

第24回 代数的組合せ論シンポジウム 報告集

2007 年 6 月 28 ～ 30 日
於 近畿大学 ノーベンバー小ホール

平成19年度文部科学省科学研究費基盤研究(B)
研究代表者 坂内 英一

まえがき

この報告集は2007年6月28日(木)から6月30日(土)にわたり、近畿大学ノーベンバー小ホールで行われた「第24回代数的組合せ論シンポジウム」の講演記録です。講演は21名の講演者によって行われ、70名を越える参加者がありません。近畿大学では大学院博士課程前・後期(理学専攻科)の制度も軌道にのり、多くの院生の手伝いを受け、このような研究集会をもてたことは非常な喜びであります。この報告集の作成、および数名の講演者の旅費は

平成19年度文部科学省科学研究費基盤研究(B)
研究代表者 坂内 英一教授(タイトル:代数的組合せ論の総合的研究、課題番号16340010)

より援助を受けています。
また、近畿大学およびノーベンバーホールの事務局の方々にはホールの使用にあたり、大変お世話になりました。
その他にも講演者の方々、参加者の方々、また会場準備等を手伝ってくれた近畿大学の院生諸君、この研究集会に関係するすべての方々にお礼を申し上げます。

2007年11月
近畿大学 中川 暢夫
浅井 恒信
東京女子大学 吉荒 聡

注意

本報告は、昭和二十一年三月三十一日現在の状況に基づき、昭和二十二年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。

昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。

昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。

昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。昭和二十二年三月三十一日現在の状況は、昭和二十一年三月三十一日現在の状況とを比較し、その増減の概況を示すものである。

第24回代数的組合せ論研究集会

代数的組合せ論とその周辺の皆様、第24回代数的組合せ論研究集会を下記の通り行いますので、ご案内申し上げます。

世話人 近畿大学 浅井 恒信
東京女子大学 吉荒 聡
近畿大学 中川 暢夫

日程：2007年6月28日(木) ～ 30日(土)

場所：近畿大学 ノーベンパー 小ホール
(大阪市東大阪市小若江3-4-1)

プログラム

6月28日(木)

- 10:00~10:50 坂内英一 (九州大学)
Euclidean designs, cubature formulas, and orthogonal polynomials
- 11:00~11:50 神谷典史 (NEC)
LDPC 符号と組合せデザイン
- 14:00~14:30 千吉良直紀 (室蘭工業大学)
群上の方程式の解の個数に関する母関数について
- 14:40~15:10 小田文仁 (富山高等専門学校)
The crossed Burnside ring and the representation ring of Drinfel'd double
- 15:20~15:50 篠原雅史 (九州大学)
Uniqueness of maximum three-distance sets in the three- dimensional Euclidean space
- 16:10~16:40 松岡武夫 (皇學館大学)
Galois groups on elliptic curves and Flavor symmetry
- 16:50~17:20 別宮耕一 (上武大学)
Type II codes over Galois rings
- 17:30~18:00 安部利之 (愛媛大学)
A generalization of the Frenkel-Zhu bimodule

6月29日(金)

- 10:00~10:50 山田裕理 (一橋大学)
Subalgebras of lattice vertex operator algebras and W algebras
- 11:00~11:50 宮本雅彦 (筑波大学)
Verlinde 予想の証明に対する一考察
- 14:00~14:30 田辺顕一郎 (北海道大学)
On modules of vertex algebras constructed from commutative algebras
- 14:40~15:10 島倉裕樹 (千葉大学)
On Ising vectors in VOAs associated with lattices
- 15:20~15:50 澤正憲 (名古屋大学)
回転不変な積分のクラスに関する求積公式について
- 16:10~16:40 花木章秀 (信州大学)
Nilpotent, solvable, and monomial schemes
- 16:50~17:20 城本啓介 (愛知県立大学)
量子信号処理における代数的組合せ論
- 17:30~18:00 谷口浩朗 (詫間電波工業専門学校)
On d -dimensional dual hyperovals in $PG(2d, 2)$ coming from finite translation affine planes

6月30日(土)

- 10:00~10:50 平木彰 (大阪教育大学)
A characterization of some distance-regular graphs
- 11:00~11:30 吉田知行 (北海道大学)
超幾何多項式の積公式
- 11:40~12:10 坂内悦子 (九州大学)
ユークリッド空間のデザインについて
- 14:00~14:30 細谷利恵 (国際基督教大学)
Terwilliger algebras of subsets with minimal width and dual width
- 14:40~15:10 末竹千博 (大分大学)、秋山献之 (福岡大学)
The nonexistence of projective planes of order 12 with a collineation group of order 8

懇親会

日時： 2007年6月29日（金）18:15-20:15

会場： 近畿大学ノーベンバーホール生協地下食堂

会費： 5000円（学生と退職者の方は割引）

ご参加いただける方は6月16日（土）までに下記の南および中川のメールまでお知らせください。

近畿大学正門（西門）を入れて突き当たりを右に曲がり、歩いて最初の角を左に約120m歩くと東門手前左の建物がノーベンバーホールです。この道沿いの2階が小ホールの入り口になっています。

その他、会場施設および近くの飲食店等の詳細は

<http://www.math.kindai.ac.jp>

の談話会・研究集会をクリック、近鉄大阪線長瀬駅下車13分（アクセスはこちら）をクリック、近大への鉄道、近大付近、近大界限偏向飲食地図をご参照ください。

世話人等・連絡先

〒577-8502 東大阪市小若江3-4-1 理工学部理学科数学教室

南 香織 (minami@math.kindai.ac.jp)

中川 暢夫 (nakagawa@math.kindai.ac.jp)

浅井 恒信 (asai@math.kindai.ac.jp)

THE STATE OF TEXAS,
COUNTY OF []
I, the undersigned, a Notary Public in and for the State of Texas, do hereby certify that the within and foregoing is a true and correct copy of the original of the same as the same appears from the records of the County of [] State of Texas.

Witness my hand and the seal of my office, this [] day of [] 19[]
Notary Public in and for the State of Texas.

My commission expires on the [] day of [] 19[]
[]

Attest my hand and the seal of my office, this [] day of [] 19[]
Notary Public in and for the State of Texas.

目次

1. 坂内英一 (九州大学大学院数理学研究院)	1
Euclidean desigus, cubature formulas, and orthogonal polynomials	
2. 千吉良直紀 (室蘭工業大学)	12
群上の方程式の解の個数に関する母関数について	
3. 小田文仁 (富山高等専門学校)	20
The crossed Burnside ring and the representation ring of Drinfel'd double	
4. 篠原雅史 (九州大学大学院数理学府)	32
Uniqueness of maximum three-distance sets in the three- dimensional Euclidean space	
5. 松岡武夫 (皇學館大学社会福祉学部)	41
Galois groups on elliptic curves and Flavor symmetry	
6. 別宮耕一 (上武大学)	51
Type II codes over Galois rings	
7. 安部利之 (愛媛大学理学部)	55
A generalization of the Frenkel-Zhu bimodule	
8. 山田裕理 (一橋大学大学院経済学研究科)	62
Subalgebras of lattice vertex operator algebras and W algebras	
9. 宮本雅彦 (筑波大学大学院数理物質科学研究科)	72
Verlinde 予想の証明に対する一考察	
10. 田辺頭一郎 (北海道大学理学部)	79
可換代数から構成される頂点代数の加群について	
11. 島倉裕樹 (千葉大学大学院自然科学研究科)	84
On Ising vectors in VOAs associated with lattices	
12. 澤正憲 (名古屋大学)	90
回転不変な積分のクラスに関する求積公式について	

13. 花木章秀 (信州大学理学部)	100
Nilpotent, solvable, and monomial schemes	
14. 城本啓介 (愛知県立大学)	107
量子信号処理における代数的組合せ論	
15. 谷口浩朗 (詫間電波工業専門学校)	112
On d -dimensional dual hyperovals in $PG(2d, 2)$ coming from finite translation affine planes	
16. 平木彰 (大阪教育大学)	121
A characterization of some distance-regular graphs	
17. 吉田知行 (北海道大学理学部)	127
超幾何多項式の積公式	
18. 坂内悦子 (九州大学大学院数理学研究院)	137
ユークリッド空間のデザインについて	
19. 細谷利恵 (国際基督教大学)	144
Terwilliger algebras of subsets with minimal width and dual width	
20. 末竹千博 (大分大学工学部)、秋山献之 (福岡大学理学部)	151
The nonexistence of projective planes of order 12 with a collneation group of order 8	

Euclidean designs, cubature formulas, and orthogonal polynomials

坂内英一 (Eiichi Bannai)

九大・数理

(Faculty of Mathematics, Kyushu University)

1 はじめに

この論文は第24回代数的組合せ論シンポジウム(2007年6月28-30日)の講演をOHPの原稿に従ってほぼ忠実に記録したものです。講演では、前もってアナウンスされていた上のタイトルとは少しだけ異なり、

Spherical designs,
Euclidean designs,
cubature formulas,

についての survey を与えることが主になりました。(Orthogonal polynomials と関係することにはほとんど触れることが出来ませんでした。)最後に極く最近得られた1つの新しい結果を述べました。この最後の結果は坂内悦子との共同研究です。詳しくはこの報告集の坂内悦子の記事も参照して下さい。

2 Spherical t -designs

多項式の積分に関して、単位球面 S^{n-1} を近似する次の良い性質を持った有限集合 X を spherical t -design と呼びます。この概念は Delsarte-Goethals-Scidel (1977) で定義されました。すなわち、

$X \subset S^{n-1} (\subset R^n), |X| < \infty$ が次の条件を満たすとき、spherical t -design と呼ぶ。

$$\frac{1}{|S^{n-1}|} \int_{S^{n-1}} f(x) d\sigma(x) = \frac{1}{|X|} \sum_{x \in X} f(x).$$

for $\forall f(x) = f(x_1, x_2, \dots, x_n)$ polynomials of degree $\leq t$.

