ代数交換式]

$$[L(i),L(j)]=(i-j)L(i+j)+\delta_{i+j,0}\binom{i+1}{3}\frac{c}{2}$$

(b) [微分]

$$Y(L(-1)v,z)=[L(-1),Y(v,z)]=\frac{d}{dz}Y(v,z)$$

(c) V_n は $L(0)$ による固有値 n の固有空間である.
(3) 真空と呼ばれる特別な元 $1 \in V_0$ があって, $Y(1,z) = 1_V$ と $v_n 1 = 0 \quad (n \geq 0)$ と $v_{-1}1 = v$ が成り立つ.

可換以外の条件はこれから説明する構成法では, 成り立つことの証明が簡単なので, 可換.

$$(z_1 - z_2)^n a(z_1)b(z_2) = (z_2 - z_1)^n b(z_2)a(z_1)$$

にもみ注目します.

これから, 上の定義の拡張を考えます. 昨年, Mossberg は頂点作用素代数の拡張を定義し, 独立に Dong と Lepowsky は一般化された頂点作用素代数の定義を与えました. [Mo], [DL]. 通常の頂点作用素代数とこれらの違いは, 頂点作用素代数が偶格子に対応し, 一般化された頂点作用素代数が通常の格子に対応しているようなものと考えることができるかもしれません. 我々の構成法は直交基底を使って偶格子を表示する事に似ており, この直交基底の部分に一般化された頂点作用素代数 (group-skew 頂点作用素代数) を使おうと考えています.

group-skew 頂点作用素代数の定義を導入しましょう. これは Mossberg の定義の一部であり, また, 一般化された頂点作用素代数の一部でもあります. 彼らの定義は group-skew 頂点作用素代数の定義と群の拡大の組合せと考えることができますが, 群の拡大部分は変形するのが難しいので, これを切り離して考えたのが, 我々の構成法のアイデアです. 群の拡大は最後の段階で使います.

A を $\mathbb{R}/2\mathbb{Z}$-値内積 $\langle a,b\rangle$ を持つアーベル群します. しばしば, 法 $2\mathbb{Z}$ で考えたとき, $\langle a,b\rangle$ と合同であるような十分大きな実数を表わすのにも $\langle a,b\rangle$ を使うことにします.

定義　A-skew 頂点作用素代数とは $\mathbb{Z} \times A$-次数付ベクトル空間

$$V = \oplus_{\alpha \in A} V^\alpha = \oplus_{\alpha \in A} (\prod_{i=0}^{\infty} V_i^\alpha)$$

で, $\dim \oplus_{\alpha \in A} V_i^\alpha < \infty$ であり, 各元 $v \in V$ に対して, 頂点作用素

$$Y(v,z) = \sum_{n \in \mathbb{R}} v_n z^{-n-1}$$

が定義され, それは A-skew 可換性: 即ち,
十分大きな実数 $\langle \alpha, \beta \rangle$ があって

1　$$(z_1 - z_2)^{\langle \alpha,\beta \rangle} Y(a,z_1)Y(b,z_2) = (z_2 - z_1)^{\langle \alpha,\beta \rangle} Y(b,z_2)Y(a,z_1)$$

が成り立ち，作用と A の次数が可換である．即ち，

2 $$Y(a,z)b=\sum_{n\in(\alpha,\beta)+\mathbb{Z}}a_nb\in V^{\alpha+\beta}z^{(\alpha,\beta)}[[z]][z^{-1}]$$

が成り立つ．ここで $a\in V^\alpha, b\in V^\beta$ とする．

また，ヴィラソロ元や真空など頂点作用素代数の他の条件はすべて成り立つ．

重要な例として，正定値格子 L から group-skew 頂点作用素代数 $\tilde{V}_L$ を構成できます．これの構成の仕方は Frenkel, Lepowsky, Meuman の本の 4 章を参照してください．

Theorem 2.1 (FLM, Theoreom 4.3) $\tilde{V}_L$ は内積 $\langle,\rangle+2\mathbb{Z}$ で定義される *L-skew* 頂点作用素代数 である．

Let $L^*=\{v\in\mathbb{Q}\otimes L:\langle v,w\rangle\in2\mathbb{Z}\text{ for all }w\in L\}$ と置くと，上記の $\tilde{V}_L$ は $L/(2L^*\cap L)$-skew 頂点作用素代数でもあります。ここでの内積は $\langle,\rangle \pmod{2\mathbb{Z}}$ で定義します。

例えば、$\langle v,v\rangle=1$ とすると、$\tilde{V}_{\mathbb{Z}v}$ は $\mathbb{Z}/2\mathbb{Z}$-skew 頂点作用素代数です。ここで内積は $(\bar{\alpha},\bar{\beta})=\langle\alpha,\beta\rangle+2\mathbb{Z}\in\mathbb{Z}/2\mathbb{Z}$ で与えます。また、$\langle v,v\rangle=1/2$ なら、$\tilde{V}_{\mathbb{Z}v}$ は $\mathbb{Z}/4\mathbb{Z}$-skew 頂点作用素代数で、内積は $(\bar{\alpha},\bar{\beta})=2\langle\alpha,\beta\rangle+2\mathbb{Z}\in\mathbb{Z}/2\mathbb{Z}$ です。

3 テンソル積構成

この章で，頂点作用素の構成法を紹介します．その前に，group-skew 頂点作用素代数のテンソル積を定義しましょう．A_iを内積 $\langle,\rangle_i$ を持つアーベル群とし，$(V^1,Y^1),...,(V^n,Y^n)$ を A_i-skew 頂点作用素代数とします．まず，テンソル積空間 $V=\otimes V^i$ を定義します．次に，各 $v^i\in V^i$ に対して，$\otimes v^i\in\otimes V^i$ の頂点作用素を $Y(\otimes v^i,z)=\prod Y^i(v^i,z)$ で定義し，これを全空間$\otimes V^i$に線形に拡張します．

これは定義可能であり，容易に，これは内積 $\langle\sum\alpha_i,\sum\beta_i\rangle=\sum\langle\alpha_i,\beta_i\rangle$ で定義される内積を持つ $A_1\oplus...\oplus A_n$-skew 頂点作用素代数でとなります．

我々が構成しようとしている頂点作用素代数は上の group-skew 頂点作用素代数の適切な条件を満たす部分代数の群の拡大による変形です．$\oplus A_i$ の部分集合 S に対して，

$$V_S=\sum_{(\alpha_1,...,\alpha_n)\in S}(V^1)^{\alpha_1}\otimes...\otimes(V^n)^{\alpha_n}$$

と置くことにします．例えば，V_S が頂点作用素代数であるためには，次の 2 条件が必要十分です．

(1) V_S は V_S の中の元の頂点作用素の作用で閉じており，

(2) V_S の中の頂点作用素が互いに可換となる．

最初の条件は S が和で閉じていることと同じであることがわかります．次に V_S が2番目の条件より弱い条件を満足していても，群の拡大を使って頂点作用素が互いに可換とできることを示しましょう．

即ち，S が次の条件を考えましょう．

(2.2) S は和で閉じている

(2.1) S の全ての元 s が $\langle s,s\rangle$ を満たす．

この時，頂点作用素代数 $\tilde{V}_S$ を以下のようにして構成します．

まず、S の± 1 による中心拡大を$\pm e^S$ とし、積を $e^t e^s = (-1)^{(t,s)} e^s e^t$ for $s,t \in S$ で定義します。さらに、V^s に e^s のテンソルした空間$\tilde{V}^s = V^s \otimes e^s$の直和 $\tilde{V} = \oplus \tilde{V}^s$ をフォック空間と考え、その元 $v \otimes e^s$ の頂点作用素を$\tilde{Y}(v \otimes e^s, z) = Y(v,z) \otimes e^s$ で定義し，線形で拡張します。この時、$\tilde{Y}(v \otimes e^s, z)$ は互いに可換となることがわかります．

Theorem 3.1 $(\tilde{V}, \tilde{Y})$ は V^S と同じ指標を持つ頂点作用素代数である。

(2.1) と (2.2) は S が $\sum A^i$ の偶数値線形コードであることを言っています。

この構成法は複雑ではないので，$\tilde{V}$ の指標が V^S の指標と同じであり、V^S の指標は S の weight enumerator から容易に計算できることが分かります．

4 Examples

4.1 中心電価$\frac{1}{2}$のヴィラソロ代数

この部分節はすべて [M2] の結果を引用したものです。

まず、$\mathbb{Z}/2\mathbb{Z}$-skew 頂点作用素代数 (頂点作用素超代数)

$$M = M^0 \oplus M^1 = L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2}),$$

を見つけることができます。ここで内積は $\langle m,n\rangle = mn$ で与えられているとします。

まず、M の n 個のテンソル積 $\otimes M$ を構成します。$v^i \in M^{|v^i|}$ に対して、$Y(\otimes v^i, z) \sim Y(\otimes w^i, z)$ である必要十分条件は$\sum |v^i||w^i|$ が偶数であることがわかります。特に、任意の長さ偶数のコードワード $c = (c_1, ..., c_n)$ に対しては、$\otimes M^c$ の2元 v, w は $Y(v,z) \sim Y(w,z)$ を満足します。

Theorem 4.1 もし C が偶線形2次コードなら，$\tilde{M}_C$ は頂点作用素代数である．特に，もし C が長さ2のコードワードを持たないなら，$\tilde{M}_C$ の全自己同型群は有限である．

4.2 $\mathbb{Z}/4\mathbb{Z}$-skew 頂点作用素代数

$L = \mathbb{Z}v$を内積 $\langle v, v\rangle = \frac{1}{2}$をもつ一次元格子とする。この時、$\tilde{V}_L$ は $\mathbb{Z}/4$-skew 頂点作用素代数

$$\tilde{V}_L = V^0 + V^{\frac{1}{2}} + V^1 + V^{\frac{3}{2}}$$

となります。ここで、$V^k = \prod_{n\in\mathbb{Z}} S(H_{\mathbb{Z}}^-)e^{2nv+kv}$ 、内積は $\langle k, h\rangle = 2hk$ で与えます。V^0+V^1 は頂点作用素代数であり、$V^{\frac{1}{2}} + V^{\frac{3}{2}}$ がそれの既約加群であることが容易にわかります。

それゆえ、

Theorem 4.2 もし、S を偶数値 $\mathbb{Z}/4\mathbb{Z}$-コードとすると、テンソル積構成によって、頂点作用素代数 $\tilde{V}_S$ を構成できる。

5 Broué-Enguehard 写像

1972年に Broué-Enguehard は self-dual doubly 偶2次コードの weight enumerators からモジュラー形式の空間への写像を定義しました。

この写像を頂点作用素代数の立場から説明してみましょう。先の章の2番目の例を使って，次の定理を得ます.

Theorem 5.1 Cを *self-centralized* コードで、コードワードの長さがすべて4の倍数となるものとする。この時、それを $0 \to \{0,2\}$ と $1 \to \{1,3\}$ によって、$\mathbb{Z}/4\mathbb{Z}$-コードに埋め込むことによって、偶数値 $\mathbb{Z}/4\mathbb{Z}$-コード$\tilde{C}$を構成し、テンソル積構成によって頂点作用素代数$\tilde{V}_{\tilde{C}}$ を構成することができる。もし、$C = C^{\perp}$, なら、$\tilde{V}_{\tilde{C}}$ の指標

$$\mathrm{ch}V_C(z) = e^{-2\pi i\frac{n}{24}z}\sum \dim(V_C)_n e^{2\pi i n z}$$

はモジュラー関数となる。

特に、写像 $C \to \mathrm{ch}V_C(z)\prod_{i=1}^{\infty}(1-q^i)^n$ は Broué-Enguehard 写像と一致しています。

証明の概略を説明しましょう. Jacobi theta functions の定義を引用すると,

$$\theta_2(\tau, z) = \textstyle\sum_{n\in\mathbb{Z}} e^{\pi i(n+\frac{1}{2})^2\tau+(2n+1)\pi iz} \quad and$$
$$\theta_3(\tau, z) = \textstyle\sum_{n\in\mathbb{Z}} e^{\pi in^2\tau+2n\pi iz}.$$

です. C を長さ n の2次コードとし, weight enumerator

$$\sum_{c\in C} x^{n-|c|}y^{|c|} \in \mathbb{C}[x, y]$$

を考えます.

Broué-Enguehard 写像は

$$\Phi : f(x, y) \in \mathbb{C}[x, y] \longrightarrow f(\theta_3(2\tau, 0), \theta_2(2\tau, 0)).$$

で与えられており，

$$\theta_3(2\tau,0)=\sum_{n\in\mathbb{Z}}e^{2\pi i n^2\tau}\qquad and$$
$$\theta_2(2\tau,0)=\sum_{n\in\mathbb{Z}}e^{2\pi i(n+\frac{1}{2})^2\tau}$$

はそれぞれ、格子 $L=\mathbb{Z}2v$ と $M=\mathbb{Z}v-\mathbb{Z}2v$の θ-関数であり，$\prod_{i=1}^{\infty}(1-q^i)$ 倍が頂点作用素代数 $\tilde{V}_L$ と既約加群 $\tilde{V}_M$ の指標となります．ここで、$<v,v>=\frac{1}{2}$ です．この時，Broué-Enguehard 写像がテンソル積構成と対応していることが分かると思います．

5.1 モジュラー形式

$SL_2(\mathbb{Z})$ の作用を説明しておきましょう．

Sと T で $S=\begin{pmatrix}0&1\\-1&0\end{pmatrix}, T=\begin{pmatrix}1&1\\0&1\end{pmatrix}$ を表すことにします．S と T は $z\to -1/z$ と $z\to z+1$ によってそれぞれ上半平面に作用しており，これらの作用によって、S と T は $\mathbb{C}v_1+\mathbb{C}v_2$ 上にそれぞれ、$A=\begin{pmatrix}1&1\\1&-1\end{pmatrix}$ と $B=\begin{pmatrix}1&0\\0&i\end{pmatrix}$ として作用しています。直接の計算することによって、$(AB)^3=\frac{1+i}{\sqrt{2}}I$ であり、$<A,B>$ は位数 192 の群であることが分かります。一方 $(ST)^3=1$ なので、$\frac{1+i}{\sqrt{2}}I$ は S,T が作用しているところに自明に作用していると考えて良いことになります。

コードワード $c=(c_i)$ に対して、$v^c=\otimes_j v(1-2c_j)$ と置き、コード C に対して、$v^C=\sum_{c\in C}v^c$ と表すことにします．もし、c の長さが 4 で割れるなら、v^c は Bで不変であり、もし、$|c|=2+4n$ なら、$Bv^c=-v^c$ であることが分かります。一方 A の作用は

$$Av^c=\frac{1}{2^{n/2}}\sum_{d\in\mathbb{Z}_2^n}(-1)^{<c,d>}v^d$$

です。これを使うと，

Lemma 5.1 もし、C が $\mathbb{Z}_2^n$ の部分空間なら、

$$A(v^C)=\frac{1}{2^{n/2}}|C|v^{C^\perp}.$$

である。

特に、もし、C が selfcentralizer なら、$Av^C=v^C$ となり、良く知られた結果を得ます。

Theorem 5.2 もし、C が *doubly even selfcentralizer* なら、$W_C(v_1,v_2)$ は $<A,B>$-不変である。

上の定理が Broué-Engruehard 写像を意味しているのです．Broué-Engruehard 写像は全射ではありません．モジュラー形式の空間は $\mathbb{C}[E_8,E_8]$ と同型ですが，E_8 は像に入っていません．最近，小関氏が weight enumerator の概念を拡張した Jacobi 多項式を定義し，この空間からは Broué-Engruehard 写像がモジュラー形式の空間へ同型に移すことを示し

ました．例えば，$e_{12} = X^{12} - 33X^8Y^4 - 33X^4Y^8 + Y^{12}$ は Jacobi 多項式で $\Phi(e_{12}) = E_6$ となります．

これも group-twist 頂点作用素代数の言葉で表わせることを紹介しておきましょう．

ここでは doubly even ではなく，single even selfcentralizer C を考えてみます。この場合、$V_{\mathbb{Z}v}$ $(\langle v, v\rangle = \frac{1}{2})$ から $\mathbb{Z}/4\mathbb{Z}$-コードによってテンソル積構成によって構成されるのは頂点作用素代数ではなく、group-skew 頂点作用素代数となります．

E_6 を構成しようとするとき，6次元で次元が4の倍数ではないので，$\Delta = \prod_{i=1}^{\infty}(1-q^i)$ の性質から，weight enumerator に対応するものは A, B-不変のものとは異なります．実際には weight enumerator が B-不変であって，A によって -1 倍されるものが必要になります．それゆえ，A の作用を考えると，Δ の部分がでてきて，$\mathrm{ch}V_C - |C|/2^6\mathrm{ch}V_{C^\perp}$ が A 不変となります．

それでは構成してみましょう．C_4 を $\mathbb{Z}_2^8$ の中の doubly even self-centralized コードとし，これを $\mathbb{Z}_2^{12} = \mathbb{Z}_2^8 \oplus \mathbb{Z}_2^4$ の中に埋めこんで考えます．$\mathbb{Z}_2^4$ の中から長さ4の元と0を取ってきて，添加して出来る線形コード C は5次元の偶コードです．さらに，$C^\perp$ も偶コードとなります．一方 D を偶数長さのコードワード全体からなるコードとします．この時，D も $D^\perp$ も偶コードで，それぞれ11次元と1次元です．それぞれのコードから構成した group-skew 頂点作用素代数を V_C，$V_{C^\perp}$，V_D，$V_{D^\perp}$ と置くと，

$$E_6 = \prod_{i=1}^{\infty}(1-q^i)^6\left(\frac{11}{20}(2\mathrm{ch}V_C - \mathrm{ch}V_{C^\perp}) - \frac{1}{20}(\mathrm{ch}V_D - 32\mathrm{ch}V_{D^\perp})\right)$$

が成り立ちます．

$2\mathrm{ch}V_C - \mathrm{ch}V_{C^\perp}$, $\mathrm{ch}V_D - 32\mathrm{ch}V_{D^\perp}$は，ともに，$q^{\frac{1}{2}}$ の巾の形式的巾級数であって，B によって $q^{\frac{n}{2}} \to (-1)^n q^{\frac{n}{2}}$ に移り，A によって不変となるものです．

6 Montague's 観察

この節ではテンソル積構成を通して Montague 気付いた orbifold 構成と格子のコードからのツイスト構成における一致の説明をしましょう。

L を先節と同じものとし、$\theta : L \to L$ を$\theta(\alpha) = -\alpha$ で定義される自己同型とします。このとき、$V^0 + V^2$ の固定空間 $(V^0 + V^2)^\theta$ は基底

$$e^v + e^{-v}; v(-1)(e^v - e^{-v}), v(-1)^2; ...$$

を持っていることが簡単に分かります。$e^v + e^{-v}$ は primary weight one をもっており、$v(-1)$ によって生成されたものと同型の部分代数を生成するので、$(V^0 + V^2)^\theta$ が

$$v(-1); v(-2), v(-1)^2, ;, ; e^{2v}, e^{2v},$$

に同型であることを見るのは難しくありません。即ち、$V_{2\mathbb{Z}v}$ と同型なのです。Dong の結果より、$V_{2\mathbb{Z}v}$ は丁度8個の既約加群を持ち、それらの直和は

$$V_{\frac{1}{4}\mathbb{Z}v},$$

と一致します。これは $\mathbb{Z}/8$-skew 頂点作用素代数です。

それ故、もし、V が V_L と $\mathbb{Z}/4\mathbb{Z}$-コード S からテンソル積構成によって構成された頂点作用素代数なら、V^θ は V_{2L} と $\mathbb{Z}/8\mathbb{Z}$-コード S' からテンソル積構成によって構成された頂点作用素代数と同じものです。ここで S' は S を埋めこんで構成したコードです.

すなわち、Monstague's orbifold 構成はこの場合には, a self-centralized $\mathbb{Z}/4$ 線形コードから self-centralized $\mathbb{Z}/8$-コードへの対応にすぎません.

特に、もし、正則偶格子が偶数値コードから構成されているのなら、上の対応は self-centralized binary code から self-centralized $\mathbb{Z}/4$-code への対応となっています。

References

[B1] R. E. Borcherds, Vertex algebra, Kac-Moody algebra, and the Monster, *Proc. Natl. Acad. Sci. USA* **83** (1986), 3068-3071.

[BE] M. Broué and M. Enguehard, Polynomes des poids de certains codes et fonctions theta de certains reseaux, Ann. Sci. Ecole Norm. Sup. 5 (1972), 157–181.

[BMO] E. Bannai, S. Minashima, and M. Ozeki, On Jacobi forms of weight 4, Kyoshu J. Math. (to appear).

[BO] E. Bannai and M. Ozeki, Construction of Jacobi forms from certain polynomials, (preprint).

[CN] J. H. Conway and S. P. Norton, Monstrous moonshine, *Bull. London Math. Soc.* 11 (1979), 308-339.

[DL] C. Dong and J. Lepowsky, Generalized Vertex Algebras and Relative Vertex Operators, *Progress in Math.* Vol. 112, Birkhäuser, Boston, 1993.

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

[M1] M. Miyamoto, Griess algebras and conformal vectors in VOAs *J. Algebra*, to appear.

[M2] M. Miyamoto, Binary codes and vertex operator (super)algebras, *J. Algebra*, to appear.

[Mo] G. Mossberg, Axiomatic vertex algebras and the Jacobi identity, J. Algebra 170, (1994) 956-1010.

[O] M. Ozeki, On the notion of Jacobi polynomials for codes, to appear in Math. Proc. Cambridge Phil. Soc..

Remarks on Topics Connected with Graphs and Groups

Michio Suzuki

§1 **Introduction** A graph Γ is said to *represent* a group G if $Aut\,\Gamma \cong G$. This note presents some new results concerning representations of groups, or a particular group, by a special class of graphs, and some remarks on interrelation between graphs and groups. An intuitive notion of graphs is sufficient for our purpose. Thus, a graph Γ consists of a pair of sets (V,E) such that V is the set of *vertices* and E is the set of *edges*; each edge being represented by a line connecting two vertices. We use the notation

$$V = vert\,\Gamma \quad \text{and} \quad E = edge\,\Gamma.$$

If an edge e is represented by a line connecting two vertices x and y, we say that the vertex x (as well as y) is *incident* with the edge e. Sometimes, we consider a *colored graph* when each edge is given a color. If Γ is a colored graph, $Aut\,\Gamma$ is the set of automorphisms of Γ which preserve the color of each edge. If Δ is a colored graph, we mean by *the underlying graph* the graph Γ obtained from Δ by erasing the colors from all edges of Δ. A graph is said to be *simple* if there is no loop or multiple edge. Thus, in a simple graph, each edge is determined by the end vertices; we may write an edge $e = (x,y)$ with $x \neq y$ where x and y are vertices incident with the edge e.

§2 **Representation by Pictures** A colored graph Δ is said to be a *picture* if each vertex is incident with exactly one edge of each color. The Cayley graph of a group with respect to a generating set is not a picture since each vertex is incident with two edges of each color, one going out and one coming in. However, *if each generator has order 2, we can modify the Cayley graph to make a picture.* Thus, if a group G is generated by a set consisting of elements of order 2, then G is represented by a picture P and, in this case, G acts transitively on the set $vert\,P$. In 1990, Behrendt [1] proved that every finite group can be represented by a picture. We can prove the following theorem.

Theorem 1 *Let m be an integer ≥ 3. Then, any finitely generated group G can be represented by a picture P of m colors such that the underlying graph Γ of P is a simple graph.*

We have constructed in [9] a picture P_3 of 3 colors that represents G. The underlying graph of P_3 is (by construction in [9]) seen to be a simple graph. The method of Sabidussi [6,7] constructs pictures of more colors that still represent G.

It should be remarked that if P is a picture of r colors, we can construct a picture Q of $r+1$ colors from P by just splitting each of the edges of the fixed color c into two edges of colors c and c' where c' is a color different from any colors of the edges of P. If P represents a group G, so does Q. Thus, without the restriction that the underlying graph of the picture P is simple, Theorem 1 is rather trivial.

§3 **Representation by a graph with given nuclear number** The *nuclear number* of a graph Γ is the maximal order of subgraphs which are complete graphs. Montenegro [5] has proved that any finite group can be represented by graphs with arbitrary large nuclear numbers greater than 3. We can prove the following theorem.

Theorem 2 *Let m be an integer greater than 3. Then, any finitely generated group G can be represented by a simple graph Γ of valency m with nuclear number m.*

This answers a question posed in [9]. To prove Theorem 2, we use another method of Sabidussi [6]. Let Γ be a graph of valency m with $m \geq 3$, *i.e.* each vertex of Γ is incident with exactly m edges. We construct a graph Γ^* where

$$vert\ \Gamma^* = \{\ (e,x) \mid e \in edge\ \Gamma,\ x \in vert\ \Gamma\ \}$$

and $((e,x),(e',x')) \in edge\ \Gamma^*$ if and only if either $e = e'$ and $x \neq x'$, or $e \neq e'$ and $x = x'$. It is clear that the graph Γ^* is of valency m and nuclear number m. In a sense, we can reconstruct Γ from Γ^*. Let $\Gamma^\wedge$ be the graph defined as follows. Vertices of $\Gamma^\wedge$ are maximal cliques of order m in Γ^*. Two maximal cliques c and d of order m are joined by an edge in $\Gamma^\wedge$ if and only if there is an edge $e = (x,y)$ of Γ such that $(e,x) \in c$ and $(e,y) \in d$. Then, for an edge (c,d) of $\Gamma^\wedge$, the map

$$(c,d) \longrightarrow e \quad \text{and} \quad c \longrightarrow x$$

is well defined and is an isomorphism of $\Gamma^\wedge$ onto Γ. Thus, if the graph Γ represents a group G, so does Γ^*. □

Remark If G is a finite group, there are in fact infinitely many nonisomorphic graphs (or pictures) of a fixed valency m which represent G in both Theorems 1 and 2. The same remark would hold for infinite groups as well, but I do not have a proof.

§4 **Representation by PCS pictures** In a recent paper [4], Marcelo, Ruiz and Shinoda have considered representations of a finite group by some PCS pictures. A *PCS picture* is a picture P with the following two properties:

(1) the group $Aut\ P$ is transitive on the set $vert\ P$, and
(2) there is a subgroup of the automorphism group of the underlying graph Γ of P which induces transitive action on the set of colors.

To paraphrase the second condition, we introduce some notation. For an edge e of a picture P, let $c(e)$ denote the color of the edge e, and let $\mathscr{C}$ be the set of colors of P. The second condition (2) means that there is a subgroup H of $Aut\ \Gamma$ having the two properties:
(a) if $\sigma \in H$ and $c(e) = c(f)$ for $e,f \in edge\ P$, then $c(\sigma(e)) = c(\sigma(f))$, *i.e.* the images $\sigma(e)$ and $\sigma(f)$ have the same color; and
(b) for any $c \in \mathscr{C}$, and $e \in edge\ P$, there is an element $\sigma \in H$ with $c(\sigma(e)) = c$.

Put $G = Aut\ P$ and let G^{pc} be the subgroup of $Aut\ \Gamma$ consisting of all the automorphisms which satisfy the condition *(a)*. If $\sigma \in G^{pc}$, σ induces a permutation $\pi(\sigma)$ of the colors of P. Clearly, the map $\pi: G^{pc} \longrightarrow Sym(\mathscr{C})$ is a homomorphism of groups and G is the kernel of π. Thus, $G \lhd G^{pc}$. The condition *(b)* is equivalent to saying G^{pc} acts transitively on the set $\mathscr{C}$ of colors.

Assume that P is a PCS picture with the underlying graph Γ *connected* (and simple). Let v_0 be a vertex of Γ which will be fixed for the discussion. Let H be the stabilizer of v_0. We will prove that G^{pc} *is a semidirect product of* $G = Aut\ P$ *and* H.

By assumption, G acts transitively on $vert\ \Gamma$. Hence, for any $v \in vert\ \Gamma$, there is an element $x \in G$ such that $v = xv_0$. If $s \in G^{pc}$, we have $sv_0 = xv_0$ with $x \in G$. Then, we have $x^{-1}s \in H$, so $s = xh$ with some $h \in H$. This proves that $G^{pc} = GH$.

If $r \in G \cap H$, r fixes v_0 and all the vertices adjacent to v_0 because each of them is connected to v_0 by some edge that is the unique edge of its color incident with v_0. Thus, r fixes all the vertices of the connected component of v_0. Since Γ is connected, r fixes all the vertices of P. Since $s \in G$ does not change the color of the edges, we have $s = 1$. Thus, $G \cap H = \{1\}$ and G^{pc} is a semidirect product of H and a normal subgroup G.

The above argument shows that G is simply transitive on the set $vert\,\Gamma$. We can identify P as the (modified) Cayley graph with a set of involutive generators which corresponds bijectively to the set of colors of P (cf. [4]).

We note that, in the above set–up, the action of H is given as follows. If $v \in vert\,\Gamma$ is written $v = xv_0$ with unique $x \in G$, then $s \in H$ sends $v \longrightarrow sv = yv_0$ $(y \in G)$ where $y = sxs^{-1}$. Thus, if the set $vert\,\Gamma$ is identified with the set G via $v = xv_0 \longrightarrow x$, then the action of H is given by conjugation in G^{pc}.

Remark If G is a nonabelian finite simple group, there are PCS pictures which represent G (cf. [4]). In fact, there are many. Let M be a maximal subgroup of G. Since G is generated by involutions, there is an involution t not contained in M so $G = < M,t >$. Let $T = \{mtm^{-1} \mid m \in M\}$. The subgroup $< T >$ generated by T is normalized by M and t. Hence, it is a normal subgroup of G. Since G is simple, we have $G = < T >$. The (modified) Cayley graph associated with the generating set T is a PCS picture that represents G. In this case, the permutation group on colors includes the group M.

§5 Characterization of Groups Having Representation by PCS Pictures of 3 Colors We need the following definition. A group G^* is said to be *(2,3) generated* if G^* is generated by two elements of orders 2 and 3, *i.e.* $G^* = < s,t >$ with $s^3 = t^2 = 1$. Thus, G^* is a homomorphic image of $PSL(2,\mathbb{Z})$ which is known to be the free product of two cyclic groups of orders 2 and 3. A *(2,3)* generated group may or may not have a normal subgroup of index 3. If it may, there is a unique one. This is because, if $G^* = < s,t >$ with $s^3 = t^2 = 1$, a normal subgroup of index 3 must be the normal subgroup generated by the conjugates of the element t. We have the following theorem.

Theorem 3 *Let G be a group. The group G has a representation by a PCS picture of 3 colors with the underlying graph connected if and only if G is isomorphic to the normal subgroup of index 3 in a (2,3) generated group.*

Proof If a group G is represented by a PCS picture of 3 colors with the underlying graph connected, then G is generated by 3 involutions t_1, t_2, and t_3. In the notation of §4, the subgroup H of G^{pc} is a transitive subgroup of the symmetric group S_3 on 3 colors. Thus, H contains an element s of order 3. We have seen in §4 that the element s permutes the involutions t_i, *i.e.* we may assume $st_is^{-1} = t_{i+1}$ with $t_4 = t_1$. Thus, if $t = t_1$, the group $G^* = < G,s >$ is generated by s and t; hence, G^* is *(2,3)* generated and G is a normal subgroup of index 3 in G^*.

Conversely, suppose that G is a normal subgroup of index 3 of a *(2,3)* generated group $G^* = < s,t >$ with $s^3 = t^2 = 1$. Then, $G = < t_1,t_2,t_3 >$ with $t_1 = t$ and $t_{i+1} = st_is^{-1}$ for $i = 1, 2$. The (modified) Cayley graph P relative to the generating set $\{t_1,t_2,t_3\}$ is a picture of 3 colors with the underlying graph connected. It represents the group G. Since the element s permutes the generators $\{t_i\}$, P is a PCS picture of three colors. □

Corollary 4 *If G is a (2,3) generated group that has no normal subgroup of index 3, then G has a PCS picture representation of 3 colors. In particular, a nonabelian simple group that is (2,3) generated has a PCS picture representation of 3 colors.*

Proof Let $G = \langle s_1, t_1 \rangle$ with $s_1^3 = t_1^2 = 1$. Let $t_2 = s_1 t_1 s_1^{-1}$ and $t_3 = s_1 t_2 s_1^{-1}$. We prove that $G = \langle t_1, t_2, t_3 \rangle$. If we write $N = \langle t_1, t_2, t_3 \rangle$, then both s_1 and t_1 normalize N. Hence, N is a normal subgroup of G. Since $t_1 \in N$, the factor group G/N is generated by a single element s_1. Since G contains no normal subgroup of index 3, we have $G = N$. This proves our claim.

Let C be the cyclic group of order 3 generated by an element r, and let $G^* = G \times C$ be the direct product of G and C. We will prove that G^* is $(2,3)$ generated. Set $s = rs_1$. Then, $s^3 = r^3 s_1^3 = 1$ since r commutes with s_1. We have $st_1s^{-1} = s_1 t_i s_1^{-1} = t_{i+1}$ with $t_4 = t_1$. Hence, the subgroup $\langle s, t_1 \rangle$ of G^* contains t_1, t_2, and t_3. Thus, it contains $G = \langle t_1, t_2, t_3 \rangle$. It follows that $s_1 \in G \subset \langle s, t_1 \rangle$. Since $s = rs_1$, we have $r \in \langle s, t_1 \rangle$. This implies that $\langle s, t_1 \rangle$ contains G and s; thus, $G^* = \langle s, t_1 \rangle$ is $(2,3)$ generated and G is a normal subgroup of index 3 of G^*. By Theorem 3, G is represented by a PCS picture of 3 colors. □

Remarks After a long line of investigations by many mathematicians, Shalev [8] has recently proved that most classical simple groups of Lie type except $PS_p(4, 2^m)$ are $(2,3)$ generated. Thus, they are represented by a PCS picture of 3 colors. There are exceptions like A_6, the alternating group on 6 letters, as A_6 has no outer automorphism of order 3 and A_6 is not $(2,3)$ generated. Some simple groups which are not $(2,3)$ generated may be represented by PCS pictures of 3 colors. For example, $Sz(8)$ is certainly not $(2,3)$ generated, but $Aut\ Sz(8)$ is. This is proved by a counting argument. In any case, $Sz(8)$ is represented by a PCS picture of 3 colors by Theorem 3. But, $Sz(2^m)$ with $(m,3) = 1$ is not represented by any PCS picture of 3 colors by the same reason as A_6.

On the other hand, any finite nonabelian simple group except $U_3(3)$ is known to be generated by 3 involutions (Malle–Saxl–Weigel [3]). Hence, any finite nonabelian simple group G except $U_3(3)$ is represented by a picture of 3 colors with G acting transitively on the set of vertices.

§6 **A Question** There are many problems concerning the relationship between graphs and groups; some of them are discussed in [9]. I will mention here just one such problem which might be of some interest.

The *prime graph* $\Gamma(G)$ of a finite group is defined as follows: the set of vertices of $\Gamma(G)$ is the set $\pi(G)$ of prime divisors of the order $|G|$ of G, and two vertices p and q are joined by an edge of $\Gamma(G)$ if and only if $p \neq q$ and G contains an element of order pq. A basic theorem is due to Williams (in [10]): *if a simple group G has a disconnected prime graph, G contains an isolated subgroup.* (A subgroup H of G is said to be *isolated* if $\{1\} \neq H \neq G$ and if $1 \neq x \in H$, then the centralizer of the element x is contained in H.) The proof of this theorem requires an application of the classification of finite simple groups (CFSG). Assume that the prime graph of the group G is not connected and let π be a connected component consisting of odd prime numbers. If there is a π–local subgroup of even order, *i.e.* if there is a π–subgroup $P \neq \{1\}$ such that the normalizer of P is of even order, it is easy to prove the Williams' theorem without using CFSG. The classic lemma due to Burnside is sufficient. To prove the Williams' theorem we may assume that all π–local subgroups are of odd order. *The question is whether it is possible to apply the methods, either the original one of Feit–Thompson or the recent improved version due to Bender–Glauberman [2], to prove the result without invoking the full power of the CFSG.* The paper by Feit–Thompson or [2] is written in such a way that the proof applies only to the minimal counterexample to obtain a contradiction; but it seems to me that their marvelous method will have some positive consequences in other situations. It is hoped that their method might be applicable here.

References

[1] Behrendt G. Automorphism groups of pictures, J. Graph Theory 14 (1990) 423–426

[2] Bender H. and Glauberman G. Local Analysis for the Odd Order Theorem, London Math. Soc. Lecture Note Series 188 (1994) pp.174

[3] Malle G., Saxl J., and Weigel T. S. Generation of classical groups, Geom. Dedicata 49 (1994) 85–116

[4] Marcelo R.M., Ruiz M–J. P., and Shinoda K. On automorphism groups of some PCS graphs, Graphs Combin. 10 (1994) 185–191

[5] Montenegro E. Graphs with given automorphism group and given nuclear number, Proyeccions 11 (1992) 21–28

[6] Sabidussi G. Graphs with given group and given graph–theoretical properties, Canadian J. Math. 9 (1957) 515–525

[7] Sabidussi G. Graph multiplication, Math. Z. 72 (1959/60) 446–457

[8] Shalev A. A (2,3) generation of classical simple groups (To appear)

[9] Suzuki M. Graphs, Geometries, and Groups, Proc. Intern. Conf. on Algebraic Combinatorics at Manila, 1994 (To appear)

[10] Williams J. S. Prime Graph Components of Finite Groups, J. Algebra 69 (1981) 487–513

Department of Mathematics
University of Illinois at Urbana–Champaign
1409 West Green Street
Urbana, IL 61801
suzuki@symcom.math.uiuc.edu

符号理論と Unitary Reflection Groups の不変式環との関連について

小関 道夫 (山形大・理)

30 July 1995

1 Introduction

本講演では次のテーマに基づいて話します。

Thesis (or Hypothesis) :

" finite unitary groups generated by reflections (略して u.g.g.r) あるいは それらに近接した群のうちで、 coding theoretic interpretation を持つものは (そしてそれらのみが?) modular form theory との関連がつく。"

このことは、すぐには立証できる性格のものではない。その代わりに、いくつかの傍証 (evidence) を挙げて説明したい。

また、それに関連して、いくつかの問題を途中で述べる。

U.g.g.r の基本文献としては、
G.C.Shephard and J.A. Todd, Finite unitary reflection groups, Can. J. Math. 6 (1954), 274-304
A.M. Cohen, Finite complex reflection groups, Ann. Sci. Ecole Norm. Sup. 9 (1976), 379-436
を挙げておく。

2 Some Definitions

本節では、後の議論で必要な最小限の用語、概念を導入する。また、さらに後の議論で必要なものはその都度追加定義する。

$\mathbf{F}_q = GF(q)$: q 個の元より成る有限体.

$V_n = \mathbf{F}_q^n$ を $\mathbf{F}_q$ 上の n 次元のヴェクトル空間とする。V_n の k 次元部分ヴェクトル空間 C を $\mathbf{F}_q$ 上の線形 $[n,k]$ 符号という。

$$\begin{aligned} V \ni \mathbf{x} &= (x_1, x_2, \cdots, x_n) \\ \mathbf{y} &= (y_1, y_2, \cdots, y_n) \end{aligned}$$

に対して、内積 $(\mathbf{x},\mathbf{y})$ が

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

により定義される。

$$C^{\perp} = \{\mathbf{z} \in | \ (\mathbf{z},\mathbf{u}) = 0 \ \forall \mathbf{u} \in C\}$$

を C の双対符号という。$\mathbf{x} = (x_1, x_2, \cdots, x_n) \in V$ の Hamming weight $wt(\mathbf{x})$ は

$$wt(\mathbf{x}) = \sharp\{i \mid x_i \neq 0\}$$

により定義される。x, y を独立な変数とするとき、

$$W_C(x,y) = \sum_{\mathbf{u} \in C} x^{n-wt(\mathbf{u})} y^{wt(\mathbf{u})}$$

を符号 C の Hamming weight enumerator という。
さらに、q が odd prime power のときには、C の Lee weight enumerator が

次のように定義される。$\mathbf{F}_q = \{0, \pm 1, \pm 2, \cdots, \pm h\}, h = \frac{q-1}{2}$ とし、$0 \leq j \leq h, \mathbf{u} = (u_1, u_2, \cdots, u_n)$ に対して

$$wt_j(\mathbf{u}) = \sharp\{i \mid u_i = \pm j\}$$

とおき、$X_0, X_1, \cdots, X_h$ を $\mathbf{C}$ 上代数的に独立な変数として、

$$L_C(X_0, X_1, \cdots, X_h) = \sum_{\mathbf{u} \in C} X_0^{wt_0(\mathbf{u})}, X_1^{wt_1(\mathbf{u})}, \cdots, X_h^{wt_h(\mathbf{u})}$$

を C の Lee weight enumerator という。

[C の complete weight enumerator]

$\mathbf{F}_q = \{0, 1, \cdots, q-1\}$ として $0 \leq j \leq q-1$ に対して

$$s_j(\mathbf{u}) = \sharp\{i \mid u_i = j\}$$

とする。$X_0, X_1, \cdots, X_{q-1}$ を $\mathbf{C}$ 上代数的に独立な変数として、

$$W_C(X_0, X_1, \cdots, X_{q-1}) = \sum_{\mathbf{u} \in C} X_0^{s_0(\mathbf{u})}, X_1^{s_1(\mathbf{u})}, \cdots, X_{q-1}^{s_{q-1}(\mathbf{u})}$$

により定まる多項式 $W_C(X_0, X_1, \cdots, X_{q-1})$ を C の complete weight enumerator という。

Example 1. $q = 5, C = \{00, 12, 24, 31, 43\}$ を $[2, 1]$ code over $\mathbf{F}_5$ とする。
$L_C(X_0, X_1, X_2) = X_0^2 + 4X_1X_2$ は C の Lee weight enumerator である。
また、$W_C(X_0, X_1, X_2, X_3, X_4) = X_0^2 + X_1X_2 + X_2X_4 + X_1X_3 + X_3X_4$ は C の complete weight enumrator.

次の変換公式はそれぞれの枚挙多項式の議論で中心的な役割を演じる。
[Hamming weight enumerator の変換公式]

$$W_C(x, y) = \frac{1}{|C|} W_C(x + (q-1)y, x - y))$$

[Lee weight enumerator の変換公式]

(C.F. MacWilliams- N.J.A. Sloane 's book "The Theory of Erroe-Correcting Codes")

$$L_{C^\perp}(X_0, X_1, \cdots, X_h) = \frac{1}{|C|} L_C(X_0 + \sum_{i=1}^{q-1}(\chi_1(\omega_0\omega_i) + \chi_1(-\omega_0\omega_i))X_i, \cdots)$$

[complete weight enumerator の変換公式]

$$W_{C^\perp}(X_0, X_1, \cdots, X_{q-1}) = \frac{1}{|C|} W_C(\sum_{i=0}^{q-1} \chi_1(\omega_0\omega_i)X_i, \cdots)$$

3 u.g.g.r.

