第17回
代数的組合せ論シンポジウム報告集

平成12年度文部省科学研究費基盤研究（A）
（課題番号　09304004　坂内英一）
平成12年度文部省科学研究費基盤研究（B）
（課題番号　0944004　宮本雅彦）

2000年6月19日～6月21日
於　つくば国際会議場

まえがき

この報告集は、2000年６月１９日（月）から２１日（水）にわたって、つくば市つくば国際会議場で行われた「第１７回代数的組合せ論シンポジウム」の講演記録です。交通の便の悪いつくばでしたが、６４名の出席者を迎え盛況に終えましたことを主催者として感謝しております。また、この研究集会は当然、代数的組合せ論を主とするものですが、つくばで開催するということもあり、前半に組合せ論に関係した範囲で、頂点作用素代数に関する講演を幾つか用意させていただきました。代数的組合せ論がますます広がり頂点作用素代数などの他の代数系とさらに結びついていくことを期待しております。

この研究集会に関しては、科学研究費（基盤研究B 課題番号0944004)による援助の他に、坂内英一様の科学研究費（基盤研究A(1) 課題番号09304004）による援助もいただきました。この場をお借りしてお礼を述べさせていただきます。

なお、私の連絡ミス等の為に報告書の発行が遅れましたことをお詫びいたします。

２０００年1月

宮本雅彦

「第１７回代数的組合せ論シンポジウム」

世話人：宮本　雅彦（筑波大学 数学系）
鈴木　寛（国際基督教大学 ）

日程: ２０００ 年 6 月 19 日(月曜日) -- 21 日(水曜日)
場所: つくば国際会議場２０２号室(つくば市竹園２丁目２０番３号)

プログラム

６月１９日（月曜日）

10:20-10:50　宮本雅彦（筑波大・数）
頂点代数と有限次元代数

11:00-11:30　佐久間伸也（筑波大・数学研究科 D2）
置換群とツイスト加群

11:40-12:30　安部利之 （阪大・理学研究科 D2）
Fusion Rules for the Vertex Operator Algebra V_{L}^{+}
for the Rank One Even Lattice

14:00-14:50　北詰 正顕(千葉大・理)
On 78-dimensional Schr¥"oder lattice for F_{22}

15:00-15:50　林　誠（愛知教育大）
Another approach to the Stellmacher's $¥Sigma_{4}$-free theorem

16:00-16:50　飯寄 信保（山口大・教養）
Generalized prime graphs

６月２０日（火曜日）

9:30-10:20　阿部 晴一（熊本大・理学研究科）
可解部分群の位数集合による有限単純群の特徴付け

10:30-11:20　竹ヶ原裕元（室蘭工業大学）
対称群の Frobenius 数の p-進的性質

11:30-12:00　平坂　貢(Postech(浦項工科大学))
On imprimitive blocks of a quasi-thin association scheme

プログラム（続き）

6月20日（火曜日）午後

13:30-14:00　坂内悦子（九大・数理）
ユークリッド空間の s-距離集合について

14:10-14:40　坂内英一（九大・数理）
On the nonexistence of certain type of association schemes whose character table entries are not in a cyclotomic number field

14:50-15:40　末竹 千博(姫路北高校)
Some blocking semiovals which admit a homology group

16:00-16:30　藤原　良（筑波大・社工）
PG(3,q)上での theta configuration の存在・非存在について

6月21日（水曜日）

9:30-10:20　田中太初（九大・数理）
On some relationships among the association schemes of finite orthogonal groups acting on hyperplanes

10:30-11:20　Jin Ho Kwak（Pohang University of Science & Technology）
Distributions of Branched Surface Coverings

11:40-12:10　Kaishun Wang（Academica Sinica）、鈴木寛（国際基督教大学）
Weakly distance-regular digraphs

13:30-14:20　田邊 顕一朗（Postech(浦項工科大学)）
Jacobi polynomials of ternary codes and generators of the invariant ring of a group

14:30-15:20　平峰　豊（熊大・教育）、Dominic Tion Elvira（熊大・自然科学）
On Relative Difference Sets in Non-Abelian p-Groups

15:30-16:20　中川暢夫（近畿大・理工）
有限群における相対差集合概観

目次

頂点代数と通常の代数

宮本雅彦

筑波大学・数学系

この講演では、頂点数から構成できる色々な代数構造について説明したいと思います。多くの構造はすでに知られているものですが、知られていなかった例としては、非可換ポアソン代数を構成することと、ズー代数を別の方法で構成できることを紹介します。最後に、ホップ代数との関係からボーチャーズが構成したフェイクモンスター形式群について述べます。

1 量子作用素の説明

V をベクトル空間とし、係数を $\mathrm{End}(V)$ に持つ形式的ベキ級数 $a(z)=\sum_{n\in\mathbf{Z}}a_nz^{-n-1}$ 全体の集合を $\mathrm{End}(V)[[z,z^{-1}]]$ で表します。

任意の元 $v\in V$ に対して十分大きな m をとると $a_mv=0$ となるとき、$a(z)\in End(V)[[z,z^{-1}]]$ を**量子作用素**と呼びます。

頂点作用素代数や頂点代数の理論において最も重要な概念は**正規積**と呼ばれる無限個の積です。これは2つの量子作用素 $a(z),b(z)$ に対して、新しい量子作用素 $a(z)_nb(z)$ を次のようにして定義します。

$$a(z)_nb(z)=\mathrm{Res}_w\{w^n(1-z/w)^na(w)b(z)-(-z)^n(1-w/z)^nb(z)a(w)\}$$

これにより、量子作用素全体の集合は無限個の積を持つ代数となります。$a(z)_nb(z)$ を $a_nb(z)$ で表します。

一応入門講義なので、少し記号の説明をしておきましょう。$\mathrm{Res}_w(\sum a_mw^{-1-m})=a_0$ で留数 $\frac{1}{2\pi i}\int_{w=0}(\sum a_mz^{-m-1})$ を拡張したものとします。Res_w は元々は整数ベキに対して定義しましたが、m として複素数ベキでも同様に w^{-1} の係数だけを取り出しますことにします。

正規積の例として

$$(a_0b)(z)=[a_0,b(z)]$$

$$(a_{-1}b)(z)=a^-(z)b(z)+b(z)a^+(z)$$

が成り立ちます。ここで、$a^+(z)=\sum_{n\geq0}a_nz^{-n-1}$, $a^-(z)=\sum_{n<0}a_nz^{-n-1}$ とします。

この正規積を成分で表示してみると、$a_m b(z)$ の z^{-n-1} での係数は

$$(a_m b)_n$$
$$= \sum_{i=0}^{\infty} (-1)^i \binom{m}{i} (a_{m-i} b_{n+i} - (-1)^m b_{m+n-i} a_i)$$

となっています。これは Associativity と呼ばれる重要な性質で、ボーチャズの最初の論文に載っていた式の一つです。
後で使う例として、

$$(a_{-1}b)_{-1}c = a_{-1}(b_{-1}c) + a_{-2}(b_0 c) + \ldots + b_{-2}a_0 c + b_{-3}(a_1 c) + \ldots$$

をあげておきます。

量子作用素全体は無限個の積を持つ代数となると言いましたが、これらを一気に調べるほど今の段階では余裕があるわけではありません。物理の場の理論からの要請もあり、我々の研究対象はある意味で可換部分代数なのです。丁度、半単純リー代数におけるカルタン部分代数を調べるようなものです。カルタン部分代数の時と同様にその部分代数から全体の構造が把握出来ることを期待しています。ただ、ここでいう可換とは本当の可換ではありません。２つの量子作用素が本当の意味で可換だと、すべての成分が互いに可換になってしまい数学的にも物理的にも意味のあるものは出来ません。ここでの可換とは次の局所可換を言います。

定義 1 量子作用素 $a(z), b(z)$ が**局所可換**とは十分大きな n があって

$$(z-w)^n a(w)b(z) = (z-w)^n b(z)a(w)$$

が成り立つことを言います。

自分自身と局所可換な量子作用素のことを**頂点作用素**と呼びます。
局所可換に対応する式を係数表示してみると

$$[a_n, b_m] = \sum_{i=0}^{\infty} \binom{n}{i} (a_i b)_{n+m-i}$$

です。この式がもっともよく使う式です。ただし、これは局所可換と同値というわけではありません。

定義 2 $(V, Y, 1, L(-1))$ が**頂点代数**とは、フォック空間と呼ばれる次数付きベクトル空間 $V = \oplus_{n \in \mathbb{Z}} V_n$ と、その各元 v に対して互いに局所可換な量子作用素

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

が線形に定義され、次の条件を満たしているものをいいます。
(1) **微分作用素** $L(-1) : V_m \to V_{m+1}$ は次を満足する

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

(2) **真空**と呼ばれる元 $\mathbf{1} \in V_0$ が存在して次を満足する $Y(1,z) = 1$
$v_n 1 = 0 \quad (n \geq 0)$ $v_{-1}1 = v$
(3) **次数作用素** $L(0)|_{V_n} := n$ あり、任意の斉次元 $v \in V_n$ に対して, $v_m(V_k) = V_{k-m-1+n}$ が成り立つ。

頂点作用素のテンソル積
$(V^1, Y^1, \mathbf{1}^1, L^1(-1))$, $(V^2, Y^2, \mathbf{1}^2, L^2(-1))$ を頂点代数とする。この時、テンソル積空間をフォック空間とする

$$(V^1 \otimes V^2, Y \otimes Y^2, \mathbf{1}^1 \otimes \mathbf{1}^2, L^1(-1) \otimes 1 + 1 \otimes L^2(-1))$$

は頂点代数となる。 ここで、テンソル積空間の頂点作用素は $Y^1 \otimes Y^2$ は $Y^1 \otimes Y^2(v^1 \otimes v^2, z) = Y^1(v^1, z)Y^2(v^2, z)$ で与えます。

簡単で重要な例

補題 1 $W = \mathbb{C}[t]$ を多項式環とし、$W_n = \mathbb{C}t^{-n}$ と置く。
$\mathbf{1} = 1$, 微分作用素 $L(-1)$ を微分 $\frac{d}{dt}$ で定義し、
頂点作用素を $Y(t^n, z) = (t+z)^n$ と置くと、$(\mathbb{C}[t], Y(*,z), 1)$ は頂点代数となる。

頂点部分代数

補題 2 頂点代数 W と $v \in W$ に対して

$$W(v) = \{w \in W | v_0 w = 0\}$$

は頂点部分代数となる。

頂点代数で与えられる通常の代数
よく知られているように、
$(V/L(-1)V, \times_0)$ はリー代数であり、
$(V_1/L(-1)V_0, \times_0)$ はその部分代数となっています。

ヴィラソロ元の頂点作用素の成分で生成されるヴィラソロ代数に対するウエイト1の最高ウエイトベクトルの集合

$$P_1 = \{v \in W_1 | L(n)v = 0 \forall n > 0\}$$

を考えてみます。この時、

$$\mathcal{G} = P_1/Rad(P_1)$$

は積 $\times_0$ によりリー代数となります。ここで内積は頂点代数の内積を制限したものです。例えば、
(1) $W = V_\Lambda \otimes V_U$ の場合には $\mathcal{G}_\Lambda$ はフェイクモンスターリー代数となり、
(2) $W = V^\natural \otimes V_U$ の場合が $\mathcal{G}^\natural$ はモンスターリー代数です。
ここで、Λ はリーチ格子を表し、U は2次元のローレンチアン偶正則格子を表しています。

頂点代数の中の結合代数
(1) Zhu 代数: 頂点作用素代数によって定義される代数のうち最も重要な結合代数はズー代数 $A(V)$ でしょう。これは V の剰余空間 $V/O(V)$ として与えられています。$O(V)$ の定義はここでは省略します。
ズー代数の重要な性質は既約 $A(V)$-加群と既約 V-加群は1対1対応していることである。特に、V-既約加群の最高ウエイト空間が $A(V)$-既約加群となっており、この関係で1対1対応がついています。
(2) $V/C_2(V)$ は結合積 $\times_{-1}$ とリー積 $\times_0$ によって可換ポアソン代数となる。ここで $C_2(V) =< u_{-2}v | u, v \in V >$ です。特に、$\dim V/C_2(V) < \infty$ であるとき、C_2-条件を満たすといい、この条件がモジュラー不変性を証明するときの条件として使われています。

(3) 新しい代数の例として、

補題 3 $W = \oplus_{n \in \mathbb{Z}} W_n$ を頂点代数とし、$Q = (W_0)_{-2}W_{-1}$ とおくと、$P(W) := (W_0/Q, \times_{-1})$ は結合代数となる。

[Proof] 結合律から容易に出てくる。

Q.E.D.

これを利用すると、ズー代数の新しい理解の方法が出てきます。

補題 4 もし V が頂点作用素代数で、$W = V \otimes \mathbb{C}[t]$ とおくと、$P(W)$ は V のズー代数 $A(V)$ と同型となる。

2 ボーチャーズ論文 Fake Monster formal group の紹介

ホップ代数と頂点代数との関係を説明するために、ボーチャーズの論文（フェイクモンスター形式群）を紹介しよう。ボーチャーズの論文の主題は整数環上でフェイクモンスター形式群を構成していることである。より一般的に、ここでのリー代数 G は環 R 上のリー代数としておきます。

定義 3 もし $\mathcal{G}$ がリー代数なら自然に R 上の普遍包絡環 $U(\mathcal{G})$ はホップ代数となる。この時の余積 は $v \in \mathcal{G}$ に対して

$$\Delta(v) = v \otimes 1 + 1 \otimes v$$

で定義される。この性質を満たす元を**原始的**と呼ぶ。

定義 4 リフティングの定義
$\mathcal{G}_\Lambda$ の元 a_1 に対して、普遍包絡環 $U(\mathcal{G}_\Lambda)$ の元 a_i があって

$$v(x) = 1 + a_1 x + \sum_{i=2}^{\infty} a_i x^i$$

とおくと、

$$\Delta(v(x)) = v(x) \otimes v(x)$$

が成り立つとき、$v(x)$ を a_1 の**リフティング**と呼ぶ。また、$\Delta(v(x)) = v(x) \otimes v(x)$ を満たすような元を**群的元**と呼ぶ。

容易に群的元の集合 $G(U(\mathcal{G}_\Lambda))$ は群となることは証明できます。ボーチャーズの証明したことは、フェイクモンスターリー代数 $\mathcal{G}_\Lambda$ のすべての元に対してリフティングが存在するということです。これにより、リフティング全体で生成される部分群 $G(U(\mathcal{G}_\Lambda))$ を核 $H = < v(x) | v_1 = 0 >$ で割ることで、**フェイクモンスター形式群** $G(U(\mathcal{G}_\Lambda))/H$ を構成したのです。簡単にこの証明を再現してみます。

リフティングの定義から容易に次の補題が分かります。

補題 5 $\mathcal{G}_\Lambda$ の元 a_1 と b_1 に対してリフティングが存在すれば、$a_1 + b_1$ に対してもリフティングが存在する。また、任意の $\lambda \in R$ に対して λa_1 もリフティングが存在する。

難しい点として

補題 6 $\mathcal{G}_\Lambda$ の元 a_1 と b_1 に対してリフティングが存在すれば、$[a_1, b_1]$ に対してもリフティングが存在する。

をボーチャーズは苦労して証明しているのですが、もっと簡単にこれが証明できるのではないかとも書いてあります。

通常の有理数体上の有限次元半単純リー代数 $\mathcal{G}$ の場合には $g \in \mathcal{G}$ に対して

$$\exp(gx) = 1 + gx + \frac{g^2x^2}{2!} + ...$$

がリフティングとなってくれています。しかし、整数係数の場合にはこれが定義できるとは限りません。上の２つの補題からリー代数としての生成元に対してリフティングが定義できると良いわけですが、フェイクモンスターリー代数はルートとノルム０の元で生成されているという特別な性質を持っています。ボーチャーズはこの点に着目して、ルートとノルム０の元に対しては整数係数の範囲でリフティングが定義できることを示し、形式群を構成したのです。

2.1 モンスター形式群の構成

$L = \Lambda \oplus U \cong \Pi_{25,1}$ を２６次元のローレンティアン格子とし、
$W = V_L$ を L から構成される格子頂点代数とすると、リー代数 $\mathcal{G}_\Lambda$ は W_1 の部分空間となります。ここで群的元 $v(x) \in U(\mathcal{G}_\Lambda)[[x]]$ で、$v_0 = 1, v_1 \in \mathcal{G}_\Lambda$ となるものを考えます。

ボーチャーズが構成した整数環上のフェイクモンスター形式群の方法を利用して、モンスター形式群を構成してみましょう。ただし、ボーチャーズが利用した V_Λ における整数環上の正則な頂点作用素代数というものは $V^\natural$ においては見つかっていません。この整数環上の正則な頂点作用素代数の存在は頂点作用素代数と有限群との関係において非常に重要な問題です。現在のところ、クリフォード代数を利用したムーンシャイン頂点作用素代数の構成法により、$\mathbb{Z}[\frac{1}{2}]$ 上ではそのような環上の正則な頂点作用素代数の存在が示されておりますので、それを利用して、$\mathbb{Z}[\frac{1}{2}]$ 上のモンスター形式群を構成して見ましょう。

ムーンシャイン頂点作用素 $V^\natural$ は V_Λ からオービフォルド構成によって最初構成されました。すなわち、ある位数２の自己同型 $\theta \in Aut(V_\Lambda)$ があって、$(V_\Lambda)^\theta \subseteq V^\natural$ となります。リー代数としてみると、

$$(V_\Lambda \otimes V_U)^\theta \subseteq V^\natural \otimes V_U$$

から

$$(\mathcal{G}_\Lambda)^\theta \subseteq (\mathcal{G}^\natural)$$

となることが分かります。$(\mathcal{G}_\Lambda)^\theta$ の元をリフティングした場合にボーチャーズの結果からだけでは、その係数が $U(\mathcal{G}_\Lambda)^\theta$ となることは証明できますが、不変包絡環では当然

$$U(\mathcal{G}_\Lambda)^\theta \not\subseteq U(\mathcal{G}^\natural)$$

ですので、$U(\mathcal{G}^\natural)$ の元を係数としているかどうか不明です。

この点をこれまで紹介した内部にある代数を使って解決しましょう。

まず、$U(\mathcal{G}_\Lambda)$ をある頂点代数の中に埋め込みます。
このような例として、$\mathcal{G}$ が有限次元半単純リー代数の場合には、これをアフィン化 G[x] し、それから構成される頂点作用素代数 [Frenkel, Zhu] $U(\mathcal{G}[x])$ を考えると、この頂点作用素代数のズー代数 $A(U(\mathcal{G}[x]))$ は元々の不変包絡環 $U(\mathcal{G})$ と同型となります。

今回の場合、頂点代数 $V_\Lambda \otimes V_U$ に補題 3 を利用するわけで、$P(V_\Lambda \otimes V_U \otimes \mathbb{C}[t])$ を考えると、この中に $\mathcal{G}_\Lambda$ と同形なものが埋めこまれていることがわかります。それゆえ、それで生成される部分結合代数 $W(\mathcal{G}_\Lambda)$ を考えます。この場合にボーチャーズが使った論法を全く同じ様に使って θ で不変な元を成分とするようなリフティングを構成します。この場合には $\mathbb{Z}[\frac{1}{2}]$ 上で考えていることを使って、θ-不変な $P(V_\Lambda \otimes V_U \otimes \mathbb{C}[t])$ の元はすべて $(V_\Lambda)^\theta \otimes V_U \otimes \mathbb{C}[t]$ の元の像として捉えられることが証明できます。それゆえ、$\mathcal{G}_\Lambda$ の θ-不変な元に対しては $U(\mathcal{G}^\natural)$ の元を係数とするリフティングが構成できることになります。

定理 1 $w \in \mathcal{G}_\Lambda^\theta$ に対して、${}^3w(x)$ は θ-不変な群的元であり、
$w(0) = 1$, $(w(1))_{-1} = w_0$　を満たしている。

次に、$\mathcal{G}^\natural$ の自己同形群（モンスター単純群）を使います。リフティングは自己同形で移してもリフティングとなります。$\mathcal{G}_\Lambda^\theta$ のモンスター単純群の作用による共役全体は $\mathcal{G}^\natural$ 全体を生成しますので、これにより $\mathcal{G}^\natural$ のすべての元に対してリフティングが構成できたことになります。

定理 2 $v_1 \in (\mathcal{G}^\natural)$ に対するリフティング

$$v(x) = 1 + v_1 x + \sum_{i=1}^{\infty} v_i x^i$$

が定義できる。特に、*Monster formal Lie group* を構成できる。

参考文献

[B1] R. E. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster, Proc. Natl. Acad. Sci. USA 83 (1986), 3068-3071.

[B2] R. E. Borcherds, Fake monster formal group, Duke Math. J. 100 (1999), 139-165.

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

[FZ] I. Frenkel and Y. Zhu, Vertex operator algebras associated to representations of affine and Virasoro algebras, Duke Math. J. 66 (1992), 123-168.

置換群とツイスト加群

佐久間伸也

筑波大学数学研究科

1 序文

今回の話では、ある code D から構成される code VOA M_D と D の自己同型から誘導される M_D の自己同型に対するツイスト加群を構成する。今回の結果は筑波大学数学系の宮本雅彦先生との共同研究によるものである。

散在型有限単純群のうち位数最大である Monster 単純群 $\mathbb{M}$ と modular 関数に関する Moonshine 予想の中で最も基本的なのが、McKay と Thompson による次の予想である。

予想 1. ある無限次元の次数付き *Monster* 加群 $V = \oplus_{n=0}^{\infty} V_n$ があって、次を満たす。

1.
$$\sum_{n=0}^{\infty} (dim\, V_n) q^{n-1} = j(\tau) - 744 = q^{-1} + 196884q + \cdots, q = e^{2\pi i \tau}$$
が成り立つ。ここで、$j(\tau)$ は古典的楕円 *modular* 関数である。

2. 各 $g \in \mathbb{M}$ に対して、種数 0 の $SL(2,\mathbb{R})$ のある離散部分群 Γ_g があって、*Thompson* 級数
$$T(g,\tau) = \sum_{n=0}^{\infty} Tr(g|_{V_n}) q^{n-1}$$
が Γ_g-不変となる。即ち、$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_g$ に対して $T(g, \frac{a\tau+b}{c\tau+d}) = T(g,\tau)$ となる。

この予想の解答として、Frenkel、Lepowsky、Meurman により Moonshine 加群 $V^\natural = \oplus_{n=0}^{\infty} V_n^\natural$ が構成され ([FLM])、これと Borcherds の考えた頂点代数の概念 [B] を合わせて、Moonshine 頂点作用素代数 (VOA) $V^\natural$ が構成された。[FLM] さらに、$V^\natural$ の全自己同型群は Monster 単純群になることが知られている。これが VOA の出発点である。

$(V,Y,\mathbf{1},\omega)$ を rank c の VOA、g,h を有限位数の可換な V の自己同型とする。g-ツイスト V-加群 $W=\oplus_{\lambda\in\mathbb{C}}W_\lambda$ に対して、h は W のある線形変換 $\phi(h)$ を与える。この時、

$$\begin{aligned} T_W(h,\tau) &= Tr_W\phi(h)q^{L(0)-\frac{c}{24}} \\ &= \sum_{\lambda\in\mathbb{C}} Tr(\phi(h)|_{W_\lambda})q^{\lambda-\frac{c}{24}} \end{aligned}$$

とする。$V=V^\natural(=W)$、$g=1$ のとき、これは上の Thompson 級数になる。

VOA と modular 不変性に関して、Zhu はある有限性の条件 C_2 を満たす有理型 VOA が modular 不変性をもつことを示した。[Z] さらに、Dong、Li、Mason がこれを拡張して、次のようなことが示された。[DLM]

定理 1. *[DLM]* $C(g,h,\tau)=\{T_W(h,\tau)|W:$ 既約g–ツイストV–加群 $\}$ とする。この時、$(V,Y,\mathbf{1},\omega)$ が条件 C_2 を満たす有理型 *VOA* のとき、$\gamma=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in S_(2,\mathbb{Z})$ に対して、

$$C(g,h,\frac{a\tau+b}{c\tau+d})=C(g^ah^b,g^ch^d,\tau)$$

が成り立つ。特に、$g=1$、$\gamma=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ の場合、

$$C(1,h,-\frac{1}{\tau})=C(h,1,\tau)$$

となる。

一方、Moonshine VOA $V^\natural$ が、holomorphic、即ち既約加群が自分自身だけである事より、次のことも示された。

定理 2. *[DLM]* 各 $h\in Aut(V^\natural)$ に対して、既約 h-ツイスト $V^\natural$-加群も唯一つ存在する。*(*これを $V^\natural(h)$ であらわすことにする。*)*

$V^\natural$ は条件 C_2 を満たすので、以上の事より、各 $h\in\mathbb{M}=Aut(V^\natural)$ に対して、

$$T(h,-\frac{1}{\tau})=\alpha T_{V^\natural(h)}(1,\tau)\ ,\ \alpha\in\mathbb{C}$$

と書ける。この事から、変換 $\tau\mapsto-\frac{1}{\tau}$ が h-ツイスト加群を通して見ることができる。ところが、上の結果ではツイスト加群の存在は示されているが、構成の方は実際位数 2 の (2 つの) 共役類に対してしかされていない。他の元に対するツイスト加群を構成するというのが、今回の話の出発点であり、最終的な目標である。

ツイスト加群を構成するために、今回は $V^\natural$ が Framed VOA であることに注目する。VOA V が互いに直交する中心電荷 $\frac{1}{2}$ の共形元 $e^1,\cdots,e^n$ でその和が V の

Virasoro 元に一致するものをもつとき、V はFramed VOA と呼ばれる。[DGH] この時、V はIsing 模型 $L(\frac{1}{2},0)$ の n 個のテンソル積 $L(\frac{1}{2},0)^{\otimes n}$ を部分VOA として含む。Dong、Mason、Zhu は、$V^{\natural}$ がそのような48 個の共形元をもつことを示した。[DMZ] $L(\frac{1}{2},0)$ は3 つの既約加群 $L(\frac{1}{2},k), k=0,\frac{1}{2},\frac{1}{16}$, をもち、Framed VOA V を $L(\frac{1}{2},0)^{\otimes n}$ の加群と見れば、V は、$L(\frac{1}{2},0)^{\otimes n}$ の既約加群 $L(k_1,\cdots,k_n)=L(\frac{1}{2},k_1)\otimes\cdots\otimes L(\frac{1}{2},k_n), k_i=0,\frac{1}{2},\frac{1}{16}$, の直和

$$V=\bigoplus_{k_i=0,\frac{1}{2},\frac{1}{16}} a_{k_1,\cdots,k_n}L(k_1,\cdots,k_n)$$

に分解する。ここで、$a_{k_1,\cdots,k_n}$ は重複度を表す。一般に Framed VOA は複雑であり、その加群を分類するのは困難である。今回は $L(\frac{1}{2},\frac{1}{16})$ がない場合、即ち

$$V=\bigoplus_{k_i=0,\frac{1}{2}} a_{k_1,\cdots,k_n}L(k_1,\cdots,k_n)$$

となる場合を考える。この時、V が単純VOA であれば、$a_{k_1,\cdots,k_n}=0$ *or* 1 であり、$D=\{(2k_1,\cdots,2k_n)|a_{k_1,\cdots,k_n}=1\}\subset\mathbb{Z}_2^n$ は(binary) code となる。さらに、V は code VOA M_D と呼ばれるVOA になる。[M1, M2] 対称群 S_n の元 g が座標の置換による作用で D を不変にする時、g は $\tilde{g}(e^i)=e^{g(i)}$ である M_D の自己同型 $\tilde{g}$ を誘導する。[M1] 記号を簡単にするためこれも g で表す。

V をVOA とする。V のk個のテンソル積(VOA)$V^{\otimes k}$ とその自己同型 $g=(1\,2\cdots k)$ を考える。Barron,Dong, Mason は、V-加群 (W,Y_W) が与えられたとき、空間 W 上に Y_W から $V^{\otimes k}$ のある g-ツイスト加群の構造 (W,Y_g) を構成した。[BDM] 今回の結果は、これをSVOA V の場合に拡張し、code VOA $M_D\subset(L(\frac{1}{2},0)\oplus L(\frac{1}{2},\frac{1}{2}))^{\otimes k}$ に応用したものである。

2 code VOA

この節では、(binary) code VOA を構成する。初めにSVOA を定義する。

定義 1. $\frac{1}{2}\mathbb{Z}$-次数付きベクトル空間 $V=\oplus_{n\in\frac{1}{2}\mathbb{Z}}V_n=V_{\bar{0}}\oplus V_{\bar{1}}$ と線形写像

$$\begin{aligned} Y(\cdot,z):V &\to (\mathrm{End}V)[[z,z^{-1}]] \\ v &\mapsto Y(v,z)=\sum_{n\in\mathbb{Z}}v_nz^{-n-1}\ \ (v_n\in\mathrm{End}V), \end{aligned}$$

と V の元 $\mathbf{1}$、ω について、次が成り立つ時、$(V,Y,\mathbf{1},\omega)$ は頂点作用素超代数 *(SVOA)* であるという。ただし、$V_{\bar{s}}=\oplus_{n\in\frac{s}{2}+\mathbb{Z}}V_n$ であり、$u\in V_{\bar{s}}$ のとき $s=\bar{u}$ とする。:

(V1) $dim\,V_n<\infty$ かつ、十分小さい n に対して $V_n=0$ となる。

(V2) 任意の $u,v\in V$ に対し、十分大きな n で $u_nv=0$ となる。

(V3) $Y(\mathbf{1},z)=Id_V$

(V4) 任意の $v\in V$ に対して、$Y(v,z)\mathbf{1}\in(\mathrm{End}V)[[z]]$ かつ $\lim_{z\to 0}Y(v,z)\mathbf{1}=v$

(V5) $m,n\in\mathbb{Z}$ に対して、

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

となる。ここで、$Y(\omega,z)=\sum_{n\in\mathbb{Z}}L(n)z^{-n-2}$、$cV\in\mathbb{C}$ である。

(V6) 任意の $v\in V$ に対して、$Y(L(-1)v,z)=\frac{d}{dz}Y(v,z)$

(V7) $L(0)|_{V_n}=nId_{V_n}$

(V8) $\mathbb{Z}_2$-*homogeneous* な $u,v\in V$ に対して、次の *Jacobi* 律が成り立つ。

$$z_0^{-1}\delta\left(\frac{z_1-z_2}{z_0}\right)Y(u,z_1)Y(v,z_2)-(-1)^{\bar{u}\bar{v}}z_0^{-1}\delta\left(\frac{z_2-z_1}{-z_0}\right)Y(v,z_2)Y(u,z_1)$$
$$=z_2^{-1}\delta\left(\frac{z_1-z_0}{z_2}\right)Y(Y(u,z_0)v,z_2)$$

$V_{\bar{1}}=0$ のときには $V=V_{\bar{0}}$ は *VOA* である。

SVOA V は超局所可換性を満たす。: $\mathbb{Z}_2$-homogeneous な $u,v\in V$ に対して、ある正整数 N があって、

$$(z-w)^NY(u,z)Y(v,w)=(-1)^{\bar{u}\bar{v}}(z-w)^NY(v,w)Y(u,z)$$

が成り立つ。

次に (binary) code VOA を構成する。k は正整数とする。$(V=V_{\bar{0}}\oplus V_{\bar{1}},Y,1,\omega)$ を SVOA とする。V の k 個のテンソル積 $F=V^{\otimes k}$ を考え、$\otimes_{i=1}^k v_i\in F$ $(v_i\in V)$ に対して、頂点作用素 $Y(\otimes_{i=1}^k v_i,z)=\otimes_{i=1}^k Y(v_i,z)$ を定義し、F 全体に線形に拡張する。codeword $\alpha=(\alpha_1,\cdots,\alpha_k)\in\mathbb{Z}_2^k$ に対して、$V_\alpha=V_{\bar{\alpha_1}}\otimes\cdots\otimes V_{\bar{\alpha_k}}$ とすれば、$F=\oplus_{\alpha\in\mathbb{Z}_2^k}V_\alpha$ である。V の超局所可換性から、$u\in V_\alpha,v\in V_\beta$ に対して、

$$(z-x)^NY(u,z)Y(v,x)=(-1)^{(\alpha,\beta)}(z-x)^NY(v,x)Y(u,z)$$

となる。

$D\subset\mathbb{Z}_2^k$ を (線形)code とする。上の $(-1)^{(\alpha,\beta)}$ を消すために、D の内積による $\langle\pm1\rangle$ での中心拡大した群 $\hat{D}=\{e^\alpha|\alpha\in D\}$ を考える。このとき、fock 空間を

$$V_D=\oplus_{\alpha\in D}(V_\alpha\otimes e^\alpha)$$

と定義し、頂点作用素を $v\in V_\alpha$ に対して

$$Y(v\otimes e^\alpha,z)=Y(v,z)\otimes e^\alpha$$

と定義すると、超局所可換が成り立つことが分かる。真空は $\hat{1} = (\otimes_{i=1}^{k} 1) \otimes e^0 \in V_{(0^k)}$ であり、

$$e^i = (\otimes_{j=1}^{i-1} 1) \otimes \omega \otimes (\otimes_{j=i+1}^{k} 1) \otimes e^0$$

とおくと、e^i は共形元であり、$\hat{\omega} = e^1 + \cdots + e^k$ は V_D の Virasoro 元になる。即ち、次が成り立つ。

定理 3. *[M1] (1) D が偶 code のとき、$(V_D, Y, \hat{1}, \hat{\omega})$ は VOA である。*
(2) $(V_{\mathbb{Z}_2^k}, Y, \hat{1}, \hat{\omega})$ は SVOA である。

3 ツイスト加群の構成

この節では、[BDM] の結果を拡張して、code VOA のツイスト加群を構成する。初めにツイスト加群の定義を与える。

定義 2. *$(V, Y, 1, \omega)$ は SVOA とし、g は位数 k の V の自己同型とする。ベクトル空間 W と線形写像*

$$\begin{aligned} Y^W(\cdot, z) : V &\to (\mathrm{End}W)[[z^{\frac{1}{k}}, z^{-\frac{1}{k}}]] \\ v &\mapsto Y(v,z) = \sum_{n \in \frac{1}{k}\mathbb{Z}} v_n z^{-n-1} \ (v_n \in \mathrm{End}W) \end{aligned}$$

が次を満たす時、(W, Y^W) は g-ツイスト V-加群であるという。

(W1) $W = \oplus_{\lambda \in \mathbb{C}} W_\lambda$ となる。ただし、$W_\lambda = \{w \in W | L^W(0)w = \lambda w\}$、$Y^W(\omega, z) = \sum_{n \in \mathbb{Z}} L^W(n) z^{-n-2}$, である。

(W2) 任意の $\lambda \in \mathbb{C}$ に対して、$W_\lambda < \infty$ かつ十分小さい $n \in \frac{1}{2k}\mathbb{Z}$ に対し $W_{\lambda+n} = 0$ となる。

(W3) 任意の $u \in V$ と $w \in W$ に対して、十分大きな n で $u_n w = 0$ となる。

(W4) $Y^W(1, z) = Id_W$

(W5) $u \in V^r = \{v \in V | gv = e^{-\frac{2\pi i r}{k}} v\}$ のとき、$Y^W(u, z) = \sum_{n \in \frac{r}{k} + \mathbb{Z}} u_n z^{-n-1}$ となる。

(W6) $\mathbb{Z}_2$-*homogeneous* な $u \in V^r$ と $v \in V$ に対して、次のツイスト *Jacobi* 律が成り立つ。

$$\begin{aligned} & z_0^{-1} \delta\left(\frac{z_1 - z_2}{z_0}\right) Y^W(u, z_1) Y^W(v, z_2) \\ & -(-1)^{\bar{u}\bar{v}} z_0^{-1} \delta\left(\frac{z_2 - z_1}{-z_0}\right) Y^W(v, z_2) Y^W(u, z_1) \\ & = z_2^{-1} \delta\left(\frac{z_1 - z_0}{z_2}\right) \left(\frac{z_1 - z_0}{z_2}\right)^{-\frac{r}{k}} Y^W(Y(u, z_0)v, z_2). \end{aligned}$$

Y^W についても超局所可換性が成り立つ。: $\mathbb{Z}_2$-homogeneous な $u, v \in V$ に対して、ある正整数 N があって、

$$(z-x)^N Y^W(u,z)Y^W(v,x) = (-1)^{\tilde{u}\tilde{v}}(z-x)^N Y^W(v,x)Y^W(u,z)$$

が成り立つ。

$(V, Y, 1, \omega)$ はSVOAとし、kは正整数とする。$g = (1\,2\cdots k)$ とする。$\sigma = e^{2\pi i L(0)}$ はVの位数2の自己同型になる。(W, Y^W) をσ^l-ツイストV-加群(l=0,1)とする。W上に$\sigma_1^{l+k-1}\tilde{g}$-ツイスト$V_{\mathbb{Z}_2^k}$-加群構造$(W, Y_g)$を定義していく。ここで、$\sigma_1$はテンソル積の第1成分だけ$\sigma$が作用する自己同型$(\sigma, 1, \cdots, 1)$であり、$\tilde{g}$は座標の置換により$g$から誘導される自己同型である。$u \in V_{\bar{0}} \cup V_{\bar{1}}$ に対して$V_{\mathbb{Z}_2^k}$の元$u^j, j = 1, \cdots, k$, を

$$(\otimes_{i=1}^{j-1} 1) \otimes u \otimes (\otimes_{j+1}^{k} 1) \otimes e^{\delta_{a,1}\kappa_j}$$

とする。ここで、$\kappa_j = (0^{j-1}10^{k-j})$である。このとき、$\{u^j | u \in V_{\bar{0}} \cup V_{\bar{1}}, j = 1, \cdots, k\}$ は$V_{\mathbb{Z}_2^k}$を生成する。まず生成元に対してY_gを定義する。

定義 3. *(c.f. [BDM])* $\Delta_k(z) \in (End\ V)[[z^{\frac{1}{2k}}, z^{-\frac{1}{2k}}]]$ を

$$\Delta_k(z) = \exp\left(\sum_{j\in\mathbb{Z}_+} a_j z^{-\frac{j}{k}} L(j)\right) k^{-L(0)} z^{\left(\frac{1}{k}-1\right)L(0)}$$

とする。ただし、$a_j, j \in \mathbb{Z}_+$, は

$$\exp\left(-\sum_{j\in\mathbb{Z}_+} a_j x^{j+1}\frac{\partial}{\partial x}\right)\cdot x = \frac{1}{k}(1+x)^k - \frac{1}{k}$$

で定義され、$k^{-L(0)}$や$z^{\left(\frac{1}{k}-1\right)L(0)}$は$u \in V_{\frac{1}{2}n}$に対して

$$k^{-L(0)}u = k^{-\frac{1}{2}n}u \ , \ z^{\left(\frac{1}{k}-1\right)L(0)}u = z^{\frac{(1-k)n}{2k}}u$$

で定義し線形に拡張する。この$\Delta_k(z)$を使って、$u \in V$に対して$\bar{Y}^W(u,z)$を

$$\bar{Y}^W(u,z) = Y^W(\Delta_k(z)u, z^{\frac{1}{k}})$$

と定義し、u^jに対してY_gを

$$Y_g(u^j, z) = \bar{Y}(u, \epsilon_k^{-j+1}z) = \lim_{z^{\frac{1}{2k}} \to \epsilon_{2k}^{-j+1} z^{\frac{1}{2k}}} \bar{Y}(u,z)$$

のように定義する。ただし、$\epsilon_{2k} = e^{-\frac{\pi i}{k}}$ とする。

例えば、Virasoro 元 $\hat{\omega}$ について、$Y_g(\hat{\omega},z)=\sum_{n\in\mathbb{Z}}\hat{L}_g(n)z^{-n-2}$ とすると

$$\hat{L}_g(n)=\frac{L(kn)}{k}\ (n\neq 0)\ ,\ \hat{L}_g(0)=\frac{L(0)}{k}-\frac{(k^2-1)c}{24k}$$

となっていることがわかる。この Y_g について次が成り立つことがわかる。

補題 1. $u\in V, j=1,\cdots,k$ に対して、

$$\left[\hat{L}_g(-1),Y_g(u^j,z)\right]=\frac{d}{dz}Y_g(u^j,z)=Y_g((L(-1)u)^j,z)$$

が成り立つ。

補題 2. $\mathbb{Z}_2$-*homogeneous* な $u,v\in V$ と $i,j=1,\cdots,k$ に対して、$Y_g(u^i,z_1)$ と $Y_g(v^j,z_2)$ は局所可換、即ち、ある正整数 N があって

$$(z_1-z_2)^NY_g(u^i,z_1)Y_g(v^j,z_2)=(-1)^{\tilde{u}\tilde{v}}(z_1-z_2)^NY_g(v^j,z_2)Y_g(u^i,z_1)\qquad(1)$$

が成り立つ。

これは $\langle Y_g(u^i,z_1)|u\in V_0\cup V_1,i=1,\cdots,k\rangle$ はどの 2 元も局所可換な $\mathbb{Z}_2$-次数付き空間になることを示している。$(End\,W)[[z^{\frac{1}{2k}},z^{-\frac{1}{2k}}]]$ においてこのような局所可換な $\mathbb{Z}_2$-次数付き空間のうち極大な空間を ($\mathbb{Z}_{2k}$-twisted) local system という。[L] $A=A_{\bar{0}}\oplus A_{\bar{1}}$ を上の空間を含む local system とする。$a(z)\in A$ に対して、$\rho a(z)=\lim_{z^{\frac{1}{2k}}\to\epsilon_{2k}^{-j}z^{\frac{1}{2k}}}a(z)$ とすれば、ρ は $\rho^{2k}=1$ である A の自己同型になる。A 上に頂点作用素 Y_A を次のように定義する。

定義 4. $\rho a(z)=e^{-\frac{\pi ir}{k}}a(z)$ である $\mathbb{Z}_2$-*homogeneous* な $a(z),b(z)\in A$ に対して、

$$\sum_{n\in\mathbb{Z}}(a(z)_nb(z))\,z_0^{-n-1}=\mathrm{Res}_{z_1}\left(\frac{z_1-z_0}{z}\right)^{\frac{r}{2k}}\cdot X\qquad(2)$$

により n-正規積 $a(z)_nb(z),n\in\mathbb{Z}$, を定義する。ここで、

$$X=z_0^{-1}\delta\left(\frac{z_1-z}{z_0}\right)a(z_1)b(z)-(-1)^{st}z_0^{-1}\delta\left(\frac{z-z_1}{-z_0}\right)b(z)a(z_1).$$

である。上の *(2)* を $Y_A(a(z),z_0)b(z)$ とおく。

このとき、次が成り立つ。

定理 4. *[L]* $(A,Y_A,I(z_0)=Id_W,D=\frac{d}{dz_0})$ は頂点超代数になり、$Y_W(a(z),z_0)=a(z_0)$ とすれば、(W,Y_W) は ρ-ツイスト A-加群になる。

一方、SVOA の加群と local system に関して次のようなことが成り立つ。

定理 5. *[L] V は SVOA* であるとし、h は位数 T の V の自己同型とする。このとき、h-ツイスト V-加群を与えることと、V からある $\mathbb{Z}_T$-*twisted local system* への頂点超代数準同型を与えることは同値である。

この定理を適用するために、次のような写像を定義する。

定義 5. 写像 $f : V_{\mathbb{Z}_2^k} \to A$ を

$$\begin{aligned} f : V_{\mathbb{Z}_2^k} &\to A \\ u_1 \otimes \cdots \otimes u_k \otimes e^\alpha = (u_1^1)_{-1} \cdots (u_{k-1}^{k-1})_{-1} u_k^k &\mapsto Y_g(u_1^1, z)_{-1} \cdots Y_g(u_{k-1}^{k-1}, z)_{-1} Y_g(u_k^k, z) \end{aligned}$$

で定義する。このとき、$f(u^i) = Y_g(u^i, z)$ である。

このとき、次が成り立つ。

補題 3. f は頂点超代数の準同型である。

この f により、すべての $v \in V_{\mathbb{Z}_2^k}$ に対して、$Y_g(v, z) = f(v)$ が定義され、上の定理から次が成り立つ。

定理 6. (W, Y^W) が σ^l-ツイスト V-加群のとき、(W, Y_g) は $\sigma_1^{l+k-1} g$-ツイスト $V_{\mathbb{Z}_2^k}$-加群である。さらに、(W, Y^W) が既約であれば、(W, Y_g) も既約である。

最後に SVOA $M = L(\frac{1}{2}, 0) \oplus L(\frac{1}{2}, \frac{1}{2})$ に対して、上の定理を適用する。M は、M を既約加群としてもち、$L(\frac{1}{2}, \frac{1}{16})$ を既約 σ-ツイスト加群として持つ。したがって、次が成り立つ。

定理 7. (M, Y_g) は既約 $\sigma_1^{k-1} g$-ツイスト $M_{\mathbb{Z}_2^k}$-加群になり、$(L(\frac{1}{2}, \frac{1}{16}), Y_g)$ は既約 $\sigma_1^k g$-ツイスト $M_{\mathbb{Z}_2^k}$-加群になる。

また、D が g-不変な偶 code のとき、code VOA $M_D \subset M_{\mathbb{Z}_2^k}$ に対して σ_1 と g を M_D の自己同型と見て、Y_g を M_D に制限すれば、次が成り立つ。

定理 8. $(L(\frac{1}{2}, 0), Y_g)$ と $(L(\frac{1}{2}, \frac{1}{2}), Y_g)$ は既約 $\sigma_1^{k-1} g$-ツイスト M_D-加群になり、$(L(\frac{1}{2}, \frac{1}{16}), Y_g)$ は既約 $\sigma_1^k g$-ツイスト M_D-加群になる。

参考文献

[BDM] K.Barron, C.Dong and G.Mason, Twisted sectors for tensor product VOAs associated to permutaion groups, math. QA/9803118.

[B] R.E.Borcherds, Vertex algebras, Kac-Moody algebras and the Monster, Proc. Natl. Acad. Sci. USA **83** (1986), 3068-3071.

[DGH] C.Dong, R.J.Griess Jr. and G.Hoeha, Framed vertex operator algebras, codes and the moonshine module, Comm. Math. Phys. **193** (1998), 407-448.

[DLM] C.Dong, H.Li and G.Mason, Modular invariance of trace functions in orbifold theory, q-alg/9703016.

[DMZ] C.Dong, G.Mason and Y.Zhu, Discrete series of the Virasoro algebra and the moonshine module, Proc. Symp. Pure. Math. American Math. Soc. **56** no.2 (1994), 295-316.

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

[L] H.Li, Local systems of twisted vertex operators, vertex superalgebras and twisted modules, Contemporary Math. **193** (1996), 203-236.

[M1] M.Miyamoto, Binary codes and vertex operator (super)algebras, J. Algebra **181** (1996), 207-222.

[M2] M.Miyamoto, Representations of code vertex operator algebras, J. Algebra **201** (1998), 115-150.

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

Fusion rules for the vertex operator algebra V_L^+ for a rank one even lattice L

安部　利之

大阪大学大学院理学研究科
e-mail: sm3002at@ecs.cmc.osaka-u.ac.jp

1　序

正定値偶格子 L に付随する頂点作用素代数 V_L は, L の -1-isometry を拡張して得られる位数 2 の自己同型写像を持つ. その自己同型写像による V_L の固定点全体 V_L^+ は, V_L の部分頂点作用素代数となっている. 本稿では, 既約な V_L^+-加群の間の fusion rule を完全に決定したので, そのことについて報告する.

V_L^+ に関する fusion rule の決定には, [A1] で決定された V_L^+ に部分頂点作用素代数として含まれる自由ボゾン頂点作用素代数 $M(1)^+$ の fusion rule が中心的な役割を果たしている.

1.1　準備

この節では頂点作用素代数 (以下, VOA) $(V, Y, \mathbf{1}, \omega)$ に対し, V-加群の間の intertwining 作用素, 及び fusion rule の定義, 及び関連する結果について述べる (定義については [FLM], [FHL] を参照). VOA 及び, その (twisted) 加群の定義については, [FLM], [FHL], [DLM] などを参照して下さい.

定義 1.1 V を VOA, (M^i, Y_{M^i}) $(i = 1, 2, 3)$ を V-加群とする. V に関する $\binom{M^3}{M^1\ M^2}$ **型の intertwining 作用素** とは線形写像

$$\begin{aligned} \mathcal{Y} : M^1 &\to (\mathrm{Hom}(M^2, M^3))\{z\}, \\ v &\mapsto \mathcal{Y}(v,z) = \sum_{n \in \mathbb{C}} v_n z^n \ (v_n \in \mathrm{Hom}(M^2, M^3)) \end{aligned}$$

で $a \in V, v \in M^1$ 及び $u \in M^2$ に対し次の公理を満たすものである:
(1) 固定した $k \in \mathbb{C}$ に対し n が十分大きな整数ならば, $v_{n+k}u = 0$ となる.

(2) (Jacobi 恒等式)

$$z_0^{-1}\delta\left(\frac{z_1-z_2}{z_0}\right)Y_{M^3}(a,z_1)\mathcal{Y}(v,z_2)-z_0^{-1}\delta\left(\frac{z_2-z_1}{-z_0}\right)\mathcal{Y}(v,z_2)Y_{M^3}(a,z_1)$$
$$=z_2^{-1}\delta\left(\frac{z_1-z_0}{z_2}\right)\mathcal{Y}(Y_{M^1}(a,z_0)v,z_2). \tag{1.1}$$

(3) ($L(-1)$-微分性)

$$\frac{d}{dz}\mathcal{Y}(v,z)=\mathcal{Y}(L(-1)v,z), \tag{1.2}$$

ここで, $Y_{M^1}(\omega,z)=\sum_{n\in\mathbb{Z}}L(n)z^{-n-2}$ である.

全ての $\binom{M^3}{M^1\ M^2}$ 型の intertwining 作用素からなるベクトル空間を $I_V\binom{M^3}{M^1\ M^2}$ と書く. そのベクトル空間 $I_V\binom{M^3}{M^1\ M^2}$ の次元を対応する型の **fusion rule** といい, $N_{M^1M^2}^{M^3}$ と書く.

V を VOA, M を V-加群とする. この時 M は, $L(0)$ の作用によって, $M=\oplus_{\lambda\in\mathbb{C}}M(\lambda)$ と固有空間分解されている. ここで, $M(\lambda)$ は $L(0)$ に関する固有値 λ の固有空間である. この時 M の制限双対 $M'=\oplus_{\lambda\in\mathbb{C}}M(\lambda)^*$ もまた V-加群の構造を持ち, $a\in V$ に対する頂点作用素 $Y_M^*(a,z)$ は,

$$u'\in M',\ v\in M \text{ に対し, } \langle Y_M^*(a,z)u',v\rangle=\langle u',Y_M(e^{zL(1)}(-z^{-2})^{L(0)}a,z^{-1})v\rangle$$

で定義される. この V-加群 (M',Y_M^*) は M の 反傾加群 と呼ばれる ([FHL] 及び [HL] 参照).

fusion rule は次の対称性を持つ事が知られている ([FHL], [HL] 参照).

命題 1.2 M^i $(i=1,2,3)$ を V-加群とする. この時, 自然な同型

$$I_V\binom{M^3}{M^1\ M^2}\cong I_V\binom{M^3}{M^2\ M^1} \text{ 及び } I_V\binom{M^3}{M^1\ M^2}\cong I_V\binom{(M^2)'}{M^1\ (M^3)'}$$

が存在する.

次の補題とその次の系は, V_L^+ に関する fusion rule を決定する際, 鍵となる補題である.

補題 1.3 ([DL] Proposition 11.9) V を VOA とし, M^1 と M^2 は既約 V-加群で M^3 は (既約とは限らない) V-加群とする. もし $\mathcal{Y}$ が $\binom{M^3}{M^1\ M^2}$ 型の 0 でない intertwining 作用素ならば, 任意の 0 でない元 $u\in M^1$, $v\in M^2$ に対して, $\mathcal{Y}(u,z)v$ は 0 ではない.

系 1.4 V 及び M^i $(i=1,2,3)$ を補題 1.3 のものとし, U を同じ Virasoro 元を持つ V の部分頂点作用素代数, N^i を M^i $(i=1,2)$ の U-部分加群とする. この時, 制限写像

$$I_V\binom{M^3}{M^1\ M^2}\to I_U\binom{M^3}{N^1\ N^2},\ \mathcal{Y}\mapsto\mathcal{Y}|_{N^1\otimes N^2}$$

は単射である. 特に不等式,

$$\dim I_V\left({}_{M^1}{}^{M^3}{}_{M^2} \right) \leq \dim I_U\left({}_{N^1}{}^{M^3}{}_{N^2} \right)$$

が成り立つ.

V, M^i $(i=1,2,3)$, U 及び N^i $(i=1,2)$ を系 1.4 のものとする. 今 M^3 は $M^3 = \oplus_{i\in I} L^i$ の様に, U-部分加群の直和に分解していると仮定する. この時, 同型

$$I_U\left({}_{N^1}{}^{\oplus_{i\in I} L^i}{}_{N^2} \right) \cong \oplus_{i\in I} I_U\left({}_{N^1}{}^{L^i}{}_{N^2} \right)$$

を得る. 従って系 1.4 より, 不等式

$$\dim I_V\left({}_{M^1}{}^{M^3}{}_{M^2} \right) \leq \sum_{i\in I} \dim I_U\left({}_{N^1}{}^{L^i}{}_{N^2} \right) \tag{1.3}$$

が成り立つ.

1.2 VOA V_L^+ とその既約加群

L を階数 1 の偶格子とし, $\langle \cdot, \cdot \rangle$ をその非退化正定値 $\mathbb{Z}$-双線形形式とする. $\mathfrak{h} = \mathbb{C}\otimes_{\mathbb{Z}} L$ と置き, $\langle \cdot, \cdot \rangle$ を $\mathfrak{h}$ の $\mathbb{C}$-双線形形式に拡張する. $\mathbb{C}[\mathfrak{h}] = \oplus_{\lambda\in\mathfrak{h}} \mathbb{C}e_\lambda$ を $\mathfrak{h}$ の 群環とする. また $\mathfrak{h}$ の部分集合 M に対し, $\mathbb{C}[M] = \oplus_{\lambda\in M} \mathbb{C}e_\lambda$ と置く.

$\hat{\mathfrak{h}} = \mathfrak{h}\otimes \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}K$ を交換関係

$$[X\otimes t^m, X'\otimes t^n] = m\,\delta_{m+n,0}\,\langle X, X'\rangle\, K, [K, \hat{\mathfrak{h}}] = 0 \ (X, X' \in \mathfrak{h}, m, n \in \mathbb{Z})$$

で定義される Lie 代数とする. この時, $\hat{\mathfrak{h}}^+ = \mathfrak{h}\otimes\mathbb{C}[t]\oplus\mathbb{C}K$ は $\hat{\mathfrak{h}}$ の可環部分代数で, 群環 $\mathbb{C}[\mathfrak{h}]$ は $\hat{\mathfrak{h}}^+$ の作用を, $\rho(X\otimes t^n)e_\lambda = \delta_{n,0}\langle X, \lambda\rangle e_\lambda$, $\rho(K)e_\lambda = e_\lambda$ $(\lambda, X\in\mathfrak{h}, n\in\mathbb{N})$ と定義することによって $\hat{\mathfrak{h}}$-加群となる. 明らかに $\mathfrak{h}$ の部分集合 M に対し, $\mathbb{C}[M]$ は $\mathbb{C}[\mathfrak{h}]$ の $\hat{\mathfrak{h}}^+$-部分加群となる. この時, V_M を誘導 $\hat{\mathfrak{h}}$-加群

$$V_M = U(\hat{\mathfrak{h}})\otimes_{U(\hat{\mathfrak{h}}^+)} \mathbb{C}[M] \cong S(\mathfrak{h}\otimes t^{-1}\mathbb{C}[t^{-1}])\otimes\mathbb{C}[M] \text{ (線形)},$$

とする. ここで $U(\hat{\mathfrak{h}})$ は $\hat{\mathfrak{h}}$ の普遍包絡代数を表す. $X\otimes t^n$ $(X\in\mathfrak{h}, n\in\mathbb{Z})$ の $V_{\mathfrak{h}}$ 上の作用を $X(n)$ と書き, 形式的変数 z の形式的巾級数として $X(z) = \sum_{n\in\mathbb{Z}} X(n)z^{-n-1}$ と書く. $\lambda\in\mathfrak{h}$ に対し e_λ に付随する頂点作用素は

$$\mathcal{Y}^\circ(e_\lambda, z) = \exp\left(\sum_{n=1}^{\infty} \frac{\lambda(-n)}{n} z^n\right) \exp\left(-\sum_{n=1}^{\infty} \frac{\lambda(n)}{n} z^{-n}\right) e_\lambda z^{\lambda(0)} \tag{1.4}$$

と定義される, ここで右辺の e_λ は $e_\lambda \in \mathbb{C}[\mathfrak{h}]$ の $\mathbb{C}[\mathfrak{h}]$ での右乗法を表し, $z^{\lambda(0)}$ は $u \in S(\mathfrak{h}\otimes t^{-1}\mathbb{C}[t^{-1}])\otimes e_\mu$ に対し $z^{\lambda(0)}u = z^{(\lambda,\mu)}u$ で定義される $V_\mathfrak{h}$ 上の作用素である. 一般の元 $v = X_1(-n_1)\cdots X_m(-n_m)\,e_\lambda \in V_\mathfrak{h}$ $(X_i \in \mathfrak{h},\, n_i \in \mathbb{Z}_{>0})$ に付随する頂点作用素は

$$\mathcal{Y}^\circ(v,z) = {:}\partial^{(n_1-1)}X_1(z)\cdots\partial^{(n_m-1)}X_m(z)\mathcal{Y}^\circ(e_\lambda,z){:} \tag{1.5}$$

で定義される, ここで $\partial^{(n)} = (\frac{1}{n!})(d/dz)^n$ で, 正規順序 ${:}\cdot{:}$ は $X(n)$ $(X\in\mathfrak{h}, n<0)$ 及び e_λ が $X(n)$ $(X\in\mathfrak{h}, n\geq 0)$ 及び $z^{\lambda(0)}$ の右側にくる様に並び替える操作を表す. $\mathcal{Y}^\circ$ を $V_\mathfrak{h}$ 上に線形に拡張する. a が V_L の元の時には, $Y(a,z) = \mathcal{Y}^\circ(a,z)$ と書くことにする.

$L = \mathbb{Z}\alpha$ と置き $\langle\alpha,\alpha\rangle = 2k$ $(k\in\mathbb{Z}_{>0})$ とする. また L° を L の双対格子とする. h を $\mathfrak{h}$ の正規直交基底とし, $1 = 1\otimes e_0$, $\omega = (1/2)\,h(-1)^2e_0$ と置く. この時, $(V_L, Y, 1, \omega)$ は単純 VOA となり, $\lambda\in L^\circ$ に対し, $(V_{\lambda+L}, Y)$ は既約な V_L-加群となる. また, $M(1) = S(\mathfrak{h}\otimes t^{-1}\mathbb{C}[t^{-1}])\otimes e_0 \subset V_L$ と置くと, $(M(1), Y, 1, \omega)$ は単純な V_L の部分 VOA となっている. 各 $\lambda\in\mathfrak{h}$ に対し, $M(1,\lambda) = U(\hat{\mathfrak{h}})\otimes_{U(\hat{\mathfrak{h}}^+)}\mathbb{C}e_\lambda$ と置くと, $(M(1,\lambda), Y)$ は既約な $M(1)$-加群となる.

θ を $X_i\in\mathfrak{h}, n\in\mathbb{Z}_{>0}, \lambda\in\mathfrak{h}$ に対し

$$\theta(X_1(-n_1)X_2(-n_2)\cdots X_\ell(-n_\ell)\otimes e_\lambda) = (-1)^\ell X_1(-n_1)X_2(-n_2)\cdots X_\ell(-n_\ell)\otimes e_{-\lambda}$$

で定義される $V_\mathfrak{h}$ の線形同型写像とすると, θ は VOA V_L, $M(1)$ の自己同型を与えている. ここで $V_\mathfrak{h}$ の θ-不変な部分空間 W に対し, θ に関する ±1-固有空間を $W^\pm$ と表すことにする. この時, $(V_L^+, Y, 1, \omega)$ 及び $(M(1)^+, Y, 1, \omega)$ は VOA となる. 更に $M(1)^\pm$, $M(1,\lambda)$ $(\lambda\neq 0)$ は既約な $M(1)^+$-加群となっている ([DN1] 参照). V_L^+-加群に関しては, $V_L^\pm$, $V_{\alpha/2+L}^\pm$, $V_{r\alpha/2k+L}$ $(1\leq r\leq k-1)$ が既約加群となっている ([DN2]) 参照).

次に θ-twisted V_L-加群の構成について説明する. $\hat{\mathfrak{h}}[-1] = \mathfrak{h}\otimes t^{1/2}\mathbb{C}[t,t^{-1}]\oplus\mathbb{C}K$ を交換関係

$$[X\otimes t^m, X'\otimes t^n] = m\,\delta_{m+n,0}\,\langle X, X'\rangle\,K, [K, \hat{\mathfrak{h}}[-1]] = 0\ (X, X'\in\mathfrak{h}, m, n\in 1/2+\mathbb{Z})$$

で定義されている Lie 代数とし, $\hat{\mathfrak{h}}[-1]^+ = \mathfrak{h}\otimes t^{1/2}\,\mathbb{C}[t]\oplus\mathbb{C}K$ をその可換部分代数とする. この時, $\mathbb{C}$ は $\hat{\mathfrak{h}}[-1]^+$ の作用を $\rho(X\otimes t^n)1 = 0$, $\rho(K)\,1 = 1$ $(X\in\mathfrak{h}, n\in 1/2+\mathbb{N})$ で定義することによって, $\hat{\mathfrak{h}}[-1]^+$-加群となっている. $M(1)(\theta)$ を誘導 $\hat{\mathfrak{h}}[-1]^+$-加群

$$M(1)(\theta) = U(\hat{\mathfrak{h}}[-1])\otimes_{U(\hat{\mathfrak{h}}[-1]^+)}\mathbb{C}\cong S\left(\mathfrak{h}\otimes t^{-\frac{1}{2}}\mathbb{C}[t^{-1}]\right)\ \text{(線形)}.$$

とする. $X\otimes t^n$ $(X\in\mathfrak{h}, n\in 1/2+\mathbb{Z})$ の $M(1)(\theta)$ 上の作用を $X(n)$ と書き, $X(z) = \sum_{n\in 1/2+\mathbb{Z}}X(n)\,z^{-n-1}$ とする. この時 $\lambda\in L^\circ$ に対し, e_λ に付随する twisted 頂点作用素は

$$\mathcal{Y}^\theta(e_\lambda,z) = 2^{-\langle\lambda,\lambda\rangle}z^{-\frac{\langle\lambda,\lambda\rangle}{2}}\exp\left(\sum_{n\in 1/2+\mathbb{N}}\frac{\lambda(-n)}{n}z^n\right)\exp\left(-\sum_{n\in 1/2+\mathbb{N}}\frac{\lambda(n)}{n}z^{-n}\right) \tag{1.6}$$

で定義される. $v = X_1(-n_1)\cdots X_\ell(-n_\ell)e_\lambda \in V_{L^\circ}$ $(X_i \in \mathfrak{h}, n_i \in \mathbb{Z}_+)$ に対して,

$$W^\theta(v,z) = :\partial^{(n_1-1)}X_1(z)\cdots\partial^{(n_\ell-1)}X_\ell(z)\mathcal{Y}^\theta(v_\lambda,z): \tag{1.7}$$

と置き, V_{L° 上に線形に拡張する, ここで正規順序 $:\cdot:$ は $X(n)$ $(X \in \mathfrak{h}, n < 0)$ が $X(n)$ $(X \in \mathfrak{h}, n > 0)$ 右側になるように並び替える操作を表す. 今定数 $c_{mn} \in \mathbb{Q}$ を形式的巾級数展開

$$\sum_{m,n\geq 0} c_{mn}x^m y^n = -\log\left(\frac{(1+x)^{\frac{1}{2}} + (1+y)^{\frac{1}{2}}}{2}\right)$$

で定義し, $\Delta_z = \sum_{m,n\geq 0} c_{mn}h(m)h(n)z^{-m-n}$ と置く. この時一般の元 $u \in V_{L^\circ}$ に付随する twisted 頂点作用素は

$$\mathcal{Y}^\theta(u,z) = W^\theta(e^{\Delta_z}u,z) \tag{1.8}$$

で定義される. この時 $a \in M(1)$ の時 $Y^\theta(a,z) = \mathcal{Y}^\theta(a,z)$ と書くことにすると, 組 $(M(1)(\theta), Y^\theta)$ は既約な θ-twisted $M(1)$-加群となる.