Spherical t -designs の有名な例としては次の物がある。

- R^3 における正多面体の頂点の集合は適当な t に対する spherical t -design となる。例えば正 20 面体の 12 個の頂点の集合は 5-design であるという具合である。
- R^8 における E_8 -型ルート系の 240 個のルートからなる集合（もちろん原点からの距離を 1 に正規化したもの）は 7-design である。
- R^{24} における Leech 格子の 196560 点の min. vectors の集合（もちろん原点からの距離を 1 に正規化したもの）は 11-design である。
- R^2 における正 $t+1$ 角形の $t+1$ 点の頂点の集合（もちろん原点からの距離を 1 に正規化したもの）は t -design である。

次にいくつかの注意を述べる。

- 直交群 $O(n)$ の有限部分群 G の軌道、すなわち $X = \{x^g \mid g \in G\}$, として多くの spherical t -design が得られる。ただし $n \geq 3$ の時、大きい t に対しては、そのようなものは作れない。（そのようにして出来る spherical t -design に対しては、ある関数 $f(n)$ が存在して、 $t \leq f(n)$ (ただし $n \geq 3$) であることが知られている。(Bannai, 1985). 絶対定数 t_0 が存在して (例えば $t_0 = 19$) $t \leq t_0$ となるのではないかと予想されるが、まだ未解決である。
- 一方、 $\forall t, \forall l$ に対して S^{n-1} における spherical t -design は存在することが知られている。(Scymour-Zaslavsky, 1984.) しかしこの定理は存在定理であり、具体的な構成は難しい。
- 我々は与えられた t, n に対して、 $|X|$ が出来るだけ小さい spherical t -design が欲しい。与えられた t, n に対して、Fischer 型不等式と呼ばれる $|X|$ の自然な下界は知られてる。更に $|X|$ がその下界と一致する場合、 X は tight spherical t -design であると呼ばれる。(Delsarte-Goethals-Seidel, 1977).
- S^{n-1} における tight spherical t -design は、 $t = 4, 5, 7$ の場合を除き分類されている。(Bannai-Damerell, 1979/80). $t = 4, 5, 7$ の場合はその後長い間全く進展はなかったが、新しい部分的進展が得られた。(Bannai-Munemasa-Venkov, 2004). ただし、完全な分類はまだ困難であり、未解決のままである。
- X を S^{n-1} における spherical t -design であり、かつ s -距離集合であるとする。(すなわち、 X の相異なる 2 つの元の間の距離が s 種類とする。) このとき次が成り立つ。
 - (1) $t \leq 2s$. (ここで等号 $t = 2s$ が成り立つことと、 X が tight $2s$ -design であることは同値である。)
 - (2) X が antipodal の時、 $t \leq 2s - 1$. (ここで等号 $t = 2s - 1$ が成り立つことと、 X が antipodal な tight $(2s - 1)$ -design であることは同値である。)
 - (3) $t \geq 2s - 2$ が成り立つときは、 X は距離を relations としてクラス s の (すなわち全部で $s + 1$ の relations からなる) アソシエーションスキームを作る。さらにこのアソシエーションスキームは、 Q -多項式アソシエーションスキームになる。

Spherical t -design の概念の拡張

これについては、

- (A) 基礎になる空間を変える、
 - (B) デザインに重みを許す (Cubature formula を考える)、
 - (C) 多項式を他の関数族に置き換える、
- などの方向がある。ここでは主に (A) と (B) を考え、(C) には触れない。(A) の例としてはたとえば次ぎのように考える。

$D(\subset R^n)$, μ を D 上の measure であり D 上で多項式の積分が定義されるとする。このとき、 (D, μ) に対して、 $X \subset D$, $|X| \leq \infty$ が t -design であるとは、

$$\frac{1}{|D|} \int_D f(x) d\mu(x) = \frac{1}{|X|} \sum_{x \in X} f(x).$$

for $\forall f(x) = f(x_1, x_2, \dots, x_n)$ polynomials of degree $\leq t$, であることと定義する。

3 Cubature Formulas (重さを持ったデザイン)

• S^{n-1} の場合。

$X \subset S^{n-1}$, $|X| < \infty$
 $\lambda: X \rightarrow R_{>0}$,

とする。このとき、 (X, λ) が S^{n-1} 上の cubature formula of degree t であるとは、

$$\int_{S^{n-1}} f(x) d\sigma(x) = \sum_{x \in X} f(x).$$

for $\forall f(x) = f(x_1, x_2, \dots, x_n)$ polynomials of degree $\leq t$, であることと定義する。

• 一般の場合。

$D(\subset R^n)$, μ を D 上の measure であり D 上で多項式の積分が定義されるとする。また、

$X \subset D$, $|X| < \infty$
 $\lambda: X \rightarrow R_{>0}$,

とする。このとき、 (X, λ) が (D, μ) 上の cubature formula of degree t であるとは、

$$\int_D f(x) d\mu(x) = \sum_{x \in X} f(x).$$

for $\forall f(x) = f(x_1, x_2, \dots, x_n)$ polynomials of degree $\leq t$, であることと定義する。

次にいくつかの注意を述べる。

• (X, λ) を S^{n-1} 上の cubature formula of degree t とするとき、 $|X|$ の自然な下界が解析学において知られていた (1970 年代、Delsarte-Goethals-Seidel と独立にかつほぼ同時期に。) この下界は実は spherical t -design に対する下界と全く同一である。実は cubature formula of degree t である X に対して、 $|X|$ がこの自然な下界と一致すると、 λ は定数関数、従って X は tight spherical t -design であることが示される。従って tight spherical t -design の分類は球面 S^{n-1} の上の tight な cubature formulas の分類も与えることにな

る。

- 解析学 (近似理論、数値解析、統計学) においていろいろな (D, μ) に対して、cubature formula が研究されている。その歴史は、Gauss まで遡ることが出来るほど古く、非常に多くの (何万といえる) 論文があるようである。めぼしい名前をいくつかあげれば、Gauss, Jacobi, Tchebycheff, Markov, Szegő, Sobolev, Mysoviskikh, Möller, Cools, Schmid, Xu, Tchakaloff, Stroud, ... などなどきりが無いと思われる。

- 一般の (D, μ) に対しての cubature formula についても、sphere S^{n-1} の場合と同様に、興味のある中心は与えられた t に対して、cubature formula of degree t である具体的な (X, λ) の構成と、 $|X|$ の出来るだけ小さいものを求めることであると思われる。 t -design (重み無しの cubature formula) よりも cubature formula (重みありのデザイン) のほうが歴史的にも古くかつ多くの研究が成されていると言えよう。

解析学においては、いろいろな空間 (D, μ) に対しての cubature formulas が研究されていますが、ここでは特に D, μ 共に $O(n)$ 不変なもの考えることにします。このような、 (D, μ) を radially symmetric であると呼びます。具体例としては次のようなものがあります。

- $D = S^{n-1}, \mu =$ 定数関数。(これは通常の S^{n-1} 上の cubature formula あるいは spherical t -design です。)

- $D = \cup_{i=1}^p S_i^{n-1}$, 有限個の原点を中心とする同心球の集まり、 μ は S_i^{n-1} 上定数関数 μ_i 、 $\int_D f(x) d\mu = \sum_i \mu_i \int_{S_i^{n-1}} f(x) d\sigma_i(x)$ 。

- $D = R^n, d\mu = e^{-\|x\|^2} dx_1 \cdots dx_n$ (この μ を Gaussian measure と呼ぶ)。

4 Euclidean t -designs

前に述べたときと同様に、

$$X \subset R^n, |X| < \infty$$

$$\lambda: X \rightarrow R_{>0}$$

とする。

- (X, λ) が Euclidean t -design であるとは、次数 t 以下の任意のモーメントが全て $O(n)$ の元 (直交変換) により不変であることと定義する。(この性質はもちろん spherical t -design に対しても成り立つ性質である。) 同値な定義は、次の様に、cubature formula の形でも述べられる。少し記号を準備する。

X と交わる原点を中心とする球面の全体を $S_i = S_i^{n-1} (1 \leq i \leq p)$ とする。 $X \cap S_i = X_i$ とおく。もちろん、 $X = X_1 \cup X_2 \cup \cdots \cup X_p$ である。

(X, λ) が Euclidean t -design であるとは、次の条件を満たすことと同値になる。

$$\sum_{i=1}^p \frac{\lambda(X_i)}{|S_i|} \int_{S_i} f(x) d\sigma_i(x) = \sum_{x \in X} \lambda(x) f(x)$$

$\forall f(x) = f(x_1, x_2, \dots, x_n)$ polynomials of degree $\leq t$.

(この定義は Neumaier-Seidel(1988), Delsarte-Seidel (1989) による。この概念は統計学

における rotatable design の概念ともほとんど同じである。)

次の事実は重要である。

- (D, μ) を radially symmetric であるとする。 (X, λ) が (D, μ) に対する cubature formula of degree t であれば、 (X, λ) は Euclidean t -design である。
従って、Euclidean t -design は種々の radially symmetric な (D, μ) に対する cubature formula of degree t の master class (親分) であると言える。従って、個々の radially symmetric な (D, μ) を考える替わりに、euclidean t -design で考えようというのが我々の立場である。

Euclidean t -design の $|X|$ の自然な下界について

$X \subset R^n$, $D = S = S(X) = S_1 \cup S_2 \cup \dots \cup S_p$ とする。 $X = X_1 \cup X_2 \cup \dots \cup X_p$ であり、 $X_i \subset S_i$ である。

(X, λ) が Euclidean t -design の時、すなわち、cubature formula of degree t のとき次の不等式がなりたつ。

- X が Euclidean t -design with $t = 2e$ ならば、

$$|X| \geq \dim(P_e(S))$$

ここで、 $P_e(S)$ は R^n の e -次以下の多項式全体で定義域を S に制限したものの作るベクトル空間を表す。(この結果は容易であり、多くの人により独立に得られている。ここで等号の成り立つとき (X, λ) を tight $2e$ -design in $S(X)$ と呼ぶことにする。)

- 詳しい説明は省略するが、 $t = 2e + 1$ に対しても、非常に一般的な自然な下界が Möller (1976, 1979) により得られている。(我々は antipodal という仮定のもとで、tight $(2e + 1)$ -design を考えて同じ下界を得ていた。ただしこの下界に一致するものは antipodal になるという Möller の結果は知らなかった。) この下界を結果のみ書くと、 $2\dim(P_e^*(S))$ あるいは $2\dim(P_e^*(S)) - 1$ で与えられる。(ここで等号の成り立つとき (X, λ) を tight $(2e + 1)$ -design in $S(X)$ と呼ぶことにする。) 我々は極く最近まで $t = 2e + 1$ の場合の Möller の結果を知らなかった。この結果については、名古屋大学の沢正憲君と平尾将剛君から教えて貰った。それを通して解析の分野での多くの文献にも新しく気付いた訳である。Möller の結果などの詳しいことは、この報告集の坂内悦子の記事を参照されたい。

R^2 の場合

- (D, μ) が radially symmetric な場合の tight $(t = 4k + 1)$ -designs (特に $O \in X$ の場合) は、Verlinden-Cools (1992) により詳しく研究されている。特に特別な (D, μ) 、例えば $D = R^2$, $\mu = e^{-\|x\|^2} dx_1 dx_2 \dots dx_n$ の場合は、tight $t = 4k + 1$ design の分類 ($t \geq 5$ の場合の非存在) が示されている。(Cools-Schmid, 1993).
- 一方、Bajnok (2006, Advances in Geom.) は R^2 において、 p 個の同心円 $S(X)$ 上の tight t -designs を組織的に作っている。(ただし p はある値より小さい時。) 実はそのような tight Euclidean t -designs は分類が完成している。(Verlinden-Cools (1992) も本質的に同じことをやっている。ただし Gaussian design の存在のための必要条件としてそれらを得ており、Euclidean t -design として存在しているという見方はしていない。)

5 Euclidean t -designs についての最近の仕事の紹介

Tight Euclidean t -designs の構成と分類に関して

Bannai-Bannai (2006, J. Math. Soc. Japan), Etsuko Bannai (2006, J. Algebraic Comb.), Bannai-Bannai-Suprijanto (2007, Europ. J. Comb.) Etsuko Bannai (preprint) などを参照されたい。より詳しいことは、この報告集の坂内悦子の記事を見られたい。Bajnok (2005, Adv. in Geom.) は R^2 の場合を詳しく取り扱っている。また、Bajnok (2007, J. Algebraic Comb.) は $W(B_n)$ の軌道の合併として構成出来る Euclidean t -designs を研究しており、そのようにして出来るいくつかの tight Euclidean t -designs も構成している。

Victoir (2004, SIAM J. Numer. Anal.)