ユニタリー空間の鏡影とは有限位数の一次変換で、その固有値がただ一つを除いて 1 に等しいようなものである。有限ユニタリー鏡影群 (u.g.g.r) とはユニタリー鏡影変換によって生成されるような有限群のことである。

G を線形一次変換よりなる有限群とし G が働く線形空間の次元を n とするとき、G は複素係数の多項式環 $\mathbf{C}[X_1, X_2, \cdots, X_n]$ にも自然に働く。このとき、$\mathbf{C}[X_1, X_2, \cdots, X_n]^G$ により、G 不変な多項式よりなる $\mathbf{C}[X_1, X_2, \cdots, X_n]$ の部分環を表すことにする。$\mathbf{C}[X_1, X_2, \cdots, X_n]^G$ の構造については、G.C.Shephard and J.A. Todd の次の定理が基本的である。

Theorem 1 (Shephard and Todd) G を線形一次変換よりなる有限群とする。このとき、$\mathbf{C}[X_1, X_2, \cdots, X_n]^G$が自由な生成元を持つ多項式環になるのは、$G$ が *u.g.g.r.* であるとき、かつそのときに限る。

この定理は重要であるが、もしこの定理にあまりにも拘れば、符号理論で現れる多くの多項式環を扱うことが困難になる。それが講演のテーマにおいて u.g.g.r. に近接した群と銘打打った理由である。U.g.g.r. に近接したという大雑把な言い方の意味は、指数が極く小さい部分群か包摂群 (over group) と

いうことである。このような群に限定しても、その不変多項式環の構造を決定する一般的方法は未だ開発途上のようで、講演者が良くその消息を述べられる立場に無いことを断って置きたい。

一次変換群 G を調べる一つの基本的な手段として、ポアンカレ級数がある (これは人によってはヒルベルト級数とも言う)。それは

$$\Phi_G(\lambda) = \sum_{n \geq 0} \dim \mathbf{C}[X_1, X_2, \cdots, X_n]_m^G \lambda^m$$

により定義される。ここで、$\mathbf{C}[X_1, X_2, \cdots, X_n]_m^G$ は $\mathbf{C}[X_1, X_2, \cdots, X_n]^G$ の m 次の斉次部分である。特に、G が有限群の場合、モリーエンによりこの級数はより計算し易い次の形で与えられている。

$$\Phi_G(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{\det(I_n - \lambda A)}$$

この最後の形でポアンカレ級数を扱うとき、しばしばモリーエン級数と呼ばれることが多い。U.g.g.r. G に対するモリーエン級数は前記の Shephard-Todd の論文で表の形で与えられている。講演の主題に関係するのでそれを再掲する。

表に於いて左端の番号は Shephard-Todd に従って付けたもの。それから先は順に、G が作用する空間の次元、G の位数、不変多項式環の生成元の次数を表す。

Numbering	dimension	group order	degrees of basic polynomials
1	n	$(n+1)!$	$2,3,\ldots,n+1$
2	n	$qm^{n-1}n!$	$m,2m,\ldots,(n-1)m,qn$
3	1	m	m
4	2	24	4,6
5	2	72	6,12
6	2	48	4,12
7	2	144	12,12
8	2	96	8,12
9	2	192	8,24
10	2	288	12,24
11	2	576	24,24
12	2	48	6,8
13	2	96	8,12
14	2	144	6,24
15	2	288	12,24
16	2	600	20,30
17	2	1200	20,60
18	2	1800	30,60
19	2	3600	60,60
20	2	360	12,30
21	2	720	12,60
22	2	240	12,20
23	3	120	2,6,10
24	3	336	4,6,14
25	3	648	6,9,12
26	3	1296	6,12,18
27	3	2160	6,12,30
28	4	1152	2,6,8,12
29	4	7680	4,8,12,20
30	4	14400	2,12,20,30
31	4	$64 \cdot 6!$	8,12,20,24
32	4	$216 \cdot 6!$	12,18,24,30
33	5	$72 \cdot 6!$	4,6,10,12,18
34	6	$108 \cdot 9!$	6,12,18,24,30,42
35	6	$72 \cdot 6!$	2,5,6,8,9,12
36	7	$8 \cdot 9!$	2,6,8,10,12,14,18
37	8	$192 \cdot 10!$	2,8,12,14,18,20,24,30

6

G.C.Shephard と J.A. Todd の論文は重要であるが、強い難点が一つある。それは 個々の u.g.g.r. の不変多項式環を文献を挙げるに止めて、具体的に与えていないことである (処方箋だけがあってお薬のない薬局のような)。この講演を機会に講演者はこの間隙を埋めることを企てた (全面的ではないが)。そのための努力は考古学的とでも言えるような種類のものであった。

Shephard-Todd のリストはいくつかの親近性のあるグループに分けられる。このうち、リストの No.1,2,28,35,36,37 の群はそれぞれリー群の $A_n, D_n, F_4, E_6, E_7, E_8$ 型の群のワイル群そのものか、それから構成されるもので Shephard-Todd の研究以前に多くの研究がなされているし、今の所枚挙多項式に関連した形での coding theoretic interpretation を持つことが、見えないので本講演では考察の対象から外した。また同じ理由で No.23,27,30,32,33,34 の群も触れなかった。

しかし、No.16 ～ 22 の群に対しては講演者は同じ扱いを出来ないと感じている。この族の群は今は枚挙多項式に関連した形での coding theoretic interpretation を持っていると立証されている訳ではないが、何らかの形で 5 元体上の自己双対符号の枚挙多項式と関連があると信じている。

4 thesis-hypothesis の検討

本題に入ることにする。

(I) 正四面体群 (Tetrahedral group) に由来する u.g.g.r.

$$\begin{aligned} f &= x^4 - 2\sqrt{3}ix^2y^2 + y^4 \\ h &= x^4 + 2\sqrt{3}ix^2y^2 + y^4 \\ t &= xy(x^4 - y^4) \end{aligned}$$

を 3 つの多項式とする。このとき、

Numbered group	group order	invarint ring
G_4	24	$\mathbf{C}[f,t]$
G_5	72	$\mathbf{C}[f^3,t]$
G_6	48	$\mathbf{C}[f,t^2]$
G_7	144	$\mathbf{C}[f^3,t^2]$

となり、
G_6 の生成元は:

$$M_1 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}$$
$$M_2 = diag(1,\omega)$$

で与えられる。ここで、ω は 1 の 3 乗根。
G_4 の生成元は:

$$L_1 = \frac{-\omega}{\sqrt{2}}\begin{pmatrix} \epsilon^7 & \epsilon \\ \epsilon^3 & \epsilon \end{pmatrix} \quad L_2 = \frac{-\omega}{\sqrt{2}}\begin{pmatrix} \epsilon & \epsilon^3 \\ \epsilon & \epsilon^7 \end{pmatrix}$$

で与えられる。
Molien 級数 :

$$\Phi_{G_4}(\lambda) = \frac{1}{(1-\lambda^4)(1-\lambda^6)}$$
$$\Phi_{G_6}(\lambda) = \frac{1}{(1-\lambda^4)(1-\lambda^{12})}$$

自己双対3元符号 C の Hamming weight enumerator $W_C(x,y)$ は MacWlliams 恒等式と、符号語の重みが 3 で割り切れることとから $\mathrm{C}[x,y]^{G_6}$. に属することが言える。

この多項式からは、2 通りの仕方で保型形式が構成できる (もっとあるかも知れないが)。
一つの仕方はこの多項式の変数に変形したヤコビテータ関数を代入する方法で、レヴェルつきの保型形式が構成できる。
もう一つの方法は A_2 型の root lattice のテータ級数および lattice をずらせてから作る疑似テータ級数を初めに考える。これらは level が 3 の合同群に属する modular form になるが、さらにこれらを Hamming weight enumerator に代入すると、full modular group に属する modular form になる。

$$\Phi_{G_5}(\lambda) = \frac{1}{(1-\lambda^6)(1-\lambda^{12})}$$

$$\Phi_{G_7}(\lambda) = \frac{1}{(1-\lambda^{12})^2}$$

$$\mathbf{C}[x,y]^{G_4} = \mathbf{C}[f,t]$$
$$\mathbf{C}[x,y]^{G_6} = \mathbf{C}[f,t]$$

(II) 正八面体群 (Octahedral group) に由来する u.g.g.r.

$$\begin{aligned} h(x,y) &= x^8 + 14x^4y^4 + y^8 \\ t(x,y) &= x^{12} - 33x^8y^4 - 33x^4y^8 + y^{12} \\ f(x,y) &= xy(x^4 - y^4) \end{aligned}$$

Numbered group	group order	invarint ring
G_8	96	$\mathbf{C}[h,t]$
G_9	192	$\mathbf{C}[h,t^2]$
G_{10}	288	$\mathbf{C}[h^3,t]$
G_{11}	576	$\mathbf{C}[h^3,t^2]$
G_{12}	48	$\mathbf{C}[f,h]$
G_{13}	96	$\mathbf{C}[f^2,h]$
G_{14}	144	$\mathbf{C}[f,t^2]$
G_{15}	288	$\mathbf{C}[f^2,t^2]$

G_9 の生成元：

$$\begin{aligned} M_1 &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \\ M_2 &= diag(1,i) \end{aligned}$$

G_8の生成元：

$$\begin{aligned} L_1 &= \frac{1-i}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \\ L_2 &= diag(-i,1) \end{aligned}$$

$$| G_9 | = 192$$

Molien 級数 :

$$\Phi_{G_8}(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{12})}$$

$$\Phi_{G_9}(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})}$$

自己双対な重偶 2 元符号 C の Hamming weight enumerator $W_C(x,y)$ に対する MacWlliams 恒等式より $W_C(x,y)$ が $\mathbf{C}[x,y]^{G_9}$. に属することが分かる。

さらに M. Broué と M. Enguehard が下記の論文において 環 $\mathbf{C}[x,y]^{G_9} = \mathbf{C}[h,t^2]$ 環 $\mathbf{C}[E_4(\tau), \Delta_{12}(\tau)]$ に同型であることを証明した。彼等の方法は、符号の weight enumerator にヤコビテータ関数のゼロ値を代入したものが符号から Leech-Sloane の方法で得られる二次形式のテータ級数と一致することを示すことが基本的アイデアであった。従って得られる modular forms の weight は 4 の倍数のものという制約があった。しかし、二次形式のテータ級数にこだわらなければこの制約ははずせることがわかった。そして環 $\mathbf{C}[x,y]^{G_8} = \mathbf{C}[h,t]$ が環 $\mathbf{C}[E_4(\tau), E_6(\tau)]$ に同型であることまでが示せる。

$$\Phi_{G_{10}}(\lambda) = \frac{1}{(1-\lambda^{12})(1-\lambda^{24})}$$

$$\Phi_{G_{11}}(\lambda) = \frac{1}{(1-\lambda^{24})^2}$$

$$\Phi_{G_{12}}(\lambda) = \frac{1}{(1-\lambda^6)(1-\lambda^8)}$$

$$\Phi_{G_{13}}(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{12})}$$

$$\Phi_{G_{14}}(\lambda) = \frac{1}{(1-\lambda^6)(1-\lambda^{24})}$$

$$\Phi_{G_{15}}(\lambda) = \frac{1}{(1-\lambda^{12})(1-\lambda^{24})}$$

関連した文献 :

1. M. Broué et M. Enguehard, Polynôme des poids de certains codes et fonction théta de certains réseaux, Ann. scien. Éc. Norm. Sup. 4^e série, t.5

(1972) 157-181.

(III) 正二十面体群 (Icosahedral group) に由来する u.g.g.r.

$$
\begin{aligned}
f &= xy(x^{10}+11x^5y^5-y^{10}) \\
h &= -x^{20}-y^{20}+228(x^{15}y^5-x^5y^{15})-494x^{10}y^{10} \\
t &= x^{30}+y^{30}+522(x^{25}y^5-x^5y^{25})-10005(x^{20}y^{10}+x^{10}y^{20})
\end{aligned}
$$

Numbered group	group order	invarint ring
G_{16}	600	$\mathbf{C}[h,t]$
G_{17}	1200	$\mathbf{C}[h,t^2]$
G_{18}	1800	$\mathbf{C}[h^3,t]$
G_{19}	3600	$\mathbf{C}[h^3,t^2]$
G_{20}	360	$\mathbf{C}[f,t]$
G_{21}	720	$\mathbf{C}[f,t^2]$
G_{22}	240	$\mathbf{C}[f,h]$

Molien 級数 :

$$\Phi_{G_{16}}(\lambda)=\frac{1}{(1-\lambda^{20})(1-\lambda^{30})}$$

$$\Phi_{G_{17}}(\lambda)=\frac{1}{(1-\lambda^{20})(1-\lambda^{60})}$$

$$\Phi_{G_{18}}(\lambda)=\frac{1}{(1-\lambda^{30})(1-\lambda^{60})}$$

$$\Phi_{G_{19}}(\lambda)=\frac{1}{(1-\lambda^{60})^2}$$

$$\Phi_{G_{20}}(\lambda)=\frac{1}{(1-\lambda^{12})(1-\lambda^{30})}$$

$$\Phi_{G_{21}}(\lambda)=\frac{1}{(1-\lambda^{12})(1-\lambda^{60})}$$

$$\Phi_{G_{22}}(\lambda)=\frac{1}{(1-\lambda^{12})(1-\lambda^{20})}$$

Problem 1: $G_{16} \sim G_{22}$ の不変多項式環と (5 元?) 符号の weight enumerator とはなんらかの関係があるか ?

(IV) G_{23} およびそれに関連した群

$$G_{23} =< A, B, C >$$

$$| G_{23} |= 120$$

$$\begin{aligned} A &= diag(1, \omega, \omega^2) \\ B &= \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 2 & 2 \\ 1 & \omega+\omega^4 & \omega^2+\omega^3 \\ 1 & \omega^2+\omega^3 & \omega+\omega^4 \end{pmatrix} \\ C &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \end{aligned}$$

ω is the fifth root of unity.

G_{23} の Molien 級数:

$$\Phi_{G_{23}}(\lambda) = \frac{1}{(1-\lambda^2)(1-\lambda^6)(1-\lambda^{10})}$$

また G_{23} の不変多項式環は $\mathrm{C}[x,y,z]^{G_{23}} = \mathrm{C}[F_2, F_6, F_{10}] = \mathcal{R}_1$ (と置く) で与えられる。ここで、

$$\begin{aligned} F_2 &= x^2 + 4yz \\ F_6 &= x^6 + 12x(y^5+z^5) + 2y^3z^3 \\ F_{10} &= 5x^6y^2z^2 - 4x^5(y^5+z^5) - 10x^4y^3z^3 + 10x^3(y^6z+yz^6) \\ &\quad +5x^2y^4z^4 - 10x(y^7z^2+y^2z^7) + 6y^5z^5 + y^{10} + z^{10} \end{aligned}$$

下記の Leon-Pless-Sloane の論文で Thm 6 として掲げられているように 自己双対 5 元符号の Lee weight enumerator は $\mathrm{C}[x,y,z]^{G_{23}}$ に属する。しかし次の問題は残っているように思われる。
Problem 2: $\mathrm{C}[x,y,z]^{G_{23}}$ は自己双対 5 元符号の Lee weight enumerators で生成されるか ?

G_{23} の指数の部分群 $G_{23}^{\flat} =< A, BC >$ は G_6 内の G_4 や G_9 内の G_8 と違って G_{23}より立場が悪くなる。

$$| G_{23}^{\flat} |= 60$$

Molien series for $G_{23}^{\flat}$:

$$\Phi_{G_{23}^{\flat}}(\lambda) = \frac{1+\lambda^{15}}{(1-\lambda^2)(1-\lambda^6)(1-\lambda^{10})}$$

$\mathbf{C}[x,y,z]^{G_{23}^{\flat}} = \mathcal{R}_1 \oplus F_{15}\mathcal{R}_1$ F_{15} については explicit には知らない。

有限体の上の符号の Lee weight enumerator と Hilbert modular form とを結び付ける F. Hirzebruch と van der Geer の仕事を W. Ebeling の本に従って紹介しておく。

p を奇素数とし、$\zeta = e^{2\pi i/p}$ とする。1 の p 乗根は $\zeta^0 = 1, \zeta, \zeta^2, \cdots, \zeta^{p-1}$ で尽くされ $x^p - 1 = (x-1)(x-\zeta)\cdots(x-\zeta^{p-1})$ となるから

$$\frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + 1 = (x-\zeta)(x-\zeta^2)\cdots(x-\zeta^{p-1}).$$

そこで、$x = 1$ とすると、$p = (1-\zeta)(1-\zeta^2)\cdots(1-\zeta^{p-1})$ が得られる。$K = \mathbf{Q}(\zeta)$ とする。埋め込み写像 $\sigma_i : K \to \mathbf{C}$ $(1 \le i \le p-1)$ を $\sigma_i(\zeta) = \zeta^i$ から定める。これから

$$Tr_{K/\mathbf{Q}}(\alpha) = \sum_{i=1}^{p-1} \sigma_i(\alpha) \quad \alpha \in K$$

が定義できる。$\mathcal{O}(K)$ を K の整数環とする。$\mathfrak{P} = (1-\zeta)$ を $1-\zeta$ から生成される単項イデアルとすると、$\mathfrak{P} \cap \mathbf{Z} = p\mathbf{Z}$ が成り立つ。$\mathfrak{P}^{p-1} = (p) \subset \mathcal{O}(K)$ となる。次に、$x, y \in \mathcal{O}(K)$ に対して、$< x, y >:= Tr(\frac{x\overline{y}}{p})$ ($\overline{y}$ は y の複素共役) とする。

$$\mathcal{O}(K) = \{\alpha = \sum_{i=0}^{p-2} a_i\zeta^i | a_i \in \mathbf{Z} 0 \le i \le p-2\}$$

となることが示せる。$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$ に対して、$\rho(\alpha) = \sum_{i=0}^{p-2} a_i$ により定義される $\rho : \mathcal{O}(K) \to \mathbf{Z}/p\mathbf{Z}$ は additive homomorphism で $ker\rho = \mathfrak{P}$ となることが確かめられる。従って $\mathcal{O}(K)/\mathfrak{P} \cong \mathbf{Z}/p\mathbf{Z} = \mathbf{F}_p$となる。$\rho$ から定まる写像 $\mathcal{O}(K)^n \to \mathbf{F}_p^n$ をも ρ で表すことにする。C を $\mathbf{F}_p$ の符号とする

とき、$\Gamma_C = \rho^{-1}(C) \subset \mathcal{O}(K)^n$ は lattice で内積 $< \mathbf{x}, \mathbf{y} = \sum_{i=1}^{n} Tr(\frac{x_i\overline{y_i}}{p}$ を持つ。ただし、$\mathbf{x} = (x_1, x_2 \cdots, x_n), \mathbf{y} = (y_1, y_2 \cdots, y_n)$. Γ_C^* をΓ_C の dual lattice とすると、$\Gamma_C^* = \Gamma_{C^\perp}$ が成り立つ。そして、C が self-dual ならば Γ_C が even unimodular になる。

$\Gamma = \mathfrak{P}, \Gamma^* = \mathcal{O}$ の場合に戻る。$\mathcal{O}(K)/\mathfrak{P} \cong \mathbf{F}_p$. $\gamma \in \Gamma^*$ に対し、

$$\theta_j(\tau_1, \cdots, \tau_{\frac{p-1}{2}}) := \sum_{x \in \mathfrak{P}+\gamma} exp\{2\pi i Tr_{k/\mathbf{Q}}(\tau \frac{x\overline{x}}{p})\},$$

ここで k は K の maximal real subfield で

$$Tr_{k/\mathbf{Q}}(\tau \frac{x\overline{x}}{p}) = \sum_{l=1}^{(p-1)/2} \tau_l \frac{\sigma_l(x\overline{x})}{p}$$

により定義される。θ_j は weight 1 の $\Gamma(\mathfrak{p}) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathcal{O}_k) \mid a \equiv d \equiv 1(mod\mathfrak{p}), b \equiv c \equiv 0(mod\mathfrak{p})\}$ についての Hilbert modular form. ここで、$\mathfrak{p} = \mathfrak{P} \cap O_k$。Lattice Γ_C に対するテータ級数は

$$\theta_{\Gamma_C} = \sum_{\mathbf{x} \in \Gamma_C} exp\{2\pi i Tr_{k/\mathbf{Q}}(\tau \frac{x\overline{x}}{p})\}$$

により定義される。θ_{Γ_C} は weight n の $SL_2(\mathcal{O}_k)$ に属する Hilbert modular form になることは知られている。

Theorem 2 *van der Geer and F. Hirzebruch*

$$\theta_{\Gamma_C} = L_C(\theta_0, \theta_1, \cdots, \theta_{\frac{p-1}{2}}),$$

ここで、L_C は C の *Lee weight enumerator*。

Problem 3: θ_{Γ_C} は Hilbert modular form のなかでどれだけの部分を占めるか？

関連した文献：

1. J.S. Leon , V. Pless and N.J.A. Sloane, Self-Dual Codes over $GF(5)$, J. Comb. Th. Ser.A 32 (1982) 178-194
2. W. Ebeling, Lattices and Codes, Vieweg (1994)

(V) G_{24} and related group

$$| G_{24} | = 336$$

Generators of G_{24} :

$$\begin{aligned} R_1 &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \\ R_2 &= diag(1,1,-1) \\ R_3 &= \frac{1}{2}\begin{pmatrix} 1 & -1 & -\alpha \\ -1 & 1 & -\alpha \\ -\overline{\alpha} & -\overline{\alpha} & 0 \end{pmatrix} \end{aligned}$$

$\alpha = \frac{1}{2}(1 - i\sqrt{7})$
Molien series for G_{24} :

$$\Phi_{G_{24}}(\lambda) = \frac{1}{(1-\lambda^4)(1-\lambda^6)(1-\lambda^{14})}$$

$\mathbf{C}[x,y,z]^{G_{24}} = \mathbf{C}[F_4, F_6, F_{14}]$

$$\begin{aligned} F_4 &= (x_1^3 + x_2^3 + x_3^3)^2 - 12(x_1^3x_2^3 + x_2^3x_3^3 + x_3^3x_1^3) \\ F_6 &= (x_1^3 - x_2^3)(x_2^3 - x_3^3)(x_3^3 - x_1^3) \\ F_{14} &= (x_1^3 + x_2^3 + x_3^3)\{(x_1^3 + x_2^3 + x_3^3)^3 + 216x_1^3x_{21}^3x_3^3\} \end{aligned}$$

$\mathbf{C}[x,y,z]^{G_{24}}$ は今の所符号理論的解釈を持っていない。しかし、G_{24}の 4 次元ユニタリー空間での実現である$\widehat{G_{24}}$ は符号理論的解釈を持つ。
$\widehat{G_{24}}$ の生成元 :

$$\begin{aligned} \widehat{R_1} &= diag(1,\omega,\omega^4,\omega^2) \\ \widehat{R_2} &= \frac{1}{\sqrt{-7}}\begin{pmatrix} 1 & 2 & 2 & 2 \\ 1 & \omega+\omega^6 & \omega^2+\omega^5 & \omega^3+\omega^4 \\ 1 & \omega^2+\omega^5 & \omega^3+\omega^4 & \omega+\omega^6 \\ 1 & \omega^3+\omega^4 & \omega+\omega^6 & \omega^2+\omega^5 \end{pmatrix} \end{aligned}$$

ここで $\omega = e^{2\pi i/7}$.
$\widetilde{G_{24}}$ の Molien 級数：

$$\Phi_{\widetilde{G_{24}}}(\lambda) = \frac{1+\lambda^8+\lambda^{10}+\lambda^{12}+\lambda^{16}+\lambda^{18}+\lambda^{20}+\lambda^{28}}{(1-\lambda^4)(1-\lambda^6)(1-\lambda^8)(1-\lambda^{14})}$$

7 元体上の自己双対符号 Cの Lee weight enumerator $L_C(X_0, X_1, X_2, X_3)$ は環 $\mathbf{C}[x,y,u,v]^{\widetilde{G_{24}}}$ に入ることが下記の Mallows-Sloaneis の仕事から知られている。従って再び F. Hirzebruch と van der Geer の結果により、Hilbert modular form が構成できたことになり講演の thesis を再び支持する。
この事に関連して、一つの問題が生じる。

Problem 4: 環 $\mathbf{C}[x,y,u,v]^{\widetilde{G_{24}}}$ は 7 元体上の自己双対符号 Cの Lee weight enumerator $L_C(X_0, X_1, X_2, X_3)$ から生成されているか？ あるいは生成されていなければその違いはどれ程か？

関連した文献：

1. F. Klein, Über die Transformationen siebenter Ordnung der elliptischen Funktionen, Math. Ann. 14 (1887) 428-471.
2. F. Brioschi, Über die Jacobi'sche Modulargleichung vom achten Grade, Math. Ann. 15 (1879) 241-250.
3. H. Maschke, The invariants of a group of 2.168 linear quaternary substitutions, International Mathematical Congress 1893, New York Macmillan, (1896) 175-186.
4. W. Burside, Theory of groups of finite order, Cambridge Univ. Press (1911).
5. W.L. Edge, The Klein group in three dimensions, Acta Math. 79 (1947) 153-223.
6. G.C. Shepard and J.A. Todd, Finite unitary reflection groups, Can. J. Math. 6(1954) 274-304.
7. C.L. Mallows and N.J.A. Sloane, On the invariants of a linear group of order 336, Proc. Camb. Phil. Soc. (1973) 435-440.

(VI) G_{25}, G_{26} およびそれに関係した群

$$G_{25} = < A, B, C >$$

$$| G_{25} |= 648$$

$$\begin{aligned} A &= diag(1,1,\omega^2) \\ B &= \frac{-i}{\sqrt{3}}\begin{pmatrix} \omega & \omega^2 & \omega^2 \\ \omega^2 & \omega & \omega^2 \\ \omega^2 & \omega^2 & \omega \end{pmatrix} \\ C &= diag(1,\omega^2,1) \end{aligned}$$

G_{25} の Molien 級数：

$$\Phi_{G_{25}}(\lambda) = \frac{1}{(1-\lambda^6)(1-\lambda^9)(1-\lambda^{12})}$$

$$\mathbf{C}[x,y,z]^{G_{25}} = \mathbf{C}[F_6, F_9, F_{12}] = \mathcal{R}_2$$

$$\begin{aligned} F_6 &= (x_1^3+x_2^3+x_3^3)^2 - 12(x_1^3x_2^3+x_2^3x_3^3+x_3^3x_1^3 \\ F_9 &= (x_1^3-x_2^3)(x_2^3-x_3^3)(x_3^3-x_1^3) \\ F_{12} &= (x_1^3+x_2^3+x_3^3)\{(x_1^3+x_2^3+x_3^3)^3 + 216x_1^3x_{21}^3x_3^3\} \end{aligned}$$

$$| G_{26} |= 1296$$

G_{26} の Molien 級数：

$$\Phi_{G_{26}}(\lambda) = \frac{1}{(1-\lambda^6)(1-\lambda^{12})(1-\lambda^{18})}$$

$$\mathbf{C}[x,y,z]^{G_{26}} = \mathbf{C}[F_6, F_{12}, F_{18}] = \mathcal{R}_3$$

$$F_{18} = 432F_9^2 - F_6^3 + 3F_6F_{12}$$

G_{26}^a の生成元

$$\begin{aligned} D &= diag(1,\omega,1) \\ E &= \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \end{aligned}$$

および 3 次の permutation matrices.
自己双対な 3 元符号 C の complete weight enumerator $W_C(x,y,z)$ に対する MacWlliams 恒等式より $W_C(x,y,z)$ が $\mathbf{C}[x,y,z]^{G_{26}^a}$ に属することが導かれる。

G_{26}^a の Molien 級数：

$$\Phi_{G_{26}^a}(\lambda) = \frac{1+\lambda^{24}}{(1-\lambda^{36})(1-\lambda^{12})^2}$$

$\mathcal{R}_4 = \mathbf{C}[F_4, F_{12}, F'_{12}]$ と置くと、$\mathbf{C}[x,y,z]^{G_{26}^a} = \mathcal{R}_4 \oplus F_6 F_{18} \mathcal{R}_4$ となることが知られている。ここで、

$$F'_{12} = x_1x_2x_3\{27(x_1x_2x_3)^3 - (x_1^3+x_2^3+x_3^3)^3\}$$

$$| G_{26}^a | = 2592$$

自己双対な 3 元符号 C の complete weight enumerator $W_C(x,y,z)$ から modular form が構成されることは 1994 年秋の数理解析研の集会で述べたが数論的なレヴェルの性質等については、その後よく調べていないのでここではこれ以上報告出来ない。

関連した文献：

1. G.A. Miller, H.F. Blichfeldt and L.E. Dickson, Theory and applications of finite groups New York (1916)
2. N.J.A. Sloane, Error-correcting codes and invariant theory: new applications of a nineteenth-century technique, Amer. Math. Month. 84 (1977) 82-107.
3. C.L. Mallows, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$, SIAM J. Appl. Math. 31 (1976) 649-666.
4. F.J. MacWilliams and N.J.A.Sloane, "The Theory of Error-Correcting Codes",North-Holl and, Amsterdam, (1977).
5. S.M. Gagola, Jr., Weight enumerators of normalized codes, SIAM J. Alg. Disc. Math. 2 (1981) 347-380.

(VII) G_{31}
G_{31} の生成元:

$$r_1 = \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix} \quad r_2 = \begin{pmatrix} 0 & i & 0 & 0 \\ i & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$r_3 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad r_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$r_5 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$| G_{31} | = 46080$$

G_{31} の Molien 級数：

$$\Phi_{G_{31}}(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{12})(1-\lambda^{20})(1-\lambda^{24})}$$

Maschke は $\mathrm{C}[x,y,u,v]^{G_{31}} = \mathrm{C}[F_8, F_{12}, F_{20}, F_{24}] = \mathcal{R}_5$ となることを証明した。ここで、

$$F_8 = x^8+y^8+u^8+v^8+14(x^4y^4+x^4u^4+x^4v^4+y^4u^4+y^4v^4+u^4v^4)+168v^2u^2y^2x^2$$

$$\begin{aligned} F_{12} = {} & x^{12}+y^{12}+u^{12}+v^{12}-33(y^4x^8+u^4x^8+v^4x^8+y^8y^4+x^4u^8 \\ & +x^4v^8+y^8u^4+y^8v^4+v^4u^8+v^8u^4+y^4u^8+y^4v^8) \\ & +330(y^4v^4u^4+x^4v^4u^4+x^4u^4y^4+x^4v^4y^4) \\ & +792x^2y^2v^2u^2(x^4+y^4+u^4+v^4) \end{aligned}$$

であり、F_{20}, F_{24} も原論文に従って計算することが出来るが紙面を徒に塞がないために省略する。

(VIII) G_{31}^a (G_{31}の over group)
G_{31}^a の生成元: G_{31} plus $diag(1,i,1,i)$

$$| G_{31}^a | = 92160$$

G_{31}^a Molien 級数:

$$\Phi_{G_{31}^a}(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})^2(1-\lambda^{40})}$$

自己双対な 2 元重偶符号 $\mathcal{C}$ の biweight enumerator $\mathcal{BW}_{\mathcal{C}}(x,y,u,v)$ に対する MacWlliams 恒等式、およびその他から $\mathcal{BW}_{\mathcal{C}}(x,y,u,v)$ が $\mathrm{C}[x,y,u,v]^{G_{31}^a}$ に属することが導かれる。

W. Duke は $\mathrm{C}[x,y,u,v]^{G_{31}^a} = \mathcal{R}_4 \oplus F_{12}F_{20}\mathcal{R}_4$ となることを証明し、さらにこの環が 2 次の Siegel modular forms で doubly even weights を持つもののなす環に同型であることまでを証明した。またしても doubly even の制約が。これは Duke のアイデアが Broué と M. Enguehard 達のそれの延長上にある以上致し方のない所である。坂内-小関はその制約を越えられるとの見通しを持っている。

関連した文献:

1. H. Maschke, Über die quaternäre, endliche, lineare Substitutionsgruppe der Borchardt'schen Moduln, Math. Ann. Vol.30 (1887) 496-515
2. G.C. Shephard, Abstract definitions for reflection groups, Can. J. Math. 9 (1957) 273-276.
3. F.J. MacWilliams, C.L. Mallows, and N.J.A. Sloane, Generalizations of Gleason's Theorem on Weight Enumerators of Self-Dual Codes, IEEE Trans. Inf. Th. IT-18 (1972) 794-805.
4. W. C. Huffman, The biweight enumerator of self-dual orthogonal binary codes, Discrete Math. 26 (1979) 129-143
5. W. Duke, On codes and Siegel modular forms, Duke Math. J. (1993) 125-136

5 Concluding Remarks

(1) 各種の weight enumerators はそれが u.g.g.r. に近かろうが遠かろうが符号理論の対象としては重要であるがあまり研究が進んでいない。例えば、$GF(p)$ 上の self-dual code の complete weight enumerator を不変にする一次変換群の Molien 級数については前記の S.M. Gagola の論文があるが、不変式環の構造についての結果は C.L. Mallows, V. Pless および N.J.A. Sloane による $p = 3$ の場合を除いては何も具体的なものはない。

(2) complete weight enumerators の研究が難しいのであれば、その準備として Lee weight enumerators を研究することも一案であろうが奇妙なことにこの場合には Molien 級数の仕事すら見かけない (ことによると筆者の不明かも知れぬが)。さらに Lee weight enumerator よりも粗雑なしかし調べるのが容易な weight enumerators (最も粗雑なものが Hamming weight enumerators であるが中間的なものは特に定義されてはいないようであるがまだあるのでは) を使って一種の composition series 的な研究も有り得ると思う。

(3) Molien 級数は有限一次変換群の元の固有値のデータが揃えば計算できて、有用な情報を与えるが、もっと踏み込んで不変式環の生成元をそのデータから直接計算できるようなプロセスは無いだろうか？

(4) 今までのうまく行った場合の 2 つの方向での一般化として、(i) weight enumerator の multiple version ,(ii) Jacobi polynomial version (すなわち介在する有限一次変換群の simultaneous invariants) はどちらも modular forms とのつながりがあり、modular form の構成法として theta series や Eisenstein series と並ぶものになり得て、かつ modular form の代数的な構造理論にも良い手がかりを提供するものと期待できる。

小関 道夫
山形大学理学部数理科学科
990 山形市小白川町 1-4-12
(Tel.) 0236-28-4530 (direct)
e-mail address : ozeki@kszaoh1.kj.yamagata-u.ac.jp

ある種の有限群の不変式環について

坂内悦子　(九大・数理)

表題にある有限群とは Shephard-Todd ([10]) の unitary reflexion group の分類表の中の No.9 (位数 192) の群のことを意味します。この群は $GL(2,\mathbb{C})$ の部分群 ですが Shephard-Todd の論文にある様に普通に 2 変数の複素多項式環に作用させた 場合の不変式環については良く知られているわけですが、ここではこの群を 2 変数の複素多項式環 の l 個の直和 $\mathbb{C}[x_1,y_1,\ldots,x_l,y_l]$ に自然に働かせた場合の不変式環 について考えます。なぜこの不変式環について興味があるのかその背景について少し述べます。

linear code の weight enumerator との関係

F_2 を標数 2 の素体、F_2^n を F_2 上の n 次元ベクトル空間とします。 F_2^n の 2 つのベクトル $\mathbf{u}=(u_1,\ldots,u_n)$ と $\mathbf{v}=(v_1,\ldots,v_n)$ に対して $\mathbf{u}*\mathbf{v}=\sharp\{\,i\mid u_i=v_i=1\}$ を定義します。ベクトル $\mathbf{u}$ に対して $wt(\mathbf{u})=\mathbf{u}*\mathbf{u}$ を $\mathbf{u}$ の weight と呼びます。又 F_2^n には内積 $(\mathbf{u},\mathbf{v})=\sum_{i=1}^n u_iv_i$ を定義しておきます。F_2^n の部分空間 (linear code と呼ばれる) C が F_2^n の中で上に定義した内積に関して直交補空間 $C^\perp$ と一致する時に C は self-dual であると言います。また linear code C の各ベクトルの weight が 4 の倍数である時に C は doubly even である と言います。linear code C の weight enumeratorを次の式で定義します。

$$w_C(x,y)\ =\ \sum_{\mathbf{u}\in C} x^{n-wt(\mathbf{u})}y^{wt(\mathbf{u})}$$

以下では Shephard-Todd の No.9 の群を G と書くことにします。G は 2 つの元

$$\sigma_1\ =\ \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\quad \sigma_1\ =\ \begin{pmatrix}\sqrt{-1} & 0\\ 0 & 1\end{pmatrix}$$

により生成される位数 192 の群です。この時 2 変数複素多項式環 $\mathbb{C}[x,y]$ の G による不変式環 $\mathbb{C}[x,y]^G$ と weight enumerator を結ぶ次の定理が知られて います ([5])。

Gleason の定理

$$\langle\ w_C(x,y)\ \mid C:\text{binary self dual かつ doubly even}\ \rangle\ =\ \mathbb{C}[x,y]^G$$

もう少し詳しく述べると G の不変式環は2つの代数的に独立な 8 次と 24 次の多項式 で生成されていることは Shephard-Todd の論文の中に記されているのですが実はこの 2 つの多項式がそれぞれ binary extended Hamming code [8,4,4] と binary extended Golay code [24,12,8] の weight enumerator でありしかも上に述べた同型対応があたえられることを Gleason が示したのです。

modular form との関係

G の不変式環から modular form が次の様にして作られることが知られている([4])。

Broué-Enguehard の定理

任意の G- 不変 n 次同次多項式 $f(x,y)$ に対し$f(\theta_3(2\tau,0),\theta_2(2\tau,0))$ は weight $\frac{n}{2}$ の modular form を与える。ここで $\theta_i(\tau,z)$, $i=2,3$ は 次に定義される $\mathcal{H}\times\mathbb{C}$ 上のJacobi の theta 関数である($\mathcal{H}$ は上半平面)。

$$\theta_2(\tau,z) = \sum_{n\in\mathbb{Z}} e^{(n+\frac{1}{2})^2\pi\sqrt{-1}\tau+(2n+1)\pi\sqrt{-1}z}$$

$$\theta_3(\tau,z) = \sum_{n\in\mathbb{Z}} e^{n^2\pi\sqrt{-1}\tau+2n\pi\sqrt{-1}z}$$

さらに詳しく述べると linear code から lattice が得られるのであるが、Broué-Enguehard はその時 weight enumerator から上記の対応によってその lattice の theta 関数が得られることを示したのです。

Jacobi form との関係

小関氏は weight enumerator のひとつの拡張としてJacobi 多項式を定義しました([8])。そしてJacobi 多項式の作る空間とG を $\mathbb{C}[x_1,y_1,\dots,x_l,y_l]$ に自然に作用させた時の不変部分空間が同型であることを示しました。さらに坂内-小関により 次に述べる 様な Broué-Enguehard の定理の拡張が得られました([3])。

ここで少し記号を導入しておきます。

$R = \mathbb{C}[x_1,y_1,\dots,x_l,y_l]$

前述の $G = \langle\, \sigma_1,\ \sigma_2 \,\rangle$ の作用は次の通りです。

$$x_i{}^{\sigma_1} = \frac{1}{\sqrt{2}}(x_i+y_i), \quad y_i{}^{\sigma_1} = \frac{1}{\sqrt{2}}(x_i-y_i)$$

$$x_i{}^{\sigma_2} = \sqrt{-1}x_i, \quad y_i{}^{\sigma_2} = y_i$$

$$(i = 1,\dots,l)$$

$$R_{s_1,\dots,s_l} = \left\{ f \in \mathbb{C}[x_1,y_1,\dots,x_l,y_l] \;\middle|\; \deg(x_i)+\deg(y_i) = s_i,\ \text{for } i=1,\dots,l \right\}$$

坂内 -小関の定理

条件 $s_1+\cdots+s_l = n$, $\sum_{i=1}^{l} s_i {m_i}^2 = m$ を満たす任意の非負整数 l, $s_1,\dots,s_l$, $m_1,\dots,m_l$ に対して以下のことが成り立つ。ただしn ($\equiv$ 0 (mod 8)) と m は任意に固定された非負整数である。任意の $f \in R^G_{s_1,\dots,s_l}$ に対して

$f(\theta_3(2\tau,2m_1z),\theta_2(2\tau,2m_1z),\dots,\theta_3(2\tau,2m_lz),\theta_2(2\tau,2m_lz))$

は weight が $\frac{n}{2}$, index が m の Jacobi form である。

坂内-小関はさらに $n(\equiv 0(\mathrm{mod}\ 8))$ とm を固定した時この定理の方法によってweight $\frac{n}{2}$, index m の Jacobi form が全て得られることを予想している。坂内-小関-皆島によって $n=8$, $m \le 48$ の場合に予想が正しいことが示されている([2])。私達はこの予想が正しいかどうか調べるためにまず $R^G_{s_1,\dots,s_l}$ の生成元を具体的に記述して見ることから取り組みを始めました。

$\mathbf{C[x_1,y_1,\dots,x_l,y_l]}$ の G−不変式環

次ぎの補題は不変式論で良く用いられる手法です([9])。

補題 (Schur) $\tilde{R} = \cup_{l=1}^{\infty}\mathbb{C}[x_1,y_1,\dots,x_l,y_l]$ とすると任意の $f \in \tilde{R}^G$ に対して $x_i\frac{\partial f}{\partial x_j}+y_i\frac{\partial f}{\partial y_j}$ も又 $\tilde{R}^G$に含まれる。

今ある $j \in \{1,\dots,l\}$ に対して $s_j \ge 2$ が成り立つときに上の補題により次のような2種類の写像を定義することができます。すなわち

$$\varphi_+ : R^G_{s_1,\dots,s_j,\dots,s_l} \longrightarrow R^G_{s_1,\dots,s_j-1,\dots,s_l,1}, \qquad \varphi_+ f = x_{l+1}\frac{\partial f}{\partial x_j}+y_{l+1}\frac{\partial f}{\partial y_j}$$

$$\varphi_- : R^G_{s_1,\dots,s_j-1,\dots,s_l,1} \longrightarrow R^G_{s_1,\dots,s_j,\dots,s_l}, \qquad \varphi_- f = x_j\frac{\partial f}{\partial x_{l+1}}+y_j\frac{\partial f}{\partial y_{l+1}}$$