T_1 と T_2 を e_α がそれぞれ $1, -1$ と作用する既約な $\mathbb{C}[L]$-加群とし, $V_L^{T_i} = M(1)(\theta)\otimes_{\mathbb{C}} T_i$ と置く. $u \in M(1,\beta)$ $(\beta \in L)$ に付随する $V_L^{T_i}$ 上の twisted 頂点作用素は $Y^\theta(u,z) = \mathcal{Y}^\theta(u,z)\otimes e_\beta$ で定義される. Y^θ の定義を V_L 上に線形に拡張する. この時, $(V_L^{T_i}, Y^\theta)$ $(i = 1,2)$ は既約な θ-twisted V_L-加群となる.

θ は $M(1)(\theta)$ 上

$$\theta(X_1(-n_1)\cdots X_m(-n_m)1) = (-1)^m X_1(-n_1)\cdots X_m(-n_m)1 \ (X_i \in \mathfrak{h}, n_i \in 1/2+\mathbb{N})$$

と作用している. その作用に関する $M(1)(\theta)$ の ± 1-固有空間を $M(1)(\theta)^\pm$ とし, $V_L^{T_i,\pm} = M(1)(\theta)^\pm \otimes T_i$ と置く. この時 $M(1)(\theta)^\pm$ 及び $V_L^{T_i,\pm}$ $(i = 1,2)$ はそれぞれ $M(1)^+$ と V_L^+ の既約加群となる ([DN1], [DN2] 参照).

[DN1] において $M(1)^+$ に既約加群が, [DN2] において V_L^+ の既約加群が次のようにそれぞれ分類されている.

定理 1.5 (1) ([DN1])

$$\{M(1)^\pm, M(1)(\theta)^\pm, M(1,\lambda)(\cong M(1,-\lambda)) \,|\, \lambda \in \mathfrak{h} - \{0\}\} \tag{1.9}$$

が非同値な全ての既約な $M(1)^+$-加群を与える.

(2) ([DN2])

$$\{V_L^\pm, V_{\alpha/2+L}^\pm, V_L^{T_i,\pm}, V_{r\alpha/2k+L} \,|\, i = 1,2, 1 \leq r \leq k-1\} \tag{1.10}$$

が非同値な全ての既約な V_L^+-加群を与える.

$V_L^\pm$, $V_{\alpha/2+L}^\pm$ と $V_{r\alpha/2k+L}$ を **非 twisted 型加群**, $V_L^{T_i,\pm}$ $(i = 1,2)$ を **twisted 型加群**と呼ぶことにする. 以下 $r \in \mathbb{Z}$ に対し, $\lambda_r = r\alpha/2k$ と置く.

2 既約 V_L^+-加群の反傾加群と $M(1)^+$-加群への既約分解

VOA の既約加群の反傾加群は, 既約である. V_L^+ に関しては, 次の対応がある.

命題 2.1 (i) k が偶数ならば, 全ての既約 V_L^+-加群 W は自己双対, すなわち V_L^+-加群として $W \cong W'$ である.
(ii) k が奇数ならば, V_L^+-加群として

$$(V_{\alpha/2+L}^{\pm})' \cong V_{\alpha/2+L}^{\mp}, (V_L^{T_1,\pm})' \cong V_L^{T_2,\pm}, (V_L^{T_2,\pm})' \cong V_L^{T_1,\pm}$$

でその他の既約加群は自己双対である.

証明には, Zhu の $A(V)$-理論 ([Z] 参照) を用いるが, 余り本質的でないと思われるので省略する. 詳しくは [A2] を参照して下さい.

次に, 既約 V_L^+-加群の既約 $M(1)^+$-加群への直和分解について述べる. 今, 零でない $\lambda \in \mathfrak{h}$ に対し, $M(1,\lambda) \oplus M(1,-\lambda)$ の部分空間 $(M(1)^+ \otimes (e_\lambda \pm e_{-\lambda})) \oplus (M(1)^- \otimes (e_\lambda \mp e_{-\lambda}))$ を考える. それぞれ θ の作用に関する ± 1 固有空間である. $M(1)^+$ の $M(1,\lambda) \oplus M(1,-\lambda)$ への作用は θ の作用と可換なので, 部分空間 $(M(1)^+ \otimes (e_\lambda \pm e_{-\lambda})) \oplus (M(1)^- \otimes (e_\lambda \mp e_{-\lambda}))$ は $M(1)^+$-部分加群である. 実際には次の補題が成り立つ.

補題 2.2 零でない $\lambda \in \mathfrak{h}$ に対し, $(M(1)^+ \otimes (e_\lambda \pm e_{-\lambda})) \oplus (M(1)^- \otimes (e_\lambda \mp e_{-\lambda}))$ は $M(1,\lambda)$ に $M(1)^+$-加群として同型である.

証明. 写像 ϕ_λ を, $u \in M(1)^+$, $v \in M(1)^-$ に対して,

$$\begin{aligned} \phi_\lambda : (M(1)^+ \otimes (e_\lambda + e_{-\lambda})) \oplus (M(1)^- \otimes (e_\lambda - e_{-\lambda})) &\to M(1,\lambda) \\ u \otimes (e_\lambda + e_{-\lambda}) + v \otimes (e_\lambda - e_{-\lambda}) &\mapsto (u+v) \otimes e_\lambda \end{aligned} \tag{2.1}$$

で定義すると, ϕ_λ が同型写像を与えることがわかる. $M(1)^+ \otimes (e_\lambda - e_{-\lambda}) \oplus M(1)^- \otimes (e_\lambda + e_{-\lambda})$ に関しても同様. □

この補題を用いて, 既約な V_L^+-加群は $M(1)^+$-加群として直和であることがわかる;

命題 2.3 各既約 V_L^+-加群は次のように, 既約 $M(1)^+$-加群の直和に分解される:

$$V_L^{\pm} \cong M(1)^{\pm} \oplus \bigoplus_{m=1}^{\infty} M(1, m\alpha), \tag{2.2}$$

$$V_{\lambda_r+L} \cong \bigoplus_{m\in\mathbb{Z}} M(1, \lambda_r + m\alpha) \ (1 \le r \le k-1), \tag{2.3}$$

$$V_{\alpha/2+L}^{\pm} \cong \bigoplus_{m=0}^{\infty} M(1, \alpha/2 + m\alpha), \tag{2.4}$$

$$V_L^{T_i,\pm} \cong M(1)(\theta)^{\pm} \ (i = 1, 2). \tag{2.5}$$

特に, 既約 $M(1)^+$-加群の既約 V_L^+-加群での重複度は高々 1 である.

証明.

定理 1.5 (1) より $\mu \in L^\circ$ が零でなければ, $M(1,\mu)$ は既約な $M(1)^+$-加群なので, V_{λ_r+L} $(1 \le r \le k-1)$ は $M(1)^+$-加群として

$$V_{\lambda_r+L} \cong \bigoplus_{m\in\mathbb{Z}} M(1,\lambda_r+m\alpha)$$

と既約分解されることがわかる.

また, $i=1,2$ に対して, t_i を T_i の基底とすると, 写像

$$\phi_i : M(1)(\theta) \to V_L^{T_i} : u \mapsto u \otimes t_i$$

は θ-twisted $M(1)$-加群としての同型写像である. θ の作用は, $M(1)^+$ の可換なので, 同型 (2.5) を得る.

$V_L^\pm$ 及び $V_{\alpha/2+L}^\pm$ は

$$\begin{aligned} V_L^\pm &= \bigoplus_{m=0}^{\infty}((M(1)^+ \otimes (e_{m\alpha} \pm e_{-m\alpha})) \oplus (M(1)^- \otimes (e_{m\alpha} \mp e_{-m\alpha}))), \\ V_{\alpha/2+L}^\pm &= \bigoplus_{m=0}^{\infty}((M(1)^+ \otimes (e_{\frac{\alpha}{2}+m\alpha} \pm e_{-\frac{\alpha}{2}-m\alpha})) \oplus (M(1)^- \otimes (e_{\frac{\alpha}{2}+m\alpha} \mp e_{-\frac{\alpha}{2}-m\alpha}))) \end{aligned}$$

と直和分解されている. よって補題 2.2 よりこの直和分解が $V_L^\pm$ と $V_{\alpha/2+L}^\pm$ の $M(1)^+$-加群としての既約分解を与えていることがわかる. 後半は既約分解と定理 1.5 (1) より明らかである. □

既約分解 (2.2)-(2.5), 系 1.4 及び, 補足で与えた定理 4.1 の $M(1)^+$ の既約加群の間の fusion rule を用いて, V_L^+ の fusion rule に関する次の命題を得る.

命題 2.4 W^1, W^2, W^3 を既約 V_L^+-加群とする. この時, 次が成り立つ.
(1) fusion rule $N_{W^1W^2}^{W^3}$ は 0 または 1 である.
(2) もし全ての W^i $(i=1,2,3)$ が twisted 型加群ならば, fusion rule $N_{W^1W^2}^{W^3}$ は 0 である.
(3) もし W^i $(i=1,2,3)$ のうち 1 つが twisted 型加群で他の 2 つが 非 twisted 型ならば, fusion rule $N_{W^1W^2}^{W^3}$ は 0 である.

証明のアイデア W^1, W^2 がそれぞれ $M(1)^+$-部分加群 M, N を持ち, W^3 は $W^3 = \oplus_{i\in I} M^i$ と既約 $M(1)^+$-加群の直和に分解されているとする. (1.3) より, 不等式

$$\dim I_{V_L^+}\binom{W^3}{W^1\ W^2} \le \sum_{i\in I} \dim I_{M(1)^+}\binom{M^i}{M\ N} \tag{2.6}$$

を得る. よって, 実際に (2.6) の右辺が 1 以下となるような既約 $M(1)^+$-加群 M, N を見つけることによって (1) が成り立つことを示すことができる. (2),(3) に関しては, (2.6) の右辺が 0 となるような既約 $M(1)^+$-加群 M, N をみつけることによって証明できる. □

例 1(命題 2.4 (2) の証明) 例えば, $W^i = V_L^{T_{k_i},\epsilon_i}$ $(i = 1,2,3, k_i \in \{1,2\}, \epsilon_i \in \{\pm\})$ とする. この時命題 2.3 より, $M(1)^+$-加群として $W^i \cong M(1)(\theta)^{\epsilon_i}$ である. したがって定理 4.1 と不等式 (2.6) より,

$$\dim I_{V_L^+}\binom{W^3}{W^1\ W^2} \leq \dim I_{M(1)^+}\binom{M(1)(\theta)^{\epsilon_3}}{M(1)(\theta)^{\epsilon_1}\ M(1)(\theta)^{\epsilon_2}} = 0$$

を得る.

例 2 (講演の時の例) $W^1 = W^2 = W^3 = V_L^-$ とする. この時 V_L^- は, 既約 $M(1)^-$-加群 $M(1)^-$ を含んでいて, 命題 2.3 より, $M(1)^+$-加群として,

$$V_L^- \cong M(1)^- \oplus \bigoplus_{m=1}^{\infty} M(1, m\alpha)$$

と既約分解される. したがって定理 4.1 と不等式 (2.6) より,

$$\begin{aligned}\dim I_{V_L^+}\binom{W^3}{W^1\ W^2} &\leq \dim I_{M(1)^+}\binom{M(1)^-}{M(1)^-\ M(1)^-} + \sum_{m=1}^{\infty} \dim I_{M(1)^+}\binom{M(1,m\alpha)}{M(1)^-\ M(1)^-} \\ &= 0\end{aligned}$$

を得る.

3 既約 V_L^+-加群の間の fusion rule

前節で, 既約な V_L^+-加群の間の fusion rule が高々 1 であることを述べた. この節では, fusion rule が 1 になるような既約 V_L^+-加群の組を, 具体的に intertwining 作用素を構成することによって与える. また, それら以外の既約 V_L^+-加群の組に対して, 対応する fusion rule が 0 になることも示す. 節 3.1 では, 全ての既約な V_L^+-加群が非 twisted 型の組について, 節 3.2 では, ある既約 V_L^+-加群が twisted 型であるような組について議論する.

3.1 非 twisted 型既約 V_L^+-加群の間 の fusion rule

[FLM] の第 8 章で示されたように, (1.4), (1.5) で与えられる作用素 $\mathcal{Y}^\circ$ は, $\beta \in L$, $\lambda \in L^\circ, a \in M(1,\beta)$ 及び $u \in M(1,\lambda)$ に対し, 次の Jacobi 恒等式と $L(-1)$-微分性を満たしている:

$$\begin{aligned}&z_0^{-1}\delta\left(\frac{z_1 - z_2}{z_0}\right) Y(a,z_1)\mathcal{Y}^\circ(u,z_2) - (-1)^{(\beta,\lambda)} z_0^{-1}\delta\left(\frac{z_2 - z_1}{-z_0}\right)\mathcal{Y}^\circ(u,z_2)Y(a,z_1) \\ &= z_2^{-1}\delta\left(\frac{z_1 - z_0}{z_2}\right)\mathcal{Y}^\circ(Y(a,z_0)u,z_2),\end{aligned}$$

$$\frac{d}{dz}\mathcal{Y}^\circ(u,z) = \mathcal{Y}^\circ(L(-1)u,z).$$

今 π_λ $(\lambda \in L^\circ)$ を $\mu \in L^\circ, v \in M(1,\mu)$ に対し, $\pi_\lambda(v) = e^{(\lambda,\mu)\pi i} v$ で定義される V_{L° の線形自己準同型とし, $r,s \in \mathbb{Z}, u \in V_{\lambda_r+L}$ に対し $\mathcal{Y}_{r,s}(u,z) = \mathcal{Y}^\circ(u,z)\pi_{\lambda_r}|_{V_{\lambda_s+L}}$ と定義する. この時, $\mathcal{Y}_{r,s}$ が V_L に関する $\binom{V_{\lambda_r+\lambda_s+L}}{V_{\lambda_r+L}\ V_{\lambda_s+L}}$ 型の intertwining 作用素を与える. ([DL] 参照).

この V_L に関する intertwining 作用素と系 1.4 を用いて, 次の命題を得る.

命題 3.1 V_L^+ に関する次の型の fusion rule は零ではない ;

(i) $\binom{V_{(\lambda_r\pm\lambda_s)+L}}{V_{\lambda_r+L}\ V_{\lambda_s+L}}$ $(1 \le r,s \le k-1)$

(ii) $\binom{V_L^\pm}{V_L^+\ V_L^\pm}, \binom{V_L^\mp}{V_L^-\ V_L^\pm}$ 及び $\binom{V_{\lambda_r+L}}{V_L^\pm\ V_{\lambda_r+L}}$ $(0 \le r \le k-1,)$

(iii) $\binom{V^\pm_{\alpha/2+L}}{V_L^+\ V^\pm_{\alpha/2+L}}, \binom{V^\mp_{\alpha/2+L}}{V_L^-\ V^\pm_{\alpha/2+L}}$ 及び $\binom{V_{(\alpha/2-\lambda_r)+L}}{V^\pm_{\alpha/2+L}\ V_{\lambda_r+L}}$ $(0 \le r \le k-1)$.

次に, 非 twisted 型加群 W^i $(i=1,2,3)$ に対し, fusion rule $N_{W^1W^2}^{W^3}$ が零でなければ, その型 $\binom{W^3}{W^1\ W^2}$ は命題 1.2 を用いて, 命題 3.1 に挙げられている型のいずれかに一致することを示す. そのためには, つぎの命題を示せば十分である.

命題 3.2 W^1, W^2, W^3 を非 twisted 型加群とする. この時 W^i $(i=1,2,3)$ が次のいずれかの場合を満たすならば, fusion rule $N_{W^1W^2}^{W^3}$ は零である :

(i) $W^1 = V_L^+$ かつ W^2, W^3 は非同値.

(ii) $W^1 = V_L^-$ かつ組 (W^2,W^3) は次の組のいずれか:

$$\begin{aligned}(W^2,W^3) \;=\; & (V_L^-,V_L^-),\ (V^\pm_{\alpha/2+L},V^\pm_{\alpha/2+L}),\\ & (V_{\lambda_r+L},V_{\lambda_s+L})\ (1\le r,s\le k-1 \text{ かつ } \lambda_r\ne\lambda_s),\\ & (V_L^-,V_{\lambda_r+L}),\ (V^\pm_{\alpha/2+L},V_{\lambda_r+L})\ (1\le r\le k-1).\end{aligned}$$

(iii) $W^3 = V^\pm_{\alpha/2+L}$ かつ組 (W^2,W^3) は次の組のいずれか:

$$\begin{aligned}(W^2,W^3) \;=\; & (V_{\lambda_r+L},V_{\lambda_s+L})\ (1\le r,s\le k-1 \text{ かつ } \lambda_r+\lambda_s\ne\alpha/2),\\ & (V^\pm_{\alpha/2+L},V_{\lambda_r+L})\ (1\le r\le k-1).\end{aligned}$$

(iv) $W^1 = V_{\lambda_r+L}$ $(1 \le r \le k-1)$ かつ組 (W^2,W^3) は次の組のいずれか:

$$(W^2,W^3) = (V_{\lambda_s+L},V_{\lambda_t+L})\ (1\le s,t\le k-1 \text{ かつ } \lambda_t\ne\lambda_r\pm\lambda_s,\lambda_s-\lambda_r).$$

証明. $\mathcal{Y}$ を $\binom{W^3}{V_L^+\ W^2}$ 型の零でない intertwining 作用素とすると, $\mathcal{Y}(1,z)$ が W^2 から W^3 への V_L^+-加群としての同型写像を与えることがわかる. よって (i) の場合に命題が成り立つ.

組 $(V^{\pm}_{\alpha/2+L}, V^{\pm}_{\alpha/2+L})$ 以外の (ii) の場合と場合 (iii), (iv) について考える. この場合, まず W^3 を $W^3 = \oplus_i M^i$ と既約 $M(1)^+$-加群の直和に分解する. この時, W^1 の既約な $M(1)^+$-部分加群 M と W^2 の既約な $M(1)^+$-部分加群 N で, 任意の i について $\binom{M^i}{M\ N}$ 型の fusion rule が零となるようなものを見つけることができる; (例えば, 第 2 節の例 2). よって (2.6) より fusion rule $N^{W^3}_{W^1W^2}$ は零である.

最後に $(W^2, W^3) = (V^{\pm}_{\alpha/2+L}, V^{\pm}_{\alpha/2+L})$ の場合にしめす. $\binom{V^+_{\alpha/2+L}}{V^-_L\ V^+_{\alpha/2+L}}$ 型の fusion rule が零になることを示す. $\binom{V^-_{\alpha/2+L}}{V^-_L\ V^-_{\alpha/2+L}}$ がたの場合も同様に示すことができる.

$m \in \mathbb{N}$ に対し,

$$V^+_{\alpha/2+L}[0] \;=\; M(1)^+ \otimes (e_{\frac{\alpha}{2}} + e_{-(\frac{\alpha}{2})}) \oplus M(1)^- \otimes (e_{\frac{\alpha}{2}} - e_{-(\frac{\alpha}{2})}) \tag{3.1}$$

と置く. 補題 2.2 より, $V^+_{\alpha/2+L}[0]$ は $M(1,\alpha/2)$ に同型である. $\mathcal{Y}$ を $\binom{V^+_{\alpha/2+L}}{V^-_L\ V^+_{\alpha/2+L}}$ 型の intertwining 作用素とする. 定理 4.1 (ii) より, $u \in M(1)^-, v \in V^+_{\alpha/2+L}[0]$ に対し, $\mathcal{Y}(u,z)v \in V^+_{\alpha/2+L}[0]((z))$ を得る. $\phi_{\alpha/2} : V^+_{\alpha/2+L}[0] \to M(1,\alpha/2)$ を (2.1) で定義した $M(1)^+$-加群としての同型とする. 簡単のため $\phi = \phi_{\alpha/2}$ と書く. この時, $u \in M(1)^-, v \in M(1,\alpha/2)$ に対し, $(\phi\circ\mathcal{Y}\circ\phi^{-1})(u,z)v = \phi\mathcal{Y}(u,z)\phi^{-1}(v)$ で定義される作用素 $\phi\circ\mathcal{Y}\circ\phi^{-1}$ は $\binom{M(1,\alpha/2)}{M(1)^-\ M(1,\alpha/2)}$ 型の intertwining 作用素を与える. $I_{M(1)^+}\binom{M(1,\alpha/2)}{M(1)^-\ M(1,\alpha/2)}$ の次元は 1 なので対応する intertwining 作用素は $M(1)$-加群 $(M(1,\alpha/2), Y)$ の頂点作用素 Y の定数倍で与えられる. よってある定数 $d \in \mathbb{C}$ が存在して全ての $u \in M(1)^-, v \in V^+_{\alpha/2+L}[0]$ に対し,

$$\mathcal{Y}(u,z)v = d\,\phi^{-1}Y(u,z)\phi(v)$$

と書ける. 今, $u \in V^-_L$ に対し, $\mathcal{Y}(u,z) = \sum_{n\in\mathbb{Z}} \tilde{u}(n)z^{-n-1}$ $(\tilde{u}(n) \in \mathrm{End}\, V^+_{\alpha/2+L})$ と書く. $u = h(-1)\mathbf{1}, v = e_{\alpha/2} + e_{-\alpha/2}$ と取れば,

$$\tilde{h}(0)(e_{\frac{\alpha}{2}} + e_{-\frac{\alpha}{2}}) \;=\; d\langle h, \frac{\alpha}{2}\rangle(e_{\frac{\alpha}{2}} + e_{-\frac{\alpha}{2}}), \tag{3.2}$$

$$\tilde{h}(-1)(e_{\frac{\alpha}{2}} + e_{-\frac{\alpha}{2}}) \;=\; d(h(-1)e_{\frac{\alpha}{2}} - h(-1)e_{-\frac{\alpha}{2}}) \tag{3.3}$$

を得る. ここで $(h(\widetilde{-1})1)(n)$ を $\tilde{h}(n)$ と書いた. また直接に計算することによって,

$$E_{k-1}(e_{\frac{\alpha}{2}} + e_{-\frac{\alpha}{2}}) = (e_{\frac{\alpha}{2}} + e_{-\frac{\alpha}{2}}), \tag{3.4}$$

$$E_k(h(-1)e_{\frac{\alpha}{2}} - h(-1)e_{-\frac{\alpha}{2}}) = \langle h,\alpha\rangle(e_{\frac{\alpha}{2}} + e_{-\frac{\alpha}{2}}) \tag{3.5}$$

を得る. ここで $E = e_\alpha + e_{-\alpha} \in V^+_L$ である. $F = e_\alpha - e_{-\alpha} \in V^-_L$ と置と, Jacobi 恒等式より, $m,n \in \mathbb{Z}$ に対して交換関係

$$[E_m, \tilde{h}(n)] = -\langle h,\alpha\rangle\tilde{F}(m+n) \tag{3.6}$$

を得る. よって (3.2), (3.4) より $\tilde{F}(k-1)(e_{\alpha/2}+e_{-\alpha/2})=0$ ((3.6) で $m=k-1,n=0$ と取る). 一方 (3.3), (3.5) より,

$$-\langle h,\alpha\rangle\tilde{F}(k-1)(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}})=[E_k,\tilde{h}(-1)](e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}})=d\langle h,\alpha\rangle(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}})$$

((3.6) で $m=k,n=-1$ と取る). 従って $d=0$. よって, $\mathcal{Y}(h(-1)1,z)(e_{\alpha/2}+e_{-\alpha/2})=0$ であり, 補題 1.3 より $\mathcal{Y}=0$ を得る. 故に, $\binom{V^+_{\alpha/2+L}}{V^-_L\quad V^+_{\alpha/2+L}}$ 型の fusion rule は零である.□

従って, 命題 1.2, 命題 2.1, 命題 2.4, 命題 3.1 及び命題 3.2 より, 次の命題を得る.

命題 3.3 W^1,W^2,W^3 を非 twisted 型 V_L^+-加群とする. この時 fusion rule $N^{W^3}_{W^1W^2}$ は高々 1 である. fusion rule $N^{W^3}_{W^1W^2}$ が 1 となる必要十分条件は W^i $(i=1,2,3)$ が次の場合のいずれかを満たすことである :

(i) $W^1=V_L^+$ かつ $W^2\cong W^3$.

(ii) $W^1=V_L^-$ かつ組 (W^2,W^3) は次の組のいずれかである:

$$(V_L^{\pm},V_L^{\mp}),\ (V^{\pm}_{\alpha/2+L},V^{\mp}_{\alpha/2+L}),\ (V_{\lambda_r+L},V_{\lambda_r+L})\ (1\le r\le k-1).$$

(iii) $W^1=V^+_{\alpha/2+L}$ かつ組 (W^2,W^3) は次の組のいずれかである:

$$(V_L^{\pm},V^{\pm}_{\alpha/2+L}),\ ((V^{\pm}_{\alpha/2+L})',V_L^{\pm}),\ (V_{\lambda_r+L},V_{\alpha/2-\lambda_r+L})\ (1\le r\le k-1).$$

(iv) $W^1=V^-_{\alpha/2+L}$ かつ組 (W^2,W^3) は次の組のいずれかである:

$$(V_L^{\pm},V^{\mp}_{\alpha/2+L}),\ ((V^{\pm}_{\alpha/2+L})',V_L^{\mp}),\ (V_{\lambda_r+L},V_{\alpha/2-\lambda_r+L})\ (1\le r\le k-1).$$

(v) $W^1=V_{\lambda_r+L}$ $(1\le r\le k-1)$ かつ組 (W^2,W^3) は次の組のいずれかである:

$$(V_L^{\pm},V_{\lambda_r+L}),\ (V_{\lambda_r+L},V_L^{\pm}),\ (V^{\pm}_{\alpha/2+L},V_{\alpha/2-\lambda_r+L}),\ (V_{\alpha/2-\lambda_r+L},V^{\pm}_{\alpha/2+L}),$$
$$(V_{\lambda_s+L},V_{\lambda_r\pm\lambda_s+L})\ (1\le s\le k-1).$$

3.2 twisted 型加群を含む fusion rule

$\mathcal{P}_{\mathcal{L}}=L^\circ\times\{1,2\}\times\{1,2\}$ とおく. 元 $(\lambda,i,j)\in\mathcal{P}_{\mathcal{L}}$ が

$$(-1)^{\langle\lambda,\alpha\rangle+\delta_{i,j}+1}=1$$

を満たすとき, **quasi-admissible triple** と呼ぶことにする. 全ての quasi-admissible triples のなす集合を $\mathcal{Q}_{\mathcal{L}}$ と表す. まず quasi-admissible triple $(\lambda,i,j)\in\mathcal{Q}_{\mathcal{L}}$ に対し, $\binom{V_L^{T_j}}{V_{\lambda+L}\quad V_L^{T_i}}$ 型の V_L^+ に関する intertwining 作用素を構成する.

[FLM] の第 9 章で示されたように, (1.6)-(1.8) で与えられる作用素 $\mathcal{Y}^\theta$ は $\beta \in L, \lambda \in L^\circ, a \in M(1,\beta)$ 及び $u \in M(1,\lambda)$ に対し, 次の twisted Jacobi 恒等式

$$z_0^{-1}\delta\left(\frac{z_1-z_2}{z_0}\right)\mathcal{Y}^\theta(a,z_1)\mathcal{Y}^\theta(u,z_2) - (-1)^{\langle\beta,\lambda\rangle}z_0^{-1}\delta\left(\frac{z_2-z_1}{-z_0}\right)\mathcal{Y}^\theta(u,z_2)\mathcal{Y}^\theta(a,z_1)$$
$$= \frac{1}{2}\sum_{p=0,1} z_2^{-1}\delta\left((-1)^p\frac{(z_1-z_0)^{1/2}}{z_2^{1/2}}\right)\mathcal{Y}^\theta(Y(\theta^p(a),z_0)u,z_2), \tag{3.7}$$

と $L(-1)$-微分性

$$\frac{d}{dz}\mathcal{Y}^\theta(u,z) = \mathcal{Y}^\theta(L(-1)u,z) \tag{3.8}$$

を満たしている. この時, 次の補題が成り立つ.

補題 3.4 (1) 作用素 $\mathcal{Y}^\theta$ は, $\lambda \in L^\circ$ に対し, $\binom{M(1)(\theta)^\pm}{M(1,\lambda)\ M(1)(\theta)^\pm}$ 型, $\binom{M(1)(\theta)^\mp}{M(1,\lambda)\ M(1)(\theta)^\pm}$ 型の零でない $M(1)^+$ に関する intertwining 作用素を与える.
(2) 作用素 $\mathcal{Y}^\theta \circ \theta$ を $u \in V_{L^\circ}$ に対し $(\mathcal{Y}^\theta \circ \theta)(u,z) = \mathcal{Y}^\theta(\theta(u),z)$ で定義する. この時 $\mathcal{Y}^\theta \circ \theta$ は $M(1)^+$ に関する $\binom{M(1)(\theta)}{M(1,\lambda)\ M(1)(\theta)^\pm}$ 型の intertwining 作用素を与える. 更に $\mathcal{Y}^\theta$ 及び $\mathcal{Y}^\theta \circ \theta$ の $M(1,\lambda)\otimes M(1)(\theta)^\pm$ への制限はベクトル空間 $I\binom{M(1)(\theta)}{M(1,\lambda)\ M(1)(\theta)^\pm}$ の基底をなす.

証明は省略する.

$T = T^1 \oplus T^2$ と置き, 線形同型写像 $\psi \in \mathrm{End}\,T$ を $\psi(t_1) = t_2, \psi(t_2) = t_1$ で定義する, ここで t_i $(i = 1,2)$ は T^i の基底である. $\lambda \in L^\circ$ に対し, $\lambda = r\alpha/2k + m\alpha$ $(-k+1 \le r \le k, m \in \mathbb{Z})$ と表し, $\psi_\lambda \in \mathrm{End}\,T$ を

$$\psi_\lambda = e_{m\alpha} \circ \underbrace{\psi \circ \cdots \circ \psi}_{r}$$

と定義する. $\lambda \in L^\circ, u \in M(1,\lambda)$ に対し, $\tilde{\mathcal{Y}}(u,z) = \mathcal{Y}^\theta(u,z) \otimes \psi_\lambda$ と定義して, それを V_{L° 上に線形に拡張する. この時 ψ_λ の定義及び (3.7) と (3.8) より, 次の命題が容易に示せる.

命題 3.5 (1) $\lambda \in L^\circ$ に対し, 線形写像 ψ_λ は次の性質を持つ:

$$\text{任意の } \beta \in L \text{ に対して } e_\beta \circ \psi_\lambda = (-1)^{\langle\beta,\lambda\rangle}\psi_\lambda \circ e_\beta = \psi_{\lambda+\beta}.$$

(2) $a \in V_L, u \in V_{\lambda+L}$ に対し,

$$z_0^{-1}\delta\left(\frac{z_1-z_2}{z_0}\right)Y^\theta(a,z_1)\tilde{\mathcal{Y}}(u,z_2) - \delta\left(\frac{z_2-z_1}{-z_0}\right)\tilde{\mathcal{Y}}(u,z_2)Y^\theta(a,z_1)$$
$$= \frac{1}{2}\sum_{p=0,1} z_2^{-1}\delta\left((-1)^p\frac{(z_1-z_0)^{1/2}}{z_2^{1/2}}\right)\tilde{\mathcal{Y}}(Y(\theta^p(a),z_0)u,z_2)$$

及び

$$\frac{d}{dz}\tilde{\mathcal{Y}}(u,z) = \tilde{\mathcal{Y}}(L(-1)u,z)$$

が成り立つ.

各 quasi-admissible triple $(\lambda,i,j)\in\mathcal{Q}_{\mathcal{L}}$ に対し, $\psi_\lambda(T^i)=T^j$ であることがわかる. よって次を得る.

命題 3.6 $(\lambda,i,j)\in\mathcal{Q}_{\mathcal{L}}$ を quasi-admissible triple とする. この時, $\tilde{\mathcal{Y}}$ の $V_{\lambda+L}\otimes V_L^{T_i}$ への制限は V_L^+ に関する $\binom{V_L^{T_j}}{V_{\lambda+L}\ V_L^{T_i}}$ 型の intertwining 作用素を与える.

$\tilde{\mathcal{Y}}$ を既約な V_L^+-加群に制限することによっていくつかの V_L^+ に関する intertwining 作用素を構成することができる:

命題 3.7 次の型に対応する V_L^+ に関する fusion rule は零ではない;

(i) $\binom{V_L^{T_j,\pm}}{V_{\lambda_r+L}\ V_L^{T_i,\pm}}$, $\binom{V_L^{T_j,\mp}}{V_{\lambda_r+L}\ V_L^{T_i,\pm}}$ $(r\in\mathbb{Z},\ (\lambda_r,i,j)\in\mathcal{Q}_{\mathcal{L}})$,

(ii) $\binom{V_L^{T_i,\pm}}{V_L^+\ V_L^{T_i,\pm}}$, $\binom{V_L^{T_i,\mp}}{V_L^-\ V_L^{T_i,\pm}}$ $(i\in\{1,2\})$,

(iii) $\binom{V_L^{T_1,\pm}}{V^+_{\alpha/2+L}\ (V_L^{T_1,\pm})'}$, $\binom{V_L^{T_2,\mp}}{V^+_{\alpha/2+L}\ (V_L^{T_2,\pm})'}$, $\binom{V_L^{T_1,\mp}}{V^-_{\alpha/2+L}\ (V_L^{T_1,\pm})'}$, $\binom{V_L^{T_2,\pm}}{V^-_{\alpha/2+L}\ (V_L^{T_2,\pm})'}$.

証明. 補題 3.4 と命題 3.6 より, $r\in\mathbb{Z},(\lambda_r,i,j)\in\mathcal{Q}_{\mathcal{L}}$ に対し $\tilde{\mathcal{Y}}$ は $\binom{V_L^{T_j,\pm}}{V_{\lambda_r+L}\ V_L^{T_i,\pm}}$ 及び $\binom{V_L^{T_j,\mp}}{V_{\lambda_r+L}\ V_L^{T_i,\pm}}$ 型の零でない intertwining 作用素を与えることが分かる. よって (i) の型の fusion rule は零ではない.

次に (ii) と (iii) の型の fusion rule が零でないことを示す. 補題 3.4 (2) と系 1.4 より, $\mathcal{Y}^\theta(u\pm\theta(u),z)v=(\mathcal{Y}^\theta\pm\mathcal{Y}^\theta\circ\theta)(u,z)v$ は任意の零でない元 $u\in M(1,\lambda)$ $(\lambda\in L^\circ)$, $v\in M(1)(\theta)^\pm$ に対し零ではない. このように命題 3.6 より, $\tilde{\mathcal{Y}}$ は $i\in\{1,2\}$ に対し,

$$\binom{V_L^{T_i}}{V_L^+\ V_L^{T_i,\pm}},\binom{V_L^{T_i}}{V_L^-\ V_L^{T_i,\pm}},\binom{V_L^{T_i}}{V^+_{\alpha/2+L}\ (V_L^{T_i,\pm})'},\binom{V_L^{T_i}}{V^-_{\alpha/2+L}\ (V_L^{T_i,\pm})'}$$

型の零でない intertwining 作用素を与える. ψ_λ $(\lambda\in L^\circ)$ の定義より, $m\in\mathbb{Z}$ に対し,

$$\psi_{-m\alpha}=\psi_{m\alpha},\ \psi_{-(\alpha/2+m\alpha)}=e_{-\alpha}\psi_{\alpha/2+m\alpha} \tag{3.9}$$

が成り立つ. $\lambda\in L^\circ,u\in M(1,\lambda)$ に対して, $\theta\tilde{\mathcal{Y}}(u,z)\theta=\mathcal{Y}^\theta(\theta(u),z)\otimes\psi_\lambda$ が成り立つので, (3.9) より

$$\theta\tilde{\mathcal{Y}}(u,z)\theta=\tilde{\mathcal{Y}}(\theta(u),z)\text{ for }u\in V_L,$$
$$\theta\tilde{\mathcal{Y}}(u,z)\theta=e_\alpha\tilde{\mathcal{Y}}(\theta(u),z)\text{ for }u\in V_{\alpha/2+L}$$

を得る. 従って, $\tilde{\mathcal{Y}}$ は (ii) と (iii) の型の零でない intertwining 作用素を与えることがわかる; 例えば, $u\in V^+_{\alpha/2+L},v\in(V_L^{T_2,-})'$ に対して,

$$\theta\tilde{\mathcal{Y}}(u,z)v=e_\alpha\tilde{\mathcal{Y}}(\theta(u),z)\theta(v)=\tilde{\mathcal{Y}}(u,z)v.$$

よって, $\tilde{\mathcal{Y}}(u,z)v\in V_L^{T_2,+}\{z\}$ である. 従って, $\tilde{\mathcal{Y}}$ は $\binom{V_L^{T_2,+}}{V^+_{\alpha/2+L}\ (V_L^{T_2,-})'}$ 型の零でない intertwining 作用素を与えている. □

次に, 次の命題を示す. 証明は命題 3.9 の後に与える.

命題 3.8 (1) $i,j \in \{1,2\}$ に対し, $i \neq j$ ならば $\binom{V_L^{T_j}}{V_L^{\pm}\ V_L^{T_i,\pm}}$ 型及び $\binom{V_L^{T_j}}{V_L^{\pm}\ V_L^{T_i,\mp}}$ 型の fusion rule は零である.
(2) $1 \leq r \leq k-1, i,j \in \{1,2\}$ に対し, $(-1)^{r+\delta_{i,j}+1} \neq 1$ ならば, $\binom{V_L^{T_j}}{V_{\lambda_r+L}\ V_L^{T_i,\pm}}$ 型の fusion rule は零である.
(3) $i,j \in \{1,2\}$ に対し, $(-1)^{k+\delta_{i,j}+1} \neq 1$ ならば, $\binom{V_L^{T_j}}{V_{\alpha/2+L}^{\pm}\ V_L^{T_i,\pm}}$ 型及び $\binom{V_L^{T_j}}{V_{\alpha/2+L}^{\pm}\ V_L^{T_i,\mp}}$ 型の fusion rule は零である.

命題 3.8 は, 次の命題の系として得られる.

命題 3.9 W を既約 V_L^+-加群とし W は ある $\lambda \in L^\circ$ に対し $M(1,\lambda)$ に同型な, $M(1)^+$-部分加群を含むと仮定する. この時, もし $(\lambda,i,j) \in \mathcal{P}_\mathcal{L}$ が quasi-admissible triple でないならば, $\binom{V_L^{T_j}}{W\ V_L^{T_i,\pm}}$ 型の fusion rule は零である.

証明は, $\binom{V_L^{T_j}}{W\ V_L^{T_i,\pm}}$ 型の intertwining 作用素 $\mathcal{Y}$ を $\binom{M(1)(\theta)}{M(1,\lambda)\ M(1)(\theta)^{\pm}}$ 型の intertwining 作用素とみて, $\mathcal{Y}^\theta$ と $\mathcal{Y}^\theta \circ \theta$ の線形結合で表し, その詳しい構造を調べることによってなされる. 詳しくは, [A2] を参照して下さい.

命題 3.8 の証明. 既約分解 (2.2)-(2.4) より, V_{λ_r+L} $(1 \leq r \leq k-1)$ は $M(1,\lambda_r)$ を, $V_{\alpha/2+L}^{\pm}$ は $M(1,\alpha/2)$ に同型な部分加群を, そして $V_L^{\pm}$ は $M(1,\alpha)$ に同型な部分加群を含むことがわかる. よって命題 3.8 は命題 3.9 より導かれる. □

最後に, 次の命題を示す.

命題 3.10 (1) $i \in \{1,2\}$ に対し, $\binom{V_L^{T_i,\mp}}{V_L^{+}\ V_L^{T_i,\pm}}$ 型及び $\binom{V_L^{T_i,\pm}}{V_L^{-}\ V_L^{T_i,\pm}}$ 型の fusion rule は零である.
(2) $\binom{V_L^{T_1,\mp}}{V_{\alpha/2+L}^{+}\ (V_L^{T_1,\pm})'}$, $\binom{V_L^{T_2,\pm}}{V_{\alpha/2+L}^{+}\ (V_L^{T_2,\pm})'}$, $\binom{V_L^{T_1,\pm}}{V_{\alpha/2+L}^{-}\ (V_L^{T_1,\pm})'}$, $\binom{V_L^{T_2,\mp}}{V_{\alpha/2+L}^{-}\ (V_L^{T_2,\pm})'}$ 型の fusion rule は零である.

証明. $V_L^{\pm}$ は既約 $M(1)^+$-加群 $M(1)^{\pm}$ をそれぞれ含み, 定理 4.1 より $\binom{M(1)(\theta)^{\mp}}{M(1)^{+}\ M(1)(\theta)^{\pm}}$ と $\binom{M(1)(\theta)^{\pm}}{M(1)^{-}\ M(1)(\theta)^{\pm}}$ 型の fusion rule は零なので, (1) は系 1.4 より導かれる.

次に, $\binom{V_L^{T_1,\mp}}{V_{\alpha/2+L}^{+}\ (V_L^{T_1,\pm})'}$ 及び $\binom{V_L^{T_2,\pm}}{V_{\alpha/2+L}^{+}\ (V_L^{T_2,\pm})'}$ 型の fusion rule が零であることを示す. (2) の残りの型に関しても同様に示すことができる.

命題 3.7 (iii) より, $i \in \{1,2\}, \epsilon \in \{\pm\}$ に対して, $\binom{V_L^{T_i,\epsilon'}}{V_{\alpha/2+L}^{+}\ (V_L^{T_i,\epsilon})'}$ 型の fusion rule が零とならないような $\epsilon' \in \{\pm\}$ が存在する. 今 $\{\tau,\epsilon'\} = \{\pm\}$ とする. この時, $\binom{V_L^{T_i,\tau}}{V_{\alpha/2+L}^{+}\ (V_L^{T_i,\epsilon})'}$ 型の fusion rule が零になることを示さなければならない. このことを示すために, 標準的射影

$$I_{V_L^+}\binom{V_L^{T_i}}{V_{\alpha/2+L}^{+}\ (V_L^{T_i,\epsilon})'} \to I_{V_L^+}\binom{V_L^{T_i,\epsilon'}}{V_{\alpha/2+L}^{+}\ (V_L^{T_i,\epsilon})'}, \quad \mathcal{Y} \mapsto p_{\epsilon'} \circ \mathcal{Y}$$

が単射であることを示す．ここで $p_{\epsilon'}$ は $V_L^{T_i}$ から $V_L^{T_i,\epsilon'}$ への標準的射影で $p_\pm \circ \mathcal{Y}$ は $u \in V^+_{\alpha/2+L}, v \in (V_L^{T_i,\epsilon})'$ に対し $(p_\pm \circ \mathcal{Y})(u,z)v = p_\pm(\mathcal{Y}(u,z)v)$ 定義される intertwining 作用素である．そのためには系 1.4 より，任意の $\binom{V_L^{T_i}}{V^+_{\alpha/2+L}\ (V_L^{T_i,\epsilon})'}$ 型の零でない intertwining 作用素 $\mathcal{Y}$ が

$$\theta\mathcal{Y}(e_{\alpha/2}+e_{-\alpha/2},z)\theta = (-1)^{\delta_{i,2}}\mathcal{Y}(e_{\alpha/2}+e_{-\alpha/2},z) \tag{3.10}$$

を満たすことを示せば十分である．

$V_L^{T_j} = (V_L^{T_i})'$ とし，$V^+_{\alpha/2+L}[0]$ を (3.1) のものとする．この時，$\mathcal{Y}$ は $M(1)^+$ に関する $\binom{V_L^{T_i}}{V^+_{\alpha/2+L}[0]\ V_L^{T_j,\epsilon}}$ 型の intertwining 作用素を与える．したがって，補題 3.4 (2) より $I_{M(1)^+}\binom{V_L^{T_j}}{V^+_{\alpha/2+L}[0]\ V_L^{T_i,\epsilon}}$ は

$$u \in V^+_{\alpha/2+L}[0] \text{ に対し}, \mathcal{Y}^\pm(u,z) = \phi_i\mathcal{Y}^\theta(\phi_{\pm\alpha/2}(u),z)\phi_j^{-1} \tag{3.11}$$

で定義される intertwining 作用素 $\mathcal{Y}^\pm$ で張られる．よって定数 $c_1, c_2 \in \mathbb{C}$ が存在して，

$$\mathcal{Y}(u,z) = c_1\mathcal{Y}^+(u,z) + c_2\mathcal{Y}^-(u,z) \tag{3.12}$$

が任意の $u \in V^+_{\alpha/2+L}[0]$ に対して成り立つ．今 $\beta \in \mathfrak{h}$ に対して，

$$\exp\left(\sum_{n=0}^{\infty}\frac{\beta(-n)}{n}z^n\right) = \sum_{n=0}^{\infty}p_n(\beta)z^n \in (\mathrm{End}\,V_L^\circ)[[z]]$$

と置く．この時 $E = e_\alpha + e_{-\alpha} \in V_L^+$ とすると，$E_0(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}}) = p_{k-1}(\alpha)e_{\frac{\alpha}{2}} + p_{k-1}(-\alpha)e_{-\frac{\alpha}{2}} \in V^+_{\alpha/2+L}[0]$ となり，

$$\phi_{\frac{\alpha}{2}}(E_0(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}})) = p_{k-1}(\alpha)e_{\frac{\alpha}{2}},\ \ \phi_{-\frac{\alpha}{2}}(E_0(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}})) = p_{k-1}(-\alpha)e_{-\frac{\alpha}{2}}$$

を得る．このように (3.11), (3.12) より，

$$\begin{aligned}&[E_0,\mathcal{Y}(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}},z)] = \mathcal{Y}(E_0(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}}),z)\\ &\quad= \phi_i(c_1\mathcal{Y}^\theta(p_{k-1}(\alpha)e_{\frac{\alpha}{2}},z) + c_2\mathcal{Y}^\theta(p_{k-1}(-\alpha)e_{-\frac{\alpha}{2}},z))\phi_j^{-1}\end{aligned} \tag{3.13}$$

を得る．一方，(3.7) より

$$\begin{aligned}[E_0,\phi_i\mathcal{Y}^\theta(e_{\pm\frac{\alpha}{2}},z)\phi_j^{-1}] &= e_\alpha\phi_i\mathcal{Y}^\theta(E_0(e_{\pm\frac{\alpha}{2}}),z)\phi_j^{-1}\\ &= (-1)^{\delta_{i,2}}\phi_i\mathcal{Y}^\theta(p_{k-1}(\mp\alpha)e_{\mp\frac{\alpha}{2}},z)\phi_j^{-1}.\end{aligned}$$

が成り立つ．従って，再び (3.11), (3.12) より，

$$\begin{aligned}&[E_0,\mathcal{Y}(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}},z)]\\ &= (-1)^{\delta_{i,2}}c_1([E_0,\mathcal{Y}^+(E_0(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}}),z)] + c_2[E_0,\mathcal{Y}^-(E_0(e_{\frac{\alpha}{2}}+e_{-\frac{\alpha}{2}}),z)])\\ &= (-1)^{\delta_{i,2}}\phi_i(c_1\mathcal{Y}^\theta(p_{k-1}(-\alpha)e_{-\frac{\alpha}{2}},z) + c_2\mathcal{Y}^\theta(p_{k-1}(\alpha)e_{\frac{\alpha}{2}},z))\phi_j^{-1}\end{aligned} \tag{3.14}$$

を得る. (3.14) から (3.13) を引くと,

$$(c_1-(-1)^{\delta_{i,2}}c_2)\phi_i[\mathcal{Y}^\theta(p_{k-1}(\alpha)e_{\frac{\alpha}{2}},z)-(-1)^{\delta_{i,2}}\mathcal{Y}^\theta(p_{k-1}(-\alpha)e_{-\frac{\alpha}{2}},z)]\phi_j^{-1}=0.$$

この時, 補題 3.4 から $c_1=(-1)^{\delta_{i,2}}c_2$ を得る. また $u\in V^+_{\alpha/2+L}[0]$ に対して, $\theta\mathcal{Y}^\pm(u,z)\theta=\mathcal{Y}^\mp(u,z)$ なので, (3.10) が成り立つことがわかる. □

結果として, 命題 1.2, 命題 2.4, 命題 3.7, 命題 3.8 及び命題 3.10 より次の命題を得る.

命題 3.11 W^1,W^2,W^3 を既約 V_L^+-加群とし, いずれかが twisted 型加群とする. この時 fusion rule $N^{W^3}_{W^1W^2}$ は高々 1 である. W^1 が twisted 型加群であると仮定すると, fusion rule $N^{W^3}_{W^1W^2}$ が 1 である必要十分条件は W^i $(i=1,2,3)$ 次の場合のいずれかを満たすことである:

(i) $W^1=(V_L^{T_1,+})'$ かつ組 (W^2,W^3) 次の組のいずれかである;

$$(V_L^\pm,(V_L^{T_1,\pm})'),\ (V_L^{T_1,\pm},V_L^\pm),\ (V^\pm_{\alpha/2+L},V_L^{T_1,\pm}),\ ((V_L^{T_1,\pm})',(V^\pm_{\alpha/2+L})'),$$
$$(V_{\lambda_r+L},(V_L^{T_1,\pm})')\text{ または }(V_L^{T_1,\pm},V_{\lambda_r+L})\ (1\le r\le k-1,\ r\text{ は偶数}),$$
$$(V_{\lambda_r+L},(V_L^{T_2,\pm})')\text{ または }(V_L^{T_2,\pm},V_{\lambda_r+L})\ (1\le r\le k-1,\ r\text{ は奇数}).$$

(ii) $W^1=(V_L^{T_1,-})'$ かつ組 (W^2,W^3) 次の組のいずれかである;

$$(V_L^\pm,(V_L^{T_1,\mp})'),\ (V_L^{T_1,\pm},V_L^\mp),\ (V^\pm_{\alpha/2+L},V_L^{T_1,\mp}),\ ((V_L^{T_1,\pm})',(V^\mp_{\alpha/2+L})'),$$
$$(V_{\lambda_r+L},(V_L^{T_1,\pm})')\text{ または }(V_L^{T_1,\pm},V_{\lambda_r+L})\ (1\le r\le k-1,\ r\text{ は偶数}),$$
$$(V_{\lambda_r+L},(V_L^{T_2,\pm})')\text{ または }(V_L^{T_2,\pm},V_{\lambda_r+L})\ (1\le r\le k-1,\ r\text{ は奇数}).$$

(iii) $W^1=(V_L^{T_2,+})'$ かつ組 (W^2,W^3) 次の組のいずれかである;

$$(V_L^\pm,(V_L^{T_2,\pm})'),\ (V_L^{T_2,\pm},V_L^\pm),\ (V^\pm_{\alpha/2+L},V_L^{T_2,\mp}),\ ((V_L^{T_2,\pm})',(V^\mp_{\alpha/2+L})'),$$
$$(V_{\lambda_r+L},(V_L^{T_2,\pm})')\text{ または }(V_L^{T_2,\pm},V_{\lambda_r+L})\ (1\le r\le k-1,\ r\text{ は偶数}),$$
$$(V_{\lambda_r+L},(V_L^{T_1,\pm})')\text{ または }(V_L^{T_1,\pm},V_{\lambda_r+L})\ (1\le r\le k-1,\ r\text{ は奇数}).$$

(iv) $W^1=(V_L^{T_2,-})'$ かつ組 (W^2,W^3) 次の組のいずれかである;

$$(V_L^\pm,(V_L^{T_2,\mp})'),\ (V_L^{T_2,\pm},V_L^\mp),\ (V^\pm_{\alpha/2+L},V_L^{T_2,\pm}),\ ((V_L^{T_2,\pm})',(V^\pm_{\alpha/2+L})'),$$
$$(V_{\lambda_r+L},(V_L^{T_2,\pm})')\text{ または }(V_L^{T_2,\pm},V_{\lambda_r+L})\ (1\le r\le k-1,\ r\text{ は偶数}),$$
$$(Vl\lambda_r,(V_L^{T_1,\pm})')\text{ または }(V_L^{T_1,\pm},V_{\lambda_r+L})\ (1\le r\le k-1,\ r\text{ は奇数}).$$

命題 1.2 と命題 2.1 によって, 任意の既約 V_L^+-加群 W^1,W^2,W^3 に対し, $\binom{W^3}{W^1\ W^2}$ 型の fusion rule は, 命題 3.3 と命題 3.11 に挙げられた型の fusion rule のいずれかに一致することがわかる. 従って, 命題 3.3, 命題 3.11, 命題 1.2 及び命題 2.1 を用いて, fusion rule が零とならない全ての型を挙げることができる. しかし, その結果は長くなるので, $M(1)^+$ に関する fusion rule とあわせて次の補足に与えることにする.

4 補足

ここでは, [A1] で決定した 既約 $M(1)^+$-加群の間の fusion rule と, この報告の主要な結果の 1 つである既約 V_L^+-加群の間の fusion rule を挙げる. その結果は, 反傾加群を用いて表せば, k による場合分けが必要なくなるが, 見にくくなってしまうので, k が偶数と奇数の場合に場合分けして述べることにする.

● **既約 $M(1)^+$-加群の間の fusion rule**

定理 4.1 ([A1]) M^1, M^2, M^3 を既約 $M(1)^+$-加群とする. この時 fusion rule $N_{M^1M^2}^{M^3}$ は高々 1 で, fusion rule $N_{M^1M^2}^{M^3}$ が 1 である必要十分条件は M^i $(i=1,2,3)$ が次の場合のいずれかを満たすことである;

(i) $M^1 = M(1)^+$ かつ $M^2 \cong M^3$.

(ii) $M^1 = M(1)^-$ かつ組 (M^2, M^3) は次の組のいずれかである:

$$(M(1)^\pm, M(1)^\mp),\ (M(1)(\theta)^\pm, M(1)(\theta)^\mp),$$
$$(M(1,\lambda), M(1,\mu))\ (\lambda,\mu \in \mathfrak{h} - \{0\},\ \langle\lambda,\lambda\rangle = \langle\mu,\mu\rangle).$$

(iii) $M^1 = M(1,\lambda)$ $(\lambda\mathfrak{h} - \{0\})$ かつ組 (M^2, M^3) は次の組のいずれかである:

$$(M(1)^\pm, M(1,\mu))\ (M(1,\mu), M(1)^\pm)\ (\mu \in \mathfrak{h} - \{0\},\ \langle\lambda,\lambda\rangle = \langle\mu,\mu\rangle),$$
$$(M(1,\mu), M(1,\nu))\ (\mu,\nu \in \mathfrak{h} - \{0\},\ \langle\nu,\nu\rangle = \langle\lambda \pm \mu, \lambda \pm \mu\rangle),$$
$$(M(1)(\theta)^\pm, M(1)(\theta)^\pm),\ (M(1)(\theta)^\pm, M(1)(\theta)^\mp).$$

(iv) $M^1 = M(1)(\theta)^+$ かつ組 (M^2, M^3) は次の組のいずれかである:

$$(M(1)^\pm, M(1)(\theta)^\pm),\ (M(1)(\theta)^\pm, M(1)^\pm),$$
$$(M(1,\lambda), M(1)(\theta)^\pm),\ (M(1)(\theta)^\pm, M(1,\lambda))\ (\lambda \in \mathfrak{h} - \{0\}).$$

(v) $M^1 = M(1)(\theta)^-$ かつ組 (M^2, M^3) は次の組のいずれかである:

$$(M(1)^\pm, M(1)(\theta)^\mp),\ (M(1)(\theta)^\pm, M(1)^\mp),$$
$$(M(1,\lambda), M(1)(\theta)^\pm),\ (M(1)(\theta)^\pm, M(1,\lambda))\ (\lambda \in \mathfrak{h} - \{0\}).$$

● **既約 V_L^+-加群の間の fusion rule**

定理 4.2 ([A2]) W^1, W^2, W^3 を既約 V_L^+-加群とする. この時, fusion rule $N_{W^1W^2}^{W^3}$ は高々 1 である. さらに, fusion rule $N_{W^1W^2}^{W^3}$ が 1 である必要十分条件は W^i $(i=1,2,3)$ が次の場合のいずれかを満たすことである:

(I) k が偶数の場合.

(i) $W^1 = V_L^+$ かつ $W^2 \cong W^3$.

(ii) $W^1 = V_L^-$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{\mp}),\ (V_{\alpha/2+L}^{\pm}, V_{\alpha/2+L}^{\mp}),\ (V_L^{T_1,\pm}, V_L^{T_1,\mp}),\ (V_L^{T_2,\pm}, V_L^{T_2,\mp}),$$
$$(V_{\lambda_r+L}, V_{\lambda_r+L})\ (1 \le r \le k-1).$$

(iii) $W^1 = V_{\alpha/2+L}^+$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_{\alpha/2+L}^{\pm}),\ (V_{\alpha/2+L}^{\pm}, V_L^{\pm}),\ (V_L^{T_1,\pm}, V_L^{T_1,\pm}),\ (V_L^{T_2,\pm}, V_L^{T_2,\mp}),$$
$$(V_{\lambda_r+L}, V_{\alpha/2-\lambda_r+L})\ (1 \le r \le k-1).$$

(iv) $W^1 = V_{\alpha/2+L}^-$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_{\alpha/2+L}^{\mp}),\ (V_{\alpha/2+L}^{\pm}, V_L^{\mp}),\ (V_L^{T_1,\pm}, V_L^{T_1,\mp}),\ (V_L^{T_2,\pm}, V_L^{T_2,\pm}),$$
$$(V_{\lambda_r+L}, V_{\alpha/2-\lambda_r+L})\ (1 \le r \le k-1).$$

(v) $W^1 = V_{\lambda_r+L}$ $(1 \le r \le k-1)$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_{\lambda_r+L}),\ (V_{\lambda_r+L}, V_L^{\pm}),\ (V_{\alpha/2+L}^{\pm}, V_{\alpha/2-\lambda_r+L}),\ (V_{\alpha/2-\lambda_r+L}, V_{\alpha/2+L}^{\pm}),$$
$$(V_{\lambda_s+L}, V_{\lambda_r \pm \lambda_s+L})\ (1 \le r \le k-1),$$
$$(V_L^{T_1,\pm}, V_L^{T_1,\pm}),\ (V_L^{T_1,\pm}, V_L^{T_1,\mp}),\ (V_L^{T_2,\pm}, V_L^{T_2,\pm}),\ (V_L^{T_2,\pm}, V_L^{T_2,\mp})\ r \text{ は偶数},$$
$$(V_L^{T_1,\pm}, V_L^{T_2,\pm}),\ (V_L^{T_1,\pm}, V_L^{T_2,\mp}),\ (V_L^{T_2,\pm}, V_L^{T_1,\pm}),\ (V_L^{T_2,\pm}, V_L^{T_1,\mp})\ r \text{ は奇数}.$$

(vi) $W^1 = V_L^{T_1,+}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{T_1,\pm}),\ (V_L^{T_1,\pm}, V_L^{\pm}),\ (V_{\alpha/2+L}^{\pm}, V_L^{T_1,\pm}),\ (V_L^{T_1,\pm}, V_{\alpha/2+L}^{\pm}),$$
$$(V_{\lambda_r+L}, V_L^{T_1,\pm}) \text{ または } (V_L^{T_1,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1, r \text{ は偶数}),$$
$$(V_{\lambda_r+L}, V_L^{T_2,\pm}) \text{ または } (V_L^{T_2,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1, r \text{ は奇数}).$$

(vii) $W^1 = V_L^{T_1,-}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{T_1,\mp}),\ (V_L^{T_1,\pm}, V_L^{\mp}),\ (V_{\alpha/2+L}^{\pm}, V_L^{T_1,\mp}),\ (V_L^{T_1,\pm}, V_{\alpha/2+L}^{\mp}),$$
$$(V_{\lambda_r+L}, V_L^{T_1,\pm}) \text{ または } (V_L^{T_1,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1, r \text{ は偶数}),$$
$$(V_{\lambda_r+L}, V_L^{T_2,\pm}) \text{ または } (V_L^{T_2,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1, r \text{ は奇数}).$$

(viii) $W^1 = V_L^{T_2,+}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{T_2,\pm}),\ (V_L^{T_2,\pm}, V_L^{\pm}),\ (V_{\alpha/2+L}^{\pm}, V_L^{T_2,\mp}),\ (V_L^{T_2,\pm}, V_{\alpha/2+L}^{\mp}),$$
$$(V_{\lambda_r+L}, V_L^{T_2,\pm}) \text{ または } (V_L^{T_2,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1, r \text{ は偶数}),$$
$$(V_{\lambda_r+L}, V_L^{T_1,\pm}) \text{ または } (V_L^{T_1,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1, r \text{ は奇数}).$$

(ix) $W^1 = V_L^{T_2,-}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{T_2,\mp}),\ (V_L^{T_2,\pm}, V_L^{\mp}),\ (V_{\alpha/2+L}^{\pm}, V_L^{T_2,\pm}),\ (V_L^{T_2,\pm}, V_{\alpha/2+L}^{\pm}),$$
$$(V_{\lambda_r+L}, V_L^{T_2,\pm}) \text{ または } (V_L^{T_2,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は偶数}),$$
$$(V_{\lambda_r+L}, V_L^{T_1,\pm}) \text{ または } (V_L^{T_1,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は奇数}).$$

(II) k が奇数の場合.

(i) $W^1 = V_L^{+}$ かつ $W^2 \cong W^3$.

(ii) $W^1 = V_L^{-}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{\mp}),\ (V_{\alpha/2+L}^{\pm}, V_{\alpha/2+L}^{\mp}),\ (V_L^{T_1,\pm}, V_L^{T_1,\mp}),\ (V_L^{T_2,\pm}, V_L^{T_2,\mp}),$$
$$(V_{\lambda_r+L}, V_{\lambda_r+L})\ (1 \le r \le k-1),$$

(iii) $W^1 = V_{\alpha/2+L}^{+}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_{\alpha/2+L}^{\pm}),\ (V_{\alpha/2+L}^{\pm}, V_L^{\mp}),\ (V_L^{T_1,\pm}, V_L^{T_2,\pm}),\ (V_L^{T_2,\pm}, V_L^{T_1,\mp}),$$
$$(V_{\lambda_r+L}, V_{\alpha/2-\lambda_r+L})\ (1 \le r \le k-1).$$

(iv) $W^1 = V_{\alpha/2+L}^{-}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_{\alpha/2+L}^{\mp}),\ (V_{\alpha/2+L}^{\pm}, V_L^{\pm}),\ (V_L^{T_1,\pm}, V_L^{T_2,\mp}),\ (V_L^{T_2,\pm}, V_L^{T_1,\pm}),$$
$$(V_{\lambda_r+L}, V_{\alpha/2-\lambda_r+L})\ (1 \le r \le k-1).$$

(v) $W^1 = V_{\lambda_r+L}$ $(1 \le r \le k-1)$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_{\lambda_r+L}),\ (V_{\lambda_r+L}, V_L^{\pm}),\ (V_{\alpha/2+L}^{\pm}, V_{\alpha/2-\lambda_r+L}),\ (V_{\alpha/2-\lambda_r+L}, V_{\alpha/2+L}^{\pm}),$$
$$(V_{\lambda_s+L}, V_{\lambda_r \pm \lambda_s+L})\ (1 \le s \le k-1),$$
$$(V_L^{T_1,\pm}, V_L^{T_1,\pm}),\ (V_L^{T_1,\pm}, V_L^{T_1,\mp}),\ (V_L^{T_2,\pm}, V_L^{T_2,\pm}),\ (V_L^{T_2,\pm}, V_L^{T_2,\mp})\ (r \text{ は偶数}),$$
$$(V_L^{T_1,\pm}, V_L^{T_2,\pm}),\ (V_L^{T_1,\pm}, V_L^{T_2,\mp}),\ (V_L^{T_2,\pm}, V_L^{T_1,\pm}),\ (V_L^{T_2,\pm}, V_L^{T_1,\mp})\ (r \text{ は奇数}).$$

(vi) $W^1 = V_L^{T_1,+}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{T_1,\pm}),\ (V_L^{T_2,\pm}, V_L^{\pm}),\ (V_{\alpha/2+L}^{\pm}, V_L^{T_2,\pm}),\ (V_L^{T_1,\pm}, V_{\alpha/2+L}^{\mp}),$$
$$(V_{\lambda_r+L}, V_L^{T_1,\pm}) \text{ または } (V_L^{T_2,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は偶数}),$$
$$(V_{\lambda_r+L}, V_L^{T_2,\pm}) \text{ または } (V_L^{T_1,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は奇数}).$$

(vii) $W^1 = V_L^{T_1,-}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{T_1,\mp}),\ (V_L^{T_2,\pm}, V_L^{\mp}),\ (V_{\alpha/2+L}^{\pm}, V_L^{T_2,\mp}),\ (V_L^{T_1,\pm}, V_{\alpha/2+L}^{\pm}),$$
$$(V_{\lambda_r+L}, V_L^{T_1,\pm}) \text{ または } (V_L^{T_2,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は偶数}),$$
$$(V_{\lambda_r+L}, V_L^{T_2,\pm}) \text{ または } (V_L^{T_1,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は奇数}).$$

(viii) $W^1 = V_L^{T_2,+}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{T_2,\pm}),\ (V_L^{T_1,\pm}, V_L^{\pm}),\ (V_{\alpha/2+L}^{\pm}, V_L^{T_1,\mp}),\ (V_L^{T_2,\pm}, V_{\alpha/2+L}^{\pm}),$$
$$(V_{\lambda_r+L}, V_L^{T_2,\pm}) \text{ または } (V_L^{T_1,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は偶数}),$$
$$(V_{\lambda_r+L}, V_L^{T_1,\pm}) \text{ または } (V_L^{T_2,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は奇数}).$$

(ix) $W^1 = V_L^{T_2,-}$ かつ組 (W^2, W^3) が次の組のいずれかである:

$$(V_L^{\pm}, V_L^{T_2,\mp}),\ (V_L^{T_1,\pm}, V_L^{\mp}),\ (V_{\alpha/2+L}^{\pm}, V_L^{T_1,\pm}),\ (V_L^{T_2,\pm}, V_{\alpha/2+L}^{\mp}),$$
$$(V_{\lambda_r+L}, V_L^{T_2,\pm}) \text{ または } (V_L^{T_1,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は偶数}),$$
$$(V_{\lambda_r+L}, V_L^{T_1,\pm}) \text{ または } (V_L^{T_2,\pm}, V_{\lambda_r+L})\ (1 \le r \le k-1,\ r \text{ は奇数}).$$

参考文献

[A1] T. Abe, Fusion rules for the free bosonic orbifold vertex operator algebra, *J. Algebra* **229** (2000), 333-374.