この文献も沢、平尾の両氏から教えて貰った。

この論文では例えば次のことをやっている。

- $W(B_n)$ 不変な (D, μ) に対して、cubature formula of degree t で、 n によらない (t のみによる) 個数の $W(B_n)$ -軌道の合併集合として出来るものが存在すること。(これは Sobolev の結果を用いる。) また、各軌道の点集合を比較的少ない個数の点で置き換えて得られる cubature formulas が存在することを示し(ここで Tchakaloff の結果を用いる)、組合せ論(通常の組合せ論的デザインなど)を用いて、比較的小さいサイズの Euclidean t -designs を具体的に構成している。

問題提起

私は、与えられた Euclidean t -design (X, λ) について、それが degree t の cubature formula になっているような radially symmetric な (D, μ) がいつ存在するか?(例えば $D = R^n$ かつ μ を原点からの距離 r に関する連続関数となるようなものがいつ具体的に構成出来るか?) という種類の問題が面白いと思う。

解析学において、いくつかの結果が知られているようであるが、私にはきちんと理解できているわけではない。 μ を r の関数として連続関数とまで強くなくて、無限個の点でジャンプする増加関数で Stieltjes 積分で考えたものでは、一般にそれが可能であると言う結果があると思われる(文献を漁った限りでは、しかし自信はない。) いずれにせよ、この問題は、1 次元の symmetric Hamburger reduced moment problem (あるいは Stieltjes reduced moment problem) の indetermined case の解の存在と密接に関係していることは確かである。

de la Harpe-Pache-Venkov (2006, Algebra i Analiz)

この論文では R^n における lattice (格子) のいくつかの shell (原点から距離一定の点の集合を shell と呼ぶ) の合併集合として、 S^{n-1} 上の cubature formulas (重さを持った spherical designs) を具体的に構成している。ここでは S^{n-1} 上の集合に直して考えているが、Euclidean t -designs として shell の合併集合を考えることも可能である。また、そのようなものは、アソシエーションスキームを拡張した概念である coherent configuration と密接に関係することを注意しよう。

Ballinger-Blekherman-Cohn-Giansiracusa-Kelly-Schürmann

(Nov 2006, arXiv:math.MG/0611451v1)

この論文では球面 S^{n-1} 上の universally optimal codes の分類問題と関係し、コンピューターで候補者を具体的に作り出す。私は非常に面白いと思う。有限集合 $X \subset S^{n-1}$ が

spherical t -design でありかつ s -距離集合でかつ $t \geq 2s - 1$ あるいは X が antipodal で、 $t \geq 2s - 2$ ならばそのような X は universally optimal codes であることが知られている。(Cohn-Kumar, 2007). 従って、universally optimal codes の分類にはそのようなものの分類が必要になる。そのようなものの分類は私が現在本気で取り組みたいと思っている研究課題である。

6 新しい結果と途中経過

新しい結果 (坂内悦子との共同研究) として次が得られた。講演の時から以降に得られた結果も一部述べる。

定理 1 2つの同心球 $S(X)$ 上の tight Euclidean 7-designs $X = X_1 \cup X_2$ は分類され、以下の表に記したものに限る。

n	$ X $	$ X_1 $	$ X_2 $	$A(X_1)$	$A(X_2)$	w
2	12	6(tight)	6(tight)	$\pm \frac{1}{2}, -1$	$\pm \frac{1}{2}r^2, -r^2$	$\frac{1}{r^6}$
4	48	24	24	$0, \pm \frac{1}{2}, -1$	$0, \pm \frac{1}{2}r^2, -r^2$	$\frac{1}{r^6}$
7	182	56(tight)	126	$\pm \frac{1}{3}, -1$	$0, \pm \frac{1}{3}r^2, -r^2$	$\frac{32}{27} \frac{1}{r^6}$

上の表で X_1 は半径 1 の球面上に、 X_2 は半径 r の球面上に載っているように正規化してある。上のどの例でも、 r を任意に取れることがみそである。上の表で X_1 上の weight は 1、 X_2 上の weight は w に正規化してある。(Tight Euclidean t -design においては weight は各 X_i の上では一定であることが知られていることに注意。) $A(X_i)$ は X_i の相異なる 2 点の内積として現れるものの集合を表す。上の表で $n = 2$ の場合 X_1 と X_2 は正六角形である。 $n = 4$ の場合は X_1 と X_2 は互いに相似で R^1 の kissing 数を与える配置になっている。 $n = 7$ の場合は X_1 は球面上の tight 5-デザインである。 E_7^* の min. vectors の集合にもなっている。 X_2 は E_7 型のルートで与えられる点集合である。最後の $n = 7$ の集合 X_1, X_2 は (両方とも半径 1 にした場合) それらの合併集合が universally optimal codes の候補者として、Ballinger, et. al. (preprint) でも述べられていて、興味深い。しかし半径を変えて新しい tight Euclidean 7-designs が出来ることは、新しい結果である。 r を適当に選ぶと、重さが全て一定の tight Euclidean 7-design が出来ることも興味深い。 $n = 4$ の場合は Bajnok (2007) により既に知られていたことに注意されたい。

定理 1 の証明の概略は省略する。この報告集の坂内悦子の記事を参照されたい。この証明の過程の副産物として得られた次の結果も重要であると思われる。

定理 2 $X \subset S^{n-1}$ は有限集合であり、 X は (i) spherical t -design, (ii) s -距離集合、さらに (iii) antipodal であると仮定する。このとき次が成り立つ。

- (1) $t \geq 2s - 3$ ならば X はクラス s のアソシエーションスキームを作る。
- (2) 特に $t = 5, s = 4$ の場合はさらに Q -多項式アソシエーションスキームになる。(これは $t \geq 2s - 3$ の場合常に成り立つと予想される。現在証明を完成させようとしているところ。)
- (3) 特に $t = 5, s = 4$ 場合、パラメーターの可能性はかなり決まる。全てのパラメーターは n と $|X|$ の 2 つのみで具体的に表される。特に面白い例がシリーズで現れる。最後にそれ

を述べてこの原稿を終える。

以下は、 $t = 5, s = 4$ の $X \subset S^n$ の例である。 r は任意の自然数で、 $n = 2^{2r}, |X| = 2^{4r} + 2^{2r+1}$ である。このようなものは任意の実 MUB (mutually unbiased bases) に対して、従って任意の r に対して存在する。重要なことは、これはクラス 4 の Q -多項式アソシエーションスキーム (ただし P -多項式アソシエーションスキームではない) になる。以下の B_i^* が 3 重対角行列であることに注意。これらはアソシエーションスキームとしては新しいものではないかもしれないが、 Q -多項式アソシエーションスキームであることは新しい結果であると思われる。(W. Martin のホームページの Q -多項式アソシエーションスキームの data base ではこれらの例は気付かれていなかった。) もう一つ重要なことは、これらは universally optimal codes かそれに非常に近いものであることである。ただし、 $r = 1$ の場合、すなわち D_4 型ルートの集合は、universally optimal code で無いことが示されている。(Cohn-Conway-Elkies-Kumar, arXiv:math.NG/0607447.) 一方 $r \geq 2$ の場合は未解決と思われる。

$$B_1 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$B_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 2^{4r-1} & 0 & 2^{r-2}(2^{2r}-2)(2^r-1) & 2^{r-2}(2^{2r}-2)(2^r+1) & 2^{4r-1} \\ 0 & 2^{4r-1} & 2^{r-2}(2^{2r}-2)(2^r+1) & 2^{r-2}(2^{2r}-2)(2^r-1) & 2^{4r-1} \\ 0 & 0 & 2^{2r}-1 & 2^{2r}-1 & 0 \end{bmatrix}$$

$$B_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 2^{4r-1} & 2^{r-2}(2^{2r}-2)(2^r+1) & 2^{r-2}(2^{2r}-2)(2^r-1) & 2^{4r-1} \\ 2^{4r-1} & 0 & 2^{r-2}(2^{2r}-2)(2^r-1) & 2^{r-2}(2^{2r}-2)(2^r+1) & 2^{4r-1} \\ 0 & 0 & 2^{2r}-1 & 2^{2r}-1 & 0 \end{bmatrix}$$

$$B_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 2^{2r}-1 & 2^{2r}-1 & 0 \\ 0 & 0 & 2^{2r}-1 & 2^{2r}-1 & 0 \\ 2(2^{2r}-1) & 2(2^{2r}-1) & 0 & 0 & 2(2^{2r}-2) \end{bmatrix}$$

$$P = \begin{bmatrix} 1 & 1 & 2^{4r-1} & 2^{4r-1} & 2(2^{2r}-1) \\ 1 & -1 & -2^{3r-1} & 2^{3r-1} & 0 \\ 1 & 1 & 0 & 0 & -2 \\ 1 & -1 & 2^r & -2^r & 0 \\ 1 & 1 & -2^{2r} & -2^{2r} & 2(2^{2r}-1) \end{bmatrix}$$

$$Q = \begin{bmatrix} 1 & 2^{2r} & (2^{2r} - 1)(2^{2r-1} + 1) & 2^{4r-1} & 2^{2r-1} \\ 1 & -2^{2r} & (2^{2r} - 1)(2^{2r-1} + 1) & -2^{4r-1} & 2^{2r-1} \\ 1 & -2^r & 0 & 2^r & -1 \\ 1 & 2^r & 0 & -2^r & -1 \\ 1 & 0 & -2^{2r-1} - 1 & 0 & 2^{2r-1} \end{bmatrix}$$

Then we obtain

$$B_1^* = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 2^{2r} & 0 & \frac{2^{2r}}{2^{2r-1}+1} & 0 & 0 \\ 0 & 2^{2r} - 1 & 0 & 2^{2r} - 1 & 0 \\ 0 & 0 & \frac{2^{4r}}{2^{4r}+2} & 0 & 2^{2r} \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

References

- [1] B. BAJNOK, *On Euclidean designs*, Adv. Geom. 6 (2006) 423-438.
- [2] B. BAJNOK, *Orbits of the hyperoctahedral group as Euclidean designs*, J. Algebraic Combin. 25 (2007), no. 4, 375-397.
- [3] B. BALLINGER, G. BLEKHERMAN, H. COHN, N. GIANSIRACUSA, E. KELLY AND A. SCHUERMAN, *Experimental study of energy-minimizing point configurations on spheres*, arXiv:math/0611451.
- [4] EI. BANNAI AND ET. BANNAI, *Algebraic Combinatorics on Spheres* (in Japanese) Springer Tokyo 1999.
- [5] EI. BANNAI AND ET. BANNAI, *Tight Gaussian 4-designs*, J. Algebraic Combinatorics, 22 (2005) 39-63.
- [6] EI. BANNAI AND ET. BANNAI, *On Euclidean tight 4-designs*, J. Math. Soc. Japan 58 (2006), 775-804.
- [7] EI. BANNAI, ET. BANNAI AND D. SUPRIJANTO, *On the strong non-rigidity of certain tight Euclidean designs*, European J. Combin. 28 (2007) no. 6, 1662-1680.
- [8] EI. BANNAI, A. MUNEMASA AND B. VENKOV, *The nonexistence of certain tight spherical designs*, With an appendix by Y.-F. S. Petermann. Algebra i Analiz 16 (2004), no. 4, 1-23; translation in St. Petersburg Math. J. 16 (2005), no. 4, 609-625
- [9] ET. BANNAI *On Antipodal Euclidean Tight $(2e+1)$ -Designs*, J. Algebraic Combinatorics 24 (2006), 391-414.
- [10] ET. BANNAI *New examples of Euclidean tight 4-designs*, preprint.
- [11] G. E. P. BOX AND J. S. HUNTER, *Multi-factor experimental designs for exploring response surfaces*, Ann. Math. Statist. 28 (1957), 195-241.