このとき $\varphi_-\varphi_+ = s_j f$ が成立することが容易にわかります。従って φ_- は全射 φ_+ は単射であります。このことを使うと一般の $R^G_{s_1,\dots,s_l}$ の構造は $R^G_{1,\dots,1}$ の構造を知れば φ_- を何回か行なうことによって求めることができます。従って問題は $R^G_{1,\dots,1}$ の場合に帰着されます。$n=8$, $s_1=s_2=\cdots=s_8=1$ の場合はすでに坂内-小関-皆島により具体的に生成元が記述されています。私達は l 次の対称群 S_l が $R^G_{1,\dots,1}$ の上に自然に働いていることを利用して $R^G_{1,\dots,1}$ の構造を決定しようとしています。すなわち S_l の $R^G_{1,\dots,1}$ 上での表現の既約分解を決定してそれを使って $R^G_{1,\dots,1}$ の生成元を具体的に記述しようというわけです。現在の所ではまだ完全に完了しているわけではありませんがほぼ完成に近づきつつ あります。以下にこれまでに得られている結果を述べます。

まずここでもう少し記号を導入します。以後変数の個数が $2l$ （すなわち$x_1, y_1, \ldots, x_l, y_l$ ）の多項式環の中で $R_{1,\ldots,1}$ を考えることにします。

$\Omega = \{1, \ldots, l\}$,

任意の Ω の部分集合 I に対して $x_I = \prod_{i \in I} x_i \prod_{i \notin I} y_i$,

$X_d = \{I \subseteq \Omega \mid |I| = d\}$,

$\mathbf{a}^{(d)} = (a_I)_{I \in X_d}$, $\mathbf{b}^{(d)} = (b_I)_{I \in X_d}$, etc., で X_d の元で添え字づけられた $\binom{l}{d}$ 次元の縦ベクトルを表わします。

$\mathbf{x}^{(d)} = (x_I)_{I \in X_d}$ は $I(\in X_d)$- 成分が x_I のd 次元ベクトル, $\mathbf{e}_I^{(d)} = (\delta_{I,J})_{J \in X_d}$ は I 成分が 1 の d 次元単位ベクトルを意味します。

この時 $R_{1,\ldots,1}$ の関数 f は $\mathbf{a}^{(d)}, \mathbf{x}^{(d)}$, $d = 0, 1, \ldots, l$ を 使って次の様に表わせます。

$$f = \sum_{d=0}^{l} \mathbf{a}^{(d)} \cdot \mathbf{x}^{(d)}$$

ただし $\cdot$ は d 次元ベクトル空間の通常の内積を表わします。

l 点集合の d 点部分集合からなる Johnson association scheme $J(l, d)$ の第一及び第二 固有行列を各々 $P^{(d)} = \left(P_j^{(d)}(i)\right)$, $Q^{(d)} = \left(Q_j^{(d)}(i)\right)$ で、隣接行列及び idempotens を各々 $\{A_i^{(d)}, 0 \le i \le d\}$, $\{E_i^{(d)}, 0 \le i \le d\}$ で表わします。

$B_r^{i,j}$ は行を X_i で、列を X_j で添え字づけられた $\binom{l}{i} \times \binom{l}{j}$ 行列で $|I| = i$, $|J| = j$ に対して(I, J) 成分は

$$|I \cap J| = r \text{ の時} \quad (B_r^{i,j})_{I,J} = 1,$$
$$|I \cap J| \neq r \text{ の時} \quad (B_r^{i,j})_{I,J} = 0,$$

で定義します。従って $B_r^{d,d} = A_{d-r}^{(d)}$ となります。

$K_j^{(d)}$ を Krawtchouk 多項式とします。

上記の記号に関する具体的な定義は [1] を参照してください。

群 G の定義によりもし $f = \sum_{d=0}^{l} \mathbf{a}^{(d)} \cdot \mathbf{x}^{(d)}$ が $R_{1,\ldots,1}^G$ に含まれているならば $\mathbf{a}^{(d)} = 0$ が任意の $d \not\equiv 0 \pmod 4$ に対してなりたつことは容易に分かります。私達は次の結果を得ました。 まず不

変式論の手法（[6]）を使うと次の命題がすぐ証明できます。

命題 $I \in X_d,\ d \equiv 0(\mathrm{mod}\ 4)$ に対して $f_I = x_I + x_{Ic} + \sum_{|J|\equiv 0(\mathrm{mod}\ 4)} (-1)^{|J\cap I|} x_J$ と定義すると $\{f_I \mid I \in X_d,\ d = 0, \ldots, \frac{l}{2}\}$ は $R^G_{1,\ldots,1}$ を張る。

命題で定義した関数を

$$f_I = \sum_{d=0}^{l} \mathbf{a}_I^{(d)} \cdot \mathbf{x}^{(d)}$$

とベクトルで表わすと各ベクトルは次の様に与えられます。

$|I| = \frac{l}{2}$ の時

$$\begin{cases} \mathbf{a}_I^{(\frac{l}{2})} &= \left(B_{\frac{l}{2}}^{\frac{l}{2},\frac{l}{2}} + B_0^{\frac{l}{2},\frac{l}{2}} + 2^{2-\frac{l}{2}} \sum_{r=0}^{\frac{l}{2}} (-1)^r B_r^{\frac{l}{2},\frac{l}{2}}\right) \mathbf{e}_I^{(\frac{l}{2})} \\ \mathbf{a}_I^{(d)} &= 2^{2-\frac{l}{2}} \sum_{r=0}^{d} (-1)^r B_r^{d,\frac{l}{2}} \mathbf{e}_I^{(\frac{l}{2})}, \qquad \text{for } d \neq \frac{l}{2},\ d \equiv 0(\mathrm{mod}\ 4) \\ \mathbf{a}_I^{(d)} &= 0, \qquad \text{for } d \not\equiv 0(\mathrm{mod}\ 4) \end{cases}$$

$|I| = t,\ t \neq \frac{l}{2},\ t \equiv 0(\mathrm{mod}\ 4)$ の時

$$\begin{cases} \mathbf{a}_I^{(t)} &= \left(B_t^{t,t} + 2^{2-\frac{l}{2}} \sum_{r=0}^{t} (-1)^r B_r^{t,t}\right) \mathbf{e}_I^{(t)} \\ \mathbf{a}_I^{(l-t)} &= \left(B_0^{t,t} + 2^{2-\frac{l}{2}} \sum_{r=0}^{t} (-1)^r B_r^{l-t,t}\right) \mathbf{e}_I^{(t)} \\ \mathbf{a}_I^{(d)} &= 2^{2-\frac{l}{2}} \sum_{r=0}^{d} (-1)^r B_r^{d,t} \mathbf{e}_I^{(t)}, \quad d \neq t,\ d \equiv 0(\mathrm{mod}\ 4) \\ \mathbf{a}_I^{(d)} &= 0, \qquad \text{for } d \not\equiv 0(\mathrm{mod}\ 4) \end{cases}$$

上の命題に挙げた関数達は互いに一次独立ではありません。しかし $J(l,d)$ の idempotents $E_i^{(d)}, 0 \leq i \leq d$ による $\mathbb{C}^{\binom{l}{d}}$ の projection $E_i^{(d)}\mathbb{C}^{\binom{l}{d}}$ 達の上に S_l が既約に働いていることより S_l の $R^G_{1,\ldots,1}$ 上の表現の既約分解の中に現われる既約表現は $E_i^{(\frac{l}{2})}\mathbb{C}^{\binom{l}{\frac{l}{2}}}$ ただし i は $\frac{l}{2}-2$ 以外の偶数 又は $\frac{l}{2}-1, \frac{l}{2}-3, \frac{l}{2}-5, \frac{l}{2}-7, \frac{l}{2}-11$ 以外の奇数 に対応するものだけであることがわかります。一般の場合には現われてくる表現の重複度の計算はまだ完了しておりませんが次に l が小さい時の例を挙げておきます。

以下では χ を S_l の $R^G_{1,\ldots,1}$ 上の表現, χ_i を $J(l,\frac{l}{2})$ の idempotents $E_i^{(\frac{l}{2})}$ に対応する S_l の既約表現とします。

(1) $l = 8$ の場合([2]参照）。

$\chi = \chi_0 + \chi_4$

(2) $l=16$ の場合。

$\chi=\chi_0+\chi_2+\chi_4+\chi_8$

(3) $l=24$ の場合。

$\chi=2\chi_0+\chi_2+\chi_3+\chi_4+\chi_6+\chi_8+\chi_{12}$

(4) $l=32$ の場合。

$\chi=2\chi_0+\chi_2+\chi_3+2\chi_4+\chi_6+\chi_7+\chi_8+\chi_{10}+\chi_{12}+\chi_{16}$

具体的に G- 不変な関数は次の様に与えられます。

$l=8$ の場合。

$R_8^G = R_{1,\dots,1}^G$ は次の二つの関数達に対称群 S_8 を作用させて得られる関数達の一次結合によって与えられる。

(1) $(x_\emptyset+x_\Omega)+\frac{1}{4}\sum_{|I|\equiv 0(\mathrm{mod}\ 4)} x_I$,

(2) 各単項 x_J の係数が次の様に定義される関数。

$|J|\not\equiv 0\ (\mathrm{mod}\ 4)$ の時; 0

$|J|=0,\ 8$ の時; $\frac{1}{4}\sum_{i=0}^{4} Q_4^{(4)}(i)\binom{4}{i}^2$

$|J|=4,\ |J\cap\{1,\dots,4\}|=t$ の時; $2Q_4^{(4)}(t)+\frac{1}{4}\sum_{i=0}^{4} Q_4^{(4)}(i)K_{4-i}^{(4)}(t)K_i^{(4)}(4-t)$

上の (1) の関数は S_8 不変です。又 (2) の関数に S_8 を作用させて得られる関数達は 14 次元部分空間を張りますそして S_8 の 14 次元の既約表現空間をあたえます。この様にして R_8^G の関数は全て上記の二つの関数達から得られます。

$l=16$ の場合。

$R_{16}^G = R_{1,\dots,1}^G$ は次の四つつの関数達に対称群 S_{16} を作用させて得られる関数達の一次結合によって与えられる。

(1) $(x_\emptyset+x_\Omega)+\frac{1}{64}\sum_{|I|\equiv 0(\mathrm{mod}\ 4)} x_I$,

(2_1) 各単項 x_J の係数が次の様に定義される関数。

$|J| \not\equiv 0 \pmod 4$ の時; $\quad 0$

$|J| = 0,\ 16$ の時; $\quad \dfrac{1}{64}\displaystyle\sum_{i=0}^{4} Q_2^{(4)}(i)\binom{4}{i}\binom{12}{i}$

$|J| = 4,\ |J \cap \{1,\dots,4\}| = t$ の時; $\quad Q_2^{(4)}(t) + \dfrac{1}{64}\displaystyle\sum_{i=0}^{4} Q_2^{(4)}(i)K_{4-i}^{(4)}(t)K_i^{(12)}(4-t)$

$|J| = 12,\ |J \cap \{1,\dots,4\}| = 4-t$ の時; $\quad Q_2^{(4)}(t) + \dfrac{1}{64}\displaystyle\sum_{i=0}^{4} Q_2^{(4)}(i)K_{4-i}^{(4)}(t)K_i^{(12)}(4-t)$

$|J| = 8,\ |J \cap \{1,\dots,4\}| = t$ の時; $\quad \dfrac{1}{64}\displaystyle\sum_{i=0}^{4} Q_2^{(4)}(i)K_{4-i}^{(4)}(t)K_i^{(12)}(8-t)$

(2_2) 各単項 x_J の係数が次の様に定義される関数。

$|J| \not\equiv 0 \pmod 4$ の時; $\quad 0$

$|J| = 0,\ 16$ の時; $\quad \dfrac{1}{64}\displaystyle\sum_{i=0}^{4} Q_4^{(4)}(i)\binom{4}{i}\binom{12}{i}$

$|J| = 4,\ |J \cap \{1,\dots,4\}| = t$ の時; $\quad Q_4^{(4)}(t) + \dfrac{1}{64}\displaystyle\sum_{i=0}^{4} Q_4^{(4)}(i)K_{4-i}^{(4)}(t)K_i^{(12)}(4-t)$

$|J| = 12,\ |J \cap \{1,\dots,4\}| = 4-t$ の時; $\quad Q_4^{(4)}(t) + \dfrac{1}{64}\displaystyle\sum_{i=0}^{4} Q_4^{(4)}(i)K_{4-i}^{(4)}(t)K_i^{(12)}(4-t)$

$|J| = 8,\ |J \cap \{1,\dots,4\}| = t$ の時; $\quad \dfrac{1}{64}\displaystyle\sum_{i=0}^{4} Q_4^{(4)}(i)K_{4-i}^{(4)}(t)K_i^{(12)}(8-t)$

(3) 各単項 x_J の係数が次の様に定義される関数。

$|J| \not\equiv 0 \pmod 4$ の時; $\quad 0$

$|J| = 0,\ 16$ の時; $\quad \dfrac{1}{64}\displaystyle\sum_{i=0}^{8} Q_8^{(8)}(i)\binom{8}{i}^2$

$|J| = 4,\ |J \cap \{1,\dots,8\}| = t$ の時; $\quad \dfrac{1}{64}\displaystyle\sum_{i=0}^{8} Q_8^{(8)}(i)K_{8-i}^{(8)}(t)K_i^{(8)}(4-t)$

$|J| = 12,\ |J \cap \{1,\dots,8\}| = 8-t$ の時; $\quad \dfrac{1}{64}\displaystyle\sum_{i=0}^{8} Q_8^{(8)}(i)K_{8-i}^{(8)}(t)K_i^{(8)}(4-t)$

$|J| = 8,\ |J \cap \{1,\dots,8\}| = t$ の時; $\quad 2Q_8^{(8)}(t) + \dfrac{1}{64}\displaystyle\sum_{i=0}^{8} Q_8^{(8)}(i)K_{8-i}^{(8)}(t)K_i^{(8)}(8-t)$

上の (1) の関数は S_{16} 不変です。 (2_1) の関数を S_{16} で動かすと 104 次元部分空間を張ります、そしてS_{16} の 104 次元の既約表現空間を与えます。 また (2_2) の関数を S_{16} で動かすと 1260 次元部分空間を張ります、そして S_{16} の 1260 次元の既約表現空間を与えます。(3) の関数を S_{16} で動かすと 1430 次元部分空間を張ります、そしてS_{16} の 1430 次元の既約表現空間を与えます。この様にして R_{16}^G の関数は全て上記の四つの関数達から得られます。

参考文献

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

[2] E. Bannai, S. Minashima and M. Ozeki, *On Jacobi forms of weight 4*, preprint.

[3] E. Bannai and M. Ozeki, *Construction of Jacobi forms from certain combinatorial polynomials*, to appear in Proc. Japan Acad..

[4] M. Broué and M. Enguehard, *Polynômes des poids de certains codes et fonctions thêta de certains réseaux*, Ann. Sci. Ecole Nolm. Sup. 5 (1972), 157–181.

[5] A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, Actes, Congres intern. Math. 3 (1970), 211–215.

[6] F. J. MacWilliams, C. L. Mallows and N. J. A. Sloane, *Generalizations of Gleason's theorem on weight enumerators of self-dual codes*, IEEE Trans. Inf. Th. IT 18 (1972), 794–805.

[7] M. Ozeki, *Determination of the ring of simultaneous invariants for a group associated with Macwilliams identity*, to appear in 数理研講究録.

[8] M. Ozeki, *On the notion of Jacobi polynomials for codes*, to appear in Proc. Cambridge Philos. Soc..

[9] I. Schur, *Vorlesungen über Invarianten theorie*, Springer, 1968.

[10] G. C. Shephard and J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math 6 (1954), 273–304.

Self Dual 群についての2,3の話題

奥山哲郎 (北教大・旭川)
花木章秀 (山梨大・工)

0.

Self dual 群の概念は、(ある種の) 可換な association schemes の研究の過程で生じてきたものである。それは、association schemes の理論と、数理物理学における共形場理論や link の invariant に関わる spin model の理論との関連で、興味深い位置にあるようである ([1], [7]) が、例がほとんどないのが現状である。Self dual 群の背景について詳しく知らない無節操な立場からであるが、問題3.12 [1] に関連して、新しい self dual 群の例を報告する。

G を有限群, $\{C_i\}$, $\{\chi_i\}$ $1 \le i \le k$ をそれぞれ、G の共役類, 複素既約指標の集合とし, $x_i \in C_i$ をとる。

定義 G が self dual $\Leftrightarrow$ 適当に番号付けをして

$$|C_i|\chi_j(x_i)/\chi_j(1) = \chi_i(1)\chi_i(x_j) \quad \forall i,j$$

G が self dual であれば、(その番号付けで) 次が成り立つ。

(0.1) $\chi_i(1)^2 = |C_i| \quad \forall i$

(0.2) $|C_i|^{1/2}\hat{C}_i \mapsto \chi_i$ は $Z(\mathbb{C}G) \cong \mathrm{Char}_{\mathbb{C}}(G)$ ($\mathbb{C}$-多元環同型) を与える。

(0.3) $Z(\mathbb{C}G)$ において基底 $\{|C_i|^{1/2}\hat{C}_i\}$ に関する構造定数は非負整数。

self dual 群に、特に、興味をもつわけだが、条件 (0.1) あるいは (0.3) をもつ群も "状況の良い" 可換な association schemes に関連している ([1])。また、条件 (0.2) は self dual であるための十分条件でもあるかという問題が考えられている ([7], p339)。

Gが可換であれば、いつも self dual である。非可換な self dual 群の最小位数は 64 で 10個 (例えば Siz(8) の 2-Sylow 群) ある ([7])。講演者の知るこれまでの self dual 群の例はこれらだけである。

条件(0,1)をもつ群の family が [4] で構成されている。

1.

最初に self dual 群についての次の事実を述べる。それは 清田正夫 氏による「条件(0,1)をもつ群は中零群ではないか」という問題に触発されて考えたものである。

定理1. Gが self dual であれば 中零群で、その各 Sylow 部分群も self dual となる。

self dual 群の定義は、見た目に(表現論の) block 理論を適用したくなるもので、実際、次のような議論を経て定理が証明される。素数 p をひとつ固定し、Gの(p-)blocks を考える。Gを self dual とし、§0の記号を用いる。

補題1. Gの blocks は、すべて full defect. これを用いて

補題2. χ_iが主block に属し、$(\chi_i(1), p) = 1$ なら $\chi_i(1) = 1$ を得る。

これから、Gは p-中零となることが従う。(pは任意から Gは中零) Gの p-Sylow 部分群が self dual であることは、次より導かれる。

補題3. χ_iが p-元なら、χ_iは主 block に属す。

詳しくは [6] を参照されたい。

清田氏より、上の議論は、self dual の定義の等式を、Gの分解体における代数的整数の環での素イデアル $\mathfrak{P}$ 上 p を法とする合同式におきかえても、大部分実行できることを注意いただいた。つまり、

定理(清田) Gにおいて、$|C_i| \chi_j(x_i)/\chi_j(1) \equiv \chi_i(1)\chi_i(x_j) \pmod{\mathfrak{P}}$ $\forall i, j$ とする。このとき、$G = O_p(G) \times O_{p'}(G)$ で、$O_p(G)$, $O_{p'}(G)$ も同じ条件をもつ。

2.

この節では、[4]における条件(0,1)をもつ群の構成を真似て、self dual群の構成を考える（詳しくは[5]を参照）。

qを素数巾、sを正の整数　$\langle\theta\rangle = Gal(GF(q^s)/GF(q))$ とする。
正の整数 ℓ に対し

$G = G(\ell, q^s, \theta) = \{u(a_1,\cdots,a_\ell)\ ;\ a_i \in GF(q^s)\}$ とおき、積を次で決める。

$u(a_1,\cdots,a_\ell)\,u(b_1,\cdots,b_\ell) = u(c_1,\cdots,c_\ell)$, ここで

$$c_i = a_i + \sum_{k=1}^{i-1} a_{i-k}^{\theta^k} b_k + b_i \qquad (1 \le i \le \ell)$$

次の仮定を考える。

(2.1)　ℓはsのどの素因子より小さい。

(2.2)　$(q, s) = 1$

(2.3)　$(q-1, s) = 1$

定理2.　仮定(2.1)～(2.3)のもとで、次が成り立つ。

(1)　Gは直既約、class ℓの巾零群、$|G| = q^{s\ell}$

(2)　Gは条件(0,1), (0,3)をみたす。

(3)　Gがself dualであれば　$\ell \le p$　($p = char.\,GF(q)$)

(4)　$\ell \le p-1$, $\ell = s-1$であれば、Gはself dual（このとき、上の仮定とあわせ、$\ell \le p-2$, s：素数となる必要がある）

上の定理は、共役類、既約指標をすべて書きあげることによって証明される。指標表が完全に出来ているから、self dualであるための必要十分条件 ℓ, q, s, θ の言葉で書けるはずと思うが、うまくいっていない。$\ell = 1$のときは可換群であるから、除外して、まず、$G(2, q^s, \theta)$について実行したいと思っている。

$G(2, 2^s, \theta)$, s：odd はいわゆるSuzuki型2-群（のひとつ）である。これが一般にself dualかどうかも講演者は確認できないが、次の言い換えができ、$s \ge 5$では、ならない気がする。

注意 1.

(1) $G(2,2^s,\theta)$ が self dual $\Leftrightarrow {}^\exists\alpha\in GL(_{GF(2)}GF(2^s))$ s.t. $\sigma^2=id.$

ここで、σ は $GF(2^s)$ 上の置換で、$\sigma(\lambda)=\alpha(\lambda)^{\sum_{i=0}^{\frac{1}{2}(s-3)}\theta^{2i+1}}$, $\lambda\in GF(2^s)$ と定義されるもの。　　同じ記号で、

(2) $G(2,2^s,\theta)$ が条件(0,2)をもつ $\Leftrightarrow {}^\exists\alpha\in GL(_{GF(2)}GF(2^s))$ s.t. $\sigma^2\in GL(_{GF(2)}GF(2^s))$.

3.

この節では、[7]に従って、もうひとつの self dual 群の構成法を述べる。

q を奇素数の中、M を $GF(q)$ 上 $n=2m+1$ $(m\geq 1)$ 次元ベクトル空間

$\Lambda(M)=\oplus_{i=0}^{n}\Lambda^i(M)$ を M の交代多元環とする。さらに

$G=G(M)=\Lambda^{od}(M)\times\Lambda^{ev}(M)$, $\Lambda^{od}(M)=\oplus_{i=1}^{m}\Lambda^{2i-1}(M)$, $\Lambda^{ev}(M)=\oplus_{i=1}^{m}\Lambda^{2i}(M)$

とおく。($\Lambda^{2m+1}(M)$, $\Lambda^0(M)$ をそれぞれ含めていない)

$G\ni(a,x)$, (b,y)　　$a,b\in\Lambda^{od}(M)$, $x,y\in\Lambda^{ev}(M)$ に対し、

$(a,x)(b,y)=(a+b,\ ab+x+y)$ と積を定義する。

定理 3.

(1) G は直既約で class 2 の中要群。 $|G|=q^{2(2^{2m}-1)}$

(2) G は self dual

$G(M)$ の共役類のサイズ、既約指標の数値、それらの個数を書きあげることは出来ていない。Self dual であることの証明は、既約指標を fully ramified な正規部分群の指標と関連づけて実行される(詳しくは[7]を参照されたい)。

既約指標の次数すら、計算できていないが、$\dim M=2m+1$ $(m\geq 2)$ のとき、$1, q, \cdots, q^m, q^{2^{2m-2}}$ などが $G(M)$ の既約指標の次数として現れる。§2 の $G(2,q^s,\theta)$ の既約指標の次数は $1, q^{\frac{1}{2}(s-1)}$ のみである。したがって、$\dim M\geq 5$ のとき $G(M)$ は §2 の群のいずれとも非同型である。

注意2

(1) $\dim M = 2m+1$ $(m \geq 1)$ のとき、$q_0 = q^{1/3(2^{2m}-1)}$ とおくと、$G(M)$ と $G(2, q_0^3, \theta)$ は同じ位数をもち、(ある条件のもとで) いずれも self dual となる群である。"群論的に同じ系統" が気になるが、これについて、P. Hall による isoclinism の概念が有効であるかもしれない。[3] にあるように 群の isoclinism は条件(0.1)を保存する。ただ、一般に isoclinism は self dual の性質を保存せず (花木による例がある)、より精密な概念が必要となろう。

(2) q が2の中のときも 記述が面倒だが、同じような群を構成できる。そのときの一番"小さい" $q=2$, $\dim M = 3$ の場合は 位数64で Suz(8) の 2-Sylow群とは 非同型なものである。

参考文献

[1] 坂内英一, 代数的組合せ論 - アソシエーションスキームの最近の話題 - , 数学45, (1993), 55-75

[2] E. Bannai, Association schemes and fusion algebras (an introduction), J. Alg. Comb. 2 (1993), 327-344

[3] 花木章秀, 有限群の共役類の元の数と既約指標の次数とのある条件について, 第10回代数的組合せ論シンポジウム報告集 (1992, 成阜) 157-164

[4] A. Hanaki, A condition on length of conjugacy classes and character degrees, to appear in Osaka J. Math.

[5]. A. Hanaki and T. Okuyama, Groups with some combinatorial properties, submitted to Osaka J. Math.

[6]. T. Okuyama, Self dual groups are nilpotent, (preprint)

[7] T. Okuyama, A construction of self dual groups, (in preparation)

基本表現のウェイトベクトルとシェーア函数

山田裕史　（都立大数学）
（YAMADA, Hiro-Fumi）

§0　はじめに

タイトルの"基本表現"とはアフィンリー環のbasic表現のことで、最高ウェイトをもつ既約な表現のうち、いちばん簡単なものです。具体的な定現もふくめて20年ぐらい前からくわしく調べられており、今更何を、という感じがしないでもありませんが、最近いくつかのアフィンリー環の基本表現の多項式環上の定現について、ちょっとおもしろい現象をみつけましたので、それについて報告いたします。これは、東京商船大の有木進氏と、都立大物理の学生、中島達洋（タツヒロ）氏との共同研究です。

§1　$A_1^{(1)}$型アフィンリー環の基本表現

この節では最も簡単なアフィンリー環である$A_1^{(1)}$の基本表現を Lepowsky - Wilson に従って構成します。

$\mathring{\mathfrak{g}} = sl(2,\mathbb{C})$とし、これを$\mathring{\mathfrak{g}} = \mathring{\mathfrak{g}}_{\underline{0}} \oplus \mathring{\mathfrak{g}}_{\underline{1}}$と分解します。ただし$\mathring{\mathfrak{g}}_{\underline{0}} = \mathbb{C}Y_{\underline{0}}$, $\mathring{\mathfrak{g}}_{\underline{1}} = \mathbb{C}Y_{\underline{1}} \oplus \mathbb{C}Z$;

$Y_{\underline{0}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $Y_{\underline{1}} = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$, $Z = \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}$ です。

こて無限次元リー環 $\mathfrak{g}$ を

$$\mathfrak{g} := \sum_{j\in\mathbb{Z}} T^j \otimes \mathfrak{g}_{\bar{j}} \oplus \mathbb{C}c \oplus \mathbb{C}d_0$$

とおきます。ここで積は次のように定義されます。

$$\begin{cases} [T^j\otimes X,\ T^i\otimes Y] = T^{i+j}\otimes [X,Y] + \frac{1}{2} j\,\mathrm{tr}(XY)\,\delta_{i+j,0}\,c \\ [d_0,\ T^j\otimes X] = jT^j\otimes X \\ [c,\ \mathfrak{g}] = 0 \end{cases}$$

ここで $X, Y \in \mathring{\mathfrak{g}}$ で $[X,Y] = XY - YX$ はいうまでもないことです。今、

$$\mathfrak{s} := \sum_{j:\,\mathrm{odd}} \mathbb{C}(T^j\otimes Z) \oplus \mathbb{C}c \oplus \mathbb{C}d_0$$

とおくと、これは $\mathfrak{g}$ のリー部分環になります。すでにわかるように $\mathfrak{s}$ は無限次元ハイゼンベルグ部分環と呼ぶにふさわしいものです。$\mathfrak{g}$ の表現を構成するのに、まず $\mathfrak{s}$ から片づけましょう。無限変数の多項式環 $V = \mathbb{C}[t_j\,;\, j\geq 1,\ \mathrm{odd}]$ を準備します。$\mathfrak{s}$ の V への作用 ρ を

$$\begin{cases} \rho(T^j\otimes Z) = \begin{cases} \partial/\partial t_j & (j\geq 1) \\ (-j)t_{-j} & (j\leq -1) \end{cases} \\ \rho(c) = 1 \quad (=\mathrm{identity}) \\ \rho(d_0) = \sum_{\substack{j\geq 1 \\ \mathrm{odd}}} j t_j \frac{\partial}{\partial t_j} \end{cases}$$

のように定義することができます。gの"残り"の部分が、Vに"頂点作用素"として作用する、というのがLepowsky とWilsonの発見でした。すなわち、今pを不定元として、

$$X(p) := \sum_{k\in\mathbb{Z}} (T^k \otimes Y_{\underline{k}})\, p^{-k}$$

という母函数を考えます。このとき、

$$\rho(X(p)) = -\frac{1}{2} e^{2\xi(t,p)} e^{-2\xi(\tilde{\partial}, p^{-1})}$$

ただし、 $\xi(t,p) = \sum_{\substack{j\geq 1 \\ \text{odd}}} p^j t_j$, $\xi(\tilde{\partial}, p^{-1}) = \sum_{\substack{j\geq 1 \\ \text{odd}}} p^{-j} \frac{1}{j} \frac{\partial}{\partial t_j}$

とすれば、gのV上の作用(表現)が得られるわけです。gの作用で既にVは既約になっているのでgの表現(ρ, V)は既約です。この表現が$A_1^{(1)}$の基本表現と呼ばれるものです。正確に言えば表現(ρ, V)は基本表現の一つの実現です。基本表現そのものは抽象的に次のように定義されます。

$$\begin{cases} L(\Lambda_0) = U(g)v_0 & \text{既約.} \\ \mathfrak{n}_+ v_0 = 0 \\ H v_0 = \langle \Lambda_0, H\rangle v_0 & \forall H \in \mathfrak{h} \\ \text{ただし} \quad \langle \Lambda_0, \alpha_0^\vee\rangle = 1, \ \langle \Lambda_0, \alpha_1^\vee\rangle = 0 \end{cases}$$

v_0を最高ウェイトベクトル、Λ_0を最高ウェイトといいます。上の(ρ, V)という実現では$v_0 = 1 \in V$と取れています。

こて $\{\alpha_0, \alpha_1\}$ を $A_1^{(1)} = \mathfrak{g}$ の単純ルートとします。上にでてきた $\{\alpha_0^\vee, \alpha_1^\vee\}$ とは次のような双対の関係にあります。

$$\langle \alpha_j, \alpha_i^\vee \rangle = a_{ij} \quad \text{ただし} \quad (a_{ij})_{i,j=0,1} = \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$$

$\delta = \alpha_0 + \alpha_1$ とおいて、基本虚ルートと呼びます。このとき $\mathfrak{g}$ のルート系は次で与えられます。

$$\Delta = \{ n\delta \pm \alpha_1 ; n \in \mathbb{Z} \} \amalg \{ n\delta ; n \in \mathbb{Z} \setminus \{0\} \}$$

↑ 実ルート　　↑ 虚ルート

また全てのルートは、重複度1を持っています。つまり、ルート空間は全て1次元ということです。

アフィンリー環には上のようなルート系とか、ワイル群などの表現の構造を知るための道具がきちんとそろっています。$\mathfrak{g} = A_1^{(1)}$ のワイル群はいわゆる無限二面体群になっています。すなわち、

$$W = \langle r_0, r_1 \rangle \Big/ r_0^2 = r_1^2 = 1 \quad \subset GL(\mathfrak{h}^*)$$

ここで r_i は鏡映で $\lambda \in \mathfrak{h}^*$ に対して

$$r_i(\lambda) = \lambda - \langle \lambda, \alpha_i^\vee \rangle \alpha_i \quad (i = 0, 1)$$

で定義されます。単純ルートのワイル群軌道に乗っている、ルートを実ルート、そうでないルートを虚ルートといいます。

有限次元単純リー環の場合には実ルートしかないことは、よく知られています。

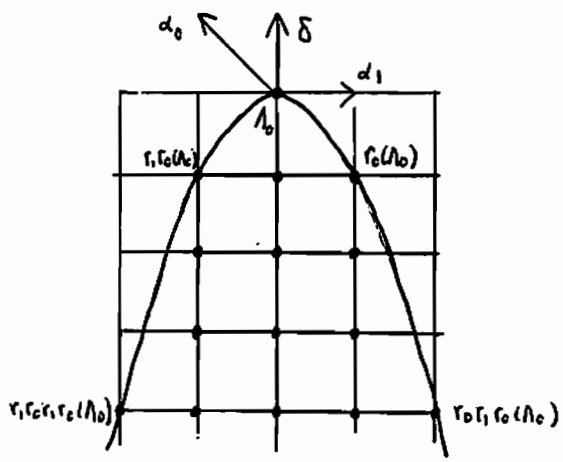
次にウェイトについて述べましょう。$\lambda \in \mathfrak{h}^*$がウェイトであるとは

$$\exists v \neq 0 \quad Hv = \langle \lambda, H \rangle v \qquad \forall H \in \mathfrak{h}$$

と定義します。$A_1^{(1)}$の基本表現$L(\Lambda_0)$のウェイトについては、次が基本的です。Pをウェイトの全体とすると、

$$P = \{\Lambda_0 - q\delta + p\alpha_1 \mid p, q \in \mathbb{Z},\ q \geq p^2\}.$$

これを絵であらわすと次のようになります。



最高ウェイトΛ_0を最高点とする放物線$q = p^2$の下に位置する格子点がウェイトをあらわしています。放物線上のウェイトは最高ウェイトΛ_0を通るワイル群の軌道であり、δだけ足すと（真上に上がると）もはやウェイトではないという

意味で"極大ウェイト"と呼ばれます。この放物線とδの整数倍だけ真下に平行移動したものもワイル群の軌道になっています。ウェイトの重複度、すなわち、ウェイト空間の次元はワイル群の作用で変わりませんから、各放物線上のウェイトは一斉に同じ重複度をもっています。すなわち、重複度は、極大ウェイトからδの何倍だけ下がったか、ということだけで決まってしまいます。Weyl-Kac の指標公式によれば、各極大ウェイト Λ に対して

$$\mathrm{Mult}(\Lambda - n\delta) = p(n) \quad (= n \text{ の分割数})$$

がわかります。

なお以上の事実に関しては V. Kac の教科書 [K] が標準的な文献です。

§2 シューア函数

我々の最初の問題は $\mathfrak{g} = A_1^{(1)}$ の基本表現 $L(\Lambda_0)$ を§1で示したように多項式環 V 上に実現したときの各ウェイトベクトルを具体的に書き下すことです。そのために、一般線型群の通常既約指標であるシューア函数を少し書き直しましょう。今、$\lambda = (\lambda_1, \lambda_2, \cdots, \lambda_n)$ を N の分割とします。すなわち λ はサイズが N のヤング図形です。λ に付随するシューア函数 $S_\lambda(t)$ を次のように定義します：([M])

$$S_\lambda(t) = \sum_\nu \chi_\lambda(\nu) \frac{t_1^{\nu_1} t_2^{\nu_2} \cdots t_N^{\nu_N}}{\nu_1!\,\nu_2! \cdots \nu_N!}$$

ここで和はサイズ N の分割 $\nu = (1^{\nu_1} 2^{\nu_2} \cdots N^{\nu_N})$, すなわち, $\nu_1 + 2\nu_2 + \cdots + N\nu_N = N$, $\nu_j \geq 0$ $\forall j = 1, \cdots, N$ を渡ります。また $\chi_\lambda(\nu)$ は対称群 $\mathfrak{S}_N$ の既約指標の値で, 既約表現 λ の指標がサイクルタイプが ν の共役類の上でとる値です。本来のシューア函数は一般線型群の元の固有値 $x_1, x_2, \cdots$ の対称函数であるわけですが, ここでは中和

$$t_j = \frac{1}{j}(x_1^j + x_2^j + \cdots) \qquad \forall j \geq 1$$

を用いた表示を採用します。この表示から $S_\lambda(t)$ は次数が $|\lambda| = N$ に等しい有次係数多項式になっていることがすぐにわかります。ただし $\deg t_j = j$ と勘定します。

後に重要な働きをする "2-被約シューア函数" も, 今ここで定義してしまいましょう。

$$S_\lambda^{(2)}(t) = S_\lambda(t)\Big|_{t_2 = t_4 = \cdots = 0} \in V$$

つまり, シューア函数において偶数変数を全て 0 においたものです。Murnaghan - Nakayama の公式によればヤング図形 λ が高さ 2 の hook (2-hook) を持たなければ

$$S_\lambda(t) = S_\lambda^{(2)}(t)$$

となります。このような λ を, 対称群の モジュラー表現論の

用語をつかって"2-core"と呼びましょう。実際には2-coreは $r=0,1,2,\cdots$ に対して

$$\kappa_r = (r, r-1, r-2, \cdots, 2, 1) \longmapsto \frac{r(r+1)}{2}$$

しかないことがすぐにわかります。($\kappa_0 = \phi$) 80年代前半の伊達-神保-柏原-三輪[DJKM]の発見の一つは、次のようなものでした。「$A_1^{(1)}$の基本表現(ρ, V)の極大ウェイトベクトルは$S_{\kappa_r}(t)$ $(r=0,1,2,\cdots)$でよろしい、これらはKdV方程式系の有次多項式解(τ-函数)をつくす。」脇本[IW]はVirasoro代数の表現を使って$S_{\kappa_r}(t)$の特徴付けを行いました。

極大ウェイトベクトルはこれで決定されましたが、一般のウェイトベクトルはどのように記述されるのでしょうか。このためにヤング図形の"2-quotient"をOssonの講義録[O]に従って導入します。分割$\lambda=(\lambda_1,\cdots,\lambda_n)$で必要ならば尻尾に0(ゼロ)をつけてnを偶数にしておきます。λの"β-set"又は"マヤ図形"を $B=(\beta_1,\cdots,\beta_n)$, $\beta_j=\lambda_j+(n-j)$ とします。次に$k=0,1$に対して

$$B[k] = \{\gamma^{(k)} \in \mathbb{N};\ 2\gamma^{(k)}+k = \beta_j \quad \exists j=1,\cdots,n\}$$

とおきます。今 $B[k]=\{\gamma_1^{(k)},\cdots,\gamma_{m(k)}^{(k)}\}$ $(\gamma_1^{(k)}>\cdots>\gamma_{m(k)}^{(k)})$ としたとき

$$\lambda[k] = \{\gamma_1^{(k)}-(m^{(k)}-1),\ \gamma_2^{(k)}-(m^{(k)}-2),\ \cdots,\ \gamma_{m(k)}^{(k)}\}$$

により分割 $\lambda[k]$ $(k=0,1)$ をつくります。分割（ヤング図形）のペア $(\lambda[0], \lambda[1])$ をもとのヤング図形 λ の "2-quotient" と呼びます。また λ の 2-core λ_c を

$$\begin{cases} |B[0]| - |B[1]| = r \geq 1 \implies \lambda_c = K_{r-1} \\ |B[1]| - |B[0]| = r \geq 0 \implies \lambda_c = K_r \end{cases}$$

により定めます。2-core λ_c は λ から 2-hook を続けて抜いていって手詰りとなったときにでてくるヤング図形です。このようにして、与えられたヤング図形 λ からヤング図形の三つ組 $(\lambda_c; \lambda[0], \lambda[1])$ がつくられます。このとき

$$|\lambda| = |\lambda_c| + 2(|\lambda[0]| + |\lambda[1]|)$$

が簡単にわかります。この三つ組を $\Gamma(\lambda)$ で表わします。Γ は 1-1 対応であることが示されます。一つだけ例を挙げましょう。

$$\begin{cases} \lambda = (4,3,1,1) \\ B = (7,5,2,1) \end{cases}$$

$$\begin{cases} B[0] = (1), \quad B[1] = (3,2,0) \\ \lambda[0] = (1), \quad \lambda[1] = (1,1,0) \\ \lambda_c = K_2 = (2,1) \end{cases}$$

2-set の "abacus" をつくると見やすくなります。この例では右のようになります。

B[0]	B[1]	
0	①	← 0
②	3	← 1
4	⑤	← 2
6	⑦	← 3
8	9	← 4

こて以上の準備の下でウェイトベクトルの記述ができます。$r=0,1,2,\cdots$ に対して $S_{k_r}(t)$ とウェイトベクトルにもつ極大ウェイトを Λ_r と書くことにします。(正しい記号の使い方でないことは十分に承知しております。)

<u>命題 1</u>　ヤング図形 λ に対して $\tau(\lambda)=(k_r;\lambda[0],\lambda[1])$, $|\lambda[0]|+|\lambda[1]|=n$ とすると対応する 2-被約シェーア函数 $S_\lambda^{(2)}(t)$ はウェイト $\Lambda_r-n\delta$ に属するウェイトベクトルである。

このような形で explicit に書いてあるものは見たことはありませんが、既に知られていても、おかしくないと思います。一旦、すべてのことをフェルミオンのフォック空間に持ち込んでそこで 2-hook をつけたり取ったりする作業をくわしく見てやります。最後にボゾン-フェルミオン対応を用いて、多項式の言葉に直すことによって上の命題はホとんます。

§3　ウェイト空間の基底

上の命題1により、どのヤング図形がどのウェイト空間に住んでいるかは、わかりました。次は各ウェイト空間の基底を決定することを問題とします。

2-複射シューア函数はその名のとおり変数を落としているのでヤング図形が異なっても一次独立とは限りません。極端な話，$S^{(2)}_{\lambda}(t) = S^{(2)}_{\lambda'}(t)$ となってしまいます。ここで，λ' は λ に共役なヤング図形，すなわち転置を表わします。ついでに言っておくと $\tau(\lambda) = (\lambda_c ; \lambda[0], \lambda[1])$ のとき，$\tau(\lambda') = (\lambda_c ; \lambda[1]', \lambda[0]')$ となっています。従って基底をとる際に工夫が必要なことがわかります。

<u>命題 2</u>　$\{ S^{(2)}_{\lambda}(t) ; \tau(\lambda) = (\kappa_r ; \phi, \lambda[1]), |\lambda[1]| = n \}$ はウェイト $\Lambda_r - n\delta$ のウェイト空間の基底である。

先に述べたように $Mult(\Lambda_r - n\delta) = p(n)$ であり，上の集合はサイズが n の $\lambda[1]$ の個数，すなわち $p(n)$ 個の元から成っているので，一次独立性だけ示せばよいわけですがテクニカルなので，ここでは証明を省略します。

こて基底が決まりました。ちょっと例を挙げてみましょう。ウェイトが $\Lambda_0 - 2\delta$ のウェイト空間は $p(2) = 2$ 次元です。基底となるヤング図形は，三つ組が $(\phi ; \phi, \square\square)$ と $(\phi ; \phi, \square^2)$ に対応するもの，すなわち，$\square\square$ と $\square^2$ です。2-複射シューア函数は

$$S^{(2)}_{\square\square}(t) = \frac{1}{24} t_1^4 + t_1 t_3, \quad S^{(2)}_{\square^2}(t) = \frac{1}{8} t_1^4$$