[A2] T. Abe, Fusion rules for the charge conjugation orbifold, math.QA/0006101.

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

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

[DMZ] C. Dong, G. Mason and Y.-C. Zhu, Discrete series of the Virasoro algebra and the moonshine module, in "Proc. Sympos. Pure Math. Vol. 56," Chap. II, pp. 295-316, *Amer. Math. Soc.*, Providence, 1994.

[DN1] C. Dong and K. Nagatomo, Classification of irreducible modules for the vertex operator algebra $M(1)^+$, *J. Algebra* **216** (1999), 384-404.

[DN2] C. Dong and K. Nagatomo, Representations of Vertex operator algebra V_L^+ for rank one lattice L, *Commun. Math. Phys.* **202** (1999), 169-195.

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

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

[HL] Y.-Z. Huang and J. Lepowsky, A theory of tensor products for module categories for a vertex operator algebra I,II, *Selecta Math., New Series* **1** (1995), 757-786.

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

On 78-dimensional Schröder lattice for F_{22}

北詰 正顕 (Masaaki Kitazume)

千葉大 理学部 数学・情報数理学科

本講演ならびに原稿は，宗政昭弘氏（九州大学）との共同研究に基づいており，さらに本質的に坂内英一氏（九州大学），原田昌晃氏（山形大学）との研究討論に多くを負っている。

1 Soicher's graph と 56 次元 lattice

事の起こりは，今年 (2000 年) の 4 月に当時カナダに滞在していた宗政氏が Bill Martin によるセミナートークについて知らせてきたことによる。それは，

L. Soicher, Electronic J. Combin 2, 1995 #N1

http://www.combinatorics.org/Volume_2/volume2.html#N1

で構成されている $M_{22}:2$ を自己同型群にもつ distance-regular graph についての問題であった。このグラフは Steiner system $S(22,6,5)$ から構成される 672 点のグラフで $\mathbb{R}^{55}$ の integral lattice に埋め込むことができるものであった。これに似た話を，我々は少し前に見聞きしていた。それは，2000 年 1 月の京大数理研での島田氏（北大）の話を発端としたもので，主たる対象は，一言で言ってしまえば $U_6(2)$ の置換表現を 22 次元の lattice に表現して，その lattice の Leech lattice との関係を明らかにするといったものであった。

宗政氏は続けて，今回の Soicher graph の埋め込みが，島田氏の話の後で自身が考察した状況に似ていると報告したのである。直ちに坂内氏が，今回の 55 次元 lattice は，$2\cdot U_6(2)$ が作用する 56 次元 lattice から得られるに違いないと予想した。詳しい事は省略するが，坂内氏は tight spherical design との関係から，この 56 次元表現を気にかけていたのであった。それならば，と私が続けたのは，この 56 次元表現と，先の島田氏の 22 次表現を合わせれば，$78(=22+56)$ 次元表現ができて，そこにはきっと Fischer 群 F_{22} が作用するに違いないという予測だったのである。実際，F_{22} は 78 次元の既約表現を持っていて，その部分群 $2\cdot U_6(2)$ への制限は $22+56$ と分解する事が指標表 (ATLAS) からわかる。すると坂内氏が続

けて，Schröder という人の学位論文を昨年もらっていて，そこで F_{22} の作用する 78 次元の lattice が構成されていることを思い出してくれたのである。

*　　*　　*

これが，今回の話の概略であり，全てでもある。話は全て予想通りに進行した。そして予想以上のことが起こらなかったことに，我々は少しがっかりしたものである。以下，ここに書いた内容について，詳しく述べることにする。

2　Fischer 群 F_{22} と Mathieu 群 M_{22}

Fischer 群 F_{22} は，いわゆる 3-transposition 群と呼ばれる有限群の内，散在型単純群を含む短い系列

$$F_{24}, F_{23}, F_{22}, F_{21}$$

の内の一つである。これらは 3-transposition の共役類 D（すなわち $\forall a, b \in D$ に対し，それらの位数は 2 で，かつ，その積の位数 $|ab|$ は $1, 2, 3$ のいずれか）で生成され ($F_n = \langle D \rangle$ $(n = 24, 23, 22, 21)$)，ひとつの元 $(d \in D)$ の中心化群を考えるとき

$$C_{F_n}(d)/\langle d \rangle \cong F_{n-1}$$

が成り立つ。この中で，F'_{24}(この場合だけ交換子を取る必要がある)，F_{23}, F_{22} の 3 つが散在型単純群で，残る一つは $F_{21} = U_6(2)$（ユニタリ群）が成り立ち，やはり単純群になる。

$F_n(n = 21, 22, 23, 24)$ の 2-Sylow 群 S を一つ取り，$L := S \cap D$ とおく。すると L は (3-transposition の性質から) 互いに可換な元からなる。添字 n は，実はこの L の元の個数を表していて，それらは位数 2^{n-12} の基本可換群を生成する。そして，その正規化群に Mathieu 群 M_n が現れるのである。

$$|L| = n,\ N_{F_n}(L)/\langle L \rangle \cong M_n,$$

$n = 24$ なら有名な 5 重可移群 M_{24} が現れる。一般に，M_n は L 上 $(n-19)$-可移に働いている。M_{24}, M_{23}, M_{22} が散在型単純群であり，同型 $M_{21} = L_3(4)$ (射影線形群) が成り立つ。

次に話を F_{22} に絞る。$F_{22} > 2 \cdot U_6(2) > M_{22}$ という包含関係が重要である。$F_{22} = \langle D \rangle$, $d \in D$ とすると，

$$C_{F_{22}}(d) \cong 2 \cdot U_6(2) \quad \text{(位数 2 の中心を持つ非分裂拡大)}$$

が成立する。さらに，

$$|L| = 22, \quad N_{F_{22}}(L) \cong 2^{10} : M_{22} \text{(半直積)}$$

である。ここは少し説明を要する。D への $N_{F_{22}}(L)$ の作用を考える。これが実は3つの軌道に分かれる。

$$D = L \cup X_1 \cup X_2$$

ここで L 以外の軌道は，$X_1 = \{x \in D : |C_L(x)| = 6\}$, $X_2 = \{x \in D : |C_L(x)| = 0\}$ を表される。さらに，$x \in X_2$ の固定部分群が M_{22} と同型な群になる。すなわち

$$N_{F_{22}}(L) \cap C_{F_{22}}(x) \cong M_{22} \quad (\text{特に，} 2 \cdot U_6(2) > M_{22})$$

である。また，X_1 の記述に現れる $C_L(x)$ という6点集合は，3-(22,6,1) というパラメータのデザイン（もしくは Steiner system $S(22,6,3)$）のブロックになっている。すなわち

$$\mathcal{B} := \{C_L(x) \mid x \in X_1\}$$

とおくと，ペア $(L, \mathcal{B})$ について，「L の任意の相異なる3点を含む $\mathcal{B}$ のブロックがただ一つ存在する」という性質が成り立つ。容易な計算から，このときのブロックの総数は，$\binom{22}{3}/\binom{6}{3} = 77$ であるとわかるだろう。

冒頭に書いた Soicher のグラフを説明するためには，もう一言必要である。最も大きい Mathieu 群 M_{24} は extended binary Golay code G_{24} の自己同型群として定義することができる。詳しい定義等は省略して，後で用いる設定のみを書いておく。24点集合 Ω を取り，その部分集合全体を2元体 $\mathbb{F}_2$ 上の24次元ベクトル空間と見なす。ここで，和は部分集合の対称差 $X + Y := (X \cup Y) \setminus (X \cap Y)$ で定義する。G_{24} はその12次元部分空間で，任意の元の重さ（集合としての濃度）が

$$0, 8, 12, 16, 24$$

に限るというものである。このようなコードは（正確には，次元と最小重さで）一意に決まり，その全自己同型群が M_{24} と同型である。このとき，M_{24} は Ω 上5重可移に作用し，その2点 $a, b \in \Omega$ の固定部分群が M_{22} という事になる。

$$M_{22} = \{\sigma \in M_{24} \mid \sigma(a) = a, \sigma(b) = b\}$$

G_{24} の8点集合のうち，a, b を含むものだけを考えて，a, b を除いた6点集合の全体を考えれば，それらが先に述べた $S(22,6,3)$ のブロックの集合を与える。また，G_{24} の12点集合のうち，a, b の一方のみを含むものを考える。この場合，その補集合も同じ性質を持つので，ペアで考える方が良い。重要な事実は，M_{22} が，そのようなペア全体に対し可移に作用する，という事である。同じ事だが，少し記号を変えれば，

$$\Sigma := \{(A, B) \mid \{a, b\} \cup A \cup B = \Omega, |A| = |B| = 11, \{a\} \cup A, \{b\} \cup B \in G_{24}\}$$

上に可移に作用するのである。その次数 ($= |\Sigma|$) は 672，置換の rank (1点の固定部分群の軌道の個数) は6である。この Σ を点集合として Soicher graph が定義される。それは距離正則グラフになり，valency は 110，diameter は3である。しかし，このグラフの edge を記述するのは，そう簡単なことではない。実際，M_{22} の言葉では簡潔には記述出来ないと思う。

3　グラフの埋め込み（代数的組合せ論から）

まず，一般論から始める。(G,Δ) を可移置換群とするとき，Δ をユークリッド空間の lattice L に埋め込むとは，

(1) lattice L は，その部分集合 Δ^* で生成され，

(2) 自己同型群 $\mathrm{Aut}(L)$ が G と同型な部分群 G^* を含み，

(3) 置換群としての同型 $(G,\Delta)\cong(G^*,\Delta^*)$ が成り立つ

ことを言うことにする。簡単のため (G,Δ) と (G^*,Δ^*) とを同一視する。このとき，生成系 Δ の Gram matrix

$$E=(E_{xy})_{x,y\in\Delta}$$

は正定値であり，G の作用に関して

$$E_{xy}=(x,y),E_{xy}=E_{g(x)g(y)}\ (\forall g\in G)$$

が成り立っている。代数的組合せ論によれば，このことは，E が，置換表現から作られる Bose-Mesner algebra $B(G,\Delta)$ に含まれることを意味している。ただし，Bose-Mesner algebra $B(G,\Delta)$ とは，次のようなものである。$a\in\Delta$ に対し，その固定部分群を G_a と表し，G_a の作用による軌道分解を

$$\Delta_0=\{a\},\Delta_1,...,\Delta_d\quad(d=\mathrm{rank})$$

とおくことにする。軌道 Δ_i に関する結合行列を A_i と表す。すなわち，A_i は Δ 次の正方行列で

$$(A_i)_{xy}=1\Leftrightarrow\exists g\in G:g(x)=a,g(y)\in\Delta_i$$

で定義されるものである。定義から $A_0=I$ となる。Bose-Mesner algebra $B(G,\Delta)$ は次で定義される。

$$B(G,\Delta):=\langle\,A_0,A_1,\cdots A_d\,\rangle_{\mathbf{C}}$$

さて，特に (G,Δ) が multiplicity free である時は，Bose-Mesner algebra $B(G,\Delta)$ は可換な代数になり，原始巾等元で生成される。これを，$E_0,E_1,...,E_d$ と表すことにしよう。ここで，$E_0=\frac{1}{|\Delta|}J$（ただし J は全ての成分が 1 である行列）とおくことができる。すると，先の Gram matrix E は，これらの線形結合で $E=\sum_i\lambda_iE_i$ という形に表される。ここで，行列のランクは

$$\mathrm{rank}(E)=\sum_{\lambda_i\neq0}\mathrm{rank}(E_i)$$

と計算できる。この値は，Δ を埋め込んだ lattice L の rank を表している。一方，左辺に現れる E_i 達は有限個 (d 個) しかないわけだから，rank が特別な値（例えば小さい値）であれば，lattice はかなり強い制限を受けることになる。

そこで，以下では E_i 達は rank の小さい順に並んでいる ($\mathrm{rank}E_i \leq \mathrm{rank}E_{i+1}$) ものとする。また，計算がしやすいように（もしくは出来上がる lattice が integral になることを想定して）成分が整数になるように定数倍しておいて，それを改めて E_i と書くことにする。（もちろん，そうすると idempotent ではなくなる。）例えば $E_0 = J$ で，その rank は 1 である。

例 1 $(U_6(2), \Gamma)$　群としてはユニタリ群 $U_6(2)$ を取り，その自然な表現空間（ユニタリ空間）$\mathbb{F}_4^6$ における maximal totally isotropic subspaces の全体を Γ とおく。$|\Gamma| = 891$ である。このとき，$\mathrm{rank}(E_1) = 21$ が (E_0 を除いて) 最小の rank である。また E_1 の成分は 4 種類しかない。前節で約束したように，成分が整数になるように定数倍しておくと，その値は $8, -4, 2, -1$ のいずれかで，8 は主対角線に並んでいる。このことは（$E = E_1$ とすれば）Γ は 21 次元の integral lattice のノルム (squared length)8 のベクトルで表されることになる。しかし，これでは (rank が奇数だし) 良い lattice はできない。そこで，次のような手段を取る。

$$\begin{aligned}(E_1)_{xy} = &\ 8, \ -4, \ 2, \ -1 \\ \to &\ 12, \ 0, \ 6, \ 3 \quad (+4) \\ \to &\ 4, \ 0, \ 2, \ 1 \quad (\times 1/3)\end{aligned}$$

全体に 4 を足して 3 で割ったということである。4 を足すということは $4J(= 4E_0)$ を足すということであるから，$E = \frac{1}{3}(4J + E_1)$ という Gram matrix を得たことになる。ここでは Γ は 22 次元 lattice のノルム 4 のベクトルで表されている。

実は，これが Leech lattice から得られる $\cdot 222$ が作用する 22 次元の lattice (すなわち，2000 年 1 月の数理研の集会で島田氏 (北大) が構成した系列のひとつ) と同型になる。これについて簡単に記述しておこう。L を Leech lattice とし，Golay code から通常の方法で構成しておく。この自己同型群が Conway の $\cdot O$ である。このとき，$a = 1/\sqrt{8}(4, -4, 0, 0, ..., 0), b = 1/\sqrt{8}(0, 4, -4, 0, ..., 0) \in L$ であり，a, b を固定する $\cdot O$ の部分群を $\cdot 222$ と表す。この群は，a, b と直交するベクトルで生成される sublattice に作用する。これを U_{22} と表すことにすると，

$$U_{22} = \{(v_1, ..., v_{24}) \in \text{Leech lattice} \mid v_1 = v_2 = v_3\}$$

であるが，等しい値を持つ 3 つの成分を一つにまとめてしまうと，

$$U_{22} \cong \left\{(\sqrt{3}v_1, v_4, ..., v_{24}) \mid (v_1, ..., v_{24}) \in U_{22}\right\}$$

というように 22 次元の lattice として表される。これが，先ほどの $E = \frac{1}{3}(4J + E_1)$ という Gram matrix もつ生成系を含んでいるのである。

なお，これらの lattice の同型から，群の同型 $\cdot 222 \cong U_6(2)$ が得られる。これが群論的にはインパクトのある事実なのであった。

例2 (M_{22}, Σ) Mathieu 群 M_{22} と，2節で導入した Σ ($|\Sigma| = 672$) である。この場合は，最小のランクは $\mathrm{rank}(E_1) = 55$ で，前の例と同様のことをすると

$$\begin{aligned}(E_1)_{xy} = &\ 55,\ 13,\ -1,\ -15 \\ \to &\ 56,\ 14,\ 0,\ -14\ \ (+1) \\ \to &\ 4,\ 1,\ 0,\ -1\ \ (\times 1/14)\end{aligned}$$

となって，$\frac{1}{14}(J + E_1)$ という Gram matrix が良い lattice を作る。これを U_{56} と表すことにしよう。

2節で詳しく述べられなかった Soicher graph は，この lattice においては簡単に記述することができる。すなわち，点集合 Σ を U_{56} に埋め込むとき，2点 $x, y \in \Sigma$ が辺で結ばれるための条件は，$(x, y) = 1$ であることと定義すればよいのである。

実は，ここで面白いことが起こっている。U_{56} の自己同型群は M_{22} より本質的に大きくなるのである。実際，

$$\mathrm{Aut}(U_{56}) > 2 \cdot U_6(2) > M_{22}$$

という2節で述べた包含関係がここに現れる。ただし，Σ への置換群として大きくなるわけではない。しかし，ほんのちょっとの細工で $2 \cdot U_6(2)$-orbit を作ることができる。Σ の元の ± 1 倍を考えて $\tilde{\Sigma} := \{\pm s | s \in \Sigma \subset U_{56}\}$ と定義すれば，これが軌道になっている。置換群としての rank は5である。

この $\tilde{\Sigma}$ を点集合として，新たにグラフを定義することもできる。$x, y \in \tilde{\Sigma}$ が辺で結ばれるための条件を，$(x, y) = -1$ であることと定義するのである。これは Meixner's graph として知られているものである。だから，この話 (U_{56}) は $(2 \cdot U_6(2), \tilde{\Sigma})$ という rank 5 の置換表現から始めて，それを lattice に埋め込み，そこで graph を定義する，という話として展開しても良かったわけである。

*　　*　　*

いずれにせよ，これで $U_6(2)$ が作用する22次元空間と，$2 \cdot U_6(2)$ が作用する56次元空間が出来上がった。これが，F_{22} の78次元表現から，$F_{22} > C_{F_{22}}(d) = 2 \cdot U_6(2)$ という包含関係を通じて得られるのではないか，というのが我々の出発点であったのである。

4 78-dim. representation of F_{22}

問題の F_{22} の78次元表現の記述は，ATLAS にも書いてある。まずは，そこから説明しよう。

まず，$H_0 = \{1, 2, ..., 22\}$ とおき，この22点集合上に Steiner system $S(3, 6, 22)$ の構造を考える（2節参照）。すると，そのブロックの個数は77個になるので，

それを $H_1, H_2, ..., H_{77}$ と表す。我々に必要な 78 次元ベクトル空間を，これらの $H_0, H_1, ..., H_{77}$ を形式的な基底として生成されるものとして定義する。

$$\mathbb{Q}^{78} = \oplus_{i=0}^{77} \mathbb{Q} H_i$$

さらに，ここへ作用する $\mathrm{GL}(78, \mathbb{Q})$ の元を以下のように定義する。

$$m_i := \begin{cases} H_k \mapsto H_k & (i \in H_k) \\ H_k \mapsto -H_k & (i \notin H_k) \end{cases} \quad (i \in H_0 = \{1, ..., 22\})$$

これらは，位数 2^{22} の elementary abelian group を生成する。さらに，

$$a := \begin{cases} H_0 & \mapsto & \frac{1}{16}(-5H_0 + 3\sum H_k) \\ H_i & \mapsto & \frac{1}{16}\left(H_0 - 7H_i - \sum_{H_i \cap H_k = \emptyset} 3H_k + \sum_{|H_i \cap H_k| = 2} H_k\right) \end{cases}$$

と定義すれば，

$$\langle m_1, ..., m_{22}, a \rangle \cong 2 \times F_{22}$$

が成り立つというのである。

この78次表現を，lattice とその自己同型群として実現したものが，表題の Schröder's lattice である。その論文

> B.Schröder: Konstruktionen und Darstellungen der Fischer-Gruppe Fi_{22}, 1998 (Ph.D.thesis)

に従って，定義の概略を述べておこう。

まず $e = (1, 1, ..., 1) \in \mathbb{Q}^{78}$ とおく。次に $j, k \in \{1, 2, ..., 77\}$ で $H_j \cap H_k = \emptyset$ をみたすものに対して $v_{jk} = ((v_{jk})_l)_{l=0,...,77}$ を次のように定義する。

$$(v_{jk})_l = \begin{cases} 2 & (l \in \{j, k\}) \\ -2 & (l \notin \{j, k\} \text{ and } (H_l \cap H_j = \emptyset \text{ or } H_l \cap H_k = \emptyset)) \\ 0 & (\text{otherwise}) \end{cases}$$

これらを用いて lattice L を

$$L := \langle m(e + v_{ij}) \mid m \in M, i, j\text{:as above} \rangle_{\mathbb{Z}}$$

とし，さらに最終的な目的物 L_{78} を

$$L_{78} := \left\{ \frac{1}{4}(\sqrt{3} c_0 e_0 + \sum c_i e_i) \mid c_0 e_0 + \sum c_i e_i \in L \right\}$$

と定義する。L から L_{78} を作った際の $\sqrt{3}$ という係数は，先に U_{22} の説明に現れたのと同じ事情であると考えればよい。この lattice は even integral で，lattice としてのパラメータは，

$$\text{determinant} = 3, \quad \text{minimum norm} = 6, \quad \text{kissing number} = 3294720$$

となる。次ページに，L_{78} の生成行列を掲げておく。実際には，我々の計算においては計算機上 (MAGMA) で，この生成行列を扱うのが主なのである。

さて，この lattice の自己同型群が

$$\mathrm{Aut}(L_{78}) \cong 2 \times F_{22} : 2$$

と得られる。その生成元は，先の ATLAS で与えてあったものと同じである。ただし，それは $H_1, ..., H_{77}$ をどのように並べるかによる。しかし，ここではその詳細は省略する。ただ一つだけ，

> $1(\in H_0)$ を含むブロック（その総数は 21 個）が $H_1, ..., H_{21}$ として並んでいる，

という事だけを明記しておこう。H_0 も 1 を含んでいることに注意すると，先に m_1 と書いた自己同型の作用が確定する。それは，

> 最初の 22 個の基底に 1 倍，後半の 56 個の基底 -1 倍で作用する

というものである。実は，この m_1 が F_{22} を生成する 3-transposition のひとつである。その $2 \cdot U_6(2)$ と同型な中心化群が，m_1 の固有空間に作用する。そこで，m_1 の固有空間を $s = \pm 1$ に対して

$$\mathbb{R} \otimes L_{78} \supset W_s := \langle\, v \in \mathbb{R} \otimes L_{78} \mid m_1(v) = sv \,\rangle_{\mathbb{R}}$$

と定義しておこう。次ページの表では，一ヶ所だけ空白を挿入してあるが，その空白の下部が W_{-1} に含まれている部分である。それぞれの固有空間への projection を π_s と表し，

$$L_{22} := \pi_1(L_{78}) \quad L_{56} := \pi_{-1}(L_{78})$$

とおく。

* * *

これらの L_{22}, L_{56} 等から，どのような lattice が出てくるだろうか，というのが我々の主たる問題である。それぞれには $U_6(2), 2 \cdot U_6(2)$ が作用しており，次元は 22, 78 である。既に述べた U_{22}, U_{78} との関係も十分に期待できるという訳である。

(Basis of Schröder's lattice) (実際の生成行列は，この 1/4 倍)

S11111111111111111111111111111111111111111111111111111111111111111111111111119
02000200020200020000060002020002000006020000202220002040064402220062226042640E
002002000002020202222600000202020222260000000000220022622666020000400060424406
0002020000020202200022000002020220002200000000000220040006600000062682060440C
0000220000000000022002600000000000220026000000000004004004620000044062664 00000
0000040000000000000040000000000000000400000000000004000400400000040044440 4004C
000000200202020000220400000000000000000202002002222220602226200222200022064004
000000020202020202020200000000000000000202002200222620200642200026404424486664
000000002200000202022400000000000000000000020202222222220642022224602000642646
000000000400000000000040000000000000000000000000000000004000000004000004404040
00000000002200022020240000000000000000000000000200602202442200002400004640440A
000000000004000000000040000000000000000000000000000400440400222226222672226006A
0000000000002207220020600000000000000000000000000002240264062422220202466220002E
000000000000040000000400000000000000000000000000000004000000400000044044440440C
00000000000000222222220000000000000000000000000000222222220440202002024422440 02A
0000000000000004000004000000000000000000000000000040040000000000000000004444448
000000000000000040000400000000000000000000000000000400040044000004000404040044
00000000000000000400040000000000000000000000000000400400404222222222222666006A
000000000000000000400400000000000000000000000000000000000000000000400000444444C
0000000000000000000404000000000000000000000000000000004404040000000004040044440
0000000000000000000044000000000000000000000000000000004404042222262226266620026
0000000000000000000008000000000000000000000000000000000000000000000000000000008

00000000000000000000002002020200002204020202200222042024224422020460666246464E
000000000000000000000002020202020202020202002222220420600606022204222264066 24A
000000000000000000000000220000020202240000022002222222660624022206024204602402
000000000000000000000000040000000000000400000000000000000400000004404000444 00C
000000000000000000000000002200022020240000000000202402022460020020004042444464
000000000000000000000000000400000000040000000000000400000444222226622262660026
0000000000000000000000000000220220020600000000000206020206062222206024682400 6A
00000000000000000000000000000400000000400000000000004000000400000400404000444 8
000000000000000000000000000000222222220000000000222222220404220220204422440028
000000000000000000000000000000004000004000000000004000400440000000004440004440
00000000000000000000000000000000040000400000000000040004000000000400400404004C
000000000000000000000000000000000040004000000000000400400404222222226626660062
000000000000000000000000000000000004004000000000000000440000000004000004444444
000000000000000000000000000000000000404000000000000000000440000000004040044448
000000000000000000000000000000000000044000000000000004404402222262226266620026
000000000000000000000000000000000000008000000000000000000000000000000000000008
000000000000000000000000000000000000000220002220022000026224400222004044000640
0000000000000000000000000000000000000000400000000000000400444222226222667 2042E
0000000000000000000000000000000000000000220200220022006200662222226266004406 2E
000000000000000000000000000000000000000004000000000000000400400000000040040408
0000000000000000000000000000000000000000222222222222222004402222222244004422 0A
000000000000000000000000000000000000000000400000000000044000000000000044440400
00000000000000000000000000000000000000000040000000400040440000000400000400404C
00000000000000000000000000000000000000000000040000040040040422222622222622406E
0000000000000000000000000000000000000000000400004000400440000000000000004404 00
000000000000000000000000000000000000000000000004000400400000000000000000440408
000000000000000000000000000000000000000000000000400400440404222226222622624426
000000000000000000000000000000000000000000000000004040000044000000400044044404
000000000000000000000000000000000000000000000000004400440044000000000044440008
000000000000000000000000000000000000000000000000000800000000000000000000000008
0000000000000000000000000000000000000000000000000000404000442222222262622644 6A
000000000000000000000000000000000000000000000000000040400440000000004040044448
000000000000000000000000000000000000000000000000000000800000000000000000000008
000000000000000000000000000000000000000000000000000000080000000000000000000008
000000000000000000000000000000000000000000000000000000004444222222222222220022
000000000000000000000000000000000000000000000000000000000800000000000000000008
000000000000000000000000000000000000000000000000000000000080000000000000000008
000000000000000000000000000000000000000000000000000000000008000000000000000008
000000000000000000000000000000000000000000000000000000000000400000004444440040
000000000000000000000000000000000000000000000000000000000000040000404040400048
000000000000000000000000000000000000000000000000000000000000004004000404400048
00000000000000000000000000000000000000000000000000000000000000040440000044000C
000000000000000000000000000000000000000000000000000000000000000044400440400044
000000000000000000000000000000000000000000000000000000000000000008000000000008
000000000000000000000000000000000000000000000000000000000000000000800000000008
00000000000000000000000000000000000000000000000000000000000000000004400404004C
000000000000000000000000000000000000000000000000000000000000000000008000000008
000000000000000000000000000000000000000000000000000000000000000000000800000008
000000000000000000000000000000000000000000000000000000000000000000000080000008
000000000000000000000000000000000000000000000000000000000000000000000008000008
000000000000000000000000000000000000000000000000000000000000000000000000800008
000000000000000000000000000000000000000000000000000000000000000000000000080008
000000000000000000000000000000000000000000000000000000000000000000000000008008
000000000000000000000000000000000000000000000000000000000000000000000000000808
000000000000000000000000000000000000000000000000000000000000000000000000000088
000000000000000000000000000000000000000000000000000000000000000000000000000008

(記号)
S=\sqrt{3}
A=10
C=12
E=14
G=16

5 結論

以下は手早く，我々の得た結論をまとめることにする。我々が調べるべき対象は，L_{22}, L_{56} である。これら自体は integral lattice にはならない。そこで，少なくともノルムが整数のものだけを考えてみようと

$$L_{22}^{\mathbb{Z}} := \{x \in L_{22} \mid (x,x) \in \mathbb{Z}\} \quad L_{56}^{\mathbb{Z}} := \{y \in L_{56} \mid (y,y) \in \mathbb{Z}\}$$

と定義する。次が基本的な observation である。

Lemma 1. (1) 任意の $x \in L_{22}$ に対し，ノルム (x,x) は半整数である。特に，$[L_{22} : L_{22}^{\mathbb{Z}}] = 2$ である。
(2) 任意の $x \in L_{56}$ に対し，ノルム (x,x) は半整数である。特に，$[L_{56} : L_{56}^{\mathbb{Z}}] = 2$ である。

L_{22} の生成系は，全体の生成行列から左上の 22×22 の部分のみ考えれば良いので，手計算でも上記の事実 (1) を確かめることができるだろう。(2) は，全体が integral lattice であることから従う。

今述べたように，L_{22} の計算は手計算で十分できる。事実，次を示すのも容易である。

Proposition 2. $\sqrt{2}L_{22}^{\mathbb{Z}} \cong U_{22}$.

この事実は，$U_6(2) \cong \cdot 222$ という同型を反映している。もちろん，ここでは $F_{21} \cong U_6(2)$ から構成される F_{22} を話の出発点にしているわけで，さほどのインパクトはない。

* * *

残る問題は，L_{56} の方である。実は一時期，我々は淡い期待を抱いていた。ここから sublattice として extremal lattice を得ることができないだろうかと。この次元では minimal norm = 6 という lattice が extremal で，これまでに小関道夫氏（山形大学）の構成したものが唯一の例と思われるからである。しかし，それは「淡い」だけのものだった。

* * *

最後の定義として，

$$M_{56} := \mathrm{Ker}(\pi_1) \cap L_{78}$$

とおく。これは L_{56} の sublattice である。次のような計算は，手計算では大変だと思うのだが，MAGMA にかかれば「おやすいご用」のようである。

Lemma 3. $\det L_{56} = 2^{-22}$, $\det M_{56} = 2^{22}$ となる。特に $M_{56} = L_{56}^{*}$ である。

そして，この M_{56} が「求めるもの」だったのである。

Proposition 4. $M_{56} \cong U_{56}$.

何のことはない。当初に期待していたものが，その通り出てきただけの事である。そして，その結果として（少なくとも sublattice としては）extremal への夢が潰えたのである。

Corollary 5. L を $L_{56}^{\mathbb{Z}}$ の *sublattice* で，かつ *unimodular* と仮定すれば，L は M_{56} を含み，従って，その *minimal norm* は 4 である。

6 付記

その後我々は，L_{78} から U_{22}, U_{56} を作るのではなくて，U_{22}, U_{56} から L_{78} を作ることができないかと考えた。今のところ，ある難点にぶつかり停滞している。また，U_{56} に関して出てきた Soicher graph と Meixner graph については，宗政氏なりの切り口で調べられている（第１２回日仏組合せ論ワークッショップ）。

また，講演後，原田耕一郎先生から「78 という次元は E_6 型の Lie 環の次元である」との指摘を受けた。言われてみればもっともで，このことは，昨年 (1999) 九大での代数的組合せ論シンポジウムで，筆者が講演した $F_{22} < {}^2E_6(2)$ という包含関係と関連しているようで，意識していなかったことが恥ずかしいくらいである。同じような事は，E_8 についてもあって，こちらは Thompson 群が作用する 248 次元の lattice が存在する。$Th < E_8(3)$ という包含関係は，余りにも有名である。E_7 についても Harada 群の 133 次元表現という魅力的なものは存在するのであるが，その表現は $\mathbb{Q}$ 上でなく，$\mathbb{Q}(\sqrt{5})$ 上であるということからか，今のところ lattice の存在等は知られていないようである。

Another approach to the Stellmacher's Σ_4-free Theorem

Makoto Hayashi
Aichi University of education

1. Introduction.

Stellmacher proved the following theorem:

Theorem [St]. Let S be a non-trivial finite 2-group. Then there is a non-trivial characteristic subgroup $W(S)$ of S which is normal in any finite group H satisfying the following conditions:

(I) $S \in Syl_2(H)$;

(II) H is Σ_4-free;

(III) $C_H(O_2(H)) \leq O_2(H)$; and

(IV) Every non-abelian simple section of H is isomorphic to $Sz(2^m)$ or $PSL_2(3^m)$ for some odd m.

The purpose of this note is to give the outline of another proof of this theorem.

Let C be the class of all embeddings (see [St]) (τ, H) of S enjoying (II), (III), (IV) and (I') $S\tau \in Syl_2(H)$.

Let $(\tau_i, H_i) \in C$ for $i = 1, 2$. (τ_1, H_1) and (τ_2, H_2) are equivalent, if there exists an isomorphism ϕ from H_1 to H_2 such that $\tau_1\phi = \tau_2$. Let $[C]$ be the class of equivalence classes of C with respect to this equivalence relation. By [St,1.2], $[C]$ is finite. Let $\Omega^* = \{(\tau_i, K_i); 1 \leq i \leq p\}$ be the set of all representatives of the class in $[C]$. Let $G(C)$ be the amalgamated product of $K_1, \cdots, K_p$ over S. We identify $S, K_1, \cdots, K_p$ with their images. For a subset Δ of Ω^*, we denote by $O_2(\Delta)$ the largest subgroup of S that is normal in all the elements in Δ. Take $|S|$ to be minimal such that $O_2(\Omega^*) = 1$. Then there is a subset $\Omega = \{H_i; 1 \leq i \leq n\}$ of Ω^* satisfying the following conditions:

(V) H_i is not 2-closed, and H_i has a unique maximal subgroup containing S for all $i; 1 \leq i \leq n$,

(VI) $O_2(\Omega) = 1$, and $O_2(\Delta) \neq 1$ for any proper subset Δ of Ω.

Notation: For $X \in \Omega$, we write $Q_X = O_2(X)$ and $Q_X^* = O^2(X) \bigcap S$. For brevity, $Q_i = Q_{H_i}$ and $Q_i^* = Q_{H_i}^*$, $1 \leq i \leq n$.

We assume further two hypothesis (which is not essential):

(H.1) $n \geq 3$;

(H.2) $\Omega_1 Z(Q_H) \leq Q_K$ for all $H, K \in \Omega$.

2. On the digraph $\mathcal{D}(\otimes)$.

(2.1) $[\Omega_1 Z(Q_H), O^2(H)] \neq 1$ if and only if $[\Omega_1 Z(Q_H^* \bigcap Q_H), O^2(H)] \neq 1$ for $H \in \Omega$.

By minimality of $|S|$ and Ω, we have:

(2.2) There is no proper subgroup T of S such that either $Q_H^* \leq T$ or $T \lhd H$ for all $H \in \Omega$.

For a proper subset Δ of Ω, we write $W_0 = W_{0,\Delta} = O_2(\Delta)$, and denote by $W_i = W_{i,\Delta}$ the pre-image of $W(S/W_{i-1})$, $i = 1, 2, \cdots$ which is normal in any elements of Δ that is normal in all the elements of Δ except for the elements H of Δ such that $[O^2(H), W_i] \not\leq S$.

Furthermore, we can define the function f_Δ from elements H of Δ to integers such that $f_\Delta(H) = \min\{i; O^2(H)W_i/W_i = O_{2',E}(HW_i/W_i)\}$.

(2.3) Under the same notation as above, let i be an integer, and $\Gamma = \{H \in \Delta;\ f_\Delta(H) = i\}$. If Γ is not empty, then

(1) $\bigcap_{H\in\Gamma} Q_H = O_2(\Gamma)$, and $Q_H^* \cap Q_H \leq O_2(\Gamma)$ for all $H \in \Gamma$.

(2) If $f_\Delta(H) < f_\Delta(K)$ for $H, K \in \Delta$, then $Q_H^* \leq Q_K$.

We define the digraph $\mathcal{D}(\otimes)$ whose vertices are all the elements of Ω. Define the directed edge $H \longrightarrow K$ by $H \neq K$ and $Q_H^* \not\leq Q_K$ for $H, K \in \Omega$. An H-K walk is the sequence $H = H_0, H_1, \cdots, H_t = K$, and $H_{i-1} \longrightarrow H_i$ $(1 \leq i \leq t)$. If $H = K$, then it is called a closed walk. If $\{H_i; 1 \leq i \leq t\}$ is a proper subset of Ω, we call it a proper walk.

(2.4) If $H \longrightarrow K$, then $f_\Delta(K) \leq f_\Delta(H)$, where $\Delta = \{H, K\}$.

(2.5) For any $H, K \in \mathcal{D}(\otimes)$, there exists an H-K walk.

(2.6) For $H, K \in \Omega$, if there is a proper closed H-K walk, then

(1) $f_\Delta(H) = f_\Delta(K)$ for any $\Delta \subset \Omega$ that is non-empty and contains no element on the walk.

(2) If $[\Omega_1 Z(Q_H), O^2(H)] \neq 1$, then $[\Omega_1 Z(Q_K), O^2(K)] \neq 1$.

The definition of $N^\infty(S)$ is given in the section 3. Since $O_2(\Omega) = 1$, by (3.1)(4) there exists $K \in \Omega$ with $N^\infty(S) \not\leq Q_K$.

(2.7) Let $H, K \in \Omega$ such that $[\Omega_1 Z(Q_H), O^2(H)] \neq 1$ and $N^\infty(S) \not\leq Q_K$. Then there is no proper closed H-K walk.

(2.8) Let P be the shortest closed H-K walk. Then P has no cross point.

Renumbering if necessary, we may assume that $H_1 \longleftarrow H_2 \longleftarrow \cdots \longleftarrow H_n \longleftarrow H_1$. Moreover, we may assume that there is $m \leq n$ such that $\Omega_1 Z(Q_1) \not\leq Z(H_1)$, $[\Omega_1 Z(Q_i), O^2(H_i)] = 1$ $(2 \leq i \leq m)$, and $N^\infty(S) \not\leq Q_m$. Let $V_1 = \Omega_1 Z(Q_1)$, and let $V_i = V_{i-1}^{H_i}$, $i = 2, 3, \cdots, m$. Take m to be minimal among them.

(2.9) Let $\Omega_i = \Omega - \{H_i\}$. Then $f_{\Omega_i}(H_{i+1}) \leq f_{\Omega_i}(H_{i+2}) \leq \cdots f_{\Omega_i}(H_{i-2}) \leq f_{\Omega_i}(H_{i-1})$ $(1 \leq i \leq n)$.

(2.10) $Q_i Q_i^* Q_{i+1}^* = S$ for all i; $1 \leq i \leq n$.

(2.11) $Q_i^* \leq Q_{i-2}$ and $[V_{i-2}, O^2(H_i)] = 1$ for all i; $3 \leq i \leq m$.

(2.12) $V_i \leq Q_i$ for all i; $1 \leq i \leq m$, and V_m is abelian.

(2.13) $C_S(V_{i-1}) \not\leq Q_i$ for all i; $2 \leq i \leq m$.

(2.14) Let i $(2 \leq i \leq m)$ and $\overline{H}_i = H_i/O_{2,2'}(H_i)$. If $\overline{H}_i$ is simple, then $\Omega_1(\overline{S}) \leq \overline{C_S(V_{i-1})}$.

3. A characteristic subgroup of S.

Let t be an integer. Let S be a finite 2-group, and V, $T \leq S$. Then we write $V \in \mu_t(S,T)$ if V is a T-invariant elementary abelian, and for any $A \leq T$ with $[V, A, A] = 1$ there exist generators $\{v_i; i \in I\}$ of V which depends on A such that $\|[v_i, A]\| \leq 2^t$ for all $i \in I$. We write $V \in \nu_t(S,T)$ if $V \in \mu_t(S,T)$ and $\|[V, a]\| > 2^t$ for all $a \in A - C_A(V)$ with $[V, A, A] = 1$. Define $\nu(S,T) = \bigcup_t \nu_t(S,T)$

Define $N_{-1}(S) = S$, $N_i(S) = \langle \nu(S, N_{i-1}(S)) \rangle$ $(i = 0, 1, \cdots)$. We write $N^\infty(S) = \bigcap_{i\,\mathrm{odd}} N_i(S)$ and

$$N_\infty(S) = \bigcup_{i \text{ even}} N_i(S).$$

Note it is possible that $\nu(S,S) = \emptyset$ and $N^\infty(S) = 1$ (c.f. (3.1)(5)).

(3.1) (1) $N_\infty(S)$ is abelian.

(2) $N^\infty(S) = C_S(N_\infty(S))$.

(3) $N_0(S) \leq N_2(S) \leq \cdots \leq N_\infty(S) \leq N^\infty(S) \leq \cdots \leq N_1(S) \leq N_{-1}(S) = S$.

(4) If $N^\infty(S) \leq T \leq S$, then $N^\infty(T) = N^\infty(S)$.

(5) If $[\Omega_1 Z(Q_H), O^2(H)] \neq 1$ for some $H \in \Omega$, then $\Omega_1 Z(Q_H) \in \nu(S,S)$, and hence $1 \neq N^\infty(S) \leq Q_H$.

The following two results are from [H].

(3.2) Let p be an odd prime. Let H be a finite solvable group with $H = O_{2,p,2}(H)$, $S \in Syl_2(H)$ and $V \in \mu_t(S,S)$ for some integer t. If V^H is abelian, then $V^H \in \mu_{t+1}(S,S)$.

(3.3) Let H be a finite group, $S \in Syl_2(H)$, $V \in \mu_t(S,S)$ for some integer t, and $\overline{H} = H/O_2(H)C_H(V^H)$. Assume that $\overline{H} = E(\overline{H})\overline{S}$. Let $\{\overline{K}_i; 1 \leq i \leq r\}$ be the set of all components of $\overline{H}$. Let $m_* = \max_{1 \leq i \leq r} \{\log_2 |N_{\overline{A}}(\overline{K}_i)/C_{\overline{A}}(\overline{K}_i)|; A$ ranges over all the subgroups of S with $[V^H, A, A] = 1\}$. Let $m = 1$ if $m_* = 0$ and $\overline{S} \neq \bigcap_{i=1}^{r} N_{\overline{S}}(\overline{K}_i)$, and let $m = m_*$ otherwise. If V^H is abelian, then $V^H \in \mu_{t+m}(S,S)$.

4. $GF(2)\overline{H}$-module.

(4.1) Let $H \in \Omega$, let D be a normal subgroup of S, and $\overline{H} = H/Q_H$. Let V be a faithful and irreducible $GF(2)\overline{H}$-module. Let A be an elementary abelian subgroup of S with $[V,A,A] = 0$. Assume that $S = Q_H^* D$ and $\Omega_1(E(\overline{H}) \cap \overline{S}) \leq \overline{D}$.

Then (1) $\|[V,\overline{x}]\| \geq |C_V(\overline{D})|$ for all $\overline{x} \in \overline{S}^\sharp$.

(2) If H is solvable, then $V = \langle v \in V; \|[v,\overline{A}]\| \leq 2\rangle$ and $\|[V,\overline{x}]\| \geq 2^2$ for all $\overline{x} \in \overline{S}^\sharp$.

(3) If $\overline{H} \simeq Sz(2^m)$, then $\|[V,\overline{x}]\| \geq 2^{2m}$ for all $\overline{x} \in \overline{S}^\sharp$ and $|V| \geq |C_V(\Omega_1(\overline{S}))|^2$.

(4) If H is solvable and $|V/C_V(\overline{S})| \leq 2^{3/2} \cdot |C_V(\overline{S})|$, then $\overline{H}$ is a dihedral group.

(5) If H is nonsolvable and $O(\overline{H}) \neq 1$, then $|\overline{A}| \leq 2$, $|C_V(\overline{x})| \geq 2^3 \cdot |C_V(\Omega_1(\overline{S}))|$ and $\|[V,\overline{x}]\| \geq 2^6$ for all $\overline{x} \in \overline{S}^\sharp$.

5. Proof of the theorem.

Let $H \in \Omega$, V be a normal subgroup of H, and $1 = W_0 \leq U_1 < W_1 < \cdots < W_r \leq U_{r+1} = V^H$ be a chain of normal subgroups of H such that W_i/U_i is a non-central chief factor of H and $[U_i, O^2(H)] \leq W_{i-1}$, $1 \leq i \leq r+1$. Define $\delta(V) = \min\{\prod_{i=1}^{r} \|[W_i/U_i, x]\|; x \in S - Q_H\}$.

(5.1) Fix i $(1 \leq i \leq m)$. Let $Z_i = C_{V_i}(O^2(H_i))$ and choose m_i as m in (3.3). Then

(a) $|V_{i+1}/Z_{i+1}| \geq m_i |V_i/Z_i|$.

(b) $\delta(V_i) \geq |V_i/Z_i|$.

(c) $N^\infty(S) \leq Q_i$.

Now we return back to the Hypothesis (H.1) and have that $n = 2$ and $V_1 \not\leq Q_2$. However, we can easily derive a contradiction in this case.

References

[Gl] Glauberman, G. Prime-power factor groups of finite groups, II Math. Z. 117. (1970) 46-56

[H] Hayashi, M. A note on the closure of an elementary abelian 2-subgroup of a finite group, preprint

[St] Stellmacher, B. A characteristic subgroup of Σ_4-free groups, Israel J. Math. 94 (1996) 367-379

Generalized prime graphs と Generalized Burnside rings

Nobuo Iiyori*
Department of Mathematics
Faculty of Education
Yamaguchi University
Yamaguchi, 753-8512
Japan

2000

1 序論

群の構造を調べる上でprime graphは強力な武器であることが分かってきた。prime graphの応用は、多くの研究者達が結果を残している。このprime graphは群指標と密接な関係があることが知られている。最近、prime graphが一般化されそのグラフ(generalized prime graph)を用いて群の構造を調べる試みがなされている。この小文では、generalized prime graphについても、prime graphと似たような事柄が成立することを説明する。

2 Generalized prime graphs

この章において、この小文に必要なgeneralized prime graphについての定義、諸結果を述べる。Gを有限群とし、Pを群論的性質とする。S_PをGのP-部分群全体の族とする。generalized prime graph $\Gamma_P(G)$とは頂点集合VをP-部分群の位数を割る素数の集合であり、$p,q \in V$がつながってるのは、pqがあるP-部分群の位数を割ってるときとする。prime graphは、Pをcyclicとすると得られるグラフである。例えばA_5においてPを可解とするとA_5は、位数1,2,3,4,5,6,10,12の可解部分群があるのでグラフは$3-2-5$のようになる。また単にP-部分群を考えるのではなく、真のP-部分群を考えてできる同様のグラフを$\Gamma_P^*(G)$で表すこととする。この小文においては共役について不変な性質を考える。つまりHがP-部分群であるなら任意の$g \in G$にたいし${}^gH$もまたP-部分群であるような性質である。このような群論的性質は、可換性、羃零性、可解性の他に「p-群である

*iiyori@po.cc.yamaguchi-u.ac.jp

とか」「p'-群であるとか」など色々なものがある。さて　generalized prime graph $\Gamma_P(G)$ にたいしその連結成分を C_P であらわすことにする。

さて generalized prime graph $\Gamma_P(G)$ について次の諸性質は基本的である。
(1)P が可換性のとき $(a)\sharp C_P$ は高々 6 以下である。$(b)\Gamma_P(G)$ は完全グラフではない。
(2)P が可解性のとき $(a)\sharp C_P$ は 1 である。$(b)\Gamma_P(G)$ は完全グラフではない。さらに
(3)P が可換性、巡回性、冪零性については $\Gamma_P(G)$ は同一のグラフになる。

講演のときは (2) の (a) は単純群の分類を用いて確認されていたが、現在は分類を用いない証明が見つかってる。(1) の諸性質についても分類を用いない証明が必要であると筆者は考えているが簡単な問題ではないように感じている。

3　Generaliez prime graphsの応用例

ここでは簡単であるが generalized prime graph の応用例について解説したい。昔から有限群の可解性の特徴づけに関する問題がある。この問題で重要な結果として Hall による次の結果は基本的であり重要なものである。

Theorem 1 G を有限群とする。G の位数を割る素数の集合を $\pi(G)$ とする。任意の $\pi(G)$ の部分集合 π にたいして群 G が *Hall* π-部分群をもつことは、G が可解であるための必要十分条件である。

この結果はすべての $\pi(G)$ の部分集合にたいして群 G が Hall 部分群をもつこと要求してるが、実はこれは条件が強すぎるのであって次のように直すことができる。これは Du の結果である。

Theorem 2 G を有限群とする。G の位数を割る素数の集合を $\pi(G)$ とする。任意の 2 を含む $\pi(G)$ の部分集合 π にたいして群 G が *Hall* π-部分群をもつことは、G が可解であるための必要十分条件である。

Du は上の条件より弱い可解になるための条件を与えているが多少複雑になるので上の形で紹介した。実は上の命題で 2 を含むという条件は 2-可解であるための条件であって素数 p でおきかえると同様な結果がえられる。詳しくは Iiyori[] を参照のこと。この Iiyori の結果に genegralized prime graph が本質的に応用されている。

筆者としてはこのような結果は対応する genegralized prime graph の理論を展開することにより自然に得られるものだと思ってる。

4　Burnside rings and generalized prime graphs

この章においては、prime graph が指標環との関係が一般化されたグラフについても成立することを説明する。ここでの話は、北大での小田氏とのディスカッションで分かったことである。近いうちに論文にまとめる予定である。

私のようなcharacter theoryの非専門家が群論の問題にcharacter theoryを用いようとするとき問題の特徴をいかにcharacterで表現するかを考えだろう。例えば、群論的性質Pについて考察する場合は、ダイレクトにPが反映するようなcharacterを考えることになる。すぐれた手本として、例外指標の理論が挙げられる。いま、generalized prime graphsの指標環的考察を考えているわけであるから、一番簡単なものはP部分群からインジュースされる誘導指標のなす環を考えることであろう。そう考えるとgeneralized prime graphsと表現論を結びつける方法として吉田によるgeneralized Burnside ringがとの関連が出てくる。実際に、先に述べた「Pが可解性のとき$\sharp C_P$は1である。」はこの考えの延長線上で容易にしめせる。

Theorem 3 Gを有限群とする。もし$\Gamma^*_{solvable}(G)$が非連結であれば$G \simeq pq$または$p^n : q$. ここでqのp^nへの作用は、既約である。

以下、Burnside ringsと generalized prime graphs　との関係について簡単に説明する。共役で不変で次の性質を満たす群論的性質Pを以下考える：

$$H, K : P - \text{部分群} \Rightarrow H \cap K : P - \text{部分群}.$$

このとき$\hat{S} = S_P \cup \{G\}$から作られるgeneralized Burnside ring R_Pが我々の考察対象である。generalized prime graphsは位数から部分群同士の関係を考えたものと捉えることができる。このような関係は、次のような素朴な代数$LA_P(G)$で捕まえることができる；$LA_P(G) = \oplus_{H \in S_P(G)} Z[H]$ ここで$[H]$はHに対するシンボルであり積を，$[H][K] = [H \cap K]$ for $H, K \in \hat{S}$によって定義する．このように定義するとp, qがgeneralized prime graphsで連結である条件は$p \in \quad \pi(H), q \in (K), [H][K] \neq [1]$を満たす$H, K$が存在することである。この代数$LA_P(G)$は　素朴にgroup latticeを代数化したものであるが実はgeneralized Burnside ringを部分代数として含んでいる。

Lemma 1 $e_H = 1/|H \cap G| \sum_{a \in G} [{}^a H]$ *for* $H \in \hat{S}$で生成される$LA_P(G)$の部分代数は自然に *generalized Burnside ring* R_Pと同一視できる。

この命題からgeneralized prime graphsはgeneralized Burnside ringの構造を表現するものであることが分かる。

5　今後の課題

前の章で見たようにgeneralized prime graphsとgeneralized Burnside ringは群の作用を持つlatticeからどうようにしてできる代数の研究と捉えることが可能である。実は、またまた素朴な計算で群の作用を持つlatticeからgeneralized Burnside ring見たいな物が得られる。この代数がlatticeのどのような性質を反映したものであるか研究することは群の作用、generalized prime graphsとgeneralized Burnside ringの研究にとって重要であると思う。

A Characterization of a Finite Simple Group by Orders of its Solvable Subgroups

Abe, Seiichi

June 17th 2000

Abstract

A brand new way to characterize a finite simple group is discovered. Some infinite series of non abelian simple groups have turned out to be determined just by each set of orders of solvable subgroups. It is quite obvious to see that the set of orders of solvable subgroups of the alternating group A_5 of degree 5 is $\{1,2,3,4,5,6,10,12\}$. But it is not very easy to see that no other non abelian simple group has such a set as mentioned one. In this paper we will try to answer the question above for any finite simple group and suceeded to do that for some infinite series of non abelian simple groups.

1 Introduction

Five kinds of infinite series of finite simple groups $A_1(q)$, ${}^2B_2(q)$, ${}^3D_4(q)$, $G_2(q)$ ${}^2G_2(q)$ and 26 sporadic simple groups are shown to be determined just by each set of orders of solvable subgroups as described in the main theorem as follows.

Theorem 1 *Let S be a non abelian finite simple group which is isomorphic to one of*

$$A_1(q),\ Sz(q),\ {}^3D_4(q),\ G_2(q),\ {}^2G_2(q).$$

or 26 sporadic simple groups and G be a finite group. If $\mathrm{ord}(\mathcal{S}_{sol}(S))$ *coinsides with* $\mathrm{ord}(\mathcal{S}_{sol}(G))$*, then G is isomorphic to S.*

We can regard this theorem as a kind of characterization of non abelian finite simple group by a set of integers which is determined by two abstract parameter "taking order" and "being solvable". The origin of this consideration is Thompson conjecture and its related problems shown as below.

Conjecture 1 (J. G. Thompson) *Let G be a finite group and S be a non abelian simple group. $N(G)$ stands for the set of sizes of conjugacy classes. If $N(G)$ coinsides with $N(S)$, then G is isomorphic to S.*

Problem 1 *Let G be a finite group and S be a non abelian finite group. $M(G)$ stands for the set of orders of all elements of G. Suppose $M(G)$ coinsides with $M(S)$, then G is isomorphic to S.*

It is clear that the set $N(G)$ is a set of integers which is determined by two abstract parameters "index" and "realized as a centralizer of an element" and that $M(G)$ is determined by "order" and "cyclic". These problems are solved in some cases using prime graphs which we regard a graph determined by the set of orders of cyclic subgroups or by the set of indices of centralizers of each element of a group in question. Now it seems natural to try to seek new couples of parameters instead of "order and cyclic" in order to get another set of integers which would reflect the properties of the group more clearly. Therefore we are going to show an outline of the generalization of prime graphs with some examples, paraphrase of Thompson conjecture and that of the related problems in the same way as the generalization of the prime graphs and known results of these problems . We will also show a generalized Thompson conjecture of which every problem mentioned above would be regarded as a special case. See[1] to go more in detail about this generalization and properties of generalized prime graphs. So we start with a definition of Λ-graph for an arbitrary set of integers Λ.

Definition 1 *For a set Λ of natural numbers, $\Gamma = \Gamma_\Lambda$ denotes the Λ-graph where the set V of vertices of Γ is defined as follows*

$$V = V_\Xi = \{p : prime |\ p|a \text{ for a } \in \Lambda\}.$$

Two vertices p and q are joined to each other in Γ_Λ if and only if there exists an element of Λ which can be divided by $p \times q$.

Ξ stands for a group theoretical property. We can consider a lot of Ξ's like being nilpotent, abelian, cyclic, maximal subgroup of a group and so on.

We put

$$\mathcal{S}_\Xi(G) := \{H \subseteq G | H \text{ is a } \Xi\text{–subgroup of } G\},$$

and let ρ be a mapping of $\mathcal{S}_\Xi(G)$ to $\mathbf{N}$, *that is,*

$$\begin{array}{c} \rho : \mathcal{S}_\Xi(G) \longrightarrow \mathbf{N} \\ (H \longmapsto \rho(H)). \end{array}$$

In this paper we are going to consider the following two mappings:

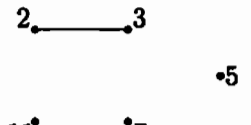
$$\mathrm{ord}(H) = |H|, \qquad \mathrm{ind}(H) = |G : H|.$$

Now note that the image $\rho(\mathcal{S}_\Xi(G))$ of ρ is a set of natural numbers and can be regarded as Λ. So we can define the $\rho(\mathcal{S}_\Xi(G))$-graph for this set. We call it the (ρ, Ξ)-gragh of G or simply the Ξ-graph of G. It can be denoted by

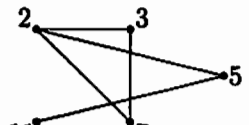
$$\Gamma_{\rho(\mathcal{S}_\Xi(G))} = \Gamma_{(\rho,\Xi)}(G) = \Gamma_\Xi(G).$$

According to the rules above, we can regard the prime gragh $\Gamma(G)$ as a kind of (ρ, Ξ)-gragh where ρ is ord and Ξ stands for cyclic, which is denoted by $\Gamma_{\rho(\mathcal{S}_\Xi(G))}$. So a prime graph $\Gamma(G)$ can sometimes be called an (ord, *cyclic*)-graph or simply a *cyclic*-graph, which are denoted by $\Gamma_{(\mathrm{ord},cyc)}(G), \Gamma_{cyc}G$ respectively.

Let us see some concrete examples of (ρ, Ξ)-graphs.

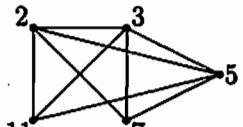


$\Gamma_{(\mathrm{ord},cyc)}(M_{22})$



$\Gamma_{(\mathrm{ord},sol)}(M_{22})$

The existence of the edge between 2 and 3 in $\Gamma_{(\mathrm{ord},sol)}(M_{22})$ tells us that M_{22} has a solvable subgroup whose order can be divided by 2×3. The rest of edges of this graph give us similar informations.



$\Gamma_{(\mathrm{ind},max)}(M_{22})$

Now we can see Thompson conjecture from a higher place. At this point, we are able to rewrite the conjecture and related problems as follows. We let that Ξ_1 stands for "cyclic" and that a subgroup H of G is said to be a Ξ_2-group if H is realized as a centralzer of some elements of G. From now, we will suppose that G is a finite group and S is a non abelian finite simple group.

Problem 2 (Thompson) *Let* $Z(G) = 1$.
If $\mathrm{ind}(\mathcal{S}_{\Xi_2}(S))$ *coincides with* $\mathrm{ind}(\mathcal{S}_{\Xi_2}(G))$, *then* S *is isomorphic to* G.

This problem is solved for some group S. The following theorem is one of the answers.

Theorem 2 (Cheng) *Let* $\mathrm{ind}(\mathcal{S}_{\Xi_2}(S))$ *coincides with* $\mathrm{ind}(\mathcal{S}_{\Xi_2}(G))$. *If the number of connected components of* (ord, cyc)*-graph* $\Gamma_{(\mathrm{ord},cyc)}(S)$ *of* G *is greater than or equal to* 3, *then* S *is isomorphic to* G.

Problem 3 *If* $\mathrm{ord}(\mathcal{S}_{\Xi_1}(S))$ *coincides with* $\mathrm{ord}(\mathcal{S}_{\Xi_1}(G))$, *then* S *is isomorphic to* G.

An answer to the question above for two infinite series of non abelian simple groups is the following theorem.

Theorem 3 (Shi-Deng) *Let* S *is isomorphic to* $Sz(q)$ *or* $PSL_2(q)(q \neq 9)$.
If $\mathrm{ord}(\mathcal{S}_{cyc}(S))$ *coincides with* $\mathrm{ord}(\mathcal{S}_{cyc}(G))$, *then* S *is isomorphic to* G.

Now we have come to the level to generalize all these problems as follows.

Problem 4 (Abe-Iiyori) *For which pair* (ρ, Ξ), *does the fact* $\rho(\mathcal{S}_{\Xi}(S)) = \rho(\mathcal{S}_{\Xi}(G))$ *imply that* G *is isomorphic to* S*?*

We get the main theorem as an answer to the question which is discribed as the following problem.

Problem 5 *Let* S *be a non abelian simple group and* G *be a finite group. If* $\mathrm{ord}(\mathcal{S}_{sol}(S))$ *coinsides with* $\mathrm{ord}(\mathcal{S}_{sol}(G))$, *then is* G *isomorphic to* S *?*

2 GKS-series and Regular Primes

We already have several theorems which stand for properties of a solvable graphs. See Abe-Iiyori[1]. But it is not enough to see such theorems in order to investigate the structure of a group. Now we need propositions that would combine the properties of a solvable graph and the structure of the group like the following lemmas.

Lemma 1 [1] *Let* G *be a group,* H *a subgroup of* G *and* N *a normal subgroup of* G.
(1) *If* p *and* q *are not joined in* $\Gamma_{(\mathrm{ord},sol)}(G)$ *for* $p, q \in \pi(H)$, *then* p *and* q *are not joined in* $\Gamma_{(\mathrm{ord},sol)}(H)$.
(2) *For* $p \in \pi(N)$ *and* $q \in \pi(G) - \pi(N)$, p *and* q *are joined in* $\Gamma_{(\mathrm{ord},sol)}(G)$.

(3) *If p and q are not in $\Gamma_{(\mathrm{ord},sol)}(G)$ for $p, q \in \pi(G/N)$, then p and q are not joined in $\Gamma_{(\mathrm{ord},sol)}(G/N)$.*

Lemma 2 [1] *Let G be a finite group and p and q be members of $\pi(G)$ which are not joined in $\Gamma_{(\mathrm{ord},sol)}(G)$ if and only if there exists a series of normal subgroups of G*

$$G \trianglerighteq N \trianglerighteq M \trianglerighteq 1 \cdots\cdots\cdots (*),$$

such that G/N and M are $\{p,q\}'-$groups and N/M is a non abelian simple group such that p and q are not joined in $\Gamma_{(\mathrm{ord},sol)}(N/M)$.

We call the series $(*)$ of normal subgroups of G a GKS-series and also call the situation in the lemma that p and q are expressed to be disjoined by a GKS-series $(*)$.

In order to get deeper information about the structure of G. We need GKS-series that hold every pair of primes of $\pi(G)$. So we are going to pay special attention to a prime that is joined to any primes of the graph. We call such a prime a regular prime.

Definition 2 *Let p be a vertex of the $\Gamma_{(\rho,\Xi)}(G)$ for a group G. p is said to be regular if and only if p is joined to any other vertices in the graph.*

We denote the set of regular primes by $\mathrm{Reg}_{(\rho,\Xi)}(G)$. Following lemmas tell us that the number of $\mathrm{Reg}_{(\mathrm{ord},sol)}(G)$ is closely related to the structure of G.

For example, 2, 3 and 5 are regular primes in $\Gamma_{(\mathrm{ind},max)}(M_{22})$, and we can see that each of $\Gamma_{(\mathrm{ord},cyc)}(M_{22})$ and $\Gamma_{(\mathrm{ord},sol)}(M_{22})$ has no regular primes. *that is,*

$$\mathrm{Reg}_{(\mathrm{ind},max)}(M_{22}) = \{2,5\}, \quad \text{and}$$
$$\mathrm{Reg}_{(\mathrm{ord},cyc)}(M_{22}) = \mathrm{Reg}_{(\mathrm{ord},sol)}(M_{22}) = \emptyset.$$

Lemma 3 *If $\mathrm{Reg}_{(\mathrm{ord},sol)}(G) = \emptyset$, then G is a non abelian simple group.*

For a graph Γ, Γ^c is said to be a complementary graph if and only if the set of vertices of Γ and Γ^c coinside with each other and two vertices p and q of Γ^c are joined in Γ^c if and only if p and q are not joined in Γ.

Let Λ be a set of positive integers and Λ_0 be its subset. Note that $\Gamma_\Lambda - \Lambda_0$ stands for a subgraph of Γ_Λ whose vertices set is $\Lambda - \Lambda_0$. Any two members p and q of $\Lambda - \Lambda_0$ are joined in $\Gamma_\Lambda - \Lambda_0$ if p and q are joined in Γ_Λ.