- [12] A. R. CALDERBANK, P. J. CAMERON, W. M. KANTOR AND J. J. SEIDEL, *Z_4 -Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets*, Proc. London Math. Soc. (3) 75 (1997), no. 2, 436-480.
- [13] J. S. CHRISTIANSEN, *The moment problem, an introduction*, (10pages) <http://www.its.caltech.edu/stordal/mp.pdf>
- [14] H. COHN AND A. KUMAR, *Universally optimal distribution of points on spheres*, J. Amer. Math. Soc. 20 (2007), 99-148.
- [15] R. COOLS AND H. J. SCHMID, *A new lower bound for the number of nodes in cubature formulae of degree $4n + 1$ for some circularly symmetric integrals*, International Series of Numerical Math., 112 (1993) 57-66.
- [16] P. DELSARTE, J. M. GOETHALS AND J. J. SEIDEL, *Bounds for systems of lines and Jacobi polynomials*, Philips Research Reports 30 (1975).
- [17] P. DELSARTE, J. M. GOETHALS, AND J. J. SEIDEL, *Spherical codes and designs*, Geom. Dedicata 6 (1977), 363-388.
- [18] P. DELSARTE AND J. J. SEIDEL, *Fisher type inequalities for Euclidean t -designs*, Linear Algebra Appl. 114-115 (1989), 213-230.
- [19] M. DEZA AND P. FRANKL, *Bounds on the maximum number of vectors with given scalar products*, Proc. Amer. Math. Soc. 95 (1985), no. 2, 323-329.
- [20] P. DE LA HARPE, C. PACHE AND B. VENKOV, *Construction of spherical cubature formulas using lattices*, Algebra i Analiz 18 (2006), no. 1, 162-186.
- [21] S. G. HOGGAR, *Tight 4- and 5-designs in projective spaces*. Graphs Combin. 5 (1989), no. 1, 87-94.
- [22] Y. HONG, *On spherical t -designs in R^2* , European J. Combin. 3 (1982), no. 3, 255-258.
- [23] H. M. MÖLLER, *Kubaturformeln mit minimaler Knotenzahl*, Numer. Math. 25 (1975/76), no. 2, 185-200.
- [24] H. M. MÖLLER, *Lower bounds for the number of nodes in cubature formulae*, Numerische Integration (Tagung, Math. Forschungsinst., Oberwolfach, 1978), 221-230, Internat. Ser. Numer. Math., 45, Birkhäuser, Basel-Boston, Mass., 1979.
- [25] E. NISHIDA, Personal communication. To be written up as a master degree thesis (Jan. 2008, Kyushu University) under the supervision of the second author.
- [26] A. NEUMAIER AND J. J. SEIDEL, *Discrete measures for spherical designs, eutactic stars and lattices*, Nederl. Akad. Wetensch. Proc. Ser. A 91=Indag. Math. 50 (1988), 321-334.

- [27] P. D. SEYMOUR AND T. ZASLAVSKY, *Averaging sets: a generalization of mean values and spherical designs*, Adv. in Math. 52 (1984) 213–240.
- [28] P. VERLINDEN AND R. COOLS *On cubature formulae of degree $4k + 1$ attaining Möller's lower bound for integrals with circular symmetry*, Numer. Math. 61 (1992) 395–407.
- [29] N. VICTOIR, *Asymmetric cubature formulae with few points in high dimension for symmetric measures*, SIAM J. Numer. Anal. 42 (2004), no. 1, 209–227 (electronic).
- [30] Y. XU, *Lower bound for the number of nodes of cubature formulae on the unit ball*, Numerical integration and its complexity (Oberwolfach, 2001). J. Complexity 19 (2003), no. 3, 392–402.

群上の方程式の解の個数に関する母関数について

室蘭工業大学
千吉良直紀

G を有限群とする。 $d \in \mathbb{N}$ に対して

$$a_d(G) = \#\{x \in G \mid x^d = 1\} = |\text{Hom}(Z_d, G)|$$

とおく。(この数は Frobenius 数と呼ばれることがある。)

無限系列の群 $\{G_n\}$ に対して

$$1 + \sum_{n=1}^{\infty} \frac{a_d(G_n)}{|G_n|} x^n$$

なる母関数を考えることにする。

$G_n, A_n, G \wr S_n, W(D_n)$ に対しては、この型の母関数および $a_d(G)$ を $|\text{Hom}(A, G_n)|$ (A は群) に置き換えた母関数は Chowla-Herstein-Scott, Okada, Chigira, Wohlfhart, Müller, Takegahara らによって求められている。

ここでは古典群について考えることにする。いくつかの古典群について [4] で母関数を調べている。ここでは特に群論で重要な役割を果たしている involution の個数 (正確にはそれプラス単位元)、すなわち、 $d = 2$ の場合を中心に述べる。その他の d への一般化については [3] を参照されたい。この研究は竹ヶ原裕元氏 (室蘭工業大学) との共同研究である。

1 $GL(n, q)$

$q = p^f$ (p は素数) とする。 $d \in \mathbb{N}$ とし、 $P \in \text{Syl}_p(Z_d)$ とする。 $\{V_1, \dots, V_r\}$ で simple left $\mathbb{F}_q(Z_d/P)$ -module の代表系を表すことにする。 $d_i = \dim_{\mathbb{F}_q} V_i$ とし、 $q_i = q^{d_i}$ とおく。

$$\mathfrak{D}_{|P|}(n) = \{\lambda = (\lambda_1, \lambda_2, \dots) \vdash n \mid |P| \geq \lambda_1 \geq \lambda_2 \geq \dots\}$$

とおく。 $\lambda = (\lambda_1, \lambda_2, \dots) \in \mathfrak{D}_{|P|}(n)$ に対して

$$m_s(\lambda) = \#\{i \mid \lambda_i = s\}, \quad \bar{\lambda} = \sum_i (i-1)\lambda_i$$

とおく。

定理 ([4]) . 上の記号のもとで、

$$1 + \sum_{n=1}^{\infty} \frac{a_d(GL(n, q))}{|GL(n, q)|} x^n = \prod_{i=1}^r \left(1 + \sum_{n=1}^{\infty} \sum_{\lambda \in \mathfrak{D}_{|P|}(n)} \frac{x^{d_i n}}{q_i^{n+2\bar{\lambda}}} \prod_{s=1}^{|P|} \frac{q_i^{m_s(\lambda)^2}}{|GL(m_s(\lambda), q_i)|} \right)$$

例．特に $q = 2^c$, $d = 2$ とすると、simple left module は $\{V_1\}$ で、 $d_1 = \dim_{\mathbb{F}_q}(V_1) = 1$ である。 $\mathfrak{D}_2(n) = \{2^l 1^{n-2l} \mid l = 1, \dots, \lfloor \frac{n}{2} \rfloor\}$ で $\lambda = 2^l 1^{n-2l}$ に対して $m_2(\lambda) = l$, $m_1(\lambda) = n - 2l$ で、

$$\bar{\lambda} = 2 \frac{l(l-1)}{2} + \left(\frac{(n-l)(n-l-1)}{2} - \frac{l(l-1)}{2} \right) = \frac{(n-l)(n-l-1) + l(l-1)}{2}$$

ある。これを上の式に代入すると

$$1 + \sum_{n=1}^{\infty} \frac{a_2(GL(n, q))}{|GL(n, q)|} x^n = 1 + \sum_{n=1}^{\infty} \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor} \frac{x^n}{q^{n+l(l-1)+(n-l)(n-l-1)}} \frac{q^{l^2+(n-2l)^2}}{|GL(l, q)| |GL(n-2l, q)|}$$

となるので、整理すると

$$\begin{aligned} 1 + \sum_{n=1}^{\infty} \frac{a_2(GL(n, q))}{|GL(n, q)|} x^n &= 1 + \sum_{n=1}^{\infty} \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor} \frac{x^n}{q^{l(l-1)+(n-l)(n-l-1)} |GL(l, q)| |GL(n-2l, q)|} \\ &= \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{x^{2s+t}}{q^{s^2+2st} |GL(s, q)| |GL(t, q)|} \end{aligned}$$

とかけることがわかる。

ところで標数 2 の場合には I_l を l 次単位行列とすると $GL(n, q)$ の involution は

$$u_l = \begin{pmatrix} I_l & & & \\ & I_{n-2l} & & \\ & & & I_l \\ & & & & & I_l \end{pmatrix} \quad (1 \leq l \leq \lfloor \frac{n}{2} \rfloor)$$

のいずれかと共役である（この形の involution は Suzuki form と呼ばれている [2]）から

$$C_{GL(n, q)}(u_l) = \left\{ \begin{pmatrix} X & & & \\ P & Y & & \\ Q & R & X & \end{pmatrix} \mid X \in GL(l, q), Y \in GL(n-2l, q) \right\}$$

となつて $|C_{GL(n, q)}(u_l)| = q^{l^2+2l(n-2l)} |GL(l, q)| |GL(n-2l, q)|$ となることがわかるので

$$\frac{a_2(GL(n, q))}{|GL(n, q)|} = \sum_{l=0}^{\lfloor \frac{n}{2} \rfloor} \frac{1}{q^{l^2+2l(n-2l)} |GL(l, q)| |GL(n-2l, q)|}$$

となり、前述の式が得られることがわかる。

例．奇標数の場合はもっと簡単で involution は

$$\begin{pmatrix} I_l & & \\ & -I_{n-l} & \end{pmatrix} \quad (0 \leq l \leq n-1)$$

のいずれかと共役であることを使えば

$$1 + \sum_{n=1}^{\infty} \frac{a_2(GL(n, q))}{|GL(n, q)|} x^n = \left(\sum_{s=0}^{\infty} \frac{x^s}{|GL(s, q)|} \right)^2$$

となるのが簡単に計算できる。

では、他の古典群ではどうなるであろうか。一般に母関数を求めることが出来るかもしれないが GL の場合から推測すると他の古典群ではもっと複雑になってしまうだろうと思われる。一方 involution に限れば比較的簡単に計算できそうである。

次の場合はすでに計算されている。

定理 ([4]) . 次の場合、母関数が得られている。

- (1) $a_2(SL(n, q))$, q odd
- (2) $a_d(GU(n, q))$, $d|q^2 - 1$
- (3) $a_d(Sp(2n, q))$, d odd, q odd, $d|q - 1$
- (4) $a_d(Sp(2n, q))$, q even, $d|q - 1$
- (5) $a_d(GO^+(n, q))$, q even, $d|q - 1$
- (6) $a_d(GO^-(n, q))$, q even, $d|q - 1$

以下、 $d = 2$ の場合についての考察を行うことにする。

2 $GU(n, q)$

$F = \mathbb{F}_{q^2}$ とし、 $x \in F$ に対して $\bar{x} = x^q$ とおくととき、

$$GU(n, q) = \{X \in GL(n, q^2) | X {}^t \bar{X} = I\}$$

である。

$$|GU(n, q)| = q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^i - (-1)^i)$$

奇標数の場合は次の結果がある。

定理 ([4]) . q を奇数とするとき、

$$1 + \sum_{n=1}^{\infty} \frac{a_2(GU(n, q))}{|GU(n, q)|} x^n = \left(\sum_{s=0}^{\infty} \frac{x^s}{|GU(s, q)|} \right)^2$$

q が 2 べきの場合次のようになる。

定理 1. $q = 2^k$ のとき、

$$1 + \sum_{n=1}^{\infty} \frac{a_2(GU(n, q))}{|GU(n, q)|} x^n = \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{x^{2s+t}}{q^{s(s+2t)} |GU(s, q)| |GU(t, q)|}$$