となっています。同じウェイトに属する他の2-般対シュー了
函数は

$$S^{(2)}_{\square\!\square}(t) = \frac{1}{12}t_1^4 - t_1t_3 = S^{(2)}_{\square\square}(t) - S^{(2)}_{\square\square}(t)$$

と表わされます。一般に2-般対シュー了函数と幾つの基底
で展開したときの展開係数を問題にすることにします。結果
を述べるために一つだけ"2-sign"というものを準備します。
ヤング図形 λ の2-sign $\delta_2(\lambda)$ を $\delta_2(\lambda) = (-1)^g$ で定義
します。ただし λ から2-hookを続けて抜いていって λ_C に
至る際，g 個のタテ2-hook(日)を抜くものとします。(g の
偶奇は well-defined です。) Olsson の講義録 [O] にこのタ
イプの符号について詳しい解説があります。

<u>定理 3</u>　　$\tau(\lambda) = (\lambda_C ; \lambda[0], \lambda[1])$, $|\lambda[0]| + |\lambda[1]| = n$

のとき

$$S^{(2)}_{\lambda}(t) = (-1)^{|\lambda[0]|}\delta_2(\lambda)\sum_{\mu[1]} LR^{\mu[1]}_{\lambda[0],\,\lambda[1]}\,\delta_2(\mu)\,S^{(2)}_{\mu}(t)$$

が成立する。ただし和は $|\mu[1]| = n$ なるヤング図形 $\mu[1]$ を渡
り，μ は三つ組 $\tau(\mu) = (\lambda_C ; \phi, \mu[1])$ に対応する。また
LR はいわゆる Littlewood - Richardson 係数である。

Littlewood - Richardson係数という名前は正式に認められているのでしょうか。要するにシューア函数の積を線型化するときの係数のことです。

$$S_\lambda(t)\,S_\mu(t) = \sum_\nu LR^{\nu}_{\lambda\mu}\,S_\nu(t)$$

いいかえれば既約表現のテンソル積を既約分解するときの各既約成分の重複度のことで表現論では一般に Clebsch-Gordan の係数と呼ばれているものです。ちなみに P. A. Gordan (1837-1912, 不変式論で有名です) と Gordon とまちがえている本も見受けられます。

この定理の式はなかなか美しいのではないでしょうか。最初は $|\lambda|$ が小さいところでいくつか実験をしてみました。誰も言ってくれないから自分で言いますが、数少ない計算例から LR係数が登場していると見抜いたセンスはなかなかのものだと思います。手垢をつけてから $\tau(\lambda)=(\phi;\square,\square)$ の場合をコンピュータを使って計算し、結果がドンピシャリ合った時は感動的でした。

我々が持っている証明は有木氏によるものですが、アフィンリー環とは無関係にシューア函数の性質だけを使います。実際、我々の論文 [ANY2] では、まず定理3の公式が述べられ、その応用として基本表現のウェイトベクトルが記述される、という順番になっていますが、発見に至った

経緯はここに述べたとおりです。

§4 対称群のモジュラー表現との関係

定理3の公式は対称群の2-モジュラー表現論の公式と見ることもできる、ということを解説しましょう。2-被約シューア函数の定義と定理3の公式を見比べると、対称群の通常既約指標の値の関係式が導出されます。

$$\chi_\lambda(\nu) = (-1)^{|\lambda[0]|} \delta_2(\lambda) \sum_{\mu[1]} LR^{\mu[1]}_{\lambda[0]',\lambda[1]} \delta_2(\mu) \chi_\mu(\nu)$$

ただしここで共役類 $\nu = (1^{\nu_1} 2^{\nu_2} \cdots)$ はいわゆる "2-regular class", すなわち $\nu_2 = \nu_4 = \cdots = 0$ とみたすものです。対称群 $\mathfrak{S}_n$ の指標表とは通常既約指標の値 $\chi_\lambda(\nu)$ を $p(n) \times p(n)$ の行列の形に書いたものです。普通は $\chi_\lambda(\nu)$ を λ 行 ν 列に書き込みます。この行列において2-regular class に対応する列だけを取り出してできる $p(n)$ 行 $p(n)$ 列の行列を考えたとき、上の公式は、この行列の行の間の関係式を与えているものと見ることができます。たとえば $n=4$ では次のようになっています。

($\chi_\lambda(\nu) = \chi_{\lambda'}(\nu)$ に注意します。)

	(1^4)	(31)
▭▭	1	1
▯▭	3	0
▯▯	2	-1

行間の関係式は一目瞭然です。

このような行列を一般に $C_n^{(2)}$ と書くことにしましょう。

次に対称群の分解行列を思い出します。そもそも対称群の標数 2 の既約表現は標準的な方法で "2-regular 分割" でパラメトライズされます。ここで分割 $\lambda=(\lambda_1,\lambda_2,\cdots,\lambda_k)$ が 2-regular であるとは $\lambda_1>\lambda_2>\cdots>\lambda_k$ となっていることです。サイズが n の 2-regular 分割の個数と 2-regular class の個数が等しいことは、母函数を使って簡単に示されます。標数 0 の時に既約であった Specht 加群は標数 2 では一般には既約でなく、その組成列に既約な表現 ($\leftrightarrow$ 2-regular 分割) がいくつ現れるかを記録したものが "分解行列" です。例えば $n=4$ の分解行列は次のようになっています。

	▭▭	⊏▭
▭▭	1	
⊏▭	1	1
⊞		1
⊏⊏	1	1
▯▯	1	

一般に標数 2 の分解行列を $D_n^{(2)}$ で表わすことにします。James - Kerber の百科全書 [JK] には $n=13$ までの $D_n^{(2)}$ が載っています。

ブラウワー指標表とはその名のとおりブラウワー指標 $\varphi_\mu(\nu)$ を μ 行 ν 列に書き並んだ行列です。ここで μ は、2-regular 分割, ν は 2-regular class です。ブラウワー指標表 $B_n^{(2)}$ は従って正方行列です。しかも表現の一般論から、可逆であることもわかります。例えば $B_4^{(2)}$ は次のようになって

います。

	(1^4)	(31)
▭	1	1
田	2	-1

$B_n^{(2)}$ も [JK] に $n=10$ まで載っています。

さて以上の三種類の行列の間には

$$D_n^{(2)} B_n^{(2)} = C_n^{(2)}$$

という関係が成り立っています。我々の公式は $C_n^{(2)}$ の行間の関係式を与えるものでしたが、これより分解行列 $D_n^{(2)}$ の行間の関係式でもあるわけです。更に対称群の"岩堀-ヘッケ環" $H_n(q)$ において $q=-1$ と特殊化したもの $H_n(-1)$ の分解行列を $\widetilde{D}_n^{(2)}$ と書けば、ある三角行列で対角成分が全て1であるもの $T_n^{(2)}$ が存在して

$$D_n^{(2)} = \widetilde{D}_n^{(2)} T_n^{(2)}$$

となっていることが知られているので、結局 $\widetilde{D}_n^{(2)}$ の行間の関係式も全く同様であることがわかります。

なお q を1の中根に特殊化した岩堀-ヘッケ環の分解行列に関しては最近 Lascoux - Leclerc - Thibon の三人組が結晶基底と関連させておもしろい予想をたてていることを注意して、この節を終わります。([LLT])

§5 その他

ここまでは最も簡単なアフィンリー環である $A_1^{(1)}$ に限って話を進めてきましたが命題1, 2, 定理3はアフィンリー環 $A_{r-1}^{(1)}$ の基本表現に対して一般化されます。見る人が見れば、一般化の方法は明らかでしょう。多項式環 V は

$$V^{(r)} = \mathbb{C}[t_j ; j \geq 1,\ j \not\equiv 0 \pmod r]$$

になるし、ウェイトベクトルとして "r-被約シューア函数"

$$S_\lambda^{(r)}(t) = S_\lambda(t)\Big|_{t_r = t_{2r} = \cdots = 0} \in V^{(r)}$$

とることができます。2-core, 2-quotient はそれぞれ、modulo r で abacus をつくって "r-core", "r-quotient" と考えればよいわけです。ヤング図形 λ に対して "小さな" ヤング図形の $(r+1)$-組 $\tau(\lambda) = (\lambda_c ; \lambda[0], \lambda[1], \cdots, \lambda[r-1])$ が対応します。λ_c は r-core, $\lambda[0], \cdots, \lambda[r-1]$ は r-quotient です。ウェイト空間の基底が $\lambda[0] = \phi$ なる λ の r-被約シューア函数 $S_\lambda^{(r)}(t)$ でとれることも、容易に想像されるとおりです。定理3の公式において $\lambda[0]$ が登場し、これが $r=2$ の場合の特殊性ではないかと、最初は疑ったのですが、そしてまた $r=3$ のときにうまくいかないという、計算まちがいすら犯していたのですが、パリ, エコールノルマルの静かな中庭でしばし考えた結果、一般化できないはず

がない、と確信するに至りました。帰国後、程なくして、中島氏の努力もあり公式は証明されました。$\mathfrak{A}[0]$の転置は、見事に取り込まれていました。$r=p=$素数のときには、対称群のp-モジュラー表現の分解行列，岩堀-ヘッケ環の$q=$「1の原始p乗根」のときの分解行列の関係式を与えていることは同様にわかります。

$A_1^{(1)}$について詳しく調べる以前に中島氏と私が最初に取り上げた問題は$A_{2l}^{(2)}$と$D_{l+1}^{(2)}$の二つのタイプのアフィンリー環の基本表現を多項式環上に実現したときのウェイトベクトルを記述することでした。$A_{r-1}^{(1)}$がKP方程式系の"reduction"を統制する、というのと同じ意味において、この二つのリー環のシリーズはBKP方程式系のreductionを統制します。数年前にシェーアの"Q-函数"がBKP方程式系の奇次多項式解であることに気づいていた私はそのreductionとQ-函数の関係を調べようと思って上のような問題を設定したわけです。[NY1]において我々は結果をマヤゲームの言葉で述べましたが、その後[G]を勉強して"bar core"と"bar quotient"を使うと、よりすっきりとした形で述べられることを理解しました。この段階で初めて、もっと簡単な$A_1^{(1)}$でやってみようと思い至ったわけです。その結果、定理3のような思いがけない転回をむかえました。そうなると$A_{2l}^{(2)}$でも

同様のことができないだろうか、と考えるのは自然の成りゆきでしょう。すなわち"複約Q-函数"の線型関係式でありまた、対称群のモジュラー射影表現の分解行列の関係式であるようなものが得られるのではないでしょうか。ちなみに、$D^{(2)}_{\ell+1}$では複約Q-函数が登場しないので、ここでは問題外です。

夏休みに入ってからの集中的な議論の末、満足すべき結論が得られました。くわしくは現在準備中の論文[NY2]に譲ることにして、ここでは次のことを注意するにとどめます。$A^{(1)}_{n-1}$のとき、すなわち複約シェーア函数の線型関係式に登場したLittlewood-Richardson係数は、複約Q-函数の線型関係式においては次式で定義される係数N^Yに取ってかわられます。

$$2^{-\ell(\lambda)} Q_\lambda(t) S_\mu(t) = \sum_\nu N^Y{}_{\lambda\mu}^{\ \nu} S_\nu(t)$$

ここでλは2-regular分割、μは任意の分割、$\ell(\lambda)$はλの"長さ"です。この係数の表現論的な意味、組合せ論的な計算方法は今の私にはわかりません。

長々と世間話を書いてしまいました。この辺で筆を措いて夜明けのコーヒーでも淹れることにします。

9/7/95　5:00 AM

文献

[ANY1] S.Ariki, T.Nakajima and H.F.Yamada: Weight vectors of the basic $A^{(1)}_1$-module and the Littlewood-Richardson rule, J. Phys. A: Math. Gen. 28(1995), L357-L361.

[ANY2] ———: Reduced Schur functions and the Littlewood-Richardson coefficients, preprint.

[DJKM] E.Date, M.Jimbo, M.Kashiwara and T.Miwa: Transformation groups for soliton equations. Euclidean Lie algebras and reduction of the KP hierarchy, Publ. RIMS. 18(1982), 1077-1110.

[JK] G.James and A.Kerber: The Representation Theory of the Symmetric Groups, Addison-Wesley 1981.

[K] V.Kac: Infinite Dimensional Lie Algebras, 3rd.ed., Cambridge 1990.

[LLT] A.Lascoux, B.Leclerc and J.Y.Thibon: Une conjecture pour le calcul des matrices de decomposition des algebres de Hecke de type A aux racine de l'unite, preprint.

[M] I.G.Macdonald: Symmetric Functions and Hall Polynomials, 2nd.ed., Oxford 1995.

[NY1] T.Nakajima and H.F.Yamada: Basic representations of $A^{(2)}_{21}$ and $D^{(2)}_{l+1}$ and the polynomial solutions to the reduced BKP hierarchies, J. Phys.A: Math. Gen. 27(1994), L171-L176.

[NY2] ———: Reduced Q-functions and the basic representation of $A^{(2)}_{21}$, 準備中.

[O] J.B.Olsson: Combinatorics and Representations of Finite Groups, Lecture Notes, University of Essen, 1993.

[W] M.Wakimoto: Basic representations of extended affine Lie algebras, 数理研講究録503 (1983), 36-46.

可換不足群を持ち惰性剰余群が位数8の2面体群である主ブロックのパーフェクトアイソメトリーについて

お茶の水女子大学　宇佐美陽子

§1. 序

はじめに、Oは完備離散付値環で、商体が、標数零のK, Oを極大 ideal で割った剰余類の体が標数$p>0$のkになるものとする。K, kは、考える群に対し充分大きいとしておく。(共通の defect group (不足群) Pを持つ p-block 達を、一般に考えるに当たっては、kは代数的閉体、Kは、1の$|P|$-乗根を含むと仮定しておくと良い。)

Broué は [Br] (Definition 4.6)において、有限群の p-block のタイプについて、新しい定義を与え、"isotypy" という言葉を導入したが、この定義は、block algebra の category 同値と関連があるものである。2つの block algebra は、これらの derived module category が triangulated category として、同値で

ある時、"derived equivalent"と言う。Brouéは[Br]で、まず、2つのblockの一般指標の間の、"きれいな"bijective isometryとして、perfect isometryなる概念(つまり、それを誘導することで、各々のblockに属すO-valued class functionの間のbijectionが得られるだけでなく、更には、各々のblockに属すK-valued class functionでp-singular class上では零となるもの達の間のbijectionをも誘導できるものとする。[Br] Definition 1.4, Proposition 4.1)を導入した。そして、次の事を、証明している。2つのblockがO-algebraとして、"derived equivalent"である時に、それが指標理論へ、落ちてくる影が、とりもなおさず"perfect isometry"であるというものである。([Br] Theorem 3.1)

さて、isotypyとは、2つのblockの間に、単に、perfect isometryが存在するというだけでなく、更に、強い条件が付けられ、大雑把に言えば、localな群論的条件のついたperfect isometryの族が存在するというものである。(Definition 3.1, 3.2を見よ。)ここで、Brouéは、群Gでabelian defect group Pを持つp-block bについては、bと、$N_G(P)$におけるそのBrauer correspondent

$Brp(b)$ とは、derived equivalent であり、かつ isotypic であろうという予想を提出している。(3節の isotypic の定義、及び Broué 予想を見よ。)

本稿は、この予想に関連しており、abelian defect group P を持つ principal block (主ブロック) b について、その inertial quotient (惰性剰余群) E が特殊な群の時、b と $Brp(b)$ は、isotypic ということを証明した事を報告するものである。(4節 II. 7) ただし inertial quotient E とは、b の $C_G(P)$ での root を e とした時 $E = N_G(P,e)/PC_G(P)$ と定義されるものである。

§2. abelian defect group を持つ時の Alperin 予想, Dade 予想と perfect isometry の関係

結論

I. G の block b は、abelian defect group P を持ち b と $N_G(P)$ の block $Brp(b)$ の間に perfect isometry 存在

$\Longrightarrow$ b について Alperin 予想 ([A]) 成立。

II. G の block b は、abelian defect group P を持ち b と $N_G(P)$ の block $Brp(b)$ の間に perfect

isometry存在。同じ defect group P を持ち、その inertial quotient が b の inertial quotient E の部分群になっている一般の block についても同様に、その Brauer correspondent との間に perfect isometry が存在していると仮定。

$\Rightarrow$ b について Dade予想 (ordinary form) 成立。

(解説 I) abelian defect group P を持つ block b では Alperin の weight 予想は、簡単に、『b と Brauer correspondent $Br_P(b)$ で既約 Brauer 指標の個数が等しい』と言い換えられるので、perfect isometry の定義から、Iは、明らかである。

(解説 II) Dade予想を一般的な形で述べる為に、少し用語を準備しよう。

一般の有限群 G について $\mathrm{Irr}_K(G)$ は通常既約指標の集合とする。G での p-chain とは、G の p-subgroup の chain

$$C : \quad P_0 < P_1 < \cdots\cdots < P_n$$

のことである。radical p-chain の定義は、略すので [D] を見よ。$\mathcal{R}$ を G の radical p-chain 全体の集合、$\mathcal{R}/G$ を $\mathcal{R}$ の G-共役代表全体の集合とする。C が上の形の

時、chain の長さを n とし、$|C|$ と表す。また

$$N_G(C) = \bigcap_{i=0}^{n} N_G(P_i)$$

と定義する。ここで、任意の非負整数 d に対して、以下の性質を持つ $N_G(C)$ の既約指標の個数を考える。

$$k(N_G(C), b, d)$$

$$\underset{\text{定義}}{=} \#\left\{ \zeta \in \mathrm{Irr}_K(N_G(C)) \;\middle|\; \begin{array}{l} \zeta \in b(\zeta),\ b(\zeta)^G = b \\ d = d(b(\zeta)) - h(\zeta) \end{array} \right\}$$

ここで $b(\zeta)$ は ζ の属す block, $d(b(\zeta))$ は $b(\zeta)$ の defect, $h(\zeta)$ は ζ の高さとする。

Dade 予想 (ordinary form [D])

b : G の p-block, b の defect 正

G の maximal normal p-subgroup $O_p(G)=1$

$\Rightarrow$ $\forall$ 整数 $d \geq 0$ について

$$\sum_{C \in \mathcal{R}/G} (-1)^{|C|} k(N_G(C), b, d) = 0 \quad \cdots\cdots(1)$$

さて、IIの証明ポイントは、次の2点を示す事である。

① $\mathcal{R}/G$ に、特別な代表の取れること。

どの C でも各 p-subgroup は P に含まれ、$\zeta \in \mathrm{Irr}_K(N_G(C))$, $b(\zeta)^G = b$ ならば、$b(\zeta)$ の defect group は P になっているように選べる。

② 上のように選んだ radical p-chain で、最終項が P でないもの

$$C : P_0 < P_1 < \cdots\cdots < P_n$$

に対して末尾に、P をつけ加えた

$$C' : P_0 < P_1 < \cdots\cdots < P_n < P$$

も radical p-chain となること。

以下、②のような C について、$N_G(C) \ni \zeta$ の属す block $b(\zeta)$ と $N_G(C') = N_{N_G(C)}(P)$ の block $Br_P(b(\zeta))$ とは、Brauer の第1主定理で、1:1 に対応する。その際 $b(\zeta)$ の inertial quotient は、E の subgroup となるため、$b(\zeta)$ と $Br_P(b(\zeta))$ の間には、仮定により、perfect isometry が存在して、通常既約指標の間に、高さを維持して 1:1 対応 (perfect isometry は、一般に通常既約指標の間に高さを保って 1:1 対応をつける。[Br] Theorem 1.5) がつく。そこで d を固定したまま、C と C' の間で対応する block の組毎に考え、$|C'| = |C| + 1$ を考慮すれば、符号つきの個数和 (1) の右辺で、相殺することがわかる。

§3 isotypy の定義

isotypy の定義には、群の local な構造に関わる subpair の概念([AB])が必要となる。群Gの block $\mathfrak{b}$ は、ここでは $Z(\mathfrak{o}G)$ の原始中等元としておく。$\mathfrak{B}$ が、それに対応して unique に決まる $Z(OG)$ の原始中等元としておく。Alperin, Broué は、[AB] で $\mathfrak{b}$-subpair (Q,u) 及び、それらの包含関係を定義した。Fong, Harris [FH] は、u に対して、unique に決まる $Z(O(C_G(Q)))$ の原始中等元 $\hat{u}$ を使って、$\hat{\mathfrak{b}}$-subpair $(Q,\hat{u})$ を定義し、包含関係も対応する $\mathfrak{b}$-subpair の方の包含関係で定義し、$\hat{\mathfrak{b}}$-element も、$\mathfrak{b}$-element をなぞって定義した。従って、$\mathfrak{b}$ の defect group が P, $C_G(P)$ での root が e の時、(P,e) が maximal $\mathfrak{b}$-subpair となり、同時に、$(P,\hat{e})$ が maximal $\hat{\mathfrak{b}}$-subpair となり、また $Q \subseteq P$ であれば $(Q,b_Q) \subseteq (P,e)$ となる b_Q は $b_Q = e^{C_G(Q)}$ と unique に決まり、$(Q,\hat{b}_Q) \subseteq (P,\hat{e})$ となる $\hat{b}_Q$ も unique となる。この[FH]の書き方で、Brauer category $\mathbb{B}r_{\hat{\mathfrak{B}}}(G)$ とは、object が G の $\hat{\mathfrak{b}}$-subpair $(Q,\hat{u})$ よりなり、$(Q,\hat{u}) \longrightarrow (R,\hat{v})$ の morphism は、$\mathrm{Hom}(Q,R)$ の写像で、G で $(Q,\hat{u})^g \subseteq (R,\hat{v})$ となる G の元 g より誘導されるものとする。$\mathbb{B}r_{\mathfrak{B},P}(G)$ は、object を $(P,\hat{e})$

に含まれるものに限ったBr$\hat{\mathcal{E}}$(G)の full subcategory とする。

さて、isotypy は、次のように2通り定義される。([FH]では $\mathcal{E}$-subpair を使っているが、ここは、元の $\mathcal{b}$-subpair にしてある。) ここで、$L_K(G,\mathcal{b})$ は、$\mathcal{b}$に属すGの一般指標に対応する Grothendieck group, $BCF_K(G,\mathcal{b})$ は、$\mathcal{b}$に属す K-valued class function で、p-singular class 上で零になるものからなる K-vector space を表すものとする。

Definition 3.1 ([Br] Definition 4.3, 4.6, [FH] 142頁)
$\mathcal{b}$は、有限群Gの block, $\mathcal{b}'$は有限群 G' の blockとし Pは、両方に共通した defect groupとする。次の2条件の成り立つ時、$\mathcal{b}'$と$\mathcal{b}$は、isotypic と言い、perfect isometry $I^{\langle 1\rangle}$ を $\mathcal{b}'$と$\mathcal{b}$の間の isotypy と呼ぶ。

(i) Pの G及び G'への包含は、Brauer category Br$\hat{\mathcal{E}}_P(G)$, Br$\hat{\mathcal{E}}'_P(G')$ 間の equivalence を誘導する。

(ii) Pの各 cyclic subgroup Qに対し perfect isometry
$$I^Q : L_K(C_{G'}(Q), \mathcal{b}'_Q) \longrightarrow L_K(C_G(Q), \mathcal{b}_Q)$$
で
$$d_G^{(x,\mathcal{b}_Q)} \cdot I^{\langle 1\rangle} = I_{P'}^{Q} \cdot d_{G'}^{(x,\mathcal{b}'_Q)}$$

が、Qの任意の生成元xについて成り立つようなものが存在する。ここで

$$I_{p'}^{Q}: \quad BCF_K(C_{G'}(Q), b'_Q) \longrightarrow BCF_K(C_G(Q), b_Q)$$

は、I^Qから誘導されたK-linear mapである。また$d_G^{(x, b_Q)}$はb-element (x, b_Q)に関するdecomposition mapである。

Definition 3.2 ([Br] Definition 4.6 後ろのRemark 2)
上述のisotypicのより"良い"定義として、上の定義の(i)と次の(ii′)をみたすものとする。

(ii′) Pの任意のsubgroup Qに対してperfect isometry

$$I^Q: L_K(C_{G'}(Q'), b'_Q) \longrightarrow L_K(C_G(Q), b_Q)$$

であって$C_P(Q)$の任意のzに対し、

$$d_{C_G(Q)}^{(z, b_{Q\langle z\rangle})} \circ I^Q = I_{p'}^{Q\langle z\rangle} \circ d_{C_{G'}(Q)}^{(z, b'_{Q\langle z\rangle})} \qquad \cdots\cdots\cdots (2)$$

をみたすものが存在する。

Broué予想 ([Br] Conjecture 6.1, Question 6.2)
bは、有限群Gのblockでabelian defect group Pを持ち、(P, e)がGでのmaximal b-subpair
$\Longrightarrow$ $OG\hat{b}$と$ON_G(P, e)\hat{e}$はderived equivalent.
Gのblock bと$N_G(P, e)$のblock eは、isotypic.

注意：この形に書いてあれば、$\mathcal{B}$と、$N_G(P)$における Brauer correspondent $\mathrm{Br}_P(\mathcal{B})$の間に言いなおせる。また abelian defect group を持つこれら $\mathcal{B}$, $\mathrm{Br}_P(\mathcal{B})$ 及び $N_G(P,e)$のe間で、Definition 3.1 の条件(i)が、いつも成立することは、$N_G(P,e)$が $\hat{\mathcal{B}}$ - subpair の fusion を controle すること（[AB] Proposition 4.21）から明らかである。

§4 Broué 予想に関する結果

I. Broué 予想 の derived equivalence

1. P が cyclic （Rickard [Ri 1] Linckelmann [L1]）
2. G が p-solvable （Fong + Puig + Dade）
3. A_5 の 主2-block （Rickard [Ri 2]）
4. P が Klein four group （Erdmann + Linckelmann [L 2]）

II. Broué 予想の isotypy

1. P が cyclic （Linckelmann [Br] を見よ.）
2. $\mathcal{B}$が主2-block （Fong, Harris [FH]）
   （abelian Sylow 2-subgroup を持つ単純群の分類使用）
3. $GL_2(p^n)$ の主 block $p \neq 2$ ([Br])
4. G 対称群 （Rouquier [Ro] Enguehard）
5. G 散在型単純群, $\mathcal{B}$が主block (Rouquier [Ro])

6. $\mathbb{G}$: connected reductive algebraic group / $\bar{\mathbb{F}}_q$

$\mathbb{G}^F$: finite group of rational points

($F : \mathbb{G} \to \mathbb{G}$ $\mathbb{F}_q$上 rational 構造定義する Frobenius endomorphism)

"大きい"素数 $p \nmid q$ ($\exists^1 d \in \mathbb{Z}^+$ s.t. $p \mid \Phi_d(q)$), $\mathbb{G}^F$ の unipotent p-block([BMM])

7. inertial quotient E の小さい場合

$|E| \leqq 4$, $E \cong D_6$ (文献略す。[U1]を見よ。)

$E \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ ($p \neq 3, 5$), $E \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ ($p \neq 2, 7$) ([U2] [U3])

$|E| = 5$ の主 block (多分 O.K. 渡辺 [W] より既約 Brauer 指標 個数5とわかっている為。)

今回 新しい結果

- $E \cong D_8$ の主 block ($p \neq 3, 5, 7$)
- E が基本可換 2-群 の主 block ($p \neq 3$) 講演後拡張

§5 方法と principal block に限った理由

Broué 予想の isotypy を E を与えておいて構成する方法は、以下のようなものである。Pが normal subgroup になる時の結果[K]によって、$kN_G(P)Br_P(b)$ や $k(N_G(P,e))e$ は、半直積 $L = P \rtimes E$ の、k上の或る twisted な群環に、Morita 同値であるので、それと b との間に、isotypy を構成する。$\hat{L}$ は、その twisted な

群環での k^*-group を表すことにする。その twisted な群環は、L の p'-group による適当な中心拡大である有限群 L' の block b'(defect group P)に同型になることで、そちらに翻訳して考える。(その際、各 b'-subpair での block は、p-subgroup の方から、unique に決まることで、b'-subpair は P の subgroup で代用し、block は略す。) そこで、良い方の isotypy の定義 3.2 にあるように、perfect isometry の族

$$\{ I^Q : L_K(C_{\hat{L}}(Q)) \longrightarrow L_K(C_G(Q), b_Q) \mid Q \subseteq P \}$$

で、(2)をみたすものを構成せねばならぬ。(2)の式は、I^Q が $Q \subseteq R \subseteq P$ なるいろいろの R について、I^R から誘導した K-linear map $I^R_{p'} : BCF_K(C_{\hat{L}}(R)) \to BCF_K(C_G(R), b_R)$ を材料に、言わば"貼り合わせ"で作られていることを示唆している。従って、P に含まれる subgroup の包含関係で、大きい方から、I^Q を構成しつつ、貼り合わせて、順次小さい方の perfect isometry を作ってゆく方法を取る。ちなみに、$C_G(Q)$ での block b_Q の defect group は P であり、inertial quotient は $C_E(Q)$ で、E の subgroup となっている。

4節の新しい結果で、principal block に限っ

てしまったのは、次のような理由がある。$1 \leqq Q \leqq P$ の各QについてI^Qを構成する際、Qが小さくなるにつれ、$C_E(Q)$は、大きくなる。$C_E(Q_1) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong C_E(Q_2)$ となるところで、I^{Q_1}, I^{Q_2}を構成する時、いずれの場合も、$C_E(R) \cong \mathbb{Z}_2$, $Q_1 \subset R$, $Q_2 \subset R$ となる或るRの所で作っておいたI^Rから誘導した$I^R_{p'}$を貼り合わせの材料に使うという状況が起こる。ところで、Rの時の perfect isometry は、2通り I^R, I'^R あるものの、貼り合わせ材料に使って、I^{Q_1}が構成可能となるのはきっかり片方のみであり、I^{Q_2}でも片方のみと(大雑把(かなり)に言って)なる。今、I^{Q_1}構成に使えるのがI^Rの時、もしI^{Q_2}構成には、I'^Rの方という事態が起これば、全体として、統一的な perfect isometry の族は、作れず、議論が進められなくなる。bを principal block にした時は、$C_{\hat{G}}(R)$の trivial character を $C_G(R)$の trivial character にうつす、言わば、自然な方をI^RにしておけばI^{Q_1}, I^{Q_2}の構成時の材料に、どちらもI^Rで大丈夫であることが示せる。一般には、b_Rの既約指標が区別できずI^R, I'^Rを外見上区別するのも難しい。なお、bが principal block の時、Dade予想の(2)式の$k(G)$も全

て principal block になることに注意すれば、principal block に限った新しい結果の方でも、Dade 予想の成り立っていることはわかる。

REFERENCES

[A] J.ALPERIN , Weights for finite groups , Proc. Sympos. Pure Math. 47 (1987) 369-379.

[AB] J.ALPERIN AND M.BROUÉ , Local methods in block theory , Ann. of Math. 110 (1979), 143-157.

[BMM] M.BROUÉ, G.MALLE AND J.MICHEL , Generic blocks of finite reductive groups , Astérisque (1993)

[Br] M.BROUÉ , Isométries parfaites, types de blocs, catégories dérivées , Astérisque 181-182 (1990), 61-92.

[D] E.C.DADE , Counting characters in blocks , I. Invent. Math. 109 (1992) 187-210.

[FH] P.FONG AND M.HARRIS, On perfect isometries and isotypies in finite groups, Invent. Math. 114 (1993) , 139-191.

[K] B.KÜLSHAMMER, Crossed products and blocks with normal defect groups, Comm. Algebra 13 (1985), 147-168.

[L1] M.LINCKELMANN, Derived equivalence for cyclic blocks over a p-adic ring , Math. Z. 207 (1991), 293-304.

[L2] M.LINCKELMANN , A derived equivalence for blocks with dihedral defect groups , J.Algebra 164 (1994) ,244-255.

[Ri1] J.RICKARD , Derived categories and stable equivalence , J.Pure Appl. Algebra 61 (1989) , 303-317.

[Ri2] J.RICKARD , Derived equivalence for the principal blocks of A_4 and A_5 , preprint

[Ro] R.ROUQUIER , Isométries parfaites dans les blocs à défaut abélien des groupes symétriques et sporadiques, J.Algebra 168 (1994), 648–694

[U1] Y.USAMI , Perfect isometries for blocks with abelian defect groups and dihedral inertial quotients of order 6 , J.ALgebra 172 (1995),113–125

[U2] Y.USAMI , Perfect isometries and isotypies for blocks with abelian defect groups and the inertial quotients isomorphic to $Z_4 \times Z_2$

[U3] Y.USAMI , Perfect isometries and isotypies for blocks with abelian defect groups and the inertial quotients isomorphic to $Z_3 \times Z_3$

[W] A.WATANABE , Some studies on p-blocks with abelian defect groups , Kumamoto J.Sci.(Math.) 16 (1985), 49-67

ある6次式の族とそのガロワ群

近藤武（東京女子大学）

1995年7月30日

1　6次式の族 $f(x;b,c,d)$

1.1　$f(x;b,c,d)$ の定義と出典

本稿で主役を演ずるのは次のような6次式である：

$$\begin{aligned}f(x;b,c,d) &= x^6+2cx^5+(c^2+2c+2)x^4+(2c^2+2c+2)x^3+(c^2+4c+5)x^2\\ &\quad +(2c+6)x+1-bdx^2(x+1)^2+b(x+1)^3-4dx^3\\ &= x^6+2cx^5+(c^2+2c+2-bd)x^4+(2c^2+2c+2-2bd+b-4d)x^3\\ &\quad +(c^2+4c+5-bd+3b)x^2+(2c+6+3b)x+(b+1)\end{aligned}$$

ここで b,c,d は有理数あるいは有理数体 $\mathbf{Q}$ 上独立な不定元である。

この式は、A.Brumer が種数2の代数曲線の族でそのヤコビ多様体の準同形環が $\mathbf{Q}(\sqrt{5})$ を含むようなものとして構成したものらしく、

M.Olivier, Corps sextique primitifs, Ann.Institute Fourier 40 (1990),757-767

の文献表に

A.Brumer, Exercises diédraux et courbes à multiplications réeles, Actes du Séminaire de théorie des nombres de Paris (1989/1990) Birkhäuser, Boston, à paraître

として出典が示されているが、この論文はその後出版された気配がなく筆者は未だ見る機会を得ていない。本稿では、A.Brumer の本来の構成意図とは無関係にこの6次式の族をガロワ理論および代数的整数論の観点から考察する。なお、定理1 (§1.3)、定理3 (§4) の証明は、富士通情報研の穴井宏和氏による数式処理(Computer Algabra)に大きく依存していることに注意されたい。

1.2　判別式

最初に $f(x;b,c,d)$ の判別式について述べておこう。$f(x;b,c,d)$ の判別式 $D(b,c,d)$ は次のようになる（§2.2 の末尾参照）：

$$D(b,c,d)=\delta(b,c,d)^2$$

ここで

$$\begin{aligned}\delta(b,c,d) &= 16bdc^5+\{(-144d+16)b-64d\}c^5\\ &\quad +\{(-48d^2-4d)b^2+(-16d^2+192d-144)b+(384d-64)\}c^4\\ &\quad +\{(288d^2-160d-4)b^2+(832d^2+1008d+208)b+(64d^2+320d+384)\}c^3\\ &\quad +\{(48d^3+8d^2)b^3+(32d^3-608d^2+1336d-108)b^2+\\ &\quad\ (-1280d^2+1184d+896)b+(-2304d^2-2752d+256)\}c^2\\ &\quad +\{(-144d^3+144d^2+36d)b^3+(-768d^3+528d^2-2880d+1008)b^2+\\ &\quad\ (-576d^3-1536d^2-10032d+432)b+(-4032d^2-9408d-2496)\}c\\ &\quad +\{(-16d^4-4d^3)b^4+(-16d^4+416d^3+24d^2+108d+27)b^3+\\ &\quad\ (2112d^3-1824d^2-264d-2268)b^2+(3456d^3-6096d^2-1936d-7744)b+\end{aligned}$$

$(1728d^3 - 5184d^2 - 2176d - 6592)\}$

まず注意すべきことは、判別式が平方数であるから、

(1.1) $f(x;b,c,d)$ の $\mathbf{Q}(b,c,d)$ 上のガロワ群は6次交代群の部分群

である。また$\delta(b,c,d)$ について次のことを注意しておこう：

(1.2) $\delta(b,c,d) \equiv 27b^3 \mod 4\mathbf{Z}[b,c,d]$

すなわち、$\delta(b,c,d)$ の係数は$27b^3$なる項を除いてすべて4で割れる。とくに

(1.3) $b,c,d \in \mathbf{Z}$ のとき、bが奇数ならば、$\delta(b,c,d)$ は奇数

である。さらに（実際に数値を入れて確かめてみると）

(1.4) $b,c,d \in \mathbf{Z}$ 、bが奇数ならば、$\delta(b,c,d)$ は平方因子のない整数である割合が大きい

ことが分かる。

1.3 主結果

本稿では、この6次式の族について次の二つの定理を示す：

定理 1 b,c,dを有理数体$\mathbf{Q}$上独立な不定元とするとき、$f(x;b,c,d)$ の $\mathbf{Q}(b,c,d)$ 上のガロワ群は（6次置換群と見て）5次交代群 A_5と同形である。

注意 この定理により$b,c,d \in \mathbf{Q}$のとき、$f(x;b,c,d)$ の$\mathbf{Q}$上のガロワ群は一般にはA_5に同形である（Hilbert の既約性定理）。しかし、たとえ$f(x;b,c,d)$ $(b,c,d \in \mathbf{Q})$ が$\mathbf{Q}$上既約であってもガロワ群がA_5とは限らない。実際

$$f(x;-2,0,d) = x^6 + (2d+2)x^4 + (2d-1)x^2 - 1$$

のガロワ群は4次交代群A_4と同形である。なお、$f(x;b,c,d)$ の定数項は$b+1$であるから$b=-1$のとき$f(x;b,c,d)$は可約である。このとき、5次式の族$f(x;-1,c,d)/x$ はガロワ群が位数10の正二面体群D_{10}の大変良い族を与えるが、これについては§4で簡単に触れる。

定理 2 $f(x;b,c,d) \in \mathbf{Z}[x]$ としよう（$b,c,d \in \mathbf{Q}$であるが、有理整数である必要はない）。$f(x;b,c,d)$ の$\mathbf{Q}$上のガロワ群はA_5とする。さらに

(*) $\delta(b,c,d)$ が平方因子を持たない

と仮定する。m を$\delta(b,c,d)|m$ なる平方因子のない有理整数とするとき、二次体$\mathbf{Q}(\sqrt{m})$ 上の$f(x;b,c,d)$ の分解体は不分岐A_5-拡大である。

注意 (1) (1.4) により定理2の条件 (*) を満たす b,c,d は沢山（恐らく無限に）存在する。$\delta(b,c,d)$ が素数であるb,c,d ですら無限に存在すると思われるが、筆者は確認していない。$\delta(b,c,d)$ が素数である$f(x;b,c,d)$ の例は付録の表1、表2で与える。

(2) (*) のもとで一つの$f(x;b,c,d)$ は無限に多くの二次体の上の不分岐A_5-拡大を与える。

(3) $b = 4b'+1$, $c = c' + \frac{1}{2}$, $d = d' + \frac{1}{4}$ $(b',c',d' \in \mathbf{Z})$ のとき、$f(x;b,c,d) \in \mathbf{Z}[x]$ である。

2 ガロワ群

2.1 6次式の15次分解式 (Resolvent)

Lを体として多項式環$L[x]$の6次式$f(x)$をとる。$f(x)$の根を$\theta_1,\theta_2,\theta_3,\theta_4,\theta_5,\theta_6$として

(2.1) $\theta_p\theta_q + \theta_r\theta_s + \theta_t\theta_u \quad \{p,q,r,s,t,u\} = \{1,2,3,4,5,6\}$

なる形の15個の式を考え、これらを根とする15次式

$$F_{15}(y;f) = \prod(y - (\theta_p\theta_q + \theta_r\theta_s + \theta_t\theta_u))$$

を$f(x)$の15次分解式という。明らかに$F_{15}(y;f) \in L[x]$である。

補題 1 $F_{15}(y;f)$ が $L[x]$ において、5次既約式と10次既約式の積に分解すれば、$f(x)$ の L 上のガロワ群は5次対称群あるいは5次交代群に同形である。

証明. 6次対称群の可移部分群は
(1) (原始群) S_6, A_6, (6次置換群と見た) S_5, A_5
(2) (非原始群) Wreath 積 $S_3 \int S_2$ (位数72), $S_2 \int S_3$ (位数48) の部分群
である。ここにあげた6個の群のそれぞれを(2.1)の15個の式に作用させて軌道分解するとその軌道の長さは

15 (S_6), 15 (A_6), 5 + 10 (S_5), 5 + 10 (A_5), 6 + 9 ($S_3 \int S_2$), 1 + 6 + 8 ($S_2 \int S_3$)

となる。既約式 $f(x)$ のガロワ群はこれら6個の群の一つ（あるいはその部分群）であり、$F_{15}(x;f)$ の $L[x]$ における因子として軌道の長さを次数とするもの（一つの既約式のベキ）が得られる。このことから補題は明らかであろう。□

2.2 定理1の証明

さて定理1は $f(x;b,c,d)$ の15次分解式が上の補題1の条件を満たすことを検証して証明するのであるが、問題はこの15次分解式の計算である。容易に想像がつくようにパソコン程度の計算機では実行不可能である。筆者は富士通情報研の穴井宏和氏にお願いして $f(x;b,c,d)$ の15次分解式を計算して頂き、これが補題1の条件を満たしていることを確かめて頂いた。たとえ大型の計算機を用いても困難であった計算を実行して下さった穴井氏に感謝したい。ちなみにこの分解式をexplicitに書き下すとA4判の用紙に殆ど隙間なくプリントして7頁にわたる長い式になる。参考のため、この15次分解式の5次部分の係数を書いておこう：

y^4 の係数: $db - c^2 - 2c - 2$

y^3 の係数: $((-4d+2)c + 2d - 6)b + 4c^3 + 2c^2 + (-8d-4)c - 10$

y^2 の係数: $(-2d^2 - 4d - 1)b^2 + ((8d-8)c^2 + (-12d+30)c - 16d^2 - 14d - 20)b$
$- 6c^4 - 4c^3 + (16d+18)c^2 + 48c - 16d^2 - 8d - 32$

y の係数: $((4d^2 + 14d + 4)c - 19d^2 - 34d - 9)b^2$
$+ ((-8d+10)c^3 + (30d-38)c^2 + (8d^2 - 8d + 26)c - 64d^2 - 70d + 2)b$
$+ 4c^5 + 5c^4 + (-8d-16)c^3 + (16d-62)c^2 + (-24d+52)c - 48d^2 - 16d + 33$