Lemma 4 *If the number of connected components of*

$$\Gamma^{rc}(G) = (\Gamma_{(ord,sol)}(G) - \mathrm{Reg}_{(ord,sol)}(G))^c$$

equals n, then at most n GKS-series of G is neccessary to express any pair of vertices of $\Gamma_{(ord,sol)}(G)$ *to be disjoined.*

References

[1] Abe, S. and Iiyori, N., *A generalization of prime graphs of finite groups.* Hokkaido Math. J. **143** (2000) 391-407.

[2] Conway, J. H. and *et al*, *Atlas of Finite Groups*, Oxford Univ. Press(Cleandon), London/New York 1985.

[3] Brandl, R. and Shi, W., *Finite groups whose element orders are consecutive integer.* J. Algebra **143** (1991), 388-400.

[4] Cater, R. *Simple groups of Lie type.* John Wiely & Sons, London-New York-Sydney-Toronto, 1989.

[5] Chang, B., *The conjugate classes of Chevalley groups of type* (G_2). J. Algebra **9**(1968), 190-211

[6] Deriziotis, D., *The centralizers of semi-simple elements of the Chevalley groups* E_7 *and* E_8. Tokyo J. Math. **6** (1983), 191-216.

[7] Enomoto, H., *The conjugacy classes of Chevalley groups of type* (G_2) *over finite fields of characteristic* 2 *or* 3. J. Fac. Sci. Univ. Tokyo **16**(1970), 497-512.

[8] Kleidman, P. B., *The maximal subgroups of the Steinberg trialiy groups* ${}^3D_4(q)$ *and their automorphism groups.* J. Algebra **115** (1988), 182-199.

[9] Suzuki, M., *On a class of doubly transitive groups.* Ann. of Math. **75** (1962), 105-145.

[10] Suzuki, M., *Group Theory I, II.* Springer, Berlin-Heidelberg- New York, 1982.

[11] Williams, J. S., *Prime graph components of finite groups.* J. Algebra **69** (1981), 487-513.

p-adic Properties of the Frobenius Numbers of Symmetric Groups

Yugen Takegahara (竹ヶ原　裕元)
Muroran Institute of Technology (室蘭工業大学)

1 Introduction

Let A be a finitely generated group, and let $h_n(A)$ be the number of homomorphisms from A to the symmetric group S_n on n letters. Put $h_0(A) = 1$. Define

$$E_A(X) = \sum_{n=0}^{\infty} \frac{h_n(A)}{n!} X^n,$$

$$\varphi_A(X) = \sum_{|A:B|<\infty} \frac{X^{|A:B|}}{|A:B|},$$

where the summation $\sum_{|A:B|<\infty}$ runs over all subgroups B of finite index $|A:B|$ in A. In [14], Wohlfahrt proved that

$$E_A(X) = \exp(\varphi_A(X)). \tag{1}$$

Let p be a prime, and let C_{p^l} be a cyclic group of order p^l. We have

$$h_n(C_p) = \sharp\{x \in S_n | x^p = 1\} = \sum_{i=0}^{[n/p]} \frac{n!}{p^i i!(n-pi)!},$$

which yields the formula (1) in the case where $A = C_p$:

$$E_{C_p}(X) = \exp\left(X + \frac{X^p}{p}\right).$$

This formula is equivalent to the recurrence formula

$$h_n(C_p) = h_{n-1}(C_p) + \frac{(n-1)!}{(n-p)!} h_{n-p}(C_p).$$

(See also [3, 14].) The formal power series $E_{C_p}(X)$ arises from another situation as well. Let Γ_p denote Morita p-adic gamma function [13, VII, 1.1] [9, pp. 88-91], and let

$$\Gamma_p(x+1) = \sum_{k \geq 0} a_k \binom{n}{k}$$

be the Mahler series of Γ_p [13, IV, 2.3]. Then its coefficients satisfy the following identity [13, VII, 1.4]:

$$\sum_{k\geq 0}(-1)^{k+1}a_k\frac{X^k}{k!}=\frac{1-X^p}{1-X}\exp\left(X+\frac{X^p}{p}\right).$$

The property of $h_p(C_p)$ is known as Wilson's Theorem :

$$h_p(C_p)=1+(p-1)!\equiv 0 \bmod p.$$

The following theorem is due to Frobenius (see [7, Theorem 9.1.1]).

Frobenius Theorem *The number of elements x in a finite group G that satisfy the equation $x^d=1$ is a multiple of* $\gcd(d,|G|)$.

Frobenius Theorem implies that, for all $n\geq p$,

$$h_n(C_p)\equiv 0 \bmod p.$$

For each real number x, $[x]$ denotes the largest integer not exceeding x, and, for each nonzero integer x, $\mathrm{ord}_p(x)$ denotes the exponent of p in the decomposition of x into prime factors. Using the preceding recurrence formula, Chowla, Herstein, and Moore proved that $\mathrm{ord}_2(h_n(C_2))\geq[(n+2)/4](=[n/2]-[n/4])$ [2, Theorem 10]. Furthermore, it was proved in [4, 5, 6, 10] that

$$\mathrm{ord}_p(h_n(C_p))\geq\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right].$$

Example 1.1 ([4, 10, 11]) Suppose that $p=2$. Then

$$\mathrm{ord}_2(h_n(C_2))=\begin{cases}\left[\frac{n}{2}\right]-\left[\frac{n}{4}\right]+1 & \text{if } n\equiv 3 \bmod 4,\\ \left[\frac{n}{2}\right]-\left[\frac{n}{4}\right] & \text{otherwise.}\end{cases}$$

Example 1.2 ([4, 11]) Suppose that $p=3$. Then

$$\mathrm{ord}_3(h_n(C_3))\geq\left[\frac{n}{3}\right]-\left[\frac{n}{9}\right]+3 \quad \text{if } n\equiv 24 \bmod 27,$$

$$\mathrm{ord}_3(h_n(C_3))=\begin{cases}\left[\frac{n}{3}\right]-\left[\frac{n}{9}\right]+2 & \text{if } n\equiv 6 \bmod 27 \text{ or if } n\equiv 15 \bmod 27,\\ \left[\frac{n}{3}\right]-\left[\frac{n}{9}\right]+1 & \text{if } n\equiv 4 \bmod 9 \text{ or if } n\equiv 7 \bmod 9,\\ \left[\frac{n}{3}\right]-\left[\frac{n}{9}\right] & \text{otherwise.}\end{cases}$$

In this paper, we will give some properties of $h_n(C_{p^l}\times C_{p^m})$, where l and m are integers with $l\geq m\geq 0$.

2 Cyclic groups

Let l be a nonnegative integer. It follows from the formula (1) that

$$E_{C_{p^l}}(X) = \left(\sum_{k=0}^{l} \frac{1}{p^k} X^{p^k}\right).$$

The p-adic power series

$$E_p(X) = \exp\left(\sum_{k=0}^{\infty} \frac{1}{p^k} X^{p^k}\right)$$

is called the Artin-Hasse exponential. The important property of $E_p(X)$ is that

$$E_p(X) \in \mathbb{Z}_p[[X]] \tag{2}$$

(see [13, VII, 2.2] and [9, p. 93]), where $\mathbb{Z}_p$ is the ring of p-adic integers. Frobenius Theorem yields this property (see Section 5). The property (2) plays an important role in the proof of the following theorem. For each nonnegative integer n, put

$$f_p^l(n) = \sum_{j=1}^{l} \left[\frac{n}{p^j}\right]$$

if $l \geq 1$, and $f_p^0(n) = 0$.

Theorem 2.1 ([10]) *Let $y_n = [n/p^{l+1}]$ for each nonnegative integer n. Then*

$$\mathrm{ord}_p(h_n(C_{p^l})) \geq f_p^l(n) - l y_n,$$

and equality holds for each n with $n \equiv 0 \bmod p^{l+1}$. Furthermore,

$$h_n(C_{p^l}) \equiv \frac{(-1)^{y_n} n!}{p^{(l+1)y_n} y_n! (n - p^{l+1} y_n)!} h_{n-p^{l+1}y_n}(C_{p^l}) \bmod p^{f_p^l(n) - l y_n + l + 1}.$$

For a nonnegative integer $n = n_0 + n_1 p + n_2 p^2 + \cdots$ with $n_0, n_1, n_2, \ldots$ are nonnegative integers less than p,

$$\mathrm{ord}_p(n!) = \frac{n - n_0 - n_1 - n_2 - \cdots}{p-1} = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right].$$

Furthermore, we have

$$\mathrm{ord}_p\left(\frac{n!}{p^{(l+1)y_n} y_n!}\right) = f_p^l(n) - l y_n,$$

where $y_n = [n/p^{l+1}]$. Also, by (2), $h_{n-p^{l+1}y_n}(C_{p^l})/(n - p^{l+1}y_n)! \in \mathbb{Z}_p$. Hence the second assertion of Theorem 2.1 yields the first one.

Corollary 2.2 ([10]) *The p-adic power series $E_{C_{p^l}}(X)$ converges only in the open disc of radius $r = p^{\mathrm{ord}_p(r)}$ where*

$$\mathrm{ord}_p(r) = -\frac{1}{p^l(p-1)} - \frac{l}{p^{l+1}}.$$

Remark 2.3 The Artin-Hasse exponential $E_p(X)$ converges only in the open disc of radius 1.

Let $\mathbb{Z}_p\langle X\rangle$ denote the set of formal power series with $\mathbb{Z}_p$-coefficients which tend to 0. Take a formal power series $f(X) = \sum_{j=0}^{\infty} f_j X^j \in \mathbb{Z}_p[[X]]$. For a positive integer k, let $f_{\bmod p^k}(X) = \sum_{j=0}^{\infty} \bar{f}_j X^j$, where $\bar{f}_j = f_j p^k \mathbb{Z}_p \in \mathbb{Z}_p/p^k\mathbb{Z}_p$. By the definition of $\mathbb{Z}_p\langle X\rangle$, the following conditions are equivalent:

(1) $f(X) \in \mathbb{Z}_p\langle X\rangle$;

(2) for any positive integer k, $f_{\bmod p^k}(X)$ is a polynomial in X with $\mathbb{Z}_p/p^k\mathbb{Z}_p$ coefficient;

(3) $f(X)$ converges for $|x|_p \leq 1$.

Let r be an integer with $0 \leq r < p^{l+1}$. Recently K. Conrad proved the following theorems.

Theorem 2.4 *If $l(p-1) \geq 2$, then there exists some $f(X) \in \mathbb{Z}_p\langle X\rangle$ such that*

$$f(y) = \frac{h_{p^{l+1}y+r}(C_{p^l})}{(p^{l+1}y+r)!}(-p^{l+1})^y y!$$

for each nonnegative integer y. If $p = 2$ and $l = 1$, then there exists some $g(X) \in \mathbb{Z}_p\langle X\rangle$ such that

$$g(y) = \frac{h_{4y+r}(C_2)}{(4y+r)!}4^y y!$$

for each nonnegative integer y.

Theorem 2.5 *If $\mathrm{ord}_p(h_r(C_{p^l})) - f_p^l(r) \leq l+1$ and if either $\mathrm{ord}_p(h_r(C_{p^l})) - f_p^l(r) \neq l+1$ or*

$$\mathrm{ord}_p\left(\frac{h_r(C_{p^l})}{p^{l+1}r!} + \frac{h_{p^{l+1}+r}(C_{p^l})}{(p^{l+1}+r)!}\right) \neq 0,$$

then

$$\mathrm{ord}_p(h_{p^{l+1}y+r}(C_{p^l})) = f_p^l(p^{l+1}y) - ly + \mathrm{ord}_p(h_r(C_{p^l}))$$

for each nonnegative integer y. If $\mathrm{ord}_p(h_r(C_{p^l})) - f_p^l(r) = l+1$ and if

$$\mathrm{ord}_p\left(\frac{h_r(C_{p^l})}{p^{l+1}r!} + \frac{h_{p^{l+1}+r}(C_{p^l})}{(p^{l+1}+r)!}\right) = 0,$$

then there exists $\alpha \in \mathbb{Z}_p - \{0\}$ *such that*

$$\mathrm{ord}_p(h_{p^{l+1}y+r}(C_{p^l})) = f_p^l(p^{l+1}y) - ly + \mathrm{ord}_p(h_r(C_{p^l})) + \mathrm{ord}_p(y-\alpha)$$

for each nonnegative integer y.

For Theorem 2.5, see also [10, 11].

3 The direct product of two cyclic groups

Hereafter, let $P = C_{p^l} \times C_{p^m}$, where l and m are integers with $l \geq m \geq 0$. Let G be a finite group, and let $G^{(n)}$ be the direct product of n copies of G. The wreath product $G \wr S_n$ is the semidirect product of $G^{(n)}$ and S_n; the product of two elements of $G \wr S_n$ is defined by

$$(g_1, g_2, \ldots, g_n)\sigma \cdot (g_1', g_2', \ldots, g_n')\tau = (g_1 g'_{\sigma^{-1}(1)}, g_2 g'_{\sigma^{-1}(2)}, \ldots, g_n g'_{\sigma^{-1}(n)})\sigma\tau.$$

Let d be a nonnegative integer. We denote by C_d a cyclic group of order d. Define $h(C_d, G) = \{x \in G | x^d = 1\}$ and $h_n(C_d; G) = h(C_d, G \wr S_n) = \{x \in G \wr S_n | x^d = 1\}$.

For a permutation $\sigma \in S_n$ that factorizes i disjoint cycles of order p^{l+1}, the centralizer of σ in S_n is isomorphic to $(C_{p^{l+1}} \wr S_i) \times S_{n-p^{l+1}i}$ (see [8, 4.1.19]). Hence

$$h_n(C_{p^{l+1}} \times C_{p^m}) = \sum_{i=0}^{y_n} \frac{n!}{p^{(l+1)i} i!(n-p^{l+1}i)!} h_i(C_{p^m}; C_{p^{l+1}}) h_{n-p^{l+1}i}(P), \tag{3}$$

where $n!/(p^{(l+1)i} i!(n-p^{l+1}i)!)$ is the number of permutations that factorize i distinct cycles of order p^{l+1} in S_n (see [8, 1.2.15]). Define

$$E_{C_d}(X; G) = \sum_{n=0}^{\infty} \frac{h_n(C_d; G)}{|G|^n n!} X^n.$$

The formula (3) is expressed as the following.

Theorem 3.1 *We have*

$$E_{C_{p^{l+1}} \times C_{p^m}}(X) = E_P(X) E_{C_{p^m}}(X^{p^{l+1}}; C_{p^{l+1}}).$$

Let $\{d_0, d_1, \ldots\}$ be the set consisting of all divisors of d. We obtain

$$\begin{aligned} h_n(C_d; G) &= \sum_{j_0 d_0 + j_1 d_1 + \cdots = n} \frac{n!}{\prod_{k\geq 0} d_k^{j_k} j_k!} \prod_{k\geq 0} |G|^{(d_k-1)j_k} h(C_{d/d_k}, G)^{j_k} \\ &= \sum_{j_0 d_0 + j_1 d_1 + \cdots = n} \frac{|G|^n n!}{\prod_{k\geq 0} d_k^{j_k} j_k!} \prod_{k\geq 0} \frac{h(C_{d/d_k}, G)^{j_k}}{|G|^{j_k}}, \end{aligned} \tag{4}$$

where the summation runs over all sequences $(j_0, j_1, \ldots)$ of nonnegative integers with $j_0 d_0 + j_1 d_1 + \cdots = n$ (see also [8, 4.2.10]).

Let $\delta = 1$ if either $p > 2$ or $m = 0$, and $\delta = 0$ otherwise. By using (4), we have the following.

Lemma 3.2 *For positive integers e and i, if $e > m$, then*

$$h_i(C_{p^m}; C_{p^e}) \equiv p^{mi} \bmod p^{mi+e-m-1+\delta},$$

and $\mathrm{ord}_p(h_i(C_{p^m}; C_{p^e})) \geq mi$.

To get the properties of $h_n(P)$, we use the following theorem due to Yoshida [15].

Yoshida's Theorem *The number of homomorphisms from a finite abelian group A to a finite group G is a multiple of* $\gcd(|A|, |G|)$.

In the case where A is cyclic, this theorem is Frobenius Theorem.

If $n < p^{l+1}$, then the order of each cycle in S_n is less than p^{l+1}. Hence Yoshida's Theorem yields the following.

Lemma 3.3 *If $n < p^{l+1}$, then $h_n(P) = h_n(C_{p^{l+u}} \times C_{p^m})$ for any nonnegative integer u, and*

$$\mathrm{ord}_p\left(\frac{h_n(P)}{n!}\right) \geq 0.$$

By using the formula (3), Lemmas 3.2 and 3.3, we can prove the following generalization of Theorem 2.1.

Theorem 3.4 ([10]) *Let $y_n = [n/p^{l+1}]$ for each nonnegative integer n. Then*

$$\mathrm{ord}_p(h_n(P)) \geq f_p^l(n) - (l-m)y_n,$$

and, excepting the case where $p = 2$ and $l = m \geq 1$, equality holds for each n with $n \equiv 0 \bmod p^{l+1}$. Furthermore,

$$h_n(P) \equiv \frac{(-1)^{y_n} n!}{p^{(l-m+1)y_n} y_n!(n - p^{l+1}y_n)!} h_{n-p^{l+1}y_n}(P) \bmod p^{f_p^l(n)-(l-m)y_n+l-m+\delta}.$$

4 p-adic properties

We will give a generalization of Theorem 2.4. For each positive integer u, Theorem 3.1 yields

$$E_{C_{p^{l+u}} \times C_{p^m}}(X) = E_P(X) \prod_{i=0}^{u-1} E_{C_{p^m}}(X^{p^{l+i+1}}; C_{p^{l+i+1}}). \tag{5}$$

Let r be an integer with $0 \le r < p^{l+1}$. By the equations (4) and (5), we obtain

$$\begin{aligned}\frac{h_{p^{l+1}j+r}(C_{p^{l+u}} \times C_{p^m})}{(p^{l+1}j+r)!} = & \sum_{y=0}^{j} \frac{h_{p^{l+1}y+r}(P)}{(p^{l+1}y+r)!} \\ & \times \sum_{\sum_{i=0}^{u-1}\sum_{k=1}^{m} j_k p^{i+k} = j-y} \prod_{i=0}^{u-1}\prod_{k=0}^{m} \frac{(p^{m-k})^{j_k}}{(p^{k+l+i+1})^{j_k} j_k!}.\end{aligned} \tag{6}$$

Here Lemma 3.3 implies that, for a sufficiently large u,

$$\frac{h_{p^{l+1}j+r}(C_{p^{l+u}} \times C_{p^m})}{(p^{l+1}j+r)!} = \frac{h_{p^{l+1}j+r}(C_{p^{l+u+1}} \times C_{p^m})}{(p^{l+1}j+r)!} = \cdots,$$

and this is p-adic integer which we denote by $c^{(m)}(p^{l+1}j+r)$. By the equation (6), we conclude that

$$\sum_{j=0}^{\infty} c^{(m)}(p^{l+1}j+r)X^j = \left(\sum_{y=0}^{\infty} \frac{h_{p^{l+1}y+r}(P)}{(p^{l+1}y+r)!}X^y\right) \prod_{i=0}^{+\infty}\prod_{k=0}^{m} \exp\left(\frac{p^{m-k}}{p^{k+l+i+1}}X^{p^{i+k}}\right). \tag{7}$$

Definition 4.1 For each integer x, let $(x)_p = \sum_{j=0}^{x-1} p^j$ if $x \ge 1$, and $(x)_p = 0$ otherwise. Define a sequence of rational number $b(0), b(1), b(2), \ldots$ by

$$\sum_{n=0}^{\infty} \frac{b(n)}{n!}X^n = \exp\left(-\sum_{i=0}^{\infty} \frac{(m+1)_p - (m-i)_p}{p^{l+i+1}}(-p^{l-m+1})^{p^i}X^{p^i}\right).$$

The formula (7) implies that

$$\begin{aligned}& \sum_{y=0}^{\infty} \frac{h_{p^{l+1}y+r}(P)}{(p^{l+1}y+r)!}(-p^{l-m+1})^y X^y \\ = & \left(\sum_{j=0}^{\infty} c^{(m)}(p^{l+1}j+r)(-p^{l-m+1})^j X^j\right) \sum_{n=0}^{\infty} \frac{b(n)}{n!}X^n.\end{aligned} \tag{8}$$

The formula (8) yields the following.

Lemma 4.2 *We have*

$$\frac{h_{p^{l+1}y+r}(P)}{(p^{l+1}y+r)!}(-p^{l-m+1})^y y! = \sum_{j=0}^{y} c^{(m)}(p^{l+1}j+r)(-p^{l-m+1})^j \frac{y!}{(y-j)!}b(y-j)$$

for each nonnegative integer y.

K. Conrad introduced these methods in the case where $m = 0$.
The main theorem is the following.

Theorem 4.3 *Assume that* $(l-m)(p-1) \geq 2$. *If* $p = 2$, *assume that either* $l \geq m+3$, *or else* $m = 0$. *Then there exists some* $f(X) \in \mathbb{Z}_p\langle X \rangle$ *such that*

$$f(y) = \frac{h_{p^{l+1}y+r}(C_{p^l} \times C_{p^m})}{(p^{l+1}y+r)!}(-p^{l-m+1})^y y!$$

for each nonnegative integer y.

The following proposition, together with Lemma 4.2, yields Theorem 4.3.

Proposition 4.4 *Under the assumption of Theorem* 4.2, *there exists some* $\tilde{b}(X) \in \mathbb{Z}_p\langle X \rangle$ *such that* $b(y) = \tilde{b}(y)$ *for each nonnegative integer* y.

5 The Wohlfahrt formula

It is easy to show that the number $m_P(p^k)$ of subgroups of order p^k in P is given by

$$m_P(p^k) = \begin{cases} (k+1)_p & \text{if } 0 \leq k < m, \\ (m+1)_p & \text{if } m \leq k \leq l, \\ (l+m-k+1)_p & \text{if } l < k \leq l+m. \end{cases}$$

Hence

$$\varphi_P(X) = \sum_{k=-\infty}^{m-1} \frac{(k+1)_p}{p^k} X^{p^k} + \sum_{k=m}^{l} \frac{(m+1)_p}{p^k} X^{p^k} + \sum_{k=l+1}^{+\infty} \frac{(l+m-k+1)_p}{p^k} X^{p^k}.$$

We will explain Theorem 3.1, Lemma 3.3, and the formula (8) by using the Wohlfahrt formula

$$E_P(X) = \exp(\varphi_P(X)).$$

The formula (4) yields the following.

Theorem 5.1 ([1, 12]) *Let* d *be a positive integer, and let* $\{d_0, d_1, \ldots\}$ *be the set consisting of all divisors of* d. *For any finite group* G,

$$E_{C_d}(X; G) = \exp\left(\sum_{k \geq 0} \frac{h(C_{d/d_k}, G)}{|G| d_k} X^{d_k}\right).$$

First, using this theorem, we have

$$\begin{aligned} E_{C_{p^{l+1}} \times C_{p^m}}(X) &= E_P(X) \exp\left(\sum_{k=l+1}^{l+m+1} \frac{p^{l+m+1-k}}{p^k} X^{p^k}\right) \\ &= E_P(X) E_{C_{p^m}}(X^{p^{l+1}}; C_{p^{l+1}}). \end{aligned}$$

This proves Theorem 3.1. Next, the p-adic power series

$$E_p^{(m)}(X) = \exp\left(\sum_{k=-\infty}^{m-1} \frac{(k+1)_p}{p^k} X^{p^k} + \sum_{k=m}^{+\infty} \frac{(m+1)_p}{p^k} X^{p^k}\right)$$

has p-adic integer coefficients (see also [9, p. 97, Exercise 18]). This fact is equivalent to Lemma 3.3, because

$$E_p^{(m)}(X) = \sum_{n=0}^{\infty} c^{(m)}(n) X^n.$$

In particular, Frobenius Theorem yields $E_p(X) \in \mathbb{Z}[[X]]$. Finally, the Wohlfahrt formula implies that

$$E_P(X) = E_p^{(m)}(X) \exp\left(-\sum_{i=0}^{\infty} \frac{(m+1)_p - (m-i)_p}{p^{l+i+1}} X^{p^{l+i+1}}\right).$$

This fact yields (8).

References

[1] N. Chigira, The solutions of $x^d = 1$ in finite groups, *J. Algebra* **180** (1996), 653–661.

[2] S. Chowla, I. N. Herstein, and W. K. Moore, On recursions connected with symmetric groups I, *Canad. J. Math.* **3** (1951), 328-334.

[3] S. Chowla, I. N. Herstein, and W. R. Scott, The solutions of $x^d = 1$ in symmetric groups, *Norske Vid. Selsk.* **25** (1952), 29–31.

[4] A. W. M. Dress and T. Yoshida, On p-divisibility of the Frobenius numbers of symmetric groups, 1991, preprint.

[5] B. Dwork, A note on the p-adic gamma function, *Groupe d'étude d'Analyse ultramétrique* 9e année, 1981/82, Exp. No. J5, 10 pp.

[6] M. Grady and M. Newman, Residue periodicity in subgroup counting functions, in: The Rademacher Legacy to Mathematics, *Contemp. Math.* **166** (1994) 265-273.

[7] M. Hall, Jr., "The Theory of Groups," 2nd ed., Chelsea, New York, 1976.

[8] G. D. James and A. Kerber, "The Representation Theory of the Symmetric Group," Encyclopedia of mathematics and its applications, Vol. 16, Addison-Wesley, Reading, MA, 1981.

[9] N. Koblitz, "p-adic Numbers, p-adic Analysis, and Zeta-Functions," 2nd ed., Springer–Verlag, New York, 1984.

[10] H. Katsurada, Y. Takegahara, and T. Yoshida, The number of homomorphisms from a finite abelian group to a symmetric group, *Comm. Algebra* **28** (2000), 2271-2290.

[11] H. Ochiai, A p-adic property of the Taylor series of $\exp(x + x^p/p)$, *Hokkaido Math. J.* **28** (1999), 71-85.

[12] S. Okada, Wreath products by the symmetric groups and product posets of Young's lattices, *J. Combin. Theory Ser. A* **55** (1990), 14-32

[13] A. Robert, "A Course in p-adic Analysis," Springer–Verlag, New York, 2000.

[14] K. Wohlfahrt, Über einen Satz von Dey und die Modulgruppe, *Arch. Math. (Basel)* **29** (1977), 455–457.

[15] T. Yoshida, $|\mathrm{Hom}(A, G)|$, *J. Algebra* **156** (1993), 125–156.

ON IMPRIMITIVE BLOCKS OF A QUASI-THIN ASSOCIATION SCHEME

MITSUGU HIRASAKA AND MIKAHIL MUZYCHUK

ABSTRACT. Let (X, R) be an association scheme in the sense of P.H. Zieschang where X is a finite set and R is a partition of $X \times X$. We say that (X, R) is *quasi-thin* if each element of R is of valency at most two. Assume now that (X, R) is a quasi-thin scheme with $|X| = 4p$ where p is a prime number. The summarized version of our results is the following: If the automorphism group of (X, R) is intransitive, then $p = 7$.

1. INTRODUCTION

In [5] we started to investigate directed graphs of valency two which could be a relation of an association scheme, and proved that a quasi-thin scheme has an automorphism group acting transitively on each equivalence class induced by its thin residue (see Section 2). We noted here that each thin closed subset can be identified with a finite group (see [7]). Since the quotient over the thin residue is thin, it must be important to consider a way to extend the equivalence classes induced by the thin residue to the whole with the aid of a finite group. The authors were trying to get the affirmative answer for the statement that each quasi-thin scheme has a transitive automorphism group. The authors believed that the above statement is true for general quasi-thin schemes. But, it was in February of 2000 when the authors received an e-mail ¿from A. Hanaki to inform the existence of a quasi-thin scheme whose automorphism group is intransitive. The example was found on the way to classify association schemes with 28 points.

Theorem 1.1 (A. Hanaki, I. Miyamoto). *The No.*176 *listed in* `http://kissme.shinshu-u.ac.jp/as/data/as28` *is a quasi-thin association scheme whose automorphism group is intransitive.*

This result gave the authors a huge impact and inspired them so much. In this paper we deal with quasi-thin closed subsets, and obtain that each quasi-thin scheme with $4p$ points has a transitive automorphism group except of the scheme given in Theorem 1.1 where p is a

Date: August 28, 2000.

As descried in Introduction, this paper owes much to be motivated to proceed further by the communication with Hanaki and Miyamaoto. The authors would like to express the deepest gratitude to them.

prime number (see Theorem 4.1). Theorem 4.1 was motivated from the enumeration by A. Hanaki and I. Miyamoto, and obtained as a corollary of the following results: Lemma 3.1; Proposition 3.3; Proposiotion 3.5; Proposition 3.4.

2. Preliminaries

Following [7] we give the notation about association schemes. Let X be a finite set. We shall denote the diagonal relation of $X \times X$ by 1_X. Given $r \subset X \times X$ and $z \in X$, we set

$$r^* := \{(x,y) | \, (y,x) \in r\} \text{ and } z^r := \{y \in X | \, (z,y) \in r\}.$$

Let R be a partition of $X \times X$ which does not contain the empty set. We say that (X,R) is an *association scheme* (or simply, a *scheme*) if it satisfies the following conditions:

(i) $1_X \in R$;
(ii) For each $r \in R$ we have $r^* \in R$;
(iii) For all $d, e, f \in R$ and each $(x,y) \in f$, $|x^d \cap y^{e^*}|$ depends only on d, e, f where we denote the cardinality of any finite set Ω by $|\Omega|$.

We denote $|x^d \cap y^{e^*}|$ with $(x,y) \in f$ by a_{def}, and $\{a_{def} | \, d,e,f \in R\}$ are called the *intersection numbers* of R. For each $r \in R$ we abbreviate $n_r := a_{rr^*1_X}$, which is called the *valency* of r. For each $(x,y) \in X \times X$ we denote the unique element of R which contains (x,y) by $r(x,y)$.

For each $F \subseteq R$ we set

$$n_F := \sum_{f \in F} n_f, \quad F^+ := \bigcup_{f \in F} f, \quad F^* := \{f^* | \, f \in F\} \text{ and } F^\times := F - \{1_X\}.$$

Given $x \in X$ we shall write x^F instead of x^{F^+}.

Following [7], we shall write the power set of R as $\mathcal{P}(R)$, and we define the complex product $\mathcal{P}(R) \times \mathcal{P}(R) \to \mathcal{P}(R)$ by

$$EF := \{r \in R | \, \sum_{e \in E} \sum_{f \in F} a_{efr} \neq 0\} \text{ for all } E, F \subseteq R.$$

One may notice that, for each $z \in X$ we have

$$EF = \{r(x,y) | \, x \in z^{E^*}, y \in z^F\}$$

and the associativity of the complex product holds. For convenience we shall write eF and Fe instead of $\{e\}F$ and $F\{e\}$ respectively where $e \in R$, $F \subseteq R$.

A subset $F \subseteq R$ is called *closed* if $FF^* \subseteq F$, or, equivalently, F^+ is an equivalence relation on X. We shall denote by $\mathcal{C}(R)$ the set of all closed subsets of R, and write $E \leq F$ if $E \subseteq F$ and $E, F \in \mathcal{C}(R)$. For each $E \subseteq R$ we set $\langle E \rangle := \bigcap \{F \in \mathcal{C}(R) | \, E \subseteq F\}$, so that $\langle E \rangle$ is the unique minimal closed subset which contains E since the intersection of closed subsets is also closed.

Following [7], for each $F \in \mathcal{C}(R)$ and $x \in X$ we set

$$(X,R)_{x^F} := (x^F, \{f_{x^F}\}_{f \in F}), \quad f_{x^F} := f \cap (x^F \times x^F).$$

Then $(X, R)_{x^F}$ is an association scheme, which is called the *subscheme* of (X, R) with respect to (F, x). We set

$$X/F := \{x^F \mid x \in X\} \text{ and } R/\!\!/F := \{r^F \mid r \in R\}$$

where $r^F := \{(y^F, z^F) \mid z \in y^{FrF}\}$. Then $(X, R)^F := (X/F, R/\!\!/F)$ is an association scheme, which is called the *factor scheme* of (X, R) over F.

We say that $F \in \mathcal{C}(R)$ is *thin* (res. *quasi-thin*) if $n_f = 1$ (res. $n_f \leq 2$) for each $f \in F$. For each $F \in \mathcal{C}(R)$ we set

$$\mathrm{O}_\theta(F) := \langle E \mid E \leq F \text{ is thin} \rangle, \quad \mathrm{O}^\theta(F) := \bigcap \{E \leq F \mid F/\!\!/E \text{ is thin}\},$$

which are called the *thin radical* and the *thin residue* of F respectively. One may notice that $\mathrm{O}_\theta(F)$ is the unique maximal thin closed subset of F and $\mathrm{O}^\theta(F)$ is the unique minimal closed subset E of F such that $F/\!\!/E$ is thin, furthermore $\mathrm{O}^\theta(F) = \langle ff^* \mid f \in F \rangle$ (see [7, p. 37]).

Let $F \in \mathcal{C}(R)$ and $x, y \in X$. A map $\sigma : x^F \to y^F$ is called *arranged* with respect to (F, x, y) if it satisfies the following conditions:

(i) σ is a bijection with $\sigma(x) = y$;
(ii) For all $w, z \in x^F$ we have $r(\sigma(w), \sigma(z)) = r(w, z)$.

We say that $F \in \mathcal{C}(R)$ is *arranged* if, for all $x, y \in X$ there exists an arranged map with respect to (F, x, y).

The following lemma is proved in [4]:

Lemma 2.1 ([4]). *Let (X, R) be an association scheme. Then the following are equivalent:*

(i) $\mathrm{Aut}(X, R)$ *is transitive on* X;
(ii) *Each closed subset of* R *is arranged*;
(iii) R *is arranged.*

3. Main Results

We shall show our main results without proofs in this section.

Lemma 3.1. *Let (X, R) be an association scheme. If $E \leq R$ is arranged and $T \leq \mathrm{O}_\theta(R)$ with $ET \in \mathcal{C}(R)$, then ET is arranged. In particular, each thin closed subset is arranged.*

Proposition 3.2. *If $F \in \mathcal{C}(R)$ is quasi-thin with $\mathrm{O}_\theta(F) = \{1_X\}$, then F is arranged.*

Proposition 3.3. *If $n_{\mathrm{O}^\theta(F)} = 2$, then F is arranged.*

Proposition 3.4. *If F is quasi-thin and $F = \langle f \rangle$ with $\langle s_f \rangle = \langle s_{f^*} \rangle$, then F is arranged.*

Proposition 3.5. *Assume that $\mathrm{O}^\theta(F) = \mathrm{O}_\theta(F)$ with $n_{\mathrm{O}^\theta(F)} = 4$. Then $n_F/4 \in \{3, 7, 4, 6, 9, 16\}$.*

4. Some application

We shall apply the results given in Section 3 for the characterization of quasi-thin schemes with some restriction on the cardinality of the point set.

Theorem 4.1. *Let (X, R) be a quasi-thin scheme with $|X| = 4p$ where p is a prime number. Then one of the following holds*:

(i) $\mathrm{Aut}(X, R)$ *is transitive on* X;

(ii) $|X| = 28$, $\mathrm{O}^\theta(R) = \mathrm{O}_\theta(R)$ *and* $n_{\mathrm{O}^\theta(R)} = 4$.

Proof. We may assume that $p \neq 2$ since the classification of association schemes with 8 points are done in [6]. We divide our consideration into the cases up to the valency of $n_{\mathrm{O}^\theta(R)}$, *i.e.*, the set of divisor of $4p$,

$$n_{\mathrm{O}^\theta(R)} \in \{1, 2, 4, p, 2p, 4p\}.$$

Case 1. $(n_{\mathrm{O}^\theta(R)} = 1,\ 4p)$ It is proved in [5] that each quasi-thin scheme whose thin residue is trivial has a transitive automorphism group.

Case 2. $(n_{\mathrm{O}^\theta(R)} = p)$ Since $n_{\mathrm{O}^\theta(R)}$ is an odd prime, the conclusion follows from Lemma 3.1 and Proposition 3.2.

Case 3. $(n_{\mathrm{O}^\theta(R)} = 2)$ It is a direct consequence of Lemma 3.3.

Case 4. $(n_{\mathrm{O}^\theta(R)} = 4)$ If $\mathrm{O}^\theta(R)$ is thin, then, by Proposition 3.5 we have $|X|/4 = n_R/4 \in \{3, 7\}$. The conclusion follows from the classification results in [3].

If $\mathrm{O}^\theta(R)$ is non-thin, then $\mathrm{O}^\theta(R) = \langle s_f \rangle$ for some $f \in R$ with $n_f = 2$. Since s_f is a unique non-thin element in $\mathrm{O}^\theta(R)$, we have $ff^* = f^*f$. It is clear that $R = \langle f \rangle$ by $f \notin \mathrm{O}^\theta(R)$. Therefore, the conclusion follows from Proposition 3.4.

Case 5. $(n_{\mathrm{O}^\theta(R)} = 2p)$ If $R = \langle f \rangle$ for some $f \in R$, then $\langle s_f \rangle = \langle s_{f^*} \rangle$ since there is a unique closed subset for each divisor of $2p$ and $n_{\langle s_f \rangle} = n_{\langle s_{f^*} \rangle}$. Thus, the conclusion follows ¿from Proposition 3.4. Assume that there is no $f \in R$ such that $R = \langle f \rangle$. If there exists $g \in R - \mathrm{O}^\theta(R)$ such that $n_{\langle s_g \rangle} = p$, then $n_{\langle g \rangle} = 2p$, and hence $\mathrm{O}_\theta(R) > \mathrm{O}_\theta(\langle g \rangle)$. This implies that $R = \langle s_g \rangle \mathrm{O}_\theta(R)$, which is arranged by Lemma 3.1. Hence we may assume that each element $f \in R - \mathrm{O}^\theta(R)$ satisfies $n_{\langle s_f \rangle} = 2$. Take an element $h \in \mathrm{O}^\theta(R)$ with $n_{\langle s_h \rangle} = p$. Then there exist g_1, $g_2 \in R - \mathrm{O}^\theta(R)$ such that $h \in g_1 g_2$. It follows that $s_h = s_{h^*} \in \mathrm{O}_\theta(R)$, contradicting $n_{\langle s_h \rangle} = p$ since s_h is symmetric. Thus, it is impossible that there is no $f \in R$ such that $R = \langle f \rangle$. This completes the proof. □

According to the classification result by A. Hanaki and I. Miyamoto there exists exactly two quasi-thin schemes which satisfies the properties as in (ii) of Theorem 4.1, one of which has a transitive automorphism group but another of which does not have it. This implies that each quasi-thin scheme except one case has a transitive automorphism group.

REFERENCES

[1] Z. Arad, E. Fisman, M. Muzychuk, Generalized table algebras, *Israel J. Math.* 114, 29–60, 1999.

[2] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, *Benjamin / Cummings, Menlo Park, CA*, 1984.

[3] M. Hirasaka, The classification of association schemes with 11 or 12 vertices, *Kyushu Journal of Mathematics*, 51, 413-428, 1997.

[4] M. Hirasaka, On Quasi-thin Association Schemes with Odd Points, submitted to *J. Algebra* , 1999.

[5] M. Hirasaka, M. Muzychuk, Association schemes with a relation of valency two, *Disc. Math.*, accepted for publiczation, 2000.

[6] E. Nomiyama, The classification of association schemes with at most 10 vertices, *Kyushu J. of Math.* 49, No. 1, 163-195, 1995.

[7] P.H. Zieschang, An Algebraic Approach to Association Schemes, Lecture Notes in Mathematics 1628, *Springer*, 1996.

COMBINATORIAL AND COMPUTATIONAL MATHEMATICS CENTER, POHANG UNIVERSITY OF SCIENCE AND TECHNOLOGY, POHANG 790-784, KOREA

E-mail address, M. Hirasaka: hirasaka@com2mac.postech.ac.kr

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, NETANYA ACADEMIC COLLEGE, 16 KIBUTZ GALUYOT ST.42365 NETANYA, ISRAEL

E-mail address, M. Muzychuk: muzy@netanya.ac.il

An upper bound for the cardinality of an s-distance set in Euclidean space

Etsuko Bannai
and
Kazuki Kawasaki
Graduate School of Mathematics
Kyushu University

Abstract

In this paper we show that if X is an s-distance set in $\mathbb{R}^m$ and X is on p concentric spheres then $|X| \leq \sum_{i=0}^{2p-1} \binom{m+s-i-1}{s-i}$.

1 Introduction

A subset X in a metric space (M, d) is called an s-distance set if the cardinality of the set $A = \{d(x,y) \mid x,y \in X,\ x \neq y\}$ is equal to s. In [5] P. Delsarte, J. M. Geothals and J. J. Seidel showed that the cardinality of a spherical $2s$-design X on the sphere S^{m-1} ($\subset \mathbb{R}^m$) is bounded below by $\binom{m+s-1}{s} + \binom{m+s-2}{s-1}$. They named the spherical $2s$-design with the smallest cardinality $\binom{m+s-1}{s} + \binom{m+s-2}{s-1}$ tight $2s$-design. In the same paper they showed that the cardinality of an s-distance set on the sphere S^{m-1} is bounded above by the same number $\binom{m+s-1}{s} + \binom{m+s-2}{s-1}$. They also showed that a finite set on the sphere S^{m-1} of cardinality $|X| = \binom{m+s-1}{s} + \binom{m+s-2}{s-1}$ is a tight $2s$-design if and only if it is an s-distance set.

The upper bound of the cardinality of an s-distance set in $\mathbb{R}^m$ was studied by Bannai-Bannai-Stanton [2] and Blokhuis [3] independently. They showed that s-distance set in $\mathbb{R}^m$ is bounded above by $\binom{m+s}{s}$. On the other hand Euclidean design is defined in the paper by P. Delsarte and J. J. Seidel [4]. They proved that Euclidean $2s$-design on p concentric spheres in $\mathbb{R}^m$ is bounded below by $\sum_{i=0}^{2p-1} \binom{m+s-i-1}{s-i}$.

In this paper we prove the following theorem which improves the upper bound of an s-distance set in $\mathbb{R}^m$.

Theorem 1.1 *Let X be an s-distance set on p concentric spheres in $\mathbb{R}^m$. Then*

$$|X| \leq \sum_{i=0}^{2p-1} \binom{m+s-i-1}{s-i}.$$

Remark If $p = 1$, then $\sum_{i=0}^{2p-1} \binom{m+s-i-1}{s-i} = \binom{m+s-1}{s} + \binom{m+s-2}{s-1}$ and the bound coincides with the bound given by Delsarte, Geothals and Seidel for the spherical case. If $s \leq 2p-1$, then $\sum_{i=0}^{2p-1} \binom{m+s-i-1}{s-i} = \sum_{i=0}^{s} \binom{m+s-i-1}{s-i} = \binom{m+s}{s}$. This means that Theorem 1.1 is true for $s \leq 2p-1$. Hence if $s = 2$ and $p \geq 2$, then the upper bound given in Theorem 1.1 coincides with the known one, $\binom{m+2}{2}$. If $s \geq 2p$, then $\sum_{i=0}^{2p-1} \binom{m+s-i-1}{s-i} < \binom{m+s}{s}$ and Theorem 1.1 gives a better upper bound.

As for the subsets in $\mathbb{R}^m$ there is an exapmle of 2-distance set in $\mathbb{R}^8$ whose cardinality is $\binom{8+2}{2}$. This example was found by Lisoněk [7] and it is on 2 concentric spheres. However it is not a tight 4-design as an Euclidean design even though whose cardinality coincides with the upper bound.

It is still unknown whether any tight $2s$-design gives an s-distance set or not. This problem seems very important and interesting.

For more information on this subject, see [1] and [4].

In §2 we give basic facts about the vector space of the polynomials on finite number of concentric spheres in $\mathbb{R}^m$. In §3 we give a proof of Theorem 1.1.

2 Polynomials on p concentric spheres in $\mathbb{R}^m$

First we give notation which will be used in the followings and then give basic facts about polynomials on finite number of concentric spheres (see [4]). Let $S_1, S_2, \ldots, S_p$ be spheres in $\mathbb{R}^m$ centered at the origin of $\mathbb{R}^m$ and radii $r_1, r_2, \ldots, r_p$ respectively. Let $S = S_1 \cup S_2 \cup \cdots \cup S_p$. Let $P(\mathbb{R}^m)$ be the set of all the polynomials of m variables $x_1, x_2, \ldots, x_m$. Let Hom $_l(\mathbb{R}^m)$ be the set of all the homogeneous polynomials of degree l. We denote the Laplacian $\frac{\partial^2}{\partial x_1^2} + \frac{\partial^2}{\partial x_2^2} + \cdots + \frac{\partial^2}{\partial x_m^2}$ by Δ. Let Harm $_l(\mathbb{R}^m)$ be the set of all the harmonic homogeneous polynomials of degree l, i.e., Harm $_l(\mathbb{R}^m) = \{f \in \text{Hom }_l(\mathbb{R}^m) \mid \Delta f = 0\}$. Let $P(S) = \{f|_S \mid f \in P(\mathbb{R}^m)\}$, Hom $_l(S) = \{f|_S \mid f \in \text{Hom }_l(\mathbb{R}^m)\}$, Harm $_l(S) = \{f|_S \mid f \in$ Harm $_l(\mathbb{R}^m)\}$. For $x = (x_1, x_2, \ldots, x_m)$ and $y = (y_1, y_2, \ldots, y_m)$ in $\mathbb{R}^m$, inner product of x and y is denoted by $\langle x, y \rangle = \sum_{i=1}^m x_i y_i$. Let $||x||^2 = \langle x, x \rangle = \sum_{i=1}^m {x_i}^2$.

The following propositions are known.

Proposition 2.1 *(See [6])*

(i) $Hom\ _l(\mathbb{R}^m) = Harm\ _l(\mathbb{R}^m) \oplus ||x||^2 Hom\ _{l-2}(\mathbb{R}^m)$

(ii) $dim\,(Hom\ _l(\mathbb{R}^m)) = \binom{m+l-1}{l}$

(iii) $dim\,(Harm\ _l(\mathbb{R}^m)) = \binom{m+l-1}{l} - \binom{m+l-3}{l-2}$

Proposition 2.2 *(See [4]) Let $\rho : P(\mathbb{R}^m) \longrightarrow P(S)$ be the linear map defined by $\rho(f) = f|_S$ for any $f \in P(\mathbb{R}^m)$. Then the followings hold.*

(i) *The kernel of ρ is the ideal generated by $\prod_{i=1}^{p}(||x||^2 - {r_i}^2)$.*

(ii) *$Hom_{\,i}(S) \cong Hom_{\,i}(\mathbb{R}^m)$, for each non-negative integer i.*

(iii) $$\sum_{i=0}^{l} Hom_{\,i}(S) = \bigoplus_{i=0}^{2p-1} Hom_{\,l-i}(S) \cong \bigoplus_{i=0}^{2p-1} Hom_{\,l-i}(\mathbb{R}^m)$$

(iv) $$dim\left(\sum_{i=0}^{l} Hom_{\,i}(S)\right) = \sum_{i=0}^{2p-1} \binom{m+l-i-1}{l-i}$$

We define some more notations which we use in this paper. For a vector $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_m)$ whose entries are non-negative integers, we define $|\lambda| = \sum_{i=1}^{m} \lambda_i$. For any $x = (x_1, x_2, \ldots, x_m) \in \mathbb{R}^m$, we write $x^\lambda = {x_1}^{\lambda_1}{x_2}^{\lambda_2} \cdots {x_m}^{\lambda_m}$. Next proposition is very elementary but useful.

Proposition 2.3 *Let $u = (u_1, u_2, \ldots, u_m) \in \mathbb{R}^m$ be a vector. Then the coefficient of the monomial x^λ in $||x||^{2i}\langle x, u\rangle^{l-2i}$ is equal to*

$$\frac{1}{(\lambda_1)!(\lambda_2)!\cdots(\lambda_m)!}(l-2i)!\ \Delta^i(x^\lambda)|_{x=u}\ ,$$

where $\Delta^i(x^\lambda)|_{x=u}$ means that after taking the i times of Laplacian for the monomial x^λ and substitute $x = u$.

The following lemma, which may be known well, is useful. We use some modification of this Lemma in our proof of Theorem 1.1.

Lemma 2.4 *Assume that there exists a vector $u = (u_1, u_2, \ldots, u_m) \in \mathbb{R}^m$ and real numbers $c_1, c_2, \ldots, c_{[\frac{l}{2}]}$ satisfying the following equation.*

$$\langle x, u\rangle^l = \sum_{i=1}^{[\frac{l}{2}]} c_i ||x||^{2i}\langle x, u\rangle^{l-2i}$$

for any $x = (x_1, x_2, \ldots, x_m) \in \mathbb{R}^m$. Then $\varphi(u) = 0$ for any $\varphi \in Harm_{\,l}(\mathbb{R}^m)$

Proof. The coefficient of the monomial ${x_1}^{\lambda_1}{x_2}^{\lambda_2} \cdots {x_m}^{\lambda_m}$ in $\langle x, u\rangle^l$ is equal to

$$\frac{l!}{(\lambda_1)!(\lambda_2)!\cdots(\lambda_m)!}\ {u_1}^{\lambda_1}{u_2}^{\lambda_2} \cdots {u_m}^{\lambda_m},$$

for any non-negative integers $\lambda_1, \lambda_2, \ldots, \lambda_m$ satisfying $\lambda_1 + \lambda_2 + \cdots + \lambda_m = l$. Hence Proposition 2.3 implies the following equation

$${u_1}^{\lambda_1}{u_2}^{\lambda_2} \cdots {u_m}^{\lambda_m} = \frac{1}{l!} \sum_{i=1}^{[\frac{l}{2}]} \alpha_i (l-2i)!\ \Delta^i({x_1}^{\lambda_1}{x_2}^{\lambda_2} \cdots {x_m}^{\lambda_m})|_{x=u}\ .$$

Since Δ^i is a linear operator we have

$$f(u) = \frac{1}{l!} \sum_{i=1}^{[\frac{l}{2}]} \alpha_i (l-2i)! \, (\Delta^i f)(u) \, .$$

for any homogeneous polynomial $f \in \mathrm{Hom}_l(\mathbb{R}^m)$. In particular if φ is a harmonic polynomial in $\mathrm{Harm}_l(\mathbb{R}^m)$ we have $\varphi(u) = 0$. ∎

3 Proof of Theorem 1.1

Let X be an s-distance set in $\mathbb{R}^m$. Let $A = A(X) = \{d(u,v) \mid u, v \in X, \ u \neq v\}$, where $d(u,v) = \sqrt{\langle u-v, u-v\rangle} = \|u-v\|$. Then by the assumption on X we have $|A| = s$. Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_s\}$. For each $u \in X$, we define a polynomial $F_u \in P(\mathbb{R}^m)$ by

$$F_u(x) = \prod_{i=1}^{s} (\|x-u\|^2 - {\alpha_i}^2).$$

Then we have

$$F_u(v) = \delta_{u,v} (-1)^s \prod_{i=1}^{m} {\alpha_i}^2 \tag{3.1}$$

for any $u, \ v \in X$. By (3.1) the set of polynomials $\mathcal{F}_X = \{F_u \mid u \in X\}$ is linearly independent in $P(\mathbb{R}^m)$. For each $u \in X$, the polynomial F_u is a polynomial of highest degree $2s$, that is, $F_u \in \sum_{i=0}^{2s} \mathrm{Hom}_i(\mathbb{R}^m)$. Since $\mathcal{F}_X$ is a set of linearly independent polynomials in a finite dimensional vector space $\sum_{i=0}^{2s} \mathrm{Hom}_i(\mathbb{R}^m)$, X has to be a finite set. Let $R = R_X = \{\|u\| \mid u \in X\}$. Then R consists of finite number of real numbers. Without loss of generality we may assume that $0 \notin R$. Let $|R| = p$ and $R = \{r_1, r_2, \ldots, r_p\}$. For each i with $1 \leq i \leq p$, let S_i be the sphere in $\mathbb{R}^m$ with center at the origin and radius r_i. Let $S = S_1 \cup S_2 \cup \cdots \cup S_p$. Then (3.1) also implies that $\mathcal{F}_X$ is linearly independent as polynomials in $P(S)$. Let $\mathcal{F}_X(S) = \{F_u|_S \mid u \in X\}$. Then $|X| = \dim(\langle \mathcal{F}_X(S) \rangle)$. In the following we look for the upper bounds for $\dim(\langle \mathcal{F}_X(S) \rangle)$. As it is mentioned in the Remark right after Theorem 1.1, if $s \leq 2p-1$ then Theorem 1.1 is true. From now on we assume $s \geq 2p$.

Lemma 3.1

$$\text{(i)} \quad \langle \mathcal{F}_X(S) \rangle \subset \bigoplus_{i=0}^{2p-1} Hom_{s-i}(S) + \sum_{i=1}^{p-1} \|x\|^{2i} Hom_{s-i}(S).$$

$$\text{(ii)} \quad \langle \mathcal{F}_X(S) \rangle \subset \bigoplus_{i=0}^{2p-1} Hom_{s-i}(S) + \sum_{i=1}^{p-1} \sum_{j=0}^{p-1-i} \|x\|^{2(i+j)} Harm_{s-i-2j}(S)$$

Proof We have the following expression for the polynomial F_u.

$$F_u(x) = \sum_{i=0}^{s} \beta_{s-i}^{(u)} (\|x\|^2 - 2\langle x, u\rangle)^i,$$

where $\beta_i^{(u)}, 0 \leq i \leq s$ is the elementary symmetric polynomial of $\{||u||^2-\alpha_1^2, \ldots, ||u||^2-\alpha_s^2\}$ of degree i. In particular $\beta_0^{(u)} = 1$. Therefore

$$\mathcal{F}_X \subset \langle \{||x||^{2i}\langle x,u\rangle^j \mid i+j \leq s\}\rangle \subseteq \sum_{\substack{i+j\leq s \\ 0\leq i,j}} ||x||^{2i}\mathrm{Hom}_j(\mathbb{R}^m\rangle.$$

If $i \neq 0$, $i+j < s$, and $2i+j \geq s+1$, then we have $i > 2i+j-s \geq 1$ and $s-i-j > 0$. Therefore we have

$$||x||^{2i}\mathrm{Hom}_j(\mathbb{R}^m) = ||x||^{2(2i+j-s)}||x||^{2(s-i-j)}\mathrm{Hom}_j(\mathbb{R}^m) \subset ||x||^{2(2i+j-s)}\mathrm{Hom}_{s-(2i+j-s)}(\mathbb{R}^m).$$

Hence we have

$$\langle \mathcal{F}_X\rangle \subset \bigoplus_{i=0}^{s} \mathrm{Hom}_i(\mathbb{R}^m) + \sum_{i=0}^{s} ||x||^{2i}\mathrm{Hom}_{s-i}(\mathbb{R}^m\rangle.$$

Hence by Proposition 2.2, we have

$$\langle \mathcal{F}_X(S)\rangle \subset \bigoplus_{i=0}^{2p-1} \mathrm{Hom}_{s-i}(S) + \sum_{i=0}^{s} ||x||^{2i}\mathrm{Hom}_{s-i}(S). \tag{3.2}$$

Next, we will show that

$$||x||^{2j}\mathrm{Hom}_{s-j}(S) \subset \bigoplus_{i=0}^{2p-1} \mathrm{Hom}_{s-i}(S) + \sum_{i=0}^{j-1} ||x||^{2i}\mathrm{Hom}_{s-i}(S), \tag{3.3}$$

for any $j \geq p$. By Proposition 2.2, $\prod_{l=1}^{p}(||x||^2 - r_l^2)$ generates the kernel of the linear map ρ defined by restriction of the polynomials on $\mathbb{R}^m$ to S. Hence, as a polynomial on S, $||x||^{2p}$ is a linear combination of $||x||^{2j}, j = 0, 1, 2, \ldots, p-1$. Therefore we have

$$||x||^{2p}\mathrm{Hom}_l(S) \subset \sum_{i=0}^{p-1} ||x||^{2i}\mathrm{Hom}_l(S). \tag{3.4}$$

for any integer $l \geq 0$.

Let $j \geq p$. Then by (3.4) we have

$$||x||^{2j}\mathrm{Hom}_{s-j}(S) = ||x||^{2p}||x||^{2(j-p)}\mathrm{Hom}_{s-j}(S) \subset$$
$$\sum_{j=1}^{p} ||x||^{2(p-j)}||x||^{2(i-p)}\mathrm{Hom}_{s-i}(S) = \sum_{k=1}^{p-1} ||x||^{2(j-k)}\mathrm{Hom}_{s-j}(S).$$

If $j \leq 2k$, then

$$||x||^{2(j-k)}\mathrm{Hom}_{s-j}(S) \subset \mathrm{Hom}_{s-(2k-j)}(S) \subset \bigoplus_{i=0}^{2p-1} \mathrm{Hom}_{s-i}(S). \tag{3.5}$$

If $j \geq 2k+1$, then

$$\begin{aligned} ||x||^{2(j-k)}\mathrm{Hom}_{s-j}(S) &= ||x||^{2(j-2k)}||x||^{2k}\mathrm{Hom}_{s-j}(S) \\ &\subset ||x||^{2(j-2k)}\mathrm{Hom}_{s-(j-2k)}(S) \subset \sum_{i=1}^{j-1} ||x||^{2i}\mathrm{Hom}_{s-i}(S) \end{aligned} \tag{3.6}$$

because $k \geq 1$. (3.5) and (3.6) imply (3.3). Induction on j using (3.3) implies

$$\sum_{i=0}^{s} ||x||^{2i}\mathrm{Hom}_{s-i}(S) \subset \bigoplus_{i=0}^{2p-1} \mathrm{Hom}_{s-i}(S) + \sum_{i=1}^{p-1} ||x||^{2i}\mathrm{Hom}_{s-i}(S). \tag{3.7}$$

Equations (3.2) and (3.7) imply Lemma 3.1, (i).

Next we prove Lemma 3.1, (ii). Proposition 2.1, (i) implies

$$||x||^{2i}\mathrm{Hom}_{s-i}(S) = \sum_{j=0}^{p-i-1} ||x||^{2(i+j)}\mathrm{Harm}_{s-i-2j}(S) + ||x||^{2p}\mathrm{Hom}_{s+i-2p}(S), \tag{3.8}$$

for any i with $1 \leq i \leq p-1$. Then by (3.4) we have

$$||x||^{2p}\mathrm{Hom}_{s+i-2p}(S) \subset \sum_{l=0}^{p-1} ||x||^{2l}\mathrm{Hom}_{s+i-2p}(S). \tag{3.9}$$

(3.8) and (3.9) imply

$$||x||^{2i}\mathrm{Hom}_{s-i}(S) = \sum_{j=0}^{p-i-1} ||x||^{2(i+j)}\mathrm{Harm}_{s-i-2j}(S) + \sum_{l=0}^{p-1} ||x||^{2l}\mathrm{Hom}_{s+i-2p}(S), \tag{3.10}$$

for any i with $1 \leq i \leq p-1$. Next we will show

$$||x||^{2l}\mathrm{Hom}_{s+i-2p}(S) \subset \bigoplus_{k=0}^{2p-1} \mathrm{Hom}_{s-k}(S) + \sum_{k=0}^{i-1} ||x||^{2k}\mathrm{Hom}_{s-k}(S) \tag{3.11}$$

for any i, l with $1 \leq i \leq p-1$ and $0 \leq l \leq p-1$.
If $i + 2l \leq 2p$, then

$$||x||^{2l}\mathrm{Hom}_{s+i-2p}(S) \subset \mathrm{Hom}_{s-(2p-2l-i)}(S) \subset \bigoplus_{k=0}^{2p-1} \mathrm{Hom}_{s-k}(S). \tag{3.12}$$

If $i + 2l \geq 2p+1$, then $i + 2l - 2p \geq 1$. On the other hand $2p - i - l \geq 2$. Hence we have

$$\begin{aligned} ||x||^{2l}\mathrm{Hom}_{s+i-2p}(S) &= ||x||^{2(i+2l-2p)}||x||^{2(2p-i-l)}\mathrm{Hom}_{s+i-2p}(S) \\ &\subset ||x||^{2(i+2l-2p)}\mathrm{Hom}_{s-(i+2l-2p)}(S) \subset \sum_{k=0}^{i-1} ||x||^{2k}\mathrm{Hom}_{s-k}(S), \end{aligned} \tag{3.13}$$

because $i + 2l - 2p < i$. Then (3.12) and (3.13) imply (3.11). Then (3.10) and (3.11) imply

$$\begin{aligned} ||x||^{2i}\mathrm{Hom}_{s-i}(S) \subset \bigoplus_{k=0}^{2p-1} \mathrm{Hom}_{s-k}(S) + \sum_{j=0}^{p-1-i} ||x||^{2(i+j)}\mathrm{Harm}_{s-i-2j}(S) \\ + \sum_{k=0}^{i-1} ||x||^{2k}\mathrm{Hom}_{s-k}(S). \end{aligned} \tag{3.14}$$

Then induction on i using (3.14) implies Lemma 3.1, (ii). ∎

Next we construct a subspace W in $\bigoplus_{i=1}^{2p-3} \mathrm{Hom}_{s-i}(S)$ satisfying

$$\langle \mathcal{F}_X(S) \rangle \cap W = \{0\},$$
$$\dim W = \dim \left(\sum_{i=1}^{p-1} \sum_{j=0}^{p-1-i} \|x\|^{2(i+j)} \mathrm{Harm}_{s-i-2j}(S) \right).$$

First we assume that there exist a polynomial $g(x) \in \langle \mathcal{F}_X(S) \rangle \cap \bigoplus_{i=1}^{2p-3} \mathrm{Hom}_{s-i}(S)$. Then we can assume $g(x) \in \bigoplus_{i=1}^{2p-3} \mathrm{Hom}_{s-i}(\mathbb{R}^m)$ and

$$\sum_{u \in X} a_u F_u(x) = g(x) + f(x) \prod_{i=1}^{p} (\|x\|^2 - r_i{}^2) \tag{3.15}$$

for any $x \in \mathbb{R}^m$ with some real numbers a_u, $u \in X$ and a polynomial $f(x) \in P(\mathbb{R}^m)$ whose leading term is of degree $2(s-p)$. Let $f(x) = \sum_{i=0}^{2(s-p)} \sum_{|\lambda|=i} b_\lambda x^\lambda$. Let us express

$$\sum_{u \in X} a_u F_u(x) = \sum_{u \in X} a_u \sum_{i=0}^{s} \beta_{s-i}^{(u)} (\|x\|^2 - 2\langle x, u \rangle)^i,$$

where $\beta_i^{(u)}$ is the elementary symmetric polynomial of degree i for $\|u\|^2 - \alpha_1^2, \|u\|^2 - \alpha_2^2, \ldots, \|u\|^2 - \alpha_m^2$. In particular $\beta_0^{(u)} = 1$. We also express

$$\prod_{j=1}^{p} (\|x\|^2 - r_j{}^2) = \sum_{j=0}^{p} \delta_{p-j} \|x\|^{2j},$$

where δ_i is the elementary symmetric polynomial of degree i for $-r_1^2, -r_2^2, \ldots, -r_m^2$. In particular $\delta_0 = 1$. With the notation given above we have

$$\sum_{u \in X} a_u F_u(x) = \sum_{u \in X} a_u \sum_{l=0}^{2s} \sum_{j=\max\{0, l-s\}}^{\min\{[\frac{l}{2}], s\}} (-2)^{l-2j} \binom{l-j}{j} \beta_{j-l+s}^{(u)} \|x\|^{2j} \langle x, u \rangle^{l-2j} \tag{3.16}$$

and

$$f(x) \prod_{j=1}^{p} (\|x\|^2 - r_j{}^2) = \left(\sum_{i=0}^{2s-2p} \sum_{|\lambda|=i} b_\lambda x^\lambda \right) \left(\sum_{j=0}^{p} \delta_{p-j} \|x\|^{2j} \right)$$
$$= \sum_{l=0}^{2s} \sum_{\substack{0 \le j \le p \\ l-2(s-p) \le 2j \le l}} \sum_{|\lambda|=l-2j} \delta_{p-j} b_\lambda \|x\|^{2j} x^\lambda \tag{3.17}$$

Since $g(x) \in \bigoplus_{i=1}^{2p-3} \mathrm{Hom}_{s-i}(\mathbb{R}^m)$ we can prove the followings, using equations (3.15), (3.16) and (3.17),

$$\sum_{j=0}^{\min\{p,[\frac{l}{2}]\}} \delta_{p-j}||x||^{2j} \sum_{|\lambda|=l-2j} b_\lambda x^\lambda = (-2)^l \sum_{j=0}^{[\frac{l}{2}]} 2^{-2j} \binom{l-j}{j} \sum_{u\in X} a_u \beta_{s-l+j}^{(u)} ||x||^{2j} \langle x,u\rangle^{l-2j},$$
$$\text{for } 0 \le l \le s-2p+2, \tag{3.18}$$

$$\sum_{0\le j\le \min\{p,\frac{2s-l}{2}\}} \delta_j ||x||^{2(p-j)} \sum_{|\lambda|=l-2p+2j} b_\lambda x^\lambda$$
$$= (-2)^{2s-l}||x||^{2(l-s)} \sum_{j=0}^{[\frac{2s-l}{2}]} 2^{-2j} \binom{s-j}{j+l-s} \sum_{u\in X} a_u \beta_j^{(u)} ||x||^{2j} \langle x,u\rangle^{2s-l-2j},$$
$$\text{for } s \le l. \le 2s. \tag{3.19}$$

Let $l = s+i$, $0 \le i \le p$, in (3.19). Then we have

$$\sum_{0\le j\le \min\{p,\frac{s-i}{2}\}} \delta_j ||x||^{2(p-j)} \sum_{|\lambda|=s+i-2p+2j} b_\lambda x^\lambda$$
$$= (-2)^{s-i}||x||^{2i} \sum_{j=0}^{[\frac{s-i}{2}]} 2^{-2j} \binom{s-j}{i+j} \sum_{u\in X} a_u \beta_j^{(u)} ||x||^{2j} \langle x,u\rangle^{s-i-2j}. \tag{3.20}$$

We have the following proposition.