3 $Sp(2m, q)$

$$|Sp(2m, q)| = q^{m^2} \prod_{i=1}^m (q^{2i} - 1)$$

である。奇標数については次が得られている。

定理 ([4]) . q を奇数とする。

$$1 + \sum_{n=1}^{\infty} \frac{a_2(Sp(2m, q))}{|Sp(2m, q)|} x^m = \left(\sum_{s=0}^{\infty} \frac{x^s}{|Sp(2s, q)|} \right)^2$$

次に $q = 2^e$ とする。 V を非退化交代形式 $(\ , \)$ に関する Symplectic space とする。 u を $Sp(2, 2^e)$ の位数 2 の元とすると、

$$V(u) = \{v \in V | (v, v^u) = 0\}$$

とおく。 u は $SL(n, q)$ で

$$\begin{pmatrix} I_l & & & \\ & I_{n-2l} & & \\ & & & \\ & & & I_l \end{pmatrix}$$

に共役であるとする。 [2] により、involution の class は次の 3 つのタイプに分かれることが知られている。

- (i) type a_l : l は偶数で、 $V(u) = V$
- (ii) type b_l : l は奇数
- (iii) type c_l : l は偶数で、 $V(u) < V$

それぞれの場合について $|C_G(u)|$ を計算すると次のようになる。

- (i) type a_l : $|C_G(u)| = q^{l(l+1)/2 + l(2m-2l)} |Sp(l, q)| |Sp(2m-2l, q)|$
- (ii) type b_l : $|C_G(u)| = q^{l(l+1)/2 + l(2m-2l)} |Sp(l-1, q)| |Sp(2m-2l, q)|$
- (iii) type c_l : $|C_G(u)| = q^{l(l+1)/2 + l(2m-2l) + (l-1)} |Sp(l-2, q)| |Sp(2m-2l, q)|$

このことから次の母関数が得られる。

定理 2. $q = 2^e$ とする。

$$1 + \sum_{n=1}^{\infty} \frac{a_2(Sp(2m, q))}{|Sp(2m, q)|} x^m = \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{x^{2s+t}}{q^{(2s-1)(s+2t)} |Sp(2s, q)| |Sp(2t, q)|}$$

4 the orthogonal groups

$$|GO(2m+1, q)| = dq^{m^2} \prod_{i=1}^m (q^{2i} - 1), \quad d = (2, q-1)$$

$$|GO^+(2m, q)| = 2q^{m(m-1)}(q^m - 1) \prod_{i=1}^{m-2} (q^{2i} - 1)$$

$$|GO^-(2m, q)| = 2q^{m(m-1)}(q^m + 1) \prod_{i=1}^{m-2} (q^{2i} - 1)$$

である。

定理 ([4]) . q を奇数とする。

$$(i) \sum_{m=0}^{\infty} \frac{a_2(GO(2m+1, q))}{|GO(2m+1, q)|} x^m = 4 \left(\sum_{s=0}^{\infty} \frac{x^s}{|GO(2s+1, q)|} \right) \left(\sum_{t=0}^{\infty} \frac{q^{2t} x^t}{|GO(2t+1, q)|} \right)$$

$$(ii) 1 + \sum_{m=1}^{\infty} \frac{a_2(GO^+(2m, q))}{|GO^+(2m, q)|} x^m = \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{q^{s+t}(q^{s+t} + 1) + q^{2t-1}(q^{2t} - 1)}{2|Sp(2s, q)||Sp(2t, q)|} x^{s+t}$$

$$(iii) \sum_{m=1}^{\infty} \frac{a_2(GO^-(2m, q))}{|GO^-(2m, q)|} x^m = \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{q^{s+t}(q^{s+t} - 1) + q^{2t-1}(q^{2t} - 1)}{2|Sp(2s, q)||Sp(2t, q)|} x^{s+t}$$

次に q が 2 べきとする。 $GO(2m+1, q) \cong Sp(2m, q)$ であるから、 $GO^{\pm}(2m, q)$ の場合を計算すればよい。 $Sp(2m, q)$ のときのように、 [2] による共役類の分かれ方をみて計算すれば次のようになることがわかる。

定理 3. $q = 2^r$ とする。

$$(i) 1 + \sum_{m=1}^{\infty} \frac{a_2(GO^+(2m, q))}{|GO^+(2m, q)|} x^m = \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{q^{s+t}(q^{2s+t} + 1) + q^{2s+t-1}(q^{2t} - 1)}{2q^{2s(s+2t)}|Sp(2s, q)||Sp(2t, q)|} x^{s+t}$$

$$(ii) \sum_{m=1}^{\infty} \frac{a_2(GO^-(2m, q))}{|GO^-(2m, q)|} x^m = \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{q^{s+t}(q^{2s+t} - 1) + q^{2s+t-1}(q^{2t} - 1)}{2q^{2s(s+2t)}|Sp(2s, q)||Sp(2t, q)|} x^{s+t}$$

5 違うタイプの母関数

ここまで、体を固定し、次元を変えることにより母関数を考えていた。逆に次元を固定し、体のべきを変えて母関数を作ることも考えられる。形の違う母関数であるが、Dwork による次の結果が知られている。

(Dwork) 有限生成な群 G に対して、

$$\exp\left(\sum_{r=1}^{\infty} \frac{|\text{Hom}(G, GL(n, q^r))|}{r} t^r\right)$$

は有理関数である。

また別の形の母関数であるが、次元を固定し、標数のべきを変えた母関数を考える。次のような結果を得ている。

定理 4. (1) $\sum_{n=1}^{\infty} \frac{a_2(GL(2, 2^n))}{|GL(2, 2^n)|} x^n = \sum_{k=0}^{\infty} \frac{(2k+3+(-1)^k)x}{4(2^{k+2}-x)} = \frac{x}{4} \sum_{l=0}^{\infty} \frac{2l-1+(-1)^l}{2^l-x}$ for $|x| < 4$,

(2) $\sum_{n=1}^{\infty} \frac{a_2(GL(2, p^n))}{|GL(2, p^n)|} x^n = \sum_{k=0}^{\infty} \frac{(4k+1+(-1)^k)x}{2(p^{k+2}-x)}$ for $|x| < p^2$, where p is an odd prime,

(3) $\sum_{n=1}^{\infty} \frac{a_2(SL(2, 2^n))}{|SL(2, 2^n)|} x^n = \sum_{m=0}^{\infty} \frac{x}{2^{2m+1}-x}$ for $|x| < 2$,

(4) $\sum_{n=1}^{\infty} \frac{a_2(SL(2, p^n))}{|SL(2, p^n)|} x^n = \sum_{m=0}^{\infty} \frac{2x}{p^{2m+3}-x}$ for $|x| < p^3$, where p is an odd prime.

6 Rogers-Ramanujan 型の恒等式

$$\begin{aligned} |GL(n, q)| &= (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) \\ &= q^{n^2} \left(1 - \frac{1}{q}\right) \left(1 - \frac{1}{q^2}\right) \cdots \left(1 - \frac{1}{q^n}\right) \end{aligned}$$

であるから $z = \frac{1}{q}$ とおくと

$$|GL(n, q)| = \frac{(1-z)(1-z^2) \cdots (1-z^n)}{z^{n^2}}$$

となる。したがって

$$1 + \sum_{n=1}^{\infty} \frac{1}{|GL(n, q)|} = 1 + \sum_{n=1}^{\infty} \frac{z^{n^2}}{(1-z)(1-z^2) \cdots (1-z^n)}$$

次のような恒等式が知られている。

(Rogers-Ramanujan Identity)

$$(i) \quad 1 + \sum_{n=1}^{\infty} \frac{z^{n^2}}{(1-z)(1-z^2)\cdots(1-z^n)} = \prod_{n=0}^{\infty} \frac{1}{(1-z^{5n+1})(1-z^{5n+4})}$$

$$(ii) \quad 1 + \sum_{n=1}^{\infty} \frac{z^{n^2+n}}{(1-z)(1-z^2)\cdots(1-z^n)} = \prod_{n=0}^{\infty} \frac{1}{(1-z^{5n+2})(1-z^{5n+3})}$$

これより

定理 ([4]). G を位数 r のアーベル群、 $\exp(G)$ は $q-1$ を割り切るとする。このとき

$$(i) \quad 1 + \sum_{n=0}^{\infty} \frac{1}{|GL(n, q)|} = \prod_{n=0}^{\infty} \frac{1}{(1-q^{-(5n+1)})^r (1-q^{-(5n+4)})^r}$$

$$(ii) \quad 1 + \sum_{n=0}^{\infty} \frac{1}{|GL(n, q)|q^n} = \prod_{n=0}^{\infty} \frac{1}{(1-q^{-(5n+2)})^r (1-q^{-(5n+3)})^r}$$

Rogers Ramanujan identity は次の形で一般化されている。

(Gordon's generalization of Rogers-Ramanujan Identity)

For $1 \leq i \leq k, k \geq 2, |z| < 1,$

$$\sum_{n_1, n_2, \dots, n_{k-1} \geq 0} \frac{z^{N_1^2 + N_2^2 + \dots + N_{k-1}^2 + N_1 + N_{i+1} + \dots + N_{k-1}}}{(z)_{n_1} (z)_{n_2} \cdots (z)_{n_{k-1}}} = \prod_{n \neq 0, \pm i \pmod{2k+1}} \frac{1}{1-z^n}$$

where $N_j = n_j + n_{j+1} + \dots + n_{k-1}.$

例えば、 $k = 2, i = 2$ のとき、Rogers-Ramanujan の (i) に対応し、 $k = 2, i = 1$ のとき、(ii) に対応している。

前述の GL の母関数を思い出してみる。 q が 2 べきのとき、

$$1 + \sum_{n=1}^{\infty} \frac{a_2(GL(n, q))}{|GL(n, q)|} x^n = \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{x^{2s+t}}{q^{s^2+2st} |GL(s, q)| |SL(t, q)|}$$

$$= \sum_{s=0}^{\infty} \sum_{t=0}^{\infty} \frac{z^{(s+t)^2 + s^2} x^{(s+t)+s}}{(z)_s (z)_t}$$

となる。ここで、 $z = \frac{1}{q}$ とおいた。従って次のことがわかる。

定理 5. q を 2 べきとする。

$$(i) \quad 1 + \sum_{n=1}^{\infty} \frac{a_2(GL(n, q))}{|GL(n, q)|} = \prod_{\substack{n=1 \\ n \neq 0, \pm 3 \pmod{7}}}^{\infty} \frac{q^n}{q^n - 1}$$

$$(ii) 1 + \sum_{n=1}^{\infty} \frac{a_2(GL(n, q))}{|GL(n, q)|q^n} = \prod_{\substack{n=1 \\ n \not\equiv 0, \pm 1 \pmod{7}}}^{\infty} \frac{q^n}{q^n - 1}$$

上の定理に現れていない $n \neq 0, \pm 2 \pmod{7}$ の場合は次のところに現れる。

定理 6. q を 2 べきとする。

$$1 + \sum_{n=1}^{\infty} \frac{a_2(Sp(2m, q))}{|Sp(2m, q)|q^m} = \prod_{\substack{n=1 \\ n \not\equiv 0, \pm 2 \pmod{7}}}^{\infty} \frac{q^{2n}}{q^{2n} - 1}$$

GL の場合にはもう少し一般に次の結果を得ている。

定理 7. P を巡回 p 群、 $q = p^f$ とする。

$$(i) 1 + \sum_{n=1}^{\infty} \frac{|\text{Hom}(P, GL(n, q))|}{|GL(n, q)|} = \prod_{\substack{n=1 \\ n \not\equiv 0, \pm(fP+1) \pmod{2fP+3}}}^{\infty} \frac{q^n}{q^n - 1}$$

$$(ii) 1 + \sum_{n=1}^{\infty} \frac{|\text{Hom}(P, GL(n, q))|}{|GL(n, q)|q^n} = \prod_{\substack{n=1 \\ n \not\equiv 0, \pm 1 \pmod{2fP+3}}}^{\infty} \frac{q^n}{q^n - 1}$$

さまざまな母関数が得られた。これらの相互の関係などより詳しく調べる必要があると考えている。

参考文献

- [1] G. Andrews, "The Theory of Partitions", Addison-Wesley, Reading, MA, (1976).
- [2] M. Aschbacher and G. Seitz, Involutions in Chevalley Groups over fields of even order, Nagoya Math. J. **63** (1976) 1-91.
- [3] N. Chigira and Y. Takegahara, On generating functions for the Frobenius numbers of finite symplectic groups, in preparation.
- [4] N. Chigira, Y. Takegahara and T. Yoshida, On the number of homomorphisms from a finite group to a general linear group, J. Algebra **232** (2000) 236-254.