定数項: $d^3b^3 + ((-3d^2 - 12d - 4)c^2 + (22d^2 + 50d + 18)c - 52d^2 - 72d - 27)b^2$
$+ ((3d-4)c^4 + (-20d+14)c^3 + (16d-8)c^2 + (48d^2 + 88d + 14)c$
$- 168d^2 - 215d - 72)b - c^6 - 2c^5 + 4c^4 + (-16d+24)c^3$
$+ (24d-21)c^2 - 30c - 144d^2 - 168d - 54$

ところで§1.2で与えた判別式の計算であるが、筆者は"未定係数法"により（二日程かけて）計算したのであるが、これも穴井氏に $f(x;b,c,d)$ とその導関数の終結式を直接計算して確かめて頂いた。

3 二次体の上の不分岐拡大

3.1 分岐条件

補題 2 $K/\mathbf{Q}$ をガロワ拡大、$p_1, p_2, \cdots, p_r$ を $K/\mathbf{Q}$ で分岐する素数全体として、簡単のため p_i $(i = 1, \cdots, r)$ は奇素数とする。次の条件：

(#) 各 p_i の $K/\mathbf{Q}$ における分岐指数は2

が満たされているとする。m を $p_1 p_2 \cdots p_r | m$ なる平方因子の無い整数とするとき、拡大 $K(\sqrt{m})/\mathbf{Q}(\sqrt{m})$ は不分岐拡大である。

証明. 各p_iの$K(\sqrt{m})/\mathbf{Q}$における分岐指数は高々4である。分岐指数が4ならば、$\sqrt{m} \notin K$で惰性群はKleinの4元群となるが、p_iは奇数であるからp_iの$K(\sqrt{m})/\mathbf{Q}$における分岐はtame、従って惰性群は巡回群となり矛盾となる。よって各p_iの$K(\sqrt{m})/\mathbf{Q}$における分岐指数は2、すなわち各p_iは$K(\sqrt{m})/\mathbf{Q}(\sqrt{m})$において不分岐である。□

例 1 $p_i^* = (-1)^{\frac{p_i-1}{2}} p_i$, $K = \mathbf{Q}(\sqrt{p_1^*}, \cdots, \sqrt{p_r^*})$, $m = p_1^* p_2^* \cdots p_r^*$とするとき、補題2の結論は、古典的な二次体の種の理論で現れる状況である。

例 2 Fがn次代数体でその判別式$d(F)$がある二次体の判別式と一致していたとする。KをFの$\mathbf{Q}$上のガロワ閉包とするとき、補題2の分岐条件(#)が満たされる。このとき、$m = d(F)$ならば$K \supset \mathbf{Q}(\sqrt{m})$で、拡大$K/\mathbf{Q}(\sqrt{m})$は不分岐$A_n$拡大（近藤[Ko: Theorem 2]参照）、$m \neq d(F)$ならば（簡単のため$d(F)$は奇数として）拡大$K(\sqrt{m})/\mathbf{Q}(\sqrt{m})$は不分岐$S_n$拡大を与える。

これらの例では$K/\mathbf{Q}$のガロワ群が単純群ではないが、次にガロワ群が単純群となる例を与えよう。

3.2 二次体の不分岐$PSL(2,7)$拡大

次の例は、本年始め頃防衛大学の山村健氏により指摘されたものである。

例 3 次のような7次式を考える。$d(f)$はこれらの判別式である。

$f(x) = x^7 + 2x^6 - 3x^4 - x^3 - x^2 - x + 2$, $d(f) = 105124009 = 10253^2$

$f(x) = x^7 - x^6 - x^5 + x^4 - x^3 - 3x^2 + 3x + 2$, $d(f) = 157979761 = 12569^2$

$f(x) = x^7 - x^4 - x^3 - 7x^2 + 4x + 5$, $d(f) = 26536735801 = 162901^2$

これらの7次式の$\mathbf{Q}$上のガロワ群は位数168の単純群$PSL(2,7)$である。後に見るように（§3.4の注意参照）これらの7次式の$\mathbf{Q}$上の分解体は補題2の分岐条件(#)を満たす。よってこれらの7次式はそれぞれ$\mathbf{Q}(\sqrt{10253}), \mathbf{Q}(\sqrt{12569}), \mathbf{Q}(\sqrt{162901})$上の不分岐$PSL(2,7)$拡大を与える。また容易に分かるようにこれら三つの式のすべての根を二次体$\mathbf{Q}(\sqrt{10253 \cdot 12569 \cdot 162901})$の上に添加した体はガロワ群が$PSL(2,7) \times PSL(2,7) \times PSL(2,7)$の不分岐拡大を与える。

例3にあげた7次式は山崎[YK]に見られるものである。1980年頃、東大教養学部数学教室に始めてミニコンが入ったとき、山崎圭次郎氏は係数の小さい整数係数5次式、7次式(5次式については絶対値5以下、7次式は絶対値3以下)のガロワ群を調べ、ガロワ群が対称群となるもの以外の式の表を作られた。その表にあるガロワ群が$PSL(2,7)$となる式で補題2の分岐条件を満たすものは、上の三つの式と

$f(x) = x^7 - 3x^6 - x^4 - 2x^3 + 3x + 1$, $d(f) = 1729312225 = 5^2 \cdot 8317^2$

である（ただしこの場合は5は分岐しない）。一方、山崎氏はガロワ群が5次交代群となる5次式の例を数十個与えられたが、その中には補題2の分岐条件(#)を満たすものは一つも存在しない。本稿の主題の一つは、A.Brumerの構成した6次式の族$f(x;b,c,d)$が補題2の分岐条件を満たすものを大量に与えることを示すことである。

3.3 Dedekindの補題等

次のよく知られた二つの補題は以下の議論において基本的である。

補題 3 (Dedekindの判別定理) Fを有限次代数体、$\mathcal{D}$を拡大$F/\mathbf{Q}$の共役差積とする。$\mathcal{P}$は素数pのFにおける素因子で、$\mathcal{P}^d \| \mathcal{D}$, $\mathcal{P}^e \| p$とするとき、

(a) $d > 0 \Longleftrightarrow e > 1$

(b) $p \nmid e \Longrightarrow d = e - 1$

(c) $p^v \| e$ $(v > 0) \Longrightarrow e \leq d \leq ev + e - 1$

補題 4 (Van der Waerden) F を n 次代数体、K をその $\mathbf{Q}$ 上のガロワ閉包とし、拡大 $K/\mathbf{Q}$ のガロワ群を n 次置換群と見る。Z, T をそれぞれ素数 p の K における或素因子の分解群、惰性群とする。さらに素数 p が F において次のような素因子分解を持ったものとする：

$$p = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\cdots\mathcal{P}_g^{e_g}, \quad N_{K/\mathbf{Q}}(\mathcal{P}) = p^{f_i}\ (i = 1, 2, \cdots, g)$$

このとき、Z は g 個の軌道 *(orbit)* を持ち、その各々は長さ e_if_i でこれらは長さ e_i の f_i 個の T-軌道に分解する。

F を n 次代数体として、その判別式 $d(F)$ が次の形をしているものとする：

(**) $d(F) = (p_1p_2\cdots p_r)^2$ $(p_1, p_2, \cdots, p_r$は異なる素数)

このとき、素数 $p = p_i$ $(i = 1, 2\cdots, r)$ の Fにおける素因子分解は次の形のいずれかである（$\mathcal{Q}$ は不分岐イデアル):

(a) $p = \mathcal{P}_1^2\mathcal{P}_2^2\mathcal{Q}$, $(\mathcal{P}_i,\ \mathcal{Q}) = 1$, $N_{F/\mathbf{Q}}(\mathcal{P}_i) = p$ $(i = 1,\ 2)$

(b) $p = \mathcal{P}^2\mathcal{Q}$, $(\mathcal{P},\ \mathcal{Q}) = 1$, $N_{F/\mathbf{Q}}(\mathcal{P}) = p^2$

(c) $p = \mathcal{P}^3\mathcal{Q}$, $(\mathcal{P},\ \mathcal{Q}) = 1$, $N_{F/\mathbf{Q}}(\mathcal{P}) = p$

これはDedekindの補題3から分かる。さらに記号はVan der Waerdenの補題4の通りとして、各場合(a),(b),(c)に応じて

(a) 惰性群T は互換二つの積である置換によって生成される位数2の群である。

(b) (a)と同じ

(c) 惰性群T は 3-cycle によって生成される位数3の群である

以上の考察から、Van der Waerdenの補題4におけるようにKをFの$\mathbf{Q}$上のガロワ閉包とするとき、

(##) $K/\mathbf{Q}$のガロワ群が3-cycle を含まなければ、ガロワ拡大$K/\mathbf{Q}$は補題2の条件(#)を満たす

ことが分かる。

3.4 定理2の証明

$f(x; b, c, d)$は定理2の条件(*)を満たすものとし、θを$f(x; b, c, d) = 0$の一つの根、$F = \mathbf{Q}(\theta)$とする。このとき、Fは前節の条件(**)を満たす。また$f(x; b, c, d)$の$\mathbf{Q}$上のガロワ群はA_5と同形な6次置換群でこれは3-cycleを含まない。よって前節の(##)から定理2が成り立つことが分かる。

注意. (1) $PSL(2, 7)$を7次置換群と見たとき、3-cycle を含まない。これから§3.2の例3で与えた7次式の$\mathbf{Q}$上の分解体が補題2の条件(#)を満たすことが分かる。

(2) 代数体Fが前節の条件(**)を満たすとき、その$\mathbf{Q}$上のガロワ閉包のガロワ群Gの構造に著しい制限がつく。実際、前節の考察から分かるように（n次置換群と見た）Gは 3-cycle あるいは互換二つの積である位数2の元を含む。このようなn次置換群 Gが原始群ならば

$G \simeq A_n$, A_5 $(n = 6)$, $PSL(2, 7)$ $(n = 7)$ または位数10の正二面体群$(n = 5)$

のいずれかであることを見るのはそれ程難しくはない。とくにGが単純群ならば（簡単な考察から）原始群となり、Gはここにあげた特殊なものに限る。

4 5次式の族 $f(x; -1, c, d)/x$

$g(x; b, c) = f(x; -1, c, d)/x$ とおく。

$$g(x; c, d) = x^5 + 2cx^4 + (c^2 + 2c + 2)x^3 + (2c^2 + 2c + 1)x^2 + (c^2 + 4c + 2)x + 2c + 3 + dx(x - 1)^2$$

となり、その判別式$d(g)$は

$$\begin{aligned} d(g) &= \{8dc^5+(-52d+8)c^4+(16d^2-16d-52)c^3 \\ &\quad +(216d^2+448d-8)c^2+(8d^3+496d^2+628d+386)c \\ &\quad +(12d^3+312d^2+204d+381)\}^2 \\ &= (2c+3)^2\Delta(c,d)^2 \end{aligned}$$

ここで

$$\begin{aligned} \Delta(c,d) &= -4d^3-8(c^2+12c+13)d^2-4(c^4-8c^3+10c^2+41c+17)d \\ &\quad -(4c^3-32c^2+44c+127) \end{aligned}$$

である。この5次式の族$g(x;c,d)$について次の二つの定理が成立する。

定理 3 c,dをQ上独立な不定元とする。このとき、
(1) $g(x;c,d)=0$のQ(c,d)上のガロワ群は位数*10*の正二面体群D_{10}である。
(2) $g(x;c,d)=0$のQ(c,d)上の分解体に含まれる二次体はQ$(c,d,\sqrt{\Delta(c,d)})$である。

この定理の(2)は、このシンポジウムの直後、穴井氏により数式処理 (Computer algebra) の応用で証明された。これは$y^2-\Delta(c.d)$が$g(x;c,d)=0$のQ(c,d)上の分解体において二つの1次因子の積に分解することを示すのであるが、そのアルゴリズムについては穴井、横山[AY:p5 ~6]を参照されたい。さらにこの定理3から次の定理を得る：

定理 4 $g(x;c,d)\in\mathbf{Z}[x]$, $(c,d\in\mathbf{Q},\ c,d$は有理整数である必要はない$)$で、そのQ上のガロワ群がD_{10}であるものとする。$\Delta(c,d)$がある二次体の判別式と一致するとき（多くのc,dに対してこの条件は満たされる)、$g(x;c,d)=0$のQ(c,d)上の分解体は二次体Q$(\sqrt{\Delta(c,d)})$上不分岐であり、二次体Q$(\sqrt{\Delta(c,d)})$の 類数は *5* で割れる。

注意. 定理4における$\Delta(c,d)$の条件は
「$\Delta(c,d)$は$p=5$ または $p\equiv\pm1\ mod\ 5$なる素数の平方で割れない」
としてよい（下記(2)参照)。

定理4の証明は、次の(1)および(2)から分かる:
(1) $g(x;c,d)\in\mathbf{Z}[x]$, $g(x;c,d)=0$の一つの根をθ, $F=\mathbf{Q}(\theta)$とする。よく知られているように
$d(g)=[\mathbf{Z}_F:\mathbf{Z}[\theta]]^2d(F)$ ($\mathbf{Z}_F$はFの整数環、$d(F)$はFの判別式)
であるが、実際は
$d(F)\mid\Delta(c,d)^2$ すなわち $2c+3\mid[\mathbf{Z}_F:\mathbf{Z}[\theta]]$
である。これは
$g(x+1;c,d)=x^6+\cdots+(2c+3)(4c+5)x+(2c+3)^2$
であることと、次の簡単な補題から分かる:

補題 5 $h(x)$は有理整係数既約式で
$h(x)=x^n+\cdots+qax+q^2b$ $(q,a,b\in\mathbf{Z})$
の形をしているとき、$q\mid[\mathbf{Z}_F:\mathbf{Z}[\theta]]$。ここで$\theta$は$h(x)=0$の一つの根、$F=\mathbf{Q}(\theta)$である。

(2) $K/\mathbf{Q}$はガロワ群がD_{10}のガロワ拡大、FをKに含まれる5次体とするとき、K において分岐する素数p の分岐指数は明らかに 2,5, または 10 であるが、より精密に
(a) $p\equiv\pm1\ mod\ 5$ならば、2または5
(b) $p\equiv\pm2\ mod\ 5$ならば、2
であることが、Hilbertの分岐理論から分かる。よって K における分岐指数が 5 または 10 ならば、$p=5$ または $p\equiv\pm1\ mod\ 5$ であるが、このとき F における分岐指数は5、従って$p^d\|d(F)$とすると $d\geq4$ となる (Dedekindの補題3)。
以上 (1)、(2)から、上の注意に述べた$\Delta(c,d)$の条件の下で $g(x;c,d)=0$ の分解体 K において分岐する素数の分岐指数は 2、よって $K/\mathbf{Q}(\sqrt{\Delta(c,d)}$ は不分岐拡大となる。

5 終りに

本稿の整数論的部分 ー 定理2, 定理4 ー では、もっぱら $f(x;b,c,d)$, $g(x;c,d)$ が有理整係数の場合を扱った。一般に

「$\mathbf{Q} \ni b,c,d$ のとき、$f(x;b,c,d)$, $g(x;c,d)$ は $\mathbf{Q}$ 上の A_5-拡大、D_{10}-拡大（とくに二次体上の不分岐 A_5-拡大、不分岐5次拡大をあたえるもの）のうち、どの位の範囲をカバーするのであろうか。」

この問題は A_5-拡大については、恐らく調べようがないであろう。一方、D_{10}-拡大については、二次体 $\mathbf{Q}(\sqrt{m})$ の不分岐5次拡大は $|m| < 1000$ の範囲で

実二次体のときは $m = 401, 439, 499, 727, 817, 982$ の6個

虚二次体のときは $-m = 47, 79, \cdots, 982$ の114個

に対して存在するが、このうち実二次体に対しては6個すべて、虚二次体に対しては数個の例外（例えば $-m = 613, 769, 977$ など）を除いて適当な $c,d \in \mathbf{Q}$ に対する $g(x;c,d)$ から得られる（例外の場合が $g(x;c,d)$ から絶対に得られないかどうかについては未確認）。いずれにしても $f(x;b,c,d)$, $g(x;c,d)$ は $\mathbf{Q}$ 上の A_5-拡大、D_{10}-拡大をかなり広範囲にカバーしているように思われる。

参考文献

[AY] 穴井宏和, 横山和弘, ガロワ群計算の最新状況, 第12回代数的組合せ論シンポジウム報告集（近刊）、於東大駒場(1995.7.29-31)

[Ko] T.Kondo, Algebraic number fields with discriminant equal to that of a quadratic number field, J.Math.Soc.Japan 47 (1995), 31-36

[YK] 山崎圭次郎, ガロワ群の計算, 1981年度科学研究費報告集(近藤武編), 東大教養学部, 9-57

以下、表1、表2において実二次体 $\mathbf{Q}(\sqrt{p})$ (p : 素数) の上の不分岐 A_5-拡大を与える $f(x;b,c,d)$ の実例を与えるが、類数の項は $\mathbf{Q}(\sqrt{p})$ の類数を表し、符号は基本単数の符号を示す。

表1. 実二次体 $\mathbf{Q}(\sqrt{p})$ (p : 素数) の上の総実な不分岐 A_5-拡大を与える $f(x;b,c,d)$

p	b	c	d	類数
8311	−7	−4	0	1
25771	−11	8	−1	1
32611	11	2	2	1
37987	−3	7	−1	1
72707	−27	−6	0	1
83443	3	4	9	3
426427	−11	−5	0	1
515993	−9	−5	0	−1
697441	−9	8	−1	−1
727427	−3	9	−3	1
877867	−19	11	−2	1
944399	31	−1	1	3
1204243	−3	8	−1	1
1207447	−23	−6	0	1
1294723	−3	−5	−1	1
1447811	−3	−5	−3	1
1606763	27	0	1	1
1648379	−3	−5	−2	1
1836811	27	−4	3	1
1924651	−67	−8	0	1
2118163	−11	−6	0	1
2214761	9	0	4	−1
2219807	−15	−6	0	1
2719001	41	−2	1	−1
2828879	15	2	2	1
2956907	−3	−8	0	1
4176239	15	1	2	1
4367879	31	0	1	1
4460909	77	4	1	−1
4748371	−3	9	−2	1
5060053	−5	−8	0	−1
5122259	−3	−9	0	1
6492137	33	0	1	−1
6874397	−29	−7	0	−1
7156883	27	4	2	1
7360273	−25	−7	0	−1
7540529	9	3	4	−5
7912319	−31	10	−1	1
8358299	−3	−10	0	1
8540509	−61	−8	0	−1
8554027	−3	10	−4	1
8573023	15	−1	3	1
8987213	21	−1	2	−3
9072919	39	−6	3	3
11059123	−3	−7	−1	3
11141743	−7	−7	−3	1
11367269	29	8	4	−1
11456923	−3	10	−1	1
11464213	45	−2	1	−11
12143441	−57	−8	0	−1
12542939	19	2	2	25
13957429	−21	−8	−1	−1
14390213	−5	−10	0	−1
15226147	−27	10	−1	1
16013611	−11	−7	−1	1
16102049	41	−1	1	−1
16237597	−5	10	−1	−3
16451047	15	−2	4	13
17110019	−3	10	−2	1
17283269	−21	−8	0	−1
17618281	−17	11	−2	−1
18279497	−25	10	−1	−1
18389779	−3	−7	−2	1
18492841	−9	−7	−1	−1
18616799	−7	−7	−1	1
20265703	−7	−10	0	1
20855221	−37	−8	0	−1
21391471	−7	−8	−5	7
21779123	43	−1	1	1
21787061	21	2	2	−1
23577859	−35	13	−2	1
23732327	79	4	1	3
23786627	−3	−7	−3	1
23881133	13	−1	4	−1
24278819	43	1	1	1
25168387	−3	11	−1	1
26204767	−23	−11	−3	43
27454211	−19	−8	−1	1
29772409	81	−5	1	−1
29961859	−83	−9	0	1

p	b	c	d	類数
30909173	13	4	4	−3
35103353	25	−1	2	−1
36184349	45	0	1	−1
36800639	47	−1	1	1
36940669	−13	−10	0	−1
37510321	71	4	1	−1
37677301	−77	−9	0	−1
39753851	−27	−9	0	3
40669361	−9	−11	0	−1
41548519	23	1	2	1
41721059	−3	−8	−2	27
43406093	−125	−10	0	−1
46009129	81	4	1	−1
46429927	−15	−8	−1	3
47108851	−3	11	−4	1
47251433	−17	−10	0	−3
50916937	−9	−9	−5	−1
51214613	−45	−9	0	−1
52034509	−53	−9	0	−3
53593391	71	−4	1	1
54887557	−5	11	−2	−3
56161943	55	−2	1	3
56963657	−9	−8	−2	−1
59651063	−119	−10	0	1
62344783	−7	−8	−2	1
64603733	−117	−10	0	−9
65892193	−25	−10	0	−1
67629299	51	0	1	3
68139857	17	5	4	−1
68990651	35	7	3	5
69327403	−115	−10	0	1
69580001	25	−3	3	−1
69879781	−29	11	−1	−5
70132163	−27	−10	0	1
71983061	13	1	4	−1
72251909	53	1	1	−1
73220177	17	−2	4	−1
73757227	51	9	3	1
74201453	−29	−10	0	−1
74618987	−3	−16	0	1
76131827	−3	−8	−5	1
76168691	−19	11	−1	1
79361669	85	−5	1	−1
83256331	−19	−11	0	3
85057279	−23	−10	−2	1
85313771	19	7	5	1
85958003	−107	−10	0	3
86890631	55	1	1	1
88745893	−37	−10	0	−3
91027507	−19	13	−3	1
91220033	−17	−10	−3	−1
97077031	−7	−14	0	5
97467199	−33	−11	−2	1
97486799	55	0	1	1
99028283	−99	−10	0	3
99032407	−23	−11	0	1
99481051	−11	12	−3	1

表2. 実二次体 $Q(\sqrt{p})$ の上の不分岐 A_5-拡大を与える $f(x;b,c,d)$
(* は $f(x;b,c,d)$ が総実であることを示す)

p	b	c	d	類数
653	3	5	0	−1
	5	4	0	
2053	−3	−3	0	−1
2083	3	4	0	1
	5	5	0	
3329	1	4	0	−1
	7	5	0	
4073	1	7	0	−1
5413	−3	2	0	−1
	35	7	0	
7433	1	3	0	−1
	15	6	0	
8311*	1	7	−1	1
	−7	−4	0	
10453	11	5	0	−1
	−3	4	0	
10597	3	−1	1	−1
10687	1	7	−2	1
11969	1	2	−1	−1
14321	1	7	2	−1
14323	3	4	1	1
15289	1	−1	0	−1
16193	1	1	0	−1
	55	8	0	
16529	15	1	1	−1
18049	7	6	0	−1
	9	3	0	
18329	1	1	−1	−1
19661	3	3	6	−1
21341	−3	0	−2	−1
21757	−3	1	−3	−1
24499	3	2	0	3
	29	7	0	
25771*	11	8	−1	1
24631	1	7	4	1
26429	1	0	1	−1
26731	21	0	1	1
27947	93	9	0	1
	−5	0	0	
32611*	11	2	2	1
32987	3	2	−1	1
36293	−3	2	−5	−1
37987*	−3	7	−1	1
38767	1	−1	2	1
39139	3	1	0	3
	53	8	0	
44053	3	5	1	−1
47623	−9	3	0	1
	25	6	0	
47653	5	5	−1	−1
51461	3	7	0	−1
	29	2	0	
53923	−5	−1	0	1
54581	3	−2	1	−1
54617	15	4	0	−1
	−7	5	0	
56923	3	−1	0	1
58567	1	−3	3	5
58603	5	−1	1	9
58907	−5	−3	0	3
61211	3	1	−1	3
63149	13	1	1	−1
63929	1	4	1	−1
67231	1	9	0	3
68891	−5	3	−2	1
72707*	−27	−6	0	1
74611	3	−2	0	1
75941	3	1	3	−1
77641	9	2	0	−7
	23	7	0	
83443*	3	4	9	3
84317	−3	1	2	−1
84871	17	1	1	11
85829	−3	1	−4	−1
87433	7	1	2	−1
94307	−5	3	−3	1
96043	5	4	1	1

— 表2 の続き —

p	b	c	d	類数
100937	1	1	4	−1
101531	3	3	4	3
102587	3	3	5	1
104393	1	2	−2	−1
112459	3	1	1	1
113567	7	4	−1	19
115499	3	1	2	1
115763	−13	4	0	7
119737	7	2	0	−1
121577	1	5	−2	−15
123373	−11	5	0	−1
125777	1	3	−2	−1
127423	−9	−4	0	1
131221	3	6	1	−7
136573	−3	3	−3	−1
137519	9	7	0	1
141761	1	2	5	−3
142217	1	4	−2	−1
144323	−13	2	0	1
149551	9	2	2	1
151517	3	4	3	−1
153487	1	2	6	1
154459	3	3	3	1
155921	1	8	−4	−1
162263	1	−1	3	3
162457	−15	3	0	−5
162671	7	0	0	1
162779	3	6	−2	3
163847	7	5	−1	3
164663	7	2	−1	1
164707	5	−2	1	1
171161	1	2	2	−1
176921	−7	−2	0	−1
177239	1	−4	6	33
183479	7	1	1	1
185221	3	2	5	−1
187193	1	4	2	−1
190097	−7	2	−2	−25
190759	1	−4	1	13
206699	3	2	2	1
208283	11	1	0	1
214673	1	6	3	−1
214723	29	−1	1	1
231901	−3	−2	−2	−1
247501	−3	1	−5	−1
251033	39	−2	1	−3
254299	5	1	6	1
263429	13	1	0	−1
264659	3	3	−2	3
269953	1	2	3	−1
302143	9	−1	1	1
305017	1	5	3	−3
308027	3	2	−2	19
308887	−17	5	9	1
312281	9	2	−1	−5
313297	−15	1	0	−1
324449	1	6	4	−3
332201	1	0	−3	−1
341603	−5	4	−2	1
343649	1	2	4	−5
362407	1	8	2	3
369407	9	3	3	1
370529	−7	7	0	−1
376351	1	−2	4	1
388099	−21	3	0	1
390353	−7	4	−2	−1
392669	−3	−1	−4	−1

—— 表2 の続き ——

p	b	c	d	類数
397673	−7	−1	−2	−1
404167	1	7	6	1
423287	−9	0	−2	1
426427*	−11	−5	0	1
431237	13	0	0	−1
434267	−5	4	−4	1
440773	−3	−2	−3	−1
449929	9	−2	0	−1
469757	85	0	0	−1
481883	−5	4	−3	1
483809	1	5	4	−1
491857	−15	0	0	−1
502829	−11	−2	0	−1
505727	−9	−1	−2	1
511859	−5	1	2	1
515993*	−9	−5	0	−1
522919	−17	6	0	1
533831	9	8	0	1
541927	15	0	0	1
546739	11	2	−1	1
551519	23	1	0	1
567997	−3	−4	−3	−1
569957	3	5	3	−1
573847	−9	4	−2	1
592463	−25	4	0	3
592919	33	3	0	1
608693	5	4	−2	−11
611557	11	8	0	−1
619793	1	6	−5	−1
620183	1	8	3	1
628267	−5	8	0	1
640043	11	−2	0	1
648331	27	1	0	1
648509	−11	−1	−2	−13
663281	1	1	−4	−1
670097	1	6	5	−1
682697	1	5	5	−1
697441*	−9	8	−1	−1
698557	3	4	8	−1
713753	15	8	0	−1
719063	25	8	0	1
727427*	−3	−9	−3	−3
733793	1	−2	−3	−3
741193	−15	−1	0	−1
741409	23	8	0	−1
761213	−3	−1	−5	−1
764447	−25	5	0	1
766169	1	4	5	−1
772493	13	4	−1	−3
786419	−5	2	2	1
788383	15	−1	0	1
814901	5	2	−2	−1
823013	3	−3	3	−3
847883	−13	7	0	1
851813	3	2	9	−1
853813	−3	9	0	−1
857513	1	3	5	−1
860501	13	−2	0	−1
868867	3	7	−2	3
870871	1	−1	5	1
877867*	−19	11	−2	1
881219	−29	4	0	1
895387	3	3	−3	1
897443	3	−1	−2	1
899413	5	7	−1	−1
919063	1	−5	5	1
944399*	31	−1	1	3
964967	7	3	4	3
971693	−3	4	2	−1
978473	17	−1	0	−1
996973	3	2	8	−3

AN ELEMENTARY RING THEORY FOR THE VERTEX OPERATOR ALGEBRAS

Koichiro Harada

This is a preliminary version of my work on the ring theory for the vertex operator algebras. Most results in it are elementary. I just wanted to say here that a deeper research of this kind would be necessary for the vertex operator algebras (VOA). All proofs will be omitted and no explicit references to the literature will be made. In fact, this note was made from a more complete research paper having all proofs and all references by deleting them. I realize that the smoothness of its exposition is now largely lost. But I would leave it this way since TEX is more complicated and more time consuming than VOA and any combination of the two is even worse.

If V be a vertex operator algebra (over a field K of chracteristic 0), then for each $v \in V$ and $n \in \mathbb{Z}$, an element $v_n \in End_K(V)$ is given. Alternatively, we can say that for each $n \in \mathbb{Z}$, V is endowed with a bilinear map :

$$\phi_n : V \times V \to V.$$

Writing $\phi_n(v, w) = v_n w$, we can view $v_n \in End_K(V)$.

Each individual element v_n is less important than its generating function :

$$Y(v, z) = \sum_{n \in Z} v_n z^{-n-1}.$$

Relations among v_n for $v \in V$ and $n \in \mathbb{Z}$ are condensed in the Jacobi identity :

$$\begin{aligned} & z_0^{-1}\delta(\frac{z_1 - z_2}{z_0})Y(u_1, z_1)Y(u_2, z_2)u_3 - z_0^{-1}\delta(\frac{z_2 - z_1}{-z_0})Y(u_2, z_2)Y(u_1, z_1)u_3 \\ & = z_2^{-1}\delta(\frac{z_1 - z_0}{z_2})Y(Y(u_1, z_0)u_2, z_2)u_3. \end{aligned} \tag{1}$$

where

$$\delta(z) = \sum_{i \in \mathbb{Z}} z^i.$$

See the book written by Frenkel, Lepowsky and Meurman for the rule to expand quantities such as $\delta(\frac{z_1 - z_2}{z_0})$ into a sum of monomials in z_0, z_1, and z_2.

One of the more important and often used relations obtained from the Jacobi identity (1) is

$$[u_m, v_n] = \sum_{i \in \mathbb{N}} \binom{m}{i} (u_i v)_{m+n-i} \tag{2}$$

where u and v are arbitrary elements of the vertex operator algebra V.

We will use $Z(A)$ to denote the center of A, with A being a group, a ring, or any other algebraic system. For any graded algebraic structure $A = \sum A_i$, we use

$$x = \sum x(i)$$

or

$$x = \sum x^i$$

to denote its weight decomposition with $wt(x(i)) = wt(x^i) = i$. We often use *mapping weight* rather than *weight* to denote the weight of endomorphisms such as $v_n \in End(V)$ for a homogeneous element v of V.

Definition 1.
(a). $End_*(V)$ is the subalgebra of $End_K(V)$ generated by all v_n where $v \in V$ and $n \in \mathbb{Z}$: i.e.

$$End_*(V) = \langle v_n : v \in V, n \in \mathbb{Z} \rangle .$$

(b). $End_*^0(V)$ is the subalgebra of $End_*(V)$ consisiting of the elements of mapping weight 0.

Both $End_*(V)$ and $End_*^0(V)$ can be generated only by homogeneous elements in the sense below :

Lemma 2. *We have :*
(a). $End_*(V) = \langle v_n : v \in V_k, k \in \mathbb{Z}, n \in \mathbb{Z} \rangle$; and,
(b). $End_*^0(V) = \left\langle v_{n_1} v_{n_2} \cdots v_{n_r} : v_{n_i} \in V_{k_i}, \sum_{i=1}^{r} wt(v_{n_i}) = 0 \right\rangle$

Definition 3. A vector space M over the field K is a $End_*(V)$ module if M is graded as

$$M = \bigoplus_{r \in K} M_r$$

with M_r being the eigenspace for the weight operator $L(0) \in End_*(V)$ with eigenvalue r and $v_n M_r \subseteq M_{wt(v)-n-1+r}$ for all $v \in V, n \in \mathbb{Z}$, and $r \in K$.

Lemma 4. *Let $\{a_i; k_1 \geq i \geq -k_2\}$ be a subset of a vector space A over K. Suppose*

$$\sum_{i=-k_2}^{i=k_1} i^m a_i = b_m, \text{ for } k_1 + k_2 \geq m \geq 0.$$

Then a_i is a linear combination of b_m, $k_1 + k_2 \geq m \geq 0$ for all i.

Corollary 5. *Let a vector space M over K be a $\mathbb{Z}$ graded module of a ring R. Suppose an element $x \in R$ acts as the weight operator : i.e. $xm = wt(m)m$ for a homogeneous element $m \in M$. Let N be a submodule and*

$$\sum_i m_i = n \in N;\ m_i \in M, \text{with } wt(m_i) = i$$

where i ranges over some finite set I of consecutive integers (positive or negative). Then $m_i \in N$ for all $i \in I$.

Corollary 6. *Suppose $N = 0$ in Corollary 5. Then all $m_i = 0$.*

Theorem 7. *Let V be a vertex operator algebra and M be a $End_*(V)$ module. Then :*
(a). *Any submodule of M is graded.*
(b). *M is irreducible if and only if V_k is an irreducible $End_*^0(V)$ module for all k.*
(c). *If M is irreducible then the center of $End_*(V)$ consists of scalars.*

Theorem 8. *Let V be a vertex operator algebra. Then the following conditions are equivalent :*
(a). *$V = V_i$ for some i ;*
(b). *$L(0)$ is a scalar multiplication ;*
(c). *$L(0)$ is in the center of $End_*(V)$;*
(d). *$L(-1) = 0$;*
(e). *$Y(v, z) = v_{-1}$ for all $v \in V$;*
(f). *$End_*(V)$ is a commutative ring ;*
(g). *$V = V_0$.*

Definition 9. If a vertex operator algebra V does not satisfy any condition in the previous theorem, then it is called *nondegenerate.*

Henceforth, all vertex operator algebras considered will be *nondegenerate.* We next show that the set of operators $\{Id, L(n) : n \in \mathbb{Z}\}$ is linearly independent. We first restate the Corollary 5 in a slightly different way.

Lemma 10. *Let $\{v(i), k_1 \geq i \geq -k_2\}$ be a subset of $End_*(V)$ and suppose*

$$\sum_{i=-k_2}^{k_1} v(i) = 0, (wt(v(i)) = i),$$

then $v(i) = 0$ for all i.

Lemma 11. *$L(n) \neq 0$ for all n.*

Lemma 12. *The set $\{I_d, L(i), i \in \mathbb{Z}\}$ is linearly independent.*

We now raise the following question :

Question. Suppose $v_i = 0$ for some i. What can we say ? (Note that $v_{-1} \neq 0$ for $v \neq 0$, since $v_{-1} \cdot 1 = v$, in other words the mapping $v \to v_{-1}$ is injective).

The following example shows that $v_n = 0$ for a none zero $v \in V$.

Example 13. Let $V = V_L = S(\mathfrak{h}_{\mathbf{Z}}^-) \otimes K\{L\}$, the standard vertex operator algebra constructed from a suitable lattice L. Let

$$v = \alpha \otimes t^n \otimes e^0.$$

Then

$$Y(v,z) = \frac{1}{(n-1)!}(\frac{d}{dz})^{n-1}\alpha(z) = \sum \alpha(-m)z^{-m-1}$$

where the summation ranges over all negative m and all positive $m > n-1$. In other words $v_m = 0$ if and only if $n-1 \geq m \geq 0$.

Let us first make a few definition.

Definition 14. An element v of a vertex operator algebra V is said to be vacuum-like if $v_n = 0$ for all $n \neq -1$.

Every scalar multiple of the vacuum 1 is vacuum-like.

Lemma 15. *The following conditions for an element v of a vertex operator algebra V are equivalent.*
(a). *v is vacuum-like;*
(b). *$L(-1)v = 0$;*
(c). *$\frac{d}{dz}Y(v,z) = 0$;*
(d). *$u_n v = 0$ for all $u \in V$ and for all $n \geq 0$;*
(e). *$v_n u = 0$ for all $u \in V$ and for all $n \geq 0$;*
(f). *$v_n \cdot 1 = 0$ for $n \neq -1$.*

Lemma 16. *If v is vacuum-like then*

$$v_{-1}u = u_{-1}v$$

for all $u \in V$.

Corollary 17. *Suppose $v_k = 0$ for all $k \geq 0$. Then v is vacuum-like.*

Lemma 18. *Let n be a positive integer. Then $L(-n)$ is injective on V_k if*

$$24kn + (n^2-1)c \neq 0.$$

The following corollary is an immediate consequnce of Lemma 18.

Corollary 19. *Suppose $L(-1)v = 0$ for $v \in V_k$ for $k \neq 0$ then $v \in V_0$.*

Lemma 20. *Suppose v is vacuum-like. Then $v \in V_0$ and $v_1 \in Z(End_*(V))$.*

Lemma 21. *Suppose $v_{-i} \cdot 1 = 0$ for a positive integer i. Then $v_k = 0$ for all nonnegative integer k. In particular, v is vacuum-like.*

Corollary 22. *If v is not vacuum-like, then $v_n \neq 0$ for all negative integer n.*

Lemma 23. *Suppose an element v_k is in $Z(End_*(V))$ for some negative integer k, then v is vacuum-like.*

Lemma 24. *Let $v_n = 0, n \neq 0$ for an element v. Then $v_{n-1} = 0$.*

Theorem 25. *Let V be a vertex operator algebra. Then for any non vacuum-like element v of V, there exists an integer N such that $v_n = 0$ if only only if $j \geq N \geq 0$.*

Example 13 shows that the situation described in Thereom 25 actually occurs. For the vertex operator algebra V_L, the vacuum 1 and its scalar multiples are the only vacuum-like elements, since $\dim V_0 = 1$.

We have seen that if $v_n = 0$, then $v_{n-1} = 0$ also unless $n \neq 0$. If v is the highest weight vector we can prove a similar result going in the opposite direction, though not much else can be proved.

Definition 26. A vector v is a highest weight vector if $L(n)v = 0$ for all $n > 0$, and it is of height h if in addition $L(0)v = hv$ holds.

Remark. The highest weight vectors are called the lowest weight vectors in the book of Frenkel-Lepowsky-Meurman.

Lemma 27. *Suppose v is a highest weight vector of height h. Then $[L(1), v_n] = (2h - n - 2)v_{n+1}$. In particular, if $v_n = 0$, then $v_{n+1} = 0$ unless $n \neq 2h - 2$.*

Problems.

1. Is it possible that $End_*(V) = End(V)$? If not, how 'dense' is $End_*(V)$ in $End(V)$?

2. Characterize the conformal vector ω algebraically.

Thompson 級数の合同式

小池　正夫
九州大学数理学研究科

1 Introduction

Conway と Norton によって予想された Moonshine は Borcherds によって証明された。保型関数論を研究している私にとっては、Moonshine の研究をとうして、保型関数に関する問題を考える時には、この枠組みの中で考えられるかどうかをいつも気にかけるようになった。保型形式の合同式について、その歴史を追いながら、Moonshine で考えられる問題について述べる。

2 Ramanujan の仕事

分割数に関する Ramanujan の仕事が出発点にある。分割数 $p(n)$ は n を正の整数の和として表す、その表し方の個数として、定義され、次の母関数で書ける：

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty}(1-q^n)^{-1}$$

Ramanujan は次のような合同式を証明した。

$$p(5n+4) \equiv 0(\mathrm{mod}\ 5)$$

$$p(7n+5) \equiv 0(\mathrm{mod}\ 7)$$

Ramanujan がこの証明のために見つけた式は次のものである。

$$\varphi(q) = \prod_{n-1}^{\infty}(1-q^n)$$

とおくと、

$$\sum_{n-0}^{\infty} p(5n+4)q^n = 5\frac{\varphi(q^5)^5}{\varphi(q)^6}.$$

この、合同式の証明は他にも、Dyson による、分割数に対して rank という概念を定義して、これを用いて分割を細かく分類することで証明する方法もある。

高いべきの合同式もあり、それは $24n \equiv 1(\mathrm{mod}\ 5^a 7^b)$ ならば、

$$p(n) \equiv 0(\mathrm{mod}\ 5^a 7^c),$$

ただし、$c = [\frac{b+2}{2}]$ となる。これに関係したものを、数学セミナー [9] に発表したので、興味のあるかたは見てください。

3 J(z) に関する Lehner,Atkin の仕事

Ramanujan による分割数の合同式の研究に示唆されて、Lehner[11],[12] は modular 不変量 $J(z)$ の係数について、合同式を調べた。$J(z)$ は $SL_2(\mathbf{Z})$ に関する保型関数で、そのフーリエ展開を次の式でかく：

$$J(z) = q^{-1} + 744 + \sum_{n=1}^{\infty} c(n) q^n.$$

Lehner の証明した定理は

定理 3.1 *(Lehner)* $n \equiv 0(mod\ 2^a 3^b 5^c 7^d)$ に対して、次の合同式が成り立つ。

$$c(n) \equiv 0(mod\ 2^{3a+8} 3^{2b+3} 5^{c+1} 7^d).$$

Atkin[2] はさらに、11 に関する合同式も証明している。しかもそこでは、$p(n)$ と $c(n)$ とが、並べて議論されている。

$p(n)$ と比べて $c(n)$ の方の合同式の形がきれいになるのは、保型関数として $J(z)$ の方が素直なことによる。

4 Thompson 級数の合同式

Conway と Norton によって、見いだされた Moonshine の示唆するところは、保型関数についての性質を調べるときには、modular 不変量 $J(z)$ を孤立させて考察するよりも、Thompson 級数を全体として眺めて、その特別な場合として、$J(z)$ に関する性質が現れているとすると、思いがけない問題が見いだされる、という点にあると思います。

Thompson 級数について簡単に説明する。F_1を Monster と呼ばれる、散在的単純群で位数最大のものとする。F_1の共役類は 194 個あり、それらは $mA, mB, mC \cdots$と名前が付けられている。ここで m はその元の位数を表し、同じ位数の中で、その中心化群の位数の大きさの順番で $A, B, C \cdots$と名前が付けられている。たとえば、$1A$ と書いて、これは単位元を表す。位数 2 の元は $2A, 2B$の共役類をなす。

F_1の各共役類 gに対して、Thompson 級数と呼ばれる、具体的に定まった関数（フーリエ係数が計算できる）:

$$T_g(z) = q^{-1} + \sum_{n=1}^{\infty} H_n(g) q^n, q = e^{2\pi i z}, z \in \mathcal{H} = \{z \in \mathbf{C} \mid \Im z > 0\}.$$

が、存在して、以下の性質を満足する。

1. $T_{1A}(z) = J(z) - 744$.