Proposition 3.2 *The assumption and notation are as given before. The the following conditions hold.*

(i) $\sum_{|\lambda|=i} b_\lambda x^\lambda \in \left\langle ||x||^{2j}\langle x,u\rangle^{i-2j} \;\middle|\; 0 \le j \le [\frac{i}{2}],\ u \in X \right\rangle$,
for any $0 \le i \le s-2p+2$

(ii) $\sum_{|\lambda|=s-p+i} b_\lambda x^\lambda \in \left\langle ||x||^{2(i+j)}\langle x,u\rangle^{s-p-i-2j} \;\middle|\; 0 \le j \le [\frac{s-p-i}{2}],\ u \in X \right\rangle$,
for any $0 \le i \le s-p$, *and the coefficient of the term* $||x||^{2(i+j)}\langle x,u\rangle^{s-p-i-2j}$ *in it is given by a linear combination of* $\beta_l^{(u)}, 0 \le l \le j$. *In particular coefficient of* $||x||^{2i}\langle x,u\rangle^{s-p-i}$ *is given by* $(-2)^{s-p-i}\binom{s}{p+i}$.

Proof We can prove (i) and (ii) inductively using (3.18) and (3.19). ∎

If $0 \leq i \leq s-p$, then by Proposition 3.2, $\sum_{|\lambda|=s-p+i} b_\lambda x^\lambda$ is a multiple of $||x||^{2i}$. Let us define $B^+_{s-p-i}(x)$ and $B_i(x)$ by

$$\sum_{|\lambda|=s-p+i} b_\lambda x^\lambda = ||x||^{2i} B^+_{s-p-i}(x), \quad 0 \leq i \leq s-p$$

and

$$B_i(x) = \sum_{|\lambda|=i} b_\lambda x^\lambda, \quad 0 \leq i \leq s-p-1$$

We express (3.20) using this notation and get

$$\sum_{j=0}^{[\frac{p-i-1}{2}]} \delta_j ||x||^{2(p-i-j)} B_{s-2p+2j+i}(x) + \sum_{j=[\frac{p-i-1}{2}]+1}^{\min\{p, \frac{s-i}{2}\}} \delta_j ||x||^{2j} B^+_{s-i-2j}(x) =$$

$$(-2)^{s-i} \sum_{j=0}^{[\frac{s-i}{2}]} 2^{-2j} \binom{s-j}{i+j} \sum_{u \in X} a_u \beta_j^{(u)} ||x||^{2j} \langle x, u \rangle^{s-i-2j}, \quad 1 \leq i \leq p-1. \tag{3.21}$$

Then by Proposition 3.2 we have

$$\sum_{j=0}^{[\frac{p-i-1}{2}]} \delta_j ||x||^{2(p-i-j)} B_{s-2p+2j+i}(x)$$

$$= \sum_{l=0}^{[\frac{2p-i-3}{2}]} \sum_{u \in X} a_u g_{i,l}(||u||^2) ||x||^{2l} \langle x, u \rangle^{s-i-2l} + h_{s-i}(x), \quad 1 \leq i \leq p-1. \tag{3.22}$$

where $h_{s-i}(x)$ is a polynomial in

$$\left\langle ||x||^{2l} \langle x, u \rangle^l \;\middle|\; 2l + j = s-i, \;\; 0 \leq j \leq s-2p+2 \right\rangle,$$

and $g_{i,l}(||u||^2)$ is a linear combination of $\beta_j^{(u)}$, $0 \leq j \leq l$. More precisely

$$g_{i,l}(||u||^2) = (-2)^{s-i-2l} \binom{s-l}{i+l} \beta_l^{(u)} + \text{ a linear combination of } \{\beta_j^{(u)}, \; 0 \leq j < l\}. \tag{3.23}$$

Let $U^{(\leq k)}_{s-i}$ be a subspace of $\mathrm{Hom}_{s-i}(\mathbb{R}^m)$ defined by

$$U^{(\leq k)}_{s-i} = \left\langle ||x||^{2j} \langle x, u \rangle^l \;\middle|\; 2j + l = s-i, \;\; 0 \leq l \leq k \right\rangle.$$

Denote the polynomial in $\mathrm{Hom}_{s-i}(\mathbb{R}^m)$, which is the first term in the right hand side of (3.22), by $\Phi_{s-i}(x)$. More precisely

$$\Phi_{s-i}(x) = \sum_{l=0}^{[\frac{2p-i-3}{2}]} \sum_{u \in X} a_u g_{i,l}(||u||^2) ||x||^{2l} \langle x, u \rangle^{s-i-2l}, \quad 0 \leq i \leq p.$$

Then (3.22) implies

$$\Phi_{s-i}(x) - \sum_{l=0}^{[\frac{p-i-1}{2}]} \delta_l ||x||^{2(p-i-l)} B_{s-2p+2l+i}(x) \in U_{s-i}^{(\leq s-2p+2)}. \tag{3.24}$$

We have the following lemma.

Lemma 3.3 *Assumption and notation are as given before. For each i and j with $1 \leq i \leq p-1$, $0 \leq j \leq p-i-1$ there exists a polynomial $G_{i,j}(t)$ of degree j in one variable t satisfying the following condition*

$$\sum_{u \in X} a_u G_{i,j}(||u||^2)\langle x, u\rangle^{s-i-2j} \in U_{s-i-2j}^{(\leq s-i-2j-2)}.$$

Moreover the polynomials $G_{i,j}(t)$, $1 \leq i \leq p-1$, $0 \leq j \leq p-i-1$, are independent of the constant a_u, $u \in X$.

Proof Let $i = p-1$ in (3.24). Then we have

$$\Phi_{s-p+1}(x) - ||x||^2 B_{s-p-1}(x) \in U_{s-p+1}^{(\leq s-2p+2)}.$$

Let $i = p-2$ in (3.24). Then we have

$$\Phi_{s-p+2}(x) - ||x||^4 B_{s-p-2}(x) \in U_{s-p+2}^{(\leq s-2p+2)}.$$

Thus induction on $p-i$ shows that for any i with $1 \leq i \leq p-1$ the following holds

$$\Phi_{s-i}(x) + \sum_{j=1}^{[\frac{p-i-1}{2}]} c_j ||x||^{2j} \Phi_{s-i-2j}(x) - ||x||^{2(p-i)} B_{s-2p+i}(x) \in U_{s-i}^{(\leq s-2p+2)},$$

with some constants c_j, $1 \leq j \leq [\frac{p-i-1}{2}]$. Hence we have

$$\Phi_{s-i}(x) + \sum_{j=1}^{[\frac{p-i-1}{2}]} c_j ||x||^{2j} \Phi_{s-i-2j}(x) \equiv 0 \mod U_{s-i}^{(\leq s-2p+i)}.$$

Then we have

$$\Delta^l \left(\Phi_{s-i}(x) + \sum_{j=1}^{[\frac{p-i-1}{2}]} c_j ||x||^{2j} \Phi_{s-i-2j}(x) \right) \equiv 0 \mod U_{s-i-2l}^{(\leq s-2p+i)}, \tag{3.25}$$

for any l with $0 \leq l \leq p-i-1$. On the other hand by the definition of $\Phi_{s-i}(x)$ the coefficient of the term $||x||^{2k}\langle x, u\rangle^{s-i-2k}$ in $\Phi_{s-i}(x) + \sum_{j=1}^{[\frac{p-i-1}{2}]} c_j ||x||^{2j} \Phi_{s-i-2j}(x)$ also has the following form

$$(-2)^{s-i-2k} \binom{s-k}{i+k} a_u \beta_k^{(u)} + \text{ a linear combination of } \{\beta_k^{(u)},\ 0 \leq j < k\}. \tag{3.26}$$

The formula (3.26) is a polynomial in $||u||^2$ of degree k and the leading term is

$$(-2)^{s-i-2k}\binom{s-k}{i+k}a_u||u||^{2k} = (-1)^{s-i}2^{s-i-2k}\binom{s-k}{i+k}a_u||u||^{2k}.$$

In general the following holds

$$\Delta(||x||^{2l}\langle x,u\rangle^k) = 2l(m+2l+2k-2)||x||^{2(l-1)}\langle x,u\rangle^k + k(k-1)||u||^2||x||^{2l}\langle x,u\rangle^{k-2}.$$

Therefor we have

$$\Delta^l\left(\Phi_{s-i}(x) + \sum_{j=1}^{[\frac{p-i-1}{2}]} c_j||x||^{2j}\Phi_{s-i-2j}(x)\right)$$
$$\equiv \sum_{u\in X} a_u G_{i,l}(||u||^2)\langle x,u\rangle^{s-i-2l}, \qquad (\mathrm{mod}\ U^{\leq s-i-2l-2}_{s-i-2l}). \tag{3.27}$$

where each $G_{i,l}(t)$ is a polynomial in one variable t of degree l which is independent of a_u, for any l with $0 \leq l \leq p-i-1$. Then (3.25) and (3.27) imply Lemma 3.3. ∎

Let W be a subspace in $\bigoplus_{i=1}^{2p-3} \mathrm{Hom}_{s-i}(S)$ defined by

$$W = \sum_{i=1}^{p-1}\sum_{j=0}^{p-i-1} G_{i,j}(||x||^2)\mathrm{Harm}_{s-i-2j}(S),$$

where $G_{i,j}(t)$, $1 \leq i \leq p-1$, $0 \leq j \leq p-i-1$, are the polynomials of degree j given in (3.27).

We have the following lemma.

Lemma 3.4 *Notation is as given before. The followings hold.*

(i) $\langle \mathcal{F}_X(S)\rangle \cap W = \{0\}$,

(ii) $\dim W = \dim\left(\sum_{i=1}^{p-1}\sum_{j=0}^{p-i-1} ||x||^{2(i+j)}\mathrm{Harm}_{s-i-2j}(S)\right)$.

Proof Let $g(x) \in \langle \mathcal{F}_X(S)\rangle \cap W$. We may assume

$$g(x) \in \left(\sum_{i=1}^{p-1}\sum_{j=0}^{p-i-1} G_{i,j}(||x||^2)\mathrm{Harm}_{s-i-2j}(\mathbb{R}^m)\right) \tag{3.28}$$

and

$$\sum_{u\in X} a_u F_u(x) = g(x) + f(x)\prod_{i=1}^{p}(||x||^2 - r_i^2) \tag{3.29}$$

for any $x \in \mathbb{R}^m$ with some real numbers a_u, $u \in X$ and a polynomial $f(x)$ whose leading term is of degree $2(s-p)$. Since we have

$$\sum_{i=1}^{p-1}\sum_{j=0}^{p-i-1} G_{i,j}(\|x\|^2)\mathrm{Harm}_{s-i-2j}(S) \subset \bigoplus_{i=1}^{2p-3} \mathrm{Hom}_{s-i}(S),$$

we can use Lemma 3.3 and we have

$$\sum_{u\in X} a_u G_{i,j}(\|u\|^2)\langle x,u\rangle^{s-i-2j} \in U_{s-i-2j}^{(\leq s-i-2j-2)},$$

for any i and j with $1 \leq i \leq p-1$, $0 \leq j \leq p-i-1$. Then a similar argument as given in the proof of Lemma 2.4 implies

$$\sum_{u\in X} a_u G_{i,j}(\|u\|^2)\varphi(u) = 0,$$

for any $\varphi(x) \in \mathrm{Harm}_{s-i-2j}(\mathbb{R}^m)$. Hence by (3.28) we have

$$\sum_{u\in X} a_u g(u) = 0. \tag{3.30}$$

On the other hand (3.29) implies $g(u) = a_u F(u) = a_u(-1)^s \prod_{i=1}^s \alpha_i^2$. Then (3.30) implies

$$(-1)^s \prod_{i=1}^s \alpha_i^2 \sum_{u\in X} a_u^2 = 0.$$

Since $(-1)^s \prod_{i=1}^s \alpha_i^2$ is a nonzero real number and $a_u^2 \geq 0$, $u \in X$, we have $a_u = 0$ for any $u \in X$. This completes the proof of Lemma 3.4, (i). Lemma 3.4, (ii) is obvious because the folowings hold

$$\sum_{i=1}^{p-1}\sum_{j=0}^{p-i-1} G_{i,j}(\|x\|^2)\mathrm{Harm}_{s-i-2j}(S) \subset \bigoplus_{i=0}^{2p-1} \mathrm{Ho\ m}_{s-1-i}(S)$$

and

$$\sum_{i=1}^{p-1}\sum_{j=0}^{p-1-i} \|x\|^{2(i+j)}\mathrm{Harm}_{s-i-2j}(S) \subset \bigoplus_{i=0}^{2p-1} \mathrm{Hom}_{s+p-1-i}(S).$$

Now we are ready to prove Theorem 1.1.

Proposition 2.2, Lemma 3.1 and Lemma 3.4 imply

$$\langle \mathcal{F}_X(S)\rangle \oplus W \subset \bigoplus_{i=0}^{2p-1} \mathrm{Hom}_{s-i}(S) + \sum_{i=1}^{p-1}\sum_{j=0}^{p-1-i} \|x\|^{2(i+j)}\mathrm{Harm}_{s-i-2j}(S).$$

Then we have

$$\begin{aligned}\dim(\langle\mathcal{F}_X(S)\rangle) + \dim W &= \dim\left(\langle\mathcal{F}_X(S)\rangle + W\right)\\ &\leq \dim\left(\bigoplus_{i=0}^{2p-1}\mathrm{Hom}_{s-i}(S)\right) + \dim\left(\sum_{i=1}^{p-1}\sum_{j=0}^{p-1-i}||x||^{2(i+j)}\mathrm{Harm}_{s-i-2j}(S)\right)\\ &= \dim\left(\bigoplus_{i=0}^{2p-1}\mathrm{Hom}_{s-i}(S)\right) + \dim W.\end{aligned}$$

Hence we have

$$|X| = \dim(\langle\mathcal{F}_X(S)\rangle) \leq \dim\left(\bigoplus_{i=0}^{2p-1}\mathrm{Hom}_{s-i}(S)\right).$$

Then Proposition 2.2 implies Theorem 1.1. ∎

References

[1] Ei. Bannai, Et. Bannai, *Algebraic Combinatorics on Spheres* , Springer Tokyo, 1999 (in Japanese).

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

[3] A Blokhuis, *An upper bound for the cardinality of s-distance sets in E^d and H^d*, Eindhoven Univ. Techn. Memorandum, 1982 May.

[4] P. Delsarte and J. J. Seidel, *Fisher type inequalities for Euclidean t-designs*, Lin. Algebra and its Appl. **114-115** (1989), 213–230.

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

[6] A. Erdélyi et al. *Higher transcendental functions II*, (Bateman Manuscript Project), MacGraw-Hill, 1953.

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

On the nonexistence of certain type of association schemes whose character table entries are not in a cyclotomic number field

By

Eiichi Bannai (Kyushu University)

and

Edgardo Cureg (De La Salle University, Manila)

この原稿は筑波での私の講演のOHPをそのまま流用しました。
説明が加わってなくて、また手書きで読みにくいとおもいますが、お許し下さい。最後に、OHPの最後のページに述べた未解決問題を質問にした手紙（横山様宛）のコピーも一枚加えました。もし、この問題に対してなにかアイデアがありましたらお知らせ下さい。
(坂内英一)

joint work with

Edgardo Cureg (De La Salle Univ. - Manila)
(Edo)

This work is very preliminary!

$\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$

commutative (or symmetric) assoc. scheme.

$A_i \longleftrightarrow R_i$

$\mathcal{A} = \langle A_0, A_1, \cdots, A_d \rangle = \langle E_0, E_1, \cdots, E_d \rangle$

$(A_0, A_1, \cdots, A_d) = (E_0, E_1, \cdots, E_d) \cdot P$

$P = (P_{ij}) = (P_j(i))_{\substack{0 \le i \le d \\ 0 \le j \le d}}$

character table of $\mathcal{X}$
(1st eigenmatrix)

Open question (X):

Let $K = \mathbb{Q}\left(\left\{ P_j^{(i)} \;\middle|\; \begin{matrix} 0 \le i \le d \\ 0 \le j \le d \end{matrix} \right\}\right)$.

Then $K \subset \mathbb{Q}(\sqrt[n]{1})$ for some n ?

$\left(\Leftrightarrow \mathrm{Gal}(K/\mathbb{Q}) = \text{abelian} \; ? \right)$

(Kronecker)

Remark: ($K/\mathbb{Q}$ is always a Galois's extension.)

Remarks

- This property is true for the character table of a finite group

- This property is true, if G is a (multiplicity-free) transitive permutation gp. on X, and $\{R_i\} \longleftrightarrow$ orbits of G on $X \times X$.

- (Munemasa, 1991)

$$\mathrm{Gal}\left(\mathbb{Q}(\{p_j^{(i)} \mid 0\le i\le d,\ 0\le j\le d\}) \Big/ \mathbb{Q}(\{q_{ij}^{k} \mid 0\le i\le d,\ 0\le j\le d,\ 0\le k\le d\})\right)$$

is abelian.

(q_{ij}^{k}: Krein parameters)

- In particular, if $\forall q_{ij}^{k} \in \mathbb{Q}$,

Then $\mathrm{Gal}(K/\mathbb{Q})$ is abelian.

- (Munemasa, 1991)

$$- : \mathcal{A} \longrightarrow \mathcal{A} \qquad (\mathcal{A} \subset M_{|X|}(\mathbb{C}))$$
$$\downarrow \qquad \downarrow$$
$$x \longmapsto \overline{x} \qquad \text{(complex conjugate)}$$

$$\Longrightarrow \quad - \in Z(\mathrm{Gal}(K/\mathbb{Q}))$$

(center)

We want to study this question (✡).

In particular, we want to find counter examples !

$\sigma \in Gal(K/\mathbb{Q})$

$\Rightarrow$ σ induces a permutation on E_i's. (E_0 is fixed by σ.)

We consider the case where $Gal(K/\mathbb{Q})$ acts transitively on $\{E_1, E_2, \cdots, E_d\}$ (✡)

$\Rightarrow \begin{cases} m_i = m & (1 \le \forall i \le d) \\ k_i = k = m & (1 \le \forall i \le d) \end{cases}$

- $d \le 3 \Rightarrow G = Gal(K/\mathbb{Q})$ is <u>always</u> abelian (without assuming (✡))

Remark

$\begin{cases} d=1 \Rightarrow \mathcal{K} \cong K_{|X|} \ (\Rightarrow K=\mathbb{Q}) \\ d=2 \Rightarrow K \subset \text{a quadratic field over } \mathbb{Q}. \end{cases}$

Suppose $d=3$.

$G = Gal(K/\mathbb{Q}) =$ **non abelian**

$\Rightarrow G \cong S_3$ and G acts E_1, E_2, E_3 transitively.

$\left(\begin{array}{l} m_i = k_i = k \ (1 \le {}^\forall i \le 3). \\ \text{Also, } \mathcal{K} = \text{symmetric} \end{array} \right)$

☺ $Z(S_3)=1$

$$P = \begin{bmatrix} 1 & k & k & k \\ 1 & x_1 & y_1 & z_1 \\ 1 & x_2 & y_2 & z_2 \\ 1 & x_3 & y_3 & z_3 \end{bmatrix}$$

(cf. Mather 1975)

$\Longrightarrow$ by orthogonality relation

$$P = \begin{bmatrix} 1 & k & k & k \\ 1 & x_1 & x_2 & x_3 \\ 1 & x_2 & x_3 & x_1 \\ 1 & x_3 & x_1 & x_2 \end{bmatrix}$$

(up to a permutation)

$\Longrightarrow$ (self-dual).

$\{\gamma_{ij}^k\} = \{p_{ij}^k\} \Longrightarrow G =$ abelian (contradiction)

$d=4$.

Suppose $G = \mathrm{Gal}(K/\mathbb{Q})$ acts transitively on E_1, E_2, E_3, E_4. (and $\mathcal{K}$ = symmetric)

$$P = \begin{bmatrix} 1 & k & k & k & k \\ 1 & x_1 & y_1 & z_1 & w_1 \\ 1 & x_2 & y_2 & z_2 & w_2 \\ 1 & x_3 & y_3 & z_3 & w_3 \\ 1 & x_4 & y_4 & z_4 & w_4 \end{bmatrix} \quad \leftarrow M$$

In M, using orthogonality relations,

- each row sum = each column sum $= -1$
- norm of each row = norm of each column $= 3k+1$
- inner product of two different rows = inner product of two different columns $= -k$

There are 3 free parameters, say x_1, x_2 and y_1.

G is one of D_8, A_4, S_4.

(We don't know whether there exists $\mathcal{K}$ with $G = \mathrm{Gal}(K/\mathbb{Q})$, one of D_8, A_4, S_4.)

Specially interesting case :

$$P = \begin{bmatrix} 1 & k & \cdots & k \\ 1 & & & \\ \vdots & & M & \\ 1 & & & \end{bmatrix}$$

M = multiplication table of non abelian group G.

with

$G = Gal(K/\mathbb{Q})$ acts transitively on $E_1, E_2, \cdots, E_d$.

(In particular, $|G| = d$)

Thm Under the above assumptions, let G be one of

$S_3 (= D_6)$, D_8 and Q_8.

Then we have a contradiction.

Proof of Theorem $f(x) = \prod_{i=1}^{d} (x - x_i)$. In our case

$$Gal(f(x)) = G.$$

Suppose $G = S_3$ or D_8 (D_6). Then it is easy to see that some of the x_i's coincide (by using orthogonality relations), a contradiction.

Suppose $G = Q_8$.

$$P = \begin{bmatrix}
1 & k & k & k & k & k & k & k & k \\
1 & x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\
1 & x_2 & x_3 & x_4 & x_1 & x_7 & x_8 & x_6 & x_5 \\
1 & x_3 & x_4 & x_1 & x_2 & x_6 & x_5 & x_8 & x_7 \\
1 & x_4 & x_1 & x_2 & x_3 & x_8 & x_7 & x_5 & x_6 \\
1 & x_5 & x_8 & x_6 & x_7 & x_3 & x_1 & x_2 & x_4 \\
1 & x_6 & x_7 & x_5 & x_8 & x_1 & x_3 & x_4 & x_2 \\
1 & x_7 & x_5 & x_8 & x_6 & x_4 & x_2 & x_3 & x_1 \\
1 & x_8 & x_6 & x_7 & x_5 & x_2 & x_4 & x_1 & x_3
\end{bmatrix}$$

(i) Suppose $\mathbb{F}$ = symmetric

(i.e., $\forall x_i \in \mathbb{R}$)

By orthogonality relations,

$$\begin{cases} 1+x_1+x_2+x_3+x_4+x_5+x_6+x_7+x_8 = 0 \\ k+(x_2+x_4)(x_5+x_6)+(x_1+x_3)(x_7+x_8) = 0 \\ k+(x_1+x_3)(x_5+x_6)+(x_2+x_4)(x_7+x_8) = 0 \\ k+(x_1+x_3)(x_2+x_4)+(x_5+x_6)(x_7+x_8) = 0 \\ k+2(x_1x_3+x_2x_4+x_5x_6+x_7x_8) = 0 \end{cases}$$

$$\Rightarrow \begin{cases} x_1+x_3 = x_2+x_4 = x_7+x_8 = \dfrac{1+\sqrt{1+8k}}{4} \\ x_5+x_6 = \dfrac{-1+3\sqrt{1+8k}}{4} \end{cases}$$

(or similar solutions)

Then

$$\frac{1+\sqrt{1+8k}}{4} \in (\text{a quadratic extension of } \mathbb{Q})$$

$$\left(\begin{array}{c} \| \\ \text{algebraic integer} \end{array}\right) \Rightarrow \quad 1+8k = \text{a square of an integer}$$

$$P_{ij}^{k} = \frac{k_i k_j}{|X|} \sum_{\ell=0}^{d} \frac{1}{m_\ell^2} Q_\ell(i) Q_\ell(j) \overline{Q_\ell(k)}$$

In our case,

$$Q_i(j) = P_j(i) \in \mathbb{R}$$

if $1 \le i \le 4$, $1 \le j \le 4$.

($\because$ $k_i = m_i = k$, $1 \le \forall i \le 4$)

$$P_{12}^{?} = \frac{(1+8k)(k-2x_2) + \sqrt{1+8k}\,(k-2x_2(1+4x_2))}{8+64k}.$$

$P_{12}^{?} \in \mathbb{Z}$.

$\therefore$ x_2 is a root of a rational coeff. polynomial of degree 2.

$\therefore$ $x_2 \in$ a quadratic ext. of $\mathbb{Q}$.

(contradiction to $\mathrm{Gal}\left(\prod_{i=1}^{8}(x-x_i)\right) = Q_8$)

(ii) The case $\mathfrak{X}$ = non-symmetric is treated similarly.

(We have $x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2 = 1+7k$ instead of $k+2(x_1x_3+x_2x_4+x_5x_6+x_7x_8)=0$.)

(End of Proof of Thm) ⌟

Concluding Remarks

- Similar results are expected for wider classes of groups.
  (Is this true for <u>any</u> finite group ?)
  non abelian

- interplay between
  Galois theory $\longleftrightarrow$ association scheme

- The concept of <u>generic polynomials</u>
  may be useful in this study.
  (suggested by Kazuhiro Yokoyama)

open problem

$$M = \begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{bmatrix} \quad (\forall x_{ij} \in \mathbb{R})$$

$$f_j(x) \overset{\text{def}}{=} \prod_{i=1}^{4} (x - x_{ij}) \in \mathbb{Z}[x]$$

(irreducible poly)

$$Q_j \overset{\text{def}}{=} Q(\{x_{1j}, x_{2j}, x_{3j}, x_{4j}\})$$

Suppose $Q_1 = Q_2 = Q_3 = Q_4$.

$$G = Gal(Q_i/Q).$$

The actions of G on $\{x_{1j}, x_{2j}, x_{3j}, x_{4j}\}$ are the same for $j = 1, 2, 3, 4$.

Suppose, in M,

the colum sum = the row sum $= -1$

the sum of the squares in a colum

= the sum of the squares in a row

$= 3k+1$

the inner product of two different columns

= the inner product of two different rows

$= -k$

$\Longrightarrow$ Can G be one of D_8, A_4, or S_4 ?

(1X1)

横山　様、

お元気でいらっしゃることと思います。
前の問題と関係して、状況はかなりちがいますが、次の問題を
考えています。なにか良いアイデアをいただけたらうれしく思います。

実数（いずれも代数的整数）を要素とする、4x4 行列

[x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4};
x_{2,1}, x_{2,2}, x_{2,3}, x_{2,4};
x_{3,1}, x_{3,2}, x_{3,3}, x_{3,4};
x_{4,1}, x_{4,2}, x_{4,3}, x_{4,4}]

を考えます。k を偶数の自然数として、
各 j 列 の 4 つの元$x_{i,j} (i=1,2,3,4)$ を根に持つ 4 次の(整数係数の
monic な）多項式を
$f_j(x) (j=1,2,3,4)¥in Z[x]$ とします。各j (j=1,2,3,4) に対して、
$f_j(x)$ の根をQ に付加した体をQ_j とします。
$Q_j (j=1,2,3,4) $ 達は全て一致していると仮定し、その体のQ上
のガロア群をG とします。また、G の各元 $¥sigma ¥in G$
は各j (j=1,2,3,4) に対して、$x_{i,j} (i=1,2,3,4)$ 達の上に同じ
置換で働いているとします。

更に、次を仮定します。上の行列の各行、各列の 4 つの元の和は -1 と等しい。
上の行列の各行、各列にあらわれる 4 つの元の 2 乗の和は 3k+1 と等しい。
相異なる 2 つの行、あるいは 2 つの列の間の内積はすべて -k と等しい。

以上の仮定のもとで、群 G が非可換になる場合があるでしょうか？
（ G を位数 8 の二面体群、あるいは、A_4, S_4 のいずれかと仮定
してそれぞれの場合、上の条件を全てみたす場合が存在するでしょうか？
例えば、Gを位数 8 の二面体群に限ればなにか言えるでしょうか？）
もし、この問題が一般に難しいようならば、更に例えば k をある数（例えば
100) 以下として、上の条件を全てみたす場合が存在するでしょうか？）

内積の条件から、f_j 達は全て、
$f_j(x)=x^4+x^3-(3k/2)x^2+¥alpha_jx+¥beta_j $ の形となっています。
内積に関する条件から、例えばx_{1,1}, x_{1,2}, x_{2,1}の 3 つから
残りのx_{i,j} 達は全て決まることがわかります。（また、実数の範囲で考えれば
x_{1,1}, x_{1,2}, x_{2,1}の 3 つは一般に自由に選べることもわかります。）

坂内英一

Some blocking semiovals which admit a homology group

Chihiro Suetake(末竹 千博)

Himeji-kita High School, Himeji, Hyogo 670-0012, Japan

1 Introduction

Definition
Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a finite projective plane.

• A *blocking set* in Π is a set B of points such that for every line $l \in \mathcal{L}$, $l \cap B \neq \phi$, but l is not entirely contained in B.

• A *semioval* in Π is a set C of points such that for every points $P \in C$, there exists a unique line $l \in \mathcal{L}$ such that $l \cap C = \{P\}$. (The idea of a semioval was introduced in [3] and [7].)

• A *blocking semioval* in Π is a set S of points which is both a semioval and a blocking set.

Motivation
The study of blocking semiovals in finite projective planes was motivated by Batten [1] in connection with cryptography. The study was started by Batten and Dover in [2] and Dover in [4,5]

Problems
• Classify all blocking semiovals.

• What can we say about sizes of blocking semiovals in a finite projective plane?

• Construct families of blocking semiovals.

Notation
Let S be a blocking semioval in a finite projective plane $\Pi = (\mathcal{P}, \mathcal{L})$ of order q.
Then, set

$$x_i = |\{l \in \mathcal{L} | |l \cap S| = i\}|$$

and

$$X(S) = (x_1, x_2, \cdots, x_{q-1}).$$

• $x_0 = 0,\ x_1 = |S|$.

• If $q > 3$, then $x_q = 0$ ([4]).

Known families of blocking semiovals
Let $\Pi = (\mathcal{P}, \mathcal{L})$ be a finite projective plane of order q.

(1) Let $q \geq 3$, and let $l_1,\ l_2$, and l_3 be any three nonconcurrent lines. Then

$$T := \{P \in \mathcal{P} | P \in l_1 \cup l_2 \cup l_3,\ P \neq l_1 \cap l_2, l_1 \cap l_3, l_2 \cap l_3\}$$

is a blocking semioval of size $3q - 3$ with $x_{q-1} \neq 0$. (This blocking semioval is called a *vertexless triangle.*)

(2) If $q \geq 5$ and Π contains a Δ−configuration (Any $PG(2,q)$ has this property.), then there exists a blocking semioval of size $3q - 4$ with $X(S) = (3q-4, 3q-6, q^2-7q+14, 2q-6, 0, \cdots, 0, 1, 1, 1)$ ([5,6]).

(3) If q is a square prime power, then there exists a blocking semioval U of size $q\sqrt{q}+1$ in $PG(2,q)$. This blocking semioval is called an *unital.* U has the following property: If l is a line of $PG(2,q)$ with $|l \cap U| \geq 2$, then $|l \cap U| = \sqrt{q}+1$.

Bounds([5])
Let Π be a finite projective plane of order q, and let S be a blocking semioval

in Π.

(1) If $q \geq 7$, then

$$2q+2 \leq |S| \leq q\sqrt{q}+1.$$

(The upper bound was proved by Hubaut and is sharp by the existence of unital. But the lower boud seems not to be sharp.)

(2) If $q \geq 3$ and S has a $(q-k)$−secant, $1 \leq k < q-1$, then

$$\frac{3k+4}{k+2}q - k \leq |S|.$$

(This bound also seems not to be sharp.)

(3) If $q \geq 7$ and $x_{q-1} \neq 0$, then

$$\frac{7}{3}q - 1 \leq |S| \leq 3q-3$$

and the upper bound is met if and only if S is a vertexless triangle.

Constructions

In this note, we consider some blocking semiovals in $PG(2,q)$ which admit a nontrivial homology group, and construct the following two families of blocking semiovals:

(i) If $q = r^e$, $r \geq 3$, r a prime power and $e \geq 2$, then there exist blocking semiovals of size $3q-4$ with $x_{q-1} = 0$ (see Theorem 3.3).

(ii) If $q = r^e$, $r \geq 3$, r a prime power, $e \geq 2$ and $3 \leq n \leq r$, then there exist blocking semiovals of size $3q-n-2$ with $x_{q-1} = 1$ (see Theorem 4.5).

2 Blocking semiovals of homology type

Notation

$V = \{(a,b,c) | a,b,c \in GF(q)\}$:three-dimensional vector space over $GF(q)$
$q \geq 7$

$PG(2,q) = (\mathcal{P}, \mathcal{L})$
$\mathcal{P} := \{P | P \text{ is a one} - \text{dimensional subspace of } V.\}$
$\quad = \{[a,b,c] | a,b,c \in GF(q),\ (a,b,c) \neq (0,0,0)\}$
$[a,b,c] := \{(ax, bx, cx) | x \in GF(q)\}$
$\mathcal{L} := \{l | l \text{ is a two} - \text{dimensional subspace of } V.\}$

$l_0 := \{[0,a,b] | a,b \in GF(q),\ (a,b) \neq (0,0)\}$
$P_0 := [0,0,1] \in l_0$
$2 \leq n \leq q-2$
$P_i := [0,1,a_i] \in l_0\ \ (i = 1,2,\cdots,n)$;distinct
$Q_0 := [1,0,0] \notin l_0$
Ω_i:a subset of $P_iQ_0 - \{Q_0, P_i\}$ with $|\Omega_i| \geq 2\ \ (i \in \{0,1,\cdots,n\})$

$S := (l_0) \cup \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_n - \{P_0, P_1, \cdots, P_n\}$

We will derive a necessary and sufficient condition for S to be a blocking semioval.

$\Delta_0 := \{x \in GF(q) | [1,0,x] \in \Omega_0\} \subseteq GF(q)^*$
$\Delta_i := \{x \in GF(q) | [1,x,a_ix] \in \Omega_i\} \subseteq GF(q)^*$
$(i = 1,2,\cdots,n)$
$\Phi_{jk} := (a_k - a_j)\Delta_k$, $\Phi_{ijk} := \frac{a_k - a_j}{a_i - a_j}\Delta_k$
$(i,j,k \in \{1,2,\cdots,n\},\ i \neq j)$

Assumption 2.1
Assume that $-\Delta_i = \Delta_i$ for all $i \in \{0,1,\cdots,n\}$.

Lemma 2.2
S is a blocking set if and only if the following (i),(ii) *hold.*
(i) $GF(q)^* = \Delta_1 \cup \Delta_2 \cup \cdots \cup \Delta_n$.
(ii) *For any* $i \in \{1,2,\cdots,n\}$,

$$GF(q)^* = \cup_{1 \leq j (\neq i) \leq n} \Phi_{ij} \cup \Delta_0.$$

Lemma 2.3

S is a semioval if and only if the following hold.
(i) *If $a \in GF(q) - \{a_1, a_2, \cdots, a_n\}$, then*

$$GF(q)^* = \Delta_0 \cup \cup_{1 \le i \le n} (a_i - a)\Delta_i.$$

(ii) *If $a \in \Delta_0$, then there exists a unique element $j \in \{1, 2, \cdots, n\}$ such that*

$$a \notin \cup_{1 \le k(\neq j) \le n} \Phi_{jk}$$

, but

$$a \in \cup_{1 \le k(\neq i) \le n} \Phi_{ik}$$

for all $i \in \{1, 2, \cdots, \hat{j}, \cdots, n\}$.
(iii) *Let $i \in \{1, 2, \cdots, n\}$ and $a \in \Delta_i$. Then one of the following* (a) *and* (b) *occurs.*
(a) *If $a \notin \cup_{1 \le k(\neq i) \le n} \Delta_k$, then*

$$a \in \frac{1}{a_i - a_j}\Delta_0 \cup \cup_{1 \le k(\neq i,j) \le n} \Phi_{ijk}$$

for all $j \in \{1, 2, \cdots, \hat{i}, \cdots, n\}$.
(b) *If $a \in \cup_{1 \le k(\neq i) \le n} \Delta_k$, then there exists a unique element $j \in \{1, 2, \cdots, \hat{i}, \cdots, n\}$ such that*

$$a \notin \frac{1}{a_i - a_j}\Delta_0 \cup \cup_{1 \le k(\neq i,j) \le n} \Phi_{ijk}$$

, but

$$a \in \frac{1}{a_i - a_s}\Delta_0 \cup \cup_{1 \le k(\neq i,s) \le n} \Phi_{isk}$$

for all $s \in \{1, 2, \cdots, \hat{i}, \cdots, \hat{j}, \cdots, n\}$.

3 $n = 2$

In this section, under Assumption 2.1 we consider the point set S of $PG(2, q)$ defined Sectin 2, when $n = 2$. Then we may assume that $a_1 = 1, a_2 = 0$. We remark that from the definition of Δ's, $|\Delta_i| \ge 2$ $(i = 0, 1, 2)$.

Theorem 3.1
Let $n = 2$ and $a_1 = 1$, $a_2 = 0$. Then, S is a blocking semioval if and only if the following hold.
(i) *If $i \neq j \in \{0, 1, 2\}$, then*

$$GF(q)^* = \Delta_i \cup \Delta_j.$$

(ii) *If* $a \in GF(q) - \{0,1\}$, *then*

$$GF(q)^* = \Delta_0 \cup (1-a)\Delta_1 \cup a\Delta_2.$$

(iii) *If* $\{i,j,k\} = \{0,1,2\}$, *then*

$$\Delta_i = (\Delta_j - \Delta_k) \cup (\Delta_k - \Delta_j).$$

Corollary 3.2
If S *is a blocking semioval, then* $|S| = 3q-4$ *and, furthermore, when* q *is odd, an involutory homology* $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ *acts on* S.

Theorem 3.4
Let $q = r^e$, $r \geq 3$, r *a prime power and* $e \geq 2$. *Set*

$$\Delta_2 = GF(r)^*.$$

Let Φ *be a nonempty subset of* $GF(r)^*$ *such that* $-\Phi = \Phi$ *and* $\Phi \neq GF(r)^*$. *Here, if* r *is even, let* $2 \leq |\Phi| \leq r-3$. *Set*

$$\Delta_1 = (GF(q)^* - GF(r)^*) \cup \Phi$$

and

$$\Delta_0 = GF(q)^* - \Phi.$$

Then Δ_0, Δ_1 *and* Δ_2 *satisfy* (i),(ii) *and* (iii) *of* Theorem 3.1. *Therefore, the point set* S *corresponding to* Δ_0, Δ_1 *and* Δ_2 *is a blocking semioval of size* $3q-4$ *such that* $x_{q-1} = 0$ *and* $x_{q-2} \neq 0$.

4 $n \geq 3$

In this section we consider the set S of points of $PG(2,q)$ defined in Section 2 for $n \geq 3$.

Assumption 4.1
(i) $q = r^e$, $r \geq 3$, r a prime power and $e \geq 2$.
(ii) $3 \leq n \leq r$ and $GF(r) \supseteq \{a_1, a_2, \cdots, a_n\}$.
(iii) For any $i \in \{0, 1, \cdots, n\}$ and for any $x \in GF(r)^*$, $x\Delta_i = \Delta_i$.

Theorem 4.2
Under Assumption 4.1, *S is a blocking semioval if and only if the following hold.*
(i) *For any $i \in \{0, 1, \cdots, n\}$,*

$$GF(q)^* = \cup_{0 \leq j(\neq i) \leq n} \Delta_j.$$

(ii) *For any $a \in GF(q) - \{a_1, a_2, \cdots, a_n\}$,*

$$GF(q)^* = \cup_{1 \leq i \leq n} (a_i - a)\Delta_i \cup \Delta_0.$$

(iii) *For any $i \in \{0, 1, \cdots, n\}$ and for any $a \in \Delta_i$, there exists a unique element $j \in \{0, 1, \cdots, \hat{i}, \cdots, n\}$ such that $a \in \Delta_j$.*

Theorem 4.3
Under Assumption 4.1, *S is a blocking semioval if and only if for all distinct $i, j \in \{0, 1, \cdots, n\}$ there exists a subset Δ_{ij} of $GF(q)^*$ which satisfies the following.*
(i) *Each Δ_{ij} is closed under multiplication by $GF(r)^*$.*
(ii) *For all distinct $i, j \in \{0, 1, \cdots, n\}$,*

$$\Delta_{ij} = \Delta_{ji}.$$

(iii) *For any $i \in \{0, 1, \cdots, n\}$,*

$$\Delta_i = \cup_{0 \leq j(\neq i) \leq n} \Delta_{ij} \neq \phi.$$

(iv) $GF(q)^* = \cup_{0 \leq i < j \leq n} \Delta_{ij}$ *is a disjoint union.*
(v) *For any $a \in GF(q) - \{a_1, \cdots, a_n\}$,*

$$GF(q)^* = \cup_{1 \leq i \leq n} (a_i - a)\Delta_i \cup \Delta_0.$$

Corollary 4.4 *If S is a blocking semioval, then $|S| = 3q - n - 2$ and the homology* $\begin{pmatrix} 1 & 0 & 0 \\ 0 & s & 0 \\ 0 & 0 & s \end{pmatrix}$ *$(s \in GF(r)^*)$ acts on S.*

Theorem 4.5

Assume Assumtion 4.1. *Set*

$$\Delta_0 = GF(q)^*$$

and let

$$GF(q)^* = \Delta_1 \cup \cdots \cup \Delta_n$$

be a mutually disjoint union. Then $\Delta_0, \Delta_1, \cdots, \Delta_n$ satisfy (i),(ii) *and* (iii) *of Theorem* 4.2, *and the size of the blocking semioval corresponding to $\Delta_0, \Delta_1, \cdots, \Delta_n$ is $3q - n - 2$ and $x_{q-1} = 1$.*

Problem

Can we construct a family of blocking semiovales of size $3q - n - 2$ with $x_{q-1} = 0$?

References

[1] L. M. Batten, Determining sets, submitted.

[2] L. M. Batten and J. M. Dover, Blocking semiovals with three intersection sizes, preprint.

[3] F. Buekenhout, Characterizations of semiquadrics. A survey., *Teorie Combinatorie (Rome,* 1973), *vol.* I *Atti Acc. Naz. Lincei* **17**, 1976, 393 – 421.

[4] J. M. Dover, Semiovals with large collinear subsets, *J. Geom.*, to appear.

[5] J. M. Dover, A lower bound on blocking semiovals, *Europ. J. Combin.*, to appear.

[6] C. Suetake, Two families of blocking semiovals, *Europ. J. Combin.* to appear.

[7] J. A. Thas, On semiovals and semiovoids, *Geom. Ded.* 3 (1974), 229–231.

Constructions of (T, M, S)-nets from twisted cubics in PG$(3, q)$

Ryoh Fuji-Hara and Ying Miao
Institute of Policy and Planning Sciences
University of Tsukuba
Tsukuba 305-8573, Japan
fujihara@sk.tsukuba.ac.jp and miao@sk.tsukuba.ac.jp

Abstract

It is known that (T, M, S)-nets are equivalent to some class of ordered orthogonal arrays, and linear ordered orthogonal arrays with strength 4 are equivalent to theta configurations in finite projective geometries. In this paper, theta configurations are constructed from twisted cubics in PG$(3, q)$. These imply the existence of $(0, 4, q+1)$-nets in base q for all prime powers q.

1 Introduction

The idea of a (T, M, S)-net in base b was introduced by Niederreiter [12] in 1987. Its applications to two important methods for pseudorandom number generation, namely the digital multistep method and the generalized feedback shift register method, which in turn can be employed in cryptographic protocols, were also presented in [12]. This new concept significantly generalized that of a family of low discrepancy point sets in the S-dimensional unit cube $[0, 1)^S$ due to Sobol' [14], which are useful for quasi-Monte Carlo methods such as numerical integration. The use of (T, M, S)-nets in the computation of definite integrals has had particular impact in the area of finance [1].

We begin with Niederreiter's definition of a (T, M, S)-net. Let $S \geq 1$ and $b \geq 2$ be integers. An *elementary interval* in base b is an interval of the form

$$E = \prod_{i=1}^{S} [a_i b^{-d_i}, (a_i + 1)b^{-d_i}),$$

where a_i and d_i are non-negative integers such that $0 \leq a_i < b^{d_i}$ for $1 \leq i \leq S$. The *volume* of E is

$$\prod_{i=1}^{S} b^{-d_i} = b^{-\sum_{i=1}^{S} d_i}.$$

For integers $0 \leq T \leq M$, a (T, M, S)-*net* in base b is a set $\mathcal{N}$ of b^M points in the S-dimensional unit cube $[0, 1)^S$ such that every elementary interval E in base b having volume b^{T-M} contains exactly b^T points of $\mathcal{N}$.

(T, M, S)-nets have received considerable attention in recent literature. Various connections with other areas have arisen in the study of (T, M, S)-nets, e.g. with finite fields, algebraic coding theory, and finite projective geometries. Especially, (T, M, S)-nets have been characterized by combinatorial structures called *orthogonal arrays*, which are defined below.

Let A be an $m \times s$ array over the set V of b symbols, and R be a subset of columns of A. We say R is *orthogonal* if R contains every $|R|$-tuple over V exactly $m/b^{|R|}$ times as rows. If A is orthogonal for any t-subset R of columns of A, then A is called an *orthogonal array* (OA) of strength t, denoted by $\mathrm{OA}_\lambda(t, s, b)$, where $\lambda = m/b^t$.

Schmid [13, 11] proved that (T, M, S)-nets are equivalent to a type of orthogonal arrays called *orthogonal orthogonal arrays*. Lawrence [7, 8] independently showed an equivalent result in terms of *generalized orthogonal arrays*. In this paper, we will follow Edel and Bierbrauer [3], and Martin and Stinson [9, 10] in using the term *ordered orthogonal arrays*. Such arrays were also called *cubical orthogonal arrays* by Colbourn, Dinitz and Stinson in [2].

Let V be a set of b symbols. An *ordered orthogonal array* (OOA) A of strength t is an $m \times sl$ array over V which satisfies the following properties:

1. The columns of A are partitioned into s groups of l columns, denoted by $G_1, G_2, \cdots, G_s$;

2. Let $(t_1, t_2, ..., t_s)$ be an s-tuple of non-negative integers such that $\sum_{i=1}^{s} t_i = t$, where $0 \leq t_i \leq l$ for $1 \leq i \leq s$. If R is the subset of the columns of A obtained by taking the first t_i columns within each group G_i, $1 \leq i \leq s$, then A is orthogonal for such an R.

We use the notation $\mathrm{OOA}_\lambda(t, s, l, b)$, where $\lambda = m/b^l$, or $\mathrm{OOA}_\lambda(t, s, b)$ when $t = l$.

When $l = 1$, the above definition reduces to that of an orthogonal array, i.e., an $\mathrm{OOA}_\lambda(t, s, 1, b)$ is equivalent to an $\mathrm{OA}_\lambda(t, s, b)$. When $l = t$, we have the following important results.

Theorem 1.1 *([7, 13]) There exists a (T, M, S)-net in base b if and only if there exists an $OOA_{b^T}(M - T, S, b)$.*

Corollary 1.2 *There exists an $OOA_{b^T}(2, S, b)$ if and only if there exists an $OA_{b^T}(2, S, b)$.*

When $t_1 = t_2 = \cdots = t_s = 1$, we obtain an orthogonal array $\mathrm{OA}_\lambda(t, s, b)$.

Theorem 1.3 *If there exists an $OOA_\lambda(t, s, l, b)$, then there exists an $OA_\lambda(t, s, b)$.*

In an earlier paper [4], we introduced the concepts of a linear orthogonal array and a linear ordered orthogonal array, and then tried to determine their equivalent configurations in finite projective geometries. These geometrical configurations were used to investigate the existence problems of such linear arrays. These, in turn, yielded the existence of the corresponding (T, M, S)-nets in base b.

Consider an $m \times s$ orthogonal array (or ordered orthogonal array, respectively) as a set of rows $\boldsymbol{A}$ over the finite field $\mathrm{GF}(b)$, where b is a prime power. If $\boldsymbol{A}$ is a linear space over $\mathrm{GF}(b)$, then $\boldsymbol{A}$ is said to be a *linear orthogonal array* (or *linear ordered orthogonal array*, respectively). Note that, since $\boldsymbol{A}$ is a set of rows, no repeated rows are permitted to occur in any linear orthogonal array (or linear ordered orthogonal array, respectively). Fuji-Hara and Miao [4] showed, among others, the following result:

Theorem 1.4 *When $b \neq 2$, there exists a linear $OOA_\lambda(3, s, b)$ if and only if there exists a linear $OA_\lambda(3, s, b)$, where $\lambda = b^{n-3}$, $n \geq 3$.*

2 Theta configurations in $\mathrm{PG}(n-1, q)$

Suppose that $\mathcal{S}$ is a set of s points in a projective geometry $\mathrm{PG}(n-1, q)$ over $\mathrm{GF}(q)$, $n \geq 4$. A *tangent line* (or *unisecant*) l to $\mathcal{S}$ at a point $P \in \mathcal{S}$ is

a line such that $l \cap \mathcal{S} = \{P\}$. A *tangent plane to* $\mathcal{S}$ at P is a plane π such that $\pi \cap \mathcal{S} = \{P\}$. For points $P_1, P_2, \ldots, P_k$ of $\mathrm{PG}(n-1,q)$, if there is a plane containing these points, then $P_1, P_2, \ldots, P_k$ are said to be *coplanar*.

Let $\mathcal{S} = \{P_1, P_2, \ldots, P_s\}$ be a set of s points in $\mathrm{PG}(n-1,q)$. We consider the following configuration in $\mathrm{PG}(n-1,q)$ for $n \geq 4$:

(C1) no four points of $\mathcal{S}$ are coplanar;

(C2) for $1 \leq i \leq s$, l_i is a tangent line to $\mathcal{S}$ at the point $P_i \in \mathcal{S}$ and every plane containing l_i meets $\mathcal{S}$ in at most one point other than P_i.

(C3) $l_1, l_2, \ldots, l_s$ are mutually disjoint;

(C4) π_i is a tangent plane to $\mathcal{S}$ at the point $P_i \in \mathcal{S}$ containing the tangent line l_i for $1 \leq i \leq s$.

Such a set $\{\mathcal{S}; l_1, l_2, \ldots, l_s; \pi_1, \pi_2, \ldots, \pi_s\}$ of points, tangent lines and tangent planes is called a *theta configuration* for $\mathcal{S}$, and is denoted by $\Theta(\mathcal{S})$. The following results can be found in Fuji-Hara and Miao [4].

Theorem 2.1 *There exists a linear* $OOA_{q^{n-4}}(4, s, q)$ *if and only if there exists a theta configuration* $\Theta(\mathcal{S})$ *for a set* $\mathcal{S}$ *of* s *points in* $PG(n-1,q)$.

Theorem 2.2 *If there exists a linear* $OOA_{q^{n-4}}(4, s, q)$, *then the following inequality holds:*

$$(q+1)s + (q-1)\binom{s}{2} \leq \frac{q^n - 1}{q-1}.$$

Theorem 2.3 *If there exists a linear* $OOA_{q^{n-4}}(4, s, q)$, *then the following inequality holds:*

$$s \leq \frac{q^{n-2} - 1}{q-1}.$$

We note that the bound required for s in Theorem 2.3 is larger than that in Theorem 2.2 for $n \geq 5$. When $n = 4$, i.e. in $\mathrm{PG}(3,q)$, the inequality $s \leq q+1$ holds. As a consequence, we [4] showed that usually it is not necessary to pay attention to the condition (C4) of the theta configuration.

3 Conics and Cones

A *k-arc* in $\mathrm{PG}(n-1,q)$ is a set of k points no n of which are in a hyperplane of $\mathrm{PG}(n-1,q)$. In $\mathrm{PG}(2,q)$ and $\mathrm{PG}(3,q)$, it is a set of k points no three of which are collinear, and no four of which are coplanar, respectively. We have the well-known result in $\mathrm{PG}(2,q)$ that $k \leq q+1$ or $k \leq q+2$ as q is odd or even.

Theorem 3.1 (Lemma 21.2.1, Theorem 21.2.4 and Theorem 21.3.8 of [5]) *There exists a k-arc in PG(3,q) if and only if*

$$k \leq \begin{cases} 5 & \text{if } q = 2,3; \\ q+1 & \text{if } q \geq 4. \end{cases}$$

Let π and P be a plane and a point in $\mathrm{PG}(3,q)$, respectively, such that P is not on π. The *projection from P onto* π in $\mathrm{PG}(3,q)$ is the map $\gamma_P : Q \mapsto PQ \cap \pi$ for any point Q in $\mathrm{PG}(3,q)$ being not P.

A *conic* is a point set of a non-singular quadrics in $\mathrm{PG}(2,q)$ $\{(X_0 : X_1 : X_2) \mid a_{00}{X_0}^2 + a_{11}{X_1}^2 + a_{22}{X_2}^2 + a_{01}X_0X_1 + a_{02}X_0X_2 + a_{12}X_1X_2 = 0\}$, where $a_{ij} \in \mathrm{GF}(q)$ are not all zero. From Lemma 7.7 of [6], any conic in $\mathrm{PG}(2,q)$ is a $(q+1)$-arc. Conversely, by Theorem 8.5 and Theorem 8.14 of [6], when q is odd, any $(q+1)$-arc in $\mathrm{PG}(2,q)$ is a conic; and by Lemma 8.21 and Corollary 8.32 of [6], when $q = 2, 4$, and 8, every $(q+2)$-arc in $\mathrm{PG}(2,q)$ contains a conic.

A *cone* $\Pi(P; l_0, l_1, ..., l_q)$ is a set of $q+1$ lines in $\mathrm{PG}(3,q)$, $l_0, l_1, .., l_q$, through a point P such that any plane not through P meets the cone in the points of a conic. A cone is also generated by a point P and a conic C on a plane π not through P, denoted by $\Pi(P, \mathrm{C})$. Note that no three lines of a cone are coplanar.

Theorem 3.2 (Corollary 7.5 of [6]) *In PG(2,q) with $q \geq 4$, there is a unique conic through a 5-arc.*

Theorem 3.3 *Let $C_1 = \Pi(P; l_0, l_1, ..., l_q)$ and $C_2 = \Pi(Q; m_0, m_1, ..., m_q)$, $P \neq Q$, be cones in PG(3,q), $q \geq 4$, If they have a line in common, say $l_0 = m_0$, then one of the following two cases holds:*

(i) each line of C_1 meets a line of C_2, say $l_i \cap m_i = P_i$ for $i = 1, 2, ..., q$;

(ii) there are $q-1$ pairs of lines (l_i, m_i) which are concurrent, say $l_i \cap m_i = P_i$ for $i = 2, ..., q$, and there is a pair of lines which are mutually skew, say $l_1 \cap m_1 = \phi$.

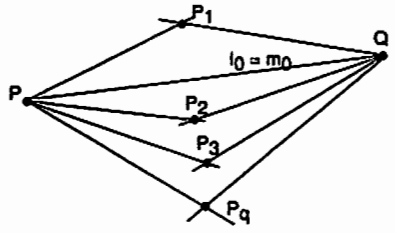


Figure 1: case (i)

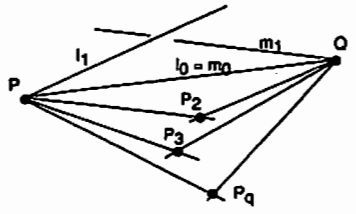


Figure 2: case (ii)

Proof Let π be a plane not through P. Consider the projection γ_P from P onto π. If $\gamma_P(m_i) = \gamma_P(m_j), i \neq j$, then m_i, m_j and m_0 are coplanar. Hence the lines $\gamma_P(m_1), \ldots, \gamma_P(m_q)$ are distinct and all pass through the point $\gamma_P(Q)$. Each line l_i for $i = 0, 1, ..., q$ maps onto π at the point $\gamma_P(l_i)$. Note $\gamma_P(l_0) = \gamma_P(Q)$. Since no three lines of l_i's are coplanar, no two points of $\gamma_P(l_i), i = 1, \ldots, q$, are on a line passing through $\gamma_P(Q)$, including $\gamma_P(m_i)$'s. Therefore, we have only two cases: (i) on each line $\gamma_P(m_i)$, there is exactly one point of $\gamma_P(l_i)$'s on it, (ii) $q-1$ points in $\gamma_P(l_i)$'s are on the lines $\gamma_P(m_i)$'s and the remaining one is not on any line of $\gamma_P(m_i)$'s. In the both cases, if a point $\gamma_P(l_i)$ is on a line $\gamma_P(m_i)$ then $\gamma_P(l_i)$ is the image of the intersection point $P_i = l_i \cap m_i$. □

For $q = 2, 3$, the number of intersection points is at most 3. Therefore the both cases are true.

Theorem 3.4 *The set of points $\{P_1, P_2, ..., P_q\}$ of (i) in Theorem 3.3 is coplanar and $\{P, Q, P_2, .., P_q\}$ of (ii) is a $(q+1)$-arc in $PG(3, q)$, $q \geq 4$.*

Proof (i) Let $\mathcal{P}_1 = \{P_1, P_2, ..., P_q\}$. If there are no four points of $\mathcal{P}_1$ which are coplanar, then $\mathcal{P}_1 \cup \{P, Q\}$ is $(q+2)$-arc in PG$(3, q)$. This goes beyond the bound. Suppose that there is a plane π which contains four points of $\mathcal{P}_1$. Note that π contains neither P nor Q. With the point $\pi \cap l_0$, the five points in π are contained in a unique conic from Theorem 3.2. Therefore all points of $\mathcal{P}_1$ are on π.

(ii) Let $\mathcal{P}_2 = \{P_2, P_3, ..., P_q\}$. Suppose that there is a plane π which contains four points of $\mathcal{P}_2$. π contains neither P nor Q. With the point $\pi \cap l_1$, the five points in π are contained in a unique conic from Theorem 3.2. The conic is the intersection of π with both C_1 and C_2. Since $l_1 \cap \pi$ and $m_1 \cap \pi$ are distinct points, the conic contains $q+2$ points. So $\mathcal{P}_2$ is a $(q-1)$-arc in PG$(3,q)$. Since any plane through P contains at most two lines of C_1, $\mathcal{P}_2 \cup \{P\}$ is a q-arc in PG$(3,q)$. Next, we show that the four points P_i, P_j, P, Q, $i \neq j$, $i, j \notin \{0,1\}$, are not coplanar. If P_i, P_j, P, Q are coplanar, then the lines l_i and m_j are concurrent. This implies that l_i, l_j and l_0 all meet the line m_j, that is, these three lines are coplanar. This contradicts the property of a cone. □

4 $\mathbf{OOA}_1(4, q+1, q)$ and $(0, 4, q+1)$-net

A *twisted cubic* in PG$(3,q)$ is the set of points which may be written in the canonical form below:

$$\mathcal{T} = \{(t^3, t^2, t, 1) |\ t \in GF(q)\} \cup \{(1,0,0,0)\}.$$

From Theorem 21.1.1(iv) of [5], any twisted cubic is a $(q+1)$-arc in PG$(3,q)$ for $q \geq 3$. When $q = 2$, it is a conic. Conversely, from Theorem 21.2.3 and Theorem 21.3.17(v) of [5], in PG$(3,q)$, $q = 2, 4, 8, 16, 64$, or odd, any $(q+1)$-arc is also a twisted cubic.

Lemma 4.1 *In PG$(2,q)$, $q = 2, 4$, or odd, a q-arc is contained in a conic.*

Proof See Lemma 8.21 and Theorem 10.28 of [6]. □

Theorem 4.2 *Let $\mathcal{T}$ be a twisted cubic in PG$(3,q)$. For any point $P \in \mathcal{T}$, the set of q lines $C(P) = \{PQ \mid Q \in \mathcal{T} \setminus \{P\}\}$ is contained in a cone.*

Proof Corollary 2 in page 237 of [5] implies that $C(P)$ is contained in a cone for $q \geq 7$. For $q < 7$, consider the projection from P to a plane π not through P. The image of $\mathcal{T}$ on the plane π is a q-arc. Lemma 4.1 says that any q-arc is contained in a conic $\mathbf{C}$ in PG$(2,q)$, $q = 2, 4$ and odd. So the cone $\Pi(P, \mathbf{C})$ contains $C(P)$. □

Theorem 4.3 *In $PG(3,q)$, q a prime power, there exists a Θ-configuration $\Theta(S)$, $|S| = s$, if and only if $1 \leq s \leq q+1$.*

Proof From Theorems 2.1 and 2.3, the existence of a Θ-configuration can imply the inequality $s \leq q+1$ in $\mathrm{PG}(3,q)$. Conversely, let S be a twisted cubic $\mathcal{T}$. For any point $P \in \mathcal{T}$, there is a cone $C(P) = C(P; PP_1, PP_2, ..., PP_q, l_P)$, where $P_i \in \mathcal{T} \setminus \{P\}$ and l_P is a tangent line at P to $\mathcal{T}$. Since l_P is a line of the cone, every plane through l_P meet $\mathcal{T}$ in at most one point other than P. For $Q \in \mathcal{T}$, $Q \neq P$, there is also a cone $C(Q)$ including a tangent line l_Q to $\mathcal{T}$ at Q. From Theorem 3.4, l_P and l_Q are mutually skew. Since $s = q+1$, there is a tangent plane π_P to $\mathcal{T}$ including the tangent line l_P for each point $P \in \mathcal{T}$. So $\{\mathcal{T}; \{l_P | P \in \mathcal{T}\}; \{\pi_P | P \in \mathcal{T}\}\}$ is a Θ-configuration. For $q = 2, 3$, Θ-configurations are constructed by a computer. □

From Theorem 1.1 and Theorem 2.1, the following results are immediate:

Corollary 4.4 *There exists a linear ordered orthogonal array $OOA_1(4, s, q)$ if and only if $1 \leq s \leq q+1$, q a prime power.*

Corollary 4.5 *There exists a (0,4,q+1)-net in base q for any prime power q.*

References

[1] P.P. Boyle, M. Broadie and P. Glasserman, *Monte Carlo methods for security pricing,* J. Economic Dynamics and Control **21** (1997), 1267–1321.

[2] C.J. Colbourn, J.H. Dinitz, D.R. Stinson, *Applications of combinatorial designs to communications, cryptography, and networking,* in: *Surveys in Combinatorics*, 1999 (Canterbury), 37–100, London Math. Soc. Lecture Note Ser., 267, Cambridge Univ. Press, Cambridge, 1999.

[3] Y. Edel and J. Bierbrauer, *Construction of digital nets from BCH-codes,* in: *Monte Carlo and Quasi-Monte Carlo Methods 1996 (Salzburg)*, Lecture Notes in Statist. **127** (1998), 221–231.

[4] R. Fuji-Hara and Y. Miao, *Geometrical Constructions for Ordered Orthogonal Arrays and (T, M, S)-Nets,* preprint

[5] J.W.P. Hirschfeld, *Finite Projective Spaces of Three Dimensions,* Oxfrod University Press, New York, 1985.

[6] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields,* Second Edition, Oxfrod University Press, New York, 1998.

[7] K.M. Lawrence, *Combinatorial bounds and constructions in the theory of uniform point distributions in unit cubes, connections with orthogonal arrays and a poset generalization of a related problem in coding theory,* PhD Thesis, University of Wisconsin-madison, USA, 1995.

[8] K.M. Lawrence, *A combinatorial interpretation of* (t, m, s)*-nets in base* b*,* J. Combin. Des. **4** (1996), 275–293.

[9] W.J. Martin and D.R. Stinson, *A generalized Rao bound for ordered orthogonal arrays and* (t, m, s)*-nets,* Canad. Math. Bull. **42** (1999), 359–370.