The crossed Burnside ring and the representation ring of Drinfel'd double

Fumilito Oda

Department of Liberal Arts, Toyama National College of Technology, Toyama 939-8630, Japan

E-mail: oda@toyama-nct.ac.jp

1 Introduction

We study the Grothendieck (character) ring of the Drinfel'd double of a finite group G over the complex field \mathbb{C} . Witherspoon studied the representation ring of the Drinfel'd double of a group algebra in positive characteristic [Wi96]. In particular, she gave a decomposition of the representation ring as a direct sum of ideals involving Green rings of subgroups by using Thévenaz's twin functor construction for Green functors [Th88]. Dress introduced the construction of a *Mackey functor* M_Γ from a Mackey functor M by simply setting $M_\Gamma(X) := M(X \times \Gamma)$ for all finite G -sets X when Γ is a finite G -set [Dr73]. We call this construction for Mackey functors the Dress construction. Bouc introduced the Dress construction for a *Green functor* ([Bo03a] Theorem 5.1): If A is a Green functor for G over a commutative ring \mathcal{O} , and Γ is a crossed G -monoid, then the Mackey functor A_Γ obtained by the Dress construction has a natural structure of a Green functor, and its evaluation $A_\Gamma(G)$ is an \mathcal{O} -algebra. Bouc's construction involves as special cases the construction of the crossed Burnside ring obtained from the Burnside ring Green functor, the Hochschild cohomology ring of G obtained from the group cohomology Green functor, and the Grothendieck ring of the Drinfel'd double of G obtained from the Grothendieck ring Green functor for a group algebra. We also point out that Bouc's construction is discussed in [Wi04]. In this paper, we obtain an induction theorem for the Drinfel'd double for G by using a formula for the primitive idempotents of the crossed Burnside ring [OY01], Bouc's construction, and some properties of Witherspoon's Green functor $R(D_G(\star))$. The theorem implies Artin's induction theorem for a group algebra over \mathbb{C} . This is a new proof of Artin induction theorem.

The paper is organized as follows: Section 2 recalls a summary of basic results on crossed G -sets and the crossed Burnside ring. Section 3 describes the relationship between the crossed Burnside ring Green functor and the Grothendieck ring Green functor for the Drinfel'd double. Section 4 exposes a kind of induction theorem for \mathbb{C} -representations of the Drinfel'd double of G . We shall note that the result is not exactly an induction theorem for the \mathbb{C} -representation of the Drinfel'd double of G , because the evaluation $R_{\mathbb{C}}(D_G(H))$ of the Green functor $R_{\mathbb{C}}(D_G(\star))$ at a subgroup H of G is not isomorphic to the \mathbb{C} -representation ring $R_{\mathbb{C}}(D(H))$ of the Drinfel'd double of H .

We refer the reader to [Bo97], [Bo00], [TW95] or [We00] for standard definitions and results regarding Burnside rings and Green functors, and to [Bo03a], [Bo03b], [OY01],

and [OY04] for basic results about crossed G -sets and crossed Burnside rings.

2 Crossed G -sets

(2.1) Notation. Let G be a finite group. If H is a subgroup of G , and $g \in G$, the conjugate subgroup gHg^{-1} of G is denoted by gH . The normalizer of H in G is denoted by $N_G(H)$. The centralizer of H (resp. $g \in G$) in G is denoted by $C_G(H)$ (resp. $C_G(g)$). A set of representatives in G of G/H is denoted by $[G/H]$. If X is a G -set, the stabilizer in G of element x of X is denoted by G_x . If X and Y are G -sets, the intersection $G_x \cap G_y$ of stabilizers in G of element (x, y) of $X \times Y$ is denoted by $G_{x,y}$. The set of orbits of H on X is denoted by $H \backslash X$, and $[H \backslash X]$ denotes a set of representatives in X of $H \backslash X$.

(2.2) Crossed Burnside rings. Let G be a finite group. In [Bo03a], Bouc defined a crossed G -monoid as follows. A *crossed G -monoid* (Γ, φ) is a pair consisting of a finite monoid Γ with a left action of G by monoid automorphisms (denoted by $(g, \gamma) \mapsto g\gamma$ or $(g, \gamma) \mapsto {}^g\gamma$, for $g \in G$ and $\gamma \in \Gamma$), and a map of G -monoids φ from Γ to the G -set G^c with G -action defined by conjugation (i.e. a map φ which is both a map of monoids and a map of G -sets). In this paper, since we use only the trivial crossed G -monoid $(\Gamma, \varphi) = (G^c, id_{G^c})$, we denote by Γ or G^c a crossed G -monoid. A *crossed G -set* (X, α) over a crossed G -monoid Γ , is a pair consisting of a finite G -set X , together with a map α of G -sets from X to Γ . A *morphism* of crossed G -sets from (X, α) to (Y, β) is a G -map f from X to Y such that $\beta \circ f = \alpha$. Crossed G -sets over Γ and crossed G -maps make a category $G\text{-xset}/\Gamma$. The *tensor product* of crossed G -sets (X, α) and (Y, β) is defined by $(X \times Y, \alpha.\beta)$, where $X \times Y$ is the direct product of X and Y , with diagonal G -action, and $\alpha.\beta$ is the map from $X \times Y$ to G^c defined by $\alpha.\beta(x, y) = \alpha(x)\beta(y)$. We denote by $X\Omega(G, \Gamma)$ the Grothendieck ring of the category $G\text{-xset}/\Gamma$ with respect to disjoint union and tensor product. We call it the *crossed Burnside ring*. The crossed Burnside ring $G\text{-xset}/\Gamma^c$ over the crossed 1^c -monoid is the ordinary Burnside ring $B(G)$. Since any crossed G -set is a disjoint union of *transitive* crossed G -sets (see 2.12 of [OY01]), $G\text{-xset}/\Gamma$ has the following free \mathbb{Z} -basis as an abelian group:

$$\{(G/D)_s \mid D \in [G \backslash S(G)], s \in [G \backslash C_\Gamma(D)]\}.$$

If Γ is a normal subgroup of G or an abelian group, then a formula for the primitive idempotents of $\mathbb{K}X\Omega(G, \Gamma)$ over a splitting field \mathbb{K} of characteristic 0 has been given by Oda and Yoshida (see Lemma (5.5) of [OY01]).

(2.3) Theorem. [OY01] *Let \mathbb{K} be a field of characteristic 0 which is a splitting field for all subgroups of G .*

(1) *For $H \leq G$ and an irreducible \mathbb{K} -character θ of $C_\Gamma(H)$, we put*

$$e_{H,\theta} = \frac{\theta(1)}{|N_G(H)||C_\Gamma(H)|} \sum_{D \leq H} \sum_{s \in C_\Gamma(H)} |D| \mu(D, H) \tilde{\theta}(s^{-1})(G/D)_s,$$

where $\tilde{\theta}$ is the sum of all distinct $N_G(H)$ -conjugates of θ . Then

$$\{e_{H,\theta} \mid H \in [G \backslash S(G)], \theta \in [N_G(H) \backslash \text{Irr}_{\mathbb{K}}(C_\Gamma(H))]\}$$

is a set of orthogonal idempotents of the crossed Burnside ring $\mathbb{K}X\Omega(G, \Gamma)$ over \mathbb{K} such that

$$(G/G)_{1_G} = 1_{\mathbb{K}X\Omega(G, \Gamma)} = \sum_{H, \theta} c_{H, \theta}.$$

Moreover, the idempotents $c_{H, \theta}$ are all primitive and conversely any primitive idempotent of $\mathbb{K}X\Omega(G, \Gamma)$ has this form.

A formula for the primitive idempotents of $\mathcal{O}X\Omega(G, G^c)$ over a p -local ring \mathcal{O} has been given by Bouc [Bo03b].

3 Bouc's constructions of Green functors

(3.1) Burnside Green functors. We recall the crossed Burnside ring Green functor $X\Omega(*, G^c)$ in terms of subgroups of G (see 4.1 of [OY04]). Let $S(H)$ be the family of all subgroups of $H \leq G$ and $C_G(D)$ the centralizer of $D \leq H$. Then the assignment

$$H(\leq G) \longmapsto X\Omega(H, G^c) = \langle (H/D)_s \mid D \in [H \setminus S(H)] \ s \in [H \setminus C_G(D)] \rangle_{\mathbb{Z}}$$

gives a Green functor for G over \mathbb{Z} equipped with

$$\begin{aligned} \text{ind}_L^H & : X\Omega(L, G^c) \longrightarrow X\Omega(H, G^c) & : (L/D)_s & \longmapsto (H/D)_s, \\ \text{res}_L^H & : X\Omega(H, G^c) \longrightarrow X\Omega(L, G^c) & : (H/D)_s & \longmapsto \sum_{g \in [L \setminus H/D]} (L/L \cap {}^g D)_{s_s}, \\ \text{con}_{H, g} & : X\Omega(H, G^c) \longrightarrow X\Omega({}^g H, G^c) & : (H/D)_s & \longmapsto ({}^g H/{}^g D)_{s_s}, \end{aligned}$$

where $D \leq L \leq H \leq G$ and $g \in G$. In order to note the Green functor structure of $X\Omega(*, G^c)$, we shall discuss briefly an equivalence between the category $G\text{-set} \downarrow_{(G/H \times G^c)}$ of finite G -sets over the G -set $G/H \times G^c$ (see 2.4 of [Bo97]) and the category $H\text{-set} \downarrow_{G^c}$ of finite H -sets over the H -set G^c with the H -action defined by conjugation. Let Ω be the Burnside Green functor for G over \mathbb{Z} in terms of G -sets. By Proposition 2.4.2 of [Bo97], $\Omega_{G^c}(G/H) = \Omega((G/H) \times G^c)$ is isomorphic to the Grothendieck group of $G\text{-set} \downarrow_{(G/H \times G^c)}$, with relations given by decomposition into disjoint union. It is easy to see that the G -sets

$$[K, s] : G/K \rightarrow G/H \times G^c : gK \mapsto (gH, {}^g s)$$

over $G/H \times G^c$, for $K \in [H \setminus S(H)]$ and $s \in [H \setminus C_G(K)]$, form a basis of $\Omega(G/H \times G^c)$ over \mathbb{Z} . We denote by $(G/K, [K, s])$ an element of the basis of $\Omega(G/H \times G^c)$. Theorem 5.1 of [Bo03a] shows that Ω_{G^c} is a Green functor. If $(G/K, [K, s])$ and $(G/L, [L, t])$ are elements of the basis of $\Omega(G/H \times G^c)$, then we have the following commutative diagram

$$\begin{array}{ccccc} \bigsqcup_{x \in K \setminus H/L} G/K \cap {}^x L & \xrightarrow{\cup_x \pi_{K \cap {}^x L} \times (\pi_{K \cap {}^x L} \circ \kappa \circ \pi_{K \cap {}^x L})} & G/K \times G/L & \xrightarrow{[K, s] \times [L, t]} & (G/H \times G^c) \times (G/H \times G^c) \\ \downarrow \cup_x [K \cap {}^x L, s \cdot {}^x t] & \text{P.B.} & \downarrow & & \downarrow f \\ G/H \times G^c & \xrightarrow{\delta_{G/H} \times 1_{G^c}} & G/H \times G/H \times G^c & \xrightarrow{id} & G/H \times G/H \times G^c. \end{array}$$

where the map f from $G/H \times G^c \times G/H \times G^c$ to $G/H \times G/H \times G^c$ maps $(xK, \gamma_1, yL, \gamma_2)$ to $(xK, yL, \gamma_1 \gamma_2)$ (see section 5 of [Bo03a]). The left square is a pullback square. Theorem