2. 各 n について、$H_n(g)$ は gの関数として、F_1の指標である。

3. $T_g(z)$ は、種数 0 の Fuchs 群Γ_gの保型関数体の生成元である。

Thompson 級数が具体的にどうなっているか、例をあげる。

p を素数として、F_1の位数を割っているとする。すると、pA と書かれる F_1の共役類が定まる。このとき

$$\Gamma_{pA} = \Gamma_0(p)^+$$

となっている。この Fuchs 群は、あとで述べる$\Gamma_0(p)$ と Athin-Lehner involution で生成された群をあらわし、$p+$という記号で書かれる。この Fuchs 群の種数がいつも 0 になることが、Ogg によって注意され、Moonshine の発見のきっかけとなったのは有名な話です。

5 Thompson 級数の合同式

Thompson 級数の間の合同式でどういうことがいえるか、調べてみる。Thompson [13], では、まだ Moonshine 予想の証明ができていなかったので、次の定理が、予想の根拠として、述べられている。

定理 5.1 p を素数とする。gを F_1の元として、g^pは gを p 乗して得られる F_1の元とする。このとき次の合同式が成り立つ。

$$T_g(z) \equiv T_{g^p}(z) \ (mod\ p).$$

Moonshine 予想が証明され、Thompson 級数のフーリエ係数が指標であることがわかれば、逆にそれを用いて簡単にいえる。

従って、Thompson 級数の間には、群の乗法性からつながっている二つの元で、いつも合同式がなりたっているわけで、本当に注目すべき合同式は p の 2 以上のべきに関する合同式である。

Thompson [13] の論文で注意されている合同式がある。それは、

$$T_{1A}(z) \equiv T_{2B}(z) \ (\mathrm{mod}\ 2^{16}).$$

これについての、Thompson の説明は、M_{24}の知識がいるようで、私には理解できない。そこで次のような証明を考えた。

実は、もうひとつ別な Thompson 級数 $T_{2A}(z)$ を用意して、これら 3 つの保型関数の間の等式を利用する。それは、Thompson 級数の間に成り立つ Replication Formula をこれらの関数の間に適用して、得られる。それを書く前に、もうひとつ記号を説明しなくてはいけない。それは t_gで、

$$t_g = T_g(z) + constant,$$

という関係をみたすものを表す。だからt_gはThompson級数と定数でしか、違わないのだが、この定数を特定しないで使うのが便利がよい。しかも、t_gと書いてただひとつの決まった関数を表してはいない。定数が違っても同じ記号を用いる。次に与える式の中のt_gは、式が成立するためには、定数が特定されてくるのだが、あえてそれを書かないで、式が書けるのが便利なわけです。

$$t_{1A} = t_{2A} + t_{2A} \mid U(2). \tag{1}$$

$$t_{2A} = t_{2B} + \frac{2^{12}}{t_{2B}}. \tag{2}$$

$$0 = t_{2B} \mid U(2) + \frac{2^{12}}{t_{2B}}. \tag{3}$$

ここで、$U(2)$、一般には$U(p)$と書かれる作用素はヘッケ作用素で、次の式で定義される。

$$(\sum a_n q^n) \mid U(p) = p \sum a_{pn} q^n.$$

うえの式から、(3)を(2)に代入して、さらに得られた式を(1)に代入して、

$$t_{2A} = t_{2B} - t_{2B} \mid U(2). \tag{4}$$

$$t_{1A} = t_{2B} - t_{2B} \mid U(2)^2 \tag{5}$$

が得られる。
この最後の式から、次の定理が得られる。

定理 5.2 *次の(A)と(B)は互いに同値である。(C)が成り立てば、(A)が成り立つ。*

$$(A) \qquad T_{1A} \equiv T_{2B} \ (mod\ 2^{16}).$$

$$(B) \quad H_{4n}(2B) \equiv 0 \ (mod\ 2^{14}), n \geq 1.$$

$$(C) \qquad \chi(1A) \equiv \chi(2B) \ (mod\ 2^{16})$$

*(C)*では、χはF_1の指標を全て動く。

この中で、(C)は194個の指標について成り立つかどうかをAtlas[7]で調べればよい。(C)と(A)が同値であることは、ありそうなことだが、それは確かめてはいない。
(B)については、Lehnerの結果をみると、$J(z)$のフーリエ係数$c(n)$については類似の結果が証明されていることになっている. さらに、論文の中まで読むと、(B)それ自身が証明されていることもわかる。
これで、Ramanujanから始まって、Lehner,Atkinと続いた保型関数のフーリエ係数の合同にかんする性質の一部が、Monsterの指標の値に関する性質と、互いに同値であることがわかった。

6 定理

前の節で保型関数の三つの組 $\{t_{1A}, t_{2A}, t_{2B}\}$ を、使って説明したフーリエ係数の合同に関する性質が、これだけの例ではなくて、他にも存在することを述べる。そこでも、Moonshine という、優れた枠組みがあればこそ、見つけることが可能であったといえる。

定理 5.2 の証明の根拠が、三つの保型関数の間に成り立つ Replication Formula にあることに、注意すれば、それを同じように満たす三つの保型関数の組をみつければよい。それは、対応する Fuchs 群Γ_g で見た方が、互いの関係がはっきりしている。

そのためにΓ_gを書き表す記号を説明する。Conway と Norton の論文では、$\Gamma = N + S$と書かれる Fuchs 群がある。N の正の約数 Q が Hall divisor であるとは、$(Q, \frac{N}{Q}) = 1$ を満たすこととする。そして、Sは Nの Hall divisor 全体のなす集合のある部分集合をあらわす。

自然数 Nに対して、Fuchs 群$\Gamma_0(N)$ を

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z}, ad - bcN = 1 \right\}.$$

Nの Hall divisor Q にたいして、

$$W_{Q,N} = \begin{pmatrix} xQ & y \\ zN & wQ \end{pmatrix}, x, y, z, w \in \mathbf{Z}, xwQ - yz\frac{N}{Q} = 1.$$

で、定まる行列を Atkin-Lehner involution という。これは$\Gamma_0(N)$ の正規化群の元である。

Sの元である　Hall divisors に対する Atkin-Lehner involution $W_{Q,N}$達と$\Gamma_0(N)$ で生成される Fuchs 群を $N + S$と書いて表す。特に、Sが空集合と全体集合になっているときは、それぞれ、$N-, N+$と略して書く。

その記号を用いれば、三つ組 $\{t_{1A}, t_{2A}, t_{2B}\}$ に対応する Fuchs 群の三つ組は

$$\{1, 2+, 2-\}.$$

になる。

一般には、p を素数として、N を p と素な自然数とする。S'を pNの Hall divisors の集合で、それに含まれる全ての元 Q が p で割れないとする。そして、p と S'で生成される Hall divisors の集合を Sで表す。

ここで、$pN + S, pN + S'$が、Thompson 級数の Fuchs 群になっていると仮定する。そして対応する F_1の共役類を g, g'とする。このとき Thompson 級数の三つ組

$$\{t_{g^p}, t_g, t_{g'}\},$$

が、望むべき Replication Formula を満たすことがいえる。このような三つ組の表は次で与えられる：

p	g^p	g	g'	p	g^p	g	g'
2	1	2+	2−	2	3+	6+	6−
2	3−	6+2	6−	2	5+	10+	10+5
2	5−	10+2	10−	2	7+	14+	14+7
2	9+	18+	18+9	2	9−	18+2	18−
2	11+	22+	22+11	2	15+	30+	30+3,5,15
2	15+15	30+2,15,30	30+15	2	23+	46+	46+23
3	1	3+	3−	3	2+	6+	6+2
3	2−	6+3	6−	3	4+	12+	12+4
3	4−	12+3	12−	3	5+	15+	15+5
3	8+	24+	24+8	3	11+	33+	33+11
5	1	5+	5−	5	2+	10+	10+2
5	2−	10+5	10−	5	4+	20+	20+4
7	1	7+	7−	7	3+	21+	21+3

定理 6.1 素数 p と三つ組 $\{t_{g^p}, t_g, t_{g'}\}$, を上の表に現れているものをとってくる。このとき 2 以上の自然数αが定まって、次の *(A)* と *(B)* が同値である。*(C)* が成り立てば、*(A)* が成り立つ。:

$$(A) \qquad T_{g^p} \equiv T_{g'} \ (mod\ p^\alpha).$$
$$(B) \quad H_{p^2n}(g') \equiv 0 \ (mod\ p^{\alpha-2}), n \geq 1.$$
$$(C) \qquad \chi(g^p) \equiv \chi(g') \ (mod\ p^\alpha)$$

(C) では、χは F_1の指標を全て動く。

証明は定理 5.2 と同様である。

7 Atkin 予想

これについては、まだ何も結果はない。Moonshine がここでも役に立っているのではないかという希望があるだけです。

Atkin 予想については、Atkin [4],Koike[10], Akiyama [1] を見てください。

参考文献

[1] Akiyama,S., On the 2^n divisibility of the Fourier coefficients of J_q functions and the Atkin conjecture for $p = 2$, preprint.

[2] Atkin,A.O.L.,Proof of a conjecture of Ramanujan, Glasgow Math. J.,

[3] Atkin,A.O.L. and O'Brien,J.N., Some properties of p(n)and c(n) modulo powers of 13,

[4] Atkin,A.O.L.,Congruence Hecke operators, Proc.Symp. Pure Math.,12, 33-40.

[5] Borcherds,R.,Monstrous moonshine and monstrous Lie superalgebras,Inventiones Math.109(1992),405-444.

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

[7] Conway,J.H.,Curtis,R.T,Norton,S.P.,Parker,R.A., and Wilson,R.A., Atlas of finite groups,Clarendon Press,Oxford,1985.

[8] Koike, M., On replication formula and Hecke operator,preprint.

[9] 小池　正夫、ラマヌジャン- 無限の秘密を知る人、数学セミナー、3 月号、1995 年.

[10] Koike,M.,Congruences between modular forms and functions and applications to the conjecture of Atkin, J. Fac. Sci. Univ. of Tokyo,sec.IA,20 (1973),129-169.

[11] Lehner,J., Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$,Amer.J.Math,71 (1949),135-148.

[12] Lehner,J., Further congruence properties of the Fourier coefficients of the modular invariant $j(\tau)$,Amer.J.Math,71 (1949),373-386.

[13] Thompson,J.G.,Finite groups and modular functions, Bull. London Math. Soc.,11(1979),347-351.

The Leech lattice and the Niemeier lattices

北詰 正顕

千葉大 理学部 数学・情報数理学科

0 はじめに

散在型単純群 Monster に関する頂点作用素代数のある部分代数へ働く自己同型を調べたてみたところ，24 次元の（最も興味深い lattice である）Leech lattice と，他の 24 次元の even unimodular lattices (Niemeier lattices) との間のある関係に気付いたので，この場を借りて報告させていただく次第である。発端になった頂点作用素代数の話については，大まかな話にとどめることをお許しいただきたい。

ただ，問題の背景ならびに考察のきっかけは，頂点作用素代数と Griess 代数に関する宮本雅彦氏（愛媛大）の結果[1]にあることを明記しておく。

1 24 次元 even unimodular lattices

まず，表題の Leech lattice と Niemeier lattices について述べる。詳細（さらに本稿の全般）については，Conway-Sloane の本[2]（以下 [CS] と引用する）が参考になるだろう。

E^{24} を 24 次元の Euclid 空間とし，そこでの内積を $(\cdot,\cdot)$ で表す。$E^{24} \supset \Gamma$ を 24 次元 lattice，すなわち，$\mathbf{Z}$-module で E^{24} の基底を含んでいるものとする。Γ がさらに，

$\forall v \in \Gamma$ に対し (v,v) は偶数

をみたすとき even，また，

$$\Gamma = \{x \in E^{24} | (x,v) \in \mathbf{Z} (\forall v \in \Gamma)\}$$

をみたすとき unimodular と呼ばれる。このとき，簡単のために，(v,v)（偶数）を v の長さ（正確に言うなら squared length）といい，長さ $2n$ の元全体を Γ_n と表すことにする。Γ_1 の元を特に roots と呼ぶ。

24 次元の even unimodular lattices としては Leech lattice が，その全自己同型群の中心による商群が Conway の単純群 ($Co.1$) であるという事実，によりよく知られているが，それ以外のものもすべて分類されている。著しい事実は，それらがその roots の構造から一意に定まるということである。すなわち，

[1] 1994 年度代数学シンポジウム報告集

[2] J.H.Conway, N.J.A.Sloane: Sphere Packings, Lattices and Groups

定理 1 (Niemeier) Γ を *24* 次元 *even unimodular lattice* とするとき，Γ_1 は次の *24* 通りのいずれかであり，それぞれの場合に Γ は同型を除き一意に定まる。

$$\emptyset\text{（空集合）}, A_1^{24}, A_2^{12}, A_3^8, A_4^6, D_4^6, A_5^4D_4, A_6^4, A_7^2D_5^2, A_8^3, D_6^4, A_9^2D_6, E_6^4,$$
$$A_{11}D_7E_6, A_{12}^2, D_8^3, A_{15}D_9, D_{10}E_7^2, A_{17}E_7, D_{12}^2, A_{24}, E_8^3, D_{16}E_8, D_{24}$$

ただし，A_n, D_n, E_n は有限型（*spherical type*）の *root system* を表す。

$\Gamma_1 = \emptyset$ となるのが Leech lattice の場合である。以下，Leech lattice を L と表し，混乱をさけるため，L 以外を Niemeier lattices と呼ぶことにする。

2 主定理

本稿で紹介したい事実は，次のことである。

定理 2 N を任意の *Niemeier lattice* とするとき，L の *sublattice* K で $K \cong \sqrt{2}N$ となるものが存在する。

L, N は unimodular だから，$(\sqrt{2}N)^\perp = \frac{1}{\sqrt{2}}N$ となり，$L \supset \sqrt{2}N$ から $\frac{1}{\sqrt{2}}N \supset L$ が従う。よって，上定理は次と同値である。

定理 3 N を任意の *Niemeier lattice* とするとき，N の *sublattice* M で $M \cong \sqrt{2}L$ となるものが存在する。

証明は case-by-case で行う。それぞれの N について K を構成するのであるが，ひとつひとつのテクニカルな部分は省略することにして，本質的と思える部分を次の順序で進めていくことにする。

1. どうやって K を見つけるのか？ （$L/2L$ の構造に注目する）
2. 何を調べたことになるのか？ （Monster のある部分群の位数 2 の元）
3. 何故，これを調べたくなったのか？ （頂点作用素代数からの話）

Leech lattice に関する事実については，self-contained に書くことをやめて [CS] に譲ることにする。

なお，Niemeier lattice のうち E_8^3型については，ここで与えた Leech lattice との関係はすでによく知られたもので，このことを利用した Leech lattice の構成法が知られている。[3]

[3] J.I.Lepowsky, A.E.Meurman, An E_8−approach to the Leech lattice and the Conway group, J.Alg. 77(1982),484-504

3 $L/2L$

Leech lattice L に対し，$\bar{L} = L/2L$ とおく。$\bar{L}$ の構造はよく知られていて，加群としては2元体 ($\mathbf{F}_2 \cong \mathbf{Z}/2\mathbf{Z}$) 上の24次元のベクトル空間になる。このとき $\bar{x} = x + 2L \in \bar{L}$ に対し，$f(\bar{x}) := \frac{1}{2}\langle x, x\rangle \pmod 2$ により2次形式が定義されるが，$\bar{L}$ はこれにより plus type の orthogonal space になる。付随する内積は，$(\bar{x}, \bar{y}) := \langle x, y\rangle \pmod 2$ で与えられる。

そこで，$\bar{K} \subset \bar{L}$ を max. totally isotropic subspace とし，L での全逆像を K とおく。このとき，totally isotropic であることから，

$f(\bar{x}) = 0$ より $\langle x, x\rangle \in 4\mathbf{Z}$

$(\bar{x}, \bar{y}) = 0$ より $\langle x, y\rangle \in 2\mathbf{Z}$

となり，これより $\frac{1}{\sqrt{2}}K$ は even integral であることがわかる。さらに，$[\bar{L} : \bar{K}] = 2^{12}$ から $\det K = 2^{12\times 2}$ であるから $\frac{1}{\sqrt{2}}K$ は unimodular である。

従って，$\frac{1}{\sqrt{2}}K$ は24次元 even unimodular lattice であるから，定理1の24通りのいずれかである。定理2の証明のためには，$(\frac{1}{\sqrt{2}}K)_1$ の構造が定理1に現れる23通り（$\emptyset$ 以外）になるように K を選べばよい。$(\frac{1}{\sqrt{2}}K)_1 \subset L_2$ であるから，L_2 から望ましいものを選んでくることになる。L_2 の typical な元を書いておく。

$$\frac{1}{\sqrt{8}}(\pm 2^8, 0^{16}), \quad \frac{1}{\sqrt{8}}(-3, 1^{23}), \quad \frac{1}{\sqrt{8}}(\pm 4^2, 0^{22})$$

ここで，第1の元の意味するところは，± 2 が8カ所に現れ（実は$-$は偶数個）他の16カ所が0であることを意味する。どういう8カ所に現れ得るかということは，Golay code もしくは Steiner system と関連して記述できるのであるが，ここでは深入りしない。

Kの構成のいくつかを例示しておこう。D_{24}型の root system を作るには，第3の種類の元をすべて取ればよい。A_{24}型の場合は，第2の種類の元24個と，第3のもののうち $4, -4$ が1カ所ずつのものすべてを取ればよい。

もちろん root system（R とおく）を作るだけでは K を作ったことにならないが，R を含む Niemeier lattice が一意的に定まる場合ならば，$\bar{R}$ を含む max. totally isotorpic を $\bar{K}$ とすれば，$(\frac{1}{\sqrt{2}}K)_1 = R$ となる。例えば $R = D_8^3$ の場合は，これが D_{24} に含まれ得るので，上記の手順では $(\frac{1}{\sqrt{2}}K)_1 = D_{24}$ となり得る。従って，このような場合には $\bar{K}$ をさらに詳しく与えなければならない。細かい議論についてはここでは省略する。

最後に後で使われる事実を2,3注意しておく。

まず，$\bar{L}$ の代表系は L_2, L_3, L_4 から取れる。さらに，長さが異なるものは $\bar{L}$ で一致することはなく，L_2, L_3 の場合は，各元の± 1 倍だけが$\bar{L}$ で一致する。L_4 の場合には48個が$\bar{L}$ で一致するが，± 1 倍を除けば本質的には24個である。これらは $\mathbf{R} \otimes L$ の直交基底を作ることが知られている。

次に $x, y \in L_2$ とする。簡単な内積計算から，

$$\begin{aligned} \langle x, y\rangle = \ & -1 \ \Leftrightarrow \ x - y \in L_2 \\ \langle x, y\rangle = \ & 0 \ \Leftrightarrow \ x - y \in L_4 \end{aligned}$$

がわかる。すなわち，でき上がった Niemeier lattice の root による鏡映の積の位数は L における計算から決定できる（前者が位数 2，後者が位数 3)。

4 Monster の 2A-involution

Monster の involution は 2 class あって，$2A$ と称されるのはその中心化群 $C(2A)$ に Baby monster が現れるもの，$2B$ は $C(2B)$ に Conway 群が現れるものである。より詳しく書くと，$C(2A) \cong 2 \cdot BM$, $C(2B) \cong 2^{1+24} \cdot (Co.1)$ である。

ここで，$Q := O_2(C(2B)) \cong 2^{1+24}$ とおく。$Q/Z(Q)$ は 2 元体上の 24 次元のベクトル空間になり，2 次形式が $\bar{x} = xZ(Q) \in Q/Z(Q)$ に対し $f(\bar{x}) := x^2 \in Z(Q)$ で与えられる。ただし，位数 2 の群 $Z(Q)$ を 2 元体と同一視している。特に，$f(\bar{x}) = 0$ は x が involution であることと同値である。

さて，この $Q/Z(Q)$ が $Co.1$−加群として $\bar{L} = L/2L$ と同型になのである。

Q での involutions に対応するのは，L の長さ偶数の元であるが，前節で注意したように，L_2, L_4 のいずれかの元が代表元に取れる。実は，L_2 に対応するのが Q の $2A$−involutions で，L_4 に対応するのが $2B$−involutions である。

また，$\bar{L}$ で考えていた totally isotropic という性質は，Q では可換部分群を考えていることに相当する。

従って，前節（従って，定理 2,3）で考えていたものは，Q の最大（位数は 2^{12}になる）可換部分群と，その中の $2A$−involutions の構造だということになる。前節の最後の部分を述べ直せば，(雑な記号を用いるが) x, y を $2A$−involutions または（対応する）L_2 の元とするとき，

$$xy \in 2B \quad \Leftrightarrow \quad x - y \in L_2$$
$$xy \in 2A \quad \Leftrightarrow \quad x - y \in L_4$$

となる。

5 頂点作用素代数と Griess 代数

頂点作用素代数 (VOA)（特に Monster 代数）と Griess 代数に対する宮本雅彦氏の結果というのは，VOA の central charge $\frac{1}{2}$ の conformal vector と Griess 代数の巾等元とが 1:1 に対応すること，さらに，これらから位数 2 の自己同型を構成する方法を与えたことである。

Monster の場合，構成される involutions は $2A$−involutions であり，(前節で調べた) 最大可換部分群（これを E とおく）には 48 個の互いに可換なものが含まれている。(このことは，Monster 代数の Virasoro 元の central charge が 24 であるという事実に対応しており，等式 $24 = \frac{1}{2} \times 48$ で表される。)

さて Monster 代数を慣例により $V^\natural$ とあらわし，E による固定元全体のなす部分代数を $V_E^\natural$ とおく。E の $2A$−involutions は $V_E^\natural$ に自明に働くが，宮本氏の構成によるとこのような（構成された自己同型が自明だった）場合には，さらに別の方法で位数 2 の自己同型が

構成される。(これも自明だったときはVOAの構造が強く制限されるが，ここでの話には該当しない。) この新たな（実際，$V^\natural$ には作用しない）$V_E^\natural$ の自己同型たちのなす構造が，定理2にあるNiemeier latticesのrootsによる鏡映たちの関係に一致するのである。

実際，自己同型たちの積の位数は $V^\natural$ における内積の値から計算することができ，それはさらに最初の $V^\natural$ の自己同型の積の状態を規定する。すなわち，$a, b \in V^\natural$ から作られる $V^\natural$ の自己同型を τ_a, τ_b，と表し，$V_E^\natural$ の自己同型を σ_a, σ_b と表すとき，

$$\tau_a\tau_b \in 2B \quad \Leftrightarrow < a, b >= \tfrac{1}{16} \quad \Leftrightarrow (\sigma_a\sigma_b)^3 = 1$$
$$\tau_a\tau_b \in 2A \quad \Leftrightarrow < a, b >= 0 \quad \Leftrightarrow (\sigma_a\sigma_b)^2 = 1$$

が成り立つ。従って，これまでの結果から，σ_a たちのなす群の構造が決定できる。

6 おわりに

講演中に坂内先生からも質問を受けたが，Niemeier lattices と Leech lattice の関連に関しては，すでによく知られた事実がある。

Leech lattice L に対し，$v \in \mathbf{R} \otimes L$ で L との距離が最も大きなものを考える。この最大値（covering radius）が $\sqrt{2}$ になるというのが，Conway-Parker-Sloaneの定理で，さらに，v たちは自己同型群の作用を除いて23通りあって，v を中心とする半径 $\sqrt{2}$ の球面上にある L の元（正確には L の元 x に対する $x - v$）たちが23通りのNiemeier latticesのfundamental roots systemを作るのである。

最初に定理2に気付いたとき，それは上の定理のcorollayなのだろうと思い（そして今でも少しはそう思っているのであるが）考えてみたのだが直接には結びつかなかったという事情がある。数学的にはcorollaryである方がすっきりしているようにも思えるのだが，実際はどうであろうか？

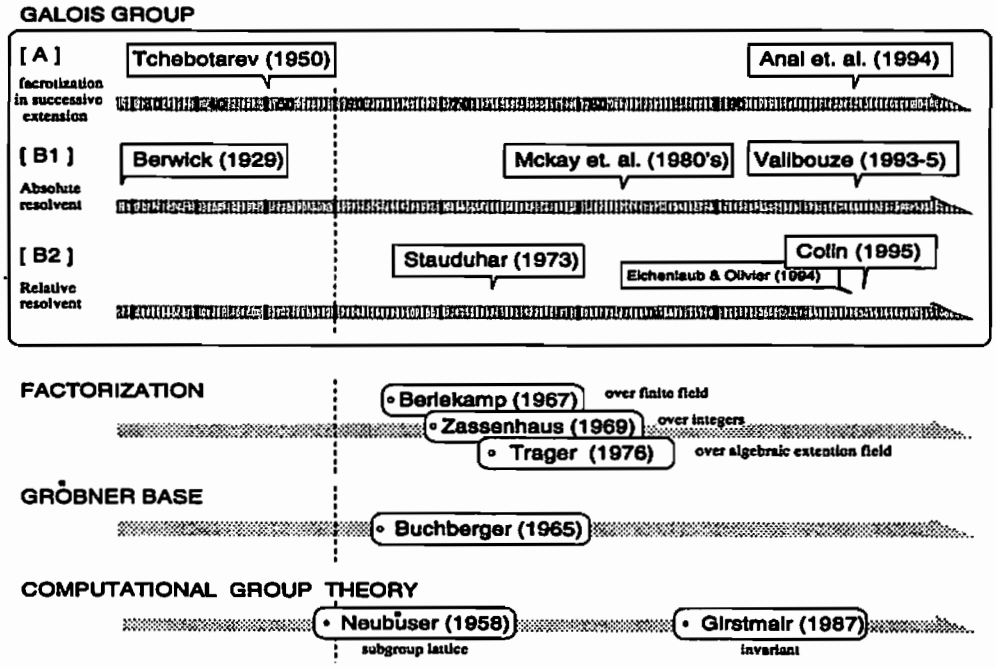
ガロア群計算の最新状況*

富士通情報研
穴井 宏和 横山 和弘
e-mail: {anai, momoko} @iias.flab.fujitsu.co.jp

1995. 7. 31

1 はじめに

現在まで, 実際に多項式の Galois 群を計算しようとする試みがいろいろとなされてきた. 本稿では, 我々自身の結果も含め, それらについて簡単に紹介する.



歴史的に見れば, Galois 群の計算は Berwick(1929) や Tchebotarev (1950) の研究に遡る. 前者は, Galois 群の決定のための完全な形での 6 次の多項式の absolute resolvent (§3 参照) の partition の表 (分割行列 (partition matrix)) (§3.1 参照) を示しているが, その構成法は algorithmic なものではなく, 後者は, 多項式

*「第 12 回代数的組合せ論シンポジウム」於 東京大学駒場 (1995. 7. 29 - 31)

の根の満たす全ての多項式からなるイデアルの標準基底から, 根の置換群として Galois 群を求める方法を提示したに留まる.

計算機の進歩と 1960 年代より始まる数式処理 (computer algebra) の研究 (算法及びシステム) の進展を背に受け, 1970~80 年代になって Stauduhar や McKay *et. al.* らの研究が現れる. McKay*et. al.* の方法は Berwick の方法に続くものであり, 有限体上での因数分解より cycle 型 (§3.3 参照) の情報も併用した. 彼らの 7 次までの成果は実際に数式処理システム Maple [24] に実装された. Stauduhar は relative resolvent (§4.1 参照) を用いた方法を示し, 数値的手法を用いて 7 次まで試された.

McKay *et. al.* 以降 10 年ほど後, ここにきて Anai *et.al.*(1994), Valibouze(1993-5) そして Colin(1995) といった次の世代の研究が出てきた. Valibouze は McKay*et. al.* の方法をさらに 8 次以上の場合にも拡張するよう, 分割行列の algorithmic な構成法を示し, また resolvent の因子の Galois 群の計算を利用した. Colin は Stauduhar の数値的手法を, 記号的に行なうことを目的とし対称関数を利用した. Anai *et.al.* は computer algebra の良い Bench-Mark として, また新たな代数拡大上の因数分解の算法の応用と根のベキ根表示を目的に, 根の置換群として Galois 群を求める方法を示した. これは, (Tchebotarev とは独立に考えて) 多項式の根の満たす全ての多項式からなるイデアルの標準基底から Galois 群の元を決める方法と新たな代数拡大上の因数分解法と strong generator の組合せにより実現された. resolvent を用いる方法では, その invariant の生成も重要な鍵でありこれについては Girstmair(1987) [20] のアルゴリズムが大きく貢献している.

これらの多項式の Galois 群の計算方法は, [A] 逐次的な拡大体 (successive field extension) における因数分解に基づくものと [B] 分解式 (resolvent) に基づくものとの大きく 2 つに分けることができる. また, resolvent を用いた Galois 群の計算法には, [B1] 絶対分解式 (absolute resolvents) と [B2] 相対分解式 (relative resolvents) のどちらを利用するかにより 2 種類の異なる方法がある. それぞれについての主な研究の特徴を簡単に記した表を示す.

	[*A*]	[*B*1]		[*B*2]	
	Anai *et. al.*	McKay *et. al.*	Valibouze	Stauduhar	Colin
Output Form	permutation group	name	name	name	name
Available Degree	arbitrary	degree ≤ 7	degree ≤ 11	degree ≤ 11	(degree ≤ 15)
Applicability	irreducible	irreducible	≤ 7 sq-fr 8~11 irred.	irreducible	need not irred.
Effectiveness	small order	degree ≤ 7	degree ≤ 11	degree ≤ 11	(degree ≤ 15)
Symbolic/Numerical	symbolic	symbolic	symbolic	numerical	symbolic
Implimentation	complete	complete	complete	complete	incomplete
Availability	Risa/Asir	Maple	GAP etc (?)	?	(AXIOM, GAP)

[A] は逐次拡大における与えられた既約多項式 f ($deg(f) = n$) の因数分解すなわち, 分解体の計算をもとに, Galois 群を根の置換群として構成する. (これは直接法 (direct approach) とでも呼べる.) よって, 任意の次数の多項式について適用可能である. しかし, 分解体の計算は, 代数拡大体上の因数分解の繰り返しにより実現され, かなり大変な計算でありこの部分が最大の障壁になる (Appendix の表 Table 1. 参照). 分解体が求まると, S_n の任意の元が Galois 群に属すかどうかを, (S_n の元を用いて定義される) ある多項式の, f の根の満たす関係式からなる ideal への所属問題に帰着させて判定する. この計算は容易であるが, 実際には, 分解体の計算のために位数が 200 程度までの Galois 群ならば計算可能という状況にある. この方法の 1 つの大きな動機付けとなるのは, 多項式の根の巾根表示である. そのためには, Galois 群の根の置換群としての表現が必要になるからである ([2] 参照).

[B1] の方法は, 考えている次数 n についての absolute resolvent の partition の表により Galois 群を同定する. そのため, n 次での partition の表を前もって構成する必要があり (この partition の表を構成するには, n 次の対称群の全ての部分群の表が必要である), その表が存在する次数に対しては, absolute resolvent の因数分解を行なえば, Galois 群は決定する. よって, この方法は, partition の表が存在する次数に対しては Galis 群を決定できるのである (Appendix の Table 2. 参照). さらに, mod p での因数分解による cycle 分解や resolvent の因子の Galois 群の情報等と兼ね合わせて Galois 群を絞っていくことで, より効率的な検索が可能になる. 実際, Mckay *et. al.* は mod p での因数分解を, Valibouze は resolvent の因子の Galois 群の情報を併用している. resolvent の因数分解で一意に Galois 群が決まるような完全な表を求めておくのが理想であるが, 次数が大きくなるとそれが大変になる. したがって, このようにいくつかの "ふるい" を使うことは効率化だけでなく, (この表だけで一意に Galois 群が決まらないと言う意味で) 不完全な表しか得られてなくても他のふるいの利用でその表も有効に利用され得ることにつながる.

[B2] の方法は, S_n の部分群の有向グラフを, Galois 群がどの部分群に含まれるかによって辿っていくことで Galois 群を同定する. よって, この方法の実現にも n 次の置換群の全ての部分群の知識 (表) が欠かせない. Galois 群がどの部分群に含まれるかのテストの際に relative resolvent を利用するのである. Stauduhar は relative resolvent の計算を根の近似値を用い数値的に計算した. この場合, 包含関係のテストの際に, resolvent の根すなわち根のある多項式が整数であるかどうかの判定が必要となるが, 数値的手法を用いて整数であることを保証するには, 少なくとも数百から数千桁の精度が要求され容易ではない. Colin の方法は relative resolvent の計算を記号的に行なう. それゆえ, S_n-共役類の有向グラフを辿ることになる. また, resolvent を記号的に計算するおかげで, 包含関係のテストは relative resolvent の因数分解によって実現される.

Galois 群の実際の計算のいろいろな場面において, 上記に見られるように, 因数分解の果たす役割は大きい. したがって, 実際の計算では因数分解の計算アルゴリズムの効率化は必然的に重要になる. 多項式の因数分解は 1967 年の Berlekamp による有限体上の因数分解法 [11] をその起源とする. そして, 1969 年の Zassenhaus による Hensel 構成を利用した整数係数多項式の因数分解法 [38] 以降, 改良拡張が重ねられ急速に発展した. 代数的拡大体上の多項式の因数分解についても 1976 年の Trager による方法 [35] を始めいくつか示されている. その果たす役割の大きさゆえに, Anai *et.al.* はもとより, 因数分解が全ての方法の共通の隘路となる. 考えている次数に対する群の表が存在したとしても, Colin や Valibouze の方法も 10 次を越えると非常に困難になる. 実際, Valibouze の方法では, 分割行列の計算において膨大な次数の因数分解が必要となり 13 次以降へは進めないし, Colin の方法では, まだ 4,5 次の場合位しかできていない. ただし, Colin の方法の場合には linear factor の計算である点で計算可能な範囲は広がる可能性はある.

それぞれの方法は, 実際の計算の結果, ある程度, 次数等に対して適性があることがわかる 曖昧な言い方ではあるが以下に列記する. ; (i) Anai *et. al.* : Galois 群の位数が小さい, または, 分解体を構成するのに基礎体に添加すべき根の数を ℓ としたとき ℓ が 2, 3 程度の場合. (ii) Valibouse : Galois 群が S_n, A_n に近い場合. (iii) Colin : Galois 群が大きくもなく小さくもない場合. よって, Galois 群の計算の効率を求めるのであれば, 適性に応じて使い分けることが大切である.

"table-based" approach とでも言える [B1][B2] の方法は, 表 (table) が求まってさえいればある程度高速に Galois 群を決定できる. これらは, n 次の全ての (可移) 群の知識を必然的に仮定するが, 現在 n 次の可移群の表は, 15 次まで得られている ([15], [16], [26], [28] 参照). よって, そもそもここに挙げた [B1][B2] の 4 つの方法は現時点で最高 15 次の多項式までしか適用できない. その意味で, Colin の方法はまだ計算機に実装はされていないが Available Degree を 15 次以下と示しておく. (GAP で 任意の群の全ての部分群の束 (lattice) の計算が可能であるが, 実際には, S_{15} より先には進めない [17].)

こうした多項式の因数分解や整係数1変数多項式のGCDといった計算のアルゴリズムの研究から現在の数式処理(Computer algebra)は始まった．数式処理とは，基本的には多項式処理である．その基礎となるのが，GCDや因数分解であり，それらを組み合わせで実現した代数的数(代数拡大)の操作である．その数学的基盤を成すのが，代数理論である．また，数式処理は，計算手順を扱う学問であり，したがって，算法の効率は非常に重要な点である．新たな算法の開発には，数学的背景を基に，計算効率の点を重視した形での理論構築を行なうことになる．(因数分解，GCDなど代表的なアルゴリズムは[21]参照.)

現在まで，30年近い時間の積み重ねと計算機の飛躍的進歩とが合間って，ある程度(かなり?)の数学上の操作を計算機で実現することが(実際の計算機で答えがでるという意味で)可能となってきている．実際に，数式処理研究と計算機の利用無しでは到底得られないさまざまな結果が示されてきている．Galois群の計算はその一例であり，Galois群の計算に限って言えば，数式処理の基本的演算である因数分解や対称関数の計算，そしてcomputational group thoryでの理論，システム両方の進歩があって始めて可能となり，それがここにきて新しい世代の成果として発現したのである．こういう様相は，純粋に数学的に見れば明らかなことであるかも知れないが，完全とは言えないまでも，数学理論の実験道具として使えるようになってきていることを物語っている．

2 体の逐次拡大による方法

Tchebotarev (1950) [34] は多項式 f の根の満たす関係式からなる ideal に注目し，辞書式順序でのこの ideal の標準基底から f の Galois 群を計算するという方法を提示した．この方法の実現には計算機代数(computer algebra)の分野での，因数分解のアルゴリズムやグレブナ基底(Gröbner base)の計算アルゴリズム[12]などの発展に依るところが大きい．実際，Anai *et. al.* (1994) [1] [3] に見られるように，代数拡大体上の因数分解の効率化とグレブナ基底についての正規形(normal form)の計算([12]参照)がその効率化の鍵となる部分である．この節では，Anai *et. al.* [1] の方法について述べる．

この方法は，考えている多項式の各根を正確に記述し，Galois群の元は各根の置換として求める．そこで，Galois群計算として，まず多項式 $f(x)$ の分解体を求め，その分解体の上で各根を表現することを行なう必要がある．そこで，整数係数の一変数多項式 $f(x)$ の最小分解体 K_f を求め，K_f 上ですべての根を表すことを考える．問題を簡単化するために，$f(x)$ は有理数体上既約であるとする．このために用意される道具が，(i)代数的拡大の表現法，(ii) (i)で表現された代数的拡大体上での多項式の因数分解である．この2つがあれば，$f(x)$ の根を逐次添加して拡大体を構成し，その体の上で $f(x)$ が一次因子の積に分解されるまで続ければ最小分解体が求まる．

2.1 代数的拡大の表現

数式処理(多項式処理)で，代数的拡大体を求めるということは，基礎体 $\mathbf{Q}$ =有理数体 上で，多項式環の剰余類環として表現することである．つまり，有限次代数的拡大体 K が代数的数 $\alpha_1, \alpha_2, \ldots, \alpha_r$ を $\mathbf{Q}$ に添加して得られるならば，各代数的数 α_i に変数 x_i を割り当てて，$\alpha_1, \ldots, \alpha_r$ が満たすすべての代数関係から導かれる多項式全体の集合 I (これは極大イデアルになる)で多項式環 $Q[x_1, \ldots, x_r]$ を割った剰余類環 $K' = Q[x_1, \ldots, x_r]/I$ を作る．このとき，体としての同型写像

$$\phi : K \to K' \text{ ここで } \phi(\alpha_i) = x_i \pmod{I}$$

が得られる．ひとたび，体が剰余類環で表現されれば，体上の四則演算は剰余類の上で定義されることになる．このとき重要な点は，「体の元にはその剰余類の代表，すなわちある多項式が割り当てられる」ことである．

この, 各剰余類から代表を一つ定める操作 ρ が与えられれば, ($\rho : \mathbf{Q}[x_1, \ldots, x_r] \to \mathbf{Q}[x_1, \ldots, x_r]$) 剰余類環の上の和および積 $\bar{+}, \bar{\times}$ は,

$$\rho(a)\bar{+}\rho(b) = \rho(\rho(a) + \rho(b)), \quad \rho(a)\bar{\times}\rho(b) = \rho(\rho(a) \times \rho(b))$$

で与えられる. ここで, $+, \times$ は多項式環での通常の和と積を表す. この一意的に定める代表系を normal form といい, この操作は, 一般のイデアルでは Grōbner 基底と M-簡約操作により実現される. (0 を含む剰余類の normal form を 0 になるように定める.)

2.2 多項式の代数的拡大体上での因数分解と最小分解体

代数的拡大体上の多項式の因数分解のスキームは単純である. (このスキームは B. Trager により提案されたもの [35] を基本とし, ノルム法と呼べるものである.)

2 つの体 K, L に対して, $L = K(\alpha)$ であるとする. (α は K 上代数的であるものとする.) このとき, L 上の多項式の因数分解は, 以下の計算法が存在すればよい.

(1) K 上の多項式の因数分解法が存在,

(2) L 上の 2 つの多項式の GCD 計算法が存在,

(3) L/K のノルム計算法が存在

ノルム写像 $Norm_{L/k}$ は 多項式環 $L[x]$ から $K[x]$ への射影に以下のように自然に拡張される.

$$Norm_{L/K}(g(x)) = \sum_{i=0}^{n} Norm_{L/K}(g_i)x^i \text{ for } g(x) = \sum_{i=0}^{n} g_i x^i.$$

因数分解のスキームは, 以下の図式で表すことができる.

$$\begin{array}{ccc} g(x) & \xrightarrow{\text{因数分解}} & g(x) \text{ の既約因子全体} \\ {\scriptstyle NormL/K}\downarrow & & \uparrow{\scriptstyle GCD\text{計算}} \\ Norm_{L/K}(g) & \xrightarrow[\text{因数分解}]{} & Norm_{L/K}(g) \text{ の既約因子全体} \end{array}$$

ここで, 次が言える.

(A) 体を係数環とする多項式の GCD は, 体上の四則演算が計算できるならば, 基本的には Euclid の互除法により実現できる. (効率化の工夫として, 部分終結式法, modular 技法による補間法等がある.)

(B) $Norm_{L/K}$ の計算は, α の K 上の最小多項式 $m(x)$ を用いて, 終結式により計算できる. すなわち, $\beta \in L$ は剰余類環 $K[y]/ < m(y) >$ の元 $\beta(y)$ として表されている. この β に対し,

$$NormL/K(\beta) = resultant(\beta(y), m(y)) = \det(S(\beta(y), m(y))$$

となる. ここで, $S(\beta(y), m(y))$ は 2 つの多項式 $\beta(y), m(y)$ の Sylvester 行列である.

この 2 点より, L 上の多項式の因数分解は K 上の多項式の因数分解が存在すれば存在することになり, 逐次添加拡大の場合には, これを繰り返せばよい. ここでの基本となる定理を挙げておく.

定理 1 $f(x)$ を $L = K(\alpha)$ 上の一変数多項式とする. このとき
(1) f が L 上既約ならば $Norm_{L/K}(f)$ は K 上既約な多項式のベキになる.