[10] W.J. Martin and D.R. Stinson, *Association schemes for ordered orthogonal arrays and* (T, M, S)*-nets,* Canad. J. Math. **51** (1999), 326–346.

[11] G.L. Mullen and W.Ch. Schmid, *An equivalence between* (T, M, S)*-nets and strongly orthogonal hypercubes,* J. Combin. Theory A **76** (1996), 164-174.

[12] H. Niederreiter, *Point sets and sequences with small discrepancy,* Monatsh. Math. **104** (1987), 273–337.

[13] W. Ch. Schmid, (t, m, s)-Nets: digital constructions and combinatorial aspects, PhD Thesis, University of Salzburg, Austria, 1995.

[14] M. Sobol', *The distribution of points in a cube and the approximate evaluation of integrals* (in Russian), Ž. Vyčisl. Mat. i. Mat. Fiz. **7** (1967), 784–802.

On Some Relationships Among the Association Schemes of Finite Orthogonal Groups Acting on Hyperplanes

田中　太初
九大・数理

この原稿では、筆者が現在関心を持って取り組んでいる association scheme、すなわち標数2の有限体上の直交群 $GO_{2m+1}(q)$ の、$GO_{2m+1}(q)/GO^{\pm}_{2m}(q)$ への作用より構成される association scheme $\mathfrak{X}(GO_{2m+1}(q), GO_{2m+1}(q)/GO^{\pm}_{2m}(q))$ に関して筆者が調べた結果を、主に $GO_{2m+1}(q)/GO^{+}_{2m}(q)$ の場合について報告する。なお、ここで用いられる基本的事実・用語等については Bannai-Ito [3], Munemasa [7], ATLAS [6] を参照されたい。

以下 $q = 2^r$ $(r \geq 1)$ とする。$\mathbb{V}$ を $GF(q)$ 上 $(2m+1)$-次元ベクトル空間、$Q : \mathbb{V} \longrightarrow GF(q)$ を $\mathbb{V}$ 上の非退化二次形式、$f : \mathbb{V} \times \mathbb{V} \longrightarrow GF(q)$ を同伴交代形式とする。また、$\mathbb{V}$ の2点部分集合 $\{u, v\}$ が $Q(u) = Q(v) = 0$, $f(u, v) = 1$ を満たすとき $\{u, v\}$ を hyperbolic pair と呼ぶ。$\mathrm{Rad}\, f := \{v \in \mathbb{V} \mid f(u, v) = 0 \text{ for every } u \in \mathbb{V}\}$ と置くと $\mathrm{Rad}\, f$ は1次元部分空間であり、$Q(r) = 1$ となる元 $v \in \mathbb{V}$ が存在して $\mathrm{Rad}\, f = \langle r \rangle$ と書ける。また、ある部分空間への Q の制限が non-degenerate (resp. degenerate, positive-type, negative-type) であるときその部分空間を non-degenerate (resp. degenerate, positive-type, negative-type) と呼ぶ。直交群 $GO_{2m+1}(q)$ は positive-type hyperplanes の全体の集合 $\Omega = \Omega_{2m+1}(q)$ に可移に作用し、ある元の安定部分群は $GO^{+}_{2m}(q)$ と同型な群である。よって

$$\begin{aligned} |\Omega| &= \frac{q^{m^2}(q^{2m}-1)(q^{2m-2}-1)\dots(q^2-1)}{2q^{m(m-1)}(q^m-1)(q^{2m-2}-1)\dots(q^2-1)} \\ &= \frac{q^m(q^m+1)}{2} \end{aligned}$$

を得る (cf. ATLAS[6, p.xii])。

Ω の異なる2つの元 U, V について $U \cap V$ が non-degenerate の場合、$Q(w) = 1$ を満たす元 $w \in U \cap V$ が存在して,

$$U \cap V = \langle w \rangle^{\perp} \cap U = \langle w \rangle^{\perp} \cap V$$

と表せる。さらに $U \cap V$ の任意の non-degenerate hyperplane W に対し

$$U = \langle u, w \rangle \perp W,\ V = \langle v, w \rangle \perp W$$

かつ $Q(u) = Q(v)$, $f(u, w) = f(v, w) = 1$ を満たす $u \in U$, $v \in V$ が存在する。この u, v に対し

$$\Delta := \frac{f(u, v)}{f(u, v) + 1}$$

と定義すると、Δ は well-defined かつ $\Delta \neq 0,1$ であり、$\Delta(U,V) := \{\Delta, \Delta^{-1}\}$ は W, u, v の取り方に依らず定まることが示され、これを用いて $\mathfrak{X}(GO_{2m+1}(q),\Omega)$ の関係は次のように記述される:

$$
\begin{aligned}
R_0 &:= \{(U,U) \in \Omega \times \Omega \mid U \in \Omega\},\\
R_1 &:= \{(U,V) \in \Omega \times \Omega - R_0 \mid U \cap V : \text{degenerate}\},\\
R_i &:= \{(U,V) \in \Omega \times \Omega - R_0 \mid U \cap V : \text{non-degenerate, } \Delta(U,V) = \{\nu^{i-1}, \nu^{-(i-1)}\}\}\\
&\qquad (2 \leq i \leq \tfrac{q}{2})
\end{aligned}
$$

ここで $\nu \in GF(q)^*$ は $GF(q)$ の原始根である。$\mathfrak{X}(GO_{2m+1}(q),\Omega)$ はクラス $\frac{q}{2}$ の対称な association scheme である。

交叉数 p_{ij}^k は次のように与えられる。

補題 1.

$$
p_{ij}^1 = p_{ij}^1 = \begin{cases} q^{m-1}(2q^{m-1}+q-1)-2 & \text{if } i=j=1 \\ q^{m-1}(2q^{m-1}-1) & \text{if } 2 \leq i=j \leq \frac{q}{2} \\ 2q^{2m-2} & \text{if } 1 \leq i < j \leq \frac{q}{2} \end{cases}
$$

$$
p_{1j}^k = p_{j1}^k = \begin{cases} (2q^{m-1}-1)(q^{m-1}+1) & \text{if } 2 \leq j=k \leq \frac{q}{2} \\ 2q^{m-1}(q^{m-1}+1) & \text{if } 1 \leq j \leq \frac{q}{2},\ 2 \leq k \leq \frac{q}{2},\ j \neq k \end{cases}
$$

$2 \leq i,j,k \leq \frac{q}{2}$ のときは、i,j,k の選び方に依り

$$
p_{ij}^k = \begin{cases} q^{m-1}(2q^{m-1}+1) \\ q^{m-1}(2q^{m-1}-1) \\ 2q^{m-1}(q^{m-1}+1) \\ 2q^{m-1}(q^{m-1}-1) \\ 2q^{2m-2} \end{cases}
$$

となる。

Proof. 煩雑過ぎるので省略する。 □

補題 1 から直ちに次の補題が得られる。

補題 2. $\mathfrak{X}(GO_3(q),\Omega_3(q))$ の交叉数を b_{ij}^k とする。このとき

$$
\begin{aligned}
p_{11}^1 &= 2q^{m-1}(q^{m-1}-1) + q^{m-1}(b_{11}^1+2) - 2\\
p_{1i}^i &= p_{i1}^i = 2q^{m-1}(q^{m-1}-1) + q^{m-1}(b_{1i}^i+1) - 1 \quad \text{for } 2 \leq i \leq \tfrac{q}{2}
\end{aligned}
$$

他の $1 \leq i,j,k \leq \frac{q}{2}$ に対しては

$$
p_{ij}^k = 2q^{m-1}(q^{m-1}-1) + q^{m-1}b_{ij}^k
$$

となる。

Proof. 略。 □

$\mathfrak{X}(GO_3(q),\Omega_3(q))$ の指標表 $\tilde{P}=(\tilde{p}_j(i))$ は次のように記述される (cf. [8, §3])。

$$\tilde{P}=\begin{bmatrix} 1 & 2(q-1) & (q-1) & (q-1) & \dots & (q-1) \\ 1 & q-3 & -2 & -2 & \dots & -2 \\ 1 & -2 & & & & \\ 1 & -2 & & & & \\ \vdots & \vdots & & (\chi_{ij})_{2\le i,j\le \frac{q}{2}} & & \\ 1 & -2 & & & & \end{bmatrix}$$

定理 1. $\mathfrak{X}(GO_{2m+1}(q),\Omega_{2m+1}(q))$ の指標表 $P=(p_j(i))$ は次で与えられる。

$$P=\begin{bmatrix} 1 & (q^{m-1}+1)(q^m-1) & q^{m-1}(q^m-1) & q^{m-1}(q^m-1) & \dots & q^{m-1}(q^m-1) \\ 1 & (q-2)q^{m-1}-1 & -2q^{m-1} & -2q^{m-1} & \dots & -2q^{m-1} \\ 1 & -(q^{m-1}+1) & & & & \\ 1 & -(q^{m-1}+1) & & & & \\ \vdots & \vdots & & (q^{m-1}\chi_{ij})_{2\le i,j\le \frac{q}{2}} & & \\ 1 & -(q^{m-1}+1) & & & & \end{bmatrix}$$

すなわち

$$\begin{aligned} &p_0(i)=1 \quad \textit{for } 0\le i\le \tfrac{q}{2} \\ &p_j(0)=k_j \quad \textit{for } 0\le j\le \tfrac{q}{2} \\ &p_1(i)=q^{m-1}\tilde{p}_1(i)+q^{m-1}-1 \quad \textit{for } 1\le i\le \tfrac{q}{2} \\ &p_j(i)=q^{m-1}\tilde{p}_j(i) \quad \textit{for } 1\le i\le \tfrac{q}{2},\ 2\le j\le \tfrac{q}{2} \end{aligned}$$

Proof. 補題 2 と上の関係式を用いて

$$B_j\begin{pmatrix} p_0(\alpha) \\ p_1(\alpha) \\ \vdots \\ p_{\frac{q}{2}}(\alpha) \end{pmatrix}=p_j(\alpha)\begin{pmatrix} p_0(\alpha) \\ p_1(\alpha) \\ \vdots \\ p_{\frac{q}{2}}(\alpha) \end{pmatrix} \quad \text{for all } j,\alpha$$

を示せば良い (cf. Bannai-Ito [3, §2.5], Bannai-Hao-Song [2, §6])。 □

定理 1 は、$\mathfrak{X}(GO_{2m+1}(q),\Omega_{2m+1}(q))$ の指標表に $q^{m-1}\longmapsto 1$ という変換を施すことにより $\mathfrak{X}(GO_3(q),\Omega_3(q))$ の指標表が得られることを主張している。また、$\mathbb{V}$ の negative-type hyperplanes の全体の集合を $\Theta=\Theta_{2m+1}(q)$ と表すと、$\mathfrak{X}(GO_{2m+1}(q),\Theta_{2m+1}(q))$ についてもこれと同様の結果が成り立つ。なお奇標数の場合は Bannai-Hao-Song[2, §6,§7] に於いて既に調べられており、前述の補題 2 及び定理 1 は [2] の全くの模倣であることを書き添えておく。さらに $\mathfrak{X}(GO_{2m+1}(q),\Theta_{2m+1}(q))$ の指標表は $\mathfrak{X}(GO_{2m+1}(q),\Omega_{2m+1}(q))$ の指標表に $q^{m-1}\longmapsto -q^{m-1}$ という変換を施すことにより得られることも示される (cf. Bannai-Kwok-Song[4])。筆者は $\Omega_{2m+1}(q)$ 及び $\Theta_{2m+1}(q)$ を標数 2 の有限体上のベクトル空間に於ける球面の類似と捉えてい

るが、それらの球函数（すなわち指標表）は本質的に $\Omega_3(q)$（又は $\Theta_3(q)$）の球函数により controll されていることになる。この様な状況は他の色々な場合に於いても見出されることが知られている。（詳しくは Bannai[1] を参照。）

ここまでは q を固定して考えていたが、次の定理は q が異なる（従ってクラスが異なる）場合に於ける相互関係を示すものである。

定理 2. $\mathfrak{X}(GO_{2m+1}(q), GO_{2m+1}(q)/GO^+_{2m}(q))$ は $\mathfrak{X}(GO_3(q^m), GO_3(q^m)/GO^+_2(q^m))$ の *subscheme* である。

Proof. この主張は次の包含関係

$$\begin{array}{ccc} GO_{2m+1}(q) & \supset & GO^+_{2m}(q) \\ \cup & & \cup \\ GO_3(q^m) & \supset & GO^+_2(q^m) \end{array}$$

及び

$$GO_3(q^m) \cap GO^+_{2m}(q) = GO^+_2(q^m)$$

を示すことにより導かれる。すなわち

$$|GO_{2m+1}(q) : GO^+_{2m}(q)| = |GO_3(q^m) : GO^+_2(q^m)| = \frac{q^m(q^m+1)}{2}$$

より、$GO_{2m+1}(q)/GO^+_{2m}(q)$ の元は $GO_3(q^m)/GO^+_2(q^m)$ の元と 1 対 1 に対応していることが分かる。 □

同様にして $\mathfrak{X}(GO_{2m+1}(q), GO_{2m+1}(q)/GO^-_{2m}(q))$ が $\mathfrak{X}(GO_3(q^m), GO_3(q^m)/GO^-_2(q^m))$ の subscheme であることも証明される。

de Caen - van Dam[5] に於いて、$\mathfrak{X}(GO_3(q), GO_3(q)/GO^+_2(q))$ と（q が偶数のとき）同型な association scheme $\mathfrak{X}(PGL(2,q), PGL(2,q)/D_{2(q-1)})$ が考察されており、その中で彼らはこの association scheme の subscheme について、$q = 4^r$ $(r \geq 2)$ のときにクラス 4 の特殊な subscheme （及びこれから得られるクラス 3 と 2 の subschemes ）が存在することを示唆し、その他には Johnson scheme $J(q+1, 2)$ や Frobenius 写像 $\alpha \longmapsto \alpha^p$ により構成されるいくつかの subschemes を除けば sporadic なもの以外は存在しないと予想した。定理 2 はこの予想に 1 つの解答を与える。例えば $q = 64 = 2^6$ のとき、この association scheme の subscheme は

- Johnson scheme $J(65, 2)$ ：クラス 2
- Frobenius 型：クラス 20 $(q = 8^2)$, 12 $(q = 4^3)$, 8 $(q = 2^6)$
- de Caen - van Dam 型：クラス 4, 3, 2
- 定理 2 により得られる subschemes ：クラス 4 $(q = 8^2)$, 2 $(q = 4^3)$

となり、新たに 2 つの subschemes が構成された。なお上に挙げた subschemes の中にクラスが同じものがあるが、これらは全て異なる。またここで全ての subschemes が挙げられているとは限らない。

参考文献

[1] E. Bannai, Character Tables of Commutative Association Schemes, in "*Finite Geometries, Buildings, and Related Topics*,"105-128, Clarendon Press, Oxford, 1990.

[2] E. Bannai, S. Hao, and S.Y. Song, Character Tables of the Association Schemes of Finite Orthogonal Groups Acting on the Nonisotropic Points, *J. Combin. Theory Ser.* A 54 (1990),164-200.

[3] E. Bannai and T. Ito, "*Algebraic Combinatorics* I," Benjamin/Cummings, Menlo Park, CA, 1984.

[4] E. Bannai, W.M. Kwok, and S.Y. Song, Ennola Type Dualities in the Character Tables of Some Association Schemes, *Mem. Fac. Sci. Kyushu Univ. Ser.* A 44 (1990),129-143.

[5] D. de Caen and E.R. van Dam, Fissioned triangular schemes via the cross-ratio, preprint(1999).

[6] J.H. Conway *et al.*, "ATLAS *of Finite Groups*," Clarendon Press, Oxford, 1985.

[7] A. Munemasa, "*The Geometry of Orthogonal Groups over Finite Fields*," JSPS-DOST Lec. Note Math., Sophia Univ., Tokyo, 1996.

[8] H. Tanaka, A 4-class Subscheme of the Association Scheme Coming from the Action of $PGL(2,4^f)$, preprint.

Enumerating surface branched coverings*

Jin Ho Kwak

Combinatorial and Computational Mathematics Center
Pohang University of Science and Technology, Pohang, 790-784 Korea

Jaeun Lee

Mathematics, Yeungnam University, Kyongsan, 712-749 Korea

Abstract

The number of nonisomorphic n-fold branched coverings of a given closed surface can be determined by the number of nonisomorphic n-fold unbranched coverings of the surface and the number of nonisomorphic n-fold graph coverings of a suitable bouquet of circles. Also, a similar enumeration can be done for regular branched coverings. Some explicit enumerations of them are also possible.

Keywords: Surface branched coverings, graph coverings, enumerations

1 Introduction

Throughout this paper, a surface $\mathbb{S}$ means a compact connected 2-manifold without boundary. By the classification theorem of surfaces, $\mathbb{S}$ is homeomorphic to one of the following:

$$\mathbb{S}_k = \begin{cases} \text{the orientable surface with } k \text{ handles} & \text{if } k \geq 0, \\ \text{the nonorientable surface with } -k \text{ crosscaps} & \text{if } k < 0. \end{cases}$$

A continuous function $p : \tilde{\mathbb{S}} \to \mathbb{S}$ from a surface $\tilde{\mathbb{S}}$ onto another surface $\mathbb{S}$ is called a *branched covering* if there exists a finite set B in $\mathbb{S}$ such that the restriction of p to $\tilde{\mathbb{S}} - p^{-1}(B)$, $p|_{\tilde{\mathbb{S}}-p^{-1}(B)} : \tilde{\mathbb{S}} - p^{-1}(B) \to \mathbb{S} - B$, is a covering projection in the usual sense. The smallest subset B of $\mathbb{S}$ which has this property is called the *branch set*.

A branched covering $p : \tilde{\mathbb{S}} \to \mathbb{S}$ is *regular* if there exists a (finite) group $\mathcal{A}$ which acts pseudofreely on $\tilde{\mathbb{S}}$ so that the surface $\mathbb{S}$ is homeomorphic to the quotient space $\tilde{\mathbb{S}}/\mathcal{A}$, say by h, and the quotient map $\tilde{\mathbb{S}} \to \tilde{\mathbb{S}}/\mathcal{A}$ is the composition $h \circ p$ of p and h. We call it simply a *branched $\mathcal{A}$-covering*. In this case, the group $\mathcal{A}$ becomes the covering

*Supported by Com^{2}MaC-KOSEF.

transformation group of the branched covering $p : \tilde{\mathbb{S}} \to \mathbb{S}$. Two branched coverings $p : \tilde{\mathbb{S}} \to \mathbb{S}$ and $q : \tilde{\mathbb{S}}' \to \mathbb{S}$ are *isomorphic* if there exists a homeomorphism $h : \tilde{\mathbb{S}} \to \tilde{\mathbb{S}}'$ such that $p = q \circ h$.

Recently, Kwak et al. [8, 11] examined which surface can be a branched $\mathcal{A}$-covering of a given surface with a given branch set when $\mathcal{A}$ is the cyclic group $\mathbb{Z}_p$ or the dihedral group $\mathbb{D}_p$ of order $2p$, p prime.

In this paper, we enumerate the total number of nonisomorphic (regular) branched coverings of any given surface $\mathbb{S}$ with a branch set B.

2 A classification of branched coverings

Let G be a finite connected graph with vertex set $V(G)$ and edge set $E(G)$. We allow self-loops and multiple edges. Notice that G can be identified with a one-dimensional CW complex in the Euclidean 3-space $\mathbb{R}^3$ so that every graph map is continuous. Every covering of a graph G can be constructed as follows (see [3]).

Every edge of a graph G gives rise to a pair of oppositely directed edges. By $e^{-1} = vu$, we mean the reverse edge to a directed edge $e = uv$. We denote the set of directed edges of G by $D(G)$. Each directed edge e has an initial vertex i_e and a terminal vertex t_e. Following [3], a *permutation voltage assignment* ϕ on a graph G is a map $\phi : D(G) \to S_n$ with a property that $\phi(e^{-1}) = \phi(e)^{-1}$ for each $e \in D(G)$, where S_n is the symmetric group on n elements $\{1, \ldots, n\}$. The *permutation derived graph* G^ϕ is defined as follows: $V(G^\phi) = V(G) \times \{1, \ldots, n\}$, and for each edge $e \in D(G)$ and $j \in \{1, \ldots, n\}$ let there be an edge (e, j) in $D(G^\phi)$ with $i_{(e,j)} = (i_e, j)$ and $t_{(e,j)} = (t_e, \phi(e)j)$. The natural projection $p_\phi : G^\phi \to G$ is a covering. In the derived graph G^ϕ, a vertex (u, i) is denoted by u_i, and an edge (e, j) by e_j. Let $\mathcal{A}$ be a finite group. An *ordinary voltage assignment* (or, *$\mathcal{A}$-voltage assignment*) of G is a function $\phi : D(G) \to \mathcal{A}$ with a property that $\phi(e^{-1}) = \phi(e)^{-1}$ for each $e \in D(G)$. The values of ϕ are called *voltages*, and $\mathcal{A}$ is called the *voltage group*. The *ordinary derived graph* $G \times_\phi \mathcal{A}$ has as its vertex set $V(G) \times \mathcal{A}$ and as its edge set $E(G) \times \mathcal{A}$, so that an edge (e, g) of $G \times_\phi \mathcal{A}$ joins a vertex (u, g) to $(v, \phi(e)g)$ for $e = uv \in D(G)$ and $g \in \mathcal{A}$. In the ordinary derived graph $G \times_\phi \mathcal{A}$, a vertex (u, g) is also denoted by u_g, and an edge (e, g) by e_g. The first coordinate projection $p_\phi : G \times_\phi \mathcal{A} \to G$, called the natural projection, commutes with the left multiplication action of the $\phi(e)$ and the right action of $\mathcal{A}$ on the fibers, which is free and transitive, so that p is a regular $|\mathcal{A}|$-fold covering, called simply an *$\mathcal{A}$-covering*.

A (branched) covering of a surface is closely related to a graph covering which is embeddable into it. To see such a kind of relation, we first review a graph emdedding into a surface.

An *embedding* of a graph G into a surface $\mathbb{S}$ is a continuous one-to-one function $\imath : G \to \mathbb{S}$. If every component of $\mathbb{S} - \imath(G)$, called a *region*, is a homeomorphic to an open disk, then $\imath : G \to \mathbb{S}$ is called a *2-cell* embedding. An *embedding scheme* (ρ, λ) for a graph G consists of a rotation scheme ρ which assigns a cyclic permutation ρ_v on $N(v) = \{e \in D(G) : \text{the initial vertex of } e \text{ is } v\}$ to each $v \in V(G)$ and a voltage assignment λ which assigns a value $\lambda(e)$ in $\mathbb{Z}_2 = \{-1, 1\}$ to each $e \in E(G)$.

Stahl [15] showed that every embedding scheme determines a 2-cell embedding of G into an orientable or nonorientable surface $\mathbb{S}$, and every 2-cell embedding of G into a surface $\mathbb{S}$ is determined by such a scheme.

Let $\imath : G \to \mathbb{S}$ be a 2-cell embedding with embedding scheme (ρ, λ) and let ϕ be a permutation voltage assignment. The derived graph G^ϕ has the *derived embedding scheme* $(\tilde{\rho}, \tilde{\lambda})$, which is defined by $\tilde{\rho}_{v_i}(e_i) = (\rho_v(e))_i$ and $\tilde{\lambda}(e_i) = \lambda(e)$ for each $e_i \in D(G^\phi)$. Then it induces a 2-cell embedding of G^ϕ into a surface, say $\tilde{\imath} : G^\phi \to \mathbb{S}^\phi$, such that the following diagram

$$\begin{array}{ccc} G^\phi & \xrightarrow{\tilde{\imath}} & \mathbb{S}^\phi \\ {\scriptstyle p_\phi}\downarrow & & \downarrow{\scriptstyle \tilde{p}_\phi} \\ G & \xrightarrow{\imath} & \mathbb{S} \end{array}$$

commutes. Moreover, if G^ϕ is connected, then $\mathbb{S}^\phi$ is connected and $\tilde{p}_\phi : \mathbb{S}^\phi \to \mathbb{S}$ is a covering possibly having branch points. Conversely, let $p : \tilde{\mathbb{S}} \to \mathbb{S}$ be a branched n-fold covering of a surface $\mathbb{S}$. Then there exist a 2-cell embedding $\imath : G \to \mathbb{S}$ of a graph G such that each face of the embedding has at most one branch point interior of it and a permutation voltage assignment $\phi : D(G) \to S_n$ such that the branched n-fold covering $\tilde{p}_\phi : \mathbb{S}^\phi \to \mathbb{S}$ is isomorphic to the given branched covering $p : \tilde{\mathbb{S}} \to \mathbb{S}$ [4].

A surface $\mathbb{S}_k$ can be represented by a $4k$-gon with identification data $\prod_{s=1}^{k} a_s b_s a_s^{-1} b_s^{-1}$ on its boundary if $k > 0$; bigon with identification data aa^{-1} on its boundary if $k = 0$; and $-2k$-gon with identification data $\prod_{s=1}^{-k} a_s a_s$ on its boundary if $k < 0$.

Let B be a finite set of points in $\mathbb{S}_k$. We note that the fundamental group $\pi_1(\mathbb{S}_k - B, *)$ of the punctured surface $\mathbb{S}_k - B$ with the base point $* \in \mathbb{S}_k - B$ can be presented by

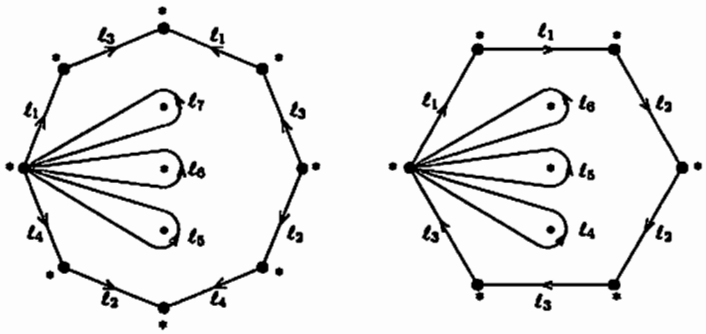
$$\left\langle a_1, \ldots, a_k, b_1, \ldots, b_k, c_1, \ldots, c_{|B|} \; ; \; \prod_{s=1}^{k} a_s b_s a_s^{-1} b_s^{-1} \prod_{t=1}^{|B|} c_t = 1 \right\rangle \quad \text{if } k > 0;$$

$$\left\langle a_1, \ldots, a_{-k}, c_1, \ldots, c_{|B|} \; ; \; \prod_{s=1}^{-k} a_s a_s \prod_{t=1}^{|B|} c_t = 1 \right\rangle \quad \text{if } k < 0;$$

$$\left\langle c_1, \ldots, c_{|B|} \; ; \; \prod_{t=1}^{|B|} c_t = 1 \right\rangle \quad \text{if } k = 0.$$

We call this the *standard presentation* of the fundamental group $\pi_1(\mathbb{S}_k - B, *)$. For each $t = 1, 2, \ldots, |B|$, we take a simple closed curve based at $*$ lying in the face determined by the polygonal representation of the surface $\mathbb{S}_k$ so that it represents the homotopy class of the generator c_t. Then, it induces a 2-cell embedding of a bouquet of m circles, say $\mathfrak{B}_m$, into the surface $\mathbb{S}_k$ such that the embedding has $|B|$ 1-sided regions and one $(|B| + 4k)$-sided region if $k > 0$; $|B|$ 1-sided regions and one $(|B| - 2k)$-sided region if $k < 0$; and $|B|$ 1-sided regions and one $|B|$-sided region if $k = 0$, where m is the number of the generators of the standard presentation of the corresponding fundamental group. We call this embedding $\imath : \mathfrak{B}_m \to \mathbb{S}_k$ the *standard embedding*, simply denoted by $\mathfrak{B}_m \hookrightarrow \mathbb{S}_k - B$.

For example, Figure 1 illustrates the standard embeddings of bouquets with $|B| = 3$. Figure 1(a) represents the standard embedding $\mathfrak{B}_7 \hookrightarrow \mathbb{S}_2 - B$ and (b) does the standard embedding $\mathfrak{B}_6 \hookrightarrow \mathbb{S}_{-3} - B$.



(a) $\mathfrak{B}_7 \hookrightarrow \mathbb{S}_2 - B$ (b) $\mathfrak{B}_6 \hookrightarrow \mathbb{S}_{-3} - B$

Figure 1: Two examples of standard embeddings

For a natural number n, let $C^1(\mathfrak{B}_m; n)$ denote the set of all permutation voltage assignments $\phi : D(\mathfrak{B}_m) \to S_n$ on the bouquet of m circles $\mathfrak{B}_m$. Notice that $C^1(\mathfrak{B}_m; n)$ can be identified with the cartesian product $(S_n)^m$ of m copies of the symmetric group S_n, i.e., each element ϕ in $C^1(\mathfrak{B}_m; n)$ can be identified with an m-tuple $(\phi(\ell_1), \ldots, \phi(\ell_m))$, where ℓ_i is a positively oriented loop in $D(\mathfrak{B}_m)$. For convenience, let $a_k = 2k$ if $k \geq 0$, and $a_k = -k$ if $k < 0$. Let $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; n)$ (resp. $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A})$) denote the subset of $(S_n)^{a_k+|B|}$ (resp. of $(\mathcal{A})^{a_k+|B|}$) consisting of all $(a_k + |B|)$-tuples $(\sigma_1, \ldots, \sigma_{a_k+|B|})$ which satisfy the following three conditions:

(C1) The subgroup $< \sigma_1, \ldots, \sigma_{a_k+|B|} >$ generated by $\{\sigma_1, \ldots, \sigma_{a_k+|B|}\}$ is transitive on $\{1, 2, \ldots, n\}$ (resp. is the full group $\mathcal{A}$), and

(C2) (i) if $k \geq 0$, then

$$\prod_{i=1}^{k} \sigma_i \sigma_{k+i} \sigma_i^{-1} \sigma_{k+i}^{-1} \prod_{i=1}^{|B|} \sigma_{2k+i} = 1,$$

(ii) if $k < 0$, then

$$\prod_{i=1}^{-k} \sigma_i \sigma_i \prod_{i=1}^{|B|} \sigma_{-k+i} = 1,$$

(C3) $\sigma_i \neq 1$ for each $i = a_k + 1, \ldots, a_k + |B|$.

Note that condition (C1) guarantees that the surface $\mathbb{S}^\phi$ is connected, and conditions (C2) and (C3) do that the set B is the same as the branch set of the branched covering $\tilde{p}_\phi : \mathbb{S}^\phi \to \mathbb{S}$. By using a similar method as in [8], we can obtain the following theorem.

Theorem 1 (Existence and classification of branched coverings) *Every permutation voltage assignment in* $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; n)$ *induces a connected branched* n*-fold covering of* $\mathbb{S}_k$ *with branch set* B*. Conversely, every connected branched* n*-fold covering of* $\mathbb{S}_k$ *with branch set* B *can be derived from a voltage assignment in* $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; n)$*. Moreover, for any given two permutation voltage assignments* $\phi, \psi \in C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S} - B; n)$*, two branched* n*-fold surface coverings* $\tilde{p}_\phi : \mathbb{S}^\phi \to \mathbb{S}$ *and* $\tilde{p}_\psi : \mathbb{S}^\psi \to \mathbb{S}$ *are isomorphic if and only if two graph coverings* $p_\phi : \mathfrak{B}^\phi_{a_k+|B|} \to \mathfrak{B}_{a_k+|B|}$ *and* $p_\psi : \mathfrak{B}^\psi_{a_k+|B|} \to \mathfrak{B}_{a_k+|B|}$ *are isomorphic. It is also equivalent to say that there exists a permutation* $\sigma \in S_n$ *such that*

$$\psi(\ell_i) = \sigma\phi(\ell_i)\sigma^{-1}$$

for all $\ell_i \in D(\mathfrak{B}_{a_k+|B|})$*, where* $a_k = 2k$ *if* $k \geq 0$*, and* $a_k = -k$ *if* $k < 0$. □

For a finite group $\mathcal{A}$, let $S_\mathcal{A}$ denote the symmetric group on the group elements of $\mathcal{A}$. It gives the (left) regular representation $\mathcal{A} \to S_\mathcal{A}$ of $\mathcal{A}$ via $g \to L(g)$, the left translation by g on $\mathcal{A}$. Clearly, this representation is faithful and the group $\mathcal{A}$ can be identified with the group of left transformations $L(g)$'s: $\mathcal{A} \equiv \{L(g) \mid g \in \mathcal{A}\}$ (Cayley Theorem). Notice that a permutation voltage assignment $\phi : D(G) \to S_\mathcal{A}$ having its images in $\mathcal{A}$ can be considered as an $\mathcal{A}$-voltage assignment of G, and for such a voltage assignment ϕ, the permutation derived graph G^ϕ is nothing but the ordinary derived graph $G \times_\phi \mathcal{A}$. By using this fact, Kwak et al. showed the following.

Corollary 1 [8](Existence and classification of regular branched coverings) *Every ordinary voltage assignment in* $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A})$ *induces a connected branched* $\mathcal{A}$*-covering of* $\mathbb{S}_k$ *with branch set* B*. Conversely, every connected branched* $\mathcal{A}$*-covering of* $\mathbb{S}_k$ *with branch set* B *can be derived from a voltage assignment in* $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A})$*. Moreover, for any given two voltage assignments* $\phi, \psi \in C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S} - B; \mathcal{A})$*, two branched* $\mathcal{A}$*-coverings* $\tilde{p}_\phi : \mathbb{S}^\phi \to \mathbb{S}$ *and* $\tilde{p}_\psi : \mathbb{S}^\psi \to \mathbb{S}$ *are isomorphic if and only if two graph coverings* $p_\phi : \mathfrak{B}_{a_k+|B|} \times_\phi \mathcal{A} \to \mathfrak{B}_{a_k+|B|}$ *and* $p_\psi : \mathfrak{B}_{a_k+|B|} \times_\psi \mathcal{A} \to \mathfrak{B}_{a_k+|B|}$ *are isomorphic. It is also equivalent to say that there exists a group automorphism* σ *of* $\mathcal{A}$ *such that*

$$\psi(\ell_i) = \sigma\left(\phi(\ell_i)\right)$$

for all $\ell_i \in D(\mathfrak{B}_{a_k+|B|})$*, where* $a_k = 2k$ *if* $k \geq 0$*, and* $a_k = -k$ *if* $k < 0$. □

3 Computational formulas

In this section, we derive some formulas for enumerating the isomorphism classes of surface branched coverings.

We define an S_n-action on the set $C^1(\mathfrak{B}_m; n)$ by a simultaneously coordinatewise conjugation, that is, for any $g \in S_n$ and any $(\sigma_1, \ldots, \sigma_m) \in C^1(\mathfrak{B}_m; n)$,

$$g \cdot (\sigma_1, \ldots, \sigma_m) = (g\sigma_1 g^{-1}, \ldots, g\sigma_m g^{-1}).$$

It follows from Theorem 1 that two voltage assignments in $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; n)$ derive isomorphic branched coverings of $\mathbb{S}_k$ if and only if they belong to the same orbit under the S_n-action. Hence we have the following.

Lemma 1 *Let k be any integer and let B be a finite subset of the surface $\mathbb{S}_k$. Then the number of nonisomorphic connected n-fold branched coverings of the surface $\mathbb{S}_k$ with branch set B is*

$$\mathbf{Isoc}\,(\mathbb{S}_k, B; n) = \left|C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; n)/S_n\right|.$$

□

Now, we aim to express the number $\mathbf{Isoc}\,(\mathbb{S}_k, B; n)$ in terms of known parameters.

Let $\mathfrak{C}(\mathfrak{B}_m; n)$ denote the set of all m-tuples $(\sigma_1, \ldots, \sigma_m)$ in $(S_n)^m$ such that the group $<\sigma_1, \ldots, \sigma_m>$ generated by $\{\sigma_1, \ldots, \sigma_m\}$ is transitive on $\{1, 2, \ldots, n\}$, that is,

$$\mathfrak{C}(\mathfrak{B}_m; n) = \{(\sigma_1, \sigma_2, \ldots, \sigma_m) \in (S_n)^m : <\sigma_1, \sigma_2, \ldots, \sigma_m> \text{ is transitive on } \{1, 2, \ldots, n\}\}.$$

Then $\mathfrak{C}(\mathfrak{B}_m; n)$ contains all representatives of connected n-fold coverings of the bouquet of m-circles $\mathfrak{B}_m$ and the number $\mathbf{Isoc}\,(\mathfrak{B}_m; n)$ of nonisomorphic connected n-fold coverings of $\mathfrak{B}_m$ is equal to $|\mathfrak{C}(\mathfrak{B}_m; n)/S_n|$, where the S_n-action on $\mathfrak{C}(\mathfrak{B}_m; n)$ is also defined by the simultaneously coordinatewise conjugation (see [9, 10]).

Lemma 2 *Let k be an integer and b a nonnegative integer. For each $0 \leq t \leq b$, let*

$$S(k, b, t) = \left\{\phi \in (S_n)^{a_k+b} : \phi \text{ satisfies (C1), (C2) and } \sigma_i = 1, {}^\forall i = a_k + 1, \ldots, a_k + t \right\},$$

where $\phi = (\sigma_1, \sigma_2, \ldots, \sigma_{a_k+b})$. If $t = b$, then the set $S(k, b, b)$ is equal to the set $C^1(\mathfrak{B}_{a_k} \hookrightarrow \mathbb{S}_k; n)$, and if $t \neq b$, then there is a one-to-one correspondence between the sets $S(k, b, t)$ and $\mathfrak{C}(\mathfrak{B}_{a_k+b-t-1}; n)$. Moreover, the correspondence preserves the S_n-action on the both sets which are defined by simultaneously coordinatewise conjugacy.

Proof: The case of $t = b$ is clear. Assume that $t \neq b$. Then every element in $S(k, b, t)$ is of the form $(\sigma_1, \ldots, \sigma_{a_k}, 1, \ldots, 1, \sigma_{a_k+t+1}, \ldots, \sigma_{a_k+b})$. It comes from conditions (C1) and (C2) that the function $f : S(k, b, t) \to \mathfrak{C}(\mathfrak{B}_{a_k+b-t-1}; n)$ defined by

$$f(\sigma_1, \ldots, \sigma_{a_k}, 1, \ldots, 1, \sigma_{a_k+t+1}, \ldots, \sigma_{a_k+b}) = (\sigma_1, \ldots, \sigma_{a_k}, \sigma_{a_k+t+1}, \ldots, \sigma_{a_k+b-1})$$

is well-defined and bijective (Note that the function f is defined by deleting 1's and the last coordinate). This completes the proof. □

Theorem 2 *Let k be any integer and let B be a b-subset of the surface $\mathbb{S}_k$. Then the number of connected n-fold branched coverings of the surface $\mathbb{S}_k$ with branch set B is*

$$\mathbf{Isoc}\,(\mathbb{S}_k, B; n) = (-1)^b \mathbf{Isoc}\,(\mathbb{S}_k, \emptyset; n) + \sum_{t=0}^{b-1} (-1)^t \binom{b}{t} \mathbf{Isoc}\,(\mathfrak{B}_{a_k+b-t-1}; n),$$

where $\mathfrak{B}_m$ is a bouquet of m circles, $a_k = 2k$ if $k \geq 0$, and $a_k = -k$ if $k < 0$.

Proof: For each $i = a_k + 1, \ldots, a_k + b$, let $\mathcal{P}_i$ be the property that the i-th coordinate of an element of $(S_n)^{a_k+b}$ is the identity. For each subset S of $\{a_k + 1, \ldots, a_k + b\}$, let $N(\mathcal{P}_S)$ be the number of elements in the product $(S_n)^{a_k+b}$ which satisfy conditions (C1), (C2) and the properties $\mathcal{P}_i$ for all $i \in S$. Notice that $N(\mathcal{P}_\emptyset)$ is the number of all elements in the product $(S_n)^{a_k+b}$ which satisfy conditions (C1) and (C2), and that the set $C^1(\mathfrak{B}_{a_k+b} \hookrightarrow \mathbb{S}_k - B; n)$ is equal to the set of elements of $(S_n)^{a_k+b}$ which satisfy conditions (C1) and (C2), but not any other property $\mathcal{P}_i$ for $i = a_k + 1, \ldots, a_k + b$. It comes from the principle of inclusion and exclusion that

$$\left|C^1(\mathfrak{B}_{a_k+b} \hookrightarrow \mathbb{S}_k - B; n)\right| = \sum_{t=0}^{b} (-1)^t \left(\sum_{\substack{S \subset \{a_k+1, \ldots, a_k+b\} \\ |S|=t}} N(\mathcal{P}_S) \right).$$

Since $N(\mathcal{P}_S) = N(\mathcal{P}_{S'})$ for any two subsets S, S' of $\{a_k + 1, \ldots, a_k + b\}$ with the same cardinality, we have

$$\sum_{\substack{S \subset \{a_k+1, \ldots, a_k+b\} \\ |S|=t}} N(\mathcal{P}_S)$$
$$= \binom{b}{t} \left| \{ \phi \in (S_n)^{a_k+b} : \phi \text{ satisfies (C1), (C2) and } \sigma_i = 1, {}^\forall i = a_k + 1, \ldots, a_k + t \} \right|.$$

Now, it comes from Lemma 2 that

$$\left|C^1(\mathfrak{B}_{a_k+b} \hookrightarrow \mathbb{S}_k - B; n)\right| = \sum_{t=0}^{b-1} (-1)^t \binom{b}{t} \left|\mathfrak{C}(\mathfrak{B}_{a_k+b-t-1}; n)\right| + (-1)^b \left|C^1(\mathfrak{B}_{a_k} \hookrightarrow \mathbb{S}_k; n)\right|.$$

By taking the S_n-action on the underlying sets of the both sides of this equation, we have

$$\mathbf{Isoc}(\mathbb{S}_k, B; n) = (-1)^b \mathbf{Isoc}(\mathbb{S}_k, \emptyset; n) + \sum_{t=0}^{b-1} (-1)^t \binom{b}{t} \mathbf{Isoc}(\mathfrak{B}_{a_k+b-t-1}; n). \qquad \square$$

The number $\mathbf{Isoc}(G; n)$ was computed for any graph G and any natural number n by Liskovets [12] and the authors (See [10]) with reductive formula, and the number $\mathbf{Isoc}(\mathbb{S}_k, \emptyset; n)$ was computed for any k and n by Mednykh (see [13, 14]). In fact, Mednykh computed the number of conjugacy classes of subgroups of index n in the fundamental group $\pi_1(\mathbb{S}_k, *)$ of a surface $\mathbb{S}_k$ which is equal to the number $\mathbf{Isoc}(\mathbb{S}_k, \emptyset; n)$.

For convenience, let $\mathfrak{P}(n)$ denote the set of all partitions of the natural number n, i.e., the set of unordered sequences $[n_1 n_2 \cdots n_\ell]$ of natural numbers such that $n_1 + \cdots + n_\ell = n$. For a partition $\mathfrak{p}$ of n, let $j_k(\mathfrak{p})$ denote the multiplicity of k in the partition $\mathfrak{p}$, so that $j_1(\mathfrak{p}) + 2j_2(\mathfrak{p}) + \cdots + nj_n(\mathfrak{p}) = n$. A partition $\mathfrak{p}$ of n is denoted by $[[k; \frac{n}{k}]]$ if every term of $\mathfrak{p}$ is k. Note that $[[k; m]]$ denotes the partition of the natural number km each of whose terms is k.

Theorem 3 [10] *For $n \geq 2$, the number of nonisomorphic connected n-fold coverings of $\mathfrak{B}_m$ is*

$$\begin{aligned}\mathbf{Isoc}(\mathfrak{B}_m; n) = & \sum_{\ell_1+2\ell_2\cdots+(n-1)\ell_{n-1}=n-1} \left((\ell_1+1)^{m-1}-1\right) \\ & \times \left(\ell_1!\, 2^{\ell_2}\ell_2! \cdots (n-1)^{\ell_{n-1}}\ell_{n-1}!\right)^{m-1} \\ & + \sum_{2\ell_2+3\ell_3+\cdots+n\ell_n=n} \left(2^{\ell_2}\ell_2!\, 3^{\ell_3}\ell_3! \cdots n^{\ell_n}\ell_n!\right)^{m-1} \\ & - \sum_{\substack{\mathfrak{p}\in\mathfrak{P}(n)-\{[\![n;1]\!]\} \\ j_1(\mathfrak{p})=0}} \prod_{j_k(\mathfrak{p})\neq 0} \left(\frac{1}{j_k(\mathfrak{p})!} \prod_{\ell=0}^{j_k(\mathfrak{p})-1} (\mathbf{Isoc}(\mathfrak{B}_m; k)+\ell)\right),\end{aligned}$$

where the summation over the empty index set is defined to be 0.

Theorem 4 [13],[14] *The number of nonisomorphic connected n-fold unbranched coverings of a surface $\mathbb{S}_k$ of genus k is*

$$\mathbf{Isoc}(\mathbb{S}_k, \emptyset; n) = \begin{cases} \frac{1}{n}\sum_{m|n} S_k(m) \sum_{d|\frac{n}{m}} \mu\left(\frac{n}{md}\right) d^{(2k-2)m+2} & \text{if } k \geq 0, \\ \frac{1}{n}\sum_{m|n}\sum_{d|\frac{n}{m}} \mu\left(\frac{n}{md}\right) d^{(k-2)m+1}[(2,d)S_k^-(m) + d\,S_k^+(m)] & \\ & \text{if } k < 0, \end{cases}$$

where $S_k(m)$ is the number of subgroups of index m in the fundamental group $\pi_1(\mathbb{S}_k, *)$ of a surface $\mathbb{S}_k$ of genus k, $\mu(m)$ is the Möbius function, $S_k^+(m) = 0$ if m is odd, and $S_k^+(m) = S_k(\frac{m}{2})$ if m is even, $S_k^-(m) = S_k(m) - S_k^+(m)$, and $(2,d)$ is the greatest common divisor of 2 and d. In fact, the number $S_k(m)$ is given as follows:

$$S_k(m) = m\sum_{s=1}^{m} \frac{(-1)^{s+1}}{s} \sum_{\substack{i_1+i_2+\cdots+i_s=m \\ i_1,i_2,\ldots,i_s\geq 1}} \beta_{i_1}\beta_{i_2}\cdots\beta_{i_s},$$

where

$$\beta_h = \sum_{\lambda\in D_h} \left(\frac{h!}{f(\lambda)}\right)^t, \qquad t = \begin{cases} 2k-2 & \text{if } k \geq 0, \\ k-2 & \text{if } k < 0, \end{cases}$$

D_h is the set of all irreducible representations of the symmetric group S_h, and $f^{(\lambda)}$ is the degree of the representation λ.

As an illustration of Theorem 2 we compute explicitly the number of nonisomorphic 3-fold branched coverings of the orientable surface $\mathbb{S}_k$ ($k \geq 0$) with branch set B ($|B| = b$). It was known that $\mathbf{Isoc}(\mathfrak{B}_m; 3) = 6^{m-1} + 3^{m-1} - 2^{m-1}$ ([10]) and $\mathbf{Isoc}(\mathbb{S}_k, \emptyset; 3) = 2\cdot 6^{2k-2} + 4\cdot 3^{2k-2} - 2\cdot 2^{2k-2}$ ([13]). Now, by applying Theorem 2, we have

$$\mathbf{Isoc}(\mathbb{S}_k, B; 3) = 6^{2k-2}\left(5^b + (-1)^b\right) + 3^{2k-2}\left(2^b + (-1)^b 3\right) - 2^{2k-2}\left(1 + (-1)^b\right).$$

Next, we aim to compute the number $\mathbf{Isoc}^R(\mathbb{S}_k, B; n)$ of nonisomorphic connected *regular* n-fold branched coverings of a surface $\mathbb{S}_k$ with branch set B. To do this, we define an $\mathrm{Aut}\,(\mathcal{A})$-action on $C^1(\mathfrak{B}_m; \mathcal{A})$ as follows: For any $\sigma \in \mathrm{Aut}\,(\mathcal{A})$ and any $(g_1, \ldots, g_m) \in C^1(\mathfrak{B}_m; \mathcal{A})$, define

$$\sigma \cdot (g_1, \ldots, g_m) = (\sigma(g_1), \ldots, \sigma(g_m)).$$

Then it follows from Corollary 1 that two voltage assignments in $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A})$ derive isomorphic branched coverings of $\mathbb{S}_k$ if and only if they belong to the same orbit under the $\mathrm{Aut}\,(\mathcal{A})$-action. Notice that this $\mathrm{Aut}\,(\mathcal{A})$-action on $C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A})$ is free because $\{g_1, \ldots, g_{a_k+b}\}$ generates $\mathcal{A}$. It implies that the number $\mathbf{Isoc}\,(\mathbb{S}_k, B; \mathcal{A})$ of nonisomorphic connected branched $\mathcal{A}$-coverings of the surface $\mathbb{S}_k$ with branch set B is

$$\mathbf{Isoc}\,(\mathbb{S}_k, B; \mathcal{A}) = \frac{\left|C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A})\right|}{|\mathrm{Aut}\,(\mathcal{A})|}.$$

It also follows from Corollary 1 that any two connected regular branched coverings are not isomorphic if their covering transformation groups (or voltage groups) are not isomorphic. Now, the following comes from the fact that every connected regular n-fold branched covering is isomorphic to a connected branched $\mathcal{A}$-covering for some group $\mathcal{A}$ of order n.

Theorem 5 *Let k be any integer and let B be a finite subset of the surface $\mathbb{S}_k$. Then the number of nonisomorphic connected regular n-fold branched coverings of the surface $\mathbb{S}_k$ with branch set B is*

$$\mathbf{Isoc}^R(\mathbb{S}_k, B; n) = \sum_{\mathcal{A}} \frac{\left|C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A})\right|}{|\mathrm{Aut}\,(\mathcal{A})|} = \sum_{\mathcal{A}} \mathbf{Isoc}\,(\mathbb{S}_k, B; \mathcal{A}),$$

where $\mathcal{A}$ runs over all representatives of isomorphism classes of groups of order n. □

By Theorem 5, we now need to compute the number $\mathbf{Isoc}\,(\mathbb{S}_k, B; \mathcal{A})$ for each finite group $\mathcal{A}$ of order n. By using a method similar to the proof of Theorem 2, we can have the following theorem.

Theorem 6 *Let k be any integer and let B be a b-subset of the surface $\mathbb{S}_k$. Then, for any finite group $\mathcal{A}$, the number of connected branched $\mathcal{A}$-coverings of the surface $\mathbb{S}_k$ with branch set B is*

$$\mathbf{Isoc}\,(\mathbb{S}_k, B; \mathcal{A}) = (-1)^b \mathbf{Isoc}\,(\mathbb{S}_k, \emptyset; \mathcal{A}) + \sum_{t=0}^{b-1} (-1)^t \binom{b}{t} \mathbf{Isoc}\,(\mathfrak{B}_{a_k+b-t-1}; \mathcal{A}),$$

where $\mathfrak{B}_m$ is a bouquet of m circles, $a_k = 2k$ if $k \geq 0$, and $a_k = -k$ if $k < 0$. □

An explicit computing of the number $\mathbf{Isoc}\,(\mathfrak{B}_m; \mathcal{A})$ was done for any m and any finite abelian group $\mathcal{A}$ or any dihedral group $\mathbb{D}_n$ of order $2n$ (See [7]). But the number $\mathbf{Isoc}\,(\mathbb{S}_k, \emptyset; \mathcal{A})$ has been known only when $\mathcal{A}$ is $\mathbb{Z}_p$ or $\mathbb{D}_p$ for a prime p (see [8, 11]).

Let $\mathcal{A} = \mathcal{A}_1 \oplus \mathcal{A}_2$ with $(|\mathcal{A}_1|, |\mathcal{A}_2|) = 1$. Then

$$|C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A})| = |C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A}_1)| \cdot |C^1(\mathfrak{B}_{a_k+|B|} \hookrightarrow \mathbb{S}_k - B; \mathcal{A}_2)|$$

and $|\mathrm{Aut}(\mathcal{A})| = |\mathrm{Aut}(\mathcal{A}_1)| \cdot |\mathrm{Aut}(\mathcal{A}_2)|$. Now, the following comes from this fact and Theorem 5.

Lemma 3 *For any finite groups $\mathcal{A}$ and $\mathcal{B}$ with $(|\mathcal{A}|, |\mathcal{B}|) = 1$ and for any surface $\mathbb{S}_k$, we have*

$$\mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A} \oplus \mathcal{B}) = \mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}) \cdot \mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{B}).$$

Now, we may compute the number $\mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A})$ for any abelian group $\mathcal{A}$. Let $\mathcal{A}$ be an abelian group. If $k \geq 0$ and $B = \emptyset$, then conditions (C2) and (C3) in the definition of the set $C^1(\mathfrak{B}_{a_k} \hookrightarrow \mathbb{S}_k; \mathcal{A})$ are satisfied clearly, so that $\mathbf{Isoc}(\mathbb{S}_k; \emptyset; \mathcal{A}) = \mathbf{Isoc}(\mathfrak{B}_{2k}; \mathcal{A})$, which was computed already in [7]. If $k < 0$ and $B = \emptyset$, then $C^1(\mathfrak{B}_{a_k} \hookrightarrow \mathbb{S}_k; \mathcal{A})$ is equal to the set of $-k$-tuples $(g_1, \ldots, g_{-k})$ with the properties that $\{g_1, \ldots, g_{-k}\}$ generates $\mathcal{A}$ and $(g_1)^2 \cdots (g_{-k})^2 = 1$. For convenience, let

$$\mathfrak{F}(\mathfrak{B}_{-k}; \mathcal{A}) = \{ (g_1, g_2, \ldots, g_{-k}) \in \mathcal{A}^{-k} : \{g_1, g_2, \ldots, g_{-k}\} \text{ generates } \mathcal{A} \text{ and } (g_{-k})^2 = 1\}.$$

We define a function $f : C^1(\mathfrak{B}_{a_k} \hookrightarrow \mathbb{S}_k; \mathcal{A}) \to \mathfrak{F}(\mathfrak{B}_{-k}; \mathcal{A})$ by

$$f(g_1, \ldots, g_{-k}) = (g_1, \ldots, g_{-k-1}, g_1 \cdots g_{-k}).$$

Then f is well-defined because $(g_1)^2 \cdots (g_{-k})^2 = (g_1 \cdots g_{-k})^2$ in the abelian group $\mathcal{A}$. Now, it is not hard to show that f is a bijection. Hence we have

$$\mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}) = |C^1(\mathfrak{B}_{a_k} \hookrightarrow \mathbb{S}_k; \mathcal{A})| \,/\, |\mathrm{Aut}(\mathcal{A})| = |\mathfrak{F}(\mathfrak{B}_{-k}; \mathcal{A})| \,/\, |\mathrm{Aut}(\mathcal{A})|.$$

By the classification theorem of finite abelian groups, we can express a finite abelian group $\mathcal{A}$ as follows.

$$\mathcal{A} = \mathcal{A}_o \oplus \mathcal{A}_e = \left(\oplus_{i=1}^{s} \oplus_{j=1}^{t_i} m_{i_j} \mathbb{Z}_{p_i^{i_j}} \right) \bigoplus \left(\oplus_{k=1}^{\ell} m_k \mathbb{Z}_{2^{t_k}} \right),$$

where p_i are odd primes and $p_i \neq p_{i'}$ if $i \neq i'$. Let $\theta(\mathcal{A})$ denote the number of direct summands of $\mathcal{A}$ whose orders are multiples of 4 and $\omega(\mathcal{A})$ denote the number of direct summands of $\mathcal{A}$ whose orders are 2. For example, $\mathbb{Z}_6 \oplus \mathbb{Z}_8 = \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_8$, $\theta(\mathbb{Z}_6 \oplus \mathbb{Z}_8) = 1$ and $\omega(\mathbb{Z}_6 \oplus \mathbb{Z}_8) = 1$. Clearly, $(|\mathcal{A}_o|, |\mathcal{A}_e|) = 1$ for any abelian group $\mathcal{A}$ and, by Lemma 3, $\mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}) = \mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}_o) \cdot \mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}_e)$. Notice that the order of $\mathcal{A}_o$ is odd. In an abelian group of odd order, $g^2 = 1$ implies $g = 1$ and hence $\mathfrak{F}(\mathfrak{B}_{-k}; \mathcal{A}_0) = |\mathfrak{C}(\mathfrak{B}_{-k-1}; \mathcal{A}_0)|$. Now, using Lemma 3 and a computational method similar to lemma

3.3 in [7], one can obtain

$$
\begin{aligned}
&|\mathfrak{F}(\mathfrak{B}_{-k};\mathcal{A})| \\
&= \frac{2^{-k}-2^{\theta(\mathcal{A})}}{(2^{-k}-1)2^{\sum_{k=1}^{t} m_k(t_k-1)}}|\mathfrak{C}(\mathfrak{B}_{-k-1};\mathcal{A}_o)||\mathfrak{C}(\mathfrak{B}_{-k};\mathcal{A}_e)| \\
&= \begin{cases}
\dfrac{2^{\theta(\mathcal{A})}\left(2^{-k-\theta(\mathcal{A})}-1\right)}{2^{-k-(\theta(\mathcal{A})+\omega(\mathcal{A}))}-1}|\mathfrak{C}(\mathfrak{B}_{-k-1};\mathcal{A})| & \text{if } \theta(\mathcal{A})+\omega(\mathcal{A})<-k, \\
\dfrac{2^{-k}-2^{\theta(\mathcal{A})}}{(2^{-k}-1)2^{\sum_{k=1}^{t} m_k(t_k-1)}}|\mathfrak{C}(\mathfrak{B}_{-k-1};\mathcal{A}_o)||\mathfrak{C}(\mathfrak{B}_{-k};\mathcal{A}_e)| & \text{if } \theta(\mathcal{A})+\omega(\mathcal{A})=-k \\
& \quad \text{and } \theta(\mathcal{A})\neq -k, \\
0 & \text{otherwise.}
\end{cases}
\end{aligned}
$$

We summarize our discussions as follows.

Lemma 4 *Let $\mathbb{S}_k$ be a surface of genus k and let $\mathcal{A}$ be any finite abelian group. Then we have the following.*

(a) *If $k \geq 0$, then* $\mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}) = \mathbf{Isoc}(\mathfrak{B}_{2k}; \mathcal{A})$.

(b) *If $k < 0$, then*

$$
\begin{aligned}
&\mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}) \\
&= \begin{cases}
\dfrac{2^{\theta(\mathcal{A})}\left(2^{-k-\theta(\mathcal{A})}-1\right)}{2^{-k-(\theta(\mathcal{A})+\omega(\mathcal{A}))}-1}\mathbf{Isoc}(\mathfrak{B}_{-k-1};\mathcal{A}) & \text{if } \theta(\mathcal{A})+\omega(\mathcal{A})<-k, \\
\dfrac{2^{-k}-2^{\theta(\mathcal{A})}}{(2^{-k}-1)2^{\sum_{k=1}^{t} m_k(t_k-1)}}\mathbf{Isoc}(\mathfrak{B}_{-k-1};\mathcal{A}_o)\mathbf{Isoc}(\mathfrak{B}_{-k};\mathcal{A}_e) & \\
\qquad \text{if } \theta(\mathcal{A})+\omega(\mathcal{A})=-k \text{ and } \theta(\mathcal{A})\neq -k, & \\
0 & \text{otherwise,}
\end{cases}
\end{aligned}
$$

where $\mathcal{A} = \mathcal{A}_o \oplus \mathcal{A}_e = \left(\oplus_{i=1}^{s} \oplus_{j=1}^{t_i} m_{i_j}\mathbb{Z}_{p_i^{\iota_{i_j}}}\right) \bigoplus \left(\oplus_{k=1}^{t} m_k\mathbb{Z}_{2^{t_k}}\right)$. □

Corollary 2 *Let $\mathbb{S}_k$ be any nonorientable surface and let $\mathcal{A}$ be any finite abelian group. Then we have the following.*

(a) *If $\mathcal{A}$ does not contain $\mathbb{Z}_2$ as its direct summand, then*

$$
\mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}) = \begin{cases} 2^{\theta(\mathcal{A})}\mathbf{Isoc}(\mathfrak{B}_{-k-1};\mathcal{A}) & \text{if } \theta(\mathcal{A})<-k, \\ 0 & \text{otherwise.} \end{cases}
$$

In particular, if the order of $\mathcal{A}$ is odd, then $\mathbf{Isoc}(\mathbb{S}_k, \emptyset; \mathcal{A}) = \mathbf{Isoc}(\mathfrak{B}_{-k-1}; \mathcal{A})$.

(b) *If $\mathcal{A}$ is $m\mathbb{Z}_2$, then* $\mathbf{Isoc}(\mathbb{S}_k, \emptyset; m\mathbb{Z}_2) = \mathbf{Isoc}(\mathfrak{B}_{-k}; m\mathbb{Z}_2)$. □

4 Explicit enumerations of some regular coverings

Recall that one can enumerate the total number of connected n-fold branched coverings of a surface by Theorem 2, but it is not easy to enumerate explicitly the number $\mathrm{Isoc}^R(\mathbb{S}_k, B; n)$ of regular n-fold branched surface coverings of a given surface $\mathbb{S}_k$ with branch set B. In this section, we compute the number $\mathrm{Isoc}^R(\mathbb{S}_k, B; p)$, $\mathrm{Isoc}^R(\mathbb{S}_k, B; 2p)$ or $\mathrm{Isoc}^R(\mathbb{S}_k, B; p^2)$ for any prime number p, as possible cases.

First, we compute $\mathrm{Isoc}^R(\mathbb{S}_k, B; p)$ for any prime p. It was known [7] that for any prime p, $\mathrm{Isoc}(\mathfrak{B}_m; \mathbb{Z}_p) = \frac{p^m-1}{p-1}$. Since every group of order p is isomorphic to the cyclic group $\mathbb{Z}_p$, it comes from Theorem 5 that $\mathrm{Isoc}^R(\mathbb{S}_k, B; p) = \mathrm{Isoc}(\mathbb{S}_k, B; \mathbb{Z}_p)$ for any k and any finite subset B of $\mathbb{S}_k$. Now, by applying Theorem 6, Lemma 4 and Corollary 2, we have the following.

Theorem 7 *Let B be a b-subset of a surface $\mathbb{S}_k$ and let p be a prime. Then the number $\mathrm{Isoc}^R(\mathbb{S}_k, B; p)$ of nonisomorphic regular connected branched p-fold coverings of $\mathbb{S}_k$ with branch set B is*

$$\mathrm{Isoc}^R(\mathbb{S}_k, B; p) = \begin{cases} \dfrac{p^{2k}-1}{p-1} & \text{if } k \geq 0 \text{ and } b = 0, \\ p^{2k-1}\left((p-1)^{b-1} + (-1)^b\right) & \text{if } k \geq 0 \text{ and } b \neq 0, \\ 2^{-k} - 1 & \text{if } k < 0,\ b = 0 \text{ and } p = 2, \\ 2^{-k-1}\left(1 + (-1)^b\right) & \text{if } k < 0,\ b \neq 0 \text{ and } p = 2, \\ \dfrac{p^{-k-1}-1}{p-1} & \text{if } k < 0,\ b = 0 \text{ and } p \neq 2, \\ p^{-k-1}(p-1)^{b-1} & \text{if } k < 0,\ b \neq 0 \text{ and } p \neq 2. \end{cases}$$

Notice that $\mathrm{Isoc}(\mathbb{S}_k, B; \mathbb{Z}_p)$ was already computed in [8], but the computational method in [8] is different from that in this paper.

Next, to compute $\mathrm{Isoc}^R(\mathbb{S}_k, B; p^2)$ for any prime p, we recall that every finite group of order p^2 is abelian and is isomorphic to $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. It was known [7] that for any prime p,

$$\mathrm{Isoc}(\mathfrak{B}_m; \mathbb{Z}_{p^2}) = \frac{p^{2m-1} - p^{m-1}}{p-1} \quad \text{and} \quad \mathrm{Isoc}(\mathfrak{B}_m; \mathbb{Z}_p \oplus \mathbb{Z}_p) = \frac{p^{2m-1} - p^{m-1}(p+1) + 1}{(p^2-1)(p-1)}.$$

By Lemma 4 and Corollary 2, we can have

$$\mathrm{Isoc}(\mathbb{S}_k, \emptyset; \mathbb{Z}_{p^2}) = \begin{cases} \dfrac{p^{4k-1} - p^{2k-1}}{p-1} & \text{if } k \geq 0, \\ 2^{-2k-2} - 2^{-k-1} & \text{if } k < 0 \text{ and } p = 2, \\ \dfrac{p^{-2k-3} - p^{-k-2}}{p-1} & \text{if } k < 0 \text{ and } p \neq 2, \end{cases}$$

and

$$\mathrm{Isoc}\,(\mathbb{S}_k, \emptyset; \mathbb{Z}_p \times \mathbb{Z}_p) = \begin{cases} \dfrac{p^{4k-1} - p^{2k-1}(p+1) + 1}{(p^2-1)(p-1)} & \text{if } k \geq 0, \\ \dfrac{2^{-2k-1} - 3 \cdot 2^{-k-1} + 1}{3} & \text{if } k < 0 \text{ and } p = 2, \\ \dfrac{p^{-2k-3} - p^{-k-2}(p+1) + 1}{(p^2-1)(p-1)} & \text{if } k < 0 \text{ and } p \neq 2. \end{cases}$$

By using these formulas and Theorems 5 and 6, we have the following theorem.