5.1 of [Bo03a] shows that the product of $(G/K, [K, s])$ and $(G/L, [L, t])$ on $\Omega(G/H \times G^c)$ is given by

$$(G/K, [K, s]) \cdot (G/L, [L, t]) = \sum_{x \in [K \setminus H/L]} (G/K \cap {}^x L, [K \cap {}^x L, s \cdot {}^x t]). \quad (3.1.1)$$

We have a functor F mapping $G\text{-set} \downarrow_{(G/H \times G^c)}$ to $H\text{-set} \downarrow_{G^c}$ defined for a transitive G -set $[K, s] : G/K \rightarrow G/H \times G^c$ over $G/H \times G^c$ by

$$F : (G/K, [K, s]) \mapsto \langle K, s \rangle : [K, s]^{-1}(\{H\} \times G^c) \rightarrow G^c$$

as in Lemma 2.4.1 of [Bo97]. We also denote by $[K, s]$ the H -map $H/K \rightarrow G^c$ defined by $gK \mapsto {}^g s$. It is clear that the H -sets

$$[K, s] : H/K \rightarrow G^c : gK \mapsto {}^g s$$

over the H -set G^c , for $K \in [H \setminus S(H)]$ and $s \in [H \setminus C_G(K)]$, form a basis of $\Omega \downarrow_H^G(G^c)$ over \mathbb{Z} , where $\Omega \downarrow_H^G$ is a Green functor for H given by the restriction to H of G . We denote by $(H/K, [K, s])$ this element of the basis of $\Omega \downarrow_H^G(G^c)$. It is easy to see that F gives an equivalence of categories from $G\text{-set} \downarrow_{(G/H \times G^c)}$ to $H\text{-set} \downarrow_{G^c}$ for any subgroup H of G . The inverse equivalence is given by the induction functor from $H\text{-set} \downarrow_{G^c}$ to $G\text{-set} \downarrow_{(G/H \times G^c)}$. The images of (3.1.1) under F are

$$(H/K, [K, s]) \cdot (H/L, [L, t]) = \sum_{x \in [K \setminus H/L]} (H/K \cap {}^x L, [K \cap {}^x L, s \cdot {}^x t]).$$

in $H\text{-set} \downarrow_{G^c}$. The Grothendieck group of $H\text{-set} \downarrow_{G^c}$ is isomorphic to $X\Omega(H, G^c)$. We can define a product

$$(H/K)_s \cdot (H/L)_t = \sum_{x \in [K \setminus H/L]} (H/K \cap {}^x L)_{s \cdot {}^x t}$$

for any two elements $(H/K)_s$ and $(H/L)_t$ of the basis of $X\Omega(H, G^c)$. It is clear that the element $(H/H)_{1_G}$ for the identity element 1_G of G is the identity element of $X\Omega(H, G^c)$. This gives a unitary ring structure to $X\Omega(H, G^c)$ for a subgroup H of G .

(3.2) Witherspoon's Green functor. Witherspoon introduced a Green functor $R_{\mathbb{C}}(D_G(\ast))$ for G over \mathbb{Z} (see [Wi96] Section 5). For each subgroup H of G , there is a subalgebra

$$D_G(H) = \sum_{g \in G, h \in H} \mathbb{C} \phi_g h$$

of the Drinfel'd (quantum) double $D(G)$ of $\mathbb{C}G$ [Dr86], where ϕ_g is an element of the basis $\{\phi_g\}_{g \in G}$ of the dual space $(\mathbb{C}G)^* = \text{Hom}_{\mathbb{C}}(\mathbb{C}G, \mathbb{C})$. Note that $D_{\mathbb{C}}(G) = D(G)$ and $R(D(G))$ is the representation ring of $D(G)$ or equivalently the Grothendieck ring of Hopf bimodules for the Hopf algebra $\mathbb{C}G$ ([Ro95], [Bo03a], [OY04]). Let $R_{\mathbb{C}}(D_G(H))$ be the Grothendieck (representation) ring of $D_G(H)$ for subgroup H of G . Then the assignment

$$H \longmapsto R_{\mathbb{C}}(D_G(H))$$

where $H \leq G$ gives a Green functor for G over \mathbb{Z} with operations given by

$$\begin{aligned} \text{Dres}_L^H & : R_{\mathbb{C}}(D_G(H)) \longrightarrow R_{\mathbb{C}}(D_G(L)) & : U & \longmapsto U \downarrow_{D_G(L)}, \\ \text{Dind}_L^H & : R_{\mathbb{C}}(D_G(L)) \longrightarrow R_{\mathbb{C}}(D_G(H)) & : V & \longmapsto D_G(H) \otimes_{D_G(L)} V, \\ \text{Dconj}_{H,g} & : R_{\mathbb{C}}(D_G(H)) \longrightarrow R_{\mathbb{C}}(D_G({}^g H)) & : U & \longmapsto {}^g U = g D_G(H) \otimes_{D_G(H)} U, \end{aligned}$$

where $U \downarrow_{D_G(L)}$ is a $D_G(L)$ -module by restriction of the action from $D_G(H)$ to $D_G(L)$, $L \leq H \leq G$ and $g \in G$. We use the equivalence of the category of H -vector bundles on G^c with the category of $D_G(H)$ -modules (see [Wi96] Section 2).

(3.3) A morphism of Green functors. Let Ω be the Burnside ring Green functor for G over \mathbb{Z} (see [Bo97] 2.4.2):

- If X is a finite G -set, then $\Omega(X)$ is the Grothendieck ring of the category of finite G -sets over X , where the relations are given by decomposition into disjoint union and product of G -sets.
- If $X \rightarrow X'$ is a G -map, then $\Omega_*(f) : \Omega(X) \rightarrow \Omega(X')$ is defined by $\Omega_*(f)((Y, \phi)) = (Y, f\phi)$ for any G -set $(Y, \phi) = Y \xrightarrow{\phi} X$ over X .
- If $X' \rightarrow X$ is a G -map, then $\Omega^*(f) : \Omega(X) \rightarrow \Omega(X')$ is defined by $\Omega^*(f)((Y, \phi)) = (Y', \phi')$, where (Y', ϕ') is the pull-back of (Y, ϕ) along f , obtained by filling the cartesian square

$$\begin{array}{ccc} Y' & \xrightarrow{a} & Y \\ \phi' \downarrow & & \downarrow \phi \\ X' & \xrightarrow{f} & X. \end{array}$$

Suppose that $R_{\mathbb{C}}$ is the \mathbb{C} -representation (character ring) Green functor for G over \mathbb{Z} , defined on subgroups of G . Then setting $R_{\mathbb{C}}(G/H) = R_{\mathbb{C}}(H)$ leads by linearity to a definition of G -equivariant \mathbb{C} -vector bundles $R_{\mathbb{C}}(X)$ on a G -set X (see [Wi96] Section 2) by using Remark 2.3 of [Bo03a]:

- If X is a finite G -set, then $R_{\mathbb{C}}(X)$ is the Grothendieck ring of the category of G -equivariant \mathbb{C} -vector bundles on the G -set X , for relations given by decomposition into direct sum of vector bundles, the ring structure being induced by the tensor product of vector bundles: one can set

$$R_{\mathbb{C}}(X) = \left(\bigoplus_{x \in X} R_{\mathbb{C}}(G_x) \right)^G$$

where the exponent denotes fixed points under the natural action of G on $\bigoplus_{x \in X} R_{\mathbb{C}}(G_x)$ by permutation of the components, and G_x is the stabilizer of x in G .

- If $f : X \rightarrow X'$ is a G -map, then $R_{\mathbb{C}*}(f) : R_{\mathbb{C}}(X) \rightarrow R_{\mathbb{C}}(X')$ is defined by

$$R_{\mathbb{C}*}(f)(u)_y = \sum_{x \in [G_y \backslash f^{-1}(y)]} t_{G_x}^{G_y}(u_x),$$

where $t_{G_x}^{G_y}$ is the induction map from $R_{\mathbb{C}}(G_x)$ to $R_{\mathbb{C}}(G_y)$, $u \in R_{\mathbb{C}}(X)$, and $y \in X'$.

- If $f : X' \rightarrow X$ is a G -map, then $R_{\mathbb{C}}^*(f) : R_{\mathbb{C}}(X) \rightarrow R_{\mathbb{C}}(X')$ is defined by

$$R_{\mathbb{C}}^*(f)(v)_x = r_{G_{f(x)}}^{G_x}(v_{f(x)}),$$

where $r_{G_{f(x)}}^{G_x}$ is the restriction map from $R_{\mathbb{C}}(G_x)$ to $R_{\mathbb{C}}(G_{f(x)})$, $v \in R_{\mathbb{C}}(X)$, and $x \in X'$.

- The product of the elements $a \in R_{\mathbb{C}}(X)$ and $b \in R_{\mathbb{C}}(Y)$ is defined by

$$(a \times b)_{x,y} = r_{G_{(x,y)}}^{G_x}(a_x) \cdot r_{G_{(x,y)}}^{G_y}(b_y).$$

If X is a finite G -set, denote the natural morphism

$$\theta : \Omega \rightarrow R_{\mathbb{C}}$$

of Green functors defined by the maps $\theta(X) : \Omega(X) \rightarrow R_{\mathbb{C}}(X)$ by

$$(Y, \varphi) = (\varphi : Y \rightarrow X) \mapsto \{\mathbb{C}[\varphi^{-1}(x)]\}_{x \in X},$$

where $\mathbb{C}[\varphi^{-1}(x)]$ is the permutation module associated to the G_x -set $\varphi^{-1}(x)$.

The following theorem is essential in the proof of Theorem 4.1 of this paper.

(3.4) Theorem (Bouc [Bo03a] 5.1). *Let A be a Green functor for G over a commutative ring \mathcal{O} , Γ a crossed G -monoid, and ε_A an element of $A(\bullet)$ such that for any G -set X and for any $a \in A(X)$*

$$A_*(p_X)(a \times \varepsilon_A) = a = A_*(q_X)(\varepsilon_A \times a)$$

denoting by p_x (resp. q_x) the bijective projection from $X \times \bullet$ (resp. from $\bullet \times X$) to X (see 1.2.1 of [Bo03a]). Then the functor A_{Γ} is a Green functor for G over \mathcal{O} , with unit $\varepsilon_{A_{\Gamma}}$,

where $\varepsilon_{A_{\Gamma}}$ is the element $A_* \left(\begin{smallmatrix} \bullet \\ 1 \\ \text{IC} \end{smallmatrix} \right) (\varepsilon_A)$ of $A(\Gamma) = A_{\Gamma}(\bullet)$. Moreover the correspondence $A \mapsto A_{\Gamma}$ is an endo-functor of the category of Green functors for G over \mathcal{O} .