(2) $Norm_{L/K}(f)$ が無平方，すなわち重複因子を持たない，とする．このとき，$Norm_{L/K}(f)$ の K 上の既約因子全体と f の L 上の既約因子全体の間に一対一対応が存在する．さらに詳しくいえば，$Norm_{L/K}(f)$ の K 上の既約因子 p に対して，$GCD(f,p)$ が対応する f の L 上の既約因子となる．
(3) f が無平方であるならば，ある整数 s が存在して，$Norm_{L/K}(f(x-s\cdot\alpha))$ は無平方にできる．このような s をとれば，f の L 上の既約因子と $Norm_{L/K}(f(x-s\cdot\alpha))$ の K 上の既約因子との間に次の一対一対応ができる．p を $Norm_{L/K}(f(x-s\cdot\alpha))$ の K 上の既約因子とすれば，$GCD(f(x),p(x+s\cdot\alpha))$ は f の L 上の既約因子となる．
(4) 上記の整数 s は，以下のように拡大体の意味で特徴付けられる．f の任意の根 β に対して，$\beta-s\cdot\alpha$ は $K(\alpha,\beta)$ の K 上の原始元である．無平方にならない s に対応する $K(\beta-s\cdot\alpha)$ は $K(\alpha,\beta)/K$ の中間体である．

注意 1 *Trager* のスキームにより，$f(x)$ の最小分解体を求める簡潔な手段が得られる．しかし，そこでは，定理 *1* で示した無平方を実現する s を探さなくてはならない．また，$Norm_{L/K}(f)$ の次数は f の次数× L/K の拡大次数であり，因数分解のコストが大変大きなものになってしまう．さらに，中間体 *(定理 1 (4)* を参照*)* を考えれば，多項式の最小分解体の計算においては，ノルムが無平方にならない場合が多発することがわかる．一般には，因数分解のコストと *GCD* のコストでは，雲泥の開きがある．*(*計算量の理論では，最悪の場合に最もよい計算量を持つ算法を比べた場合でも，入力される多項式の次数に関して $O(n^9):O(n^4)$ である．*)* かえって，無平方でない場合の方が，$Norm_{L/K}(f(x-s\cdot\alpha))$ の自明でない因子 *(*既約でなくてもよい*)* を効率良く求めることができ，その自明でない因子分解 $Norm_{L/K}(f(x-s\cdot\alpha))=\prod_{i=1}^{r}p_i^{e_i}$ より *(*e_i は p_i の重複度*)*，f の自明でない因子分解 $f(x)=\prod_{i=1}^{r}GCD(f,p_i(x+s\cdot\alpha))$ が得られる．この方法は，非常に最小分解体の逐次添加表現の計算に適していることが，体の性質から，さらには具体的な実験例から示すことができる．この方法を修正ノルム *(Modified Trager)* 法と呼ぶ．

与えられた $\mathbf{Q}$ 上の多項式 $f(x)$ の最小分解体は，以上の代数拡大体上の因数分解を繰り返すことで求まる．すなわち，

方法 1 $f(x)$ の根を一つとり α_1 とする．また，$f_1=f$ とおく．
(1) f を $\mathbf{Q}(\alpha_1)=\mathbf{Q}[x_1]/<f_1(x_1)>$ で因数分解する．このとき，$f=(x-\alpha_1)\cdot g_{1,1}\cdots g_{1,s}$ と因数分解される．f の既約因子がすべて一次因子なら $\mathbf{Q}(\alpha_1)$ が求める最小分解体．そうでない場合は，一次でない既約因子を一つとり f_2 とおく．f_2 の根を一つ決め α_2 とおく．
(2) f を $\mathbf{Q}(\alpha_1,\alpha_2)=\mathbf{Q}[x_1,x_2]/<f_1(x_1),f_2(x_2,x_1)>$ で因数分解する．このとき，$f=(x-\alpha_1)(x-\alpha_2)\cdot g_{2,1}\cdots g_{2,s_2}$ と因数分解される．f の既約因子がすべて一次因子なら $\mathbf{Q}(\alpha_1,\alpha_2)$ が求める最小分解体．そうでない場合は，一次でない既約因子を一つとり f_3 とおく．f_3 の根を一つ決め α_3 とおく．

$\vdots$

(k) f を $\mathbf{Q}(\alpha_1,\ldots,\alpha_k)=\mathbf{Q}[x_1,\ldots,x_k]/<f_1,\ldots,f_k>$ で因数分解する．このとき，$f=(x-\alpha_1)\cdots(x-\alpha_k)\cdot g_{k,1}\cdots g_{k,s_k}$ と因数分解される．f の既約因子がすべて一次因子なら $\mathbf{Q}(\alpha_1,\ldots.\alpha_k)$ が求める最小分解体．そうでない場合は，一次でない既約因子を一つとり f_{k+1} とおく．f_{k+1} の根を一つ決め α_{k+1} とおく．

結局，ある整数 $\ell\le\deg(f(x))$ が存在して，この手続きは終了する．この ℓ を最小分解体の表現の長さという．ℓ は選ぶ $f_2,\ldots$ に依存して決まることに注意する．

2.3 Galois 群の計算

前節で，代数的拡大体上の多項式の因数分解を用いて $f(x)$ の最小分解体がもとまる．このとき，次のように表現されている．$f(x)$ の根 $\alpha_1,\ldots,\alpha_n$ には変数 $x_1,\ldots,x_n$ が割り当てられる．表現の長さを ℓ とすれば，

$\alpha_{\ell+1},\ldots,\alpha_n$ は$\alpha_1,\ldots,\alpha_\ell$ の多項式で表されていることになる. したがって,

$$K_f = \mathbf{Q}[x_1,\ldots,x_n]/ < f_1,\ldots,f_n >$$

ここで, $i=\ell+1,\ldots,n$ に対して, $f_i = x_i - A_i(\alpha_1,\ldots,\alpha_\ell)$, A_i は多項式 となる. イデアル $< f_1,\ldots,f_n >$ を J で表すことにする.

この表現が与えられていれば, Galois 群 (の元) をすべての根の間の置換の中から探すことができる. そこで, 根の上の置換 σを考えるのであるが, 簡単のため, σ は各 index $1,...,n$ の上の置換とみなす. すなわち, k^σ, $k=1,...,n$ はやはり, $\{1,...,n\}$ の元となる.

定理 2 σ を置換とする. このとき,
(1) σ が G_f の元であるための必要条件はすべての $k=1,...,n$ に対して, $f_k(\alpha_{k^\sigma},\ldots,\alpha_{1^\sigma})=0$ となる.
(2) *(1)* をイデアルの言葉になおせば, σ が G_f の元であるための必要条件はすべての $k=1,...,n$ に対して, $f_k(x_{k^\sigma},\ldots,\alpha_{1^\sigma})$ がイデアル$< f_1,\ldots,f_n >$ に属する.
(3) *(2)* を計算手順の言葉になおせば, σ が G_f の元であるための必要条件はすべての $k=1,...,n$ に対して, $f_k(x_{k^\sigma},\ldots,\alpha_{1^\sigma})$ のイデアル$< f_1,\ldots,f_n >$ に関する *normal form* が 0 になる.

ランダムに生成した置換に対して, 定理 2 の判定法より, Galois 群が求まることになる. (この判定を membership 判定とここでは呼ぶことにする.) しかし, なんの工夫もなければ $O(n!)$ 回もの membership 判定が必要となり実際の計算が非常に困難となる. そこで, なんらかの工夫を与えて効率良く求めることになる. ここで, 導入するのが, strong generating set である.

定義 1 G を $\{1,...,n\}$ 上の置換群とする. $G_{(0)}=G$ とし, 更に $i=1,...,n$ に対して, $G_{(i)}=G_{1,...,i}=\{\sigma\in G \mid j^\sigma = j \text{ for } j=1,\ldots,i\}$ と定義する. また, k を $G_{(k)}=1$ なる最小の整数とする. $i=1,...,k$ に対して $G_{(i)}\backslash G_{(i-1)}$ の *coset representative* $S_i=\{s_{i,1},\ldots,s_{i,t_i}\}$ を各々一つ定める. *(*すなわち, $G_{(i-1)}=G_{(i)}s_{i,1}\cup\cdots\cup G_{(i)}s_{i,t_i}$. *)*
このとき, $S=S_1\cup S_2\cup\cdots\cup S_k$ を G の *strong generating set* といい, S の各元を *strong generator* という.

我々の設定は strong generating set を求めることに以下の理由で大変適している.

(A) 各 coset $G_{(i-1)}\backslash G_{(i)}$ の代表元として i の $G_{(i-1)}$ での行き先から選べる. ここで, $i^{G}_{(i-1)}=\{t_1=i,t_2,\ldots,t_m\}$ とすれば, $s_{i,u}$ として $j^\sigma=j, j=1,\ldots,i-1, i^\sigma=t_u$ なる σ をとればよい.

(B) $1,\ldots,i$ の行き先を指定した元で Galois 群に属する元は $i+1,\ldots,n$ の行き先を逐次決めていくことにひとつ取り出すことができる.

この, strong generating set を求める戦略を採用することで, 計算の手間がおおいに省けることがわかる.

定理 3 *Galois* 群の *strong generator* を求めるための *membership* 判定での必要な *normal form* の計算は, 高々 $O(n^4)$ 回 *(*詳しくは $O(\ell^2n^2)$ 回*)* でよい.

3 Absolute resolvents を用いる方法

Lagrange により導入された resolvent を利用して Galois 群を計算する 1 つ目の方法は, 絶対分解式 (absolute Lagrange resolvents) の因数分解を利用する方法である. この absolute resolvents を用いて多項式の Galois 群を決める研究としては, Berwick (1915, 1929) [13] [14], McKay *et. al.* (1985, 1989) [32] [18], Arnaudiés & Valibouze (1993-95) [37] などが挙げられる. ここでは Arnaudiés & Valibouze の方法を中心に述べるが, その前に Berwick の結果と McKay らの方法について簡単に触れる.

さて, 体 K 上の n 次の多項式 f について考えるとする. その Galois 群を $Gal_K(f)$ とする. n 次の対称群 S_n を n 個の変数の上の置換群と考える. S_n のある部分群を H とする. この部分群 H の全ての元の作用により不変な (n 変数の) 多項式を Θ とする;

$$\sigma(\Theta) = \theta \Leftrightarrow \sigma \in H.$$

これを絶対 H-不変量 (absolute H-invariant) と言い, 部分群 H をテスト群という. このとき, S_n に関する H-分解式 (S_n-relative H-rsolvent) は次で定義される;

$$\mathcal{L}_{\Theta,f}(y) = \prod_{\tau \in \mathbf{R}} (y - \widetilde{\tau\Theta})$$

ここで, $\mathbf{R} = \{\tau_i \in S_n | S_n = \tau_1 H \cup \cdots \cup \tau_e H\}$ で $\widetilde{\tau\Theta}$ は $\tau\Theta$ の f の根による特殊化を表す. すなわち, 各変数 x_i に根 α_i を代入したものである. この $\mathcal{L}_{\Theta,f}$ を 絶対 H-分解式 (absolute H-resolvent) という. ある invariant に関する resolvent が重複因子を持たないとき, その invariant 及び resolvent は f-分離 (f-separable) だという. 以後, この節では resolvent は全て f-separable だと仮定する. また, 任意の多項式に対して, その (係数体上の) 既約因子全ての次数の集合 $(i_1, \cdots, i_q)$ (ここで, $i_1 \geq \cdots \geq i_q$) を多項式の分割 (partition) と言う.

注意 2 *f-separable な resolvent の存在については次が言える; S_n の全ての部分群に対し, f-separable な H-resolvent は存在する. また, 同様に, 全ての f について separable な resolvent が存在する. (Arnaudiés & Valibouze (1993) [4] 参照.)*

3.1 背景となる考え

absolute invariant を利用した方法の背後にあるアイディアを説明する.

f の absolute H-resolvents の K 上の既約因子の次数すなわち partition は H と S_n の抽象部分群としての $Gal_K(f)$ にのみ依存する. よってこの場合, この partition を $[Gal_K(f), H]$ と書くことにする. また, H-invariant Θ についての H-resolvent は, $\sigma\Theta$ ($\sigma \in S_n$) についての $\sigma H \sigma^{-1}$-resolvent に等しいので $Gal_K(f)$ は, 共役 (すなわち, 根の置換) を除いて決められる.

したがって, 一度 S_n の全ての部分群 G, H について, それらの partition $[G, H]$ の (正方の) 表を構成すれば, (この次数については) Galois 群を決めることが可能となる. すなわち, 与えられた多項式 f に対して H-resolvent を計算し, K 上で因数分解すれば partition が得られ, この表 (このような表を分割行列 (partition matrix) という) に照らして Galois 群を同定することができる. 分割行列には 2 つの側面がある; (a) partition すなわち resolvent の因数分解と (b) $Gal_K(f)$ の S_n/H への orbit 分解とが 1 対 1 に対応する. そして, 分割行列は (b) により構成され Galois 群の判定は (a) によるという点 (かたや group theoretical 他方は computer algebra) がこの方法の特徴でもありアイデアの本質である.

partition $[G, H]$ において, 群 G は Galois 群の候補となる群であるので候補群 (candidate group), 群 H は Galois 群の決定の際 H-resolvent という形で試金石となる群なので試験群 (test group) という. 試験群と

しては, S_n の部分群全てが必ずしも必要なわけではない. S_n 部分群の中より, 適当に試験群を選び, それらだけについて得られる partition からなる分割行列 (これを, 部分分割行列という) が, それぞれ異なる行を持てば十分であるし, ある部分分割行列がいくつかの同じ行を持っていても, それらを区別する付加的な情報が得られればよい. 付加的な情報として, resolvent の既約因子の Galois 群 や mod p での因数分解により得られる cycle 型 などが用いられ, これらはまた, Galois 群を決める過程の効率化にも役に立っている.

3.2 Berwick の方法 (6 次の場合)

この scheme により Galois 群の決定を試みた最初の完全な形での Berwick (1929) [14] による 6 次の場合 ($deg(f) = 6$) の結果を示す. 以下の表が Berwick による S_n の部分分割行列である. 試験群については, order がそれぞれ 48, 72, 120, 360 の 4 つの S_n の極大部分群 $H_{48}, H_{72}, H_{120}, H_{360}$ を選んでいる. 候補群は S_6 の 16 個の可移部分群であり, その位数によって示し $G_1, \cdots, G_{16}$ とあらわす.

この分割行列は, 全ての行が異なっている訳ではないことに気付く. すなわち, これだけでは Galois 群を決めるのに十分ではない. そこで, resolvent の既約因子の Galois 群に注目する. f の H-resolvent の因子 g の Galois 群 Γ が, $G = Gal_K(f)$ に同型である (i. e. f のどの根も g の根の函数として表される) とき, この因子を太字で表している. Berwick は 6 次の場合に G は Γ に同型か, あるいは, G を求めるには Γ と他の resolvent の既約因子の Galois 群 Γ' を組み合わせる必要があることを示した. 後者の場合, resolvent の既約因子で組合せるものには $*$ が上の表中に同じ個数つけてある. すなわち, これら組み合わせられる因子の根の集合により生成される拡大体は f の分解体に等しい.

このように, 表の各行が全て異なってはいない場合でも, ある resolvent の既約因子の Galois 群を計算することで, 群を区別することは可能である.

	order	H_{360}	H_{120}	H_{72}	H_{48}
G_1	720	2	**6**	**10**	**15**
G_2	360	1^2	**6**	**10**	**15**
G_3	120	2	**5, 1**	**10**	**10, 5**
G_4	60	1^2	**5, 1**	**10**	**10, 5**
G_5	72	2	**6**	**9, 1**	**9, 6**
G_6	36	1^2	**6**	**9, 1**	**9, 6**
G_7	36	2	**3^*, 3^{**}**	**9, 1**	**9, 3^*, 3^{**}**
G_8	18	2	**3^*, 3^{**}**	**9, 1**	**9, 3^*, 3^{**}**
G_9	48	2^{**}	**4^*, 2**	**6^*, 4^***	**8, 6^*, 1**
G_{10}	24	2^{**}	**4^*, 2**	**6, 4^***	**8, 6^*, 1**
G_{11}	24	2^{**}	**4, 1^2**	**6, 4**	**4, 4, 6, 1**
G_{12}	24	1^2	**4, 2**	**6, 4**	**8, 6, 1**
G_{13}	12	1^2	**4, 1^2**	**6, 4**	**4, 4, 6, 1**
G_{14}	12	2^{***}	**3^*, 1, 2^{**}**	**6, 3^*, 1**	**6, 3^*, 3^*, 2^{**}, 1**
G_{15}	6	2^{**}	**3^*, 1, 2^{**}**	**6, 3^*, 1**	**6, 3^*, 3^*, 2^{**}, 1**
G_{16}	6	2	**3, 1^3**	**3, 3, 3, 1**	**3, 3, 3, 3, 1^3**

彼は, 下の表に示すように H_{120}-resolvent の各因子の群の表現を得た. この表と判別式の計算もあわせて可移群の全てを区別した. ここでは述べないが, Berwick の方法は H. O. Foulkes (1931) [19] により 7 次の場合に適用された.

G_3	G_4	G_7	G_8	G_9	G_{10}	G_{14}	G_{15}
$\mathcal{S}_5, \mathcal{S}_1$	$\mathcal{A}_5, \mathcal{S}_1$	$\mathcal{S}_3^2$	$\mathcal{S}_3, \mathcal{A}_3$	$\mathcal{S}_4, \mathcal{S}_2$	$\mathcal{A}_4, \mathcal{S}_2$	$\mathcal{S}_3, \mathcal{S}_2, \mathcal{S}_1$	$\mathcal{A}_3, \mathcal{S}_2, \mathcal{S}_1$

3.3 Mckay et. al. の方法

Soicher は試験群を resolvent とその partition が計算しやすいよう $H_m = S_m \times S_{n-m}$ あるいは $K_m = Id^m \times S_{n-m}$ という型の可移的でない群とした. ここで, Id は単位群である (McKay & Soicher (1985) [32]). このとき, H_m の invariant として和 $x_1 + x_2 + \cdots + x_m$ を, また, K_m の invariant として線形和 $a_1x_1 + a_2x_2 + \cdots + a_mx_m$ をとる. ここで, 各 a_i は互いに異なる. これらの invariant について resolvent を計算し, K 上で因数分解する. Soicher が示した表すなわち分割部分行列は, その因数分解より得られる候補群の試験群 H_m に対する m-sets 上の作用と試験群 K_m に対する m-tuples 上の作用から得られた (orbit length). この分割部分行列を用いて Soicher は 7 次までの既約多項式の計算が可能になることを示した.

実際には, 彼らは判別式の計算はもちろん採用しているが, さらに, 次に述べる van der Waerden の定理と Tchebotarev の (密度) 定理に基ずく方策も利用している.

定理 4 p を素数とする. 分離多項式 $f(x) \in \mathbf{Z}[x]$ の $mod\ p\mathbf{Z}[x]$ に関する相違なる既約多項式への分解が

$$f(x) \equiv \phi_1(x) \cdots \phi_h(x) \quad mod\ p \qquad (\star)$$

であり, ここで, $\phi_i(x) \in \mathbf{Z}[x]$ は単多項式であり, $deg(\phi_i) = \ell_i\ (1 \leq i \leq h)$ で$\phi_i(x)$ と $\phi_j(x)(i \neq j)$ は $mod\ p$ で相異なるならば, $f(x)$ の *Galois* 群は $(12\cdots\ell_1)(\ell_1+1\cdots\ell_1+\ell_2)\cdots(\ell_1+\cdots+\ell_{h-1}\cdots\ell_1+\cdots+\ell_h)$ と同じ型の置換を含む.

この van der Waerden の定理の条件をみたすために, p は判別式を割らないような素数をとればよい. そういう p に対して $(\star)$ が得られたとき, その cycle 型を shape といい, $shape(p) = (\ell_1, \cdots, \ell_h)$ と書くことにする. このとき Tchebotarev の定理は

定理 5 ある正の整数 x に対し $N(n_1, \cdots, n_t, x)$ は, $p \leq x$ なる素数 p で, 多項式 f の p による *shape* $shape(p)$ が $(n_1, \cdots, n_t)$ であるものの個数を表すとする. また, $\nu(x)$ を x 以下の素数の個数だとすると, $x \to \infty$ のとき $\frac{N(n_1,\cdots,n_t,x)}{\nu(x)}$ は, f の *Galois* 群における $(n_1, \cdots, n_t)$ と同じ型をもつ置換の割合いに収束する.

である. 考えている多項式の次数の shape の表が前もって準備されて, かつ, 有効な p の個数の bound が存在すれば上記 2 つの定理に基ずく Galois 群計算が可能になるであろう. cycle 型 の分布についての結果は, 11 次までについては Butler & McKay (1983) [16] に見られ, bound についての最近の結果としては Lagarias & Montgomery (1979) [23], Serre (1981) [30] がある. しかし, これらの bound は非常に大きいため, McKay らの方法では, 分割部分行列を用いる方法の一助として併用されている. この McKay らの方法は 7 次までの既約多項式について 実際, 数式処理システム Maple に実装されている. その実施例を Appendix に付しておく (Fig.1).

より高次の場合については, Butler & McKay (1983) [16] において $S_n\ (n \leq 11)$ の可移部分群のリストが示され, McKay & Regener (1985) [25] において H_m, K_m 型の試験群に対する $S_n\ (n \leq 11)$ の partition の表 (分割部分行列) が示されている. ただし, この表より, 8〜11 次については彼らの示した試験群だけでは, 分割行列と absolute resolvent だけを用いて Galois 群を決定するのは十分ではないことがわかる.

3.4 Arnaudiés & Valibouze の方法

これまで見てきたように, 試験群の選択はいわば直観的に行なわれている. Arnaudiés & Valibouze の示した方法 [4] によると, S_n の任意の部分群 L_0 に対して L_0 の部分群の共役類だけをもとに, L_0 の分割行列の自動的な計算が可能になる. まず, その方法について述べる (詳細は [4] 参照). さらに, resolvent の因子の

Galois 群に着目するのは Berwick に遡るが, Valibouze は resolvent の因子の Galois 群の (a priori) 計算の新しい方法を提案し, その情報を用いて Galois 群を決定する方法を示した [37].

Partition matrix の計算　まず, (1 以上の) 整数の分割 (partition) を定義する. $n \in \mathbf{N}$ について, $\sum_{i=1}^{n} i\alpha_i = n$ であるとき, 全ての $(\alpha_1, \cdots, \alpha_n) \in \mathbf{N}^n$ を n の partition という. このとき 集合 $\{i \in [1,n] | \alpha_i \geq 1\}$ を partition の支柱 (support) と言う. すなわち, α_i はその partition における i の多重度 (multiplicity) であり, support の個数はその partition における要素の数である. n の partition B は, support の項によって構成される必ず増加する列 $(d_1, \cdots, d_r)$ と, それら要素の multiplicity の列 $\nu_1 = \alpha_{d_1}, \cdots, \nu_r = \alpha_{d_1 r}$ とより決まる. よって,

$$B = [(\nu_1, d_1), \cdots, (\nu_r, d_r)]$$

である. ここで, 全ての i に対して $1 \leq d_1 \leq \cdots \leq d_r \leq n$, $r \geq 1$, $\nu_i \geq 1$ である.

G を 有限群で $|G| = N$ であるとする. C を G の位数 (index) が $e = e_C$ のある部分群の共役類だとする. H を G のある部分群を表すとし, 全ての組 (H, C) と e の partition の関係を考える. $C_1 \in C$ を固定する. $C_1, C_2, \cdots, C_e$ は $G \bmod C_1$ の左剰余類で, H を $C' = \{C_1, \cdots, C_e\}$ に作用させるとする. このとき, α_i は C' における 濃度が i であるような H-orbit の個数だとすると, $(\alpha_1, \cdots, \alpha_e)$ は e の partition である. さらに, 次の補題が成立する.

補題 6 上に定義した *partition* $(\alpha_1, \cdots, \alpha_e)$ は, C だけに依存し, $C_1 \in C$ の選び方には依らない.

この補題より, ここで得られた $e = e_C$ の partition $(\alpha_1, \cdots, \alpha_e)$ は, 組 (H, C) だけに依存するので, これを (H, C) に関する partition といい, $B(H, C)$ とかく.

補題 7 H は G の部分群で, C を G のある部分群の共役類だとする. *prtition* $B(H, C)$ は H の共役類と C だけに依存する.

$\bar{C}$ を G のある部分群の共役類の集合だとする; $\bar{C} = \{C_1, \cdots, C_s\}$. $C \in \bar{C}, \mathcal{D} \in \bar{C}$ に対して, $B(C, \mathcal{D})$ は $B(H, \mathcal{D})$ に等しいとする. ただし, $H \in C$. この $B(C, \mathcal{D})$ は C, $\mathcal{D}$ に関する partition という. $\bar{C}$ を次数の小さい方から $C_1, \cdots, C_s$ と並べる ($C_1 = \{\{e_G\}\}, C_s = \{G\}$). このとき, 正方行列;

$$\mathcal{P} = [B(C_i, C_j)]_{1 \leq i,j \leq s}$$

を得るが, これが G によって定義される分割行列である. これを計算するために, $H_i \in C_i$ と $H_j \in C_j$ をそれぞれ選ぶ. $e_j = [G : H_j]$ とする. また, $G \bmod H_j$ の代表系を $\{\gamma_m\}$ とする. ただし $\gamma_1 = 1_G$ とする.

このとき, $B(C_i, C_j) = (\alpha_1, \cdots, \alpha_{e_j})$ であり, ここで全ての $\ell \in [1, e_j]$ について,

$$\alpha_\ell = \frac{1}{\ell}\, card\{m \in [1, e_j] \mid [H_i : \gamma_m H_j \gamma_m^{-1} \cap H_i] = \ell\} \quad (\star\star)$$

である. ある集合 A に対して $card(A)$ は A の濃度を表す. また,

$$B(C_i, C_j) = [(\nu_{i,j,1}, d_{i,j,1}), \cdots, (\nu_{i,j,r_{i,j}}, d_{i,j,r_{i,j}})]$$

とすると (ただし, $1 \leq d_{i,j,1} < \cdots < d_{i,j,r_{i,j}} \leq e_j$, $\nu_{i,j,\ell} \geq 1$), $(\star\star)$ より $B(C_i, C_j)$ の support の元 $d_{i,j,\ell}$ は $card(H_i) = N/[G : H_i]$ の 除数 (divisor) であるのは明らかである. この式 $(\star\star)$ より, S_n の全ての部分群 L_0 の分割行列の (自動的な) の計算が可能となる. ここで, Galois 群を決めるために基礎となる次の定理が成立する.

定理 8 上で定義された行列 $\mathcal{P}$ の行は異なる. 従って, この行の集合と集合 $\bar{\mathcal{C}} = \{\mathcal{C}_1, \cdots, \mathcal{C}_s\}$ の間の自然な全単射が存在する.

よって, これより $L_0 = S_n$ のとき (★★) より得られる分割行列をもとに, absolute resolvent の partition を用いて Galois 群を決定できる. この分割行列の長所は, 多項式が既約である (i.e. Galois 群が可移的である) 必要がないということである.

$L_0 = S_n$ のときの (★★) による方法を用いて得られた結果 (全て Arnaudiés & Valibouze による) についてであるが, これらは GAP [29] を用いて計算された. 4 ～ 7 次については $S_n (4 \leq n \leq 7)$ の完全な分割行列が得られている ([8] , [9] 参照). よってこれより square free な多項式について Galois 群の計算が実現される. 8 次については S_8 の分割行列の部分行列が得られている. これは, 672 以下の次数を持つ試験群と候補群は可移なもの全て (50 個) についてのみの結果である. 候補群は Butler & McKay [16] の可移群の表による. S_8 の 296 個の群が残っているが, これで既約多項式については済んだことになる. 時間さえ許せば, 残りも同様に計算でき, 分割行列が完成する ([5] 参照). 9, 10, 11 次の場合 ([6], [10]) は, 部分群の class の全てを計算するのは大変なので適当な次数を持つものに制限して考えざるをえない. 候補群については, 同様に Butler & McKay [16] の可移群の表による. 試験群については 8 次の時に見つかった新たな resolvent 全てを考える. この方法で, 9 次と 11 次について, 既約多項式の Galois 群の決定が可能になる. 10 次については, relative resolvent も必要である.

一方, $L_0 \neq S_n$ のときは, Galois 群の決定には relative resolvent を必要とする. これは, $L_0 \neq S_n$ の場合に (★★) より得られる分割行列は, 後節に述べる relative resolvent を用いる Galois 群の計算方法にも利用され得ることを意味する.

Resolvent の因子の Galois 群　さて次に Valibouze (1995) [37] による resolvent の因子の Galois 群の計算を利用した Galois 群の計算法について述べる. まず, この方法の礎となる定理を与ることにする.

H が S_n の部分群のとき, H の置換によって不変であるような体 $K(x_1, \cdots, x_n)$ の元の集合は $K(x_1, \cdots, x_n)$ の部分体を構成する. これを $K(x_1, \cdots, x_n)^H$ と書く.

定理 9 f を *square free* な次数 n の $K(x)$ の多項式とし, その根の集合を Ω とする. H を S_n の部分群とし, Θ を H の *invariant* だとする. Θ が *resolvent* $\mathcal{L}_{\Theta,f}$ の単根ならば, $\tilde{\Theta}$ は $K = K(\Omega)^{Gal(f) \cap S_n}$ 上の体 $K(\Omega)^{Gal(f) \cap H}$ の原始元である.

$Gal_K(f) = G$ とするとこの定理は次を意味する;

$$K = K(\Omega)^G \xrightarrow{[G:G\cap H]} K(\Omega)^{G\cap H} = K(\tilde{\Theta}) \xrightarrow{|G\cap H|} K(\Omega)$$

h を次数 r の $\mathcal{L}_{\Theta,f}$ の単既約因子であり, $\tilde{\Theta}$ を根に持つとする. $S_n \bmod H$ の左剰余類の代表系 $\gamma = id, \cdots, \gamma_e$ は $\gamma = id, \cdots, \gamma_r$ が $S_n \bmod G \cap H$ の左剰余類の代表系であるように番号付けする. K 上の $\tilde{\Theta}$ の共役は $\widetilde{\gamma_1\Theta}, \cdots, \widetilde{\gamma_r\Theta}$ であり, これらは h の r 個の根である. $i = 1, \cdots, e$ に対して $H_i = \gamma_i H \gamma_i^{-1}$ の invariant $\Theta_i = \gamma_i\Theta_i$ は $\mathcal{L}_{\vartheta_i} = \mathcal{L}_\vartheta$ を満たすので, 上の定理と図は, 組 (H, Θ) を組 (H_i, Θ_i) に換えても同様に成立する. これより, 次の定理を得る.

定理 10 定理 9 の仮定の下に, $\widetilde{\Theta_{i_1}}, \cdots, \widetilde{\Theta_{i_q}}$ が $\mathcal{L}_{\Theta,f}$ の単根ならば, $K(\widetilde{\Theta_{i_1}}, \cdots, \widetilde{\Theta_{i_q}})$ 上の $K(\Omega)$ の *Galois* 群は $Gal(f) \cap H_{i_1} \cap \cdots \cap H_{i_q}$ である.

この定理より直ちに次を得る.

定理 11 定理 *9* の仮定の下に, V を $V=\bigcap_{i=1}^{e} H_i$ で与えられる S_n の正規部分群であるとする. このとき, $\mathcal{L}_{\Theta,f}$ の *Galois* 群は $G/G\cap V$ に同型である.

注意 3 この定理より, " $n\geq 5, H\notin\{S_n, A_n\}$ に対して, *resolvent* $\mathcal{L}_{\Theta,f}$ の *Galois* 群は $Gal(f)$ である. " を得る.

定理 10 はまた resolvent の全ての因子の Galois 群を与える. 以下の定理においては既約因子のみを考慮する.

定理 12 h が次数 r の $\mathcal{L}_{\Theta,f}$ の単既約因子で, その根は $\widetilde{\Theta_1},\cdots,\widetilde{\Theta_r}$ だとする. このとき, h の K 上の *Galois* 群は $G/G\bigcap_{i=1}^{r} H_i$ に同型である. ここで, $Gal(f)=G$ で, 各 $\Theta_i=\gamma\Theta$ は群 $H_i=\gamma H_i\gamma^{-1}$ の *resolvent* である.

系 13 K 上の h の *Galois* 群の位数は $[G:G\bigcap_{i=1}^{r} H_i]$ である.

注意 4 ここで述べた定理等は, *absolute resolvent* と S_n についての結果であるが, 一般に, *relative resolvent* と f の *Galois* 群を含む S_n の部分群 L_0 についても同様の結果が有効である.

各 $i=1,\cdots,r$ に対して h の次数は指数 $[G:G\cap H_i]$ に等しいので, 定理 9 より, S_n の分割行列を構成することができた. また, 定理 12 より, h の Galois 群はわかるし, 前もって S_n の部分群 G と H のみを用いて計算できる. よって, resolvent の既約因子の Galois 群の表を構成できる.

この resolvent の既約因子の表と分割行列を併用することで, 任意の separable な多項式 に対して Galois 群とその既約因子の次数を得る. そして, これは分割行列のみを用いる場合よりも効率的である. [37] では 8 次と 10 次の場合について扱っている. 8 次については resolvent の既約因子の Galois 群の情報がないと Galois 群が決まらないものについてのみ, resolvent の既約因子の Galois を与えた. 10 次については [10] で与えた部分分割行列の中の次数が 10 次よりも小さい resolvent の既約因子の Galois 群を与えた. この方法を用いれば 4~8 次についてもかなり高速に Galois 群が決定できるようになる.

3.5 Absolute resolvent の計算

実際の absolute resolvent の計算について少し触れておく. 主として用いられるものに (i) resultant を用いた方法 [31] [22] や (ii) symmetric function を用いた方法 [36] [7] がある. 他に, Gröbner bases を用いる方法も考えられるが, 方法として自然ではあるが実際の計算にはほとんど使えない. また, Stauduhar のように, 根の近似値を用いて absolute resolvent を計算することもできる.

4 Relative resolvents を用いる方法

2 つ目の resolvent を利用する方法は, 相対分解式 (relative resolvents) を用いた方法である. これは, Stauduhar (1973) によって導入され 3~7 次の既約多項式について試みられ, 引続き Eichenlaub & Olivier (1994) により 11 次までの多項式について研究されている. Stauduhar の方法は resolvent の計算を数値的に行なう. すなわち, 元の多項式の根の数値的な近似値を用いる. Galois 群は, Galois 群がどの極大部分群に含まれるかということによって S_nの部分群の有向グラフを辿っていくことで決まる. 包含関係のテストは, 数値的に計算された resolvent を用いる. また, Stauduhar の方法では resolvent を根の近似値を用いて数値的に求めているが, 記号的 (symbolic) に計算する方法が Colin (1995) により提案された.

4.1 Stauduhar の方法

Stauduhar の方法 (1973) [33] について述べる. Z 上の monic な既約多項式 を $f(x)$ とし, f の次数を n とする. f の根を $r_1, r_2, \cdots, r_n$ とし f の分解体を Kとする. また, 根の数値的な近似値は既にわかっているとし, n 次の全ての可移置換群の知識 (S_nの部分群の有向グラフ) を仮定する. $r_1, r_2, \cdots, r_n$ を $f(x)$ の根のある固定した順序とする. H を S_n の可移部分群とし, この与えられた根の順序についての f の Galois 群 Γ は H の部分群であるとする. G は H の部分群で $F(x_1, \cdots, x_n)$ は群 G によって不変な n 変数多項式 (i. e. H-relative G-invariant) であるとする. $\pi_i, \cdots, \pi_k$ を H における G の右剰余類の代表系だとする. このとき, 分解式 (H-relative G-resolvent) は

$$\mathcal{L}^H_{F,f}(y) = \prod_{i=1}^{k} (y - \pi_i(F(r_1, \cdots, r_n)))$$

で定義され, これは整数 (rational integer) 係数をもつ. ここで, 次の定理により Stauduhar の方法の包含関係のテスト (inclusion test) が実現される.

定理 14 H における G の右剰余類の代表系のうちの一つは G 自身に含まれるので, $F(r_1, \cdots, r_n)$ は $\mathcal{L}^H_{F,f}(y)$ の根である. $F(r_1, \cdots, r_n)$ が $\mathcal{L}^H_{F,f}(y)$ の重複因子でないと仮定する. このとき, $F(r_1, \cdots, r_n)$ が整数 *(rational integer)* であるときに限り $\Gamma \subset G$ である.

すなわち, resolvent の根 $\pi_i(F(r_1, \cdots, r_n))$ $i = 1, \cdots, k$ が整数であるかどうか調べれば包含関係がわかる. もし, 整数根が存在しなければ, Γ は G のどの共役にも含まれていないことになり, 他の候補 $G'(\subset H)$ について同様に繰り返す. 整数根 $\pi_j(F(r_1, \cdots, r_n))$ が存在したとすると, このとき $\Gamma \subset \pi_j G \pi_j^{-1}$ である. これは, 根を $r'_i = r_{\pi_i(i)}$ に従って並べ換えた順序について, $\Gamma \subset G$ を意味する. $\Gamma \subset G$ であれば, 後は G の可移部分群 $G^*(\subset G)$ について同様のことを行なえば良い. こうして, あるステップにおいてどの resolvent も整数根を持たないか, あるいは最小の部分群までいった時点で, Galois 群が決まる.

4.2 記号的 Stauduhar の方法

次に, Colin [17] の方法について述べる. Stauduhar の方法では S_n の部分群の有向 (非環状) グラフを inclusion test を繰り返し行ない辿っていくことで Galois 群 Γ を求めるというものである. Colin の方法も, この scheme に追随するもので, relative resolvent の計算を記号的に行なう点と, それにより多項式 f の Galois 群 Γ を S_n における Γ の共役類 $[\Gamma]$ として求めるという点が異なる. ゆえに Formal(or Symbolic) Stauduhar method というべき方法である. resolvent の記号的に行なう計算は, 2 次計量空間の構造を導入することによって resolvent の係数を原始元の巾を用いて表すことから成っている.

Relative resolvent の計算とその特殊化 群 G がある集合 E に作用しているとき, $Stab_G(A)$ で G における E の部分集合 A の固定部分群を表す. H が G の部分群ののとき $(G/H)_g$ で G における H の左剰余類の集合を表し, $(G//H)_g$ でその代表系を表す. K を標数 0 の体とする. $\mathbf{X} = (x_1, \cdots, x_n)$ とする. ここで x_i は K 上の不定元である. $\Sigma = (\Sigma_1, \cdots, \Sigma_n)$ とする. ここで $i = 1, \cdots, n$ に対して $\Sigma_i = \sum_{j \in \mathbf{N}, j_1 < \cdots < j_i} \prod_{k=1}^{i} X_{jk}$ である (すなわち, 基本対称式である). 多項式 $f \in K[T]$ は separable だとする.

L を S_n の部分群とする. $\Theta \in K[\mathbf{X}]$ を $Stab_{S_n}(\Theta) = L$ なる多項式とする. すなわち, Θ は L-不変多項式 (L-invariant polynomial) である. このとき, L によって不変な $K(\mathbf{X})$ の元からなる $K(\mathbf{X})$ の部分体を $K(\mathbf{X})^L$ とし, $e = |K(\mathbf{X})^L : K(\Sigma)| = |S_n : L|$ とすると, Θ は拡大 $K(\mathbf{X})^H : K(\mathbf{X})^L$ の原始元である. すなわ

ち, $(1, \Theta, \Theta^2, \cdots, \Theta^{e-1})$ は $K(\Sigma)$-ベクトル空間 $K(\mathbf{X})^L$ の基底である. したがって, 任意の多項式 $p \in K(\mathbf{X})^L$ は一意的に

$$p = A_0 + A_1\Theta + \cdots + A_{e-1}\Theta^{e-1} \quad A_i \in K(\Sigma), \qquad (\#)$$

と表せる. この形に p を表すことの意義は, relative resolvent の各係数が $K(\mathbf{X})^L$ の元であることにある.

$K(\mathbf{X})^L$ の元を $(\#)$ の形に表すために, $K(\mathbf{X})^L$ 上の $K(\Sigma)$-2 次計量空間の構造を導入する. $K(\mathbf{X})^L$ 上の $K(\Sigma)$-対称 2 次形式 $< .,. >$ を以下のように定義する. $(P, Q) \in (K(\mathbf{X})^L)^2$ に対して,

$$< P, Q >= \sum_{\sigma \in (\mathcal{S}_n//L)_g} \sigma(PQ) = \frac{1}{|L|} \sum_{\sigma \in \mathcal{S}_n} \sigma(PQ).$$

この $K(\Sigma)$-対称 2 次形式 $< .,. >$ は次のような有益な性質をもつ.

命題 15 *$K(\mathbf{X})^L$ 上の $K(\Sigma)$-対称 2 次形式 $< .,. >$ は非退化である.*

これより, $K(\mathbf{X})^L$ の元を $(\#)$ の形に表すことが以下のようにして可能になる. $K(\Sigma)$ 上 A_j $(0 \leq j \leq e-1)$ についての e 個の線形方程式

$$< p, \Theta^i >= A_0 < 1, \Theta^i > + A_1 < \Theta, \Theta^i > + \cdots + A_{e-1} < \Theta^{e-1}, \Theta^i >,$$

$(i = 0, \cdots, e-1)$ を解けばよい. ($K(\mathbf{X})^L$ の元を $(\#)$ の形に表す方法をもう一つ Colin は挙げているが, 本稿では割愛する.) こうして, $K(\mathbf{X})^L$ の元である resolvent の各係数を $(\#)$ の形に表せる. こうして得られた resolvent は f の根による特殊化を考える上で以下で述べるように都合がよい形となっている.

定義 2 *L を $\mathcal{S}_n$ の部分群, H を L の部分群とする. $Stab_L(\Psi) = H$ であるような $\Psi \in K[\mathbf{X}]$ すなわち, 拡大 $K(\mathbf{X})^L : K(\Sigma)$ の原始元を n 次の L-相対 H-不変量 (L-relative H-invariant) という. $K(\mathbf{X})^L$ 上の Ψ の最小多項式を Ψ の一般 L-相対分解式 (generic L-relative resolvent) という. すなわち,*

$$\mathcal{L}_\Psi^L = \prod_{\sigma \in (L//H)_g} (y - \sigma\Psi(x_1, \cdots, x_n)) \qquad \in K(\mathbf{X})^L[y].$$

(補捉 : absolute invariant (resolvent) は, すなわち $\mathcal{S}_n$-relative invariant (resolvent) のことである.)

次に, resolvent の特殊化を考える. $\mathbf{r} = (r_1, \cdots, r_n)$ とし, r_i は f の根であるとする. また, $g \in K(\mathbf{X})$ に対して g の f の根による特殊化を $\tilde{p} = p(r_1, \cdots, r_n)$ と表す.