Theorem 8 *Let B be a b-subset of the surface $\mathbb{S}_k$. Then the number $\mathrm{Isoc}^R(\mathbb{S}_k, B; 4)$ of nonisomorphic regular connected branched 4-fold coverings of $\mathbb{S}_k$ with branch set B is*

$$\mathrm{Isoc}^R(\mathbb{S}_k, B; 4) = \begin{cases} \dfrac{1}{3}\left(2^{4k+1} + 1\right) - 2^{2k} & \text{if } k \geq 0 \text{ and } b = 0, \\ 2^{2k-1}\left[2^{2k}\left(3^{b-1} + (-1)^b\right) - \left(1 + (-1)^b\right)\right] & \text{if } k \geq 0 \text{ and } b \neq 0, \\ \dfrac{1}{3}\left(5 \cdot 2^{-2(k+1)} + 1\right) - 2^{-k} & \text{if } k < 0 \text{ and } b = 0, \\ 2^{-k-1}\left[2^{-k-1}\left(2 \cdot 3^{b-1} + (-1)^b\right) - \left(1 + (-1)^b\right)\right] & \text{if } k < 0 \text{ and } b \neq 0. \end{cases}$$

Theorem 9 *Let B be a b-subset of the surface $\mathbb{S}_k$ and let p an odd prime. Then the number $\mathrm{Isoc}^R(\mathbb{S}_k, B; p^2)$ of nonisomorphic regular connected branched p^2-fold coverings of $\mathbb{S}_k$ with branch set B is*

$$\mathrm{Isoc}^R(\mathbb{S}_k, B; p^2) = \begin{cases} \dfrac{\left(p^{2k+1} - 1\right)\left(p^{2k} - 1\right)}{(p^2-1)(p-1)} & \text{if } k \geq 0 \text{ and } b = 0, \\ \dfrac{p^{2k-1}}{p-1}\left[(p-1)^{b-1}\left(p^{2k}(p+1)^{b-1} - 1\right) + (-1)^b\left(p^{2k} - 1\right)\right] & \text{if } k \geq 0 \text{ and } b \neq 0, \\ \dfrac{\left(p^{-k} - 1\right)\left(p^{-k-1} - 1\right)}{(p^2-1)(p-1)} & \text{if } k < 0 \text{ and } b = 0, \\ p^{-k-1}(p-1)^{b-2}\left[p^{-k}(p+1)^{b-1} - 1\right] & \text{if } k < 0 \text{ and } b \neq 0. \end{cases}$$

Finally, we compute $\mathrm{Isoc}^R(\mathbb{S}_k, B; 2p)$ for any odd prime p. Recall that every finite group of order $2p$ (p is odd prime) is isomorphic to the cyclic group $\mathbb{Z}_{2p} = \mathbb{Z}_2 \times \mathbb{Z}_p$ or the dihedral group $\mathbb{D}_p$. It was known [7] that for any odd prime p,

$$\mathrm{Isoc}\,(\mathfrak{B}_m; \mathbb{Z}_{2p}) = \frac{(2p)^m - p^m - 2^m + 1}{p-1}$$

and

$$\mathrm{Isoc}\,(\mathfrak{B}_m; \mathbb{D}_p) = \frac{2 \cdot (2p)^{m-1} - p^{m-1} - 2^m + 1}{p-1}.$$

By Lemmas 3 and 4, and Corollary 2, one can have

$$\mathrm{Isoc}\,(\mathbb{S}_k, \emptyset; \mathbb{Z}_{2p}) = \begin{cases} \dfrac{(2p)^{2k} - p^{2k} - 2^{2k} + 1}{p-1} & \text{if } k \geq 0, \\ \dfrac{2 \cdot (2p)^{-k-1} - p^{-k-1} - 2^{-k} + 1}{p-1} & \text{if } k < 0. \end{cases}$$

The number $\mathrm{Isoc}\,(\mathbb{S}_k, \emptyset; \mathbb{D}_p)$ was known as follows (see [11]).

$$\mathrm{Isoc}\,(\mathbb{S}_k, \emptyset; \mathbb{D}_p) = \begin{cases} \dfrac{4 \cdot (2p)^{2k-2} - p^{2k-2} - 4 \cdot 2^{2k-2} + 1}{p-1} & \text{if } k \geq 0, \\ \dfrac{4 \cdot (2p)^{-k-2} - p^{-k-2}(p-2) - 2^{-k} + 1}{p-1} & \text{if } k < 0. \end{cases}$$

Now, the following comes from these facts and Theorems 5 and 6.

Theorem 10 *Let B be a b-subset of the surface $\mathbb{S}_k$ and let p be an odd prime. Then the number $\mathrm{Isoc}^R(\mathbb{S}_k, B; 2p)$ of nonisomorphic regular connected branched $2p$-fold coverings of $\mathbb{S}_k$ with branch set B is*

$$\mathrm{Isoc}^R(\mathbb{S}_k, B; 2p)$$

$$= \begin{cases} \dfrac{1}{p-1}\left(2^{2k}-1\right)\left((p^2+1)p^{2k-2}-2\right) & \text{if } k \geq 0 \text{ and } b = 0, \\ \dfrac{2^{2k-1}p^{2k-2}}{p-1}\left[(2p-1)^b(p+1) + (-1)^b\left(2p^2-p+1\right)\right] & \\ \quad -\dfrac{2^{2k}\left(1+(-1)^b\right)}{p-1} - p^{2k-2}\left[(p-1)^{b-1}(p+1) + (-1)^b p\right] & \text{if } k \geq 0 \text{ and } b \neq 0, \\ \dfrac{1}{p-1}\left[2^{-k}\left(p^{-k-1}-1\right) + 2\left(p^{-k-2}-1\right)\left(2^{-k-1}-1\right)\right] & \text{if } k < 0 \text{ and } b = 0, \\ \dfrac{2^{-k-1}p^{-k-2}}{p-1}\left[\left((2p-1)^b + (-1)^b\right)(p+1)\right] & \\ \quad -\dfrac{2^{-k}\left(1+(-1)^b\right)}{p-1} - p^{-k-2}\left[(p-1)^{b-1}(p+1) + (-1)^b p\right] & \text{if } k < 0 \text{ and } b \neq 0. \end{cases}$$

Acknowledgement: The second author gratefully thanks the University of Waterloo, which hosted him on his sabbatical leave during the time the research was completed.

References

[1] I. Berstein and A.L. Edmonds, On the construction of branched coverings of low-dimensional manifolds, *Trans. Amer. Math. Soc.* **247** (1979), 87–124.

[2] _____, On the classification of generic branched coverings of surfaces, *Illinois J. Math.* **28** (1984), 64–82.

[3] J.L. Gross and T.W. Tucker, Generating all graph coverings by permutation voltage assignments, Discrete Math. **18** (1977) 273–283.

[4] _____, *Topological Graph Theory*, Wiley, New York, 1987.

[5] U. Hirsch, On regular homotopy of branched coverings of the sphere, *Manuscripts Math.* **21** (1977), 293–306.

[6] A. Hurwitz, Uber Riemann'sche Flächen mit gegebenen Verzweigungspunkten, *Math. Ann.* **39** (1891), 1–60.

[7] J.H. Kwak, J. Chun and J. Lee, Enumeration of regular graph coverings having finite abelian covering transformation groups, *SIAM J. Discrete Math.* **11** (1998) 273–285.

[8] J.H. Kwak, S. Kim and J. Lee, Distribution of regular branched prime-fold coverings of surfaces, *Discrete Math.* **156** (1996), 141–170.

[9] J.H. Kwak and J. Lee, Isomorphism classes of graph bundles, *Canad. J. Math.* **XLII** (1990), 747–761.

[10] _____, Enumeration of connected graph coverings, *J. Graph Theory* **23** (1996) 105–109.

[11] _____, Distribution of branched $\mathbb{D}_p$-coverings of surfaces, *Discrete Math.* **183** (1998), 193–212.

[12] V. Liskovets, Towards the enumeration of subgroups of the free group, Dokl. Akad. Nauk BSSR, 15 (1971) 6-9 (in Russian).

[13] A.D. Mednykh, On unramified coverings of compact Riemann surfaces, *Soviet Math. Dokl.* **20** (1979), 85-88.

[14] A.D. Mednykh and G.G. Pozdnyakova, Number of nonequivalent coverings over a nonorientable compact surface, *Siber. Math. J.* **27** (1986), 99-106.

[15] S. Stahl, Generalized embedding schemes, *J. Graph Theory*, **2** (1978), 41–52.

Weakly Distance-Regular Digraphs

Hiroshi SUZUKI*
Department of Mathematics
International Christian University
Mitaka-shi, Tokyo 181-8585, JAPAN

Kaishun WANG†
Institute of Systems Science
Academia Sinica
Beijing 100080, P.R.CHINA

1 Introduction

Lam [5] considered the following generalization of distance-transitive graphs and made some basic theory. A connected digraph is said to be *distance-transitive* if, for any vertices x, y, x' and y' with $\partial(x,y) = \partial(x',y')$, there is an automorphism $\delta \in \mathrm{Aut}(\Gamma)$ taking x to x' and y to y'. A connected digraph Γ is said to be *distance-regular* if $|\{z \in V\Gamma \mid \partial(x,z) = i \text{ and } \partial(z,y) = j\}|$ depends only on i, j and $\partial(x,y) = k$, rather than the individual vertices x and y with $\partial(x,y) = k$. Damerell [4] introduced the concept and proved that $d = g$ or $d = g-1$. Moreover a distance-regular digraph with $d = g$ is a coclique extension of a distance-regular digraph with $d = g-1$. Using these results, Bannai, Cameron and Kahn [1] proved that a distance-transitive digraph of odd girth is a Paley tournament or a directed cycle. Leonard and Nomura [6] proved that except directed cycles all distance-regular digraphs with $d = g-1$ have girth $g \leq 8$. In order to find 'good' classes of digraphs with unbounded diameter, the condition of distance-regularity seems to be too strong. Damerell [4] suggested a more natural definition of distance-transitivity, i.e., weakly distance-transitivity. In this talk, we not only introduce weakly distance-regular digraphs and give some constructions, but discuss connections to association schemes. Finally, we determine all commutative weakly distance-regular digraphs of valency 2.

In this talk, Γ denotes a finite digraph. For any two vertices $x, y \in V\Gamma$, define $\tilde{\partial}(x,y) = (\partial(x,y), \partial(y,x))$.

Definition 1.1 ([4]) A connected digraph Γ is said to be *weakly distance-transitive* if, for any vertices x, y, x' and y' of Γ satisfying $\tilde{\partial}(x,y) = \tilde{\partial}(x',y')$, there exists an automorphism $\sigma \in Aut(\Gamma)$ such that $x' = \sigma(x)$ and $y' = \sigma(y)$.

Definition 1.2 ([7]) A connected digraph Γ is said to be *weakly distance-regular* if

$$p^{\tilde{k}}_{\tilde{i},\tilde{j}}(x,y) = |\{z \in V\Gamma \mid \tilde{\partial}(x,z) = \tilde{i} \text{ and } \tilde{\partial}(z,y) = \tilde{j}\}|$$

depends only on $\tilde{k}, \tilde{i}, \tilde{j}$ and does not depend on the choices of x and y with $\tilde{\partial}(x,y) = \tilde{k}$. The numbers $p^{\tilde{k}}_{\tilde{i},\tilde{j}}$ are called *intersection numbers* of Γ.

*Electronic mail: hsuzuki@icu.ac.jp
†Electronic mail: wangks@lsc02.iss.ac.cn

It is easy to see that a weakly distance-transitive digraph is weakly distance-regular .

A weakly distance-regular digraph Γ is *commutative* if $p^{\tilde{k}}_{\tilde{i}\tilde{j}} = p^{\tilde{k}}_{\tilde{j}\tilde{i}}$ for all $\tilde{i}, \tilde{j}, \tilde{k}$. Let $\Gamma_i(x) = \{y \in V\Gamma \mid \partial(x,y) = i\}$. $k_i = |\Gamma_i(x)|$ does not depend on the choice of $x \in V\Gamma$ and $k_1 = |\Gamma_1(x)|$ is called the *valency* of Γ.

Definition 1.3 Let G be a finite group and S a subset of G not containing the identity element. We define the *Cayley digraph* $\Gamma = \mathrm{Cay}(G,S)$ of G with respect to S by

$$V(\Gamma) = G \text{ and } E(\Gamma) = \{(g, sg) \mid g \in G, s \in S\}.$$

A Cayley digraph $\Gamma = \mathrm{Cay}(G,S)$ is connected if and only if $G = \langle S \rangle$. It is obvious that $\mathrm{Aut}(\Gamma)$ contains the right regular representation $R(G)$ of G, and Γ is vertex transitive.

The following is our main result.

Theorem 1.1 ([7]) *If Γ is a commutative weakly distance-regular digraph of valency 2 and girth g, then Γ is isomorphic to one of the following.*

(1) $\mathrm{Cay}(Z_{2g}, \{\bar{1}, \bar{2}\})$.

(2) $\mathrm{Cay}(Z_2 \times Z_q, \{(0,\bar{1}), (\bar{1},0)\}), q \geq 3$.

(3) $\mathrm{Cay}(Z_n, \{\bar{1}, \overline{n-1}\}), n \geq 3$.

(4) $\mathrm{Cay}(Z_{2g}, \{\bar{1}, \overline{g+1}\})$.

(5) $\mathrm{Cay}(Z_3^2, \{(0,\bar{1}), (\bar{1},0)\})$.

2 Constructions

Now we give another characterization of weakly distance-transitive digraphs. Let Γ be a weakly distance-regular digraph. For each vertex x of Γ, we define

$$\Gamma_{i,j}(x) = \{y \in V\Gamma \mid \tilde{\partial}(x,y) = (i,j)\}.$$

It is easy to see that $k_{i,j} = |\Gamma_{i,j}(x)|$ does not depend on the choice of $x \in V\Gamma$. For vertices x and y of Γ, let

$$P_{\tilde{i}\tilde{j}}(x,y) = \{z \in V\Gamma \mid \tilde{\partial}(x,z) = \tilde{i} \text{ and } \tilde{\partial}(z,y) = \tilde{j}\}.$$

If $\tilde{\partial}(x,y) = \tilde{k}$, then $|P_{\tilde{i}\tilde{j}}(x,y)| = p^{\tilde{k}}_{\tilde{i}\tilde{j}}(x,y)$.

The proof of next proposition is similar to the one in the undirected case. (See [3].)

Proposition 2.1 *A connected digraph Γ with diameter d is weakly distance-transitive if and only if it is vertex transitive and the vertex stabilizer $Aut(\Gamma)_v$ is transitive on the sets $\Gamma_{i,j}(v)$ for all $i,j = 0,1,\cdots,d$ and for a fixed $v \in V\Gamma$.*

Example 2.1 The simplest of weakly distance-regular digraphs is a directed cycle.

Proposition 2.2 *Let G be a finite abelian group and S a subset of G not containing the identity element. If $\Gamma = \mathrm{Cay}(G, S)$ is a weakly distance-regular digraph, then Γ is commutative.*

Proposition 2.3 *Let Z_{2g} be a cyclic group of order $2g$. Then*

$$\Gamma = \mathrm{Cay}(Z_{2g}, \{\overline{1}, \overline{2}\})$$

is a commutative weakly distance-transitive digraph.

Definition 2.1 Let Γ be a digraph. For any integer $k \geq 2$, we can construct a digraph Γ' with vertex set

$$V\Gamma' = \{(u, i) \mid u \in V\Gamma \text{ and } 0 \leq i \leq k-1\}$$

and the arc set

$$E\Gamma' = \{((u, i), (v, j)) \mid (u, v) \in E\Gamma\}.$$

The digraph Γ' is said to be a *k-coclique extension* of Γ. Γ'' is said to be a *k-clique extension* of Γ if

$$V\Gamma'' = \{(u, i) \mid u \in V\Gamma \text{ and } 0 \leq i \leq k-1\}$$

and

$$E\Gamma'' = \{((u, i), (v, j)) \mid (u, v) \in E\Gamma \text{ or } u = v \text{ and } i \neq j\}.$$

Theorem 2.4 *Let Γ be a weakly distance-regular digraph of girth g. Then a k-coclique extension Γ' of Γ is weakly distance-regular if and only if one of the following holds.*

(1) *There exist no vertices x and y of Γ with $\tilde{\partial}(x, y) = (g, g)$.*

(2) $p_{\bar{i},\bar{j}}^{(0,0)} = p_{\bar{i},\bar{j}}^{(g,g)}$ *for $\bar{i}$ and $\bar{j}$.*

If Γ is commutative, then Γ' is commutative. Moreover, if Γ is a weakly distance-transitive digraph satisfying (1)*, then Γ' is also weakly distance-transitive.*

Corollary 2.5 *Let Z_n be a cyclic group of order n. Then the following hold.*

(1) $\Gamma = \mathrm{Cay}(Z_{2kg}, \{\overline{1}, \overline{2}, \overline{2g+1}, \overline{2g+2}, \cdots, \overline{2(k-1)g+1}, \overline{2(k-1)g+2}\})$ *is a commutative weakly distance-transitive digraph, where $k, g \geq 2$.*

(2) $\Gamma = \mathrm{Cay}(Z_{kg}, \{\overline{1}, \overline{g+1}, \cdots, \overline{(k-1)g+1}\})$ *is a commutative weakly distance-transitive digraph, where $k, g \geq 2$.*

Theorem 2.6 *If Γ is a weakly distance-regular [resp. distance-transitive] digraph of girth $g \geq 3$, then a k-clique extension of Γ is weakly distance-regular [resp. distance-transitive].*

Theorem 2.7 *Let $\Gamma_1 = (X, E_1), \cdots, \Gamma_n = (X, E_n)$ be distance-regular digraphs of diameter 2 with the same intersection numbers. Let $\tilde{X} = X^n$, i.e., the directed product of n copies of X. Two vertices $\tilde{x} = (x_1, x_2, \cdots, x_n), \tilde{y} = (y_1, y_2, \cdots, y_n) \in \tilde{X}$ are adjacent if there exists some j such that*

$$\partial_{\Gamma_j}(x_j, y_j) = 1 \text{ and } x_i = y_i \text{ for all } i \neq j.$$

Then the digraph $\tilde{\Gamma}$ defined above is weakly distance-regular. Moreover, $\tilde{\Gamma}$ is commutative if Γ_i is commutative for some i.

Proposition 2.8 *Let m, n be integers at least 3. If*

$$\Gamma = \mathrm{Cay}(Z_n \times Z_m, \{(\bar{1}, 0), (0, \bar{1})\})$$

is weakly distance-regular, then $n = m = 3$ and Γ is a commutative weakly distance-transitive digraph.

Proposition 2.9 $\Gamma = \mathrm{Cay}(Z_2 \times Z_n, \{(0, \bar{1}), (\bar{1}, 0)\})$ *is a weakly distance-transitive digraph.*

3 Connections to Association Schemes

In this section, we will discuss the relations between wealky distance-regular digraphs and association schemes.

Definition 3.1 Let X be a finite set. Let $R_0, R_1, \cdots, R_d$ be relations defined on X satisfying the following.

(*i*) $R_0 = \{(x, x) \mid x \in X\}$.

(*ii*) $X \times X = R_0 \cup \cdots \cup R_d$ and $R_i \cap R_j = \emptyset$ if $i \neq j$.

(*iii*) ${}^tR_i = R_{i'}$ for some $i' \in \{0, 1, \cdots, d\}$, where ${}^tR_i = \{(x, y) \mid (y, x) \in R_i\}$.

(*iv*) For $h, i, j \in \{0, 1, \cdots, d\}$ and $(x, y) \in R_h$,

$$p^h_{i,j} = |\{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\}|$$

depends only on h, i, j and does not depend on the choice of $(x, y) \in R_h$.

Such a configuration $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ is called an *association scheme* of class d on X. If $p^h_{i,j} = p^h_{j,i}$ for all $h, i, j \in \{0, 1, \cdots, d\}$, $\mathcal{X}$ is called a *commutative association scheme*. If ${}^tR_i = R_i$ for all i, $\mathcal{X}$ is called a *symmetric association scheme*.

For more information about association schemes we would like to refer the readers to [2].

Theorem 3.1 *Let $\mathcal{X} = (X, \{R_{0,0}, R_{1,r(1,1)}, \cdots, R_{1,r(1,k_1)}, \cdots, R_{d,r(d,1)} \cdots, R_{d,r(d,k_d)}\})$ be a nonsymmetric association scheme satisfying*

$${}^tR_{i,j} = \{(x, y) \in X \times X \mid (y, x) \in R_{i,j}\} = R_{j,i}.$$

Let $A_{j,r(j,i)}$ be the adjacency matrix with respect to $R_{j,r(j,i)}$ and let $A = A_{1,r(1,1)} + \cdots + A_{1,r(1,k_1)}$. Then the following are equivalent.

(i) Let $\Gamma = (X, \{R_{1,r(1,1)} \cup \cdots \cup R_{1,r(1,k_1)}\})$ be a digraph. Then $\tilde{\partial}(x, y) = (j, r(j, i))$ if and only if $(x, y) \in R_{j,r(j,i)}$, i.e., Γ is a weakly distance-regular digraph.

(ii) For any non-negative integer $s \leq d$,

$$A^s = \sum_{j=0}^{s} \sum_{i=1}^{k_j} n(j, r(j,i), s) A_{j,r(j,i)}, \tag{1}$$

where $n(j, r(j,i), s)$ is the number of paths of length s connecting x and y with $(x,y) \in R_{j,r(j,i)}$ and $n(j, r(j,i), j) \neq 0$ for all $0 \leq j \leq d$ and $1 \leq i \leq k_j$.

(iii) For any non-negative integers $j, i \leq d$ and $1 \leq l \leq k_j$, let

$$\tilde{p}_{i,1}^{(j,r(j,l))} = \sum_{1 \leq k \leq k_i, 1 \leq m \leq k_1} p_{(i,r(i,k)),(1,r(1,m))}^{(j,r(j,l))}.$$

Then $\tilde{p}_{i,1}^{(j,r(j,l))} = 0$ if $j - i \geq 2$ and $\tilde{p}_{j-1,1}^{(j,r(j,l))} \neq 0$.

Corollary 3.2 *Let Γ be a weakly distance-regular digraph with adjacency matrices*

$$A_{0,0}, A_{1,r(1,1)}, \cdots, A_{1,r(1,k_1)}, \cdots, A_{d,r(d,1)}, \cdots, A_{d,r(d,k_d)}$$

and let $\mathcal{A}(\Gamma)$ be the Bose-Mesner algebra of Γ. Then

$$d + 1 \leq \dim \mathcal{A}(\Gamma) \leq 1 + k_1 \cdots + k_d. \tag{2}$$

Moreover, if both equalities hold in (2), then Γ is distance-regular.

4 Proof of Theorem 1.1

Throughout this section, we assume that Γ is a commutative weakly distance-regular digraph of valency 2 and girth g.

Lemma 4.1 *If there exists an arc (u,v) with $\partial(v,u) = q - 1 \geq g$, then, for any $x \in V\Gamma$, there exist the following two circuits with only one common vertex*

$$(x = x_1, x_2, \cdots, x_g) \text{ and } (x = y_1, y_2, \cdots, y_q)$$

such that

$$\tilde{\partial}(y_1, y_2) = \tilde{\partial}(y_q, y_1) = (1, q-1).$$

Proposition 4.2 *If there exists an arc (u,v) with $\partial(v,u) = q - 1 \geq g$, then Γ is isomorphic to one of the following.*

(1) $\mathrm{Cay}(Z_{2g}, \{\overline{1}, \overline{2}\})$.

(2) $\mathrm{Cay}(Z_2 \times Z_q, \{(0,\overline{1}), (\overline{1},0)\})$.

Lemma 4.3 *If every arc is contained in a minimal circuit, then, for any $x \in V\Gamma$, there exist the following two minimal circuits*

$$(x = x_1, x_2, \cdots, x_g) \text{ and } (x = y_1, y_2, \cdots, y_g)$$

satisfying $|\{x_2, x_g, y_2, y_g\}| = 4$.

Proposition 4.4 *If every arc is contained in a minimal circuit, then* Γ *is isomorphic to one of the following.*

(1) $\mathrm{Cay}(Z_n, \{\overline{1}, \overline{n-1}\})$.

(2) $\mathrm{Cay}(Z_{2g}, \{\overline{1}, \overline{g+1}\})$.

(3) $\mathrm{Cay}(Z_3^2, \{(0,\overline{1}), (\overline{1},0)\})$.

Combining Proposition 4.2 and Proposition 4.4, we complete the proof of Theorem 1.1.

Remarks. Theorem 1.1 also holds for a weakly distance-transitive digraph.

Problems

(1) Find examples of non-commutative weakly distance-regular digraphs.

(2) Given a distance-regular graph Γ' of even valency. Let Γ be a digraph by adding direction in Γ'. When is Γ weakly distance-regular?

(2′) Given a weakly distance-regular digraph Γ. Let Γ' be a graph by deleting the direction of Γ. When is Γ distance-regular?

References

[1] E. Bannai, P. J. Cameron and J. Kahn, Nonexistence of certain distance-transitive digraphs, *J. Combin. Theory Ser.B* **31** (1981), 105-110.

[2] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin/Cummings, California, 1984.

[3] N. L. Biggs, *Algebraic Graph Theory*, Second Edition, Cambridge University Press, 1993.

[4] R. M. Damerell, Distance-transitive and distance regular digraphs, *J. Combin. Theory, Ser.B* **31** (1981), 46-53.

[5] C. W. Lam, Distance-transitive digraphs, *Discrete Math.* **29** (1980), 265-274.

[6] D. A. Leonard and K. Nomura, The girth of a directed distance-regular digraph, *J. Combin. Theory Ser.B* **58** (1993), 34-39.

[7] H. Suzuki and K.S. Wang, Weakly distance-regular digraphs, preprint.

Jacobi polynomials of ternary codes and generators of the invariant ring of a group

田辺顕一朗
Com²MaC, POSTECH
Pohang, 790-784, Korea
tanabe@com2mac.postech.ac.kr

1 イントロダクション

1997年、小関[5]によって符号のJacobi多項式が導入されました。この多項式はJacobi formの構成([1],[2])、及び符号の被覆半径の決定に有効な多項式です。Jacobi多項式は任意の有限体、あるいはもっと広く任意の有限アーベル群上の符号に対して定義することが可能です。ここではタイトルにあるように三元体上の符号のJacobi多項式に関して得られた結果を述べます。ここで述べる結果のbinary codeに対する同様の結果は既に[3]で得られています。

Jacobi多項式と符号の被覆半径の関係について初めに簡単に紹介しておきます。三元体 $\mathbb{F}_3$ 上の n 次元ベクトル空間 $\mathbb{F}_3^n$ の部分空間 C を三元体上の長さ n の線形符号と呼びます。以下簡単に C のことを符号と呼びます。

$a = (a_k), b = (b_k) \in \mathbb{F}_3^n$ と $i, j \in \{0,1,2\}$ に対して、記号 $\mathrm{wt}(a) := |\{k \mid a_k \neq 0\}|$ と $\mathrm{wt}_{ij}(a,b) := |\{k \mid a_k = i \text{ and } b_k = j\}|$ を準備します。また内積 $(a,b) := \sum_{k=1}^n a_k b_k$ を定義します。符号 C に対してその直交空間 $C^\perp := \{a \in \mathbb{F}_3^n \mid (a,c) = 0, \text{ for all } c \in C\}$ を定義します。$C = C^\perp$ を満たす符号 C はself-dualであると呼ばれます。$a \in \mathbb{F}_3^n$ と符号 C に対して x, y, u, v, w を変数とする多項式

$$\begin{aligned} & HM\text{-}Jac(C, a; x, y, u, v, w) \\ := & \sum_{c \in C} x^{\mathrm{wt}_{00}(a,c)} y^{\mathrm{wt}_{01}(a,c)+\mathrm{wt}_{02}(a,c)} \\ & \times u^{\mathrm{wt}_{10}(a,c)+\mathrm{wt}_{20}(a,c)} v^{\mathrm{wt}_{11}(a,c)+\mathrm{wt}_{22}(a,c)} w^{\mathrm{wt}_{12}(a,c)+\mathrm{wt}_{21}(a,c)} \end{aligned}$$

を a に関する C のhomogeneous modified Jacobi polynomialと呼びます。以下簡単にJacobi多項式と呼びます。Jacobi多項式において変数を以下のよう

に置き換えると、

$$\begin{aligned} & HM\text{-}Jac(C,a;x,y,y,y,x) \\ = & \sum_{c\in C} x^{\mathrm{wt}_{00}(a,c)+\mathrm{wt}_{12}(a,c)+\mathrm{wt}_{21}(a,c)} \\ & \times y^{\mathrm{wt}_{01}(a,c)+\mathrm{wt}_{02}(a,c)+\mathrm{wt}_{10}(a,c)+\mathrm{wt}_{20}(a,c)+\mathrm{wt}_{11}(a,c)+\mathrm{wt}_{22}(a,c)} \\ = & \sum_{c\in C} x^{n-\mathrm{wt}(a+c)}y^{\mathrm{wt}(a+c)} \\ =: & \ W_{a+C}(x,y) \end{aligned}$$

となり、coset weight enumerator と呼ばれる多項式 $W_{a+C}(x,y)$ を得ます。$W_{a+C}(x,y)$ から値 $\min_{c\in C}\mathrm{wt}(a+c)$ が決定できることに注意します。したがって、全ての $a\in\mathbb{F}_3^n$ に対して $W_{a+C}(x,y)$ が分かれば、

$$\rho(C) := \max_{a\in\mathbb{F}_3^n}\min_{c\in C}\mathrm{wt}(a+c)$$

という値が決定できます。実は $\rho(C)$ は $\mathbb{F}_3^n = \cup_{c\in C}\{a\in\mathbb{F}_3^n \mid \mathrm{wt}(a-c)\le r\}$ を満たす r の最小値に一致することが簡単に確かめられ、符号 C の被覆半径と呼ばれています。与えられた符号に対してその被覆半径を決定するのは符号理論における重要な問題の一つです。

以上 Jacobi 多項式から符号の被覆半径及び coset weight enumerator が得られることを見てきたわけですが、一般に与えられた符号に対してその Jacobi 多項式を計算するのは困難な問題です。しかし以下に見るように符号が self-dual である場合には不変式論の方から Jacobi 多項式に関する情報を得ることが可能になります。

符号 C に対して次の MacWilliam 型の恒等式が成り立ちます [6]。

$$\begin{aligned} & HM\text{-}Jac(C^{\perp},a;x,y,u,v,w) \\ = & \ \frac{1}{|C|}HM\text{-}Jac(C,a;x+2y,x-y,u+v+w,u+\omega v+\omega^2 w,u+\omega^2 v+\omega w). \end{aligned}$$

ここで $\omega := e^{2\pi\sqrt{-1}/3}$. また符号 C が self-dual の場合には、$a\in C$ に対して mod 3 で

$$\begin{aligned} & 0=(a,a)=\textstyle\sum_{k=1}^n a_k = |\{k\mid a_k=1\}|+2^2|\{k\mid a_k=2\}| \\ & =|\{k\mid a_k=1\}|+|\{k\mid a_k=2\}| = \mathrm{wt}(a) \end{aligned}$$

が成り立つことより $\mathrm{wt}(a)$ は 3 の倍数であることが分かります。したがって符号 C が self-dual である場合には $HM\text{-}Jac(C,a;x,y,u,v,w)$ は次の行列 L_1

と L_2 で生成される群で不変であることが分かります。

$$L_1 := \frac{1}{\sqrt{3}}\left[\begin{array}{cc|ccc} 1 & 1 & 0 & 0 & 0 \\ 2 & -1 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & \omega^2 & \omega \\ 0 & 0 & 1 & \omega & \omega^2 \end{array}\right],$$

$$L_2 := \mathrm{diag}(1, \omega, 1, \omega, \omega).$$

さらに C が $(1, \ldots, 1) \in \mathbb{F}_3^n$ を含む場合には行列 $L_3 := \mathrm{diag}(\omega, 1, \omega, 1, 1)$ でも不変になることが確認できます。したがって Γ を L_1, L_2 と L_3 で生成される $GL_5(\mathbb{C})$ の部分群とすると $(1, \ldots, 1) \in \mathbb{F}_3^n$ を含む self-dual code C に対して $HM\text{-}Jac(x, y, u, v, w)$ は不変式環 $\mathbb{C}[x, y, u, v, w]^\Gamma$ の元となります。この講演の目的は $\mathbb{C}[x, y, u, v, w]^\Gamma$ の生成元を求めることです。より正確には次の定理 1 に表れる生成元の組 $\{\theta_1, \ldots, \theta_N, \rho_1, \ldots, \rho_m\}$ を求めます。

G を $GL_N(\mathbb{C})$ の有限部分群とし、多項式環 $\mathbb{C}[x_1, \ldots, x_N]$ への作用に対する不変式環 $\mathbb{C}[x_1, \ldots, x_N]^G$ を考えます。次の結果が知られています:

定理 1 ([9] Theorem 6.8.4.) N 個の $\mathbb{C}$ 上代数的に独立な斉次不変式 $\theta_1, \ldots, \theta_N \in \mathbb{C}[x_1, \ldots, x_N]^G$ と有限個の斉次不変式 $\rho_1, \ldots, \rho_m \in \mathbb{C}[x_1, \ldots, x_N]^G$ が存在して

$$\mathbb{C}[x_1, \ldots, x_N]^G = \oplus_{i=1}^m \rho_i \mathbb{C}[\theta_1, \ldots, \theta_N].$$

が成り立つ。特に $\mathbb{C}[x_1, \ldots, x_N]^G$ は Cohen-Macaulay 環となる。

したがって $\mathbb{C}[x, y, u, v, w]^\Gamma$ は有限個の斉次多項式から成る生成元を持つことが保証されます。生成元が分かると、次数が n の各斉次空間 $\mathbb{C}[x, y, u, v]_n$ の基底がそれらを使って構成でき、長さ n の符号の Jacobi 多項式はその基底を用いて書くことが出来ます。さらに C が extremal という仮定をすると、Jacobi 多項式の定義から y, v と w に関する次数が $3\lfloor n/12 \rfloor + 3$ より小さい項の係数は消えてなければならないので C の Jacobi 多項式の係数に関する情報が得られます。

しかし一般に、与えられた群に対して生成元 $\{\theta_1, \ldots, \theta_N, \rho_1, \ldots, \rho_m\}$ を具体的に求めることは難しい問題になります。

Remark. L_1 と L_2 で生成される群 Γ_1 に対してもこれから述べる方法を用いて不変式環 $\mathbb{C}[x, y, u, v, w]^{\Gamma_1}$ の生成元を求めることが出来ます。これは必ずしも $(1, \ldots, 1)$ を含んでいない self-dual code の Jacobi 多項式が入る不変式環です。

2 $\mathbb{C}[x,y,u,v,w]^{\Gamma}$ の生成元

群がユニタリ行列の全体の中に入っている方が取り扱いがしやすいので以下のように基底を変更します。

$$\begin{aligned} x_1 &:= x, \\ y_1 &:= \sqrt{2}y, \\ x_2 &:= \sqrt{2}u, \\ y_2 &:= v+w, \\ z &:= v-w. \end{aligned}$$

この変更の下で L_i $(i=1,2,3)$ は次の行列表示 $\tilde{L}_i$ $(i=1,2,3)$ を持ちます:

$$\tilde{L}_1 := \begin{bmatrix} \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{2} & -1 \end{bmatrix} & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{2} & -1 \end{bmatrix} & 0 \\ 0 & 0 & -\sqrt{-1} \end{bmatrix},$$

$$\tilde{L}_2 := \mathrm{diag}(1,\omega,1,\omega,\omega), \text{ and}$$

$$\tilde{L}_3 := \mathrm{diag}(\omega,1,\omega,1,1).$$

$\tilde{\Gamma}$ を $\tilde{L}_1, \tilde{L}_2$ と $\tilde{L}_3$ から生成される群として、$\mathbb{C}[x_1,y_1,x_2,y_2,z]^{\tilde{\Gamma}}$ の不変式環を求めます。

$$\sigma_1 := \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & \sqrt{2} \\ \sqrt{2} & -1 \end{bmatrix}, \ \sigma_2 := \begin{bmatrix} 1 & 0 \\ 0 & \omega \end{bmatrix}, \text{ and } \sigma_3 := \begin{bmatrix} \omega & 0 \\ 0 & 1 \end{bmatrix}.$$

とおき、$G_7 := \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ とおきます。G_7 は Shephard-Todd[8] によって分類された複素鏡映群の一つであり、その位数は 144 です。G_7 の不変式環は

$$\begin{aligned} \mathbb{C}[x,y]^{G_7} &= \mathbb{C}[\theta_1^3, \theta_2^2], \\ \theta_1 &:= x^4 + 2\sqrt{2}xy^3, \\ \theta_2 &:= x^6 - 5\sqrt{2}x^3y^3 - y^6, \end{aligned}$$

で与えられます。$f \in \mathbb{C}[x,y]$ が、

$$\theta_1^3(\partial_x, \partial_y)f = \theta_2^2(\partial_x, \partial_y)f = 0$$

を満たす時、f は G_7 の調和多項式と呼ばれます。ここで $\partial_x := \partial/\partial_x, \partial_y := \partial/\partial_y$. G_7 の調和多項式の全体のなす $\mathbb{C}[x,y]$ の部分空間を H で表すことにします。H は $\mathbb{C}[x,y]$ の G_7-部分加群となります。

$\mathbb{C}[x_1,y_1,x_2,y_2,z]^{\tilde{\Gamma}}$ の生成元を求めるために次に紹介する Steinberg と Chevalley の結果を用います。これらの結果は一般の複素鏡映群に対して成り立つ結果です。

補題 2 (1) (Steinberg [11]) $\dim_{\mathbb{C}} H = |G_7|$. また G_7-加群としての同型

$$\begin{aligned} H \otimes_{\mathbb{C}} \mathbb{C}[x,y]^{G_7} &\simeq \mathbb{C}[x,y], \\ f \otimes g &\mapsto fg \end{aligned}$$

が成り立つ。

(2) (Chevalley [4]) G_7 の H 上の表現は正則表現である。

$H^1 \subset \mathbb{C}[x_1,y_1]$, $H^2 \subset \mathbb{C}[x_2,y_2]$ を G_7 の調和多項式達の成す部分空間とします。Steinberg の結果を用いると、

$$\begin{aligned} \mathbb{C}[x_1,y_1,x_2,y_2,z] &\simeq \mathbb{C}[x_1,y_1] \otimes_{\mathbb{C}} \mathbb{C}[x_2,y_2] \otimes_{\mathbb{C}} \mathbb{C}[z] \\ &\simeq H^1 \otimes \mathbb{C}[x_1,y_1]^{G_7} \otimes H^2 \otimes \mathbb{C}[x_2,y_2]^{G_7} \otimes (\oplus_{i=0}^{11} \mathbb{C} z^i) \otimes \mathbb{C}[z^{12}] \end{aligned}$$

したがって $\tilde{L}_i$ $(i=1,2,3)$ の作用を考えると、

$$\begin{aligned} & \mathbb{C}[x_1,y_1,x_2,y_2,z]^{\tilde{\Gamma}} \\ \simeq\ & \oplus_{i=0}^{11} (H^1 \otimes H^2 \otimes z^i)^{\tilde{\Gamma}} \\ & \otimes \mathbb{C}[\theta_1^3(x_1,y_1), \theta_2^2(x_1,y_1)] \otimes \mathbb{C}[\theta_1^3(x_2,y_2), \theta_2^2(x_2,y_2)] \otimes \mathbb{C}[z^{12}], \end{aligned}$$

を得ます。$\mathrm{Irr}(G_7)$ を G_7 の既約指標の全体とします。Chevalley の結果より、各 $\chi \in \mathrm{Irr}(G_7)$ の H での重複度は $\chi(1)$ です。H の G_7-既約加群への分解が具体的に与えられたとします:

$$\begin{aligned} H &= \oplus_{\chi \in \mathrm{Irr}(G_7)} \oplus_{i=1}^{\chi(1)} H_{\chi,i}, \\ & (H_{\chi,j} \text{ の指標 }) = \chi. \end{aligned}$$

この分解から G_7-加群としての分解

$$\begin{aligned} & H^1 \otimes H^2 \otimes z^k \\ =\ & \oplus_{\chi^1,\chi^2 \in \mathrm{Irr}(G_7)} \oplus_{i=1}^{\chi^1(1)} \oplus_{j=1}^{\chi^2(1)} H^1_{\chi^1,i} \otimes H^2_{\chi^2,j} \otimes z^k \end{aligned}$$

を得ます。$\chi^1, \chi^2 \in \mathrm{Irr}(G_7)$, $1 \le i,j \le \chi(1)$, $1 \le k \le 11$ とし、G_7-部分加群

$$H^1_{\chi^1,i} \otimes H^2_{\chi^2,j} \otimes z^k,$$

を考えます。φ_k を G_7 の線形指標で $\varphi_k(\sigma_1) = (-\sqrt{-1})^k$, $\varphi_k(\sigma_2) = \omega^k$, $\varphi_k(\sigma_3) = 1$ を満たすものとします。σ_1 の位数は 2 なので実際は k が偶数の場合しかそ

のような指標は存在しないことに注意します。$\tilde{L}_1 z^k = (\sqrt{-1})^k z^k$, $\tilde{L}_2 z^k = \omega^{2k} z^k, \tilde{L}_3 z^k = z^k$ に注意すると、

$$\{g \in H^1_{\chi^1,i} \otimes H^2_{\chi^2,j} \mid \sigma \cdot g = \varphi_k(\sigma) g \text{ for all } g \in G_7\}$$

を求めれば $(H^1_{\chi^1,i} \otimes H^2_{\chi^2,j} \otimes z^k)^{\tilde{\Gamma}}$ を得ることが出来ることが分かります。ただし G_7 の $H^1 \otimes H^2 \subset \mathbb{C}[x_1, y_1] \otimes \mathbb{C}[x_2, y_2]$ 上の表現は $g \mapsto g \otimes g$, $g \in G_7$ で考えています。

$\chi^1, \chi^2 \in \mathrm{Irr}(G_7)$ に対して、$\langle \chi^1 \times \chi^2, \varphi \rangle = \langle \chi^1, \varphi \times \bar{\chi^2} \rangle = \delta_{\chi^1, \varphi \times \bar{\chi^2}}$ が成り立つことより、

$$\dim_{\mathbb{C}}\{g \in H^1_{\chi^1,i} \otimes H^2_{\chi^2,j} \mid \sigma \cdot g = \varphi_k(\sigma) g \text{ for all } g \in G_7\} = \delta_{\chi^1, \varphi \times \bar{\chi^2}}$$

となります。まとめると次の結果を得ました。

定理 3 $\theta_1^3(x_1, y_1), \theta_2^2(x_1, y_1), \theta_1^3(x_2, y_2), \theta_2^2(x_2, y_2), z^{12}$ と

$$\mathcal{M}_{\chi,i,j,k} := (H^1_{\chi,i} \otimes H^2_{\varphi_k \times \bar{\chi},j} \otimes z^k)^{\tilde{\Gamma}},$$
$$k = 0, 2, 4, \ldots, 10,\ \chi \in \mathrm{Irr}(G_7),\ 1 \le i, j \le \chi(1)$$

は $\mathbb{C}[x_1, y_1, x_2, y_2, z]^{\tilde{\Gamma}}$ の生成元を与える。各 $\mathcal{M}_{\chi,i,j,k}$ は 1 次元である。

定理 1 に対応させると、$\theta_1^3(x_1, y_1), \theta_2^2(x_1, y_1), \theta_1^3(x_2, y_2), \theta_2^2(x_2, y_2), z^{12}$ は $\mathbb{C}$ 上代数的独立な不変式を与え、$\mathcal{M}_{\chi,i,j,k}$ はそれ以外の有限個の不変式を与えていることになります。

$\mathcal{M}_{\chi,i,j,k}$ の基底は、例えば $k = 0$ とすると以下のようにして求めることが出来ます。φ_0 は G_7 の自明な指標となります。$H^1_{\chi,i}$ の基底を $f_1, \ldots, f_{\chi(1)}$, $H^2_{\bar{\chi},j}$ の双対基底を $f_1^*, \ldots, f_{\chi(1)}^*$ とすると、$\mathcal{M}_{\chi,i,j,0}$ の基底は $\sum_{k=1}^{\chi(1)} f_k f_k^*$ で与えられます。k が他の値を取る場合もほぼ同様にして $\mathcal{M}_{\chi,i,j,k}$ の基底を具体的に求めることが出来ます。

以上のことから H の G_7-既約加群への分解 $H = \oplus_{\chi \in \mathrm{Irr}(G_7)} \oplus_{i=1}^{\chi(1)} H_{\chi,i}$ が具体的に分かれば $\mathbb{C}[x_1, y_1, x_2, y_2, z]^{\tilde{\Gamma}}$ の生成元が構成できることが分かりました。次にその分解の方法の概略を述べます。G_4 を $\sqrt{-1}\sigma_1$ と σ_2 で生成される群とします。G_4 も複素鏡映群で位数は 24, また G_7 の指数 6 の正規部分群となっています。さらに $G_7 = \langle G_4, \zeta_{12} \rangle$ が成り立ちます。ここで

$$\zeta_{12} := \begin{bmatrix} e^{2\pi\sqrt{-1}/12} & 0 \\ 0 & e^{2\pi\sqrt{-1}/12} \end{bmatrix}.$$

したがって $U \subset \mathbb{C}[x, y]$ を斉次多項式から成る G_4-部分加群とすると、U は G_7-部分加群にも成ります。G_4 の調和多項式からなる部分空間 $H(G_4)$ を G_4-

既約加群の直和に分解しておきます。GAP[7] と Maple を使用しますが群の位数が小さいためこれは比較的容易に出来ます。調和多項式の定義から $H = \oplus_{i=0}^{2} \oplus_{j=0}^{1} \theta_1^i \theta_2^j H(G_4)$ が分かります。したがって目的の H の G_7-既約加群への分解が得られます。$H(G_4)$ の G_4-既約加群の直和への分解のデータ、およびそれを利用しての $\mathcal{M}_{\chi,i,j,k}$ の基底の具体的な構成などは全て [12] に載せてあります。

References

[1] E. Bannai, S. Minashima, and M. Ozeki, On Jacobi forms of weight 4, *Kyushu J. Math.* Vol. 50 (1996), 335–370.

[2] E. Bannai and M. Ozeki, Construction of Jacobi forms from certain combinatorial polynomials, *Proc. Japan Acad. Ser. A Math. Sci.* Vol. 72 (1996), 12–15.

[3] E. Bannai, M. Ozeki, and K. Tanabe, Determination of the ring of simultaneous invariants for a group associated with MacWilliams identity, in preparation.

[4] C. Chevalley, Invariants of finite groups generated by reflections, *Amer. J. Math.* Vol. 77 (1955), 778–782.

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

[6] M. Ozeki, On the covering radius problem for ternary self-dual codes, to appear in Theoretical Computer Science.

[7] M. Schönert (ed.), *Groups, Algorithms and Programming*, Lehrstuhl D für Mathematik, RWTH Aachen, Germany (1994) available via anonymous ftp on the server ftp://ftp-gap.dcs.st-and.ac.uk/pub/gap

[8] G. C. Shephard and J. A. Todd, Finite unitary reflection groups. *Canadian J. Math.* Vol. 6, (1954). 274–304.

[9] L. Smith, *Polynomial invariants of finite groups*, Research Notes in Mathematics, 6, A K Peters, Ltd., Wellesley, MA, 1995.

[10] R. Stanley, Relative invariants of finite groups generated by pseudoreflections, *J. Algebra* 49 (1977), 134–148.

[11] R. Steinberg, Differential equations invariant under finite reflection groups, *Trans. Amer. Math. Soc.* Vol. 112 (1964) 392–400.

[12] K. Tanabe, Modified Jacobi polynomials of ternary codes and the invariant ring of a related group, preprint.

On Relative Difference Sets in Non-Abelian p-Groups

Dominic Elvira* and Yutaka Hiramine

Abstract

In this article, we study semi-regular relative difference sets (RDS's) in non-abelian p-groups containing a maximal cyclic subgroup of index p. In particular, we prove that if the modular p-group $M_n(p)$ has a non-trivial semi-regular RDS then the order of the forbidden subgroup is p. We also show that $M_3(p)$, $p \geq 3$ contains a semi-regular RDS. On the other hand, we prove that $M_n(2)$ and the semi-dihedral group SD_{2^n} do not contain a non-trivial RDS for any $n \geq 4$.

1 Introduction

An (m, u, k, λ) *relative difference set* (RDS) in a group G of order mu relative to a normal subgroup U of order u is a k-element subset R of G such that the number of ordered pairs (r_1, r_2) with $r_1 r_2^{-1} = g$ $(r_1, r_2 \in R)$ for every $g \in G$, $g \neq 1$ is λ if $g \in G \setminus U$ or 0 if $g \in U$. By this inherent property of U, we often call it the *forbidden subgroup*. If $k = u\lambda$, we call R a *semi-regular* RDS and its parameters are given by $(u\lambda, u, u\lambda, \lambda)$. In this case, R is a set of coset representatives of G/U. Moreover, if $u = 1$, R is called a *trivial semi-regular RDS*. Any group G itself is a trivial semi-regular RDS.

Previous studies on RDS's, especially the semi-regular case have been focused mainly in abelian p-groups ([2], [9], [13]). In contrast, examples and results in non-abelian case are rather scarce. Thus we aim to explore the properties of RDS's in some non-abelian groups and exhibit examples when possible. This may help to enlighten us what is going on at least in non-abelian p-groups. Specifically, we have been considering non-abelian p-groups G of order p^n which contains a cyclic subgroup H of order p^{n-1}. In [5], a complete classification of these groups was given, namely:

(1) $M_n(p)$, the modular p-group of order p^n with $n \geq 3$ if $p > 2$ and $n \geq 4$ if $p = 2$,

(2) D_{2^n}, the dihedral group of order 2^n with $n \geq 3$,

(3) Q_{2^n}, the generalized quaternion group of order 2^n with $n \geq 3$, and

(4) SD_{2^n}, the semi-dihedral group of order 2^n with $n \geq 4$.

*This author is a faculty member of Philippine Normal University (PNU), Manila on study leave at Kumamoto University under a Monbusho grant.

As a review, in [4] the authors were able to prove the non-existence of non-trivial semi-regular RDS's in D_{2^n} for $n \geq 3$, in fact, in any dihedral group D_{2m} for any positive integer m. In the same paper, we constructed an example of a semi-regular RDS in Q_{2^n} with parameters $(2^{n-1}, 2, 2^{n-1}, 2^{n-2})$ relative to is center for $n \geq 3$. This result, as we found out, is related to a conjecture of N. Ito that asserts the existence of a $(4t, 2, 4t, 2t)$ RDS in the dicyclic group Q_{8t}, see [13]. On the other hand, the search for RDS's in the modular p-group $M_n(p)$ and the semi-dihedral group SD_{2^n} have been open problems.

In this note, we focus our attention to the groups SD_{2^n} and $M_n(p)$ where p is any prime. In particular, we prove that if the modular p-group $M_n(p)$ has a non-trivial semi-regular relative difference set then the forbidden subgroup is of order p unless $(n, p) = (4, 2)$. We also show that $M_n(2)$ and the semi-dihedral group SD_{2^n} do not contain a non-trivial RDS for any $n \geq 4$. Moreover, we show that $M_3(p)$ has a (p^2, p, p^2, p)-RDS when $p > 2$. As a consequence of this construction, we show the existence of a semi-regular RDS in any extra-special p-group of order p^{2m+1} with parameters $(p^{2m}, p, p^{2m}, p^{2m-1})$ relative to its center for any $m \geq 2$.

2 Preliminaries and Terminologies

In this section, known results that will be used frequently are provided. All groups and sets are assumed to be finite and the terminologies applied are as in [5] and [11].

For a subset X of G, we set $X^{-1} = \{x^{-1} \mid x \in X\}$ and throughout this article we identify a subset X of G with a group ring element $\widehat{X} = \sum_{x \in X} x \in \mathbb{Z}[G]$. By definition, a k-subset R of G is an (m, u, k, λ) RDS in G relative to $U (\triangleleft G)$ if and only if R satisfies the following equation in the group ring $\mathbb{Z}[G]$:

$$RR^{-1} = k + \lambda(G - U).$$

As any group G itself is a trivial semi-regular RDS relative to $\{1\}$, in the rest of this article we consider only *non-trivial semi-regular RDS's*. We also consider the forbidden subgroup U to be always a normal subgroup of G and by the symbol p, we mean a prime number.

The following result due to Elliot and Butson [3] is basic in the study of relative difference sets.

Result 2.1 *Let R be an (m, u, k, λ) RDS in a group G relative to a normal subgroup U and let U_1 be a normal subgroup of G contained in U. Set $\overline{G} = G/U_1$. Then $\overline{R}$ is an $(m, u/u_1, k, u_1\lambda)$ RDS in $\overline{G}$ relative to $\overline{U}$.*

For a group X, we denote its exponent by $\exp(X)$.

Result 2.2 *Let G be an abelian group of order p^{a+b}. If G contains a (p^a, p^b, p^a, p^{a-b}) RDS R relative to U then the following exponent bound conditions hold:*

(i) $exp(G) \leq p^a$ unless $G \simeq \mathbb{Z}_4$,

(ii) $exp(G) \leq p^{a+b-\lceil a/2 \rceil}$, and

(iii) if a is odd and $p > 2$, then $exp(G) \leq p^{(a+1)/2}$ and if $p = 2$, then $exp(U) \leq p^{(a+1)/2}$.

In the above result, (i) and (ii) are Corollaries 3.2 and 3.5 in [10], respectively, while (iii) is Theorem 4.2 in [8]. The next result is called the *product construction for semi-regular RDS's.*

Result 2.3([1], [12]) *Let G satisfy the following:*

(i) $G = G_1G_2$ for some subgroups G_1 and G_2,

(ii) either $G \rhd G_1$ or $G \rhd G_2$,

(iii) $G \rhd G_1 \cap G_2$, and

(iv) R_i is a $(u\lambda_i, u, u\lambda_i, \lambda_i)$ RDS in G_i relative to $U = G_1 \cap G_2$ for each $i \in \{1, 2\}$.

Then R_1R_2 is a $(u^2\lambda_1\lambda_2, u, u^2\lambda_1\lambda_2, u\lambda_1\lambda_2)$ RDS in G relative to U.

At this point, we shift our attention to the *modular p-group* $M_n(p)$. Using generators x and y, this group is defined by:

$$M_n(p) = \langle x, y \mid x^{p^{n-1}} = y^p = 1,\ y^{-1}xy = x^{1+p^{n-2}} \rangle.$$

Set $G = M_n(p)$ and $z = x^{p^{n-2}}$. Then, by Theorem 5.4.3 in [5],

$$[G, G] = \langle z \rangle \quad \text{and} \quad Z(G) = \langle x^p \rangle.$$

We note that when $p = 2$, we have $n \geq 4$ as $M_3(2) \simeq D_8$, the dihedral group of order 8 and if $p > 2$, we have $n \geq 3$.

For every $g \in G$, we can write $g = x^iy^j$ where $0 \leq i \leq p^{n-1} - 1$ and $0 \leq j \leq p-1$. The next lemma provides a summary of the group operations in G that we will use most often. The proof can be obtained by simple computations.

Lemma 2.4 *Let x^ay^b and x^cy^d be elements of $G = M_n(p)$. Then the following hold:*

(i) $(x^ay^b)(x^cy^d) = x^{a+c-bcp^{n-2}}y^{b+d}$.

(ii) $(x^ay^b)(x^cy^d)^{-1} = x^{a-c+c(b-d)p^{n-2}}y^{b-d}$.

(iii) $(x^ay^b)^m = x^{ma-ab(1+2+\cdots+m-1)p^{n-2}}y^{mb}$.

(iv) Let $Aut(G)$ be the full automorphism group of G. Then $Aut(G) = \{\theta_{i,j,k} \mid 0 \leq i \leq p^{n-1} - 1, i \not\equiv 0 \pmod p,\ 0 \leq j, k \leq p-1\}$, where $\theta_{i,j,k}$ is an automorphism of G determined by $\theta_{i,j,k}(x) = x^iy^j$, $\theta_{i,j,k}(y) = x^{kp^{n-2}}y$.

Definition 2.5 *Let $\langle x \rangle$ be a cyclic group of order n. Let S be a collection of elements of $\langle x \rangle$. Here we assume that S can contain an element several times. Set $S = \{x^{m_1}, x^{m_2}, \cdots, x^{m_r}\}$. We define*

$$\varepsilon(S) = m_1 + m_2 + \cdots + m_r \pmod n.$$

We note that $\varepsilon(S)$ is uniquely determined modulo n.

3 The Parameters of a Semi-Regular RDS in $M_n(p)$

In this section, we let $G = M_n(p)$, the modular p-group of order p^n and we assume that R is a (p^a, p^b, p^a, p^{a-b}) RDS in G relative to a normal subgroup U. As $|G| = p^{a+b}$, we must have $n = a + b$ and $a \geq b$.

Lemma 3.1 *If R is a semi-regular RDS in G relative to U then its parameters are either one of the following cases:*

(i) $(8, 4, 8, 2)$,

(ii) $(p^2, p^2, p^2, 1)$ *with* $p \geq 2$,

(iii) $(p^{n-1}, p, p^{n-1}, p^{n-2})$ *with* $p \geq 2$.

Proof. If $|U| = p$, then we have case (iii). Assume $|U| = p^b \geq p^2$, that is, $b \geq 2$. Since $\langle z \rangle = [G, G] \leq Z(G) = \langle x^p \rangle$, we have $[G, G] \leq U$. Set $\overline{G} = G/[G, G] (\simeq \mathbb{Z}_{p^{n-2}} \times \mathbb{Z}_p)$. Then by Result 2.1, $\overline{R}$ is a non-trivial abelian $(p^a, p^{b-1}, p^a, p^{a-b+1})$ RDS in $\overline{G}$ relative to $\overline{U}$. Applying Result 2.2(i) to $\overline{G}$, we have $a + b - 2 \leq a$ and so $b = 2$. As $a \geq b$, $a \geq 2$.

By Result 2.2(ii), $a + b - 2 \leq a + b - 1 - [a/2]$. Hence $a \leq 3$. Thus we have $(a, b) = (2, 2)$ or $(3, 2)$. By Result 2.2(iii), $(a, b) \neq (3, 2)$ when $p > 2$. Hence $(a, b) = (2, 2)$ or $(a, b, p) = (3, 2, 2)$. Therefore we have the lemma.

We first settle case (i) of Lemma 3.1 by the following:

Lemma 3.2 *There exists no* $(8, 4, 8, 2)$ *RDS R in $M_5(2)$ relative to any subgroup U of order 4.*

Proof. Set $G = M_5(2)$ and let $G = \langle x, y \mid x^{16} = y^2 = 1,\ y^{-1}xy = xz \rangle$ where $z = x^8$. Assume that R is an $(8, 4, 8, 2)$ RDS in $M_5(2)$ relative to a normal subgroup U. Set $\overline{G} = G/\langle z \rangle (\simeq \mathbb{Z}_8 \times \mathbb{Z}_2)$. Then, by an argument similar to the proof of Lemma 3.1, $\langle z \rangle \subset U$ and $\overline{R}$ is an $(8, 2, 8, 4)$ RDS in $\overline{G}$ relative to $\overline{U}$. By Theorem 4.4 of [9], $\overline{U} = \langle x^4 \rangle$. Hence $U = \langle x^4 \rangle$.

Set $H = \langle x^2 \rangle (= Z(G))$ and $R = A + Bx + Cy + Dxy$, where $A, B, C, D \subset H$. Then A, B, C, D are sets of coset representatives of $H/\langle z \rangle$. Since $RR^{-1} = 8 + 2(G - U) = 8 + 2(H - U) + 2Hx + 2Hy + 2Hxy$, we have $2Hx = A(Bx)^{-1} + (Bx)A^{-1} + (Cy)(Dxy)^{-1} + (Dxy)(Cy)^{-1}$. Hence

$$AB^{-1}x^{-2} + A^{-1}B + CD^{-1}x^{-2} + C^{-1}D = 2H. \qquad (1)$$

Set $A = x^{4a} + x^{4b+2}$, $B = x^{4c} + x^{4d+2}$, $C = x^{4e} + x^{4f+2}$ and $D = x^{4g} + x^{4h+2}$. By (1), we have $2(x^2 + x^6 + x^{10} + x^{14}) = x^{4a-4c-2} + x^{4b-4d-2} + x^{-4a+4d+2} + x^{-4b-2+4c} + x^{4e-4g-2} + x^{4f-4h-2} + x^{-4e+4h+2} + x^{-4f-2+4g}$. Thus $\varepsilon(2(x^2 + x^6 + x^{10} + x^{14})) \equiv -8 \pmod{16}$ (see Definition 2.5). Therefore $0 \equiv 8 \pmod{16}$, a contradiction.

In section 4, we are going to settle case (ii) of Lemma 3.1 and in section 5, we show the existence of a (p^2, p, p^2, p) RDS in $M_3(p)$, $p > 2$.

4 On $(p^2, p^2, p^2, 1)$ RDS in $M_4(p)$

In this section, we assume that the RDS R in $G = M_n(p)$ has parameters $(p^a, p^b, p^a, p^{a-b}) = (p^2, p^2, p^2, 1)$. We recall that $M_4(p) = \langle x, y \mid x^{p^3} = y^p = 1,\ y^{-1}xy = xz \rangle$ where $z = x^{p^2}$ and $p \geq 2$. There are exactly $p+1$ normal subgroups of G of order p^2 : $\langle x^p \rangle$, $\langle z, y \rangle$, $\langle x^i y \rangle (1 \leq i \leq p-1)$. By Lemma 2.4(iv), $\theta_{i,0,0}(x^p y) = x^{ip} y$. Hence, it suffices to consider only the following three cases:

(i) $U = \langle x^p \rangle \simeq \mathbb{Z}_{p^2}$,

(ii) $U = \langle z, y \rangle \simeq \mathbb{Z}_p \times \mathbb{Z}_p$,

(iii) $U = \langle x^p y \rangle \simeq \mathbb{Z}_{p^2}$.

We define subsets A_i $(0 \leq i \leq p-1)$ by $A_i = Ry^{-i} \cap \langle x \rangle$. Then $R = A_0 + A_1 y + \cdots + A_{p-1} y^{p-1}$.

Lemma 4.1 *Set* $RR^{-1} = B_0 + B_1 y + \cdots + B_{p-1} y^{p-1}$, *where* $B_0, B_1, \cdots, B_{p-1} \in \mathbb{Z}[\langle x \rangle]$. *Then*

$$B_0 = \sum_{0 \leq i \leq p-1} A_i A_i^{-1} = p^2 + \langle x^p \rangle x + \cdots + \langle x^p \rangle x^{p-1}.$$

Proof. As $R = A_0 + A_1 y + \cdots + A_{p-1} y^{p-1}$, we have

$$RR^{-1} = \sum_{0 \leq i,j \leq p-1} (A_i y^i)(A_j y^j)^{-1} = \sum_{0 \leq i,j \leq p-1} A_i y^{i-j} A_j^{-1}$$
$$= \sum_{0 \leq i,j \leq p-1} A_i A_j^{-(1-(i-j))p^2} y^{i-j} = p^2 + (G - U) \text{ by Lemma 2.4.}$$

In particular,

$$B_0 = \sum_{0 \leq i \leq p-1} A_i A_i^{-1} = p^2 + \langle x^p \rangle x + \cdots + \langle x^p \rangle x^{p-1}.$$

Lemma 4.2 *Case (i) does not occur.*

Proof. Set $S = RR^{-1} \cap \langle x^p \rangle x$. By Lemma 4.1, $S = \langle x^p \rangle x$. Since R is a set of coset representatives of G/U and $U = \langle x^p \rangle \geq \langle z \rangle$, it follows that $A_i = x^{pa_{i,0}} + x^{pa_{i,1}+1} + x^{pa_{i,2}+2} + \cdots + x^{pa_{i,p-1}+p-1}$ $(a_{ij} \in \mathbb{Z})$ for each $i \in \{0, 1, \cdots, p-1\}$. Hence

$$\varepsilon(\langle x^p \rangle x) = 1 + (1+p) + (1+2p) + \cdots + (1+(p^2-1)p)$$
$$\equiv (p(a_{i,0} - a_{i,p-1}) - (p-1)) + (p(a_{i,1} - a_{i,0}) + 1) + (p(a_{i,2} - a_{i,1}) + 1)$$
$$+ \cdots + (p(a_{i,p-1} - a_{i,p-2}) + 1) \pmod{}p^3 \text{ (see Definition 2.5).}$$

Thus $p^2 \equiv 0 \pmod{p^3}$, a contradiction.