L が Γ を含むとき, $\mathcal{L}_\Psi^L$ の特殊化を各変数 x_i に r_i を代入して得られる多項式 $\mathcal{L}_{\Psi,\mathbf{r}}^L \in K[y]$ として定義する. また, $\mathcal{L}_{\Psi,\mathbf{r}}^L$ が square-free である時に限り Ψ , $\mathcal{L}_\Psi^L$ は r-separable だと言うことにする.

f の Galois 群 Γ が $\mathcal{S}_n$ の部分群 L に含まれるとする. H を L の部分群とする. $\mathcal{L}_\Psi^L$自体の計算は容易であり, 求めたいのは $\mathcal{L}_{\Psi,\mathbf{r}}^L$ なので, $\mathcal{L}_\Psi^L$ の係数を特殊化したものを求める方法を考える. ここで, Θ を absolute L-invariant とし, その特殊化の値 $\tilde{\Theta} = \Theta(r_1, \cdots, r_n) \equiv \theta$ は既知であるとする. まず, $\mathcal{L}_\Psi^L$ の各係数 R は $K(\mathbf{X})^L$ の元である. よって上述の方法で R を Θ と根の対称式で表すことができる. 仮定より $\tilde{\Theta}$ はわかっているし, 基本対称式 $\tilde{\Sigma}_i$ は f の係数であるからわかっている. よって, $\tilde{R}$ もわかる. こうして所望の $\mathcal{L}_{\Psi,\mathbf{r}}^L$ が得られる.

ここで注意すべきは, 特殊化の際に分母が 0 になる場合があり得ることである. この場合, 特殊化の際に分母が 0 にならないような, 別の r-separable L-invariant Θ' を選んで上記の方法で $\mathcal{L}_{\Psi,\mathbf{r}}^L$ を求めればよい. そのような Θ' は必ず存在し, Θ' を見つけ出すアルゴリズムも示されている (詳細は [17]).

包含関係の判定 Stauduhar の scheme に従い, まず, 次の命題によって $\mathcal{S}_n$ の部分群の全ての共役類の有向グラフを定義する.

命題 16 L を有限群とする. $C(L)$ を L の部分群の全ての L-共役類の集合とする. $C(L)$ 上で

$$\forall \mathcal{H} \in C(L), \forall \mathcal{K} \in C(L), \mathcal{H} \prec \mathcal{K} \Longleftrightarrow \exists H \in \mathcal{H}, \exists K \in \mathcal{K}, H \subset K$$

によって定義される関係 $\prec$ は順序関係である.

H が L の部分群で $L \subset S_n$ ならば, H の L-共役類を $[H]_L$ で表す ($L = S_n$ の場合 $[H]$ と書く). $C(S_n)$ 上で $\prec$ により定義される S_n の部分群の全ての S_n-共役類の有向グラフを $\mathcal{G}_{S_n}$ とする. すなわち, ある $\mathcal{H} \in C(S_n)$ の子 (children) は $\{\mathcal{K} \in C(S_n) | \mathcal{K} \prec_{\neq} \mathcal{H}\}$ の極大な元である. このグラフはもちろん connected であるが一般に tree ではない. 複数の親 (parents) をもつものがあり得る.

後は, グラフ $\mathcal{G}_{S_n}$ において Galois 群 Γ の共役類 $[\Gamma]$ を見つけるまで inclusion test をし, $\mathcal{G}_{S_n}$ を辿っていく. この場合 inclusion test は次の命題に依る.

命題 17 L, H は S_n の部分群で $\Gamma \subset L, L \subset H$ であるとする. ***r-separable L-relative H-invariant*** を Ψ とすると, $\mathcal{L}^L_{\Psi,\mathbf{r}}$ が K に根を持つときに限り $[\Gamma]_L = [H]_L$ が成立する.

すなわち, $\mathcal{L}^L_{\Psi,\mathbf{r}}$ が K に根を持つかどうかは, $\mathcal{L}^L_{\Psi,\mathbf{r}}$ を K 上で因数分解すればよいことがわかる. (ここで, S_n の全ての部分群 H と H の全ての極大部分群 M に対して最大の指数 (index) $[H:M]$ を N とすると, 因数分解すべき $\mathcal{L}^L_{\Psi,\mathbf{r}}$ の次数は N より小さい.)

Galois 群決定アルゴリズム　$\mathcal{G}_{S_n}$ を辿っていく際の各ステップでのアルゴリズムは以下のようになる; ν 番目のステップを考える. このとき, S_n の部分群の列 $L_0 = S_n \supset L_1 \supset \cdots \supset L_\nu$ について $[\Gamma] \prec [L_\nu]$ を確かめたい. また, absolute L_ν-invariant を Θ_ν とする. 便宜上, $L = L_\nu$, $\Theta = \Theta_\nu$, $\theta = \theta_\nu = \widetilde{\Theta_\nu}$ とする. $\mathcal{M}$ を $C(L) \setminus \{L\}$ の $\prec$ についての極大元の集合だとする. ある unknown な $\tau \in S_n$ に対して $\Gamma \subset \tau L \tau^{-1}$ であることはわかっている. $[\Gamma] \prec [L]$ は言い換えると $\exists \mathcal{H} \in \mathcal{M}, \exists H \in \mathcal{H}$, $\Gamma \subset \tau H \tau^{-1}$ ということである.

このテストは次のように実現される. $\mathcal{H} \in \mathcal{M}$ とする. 適当に $H \in \mathcal{H}$ を選ぶ ($[H]_L = \mathcal{H}$). 特殊化の際に分母が 0 にならないような absolute r-separable H-invariant Ψ を計算し resolvent $\mathcal{L}^L_\Psi$ を計算する. ここで計算したいのは $\mathcal{L}^{\tau L \tau^{-1}}_{\tau\Psi,\mathbf{r}}$ である. ここで, $\mathcal{L}^{\tau L \tau^{-1}}_{\tau\Psi} = \tau \mathcal{L}^L_\Psi$ であるので特殊化すれば $\mathcal{L}^{\tau L \tau^{-1}}_{\tau\Psi,\mathbf{r}} = \mathcal{L}^L_{\Psi,\tau\mathbf{r}}$ である.

L は $\tau\Gamma\tau^{-1}$ を含み, $\tau\Gamma\tau^{-1}$ は f の根の順序 $\tau\mathbf{r}$ に対する f の Galois 群 $Gal_K(f)$ の S_n における表現である. Θ の $\tau\mathbf{r}$ による特殊化の値 (すなわち, $\tau\Theta$ の $\mathbf{r}$ による特殊化の値, これが θ である.) はわかっているし, Θ は, $\mathbf{r}$ と $\tau\mathbf{r}$ による特殊化でともに分母が 0 にならない. したがって, (τ はわかっていないが) $\mathcal{L}^{\tau L \tau^{-1}}_{\tau\Psi,\mathbf{r}}$ を計算できる.

そして, 因数分解によって $\mathcal{L}^{\tau L \tau^{-1}}_{\tau\Psi,\mathbf{r}}$ が 1 次因子を持つかどうかテストする. もし 1 次因子をもてば, そのうちの 1 つを $y - \psi$ とする. このとき, $\psi = \widetilde{t\Psi}$ を満たす $t \in \tau L$ が存在し, $L_{\nu+1} = H, \Theta_{\nu+1} = \Psi, \theta_{\nu+1} = \psi$ とし, 次のステップへ進む. また, もし 1 次因子を持たない場合は, 1 次因子をもつ resolvent が得られるまで他の $\mathcal{H} \in \mathcal{M}$ について同様に繰り返す. どの $\mathcal{H} \in \mathcal{M}$ についても 1 次因子を持たない場合は, $\Gamma = \tau L \tau^{-1}$ で, よって $[\Gamma] = [L]$ である.

包含関係のテストで, Stauduhar の方法では数値的に計算された resolvent の根 (i.e. f の根の多項式) の整数かどうかの判定を正確に保証するにははかなりの精度を要求される. Stauduhar が実際にどういう手法でどの程度の時間を要したのか記述はなくわからないが, [18] に依ると, 整数の判定を保証する方法に, 代数的数の対数の線形形式の近似に関する Baker の結果があり, この Baker の方法では, 一般に (十進で) 数百から数千桁の根の近似値が必要となるようである. 一方, Colin の方法では, resolvent を 1 回因数分解すればよく, その resolvent の次数は 高々 N である (N に関する bound はわかっていない). よってこの因数分解はかなり小さい計算量ですむと思われる. この方法の計算機への実装は未完成で, 現在著者自身によって進行中である.

4.3 Invariant の計算

resolvent を用いる方法 [B1][B2] に共通して, アルゴリズムの点から言うと, invariant の計算という問題が残っている. というのも, invariant の構成は, これまで直観に頼って行なわれてきたからである. 実際, これまでは invariant は, 与えられた群に対して逐次構成するか, McKay & Soicher が使った和や線形和のように計算の効率の面から優れている invariant の class から始めて求めている. これらの直観によるアプローチでは, 殊に relative invariant を見つけるのは困難になってくる.

1987 年に Girstmair が [20] において, 群の invariant を自動的に生成する方法を示した. これは, absolute と relative の両方に適用可能である. この方法は, より次数と単項式の数が小さいと言う意味で "最小の" invariant を与える. よって, この方法は resolvent の計算の効率の面でも有益である.

参考文献

[1] Anai, H. , Noro M. , Yokoyama K. (1995). Computation of the splitting fields and the Galois groups of polynomials. MEGA '94.

[2] Anai, H. , Yokoyama K. (1994). Radical Representation of Polynomial Roots. ISIS Reserch Report ISIS-RR-94-13E.

[3] Anai, H. , Noro M. , Yokoyama K. (1994). Computation of Galois groups and Radical representation of polynomial roots. 研究集会「代数的組合せ論」於 京都大学数理解析研究所.

[4] Arnaudiés, J. M. , Valibouze, A. (1993). *Résolvantes de Lagrange.* Rapport interne LITP 93. 61.

[5] Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 8* Rapport interne LITP 94. 25.

[6] Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 9* Rapport interne LITP 94. 30.

[7] Arnaudiés, J. M. , Valibouze, A. (1994). *Calculs de résolvantes* Rapport interne LITP 94. 46.

[8] Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 4 à 6.* Rapport interne LITP 94. 48.

[9] Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 7* Rapport interne LITP 94. 49.

[10] Arnaudiés, J. M. , Valibouze, A. (1994). *Groupes de Galois de polynôme de degré 10 et 11* Rapport interne LITP 94. 50.

[11] Berlekamp, E. R. (1967). Factoring Polynomials over Finite Fields. Bell System Technical Journal, **46**, 1853-1859.

[12] Becker, T., Weispefenning, V. (1993). Gröbner Bases A Computational Approach to Commutative Algebra. Springer-Verlag.

[13] Berwick, E. H. (1915). The condition that a quintic equation should be solube by radicals. Proc. London Math. Soc. (2) **14** 301-307.

[14] Berwick, E. H. (1929). On solube sextic equations. Proc. London Math. Soc. (2) **29** 1-28.

[15] Butler, G. (1993). The transitive groups of degree fourteen and fifteen. J. Symb. Comp. **16**, 423-422.

[16] Butler, G. , McKay, J. (1983). The transitive groups of degree up to eleven. Comm. Algebra **11**, 863-911.

[17] Colin, A. (1995). Formal Computation of Galois Groups with Relative Resolvent Polynomials. AAECC 11 (July 17-21).

[18] Ford, D. J. , McKay, J. (1989). Computation of Galois Groups from Polynomials over the Rationals. Computer algebra.

[19] Foulkes, H. O. (1931). The resolvent of an equation of seventh degree. Quart. J. Math. Oxford Ser. (2), 9-19.

[20] Girstmair, K. (1987). On Invariant Polynomials and Their Application in Field Theory. Math. Comp. **48**, 178, 781-797.

[21] Geddes, K.O., Czapor, S.R., Labahn, G.
(1992). Algorithms for Computer Algebra. Kluwer Academic Publishers.

[22] Giusti, M. , Lazard, D. , Valibouze, A. (1988). Algebraic transformations of polynomial equations, symmetric polynomials and elimination. ISSAC '88, LNCS **358**, 309-314.

[23] Lagarias, J. C. , Montgomery, H. L. (1979). A bound for the least prime ideal in the Chebotarev Density Theorem. Invent. Math. **54** 271-296.

[24] Char, B. W.; Geddes, K.O., Gonnet, G.H., Leong, B.L., Monagan, M.B., Watt, S.M. (1992). First Leaves: A Tutorial Introduction to Maple V. Springer-Verlag.

[25] McKay, J. , Regener, E. (1985). Action of permutation groups on r-sets Comm. Algebra **13**, 619-630.

[26] Miller, G. A. (1988). On the transitive substitution groups of degree thirteen and fourteen. Quarterly J. Pure and Applied Maths. **29**, 224-249.

[27] Pohst, M. , Zassenhaus, H. (1989) ENCYCLOPEDIA OF MATHEMATICS ALGORITHMIC ALGEBRAIC NUMBER THEORY Cambridge University Press

[28] Royle, C. F. (1987). The transitive groups of degree twelve. J. Symb. Comp. **4**, 255-268.

[29] Schönert, M. (1993). GAP groups, algorithms and programming version 3 release 2. (a manual of GAP), ftp portable document.

[30] Serre, J. P. (1981). Quelques applications de théoreme de densité de Chebotarev. Publ. Math. I. H. E. S. , Bures-sur-Yvette.

[31] Soicher, L. (1984). An Algorithm for Computing Galois Groups. Computational Group Theory, Academic Press, London, 291-296.

[32] Soicher, L. , McKay, J. (1985). Computing Galois Groups over the Rationals. J. Number Theory 20, 273-281.

[33] Stauduhar, R. P. (1973). The Computation of Galois Groups. Math. Comp. **27**, 124.

[34] Tchebotarev, N. (1950). Grundzüge des Galois'shen Theorie. P. Noordhoff, 1950.

[35] Trager, B. M. (1976). Algebraic factoring and rational function integration. in Proc. SYMSAC '76, ACM Press, 219-226.

[36] Valibouze , A. (1988). *Manipulations de fonctions symmétriques.* Thèse de l'Université Paris VI.

[37] Valibouze , A. (1995). Computation of the Galois Groups of the Resolvant Factors for the Direct and Inverse Galois Problem. AAECC 11 (July 17-21).

[38] Zassenhaus, H. (1969). Hensel Factorization I. J. Number. Theory. **1**, 291-311.

5 Appendix

Fig. 1

```
    |\^/|     Maple V Release 3 (Fujitsu Ltd)
  _|\|  |/|_.  Copyright (c) 1981-1994 by Waterloo Maple Software and the
  \ MAPLE /  University of Waterloo. All rights reserved. Maple and Maple V
  <____ ____>  are registered trademarks of Waterloo Maple Software.
> galois(x^5-5*x+12);
galois:   Computing the Galois group of    x^5-5*x+12
galois:   64000000 = (8000)^2
galois:   Possible groups:   {+Z5,  +D5,  +A5}
galois:   p = 3   gives shape   2,  2,  1
galois:
Removing   {+Z5}
Possible groups left:   {+D5,  +A5}
galois:   p = 7   gives shape   5
galois:   p = 11   gives shape   5
galois:   p = 13   gives shape   5
galois:   p = 17   gives shape   2,  2,  1
galois:   p = 19   gives shape   5
galois:   p = 23   gives shape   5
galois:   The Galois group is probably   +D5
galois:   Using the orbit-length partition of 2-sets.
galois:   Calculating a resolvent polynomial. . .
galois:   Factoring the resolvent polynomial. . .
galois:   Orbit-length partition is   5,  5
galois:
Removing   {+A5}
Possible groups left:   {+D5}
                  +D5,  10,  {(1 2 3 4 5),  (2 5)(3 4)}
```

Example polynomials

(1) $x^5+x^4-4x^3-3x^2+3x+1$
(2) x^5-3x^2+2x+1
(3) x^5-2
(4) $x^5-2x^4+10x^3-10x^2-10x-10$
(5) x^5-x^2-2x-3
(6) x^5-x+1
(7) x^6+x^3+1
(8) $x^6+2x^3+9x^2-6x+2$
(9) x^6-3
(10) $x^6+9x^4-4x^2-4$
(11) x^6+x^3+7
(12) x^6-3x^4+1
(13) x^6+x^4-9
(14) x^6+6x^2+4
(15) x^6-2x^3-2
(16) $x^6+6x^4+2x^3+9x^2+6x-4$
(17) x^6+x^4-8
(18) $x^6-9x^3+6x^2+9x+2$
(19) $x^6+x^4-x^2+5x-5$
(20) $x^6+10x^5+55x^4+140x^3+175x^2-3019x+25$
(21) $x^6-9x^3+3x^2-6x+1$
(22) x^6+x+1
(23) $x^7+x^6-12x^5-7x^4+28x^3+14x^2-9x+1$
(24) $x^7+7x^3+7x^2+7x-1$
(25) $x^7-14x^5+56x^3-56x+22$
(26) x^7-2
(27) x^7-7x+3
(28) $x^7+7x^4-7x^3-9$
(29) x^7+x+1
(30) x^8-2
(31) x^9-2
(32) $x^9-15x^6-87x^3-125$
(33) $x^{10}-2$
(34) $x^{11}-2$
(35) $x^{12}-2$
(36) $x^{15}-2$
(37) $x^{16}-2$

Table 1 : Timing for constructing Galois group (seconds on SPARCstation 2)

	order	ℓ	split	total
(1)	5	1	1. 18	1. 56
(2)	10	2	4. 20	5. 06
(3)	20	2	3. 50	4. 26
(4)	20	2	24. 02	50. 73
(5)	60	3	7415. 04	7430. 39
(6)	120	4	2059. 06	2060. 25
(7)	6	1	1. 61	1. 91
(8)	6	1	1. 86	2. 56
(9)	12	2	0. 96	2. 03
(10)	12	2	2. 32	4. 01
(11)	18	2	1. 98	3. 56
(12)	24	3	2. 17	3. 17
(13)	24	2	2. 48	4. 09
(14)	24	2	26. 49	28. 45
(15)	36	3	13. 51	14. 82
(16)	36	3	364. 55	369. 91
(17)	48	3	15. 20	16. 62
(18)	60	3	953. 42	1029. 02
(19)	72	4	92. 03	95. 24
(20)	120	3	x	x+162. 38
(21)	360	4	—	—
(22)	720	5	—	—
(23)	7	1	6. 43	7. 68
(24)	14	2	17. 46	27. 00
(25)	21	2	50. 18	65. 41
(26)	42	2	21. 4	25. 06
(27)	168	3	25157. 98	25497. 72
(28)	2520	5	—	—
(29)	5040	6	—	—
(30)	16	2	2. 33	4. 93
(31)	54	2	18. 04	23. 38
(32)	18	2	9. 79	27. 55
(33)	40	2	18. 39	26. 54
(34)	110	2	2738. 16	2744. 18
(35)	48	2	7. 91	20. 51
(36)	120	2	225. 78	240. 06
(37)	64	2	89. 92	119. 74

(x : 約 6 時間)

Table 2 : Comparison of method [A] and [B1] (seconds on SPARCstation 2)

	Group	ℓ	Mckay (Maple)	Anai (Asir)
(1)	+Z5	1	0. 68	1. 56
(2)	+D5	2	0. 82	5. 06
(3)	F20	2	0. 37	4. 26
(4)	F20	2	0. 78	50. 73
(5)	+A5	3	0. 12	7430. 39
(6)	S5	4	0. 13	2060. 25
(7)	Z6	1	2. 02	1. 91
(8)	S3	1	1. 75	2. 56
(9)	D6	2	1. 55	2. 03
(10)	+A4	2	3. 07	4. 01
(11)	3. S3	2	6. 73	3. 56
(12)	2. A4	2	2. 02	3. 17
(13)	+S4/V4	2	1. 97	4. 09
(14)	S4/Z4	2	17. 65	28. 45
(15)	3^2. 2^2	3	2. 37	14. 82
(16)	+3^2. 4	3	1. 88	369. 91
(17)	2. S4	3	1. 68	16. 62
(18)	+PSL2(5)	3	1. 78	1029. 02
(19)	3^2. D4	4	1. 43	95. 24
(20)	PGL2(5)	3	24. 25	x+162. 38
(21)	+A6	4	0. 26	—
(22)	S6	5	0. 27	—
(23)	+Z7	1	1. 28	7. 68
(24)	D7	2	1. 57	27. 00
(25)	+F21	2	5. 33	65. 41
(26)	F42	2	6. 41	25. 06
(27)	+PSL3(2)	3	5. 73	25497. 72
(28)	+A7	5	0. 42	—
(29)	S7	6	0. 25	—

Result of method [A]

(27) $x^7 - 7x + 3$

$\Rightarrow \underline{63 \cdot 441^3 \cdot f = h_1 h_2 \cdots h_7}$ over $Q(a,b,c)$

$h_1 = x - a$

$h_2 = x - b$

$h_3 = 63x + ((2a^5 + 5a^4 + a^3 + 7a^2 - 3a - 6)b^5 + (5a^5 + 5a^3 + 3a^2 - 7a)b^4 + (a^5 + 5a^4 - 8a^2 - 4a + 24)b^3 + (7a^5 + 3a^4 - 8a^3 - 6a^2 + 28a - 6)b^2 + (-3a^5 - 7a^4 - 4a^3 + 28a^2 - 14a + 45)b - 6a^5 + 24a^3 - 6a^2 + 45a - 12)$

$h_4 = x - c$

$h_5 = 441x + (((a^6 + 4a^5 + 9a^4 - 6a^3 - 10a^2 + 2a + 15)b^4 + (5a^6 + 6a^5 + 3a^4 - 23a^3 - 8a^2 + 38a - 9)b^3 + (5a^6 - a^5 - 18a^4 + 12a^3 + 13a^2 + 31a + 12)b^2 + (10a^6 - 9a^5 + 6a^4 + 17a^3 - 16a^2 + 55a - 18)b - 45a^6 + 9a^5 - 6a^4 - 24a^3 - 12a^2 - 174a + 207)c^3 + ((9a^6 + 15a^5 + 11a^4 + 9a^3 - 6a^2 + 11a - 12)b^5 + (18a^6 + 16a^5 + a^4 - 10a^3 + 2a^2 + 57a - 24)b^4 + (15a^6 + 4a^5 - 33a^4 - 13a^3 + 53a^2 + 107a - 27)b^3 + (11a^6 - 19a^5 + a^4 + 25a^3 + 114a^2 + 78a - 45)b^2 + (-24a^6 - 5a^5 + 22a^4 + 39a^3 + 16a^2 - 62a - 3)b - 3a^6 + 9a^5 + 36a^4 - 24a^3 - 117a^2 - 27a + 60)c^2 + ((-2a^6 - a^5 + 10a^4 - 2a^3 + 20a^2 + 10a - 9)b^5 + (-3a^6 - 5a^5 - 27a^4 - 17a^3 - 12a^2 + a + 18)b^4 + (4a^6 - 40a^5 - 13a^4 + 11a^3 - 26a^2 + 36a - 3)b^3 + (-41a^6 - 10a^3 - 26a^4 - 13a^3 + 4a^2 - 61a + 57)b^2 + (-8a^6 - 39a^5 - 93a^4 - 8a^3 + 3a^2 - 198a + 90)b - 42a^6 - 42a^5 + 21a^4 - 63a^3 - 42a^2 + 21a + 357)c + (4a^6 - 12a^5 - 27a^4 + 18a^3 - 47a^2 + 8a + 18)b^5 + (-11a^6 - 37a^5 + 20a^4 - 18a^3 - 9a^2 + 13a + 3)b^4 + (-30a^6 + 27a^5 - 18a^4 - 2a^3 + 62a^2 - 116a - 9)b^3 + (18a^6 - 40a^5 + 8a^4 + 25a^3 - 89a^2 - 174a + 81)b^2 + (-21a^6 + 7a^5 + 70a^4 - 63a^3 - 182a^2 + 238a - 21)b + 9a^6 + 15a^5 - 108a^4 - 54a^3 + 225a^2 - 3a + 30)$

$h_6 = 441x + (((a^5 + a^4 - a^3 + 11a^2 - 36a - 9)b^5 + (a^5 - 13a^4 + 13a^3 - 17a^2 - 8a - 9)b^4 + (-a^5 + 13a^4 + a^3 - 4a^2 - 48a + 30)b^3 + (11a^5 - 17a^4 - 4a^3 - 19a^2 + 17a - 15)b^2 + (-36a^5 - 8a^4 - 48a^3 + 17a^2 - 90a + 177)b - 9a^5 - 9a^4 + 30a^3 - 15a^2 + 177a - 129)c^3 + ((-12a^5 - 12a^4 - 2a^3 + a^2 - 9a + 3)b^5 + (-12a^5 + 9a^4 + 19a^3 - 6a^2 - 16a - 39)b^4 + (-2a^5 + 19a^4 + 23a^3 - 15a^2 - 47a - 3)b^3 + (a^5 - 6a^4 - 15a^3 - 129a^2 - 43a + 117)b^2 + (-9a^5 - 16a^4 - 47a^3 - 43a^2 + 156a - 3)b + 3a^5 - 39a^4 - 3a^3 + 117a^2 - 3a - 27)c^2 + ((-a^5 - a^4 + a^3 - 18a^2 - 13a + 51)b^5 + (-a^5 + 13a^4 + 22a^3 - 4a^2 + 78a - 33)b^4 + (a^5 + 22a^4 - 64a^3 + 25a^2 - 43a + 75)b^3 + (-18a^5 - 4a^4 + 25a^3 - 23a^2 + 95a - 27)b^2 + (-13a^5 + 78a^4 - 43a^3 + 95a^2 + 97a + 12)b + 51a^5 - 33a^4 + 75a^3 - 27a^2 + 12a + 45)c + (-a^5 - a^4 - 34a^3 + 17a^2 + 15a + 9)b^5 + (-a^5 - 22a^4 - 20a^3 - 11a^2 - 6a + 93)b^4 vvv + (-34a^5 - 20a^4 + 13a^3 - 3a^2 + 118a - 72)b^3 + (17a^5 - 11a^4 - 3a^3 + 131a^2 - 17a - 174)b^2 + (15a^5 - 6a^4 + 118a^3 - 17a^2 - 162a + 96)b + 9a^5 + 93a^4 - 72a^3 - 174a^2 + 96a + 24)$

$h_7 = 441x + (((-a^5 - a^4 + a^3 - 11a^2 + 36a + 9)b^5 + (-a^6 - 5a^5 + 4a^4 - 7a^3 + 27a^2 + 6a - 6)b^4 + (-5a^6 - 5a^5 - 16a^4 + 22a^3 + 12a^2 + 10a - 21)b^3 + (-5a^6 - 10a^5 + 35a^4 - 8a^3 + 6a^2 - 48a + 3)b^2 + (-10a^6 + 45a^5 + 2a^4 + 31a^3 - a^2 + 35a - 159)b + 45a^6 + 15a^4 - 6a^3 + 27a^2 - 3a - 78)c^3 + ((-9a^6 - 3a^5 + a^4 - 7a^3 + 5a^2 - 2a + 9)b^5 + (-18a^6 - 4a^5 - 10a^4 - 9a^3 + 4a^2 - 41a + 63)b^4 + (-15a^6 - 2a^5 + 14a^4 - 10a^3 - 38a^2 - 60a + 30)b^3 + (-11a^6 + 18a^5 + 5a^4 - 10a^3 + 15a^2 - 35a - 72)b^2 + (24a^6 + 14a^5 - 6a^4 + 8a^3 + 27a^2 - 94a + 6)b + 3a^6 - 12a^5 + 3a^4 + 27a^3 + 30a - 33)c^2 + ((2a^6 + 2a^5 - 9a^4 + a^3 - 2a^2 + 3a - 42)b^5 + (3a^6 + 6a^5 + 14a^4 - 5a^3 + 16a^2 - 79a + 15)b^4 + (-4a^6 + 39a^5 - 9a^4 + 53a^3 + a^2 + 7a - 72)b^3 + (41a^6 + 28a^5 + 30a^4 - 12a^3 + 19a^2 - 34a - 30)b^2 + (8a^6 + 52a^5 + 15a^4 + 51a^3 - 98a^2 + 101a - 102)b + 42a^6 - 9a^5 + 12a^4 - 12a^3 + 69a^2 - 33a + 39)c + (-4a^6 - a^5 - 7a^4 + 9a^3 - 19a^2 - 2a + 15)b^5 + (11a^6 + 3a^5 + 2a^4 + 3a^3 - a^2 + 42a - 96)b^4 + (30a^6 + 3a^4 - 11a^3 - 3a^2 + 26a - 87)b^3 + (-18a^6 - 26a^5 - 18a^4 + 34a^3 - 5a + 135)b^2 + (21a^6 - a^5 - 15a^4 - 27a^3 + 3a^2 + 22a + 51)b - 9a^6 + 18a^5 + 15a^4 - 42a^3 - 9a^2 + 33a + 30)$

$f_1 = a^7 - 7a + 3$

$f_2 = b^6 + b^5 a + b^4 a^2 + b^3 a^3 + b^2 a^4 + b a^5 + a^6 - 7$

$f_3 = 63c^4 + ((-2a^5 - 5a^4 - a^3 - 7a^2 + 3a + 6)b^5 + (-5a^5 - 5a^3 - 3a^2 + 7a)b^4 + (-a^5 - 5a^4 + 8a^2 + 4a - 24)b^3 + (-7a^5 - 3a^4 + 8a^3 + 6a^2 - 28a + 6)b^2 + (3a^5 + 7a^4 + 4a^3 - 28a^2 + 14a + 18)b + 6a^5 - 24a^3 + 6a^2 + 18a + 12)c^3 + ((a^4 - 2a^3 - 4a^2 + 5a)b^5 + (a^5 - 2a^3 + 12a^2 + 22a)b^4 + (-2a^5 - 2a^4 + 8a^3 + 20a^2 + 15a - 12)b^3 + (-4a^5 + 12a^4 + 20a^3 + 12a^2 + 5a + 15)b^2 + (5a^5 + 22a^4 + 15a^3 + 5a^2 + 25a - 6)b - 12a^3 + 15a^2 - 6a + 48)c^2 + ((5a^4 + 2a^3 + a^2 + 16a - 18)b^5 + (5a^5 + 6a^4 - 4a^3 + 18a^2 - 13a)b^4 + (2a^5 - 4a^4 + 16a^3 - 11a^2 - 18a + 48)b^3 + (a^5 + 18a^4 - 11a^3 - 6a^2 + 43a - 6)b^2 + (16a^5 - 13a^4 - 18a^3 + 43a^2 + 14a - 48)b - 18a^5 + 48a^3 - 6a^2 - 48a + 24)c + (4a^5 - a^4 + 9a^3 - 2a^2 - 16a + 6)b^5 + (-a^5 + 6a^4 + 2a^3 - 15a^2 - a + 45)b^4 + (9a^5 + 2a^4 - 22a^3 - 5a^2 + 40a)b^3 + (-2a^5 - 15a^4 - 5a^3 + 33a^2 - 8a + 84)b^2 + (-16a^5 - a^4 + 40a^3 - 8a^2 + 36a - 6)b + 6a^5 + 45a^4 + 84a^2 - 6a - 84$

Strong generators of the Galois group (order: 168),
(以下は [1,2,3,4,5,6,7] の像を示す.)

(1 2 3 4 5 6 7), (1 2 5 4 3 7 6),
(1 2 6 4 7 3 5), (1 2 7 4 6 5 3),
(1 3 2 5 4 6 7), (1 4 3 2 5 7 6),
(1 5 2 3 4 7 6), (1 6 2 7 4 3 5),
(1 7 2 6 4 5 3), (2 1 3 4 7 6 5),
(3 1 2 5 7 6 4), (4 1 3 2 6 7 5),
(5 1 2 3 6 7 4), (6 1 2 7 5 3 4),
(7 1 2 6 3 5 4).

A set of orders of abelian subgroups in finite groups

熊本大学大学院自然科学研究科　千吉良直紀

G を有限群とし、$\pi(G) = \{\, p : 素数 \mid p は |G| を割る \,\}$ とする。

$$\begin{aligned} \pi_e(G) &:= \{\, o(g) \mid g \in G \} \\ &= \{\, |H| \mid H は G の巡回部分群 \,\} \end{aligned}$$

とおく。$\pi_e(G)$ による G の特徴づけを考える。このような問題は古くから考えられていた。次のような定理がある。

定理 (B. H. Neumann (1937) [8]) $\pi_e(G) = \{1,2,3\}$ ならば、$G \simeq (Z_3 \times Z_3 \times \cdots \times Z_3) : Z_2$ または $((Z_2 \times Z_2) \times (Z_2 \times Z_2) \times \cdots (Z_2 \times Z_2)) : Z_3$ である。

定理 (G. Higman (1957) [5]) G を可解群とし、$\pi_e(G)$ が素数巾からなる集合とする。このとき $|\pi(G)| \leq 2$ である。

定理 (M. Suzuki (1962) [11]) G を単純群とし、$\pi_e(G)$ が素数巾からなる集合とする。このとき G は次のいずれかと同型である。

$$G \simeq L_2(q) \quad q = 5,7,8,9,17,\ L_3(4),\ Sz(8),\ Sz(32).$$

$M \subset \mathbb{N}$ に対して、

$$h(M) = \sharp\{G : 有限群 \mid \pi_e(G) = M\}/\simeq$$

とおく。$\pi_e(G)$ により、G が一意的に定まる場合もある。すなわち、$h(\pi_e(G)) = 1$ となる群 G については次のような定理がある。

定理 (Brandl, Praeger, Shi [2, 9, 10])
(1) $n = 5,7,8,9,11,13$ に対して、$h(\pi_e(A_n)) = 1$ である。
(2) $q > 3$, $q \neq 9$ に対して、$h(\pi_e(L_2(q))) = 1$ である。
(3) G を J_2, Co_1 以外の散在型単純群とする。このとき、$h(\pi_e(G)) = 1$ である。

注意 (1) $\pi_e(A_6) = \pi_e(2^4 : SL(2,4)) = \pi_e(2^{4n} : SL(2,4))$ より、$h(\pi_e(A_6)) = \infty$ である。
(2) $\pi_e(J_2) = \pi_e(S_8) = \pi_e(2^6 : A_8) = \pi_e(2^{6n} : A_8)$ より、$h(\pi_e(J_2)) = \infty$ である。

次のようなことも示されている。

定理 (**W. Shi [10]**) G が可解群ならば、$h(\pi_e(G)) = \infty$ である。

次のような予想があった。

予想 (**Praeger, Shi [9]**) 任意の $M \subset \mathbf{N}$ に対して、$h(M) \in \{0, 1, \infty\}$?

しかし、次のような定理が示された。

定理 (**Mazurov [7]**) $\pi_e(G) = \pi_e(L_3(5))$ ならば、$G \simeq L_3(5)$ または $Aut(L_3(5))$ である。すなわち、$h(\pi_e(L_3(5))) = 2$ である。

すなわち、予想は正しくなかった。このような例はほかにもある。

定理 (**Chigira, Shi [4]**) $\pi_e(G) = \pi_e(L_3(9))$ ならば、$G \simeq L_3(9)$ または $L_3(9).2_1$ である。

次に$\pi_e(G)$ が特徴のある集合のときを考える。

定義 $\pi_e(G) = \{1, 2, \cdots, n\}$ であるとき、G を OC_n群 という。

定理 (**Brandl, Shi [1]**) G が OC_n群 ならば、$n \leq 8$ であり、次のいずれかと同型である。ここで、$G = [N]Q$ は G が N の分裂拡大で、その補群が Q であることをあらわす。
(1) $n \leq 2$ のとき、$G \simeq {Z_2}^t$ である。
(2) $n = 3$ のとき、$G = [N]Q$ は *Frobenius* 群で、$N \simeq {Z_3}^t$, $Q \simeq Z_2$ または $N \simeq {Z_2}^{2t}$, $Q \simeq Z_3$ である。
(3) $n = 4$ のとき、$G = [N]Q$ で次のいずれかが成り立つ。

i) N は $\exp(N) = 4$, *class* 2 以下であり、$Q \simeq Z_3$ である。

ii) $N \simeq {Z_2}^{2t}$, $Q \simeq S_3$ である。

iii) G は *Frobenius* 群で、$N \simeq {Z_3}^{2t}$, $Q \simeq Z_4$ または $Q \simeq Q_8$ である。

(4) $n = 5$ のとき、$G \simeq A_6$ または $G = [N]Q$ で $N \simeq {Z_2}^{2t}$, $Q \simeq A_5$ で $SL(2,4)$-*module* として作用する。
(5) $n = 6$ のとき、次のいずれかが成り立つ。

i) $G = [P_5]Q$ は *Frobenius* 群 であり、$P_5 \simeq {Z_5}^{2t}$, $Q \simeq [Z_3]Z_4$ または $Q \simeq SL(2,3)$ である。

ii) $G/O_2(G) \simeq A_5$ で $O_2(G) \simeq Z_2{}^{2t}$ で *orthogonal* $SL(2,4)$-*module* である。

iii) $G \simeq S_5$ $G \simeq S_6$ である。

(6) $n=7$ のとき、$G \simeq A_7$ である。
(7) $n=8$ のとき、$G \simeq [PSL(3,4)] < \beta >$ で β は $PSL(3,4)$ の *unitary automorphism* である。

元の位数の集合すなわち巡回部分群の位数の集合を考えてきたが、これを可換部分群の位数の集合に拡張する。

$$\pi_a(G) = \{\ |A|\ |\ A \text{ は } G \text{ の可換部分群}\ \}$$

$\pi_a(G)$ による特徴づけを考える。OC_n群 と同様に次のような群を定義する。

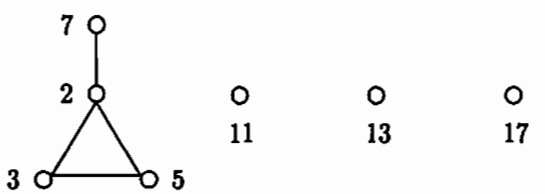
定義 $\pi_a(G) = \{1, 2, \cdots, n\}$ であるとき、G を OA_n群 という。

注意 明らかに $\pi_e(G) \subseteq \pi_a(G)$ であるが、OC_n群 であっても OA_n群 であるわけではない。例えば、$\pi_e(A_7) = \{1, 2, 3, 4, 5, 6, 7\}$ であるから OC_7群 であるが、$\pi_a(A_7) = \{1, 2, 3, 4, 5, 6, 7, 9, 12\}$ であるから OA_n群 ではない。

以下、OA_n群 の分類を考える。ここで、素数グラフが重要な役割を果たす。

定義 素数グラフ $\Gamma(G)$ とは $\pi(G)$ を頂点集合とし、2つの頂点 p, q は G の中に位数 pq の元が存在するときに辺で結ばれるというグラフである。$\nu(G)$ で素数グラフの連結成分の個数を表す。

$\pi_a(G)$ を与えると素数グラフを描くことができる。例えば、$\pi_a(G) = \{1, 2, \cdots, 17\}$ すなわち G が OA_{17}群 ならば、素数グラフ $\Gamma(G)$ は次のようになる。



G が OA_n群 のとき、次が成り立つ。

補題 G を OA_n群 とする。このとき、$n/2 < p \leq n$ なる素数 p に対して、$\{p\}$ は素数グラフの1つの連結成分を成す。

次の定理はよく知られている。

定理 (Bertrand's postulate) 任意の実数 $t \geq 1$ に対して、$t/2 < p \leq t$ を満たす素数 p が少なくとも 1 つ存在する。

これより次のことがわかる。

系 G を $n \geq 3$ なる OA_n群 とする。このとき、$\nu(G) \geq 2$ である。

次の定理は素数グラフの最も重要な定理の 1 つである。

定理 (Iiyori-Yamaki [6], Williams [12]) 任意の有限群 G に対して、$\nu(G) \leq 6$ である。

そこで、$n/2$ と n の間の素数の個数を数える。次のようなことが知られている。

補題 自然数 n に対して、$\pi(n)$ で n を越えない素数の個数を表すとする。このとき $n \geq 4000$ に対して、

$$\pi(2n) - \pi(n) > \frac{\log 2}{30} \frac{n}{\log 2n}$$

が成り立つ。

8000 以下の n についてはそれぞれ調べることにより、次が得られる。

補題 $n \geq 47$ のとき、$\sharp\{\, p : \text{素数} \mid n/2 < p \leq n \,\} \geq 6$ が成り立つ。

これより次のことがわかる。

系 G が OA_n群 ならば、$n \leq 46$ である。

また、次は素数グラフの基本定理である。

定理 (Gruenberg, Kegel [12]) $\nu(G) \geq 2$ のとき次のいずれかが成り立つ。
(1) G は *Frobenius* 群または 2-*Frobenius* 群 である。
(2) 正規部分群列 $G \trianglerighteq G_0 \trianglerighteq N \trianglerighteq 1$ が存在して、G/G_0 は可解 π_1 群、G_0/N は非可解単純群、N はべき零 π_1 群 である。ここで、π_1 は素数グラフ $\Gamma(G)$ の 2 を含む連結成分をあらわす。

OA_n群 の素数グラフの連結成分の個数は 2 以上であるから上の定理の群を調べることにより次の結果が得られる。

定理 (Chigira [3]) G が OA_n群 ならば、$n \leq 6$ であり、G は次のいずれかと同型である。

$$G \simeq 1,\ S_2,\ S_3,\ S_4,\ S_5,\ A_4,\ A_5.$$

参考文献

[1] R. BRANDL AND W. SHI, Finite groups whose element orders are consecutive integers, *J. Algebra* **143** (1991), 388–400.

[2] R. BRANDL AND W. SHI, The characterization of $PSL(2,q)$ by its element orders, *J. Algebra* **163** (1994), 109–114.

[3] N. CHIGIRA, Finite groups whose abelian subgroups have consecutive orders, preprint.

[4] N. CHIGIRA AND W. SHI, More on the set of element orders in finite groups, preprint.

[5] G. HIGMAN, Finite groups in which every element has prime power order, *J. London Math. Soc.* **32** (1957), 335–342.

[6] N. IIYORI AND H. YAMAKI, Prime graph components of the simple groups of Lie type over the field of even characteristic, *J. Algebra* **155** (1993), 335–343.

[7] V. D. MAZUROV, On the set of elements of finite groups, *Algebra and Logic* **33** (1994), 81–89.

[8] B. H. NEUMANN, Groups whose elements have bounded orders, *J. London Math. Soc.* **12** (1937), 195–198.

[9] C. PRAEGER AND W. SHI, A characterization of some alternating and symmetric groups, *Comm. Alg.* **22** (1994), 1507–1530.

[10] W. SHI, The characterization of the sporadic simple groups by their element orders, *Algebra Colloq.* **1** (1994), 159–166.

[11] M. SUZUKI, On a class of doubly transitive groups, *Ann. of Math.* **75** (1962), 105–145.

[12] J. S. WILLIAMS, Prime graph components of finite groups, *J. Algebra* **69** (1981), 487–513.