Lemma 4.3 *Assume* $p > 2$. *Then, in cases (ii) and (iii) we may assume the following :*

$$A_0 = \sum_{0 \leq j \leq p-1} x^{jp + a_j p^2} + \sum_{1 \leq j \leq p-1} x^{m_j + b_j p^2},$$

$$A_i = \sum_{1 \le j \le p-1} x^{m_j + c_{i,j}p} \quad (1 \le i \le p-1)$$

where $a_j, b_j, c_{ij}, m_j \in \mathbb{Z}$ *and* $m_j \equiv j \pmod p$ *for any* i, j.

Proof. Set $\overline{G} = G/\langle z \rangle \simeq \mathbb{Z}_{p^2} \times Z_p$. Then $\overline{R}$ is a (p^2, p, p^2, p) RDS in $\overline{G}$ relative to $\overline{U} \simeq \mathbb{Z}_p$. Here $\overline{U} = \langle \overline{y} \rangle$ or $\langle \overline{x^p y} \rangle$. By Theorem 3.2 of [8], a translate of R has the following property :

$$\overline{R} = \langle \overline{x^p} \rangle + \overline{g_1}\overline{H_1} + \sum_{2 \le i \le p-1} \overline{g_i}\langle \overline{x^p y^i} \rangle, \quad \text{where}$$

$$\overline{H_1} = \begin{cases} \langle \overline{x^p y} \rangle & \text{if } \overline{U} = \langle \overline{y} \rangle \\ \langle \overline{y} \rangle & \text{if } \overline{U} = \langle \overline{x^p y} \rangle \end{cases}$$

and

$$g_i = x^{n_i} \ (1 \le i \le p-1) \text{ and } \{n_1, \cdots, n_{p-1}\} = \{1, \cdots, p-1\} \pmod p$$

Hence, by Lemma 2.4(iii),

$$R = \sum_{0 \le j \le p-1} x^{jp + a_j p^2} + \sum_{1 \le i \le p-1} \sum_{0 \le j \le p-1} x^{n_i + jp + e_{i,j}p^2} y^{ij} \quad \text{or}$$

$$R = \sum_{0 \le j \le p-1} x^{jp + a_j p^2} + \sum_{0 \le j \le p-1} x^{n_1 + e_{1,j}p^2} y^j + \sum_{2 \le i \le p-1} \sum_{0 \le j \le p-1} x^{n_i + jp + e_{i,j}p^2} y^{ij}$$

depending on whether $\overline{U} = \langle \overline{y} \rangle$ or $\overline{U} = \langle \overline{x^p y} \rangle$, respectively. Here $a_j, e_{ij} \in \mathbb{Z}$. Set

$$w_1 = \begin{cases} n_1 & \text{if } \overline{U} = \langle \overline{y} \rangle \\ n_1 - p & \text{if } \overline{U} = \langle \overline{x^p y} \rangle \end{cases} \quad \text{and } w_i = n_i \ (2 \le i \le p-1).$$

Then

$$R = \sum_{0 \le j \le p-1} x^{jp + a_j p^2} + \sum_{1 \le i \le p-1} \sum_{0 \le j \le p-1} x^{w_i + jp + e_{i,j}p^2} y^{ij}.$$

Hence

$$A_0 = \sum_{0 \le j \le p-1} x^{jp + a_j p^2} + \sum_{1 \le i \le p-1} x^{w_i + e_{i,0}p^2}. \tag{2}$$

We now consider $A_t y^t$ for $t \in \{1, 2, \cdots, p-1\}$. Let $s \in \{1, \cdots, p-1\}$. Then there is a unique solution (i, j) of the following simultaneous equations :

$$\begin{cases} ij \equiv t & \pmod p \\ w_i + jp + e_{i,j}p^2 \equiv s & \pmod p \end{cases}$$

Thus for any $t \in \{1, 2, \cdots, p-1\}$, we have

$$A_t = \sum_{1 \le s \le p-1} x^{s + c_{t,s}p} \quad (1 \le t \le p-1) \tag{3}$$

for some $c_{t,s} \in \mathbb{Z}$. By (2) and (3), we have the lemma.

Lemma 4.4 *Set* $S = RR^{-1} \cap \langle x^p \rangle x$ *and assume* $p > 2$. *Then* $\varepsilon(S) \equiv p^2 \pmod{p^3}$ *in cases (ii) and (iii).*

Proof. As $RR^{-1} = p^2 + G - U$ and $U \cap \langle x^p \rangle x = \phi$, we have $S = \sum_{0 \le i \le p^2-1} x^{1+ip}$, hence $\varepsilon(S) \equiv 1 \cdot p^2 + p(0 + 1 + \cdots + (p^2 - 1)) \equiv p^2 \pmod{p^3}$.

Lemma 4.5 *Case (ii) and (iii) do not occur if* $p > 2$.

Proof. By Lemma 4.3,

$$A_0 = \sum_{0 \le j \le p-1} x^{u_j} + \sum_{1 \le j \le p-1} x^{v_j} \quad \text{and}$$

$$A_i = \sum_{1 \le j \le p-1} x^{w_{ij}}$$

for each $i \in \{1, \cdots, p-1\}$ where $u_j \equiv 0 \pmod{p}$, $v_j \equiv j \pmod{p}$, and $w_{ij} \equiv j \pmod{p}$. Set $S_i = A_i A_i^{-1} \cap \langle x^p \rangle x$ for each $i \in \{0, 1, \cdots, p-1\}$. Then by Lemma 4.1, $S = S_0 + S_1 + \cdots + S_{p-1}$, where

$$S_0 = x^{v_1 - v_0} + x^{v_2 - v_1} + \cdots + x^{v_0 - v_{p-1}} + \sum_{0 \le i \le p-1} x^{v_i - u_i} \quad \text{and}$$

$$S_i = x^{w_{i,2} - w_{i,1}} + x^{w_{i,3} - w_{i,2}} + \cdots + x^{w_{i,p-1} - w_{i,p-2}} \ (1 \le i \le p-1).$$

Therefore,

$$\varepsilon(S) = pv_1 - (u_0 + \cdots + u_{p-1}) + \sum_{1 \le i \le p-1} (w_{i,p-1} - w_{i,1})$$

$$\equiv (p-1)(p-2) \equiv 2 \pmod{p}.$$

On the other hand, $\varepsilon(S) \equiv 0 \pmod{p}$ by Lemma 4.4. As $p > 2$, this is a contradiction. Thus we have the lemma.

We remark that the only case excluded by Lemma 4.5 is when $p = 2$. In this case, K. Akiyama has found out that $R_0 = \{1, x^2y, x^3y, x^5y\}$ is a (4,4,4,1) RDS in $M_4(2)$ relative to $U = \langle z, y \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. Any (4,4,4,1)RDS in $M_4(2)$ corresponds to a projective plane of order 4.

Lemma 4.6 *Assume* $p = 2$. *Then* $U = \langle x^4, y \rangle$ *and there exist* $\theta \in Aut(M_4(2))$ *and* $g \in M_4(2)$ *such that* $\theta(Rg) = \{1, x, x^3, x^2y\}$.

Proof. We first note that $G \setminus U$ contains no involution, otherwise, $d_1 d_2^{-1}$ is an involution for some $d_1, d_2 \in R$ and so $d_1 d_2^{-1} = d_2 d_1^{-1}$, contrary to $\lambda = 1$. In particular $U = \langle x^4, y \rangle$. Clearly $G = U \cup Ux \cup Ux^2 \cup Ux^3$ is a coset decomposition where:

$$U = \{1, x^4, y, x^4y\}, \quad Ux = \{x, x^5, xy, x^5y\},$$

$$Ux^2 = \{x^2, x^6, x^2y, x^6y\}, \quad Ux^3 = \{x^3, x^7, x^3y, x^7y\}.$$

We may assume that $1 \in R$. By Lemma 2.4(iv), $Ux \subset \{\theta(x) \mid \theta \in Aut(M_4(2))\}$. Hence we may assume that

$x \in R$ and so $\{1, x\} \subset R$. As $x^2x^{-1} = x1^{-1} (= x \notin U)$, $x^2 \notin R$. Since $\theta_{001}(x) = x$ and $\theta_{001}(x^2y) = x^6y$, we may assume either $\{1, x, x^6\} \subset R$ or $\{1, x, x^2y\} \subset R$.

Assume $\{1, x, x^6\} \subset R$. As $x^31^{-1} = xx^{-6} (= x^3 \notin U)$ and $x^71^{-1} = 1x^{-1} (= x^7 \notin U)$, we have $x^3, x^7 \notin R$. Since $\theta_{001}(x) = x$ and $\theta_{001}(x^3y) = x^7y$, we may assume that $R = \{1, x, x^6, x^3y\}$. Moreover $\theta_{700}(\{1, x, x^6, x^3y\}x^7) = \{1, x, x^3, x^2y\}$.

Assume $\{1, x, x^2y\} \subset R$. As $x^71^{-1} = 1x^{-1} (= x^7 \notin U)$, $x1^{-1} = x^3y(x^2y)^{-1} (= x \notin U)$ and $x^7y1^{-1} = x(x^2y)^{-1} (= x^7y \notin U)$, we have $x^7, x^3y, x^7y \notin R$.

Hence $R = \{1, x, x^3, x^2y\}$. We can easily check that R is actually a (4,4,4,1) RDS. Therefore the lemma holds.

By Lemmas 3.1, 3.2, 4.2, 4.5 and 4.6, we obtain the following:

Proposition 4.7 *Let R be a non-trivial semi-regular RDS in the modular p-group $M_n(p)$ relative to a normal subgroup U. Then either $U \simeq \mathbb{Z}_p$ or $(n, p) = (4, 2)$ and $U \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.*

5 Non-Existence when $G \simeq M_n(2)$ or SD_{2^n}

In this section, we show the nonexistence of $(2^{n-1}, 2, 2^{n-1}, 2^{n-1})$ RDS in $M_n(2)$ and SD_{2^n}.

Lemma 5.1 *Let $H = \langle w \rangle$ be a cyclic 2-group of order at least 4 and z the unique involution in H. Let A and B be sets of coset representatives of $H/\langle z \rangle$. Then $AB^{-1} \neq A^{-1}Bw^c$ for any odd integer c.*

Proof. Let 2^{m+1} be the order of w. Since A and B are sets of coset representatives of $H/\langle z \rangle$ ($z = w^{2^m}$), we can put

$$A = \sum_{0 \le i \le 2^m - 1} w^{2^m a_i + i}, \quad \text{and} \quad B = \sum_{0 \le i \le 2^m - 1} w^{2^m b_i + i},$$

for suitable $a_i, b_j \in \{0, 1\}$. We also set

$$AB^{-1} = \sum_{0 \le i \le 2^{m+1} - 1} c_i w^i.$$

As $z = w^{2^m}$ and B^{-1} is a set of cosets representatives of $H/\langle z \rangle$, we have $AB^{-1}(1 + w^{2^m}) = AH = 2^m H$. Hence

$$c_i + c_{2^m + i} = 2^m \quad (0 \le i \le 2^m - 1). \tag{4}$$

Let S be the sum of exponents of the terms 1 or w^{2^m} in AB^{-1} and let T be the sum of exponents of the terms w or w^{2^m+1} in AB^{-1}. Then

$$S = \sum_{0 \le i \le 2^m - 1} (2^m a_i - 2^m b_i) = \sum_{0 \le i \le 2^m - 1} 2^m a_i - \sum_{0 \le i \le 2^m - 1} 2^m b_i$$

and

$$T = 2^m a_0 - (2^m b_{2^m - 1} + 2^m - 1) + \sum_{1 \le i \le 2^m - 1} (2^m a_i - 2^m b_{i-1} + 1)$$

$$= \sum_{0 \le i \le 2^m - 1} 2^m a_i - \sum_{0 \le i \le 2^m - 1} 2^m b_i$$

Thus $S = T$.

First assume that

$$AB^{-1} = A^{-1}Bw. \tag{5}$$

Since

$$A^{-1}Bw = \sum_{0 \le i \le 2^{m+1}-1} c_i w^{2^{m+1}+1-i} = c_1 + c_0 w + \sum_{2 \le j \le 2^{m+1}-1} c_{2^{m+1}+1-j} w^j,$$

it follows that

$$c_0 = c_1, \quad c_i = c_{2^{m+1}+1-i} \ \ (2 \le i \le 2^{m+1} - 1). \tag{6}$$

On the other hand $S = 0 \cdot c_0 + 2^m c_{2^m}$ and $T = 1 \cdot c_1 + (2^m + 1)c_{2^m+1} \equiv c_0 + (2^m + 1)c_{2^m} \pmod{2^{m+1}}$ by (6). As $S = T$, we have $c_0 + c_{2^m} \equiv 0 \pmod{2^{m+1}}$, contrar y to (4).

We now assume that $AB^{-1} = A^{-1}Bw^c$ for some odd integer c. We consider an automorphism σ of H given by $\sigma(x) = x^d$, where d is an integer such that $cd \equiv 1 \pmod{2^{m+1}}$. We note that $\sigma(A)$ and $\sigma(B)$ are also sets of coset representatives of of $H/\langle z \rangle$ and that $\sigma(A)\sigma(B)^{-1} = \sigma(A)^{-1}\sigma(B)\sigma(w^c) = \sigma(A)^{-1}\sigma(B)w$. The last equation is similar to (5) and so this is a contradiction. Therefore the lemma holds.

Lemma 5.2 *Let R be a $(2^{n-1}, 2, 2^{n-1}, 2^{n-2})$ RDS in $G \simeq M_n(2)$ or SD_{2^n} relative to U. Set $G = \langle x, y \mid x^{2^{n-1}} = y^2 = 1,\ y^{-1}xy = x^{2^{n-2}\pm 1} \rangle$ so that $R = A_0 + A_1 x + B_0 y + B_1 xy$, where $A_0, A_1, B_0, B_1 \subset \langle x^2 \rangle$.*

Then

(i) A_0, A_1, B_0, B_1 are sets of coset representatives of $\langle x^2 \rangle / \langle z \rangle$, where z is the unique involution of $\langle x^2 \rangle$.

(ii) We have $B_0 B_1^{-1} = B_0^{-1} B_1 x^2 z$.

Proof. Set $H = \langle x^2 \rangle (\simeq \mathbb{Z}_{2^{n-2}})$. Since $U = \langle z \rangle$, (i) is obvious. We note that y centralizes or inverts H depending on whether $G \simeq M_n(2)$ or $G \simeq SD_{2^n}$.

We first assume that $G \simeq M_n(2)$. Then $RR^{-1} = A_0A_0^{-1} + A_1A_1^{-1} + B_0B_0^{-1} + B_1B_1^{-1} + (A_0A_1^{-1}x^{-2} + A_0^{-1}A_1 + B_0B_1^{-1}x^{-2} + B_0^{-1}B_1)x + (A_0B_0^{-1} + A_0^{-1}B_0 + A_1B_1^{-1}z + A_1^{-1}B_1z)y + (A_1B_0^{-1} + A_0^{-1}B_1 + A_1^{-1}B_0x^{-2}z + A_0B_1^{-1}x^{-2}z)xy$. On the other hand, $RR^{-1} = 2^{n-1} + 2^{n-2}((H - U) + Hx + Hy + Hxy)$. Hence $(A_0A_1^{-1}x^{-2} + A_0^{-1}A_1 + B_0B_1^{-1}x^{-2} + B_0^{-1}B_1)x = 2^{n-2}Hx$. ¿From this we have

$$A_0A_1^{-1} + A_0^{-1}A_1x^2 + B_0B_1^{-1} + B_0^{-1}B_1x^2 = 2^{n-2}H. \tag{7}$$

As $R^{-1}R = RR^{-1}$ by Proposition 2.8 of [7], similarly we have

$$A_0A_1^{-1} + A_0^{-1}A_1x^2 + B_0B_1^{-1}z + B_0^{-1}B_1x^2z = 2^{n-2}H. \tag{8}$$

By (7) and (8), we have $B_0B_1^{-1} + B_0^{-1}B_1x^2 = (B_0B_1^{-1} + B_0^{-1}B_1x^2)z$. On the other hand, $(B_0B_1^{-1} + B_0^{-1}B_1x^2) + (B_0B_1^{-1} + B_0^{-1}B_1x^2)z = (B_0B_1^{-1} + B_0^{-1}B_1x^2)U = 2^{n-2}H$ since B_0 and B_1 are sets of cosets representatives of H/U.

Thus we have $B_0B_1^{-1} + B_0^{-1}B_1x^2 = 2^{n-3}H$. Moreover $B_0B_1^{-1} + B_0B_1^{-1}z = B_0B_1^{-1}U = 2^{n-3}H$. It follows that $B_0^{-1}B_1x^2 = B_0B_1^{-1}z$. Therefore we have $B_0B_1^{-1} = B_0^{-1}B_1x^2z$.

We now assume that $G \simeq SD_{2^n}$. By a similar argument as in the last paragraph, we have

$$A_0A_1^{-1} + A_0^{-1}A_1x^2 + B_0B_1^{-1} + B_0^{-1}B_1x^2 = 2^{n-2}H$$

and

$$A_0A_1^{-1} + A_0^{-1}A_1x^2 + B_0B_1^{-1}z + B_0^{-1}B_1x^2z = 2^{n-2}H.$$

It follows that $B_0B_1^{-1} + B_0^{-1}B_1x^2 = (B_0B_1^{-1} + B_0^{-1}B_1 + x^2)z$. By a similar argument as in the last paragraph we have $B_0B_1^{-1} = B_0^{-1}B_1x^2z$. Therefore the lemma holds.

Proposition 5.3 *There is no* $(2^{n-1}, 2, 2^{n-1}, 2^{n-2})$ *RDS in* $M_n(2)$ *or* SD_{2^n}.

Proof. Let notations be as in Lemma 5.2 and suppose that the proposition is false. Set $w = x^2$, $H = \langle w \rangle$, $A = B_0$ and $B = B_1$. Then, as $n \geq 4$, $|H| \geq 4$. By Lemma 5.2(ii), $AB^{-1} = A^{-1}Bw^{1+2^{n-3}}$, contrary to Lemma 5.1.

By Propositions 4.7 and 5.3 and the results of section 3 in [4], we have

Theorem 5.4 *Let G be a non-abelian p-group with a maximal cyclic subgroup. If G contains a non-trivial semi-regular RDS relative to a normal subgroup U, then one of the following holds :*

(i) $G \simeq Q_{2^n}$ *and* $U \simeq \mathbb{Z}_2$,

(ii) $G \simeq M_n(p)$ *and* $U \simeq \mathbb{Z}_p$ *with p an odd prime,*

(iii) $G \simeq M_4(2)$ *and* $U \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

6 Existence of a (p^2, p, p^2, p) RDS in $M_3(p)$

In this section, we consider case (iii) of Lemma 3.1, that is, when the RDS R in G has its forbidden subgroup $U \simeq \mathbb{Z}_p$. In particular, we take $n = 3$ and $p > 2$. Then we can construct a (p^2, p, p^2, p) RDS in $M_3(p)$

for any odd prime p. Set $R_p = \{x^{a+abp}y^b \mid a, b \in I\}$ where $I = \{0, 1, \cdots, p-1\}$. Take note that we compute the elements of I modulo p.

Proposition 6.1 *Let p be an odd prime. Then R_p is a (p^2, p, p^2, p) RDS in $M_3(p)$.*

Proof. Set $R = R_p$ and let w_1, w_2 be elements of R. Then $w_1 = x^{a+abp}y^b$, $w_2 = x^{c+cdp}y^d$ for suitable $a, b, c, d \in I$. Let $r, s, t \in I$ and assume that $(r, s) \neq (0, 0)$. Set $S_{r,s,t} = \{(w_1, w_2) \in R \times R \mid w_1w_2^{-1} = x^{r+tp}y^s\}$.
As $w_1w_2^{-1} = x^{a-c+(ab+bc-2cd)p}y^{b-d}$ by Lemma 2.4, we have

$$a - c + (b(a+c) - 2cd)p \equiv r + tp \pmod{p^2} \tag{9}$$

and

$$b - d \equiv s \pmod{p}. \tag{10}$$

By (10), $b \equiv d + s \pmod{p}$.

First assume that $r = 0$. Then $s \not\equiv 0 \pmod{p}$ by assumption. By (9), $a = c$ and so we have $2sa \equiv t \pmod{p}$. Hence we have $c = a \equiv t(2s)^{-1} \pmod{p}$ and so there exists a unique $i_0 \in I$ such that $c = a = i_0$. It follows that $(a, b, c, d) = (i_0, d + s, i_0, d)$, where $d \in I$ is arbitrary. Hence $|S_{r,s,t}| = p$ in this case.

We now assume that $r \neq 0$. Then we have to consider following two cases:
(1) $a > c$, $a - c = r$, $(a + c)b - 2c \cdot d \equiv t \pmod{p}$, $b - d \equiv s \pmod{p}$
(2) $a < c$, $p + a - c = r$, $(a + c)b - 2c \cdot d \equiv t + 1 \pmod{p}$, $b - d \equiv s \pmod{p}$.

In (1), $(a, c) \in \Delta = \{(r, 0), (r + 1, 1), \cdots, (p - 1, p - r - 1)\}$. Moreover, as $\begin{vmatrix} a + c & -2c \\ 1 & -1 \end{vmatrix} \equiv c - a \not\equiv 0 \pmod{p}$, $(b, d) \in I \times I$ is uniquely determined for each $(a, c) \in \Delta$. Hence there are exactly $p - r$ (a, b, c, d)'s in this case. In (2), $(a, c) \in \Gamma = \{(0, p - r), (1, p - r + 1), \cdots, (r - 1, p - 1)\}$. As $\begin{vmatrix} a + c & -2c \\ 1 & -1 \end{vmatrix} \equiv c - a \not\equiv 0 \pmod{p}$, (b, d) is also uniquely determined for each $(a, c) \in \Gamma$. Hence there are exactly r (a, b, c, d)'s in this case. Thus we have $|S_{r,s,t}| = |\Delta| + |\Gamma| = (p - r) + r = p$ when $r \neq 0$. Therefore $|S_{r,s,t}| = p$ for any r, s, t such that $(r, s) \neq (0, 0)$. It follows that R is a (p^2, p, p^2, p) RDS in $M_3(p)$ for any prime $p > 2$.

As a consequence of Proposition 6.1, we can construct a semi-regular RDS in any extra-special p-group to be shown in the following corollary.

Corollary 6.2 *Let P be an extra-special p-group of order p^{2m+1} with $m \geq 1$. Then there exists a $(p^{2m}, p, p^{2m}, p^{2m-1})$ RDS in P relative to $[P, P] (\simeq \mathbb{Z}_p)$ unless $P \simeq D_8$.*

Proof. By Proposition 3 of [6], it suffices to consider the case that p is an odd prime. Then, by Theorem 5.5.2 of [5], P is isomorphic to one of the central product M^r or $M^{r-1}N$, where

$M = M(p) = \langle x, y, z \mid x^p = y^p = z^p = 1, [x, z] = [y, z] = 1, [x, y] = z \rangle$,
$N = M_3(p) = \langle x, y \mid x^{p^2} = y^p = 1, y^{-1}xy = x^{1+p^2} \rangle \quad (p > 2)$.

By Result 2.3 and Proposition 6.1, it suffices to consider the cases when P is isomorphic to M.

Assume $P \simeq M$. Then there exist normal subgroups A and B of P such that $A \simeq B \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ and $P = AB$. Since a noncyclic abelian group of order p^2 has a $(p, p, p, 1)$ RDS for any odd prime p (see [11]), P also has a (p^2, p, p^2, p) RDS by Result 2.3. Thus the corollary holds.

Example 6.3 If $G \cong M(p)^r = \langle x_1, y_1, \cdots, x_r, y_r, z \rangle$, then

$$R = \{x_1^{i_1}, y_1^{j_1}, x_2^{i_2}, y_2^{j_2}, \cdots, x_r^{i_r}, y_r^{j_r}, z^f \mid i_k, j_k \in GF(p), 1 \leq k \leq r\},$$

is a $(p^{2r}, p, p^{2r}, p^{2r-1})$ RDS relative to $Z(G) = \langle z \rangle$ where $f = \sum_{k=1}^{r} (i_k^2 + j_k^2)$.

Example 6.4 If $G \cong M_3(p)M(p)^{r-1} = \langle x_1, y_1, \ldots, x_r, y_r, z \rangle$, $[x_i, y_i] = z$, $2 \leq i \leq r$ then

$$R = \left(\sum_{i=0}^{p-1} \sum_{j=0}^{p-1} x_1^{i+pij} y_1^j \right) \left(\sum_{i_k j_k \in GF(p), 2 \leq k \leq r} x_2^{i_2} y_2^{j_2} \ldots x_r^{i_r} y_r^{j_r} z^f \right)$$

is a $(p^{2r}, p, p^{2r}, p^{2r-1})$ RDS relative to $Z(G) = \langle x_1^p \rangle = \langle z \rangle$ where $f = \sum_{k=2}^{r} (i_k^2 + j_k^2)$.

In this article, we have shown that if an RDS R is contained in $G = M_n(p)$ of order p^n relative to a normal subgroup U then its parameters are given by $(p^{n-1}, p, p^{n-1}, p^{n-2})$ and $U \simeq \mathbb{Z}_p \subseteq Z(G)$ except when $G = M_4(2)$ and $U \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. In addition, if $p > 2$ and $n = 3$, we have shown the existence of an RDS in G and if $p = 2$ and $n \geq 4$, we have shown the non-existence. At this point, we pose the following:

Problem: Does there exist a $(p^{n-1}, p, p^{n-1}, p^{n-2})$ RDS in $G = M_n(p)$ relative to $U \simeq \mathbb{Z}_p$ when $p > 2$ and $n \geq 4$?

We note, however, that when $G \simeq M_4(3)$, we have checked the non-existence of such an RDS in G by conducting a computer search.

Dominic Elvira
Department of Mathematics, Graduate School of Science and Technology
Kumamoto University
Kurokami, Kumamoto, Japan
dtelvira@math.sci.kumamoto-u.ac.jp

Yutaka Hiramine
Department of Mathematics, Faculty of Education
Kumamoto University
Kurokami, Kumamoto, Japan
hiramine@gpo.kumamoto-u.ac.jp

References

[1] J.A. Davis, *A Note on Products of Relative Difference Sets* , Designs, Codes and Cryptography 1 (1991), 117-119.

[2] J.A. Davis and J. Jedwab, *A New Family of Relative Difference Sets in 2-Groups*, Designs, Codes and Cryptography, 17, (1998), 305-3 12.

[3] J.E.H. Elliot and A.T. Butson, *Relative Difference Sets*, Illinois J. Math. 10 (1966), 517 - 531.

[4] D.T. Elvira and Y. Hiramine, *On Non-Abelian Semi-Regular Relative Difference Sets*, to appear.

[5] D. Gorenstein, *Finite Groups* , Harper and Row, New York, 1968.

[6] N.Ito, *Remarks on Hadamard Groups* , Kyushu. J. Math. 50 (1996), 83 - 91.

[7] D. Jungnickel, *On automorphism groups of divisible designs* , Can. J. Math. 34 (1982), 257 - 297.

[8] S.L. Ma and A. Pott, *Relative Difference Sets, Planar Functions and Generalized Hadamard Matrices*, J. Algebra 175 (1995), 505-525.

[9] S.L. Ma and B. Schmidt, *On* (p^a, p, p^a, p^{a-1})*-Relative Difference Sets*, Designs, Codes and Cryptography, 6, (1995), 57-71.

[10] A. Pott, *On the structure of abelian groups admitting divisible difference sets*, J. Comb. Th. (A) 65 (1994), 202-213.

[11] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin (1995).

[12] B. Schmidt, *On* (p^a, p^b, p^a, p^{a-b}) *Relative Difference Sets*, J. Algebraic Combin. 6 (1997), 279-297.

[13] B. Schmidt, *Williamson Matrices and a Conjecture of Ito's*, Designs, Codes and Cryptography, 17, (1999), 61-68.

A general survey of relative difference sets

Nobuo NAKAGAWA
(Kinki University)

1 Introduction

We will mention the definition of relative difference sets in finite groups and a geometrical meaning of relative difference sets in this section.

Definition 1.1 .
Let G be a group of order mn and N be a normal subgroup of order n. Then a k-subset R of the group G is named to be a (m, n, k, λ) relative difference set in G relative to N if and only if

$$RR^{-1} = k \cdot 1 + \lambda(G - N)$$

in the group ring $\mathbb{Z}|G|$, namely for every element $g \in G$, the equation

$$g = xy^{-1}$$

has exactly λ solusions (x, y) with $x, y \in R$ and for every nonidentity element $h \in N$ the equation above has no solusion (x, y) with $x, y \in R$.

We remark that R is a ordinary difference set in G if $N = \{1\}$.

From a relative difference set in G a divisible design admitting G is constructed.
We define a divisible design as the following.

Definition 1.2 .
Let $\mathbf{P}$ and $\mathbf{L}$ be finite sets and I be a incident relation between $\mathbf{P}$ and $\mathbf{L}$. Set $(\ell) = \{ A \in \mathbf{P} \mid AI\ell \}$ for $\ell \in \mathbf{L}$. We call ℓ and ℓ' are paralell if $(\ell) \cap (\ell') = \emptyset$. Then $(\mathbf{P}, \mathbf{L}; I)$ is named a divisible design with (m, n, k, λ) if and only if
(1) $|\mathbf{P}| = |\mathbf{L}| = mn$,
(2) $|(\ell)| = k$ for all $\ell \in \mathbf{L}$,
(3) $\mathbf{L} = \mathbf{L}_1 \cup \mathbf{L}_2 \cup \cdots \cup \mathbf{L}_m$ where $\mathbf{L}_i$ is a parallel class of lines for $1 \leq i \leq m$,
(4) $|\mathbf{L}_i| = n$ for $1 \leq i \leq m$,
(5) $|\ell_1 \cap \ell_2| = 0$ if $\ell_1, \ell_2 \in \mathbf{L}_i$ for some i and $|\ell_1 \cap \ell_2| = \lambda$ if ℓ_1 and ℓ_2 are not paralell.

Theorem 1.1 .
Let $\mathcal{D} = (\mathbf{P}, \mathbf{L})$ be a divisible design with parameters (m, n, k, λ) where $\mathbf{L} = \mathbf{L}_1 \cup \mathbf{L}_2 \cup \cdots \cup \mathbf{L}_m$. Suppose that a subgroup G of $Aut(\mathcal{D})$ acts on $\mathbf{P}$ and $\mathbf{L}$ regularly and the global stabilizar of $\mathbf{L}_i$ coincide with a central subgroup N for each i such that $1 \leq i \leq m$. Then for each $P \in \mathbf{P}$ and each $\ell \in \mathbf{L}$, $R = \{ x \in G \mid P^x \in \ell \}$ is a (m, n, k, λ)-relative difference set in G relative to N.
Conversely from a (m, n, k, λ)-relative difference set R in G relative to N a divisible design with same parameters admitting G as a regular autumorphism group on $\mathbf{P}$ and $\mathbf{L}$ is constructed.

The following lemma is fundamental to be constructed a new one from a relative difference set.
Lemma
Let R be a relative (m, n, k, λ)-difference set in G relative to N. If U is a normal subgroup of G contained in N, then there exists an $(m, \frac{n}{u}, k, \lambda u)$-difference set in G/U relative to N/U. In particular G/N contains an (m, k, λ)-difference set.

2 $(4m, 2, 4m, 2m)$-relative difference sets

A $(4m, 2, 4m, 2m)$-divisible design is a divisible Hadamard design introduced by N.Ito. Let $\mathcal{D} = (\mathrm{P}, \mathrm{L})$ be a $(4m, 2, 4m, 2m)$-divisible design and set $\mathrm{L}_1 = \{\ell_1, \ell_1'\}, \cdots, \mathrm{L}_{4m} = \{\ell_{2m}, \ell_{2m}'\}$ where $\ell_1 = \{\ a_1, a_2, \cdots, a_{4m}\ \}$. We put the matrix A as

$$A = (a_{i,j})$$

where $a_{i,j} = 1$ if $a_i \in (\ell_j)$ and $a_{i,j} = -1$ if otherwise. Then A is a Hadamard matrix.

If there exist a $(4m, 2, 4m, 2m)$-r.d.set in G relative to $N =< e^* >$ where $e^* \in G$ and $|e^*| = 2$, then G is called a Hadamard group with respect to e^*.

Theorem 2.1 (N.Ito) .
(1) $\mathrm{Z}_4 \times \mathrm{Z}_2$, $\mathrm{Z}_8 \times \mathrm{Z}_2$ *and* $\mathrm{Z}_4 \times \mathrm{Z}_4$ *are Hadamard groups.*
(2) Extra special 2-groups are Hadamard groups.
(3) $SL(2,3)$, *the Sylow* $\{2,3\}$*-subgroup of* $SL(2,7)$ *and* $SL(2,5)$ *are Hadamard groups.*
(4) Let q *be a prime power. There exist a Hadamard group of order* $4(q+1)$ *if* $q \equiv 1 (mod\ 4)$.
(5) Let q *be a prime power. There exist a Hadamard group of order* $2(q+1)$ *if* $q \equiv 3 (mod\ 4)$.

(Ito 's Conjecture)
A group

$$\mathrm{Q}_{8m} =< a, b \mid a^{4m} = b^4 = 1,\ a^{2m} = b^2 = z,\ b^{-1}ab = a^{-1} >$$

shoud be a Hadamard group.

It have be proved that Q_{8m} is a Hadamard group for $m \leq 46$.
We would like that Q_{856} ia a Hadamard group. Because a Hadamard group of degree 428 is not known up to the present.

The existence of $(4u^2, 2u^2-u, u^2-u)$-Hadamard difference sets means the existence of $(4u^2, 2, 4u^2, 2u^2)$-relative difference sets. It is known that there exist a $(4u^2, 2u^2-u, u^2-u)$-Hadamard difference sets for $u = 2^{2a}3^{2b}p_1^4p_2^4\cdots p_t^4$, here $p_1, p_2, \cdots, p_t$ are primes.

3 $(m+1, m-1, m, 1)$-relative difference sets and $(m+\sqrt{m}+1, m-\sqrt{m}, m, 1)$-relative difference sets

We will describe relative difference sets in abelian groups from this section.

Various divisible designs are observed in projective planes as substructures of them.

We say that a group acts quasiregularly on a set S if the stabilizers of all elements in S are normal subgroups. It is known that a quasiregular group of a projective plane acts regularly on orbits of maximal size.

Theorem 3.1 (P.Dembowski and F.Piper) .
Let G *be an automorphism group acting quasiregularly on points and lines of a projective plane of order* m, *If* $|G| > \frac{m^3+m+1}{2}$ *then one of the following holds where* t *denotes the number of point orbits(=the number of line orbits) and* $\mathcal{F}$ *denotes the incidence structure consisting of fixed points and fixed lines.*
(1) $|G| = m^2+m+1, t = 1, \mathcal{F} = \emptyset$.
(2) $|G| = m^2, t = 3$, $\mathcal{F}$ *is an incident point-line pair* (P, ℓ).
(3) $|G| = m^2, t = m+2$, $\mathcal{F}$ *is either a line and all its points, or its dual..*
(4) $|G| = m^2-1, t = 3$, $\mathcal{F}$ *is a non-incident point-line pair* (P, ℓ).
(5) $|G| = m^2-\sqrt{m}, t = 2, \mathcal{F} = \emptyset$. *In this case one of the point orbits is precisely the set of points of a Baer subplane.*

(6) $|G| = m^2 - m, t = 5$, $\mathcal{F}$ *consists of 2 points, the line joining them and another line through one of the points.*
(7) $|G| = m^2 - 2m + 1, t = 7$, $\mathcal{F}$ *consists of the vertices and sides of triangle,*
(8) $|G| = (m - \sqrt{m} + 1)^2, t = 2\sqrt{m} + 1, \mathcal{F} = \emptyset$.

The case(1) correponds to the projective plane itself, planes of type (3) are translation planes or dual translation planes. Ganley and McFarland have proved that case (8) cannot occur if $m > 4$. The case (2), (4) and (5) can be described relative difference sets.

The following problem is one of the most striking problem in the relative difference sets concerning Prime Power Conjecture.

(Problem 1.)
If there exist a $(m+1, m-1, m, 1)$, $(m+\sqrt{m}+1, m-\sqrt{m}, m, 1)$ or $(m, m, m, 1)$-relative difference set, then should m be a prime power.

The desarguesian plane of order q where q is a prime power admits a cyclic automorphism group G of order $q^2 - 1$, and there exists a $(q+1, q-1, q, 1)$-relative differece set in G. The following example is this type.

Eample 1.
Let q be a prime power. The set of elements a in $GF(q^2)$ with $a + a^q = 1$(i.e. with trace 1) form a $(q+1, q-1, q, 1)$-cyclic relative difference set in the multiplicative group of the field $GF(q^2)$.

Theorem 3.2 (K.T.Arasu and A.Pott) .
Suppose that there exsits a $(m+1, m-1, m, 1)$*-relative diff. set in a group* G*. Then the Sylow 2-subgroup of* G *is cyclic.*

Theorem 3.3 (K.T.Arasu and A.Pott) .
Suppose that R *is a* $(m+1, m-1, m, 1)$*-relative diff. set in an abelian group* G *relative to* N *and* t *is a divisor of* m*. Then* t *has to satisfy the following conditions:*
(1) The order of t *modulo the exponent of* G/N *is the same as the order modulo the exponent of* G*.*
(2) If $t^f \equiv 1 \ mod \ exp(N)$*, then* $t^f \equiv 1$ *or* $t^f \equiv m \ mod \ exp(G)$*.*
(3) If $t^{2f} \equiv 1 \ mod \ exp(G/N)$*, then* $t^f \equiv 1$ *or* $t^f \equiv m \ mod \ exp(G)$*.*

Theorem 3.4 (K.T.Arasu and D.Jungnickel) .
Suppose that R *is a* $(m+1, m-1, m, 1)$*-relative diff. set in an abelian group* G*. If* $m \equiv 0 \ mod \ 2$*, then* $m = 2, 4$ *or* $m \equiv 0 \ mod \ 8$*. If* $m \equiv 0 \ mod \ 3$*, then* $m = 3$ *or* $m \equiv 0 \ mod \ 9$*.*

Theorem 3.5 (K.T.Arasu and A.Pott) .
Suppose that R *is a* $(m+1, m-1, m, 1)$*-relative diff. set in an abelian group* G*. If* $m \equiv 8 \ mod \ 16$*, then* $m - 1$ *must be a prime power. If* G *is a cyclic group, then* $m - 1$ *must be a prime.*

Theorem 3.6 (H.P.Ko and D.K. Ray-Chaudhuri) .
Suppose that R *is a* $(m+1, m-1, m, 1)$*-relative diff. set in a cyclic group* G*. Let* p *be a prime divisor of* m*.*
(1) If $p^j \equiv 1 \ mod \ m+1$*, then* $p^j \equiv 1 \ mod \ m^2 - 1$*.*
(2) If $p^j \equiv m \ mod \ m+1$*, then* $p^j \equiv m \ mod \ m^2 - 1$*.*
(3) If $p^j \equiv 1 \ mod \ m-1$*, then* $p^j \equiv 1$ *or* $m \ mod \ m\,2 - 1$*.*

By using theorems above the following theorem holds.

Theorem 3.7 (D.Jungnickel and A.Pott) .
Suppose that R *is a* $(m+1, m-1, m, 1)$*-relative diff. set in an abelian group* G*. If* $m \leq 10000$ *then* m *has to be a prime power.*

Concerning $(m + \sqrt{m} + 1, m - \sqrt{m}, m, 1)$-relative difference sets we have the following.

Theorem 3.8 (M.J.Ganley and E.Spence) .
Let R be a $(m+\sqrt{m}+1, m-\sqrt{m}, m, 1)$-relative difference set in an abelian group. Then $m = 4$ or m is not a prime power.

4 $(m, m, m, 1)$-relative difference sets

Example 2.
Let q be an odd prime power. Then it is rather easy to check that the set

$$R = \{(x, x^2) \mid x \in GF(q)\} \subset (GF(q), +) \times (GF(q), +)$$

is a $(q, q, q, 1)$-relative difference set relative to N where N is the subgroup of elements whose first coordinate is 0.

Example 3
Let $q = 2^e$ be a power of 2. Then the set $\{(x, y) \mid x, y \in GF(q)\}$ becomes a group G if we define the multiplication $(x, y) \cdot (u, v) = (x + u, y + v + xu)$. The group G is isomorphic to $(\mathbf{Z}_4)^e$ and $N := \{(0, y) \mid y \in GF(q)\}$ is a subgroup isomorphic to $(\mathbf{Z}_2)^e$. Then the set

$$R = \{(x, x) \mid x \in GF(q)\}$$

is a $(q, q, q, 1)$-relative difference set in G relative to N.

Theorem 4.1 (M.J.Ganley) .
Let R be a $(m, m, m, 1)$-relative difference set in an abelian group G relative to N. If m is even, then n has to be a power of 2, say $m = 2^e$, and $G \cong (\mathbf{Z}_4)^e, N \cong (\mathbf{Z}_2)^e$.

Theorem 4.2 (C.I.Fung, M.K.Siu and S.L.Ma) .
Let R be a $(m, m, m, 1)$-splitting relative difference set in $\mathbf{Z}_m \times \mathbf{Z}_m$. Then m is the product of distinct primes.

Theorem 4.3 (Y.Hiramine, C.I.Fung, M.K.Siu and S.L.Ma) .
(1) Let R be a $(m, m, m, 1)$-splitting relative difference set in $\mathbf{Z}_m \times \mathbf{Z}_m$.
Then it does not occur that $m = pq$ where p and q primes.. (First Y.Hiramine proved the theorem in the case $p = 3$.)
(2) Let R be a $(m, m, m, 1)$-splitting relative difference set in $\mathbf{Z}_m \times \mathbf{Z}_m$. Then it does not occur that $m = pqr$ where p, q and r primes.

Theorem 4.4 (D.Gluck, Y.Hiramine, L.Ronayi and T.Szonyi) .
Let R be a $(p, p, p, 1)$-relative difference set where p is a prime. Then the corresponding projective plane is dedarguesian.

Theorem 4.5 (N.Nakagawa) .
Let R be a $(p^n, p^n, p^n, 1)$-relative difference set in a group $H \times N$ relative to N where p is an odd prime. Then

$$exp(N) \leq \begin{cases} p^{\frac{n+1}{2}} & (n : odd) \\ p^{\frac{n}{2}} & (n : even) \end{cases}$$

Moreover $exp(H) < p^n$.

Remark
In the theorem above it is unknown whether the group $H \times N$ is an elementary abelian group or not. However the following theorem holds in the case $|H| = |N| = p^2$.

Theorem 4.6 (S.L.Ma and A.Pott) .
Let R be an abelian $(p^2, p^2, p^2, 1)$-relative difference set in G where p is an odd prime. Then G has to be the elementary abelian group.

Now we would state an important theorem about splitting (p^2, p, p^2, p)-relative difference sets by S.L. Ma and A. Pott.

Theorem 4.7 (S.L.Ma and A.Pott) .
Let R be a $(p^2, p, p^2, 1)$-relative difference set in $G = \mathbf{Z}_{p^2} \times \mathbf{Z}_p$ relative to N where p is an odd prime power. Let $H_1, \cdots, H_{p-1}$ denote $p-1$ subgroups of G with $|H_i| = p$, $H_i \neq N$, and $G/H_i \cong \mathbf{Z}_{p^2}$. Let U be the subgroup of G with $U \cong \mathbf{Z}_p \times \mathbf{Z}_p$. Then there are $p-1$ group elements h_i and a subgroup $H_0 (\neq H_i$ for $i \neq 0)$ of U such that

$$R' = H_0 \cup \sum_{i=1}^{p-1} h_i \cdot H_i \qquad (\diamond)$$

for some translate R' of R. Moreover $\{id_G, h_1, \cdots, h_{p-1}\}$ is a complete system of coset representatives of U.
Conversely any subset of G defined by $(\diamond)$ is a relative $(p^2, p, p^2, 1)$-difference set in G.

5 Planar functions of elementary abelian p-groups type

In this section we will study about $(p^a, p^a, p^a, 1)$-relative difference sets in an elementary abelian p-group. Let G and H be groups isomorphic to the additive group of the finite group $GF(p^n)$ for an odd prime p. Let f be a function from G into $H (G = H \cong \mathbf{Z}_p^n)$. We define a Gauss sum of f with respect to $\chi \in \hat{G}$ and $\rho \in \hat{H}$ where $\hat{G}$ and $\hat{H}$ are the character groups of G and H respectively.

$$z_{\chi,\rho} = \sum_{x \in G} \chi(x)\rho(f(x))$$

We have the following theorem.

Theorem 5.1 () .
A function f from G into H is a planar function if and only if

$$z_{\chi,\rho}\bar{z}_{\chi,\rho} = p^n$$

for any $\chi \in \hat{G}$ and any$\rho \in \hat{H}$ such that $\rho \neq 1$. Then

$$z_{\chi,\rho} = \begin{cases} \pm p^{\frac{n}{2}}\omega^t & (n : even) \\ \pm p^{\frac{n-1}{2}}\tau\omega^t & (n : odd) \end{cases}$$

where ω is a primitive p-th root and $\tau = \sum_{i \in \mathbf{Z}_p} \lambda(i)\omega^i$.
(Here λ is the character of $\mathbf{Z}_p^*$ of order 2.)

Put $f(x) = (f_1(x), \cdots, f_n(x))$ where $x = (x_1, \cdots, x_n) \in G$.
We note f_i is a polynomial in n indeterminates.$(1 \leq i \leq n)$.
χ corresponds to $(i_1, \cdots, i_n)$ for $i_1, \cdots, i_n \in \mathbf{Z}_p$ by the definition

$$\chi(\mathbf{x}) = \chi(x_1, \cdots, x_n) = \omega^{\mathbf{i}\cdot\mathbf{x}}$$

where $\mathbf{i} \cdot \mathbf{x} = i_1x_1 + \cdots + i_nx_n$. Simularly ρ also correspond to $(s_1, \cdots, s_n)$ for $(s_1, \cdots, s_n) \in \mathbf{Z}_p$.
Then

$$z_{\chi,\rho} = \sum_{\mathbf{x}=(x_1,\cdots,x_n)\in G} \omega^{\mathbf{i}\cdot\mathbf{x}+f(\mathbf{x})\cdot\mathbf{s}} \qquad (\clubsuit)$$

where $f(\mathbf{x}) = (f_1(\mathbf{x}), \cdots, f_n(\mathbf{x}))$ and $\mathbf{s} = (s_1, \cdots, s_n)$.

Now we define the bent polynomials family over $\mathbf{Z}_p$ for any prime number p coming from planar functions naturally in spite of planar functions are defined only on vector spaces over $\mathbf{Z}_p$ for an

odd prime number p.
A linear polynomial at a in n indeterminates over $\mathbf{Z}_p$ is defined as

$$L_{\mathbf{a}}(\mathbf{x}) = a_1x_1 + \cdots + a_nx_n$$

where $\mathbf{a} = (a_1, \cdots, a_n)$ and $\mathbf{x} = (x_1, \cdots, x_n)$.
The number of solutions of g at $k \in \mathbf{Z}_p$ is

$$c_k(g) = \sharp\{(x_1, \cdots, x_n) \in \mathbf{Z}_p^n \mid g(x_1, \cdots, x_n) = k\}$$

for a polynomial $g(x_1, \cdots, x_n)$ in n determinates over $\mathbf{Z}_p$.
Then the bent polynomials $\mathcal{F}_p(n)$ is defined as follows.

$$\mathcal{F}_p(n) = \{f(x_1, \cdots, x_n) \mid f \text{is satisfied the condition}(\heartsuit) \text{ below for any } \mathbf{a} \in \mathbf{Z}_p^n\}$$

Suppose that n is even.

$$c_k(L_a + f) = \begin{cases} p^{n-1} \pm p^{\frac{n}{2}} \mp p^{\frac{n-2}{2}} & (k = k_0) \\ p^{n-1} \mp p^{\frac{n-2}{2}} & (k \neq k_0) \end{cases} \qquad (\heartsuit 1)$$

where k_0 is a fixed suitable element of $\mathbf{Z}_p$.
Suppose that n is odd.

$$c_k(L_a + f) = \begin{cases} p^{n-1} & (k = k_0) \\ p^{n-1} + p^{\frac{n-1}{2}} & (k \in A) \\ p^{n-1} - p^{\frac{n-1}{2}} & (k \in B) \end{cases} \qquad (\heartsuit 2)$$

where k_0 is a fixed suitable element of $\mathbf{Z}_p$ and $\mathbf{Z}_p = \{k_0\} \cup A \cup B$ such that $|A| = |B| = \frac{p-1}{2}$.
We have the following theorem by Theorem 5.1 and (♣).

Theorem 5.2 () .
A function $f(\mathbf{x}) = (f_1(\mathbf{x}), \cdots, f_n(\mathbf{x}))$ *from* G *into* H *is a planar function if and only if*

$$s_1f_1 + \cdots + s_nf_n \in \mathcal{F}_p(n)$$

for $\forall(s_1, \cdots, s_n) \in \mathbf{Z}_p^n$ *such that* $(s_1, \cdots, s_n) \neq (0, \cdots, 0)$.

Example 4
If a polynomial g in n indeterminates over $\mathbf{Z}_p$ is a nondegenerate quadratic form, then $f \in \mathcal{F}_p(n)$.
Example 5
Let $f(\mathbf{x}) = \mathbf{a}\mathbf{x}^2 + \mathbf{b}\mathbf{x} + \mathbf{c}$ be a quadratic polynomial over $GF(p^n)$. Put $f(\mathbf{x}) = (f_1(\mathbf{x}), \cdots, f_n(\mathbf{x}))$ where $f_i(\mathbf{x})$ is a polynomial in n indetaminates over $\mathbf{Z}_p$. Then $s_1f_1 + \cdots + s_nf_n \in \mathcal{F}_p(n)$ for $\forall(s_1, \cdots, s_n) \in \mathbf{Z}_p^n$ such that $(s_1, \cdots, s_n) \neq (0, \cdots, 0)$.
Example 6
Set $p = 5, n = 2, f(\mathbf{x}) = \mathbf{x}^2$ in **Example 5**
Then $f_1(x, y) = x^2 + 2y^2$, $f_2(x, y) = 2xy$. Moreover $p^{n-1} + p^{\frac{n}{2}} - p^{\frac{n-2}{2}} = 9, p^{n-1} - p^{\frac{n}{2}} + p^{\frac{n-2}{2}} = 1$, $p^{n-1} - p^{\frac{n-2}{2}} = 4$, $p^{n-1} + p^{\frac{n-2}{2}} = 6$.

k	0	1	2	3	4	.	k	0	1	2	3	4
$c_k(f_1)$	1	6	6	6	6	.	$c_k(f_2)$	9	4	4	4	4
$c_k(2f_1)$	1	6	6	6	6	.	$c_k(2f_2)$	9	4	4	4	4
$c_k(3f_1)$	1	6	6	6	6	.	$c_k(3f_2)$	9	4	4	4	4
$c_k(4f_1)$	1	6	6	6	6	.	$c_k(4f_2)$	9	4	4	4	4
$c_k(f_1+f_2)$	9	4	4	4	4	.	$c_k(2f_1+f_2)$	1	6	6	6	6
$c_k(f_1+2f_2)$	1	6	6	6	6	.	$c_k(3f_1+f_2)$	1	6	6	6	6
$c_k(f_1+4f_2)$	9	4	4	4	4	.	$c_k(4f_1+f_2)$	9	4	4	4	4
$c_k(f_1+3f_2)$	1	6	6	6	6	.	$c_k(2f_1+2f_2)$	9	4	4	4	4
$c_k(2f_1+3f_2)$	9	4	4	4	4	.	$c_k(3f_1+2f_2)$	9	4	4	4	4
$c_k(2f_1+4f_2)$	1	6	6	6	6	.	$c_k(4f_1+2f_2)$	1	6	6	6	6
$c_k(3f_1+3f_2)$	9	4	4	4	4	.	$c_k(4f_1+4f_2)$	9	4	4	4	4
$c_k(3f_1+4f_2)$	1	6	6	6	6	.	$c_k(4f_1+3f_2)$	1	6	6	6	6

For a = (1, 2),

k	0	1	2	3	4
$c_k(L_a+f_1)$	6	6	6	1	6
$c_k(L_a+f_2)$	4	4	4	4	9
$c_k(L_a+f_1+f_2)$	4	4	9	4	4
$c_k(L_a+2f_1+f_2)$	6	6	6	6	1

Example 7(Coulter and Matteiws)
Suppose that the greatest common divisor of α and 2e is 1. Then the following polynomial is a planar function.

$$f:\ GF(3^e) \longrightarrow GF(3^e) \qquad x \longrightarrow x^{3^e+1}2$$

(Here we consider $GF(3^e)$ as the additive group.)
Specially $f(x) = x^{14}$ is a planar function from $(GF(3^4), +)$ into $(GF(3^4), +)$.

From this example if we put

$$f(x_1,x_2,x_3,x_4) = x_1^2-x_1x_2+x_1^2x_2^2+x_1^2x_3^2+x_1^2x_2x_3+x_1x_2^2x_3+x_1x_2x_3^2-x_1x_4-x_1^2x_4^2+x_1x_2^2x_4-x_1x_2x_4^2+$$

$$x_1^2x_3x_4 + x_1x_3^2x_4 + x_2^2x_3x_4 - x_2x_3^2x_4 + x_2x_3x_4^2 + x_3^2x_4^2$$

then $f(x_1, x_2, x_3, x_4) \in \mathcal{F}_3(4)$.

Lemma(N.Nakagawa)
Let f(x,y) be m-form over $\mathbf{Z}_p$.

$$f(x,y) = a_0x^m + a_1x^{m-1}y + \cdots + a_{m-1}xy^{m-1} + a_my^m$$

If (1) $m = 3$,
or (2) $4 \le m \le p-1, a_0 \neq 0, a_m \neq 0$ and $(\mathbf{Z}_p{}^*)^{m-1} = (\mathbf{Z}_p{}^*)^2$,then $f \notin \mathcal{F}_p(2)$.

Problem 2
How many are there bent polynomials in $\mathcal{F}_p(n)$ for an odd prime p except nondegenerate quadratic forms.
(1) Classify bent polynomials in $\mathcal{F}_3(2), \mathcal{F}_3(3)$ and $\mathcal{F}_3(4)$.
(2) Let $\{f_1, f_2, \cdots, f_n\}$ be a system of polynomials in n indeterminates over $\mathbf{Z}_p$ such that

$$s_1f_1 + \cdots + s_nf_n \in \mathcal{F}_p(n)$$

for $\forall(s_1,\cdots,s_n)\neq(0,\cdots,0)$. Then is $F(x_1,\cdots,x_n)=(f_1(x_1,\cdots,x_n),\cdots,f_n(x_1,\cdots,x_n))$ a planar function from $(GF(p^n,+))$ into $(GF(p^n,+))$?

6 Finite geometries related to bent families over $\mathbf{Z}_2$

In this section we take $n=2m$ to be even and $p=2$.
Bent families over $\mathbf{Z}_2$ is well known as bent functions ago.

$$2^{2m-1}\pm 2^{\frac{2m}{2}}\mp 2^{\frac{2m-2}{2}}=2^{2m-1}\pm 2^{m-1},\qquad 2^{2m-1}\mp 2^{\frac{2m-2}{2}}=2^{2m-1}\mp 2^{m-1}$$

Hence $\mathcal{F}_2(n)$ is the family of a function f from $(\mathbf{Z}_2)^n$ into $\mathbf{Z}_2$ with the following property.

$$c_0(f+L_a)=2^{2m-1}\pm 2^{m-1},\quad c_1(f+L_a)=2^{2m-1}\mp 2^{m-1}\qquad(\spadesuit 1)$$

for $\forall a\in(\mathbf{Z}_2)^n$.
This property is also said in the following statement.

$$\sharp\{v\in\mathbf{Z}_2)^n\mid f(v)\neq L_a(v)\}=2^{2m-1}\pm 2^{m-1}\qquad(\spadesuit 2)$$

for $\forall a\in(\mathbf{Z}_2)^n$.
We denote the hamming distance of f and g by $\delta(f,g)$ for $f,g:\ (\mathbf{Z}_2)^n\longmapsto\mathbf{Z}_2$. For $0\leq r\leq n$, the r-th order *Reed-Muller code* of length 2^n is spanned by the set of polynomial functions of degree at most r on $(\mathbf{Z}_2)^n$. It is denoted by $\mathcal{R}(n,r)$.

$$\mathcal{R}(n,1)=\{\ f(x_1,\cdots,x_n)=a_0+a_1x_1+\cdots+a_nx_n\mid a_i\in\mathbf{Z}_2\}$$

The covering radius of $\mathcal{R}(n,1)$ is denoted by $r(\mathcal{R}(n,1))$.

$$r(\mathcal{R}(n,1))=\max\{\delta(f)\mid f\in\mathrm{Map}((\mathbf{Z}_2)^n,\ \mathbf{Z}_2)\ \}$$

where

$$\delta(f)=\min\{\ \delta(f,L)\mid L\in\mathcal{R}(n,1)\ \}$$

Then it is well known that $r(\mathcal{R}(2m,1))\leq 2^{2m-1}-2^{m-1}$. On the other hand by $(\spadesuit 2)$
$\delta(f)=2^{2m-1}-2^{m-1}$ for any bent function f.
Thus a bent function is a function which lies most far (bent) from the polynomial functions of degree at most 1 on $\mathbf{Z}_2$.
Example 8
Nondegenerate quadratic forms over $\mathbf{Z}_2$ are bent functions.

$$x_1x_2+x_3x_4+\cdots+x_{2m-1}x_{2m}$$

$$x_1x_2+x_3x_4+\cdots+x_{2m-3}x_{2m-2}+x_{2m-1}^2+x_{2m-1}x_{2m}+x_{2m}^2$$

Example 9

$$x_1x_2+x_3x_4+\cdots+x_{2m-1}x_{2m}+x_1x_3\cdots x_{2m-1}$$

P.J.Cameron says the problem of classifying bent functions appears to be hopeless.

(I) (Bent functions coming from crooked functions and distance regular graphs with $d=3,\lambda=0,\mu=2$.)(T.D.Bending and D.Fon-Der-Flaass)
Let V and W be n-dimensional vecter spaces over $\mathbf{Z}_2$, and $Q:\ V\longmapsto W$ any mapping.

Definition 6.1 .
A mapping Q is called crooked if it satisfies the following three properties:
(1) $Q(0)=0$;
(2) $Q(x)+Q(y)+Q(z)+Q(x+y+z)\neq 0$ *for any three distinct* x,y,z;
(3) $Q(x)+Q(y)+Q(z)+Q(x+a)+Q(y+a)+Q(z+a)\neq 0$ *if* $a\neq 0(\forall x,y,z)$.

Then Q is a bijection.

Example 10

Let n be an odd positive intege and k be a positive integer and $(n,k)=1$. We put

$$Q(x)=x^{2^k}+1 \quad \text{for } V=W=GF(2^n)$$

Then Q ia a crooked function.

Suppose that Q is a crooked function.

For $0\neq a$, we denote by $H_a(Q)$, the set

$$H_a(Q)=\{\, Q(x)+Q(x+a) \mid x\in V\}.$$

Then $H_a(Q)$ is the complement of a hyperplane.

Let $0\neq a\in V$. Moreover we define a linear functioal h_a on W, and a mapping $Q_a : V\longmapsto \mathbf{Z}_2$, by the following fules:

$$h_a(w)=1 \text{ if and only if } w\in H_a(Q)$$

$$Q_a(v)=h_a(Q(v))$$

Theorem 6.1 (Bending and Flaass) .

If $0\neq a\in V$ then for any hyperplane $U\subset V$ not containing a:

(i) *The two functions obtained by restricting Q_a to U and to V/U are complementary, in the sense that we can translate one to the complement of the other.*

(ii) *The function $Q_a|U$ is a bent function.*

Now a crooked function corresponds to a distance regular graph with intersection array

$$\begin{pmatrix} 0 & 1 & 2 & 2^{n+1}-1 \\ 0 & 0 & 2^{n+1}-4 & 0 \\ 2^{n+1}-1 & 2^{n+1}-2 & 1 & 0 \end{pmatrix}$$

as following.

The set of vertices :$V\times\{0,1\}\times W$

The incidence relation : $(a,i,\alpha)\sim(b,j,\beta)\Longleftrightarrow \alpha+\beta=Q(a+b)+(i+j+1)(Q(a)+Q(b))$ for $(a,i,\alpha),(b,j,\beta)\in V\times\{0,1\}\times W$

This graph is a 2^n-cover of the complete graph $K_{2^{n+1}}$ of vertex size 2^{n+1}.

(II) (Bent functions and symmetric designs with S.D.P)(W.M.Kantor and P.J.Cameron) $\mathrm{Map}((\mathbf{Z}_2)^n,\mathbf{Z}_2)$ is the 2^n-dimensional vector space over $\mathbf{Z}_2$. The rth order *Reed-Muller code* is a subspace of $\mathrm{Map}((\mathbf{Z}_2)^n,\mathbf{Z}_2)$ with $({}_nC_0+{}_nC_1+\cdots+{}_nC_r)$-dimension and minimal distance $d=2^{n-r}$.

$$\mathcal{R}(n,1)\subset\mathcal{R}(n,2)$$

Let D be a coset of $\mathcal{R}(n,1)$ in $\mathcal{R}(n,2)$. Put $D=\mathcal{R}(n,1)+f$ for some $f\in\mathcal{R}(n,2)$.

We have $\sharp\{\, w(g)\mid g\in D\,\}\leq 3$ where $w(g)$ is the weight of g, and

$$\sharp\{\, w(g)\mid g\in D\,\}=2\Longleftrightarrow f \text{ is nondegenerate bilinear form (bent function).}$$

Then all elements of D are bent functions.

$$\{\, w(g)\mid g\in D\,\}=\{\, 2^{2m-1}\pm 2^{m-1}\}$$

where $n=2m$. We also have

$$\sharp\{\, g\in D\mid w(g)=2^{2m-1}-2^{m-1}\,\}=\sharp\{\, g\in D\mid w(g)=2^{2m-1}+2^{m-1}\,\}=2^{2m}$$

We remark that the dimension of $\mathcal{R}(2m,1)$ is 2^{2m+1}.

Now we set as following.

$$B_g = \mathrm{supp}(g) = \{\, v \in V \mid g(v) = 1 \,\}$$

$$\mathrm{B} = \{\, B_g \mid w(g) = 2^{2m-1} - 2^{m-1},\ g \in D\}$$

Then $\mathcal{D} = ((\mathrm{Z}_2)^{2m}, \mathrm{B}, \in)$ is a $2-(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ symmetric design with symmetric difference property.

Problem 3
What sort of finite geometries is related to bent polynomials of odd type?

References

[1] T.D.Bending and D.G. Fon-Der-Flaass. Crooked functions, bent function, and distance-regular graphs, Electronic Journal of Combinatorics 5(1998), # R34,14pp.

[2] P.J. Cameron. Finite geometry and coding theory, Socrates Intensive Programme Finite Geometries and Their Automorphisms, Potenza,Italy June 1999.

[3] N.Ito. On Hadamard groups, J.Algebra 168(1994), 981-987.

[4] N.Ito. On Hadamard groups, II. J.Algebra 169(1994), 936-942.

[5] N.Ito. Some remarks on Hadamard groups, In Groups-Korea 94, de Gruyter, Berlin/New York 1995, 149-155.

[6] N.Ito. Remarks on Hadamard groups, Kyushu J. Math. 50(1996), 83-91.

[7] N.Ito. Remarks on Hadamard groups, II. Rep. Fac. Sci.Technol.Meijo Univ. No. 37(1997), 1-7.

[8] N.Ito. On Hadamard groups III, Kyushu J.Math. 51(1997), 365-379.

[9] Y.Hiramine. A conjecture on affine planes of prime oeder, J. Combin. Theory Ser.A 52(1989), 44-50.

[10] Y. Hiramine. On planar functions, J.Algebra 133(1990), 103-110.

[11] Y. Hiramine. Facter sets associated with regular collineation groups, J.Algebra 142(1991), 414-423.

[12] Y. Hiramine. Planar functions and related group algebras, J.Algebra 152(1992), 135-145.

[13] S.L.Ma. On (p^a, p, p^a, p^{a-1})-relative difference sets, manuscript.

[14] S.L.Ma and A Pott. Relative difference sets, planar functions and generalized Hadamard matrices, J.Algebra 175(1995), 505-525.

[15] N. Nakagawa. The non-existence of right cyclic planar functions of degree p^n for $n \leq 2$, J. Combin. Theory Ser A 63(1993), 55-64.

[16] A.Pott. A survey on relative difference sets, Groups, Difference Sets and the Monster, Ohio State University Mathematical Research Institute Publications 4, de Gruyter.