(3.5) Lemma. *Let Ω be the Burnside ring Green functor and G^c the crossed G -monoid. Then there is an isomorphism of Green functors*

$$X\Omega(*, G^c) \cong \Omega_{G^c}.$$

PROOF: Let H be a subgroup of G . We set $\Omega_{G^c}(H) = \Omega_{G^c}(G/H) (= \Omega((G/H) \times G^c))$. By Bouc's Theorem (3.4), we have

$$\Omega((G/H) \times G^c) = \left(\bigoplus_{(aH,g) \in G/H \times G^c} \Omega(G_{aH,g}) \right)^G \cong \bigoplus_{(H,g) \in \mathcal{C} \setminus (G/H \times G^c)} \Omega(G_{H,g}),$$

where $G_{aH,g} = G_{aH} \cap G_g = {}^aH \cap C_G(g) = C_{{}^aH}(g)$. The map

$$f_H : X\Omega(H, G^c) \longrightarrow \left(\bigoplus_{(aH,g) \in G/H \times G^c} \Omega(G_{aH,g}) \right)^G$$

is defined for $(H/K)_s \in X\Omega(H, G^c)$ by

$$(H/K)_s \longmapsto ([K, s]^{-1}(aH, g))_{(aH, g) \in G/H \times G^c},$$

where the map $[K, s] : G/K \rightarrow G/H \times G^c$ is the G -map defined by $xK \mapsto (xH, {}^x s)$. It is well known that the natural projection $p_L^H : G/L \rightarrow G/H$ gives the induction $\Omega_{G^c}^*(p_L^H)$ and the restriction $\Omega_{G^c}^*(p_L^H)$. Moreover,

$$\gamma_{x, H} : G/H \rightarrow G/{}^x H : gx^{-1}xH = gHx^{-1}$$

gives the conjugation $\Omega_{G^c}^*(\gamma_{x, H})$. It is clear that the collection of homomorphisms of \mathbb{Z} -modules $f_H : X\Omega(H, G^c) \rightarrow \Omega_{G^c}(H)$ makes a morphism f from the Mackey functor $X\Omega(*, G^c)$ to the Mackey functor Ω_{G^c} , which commutes with restriction, induction and conjugation. Since f_H is the inverse of the homomorphism from $\Omega_{G^c}(H)$ to $X\Omega(H, G^c)$ obtained by the functor F of (3.1) and we defined the Green functor structure on $X\Omega(*, G^c)$ using Green functor structure on Ω_{G^c} , f_H is an isomorphism of rings for H .

Finally we have to check that the morphism f_H preserves the identity element. Recall from Theorem 5.1 of [Bo03a] that the identity element $\varepsilon_{\Omega_{G^c}}$ of the Green functor Ω_{G^c} is the element $\Omega_* \left(\begin{smallmatrix} \bullet \\ 1_G \end{smallmatrix} \right) (\varepsilon_\Omega)$ of $\Omega(G^c) = \Omega_{G^c}(\bullet)$. The identity element ε_Ω of the Burnside

Green functor Ω is the identity element \bullet of the Burnside ring $\Omega(G)$, so $\Omega_* \left(\begin{smallmatrix} \bullet \\ 1_G \end{smallmatrix} \right) (\varepsilon_\Omega)$ is the composition $\bullet \rightarrow \bullet \rightarrow G^c$: the identity element of the crossed Burnside ring $\Omega(G^c)$ (see 3.1 of [OY01] or 2.1 of [Bo03a]). Moreover, the identity element $(\varepsilon_{\Omega_{G^c}})_{G/H}$ of the ring $\Omega_{G^c}(G/H)$ is obtained by the formula (see 2.3 of [Bo97]) $(\varepsilon_{\Omega_{G^c}})_{G/H} = \Omega_{G^c}^*(\pi_H^G)(\varepsilon_{\Omega_{G^c}})$, where π_H^G is the natural projection $G/H \rightarrow G/G = \bullet$. The pull-back diagram

$$\begin{array}{ccc} G/H & \xrightarrow{\quad} & \bullet \\ \downarrow & & \downarrow \\ G/H \times G^c & \xrightarrow{\pi_H^G \times \text{id}_{G^c}} & \bullet \times G^c \end{array}$$

shows that $(\varepsilon_{\Omega_{G^c}})_{G/H}$ is the G -set $[H, 1_G] : G/H \rightarrow G/H \times G^c$ over $G/H \times G^c$. By the definition of f_H ,

$$f_H((H/H)_{1_G}) = ([H, 1_G]^{-1}(aH, \alpha))_{(aH, \alpha) \in G/H \times G^c}.$$

We have that $[H, 1_G]^{-1}(aH, \alpha)$ is the coset aH for $\alpha = 1_G$ and the empty set ϕ for all other elements, so f_H preserves the identity element, and this completes the proof of the lemma. \square

We will denote by $\mathbb{C}[X]$ the \mathbb{C} -permutation module associated to a set X . The endofunctor of the category of Green functors of Theorem (3.4) applied to the morphism θ from Ω to $R_{\mathbb{C}}$ leads to the following lemma.

(3.6) Lemma. *Let $\theta : \Omega \rightarrow R_{\mathbb{C}}$ be the natural morphism from the Burnside Green functor to the Grothendieck ring Green functor. Then the morphism $\theta_{G^c} : \Omega_{G^c} \rightarrow R_{\mathbb{C}G^c}$ given by the Bouc's construction is a morphism of Green functors.*

(3.7) **Lemma.** *There is a morphism*

$$\theta_{G^c} : X\Omega(\ast, G^c) \rightarrow R_{\mathbb{C}}(D_G(\ast))$$

of Green functors.

PROOF: Lemma (3.6) shows that there is a morphism θ_{G^c} of Green functors from Ω_{G^c} to $R_{\mathbb{C}G^c}$, whose evaluation at the transitive G -set G/H is the map

$$(\theta_{G^c})_{G/H} = \theta_{G/H \times G^c} : \Omega_{G^c}(G/H) = \Omega(G/H \times G^c) \rightarrow R_{\mathbb{C}}(G/H \times G^c) = R_{\mathbb{C}G^c}(G/H)$$

defined for the transitive G -set $[K, s] : G/K \rightarrow G/H \times G^c$ over $G/H \times G^c$ by

$$\left(\coprod_{aH \in G/H} [K, s]^{-1}(aH, \alpha) \right)_{\alpha \in G^c} \mapsto \left(\bigoplus_{aH \in G/H} \mathbb{C}[[K, s]^{-1}(aH, \alpha)] \right)_{\alpha \in G^c}.$$

The maps f_H of the proof of Lemma (3.5) and $\theta_{G/H \times G^c}$ induce maps

$$X\Omega(H, G^c) \xrightarrow{f_H} \Omega_{G^c}(G/H) \xrightarrow{\theta_{G/H \times G^c}} R_{\mathbb{C}G}(G/H)$$

for a subgroup H of G . The compositions $\theta_{G/H \times G^c} \circ f_H$ form a morphism of Green functors from $X\Omega(\ast, G^c)$ to $R_{\mathbb{C}G}(\ast)$. The isomorphism (see Remark 2.3 of [Bo03a])

$$\begin{aligned} R_{\mathbb{C}G^c}(G/H) &= \left(\bigoplus_{(aH, \alpha) \in G/H \times G^c} R_{\mathbb{C}}(G_{aH, \alpha}) \right)^G \\ &\rightarrow \bigoplus_{(H, \alpha) \in [G \setminus (G/H \times G^c)]} R_{\mathbb{C}}(G_{H, \alpha}) = \bigoplus_{(H, \alpha) \in [G \setminus (G/H \times G^c)]} R_{\mathbb{C}}(C_H(\alpha)) \end{aligned}$$

defined by

$$(U_{aH, \alpha})_{(aH, \alpha) \in G/H \times G^c} \mapsto (U_{H, \alpha})_{(H, \alpha) \in [G \setminus (G/H \times G^c)]}$$

and Theorem 2.4 of [Wi96] induce an isomorphism of Green functors $R_{\mathbb{C}G^c} \cong R(D_G(\ast))$, and complete the proof of the lemma. \square

Let $(H/L)_g$ be an element of the basis of $X\Omega(H, G^c)$. Then the previous lemma shows that $\theta_{G^c}((H/L)_g)$ is an H -vector bundle on G^c . We denote by $[H/L]_g$ this H -vector bundle. Lemma (3.5) shows the following lemma.

(3.8) **Lemma.** *The H -vector bundle $[H/L]_g$ is the $\mathbb{C}C_H(\ast g)$ -module $\mathbb{C}[[\ast L, \ast g]^{-1}(\ast g)]$ in the $\ast g$ -component, for $x \in [H/C_H(g)]$, and 0 in all other components.*

We recall the maps $\text{Incl}_{J, h} : R_{\mathbb{C}}(J) \rightarrow R_{\mathbb{C}}(D_G(J))$, where J is a subgroup of G and $h \in C_G(J)$, introduced in Section 2 of [Wi96]: Given a $\mathbb{C}J$ -module V , $\text{Incl}_{J, h}(V)$ is the $D_G(J)$ -module which is V in the h -component and 0 elsewhere.

(3.9) Lemma. *Let θ_{G^c} be the ring homomorphism $\theta_{(G/G) \times G^c}$ from the crossed Burnside ring $X\Omega(G, G^c)$ to the Grothendieck ring $R_{\mathbb{C}}(D_G(G))$ given by the previous lemma. Then the $D(G)$ -module corresponding to the G -vector bundle $\theta_{G^c}((G/L)_g)$ is the induced module*

$$D(G) \otimes_{D_G(L)} \text{Incl}_{L,g}(\mathbb{C}[L/L]).$$

PROOF: By the previous lemma, the ring homomorphism θ_{G^c} assigns to a transitive crossed G -set $(G/L)_g$ the G -vector bundle $[G/L]_g$ which is $\mathbb{C}[[{}^xL, {}^xg]^{-1}({}^xg)] \cong \mathbb{C}[C_G({}^xg)/{}^xL]$ as $\mathbb{C}C_G({}^xg)$ -modules in the xg -component for $x \in [G/C_G(g)]$ and 0 in all other components. Section 2 of [Wi96] shows that the $\mathbb{C}D_G(G)$ -module corresponding to the G -vector bundle $[G/L]_g$ is the induced module

$$D(G) \otimes_{D_G(C_G(g))} \text{Incl}_{C_G(g),g}(\mathbb{C}[C_G(g)/L]).$$

Since $L \leq C_G(g)$ and $g \in C_G(C_G(g))$, we have

$$\text{Incl}_{C_G(g),g} \circ \text{Ind}_L^{C_G(g)} = \text{Dind}_L^{C_G(g)} \circ \text{Incl}_{L,g}$$

by Lemma 5.4 of [Wi96]. Finally, we see that

$$\begin{aligned} D_G(G) \otimes_{D_G(J)} \text{Incl}_{J,g}(\mathbb{C}[J/L]) &\cong D(G) \otimes_{D_G(J)} \text{Incl}_{J,g} \circ \text{Ind}_L^J(\mathbb{C}[L/L]) \\ &\cong D(G) \otimes_{D_G(J)} \text{Dind}_L^J \circ \text{Incl}_{L,g}(\mathbb{C}[L/L]) \\ &\cong D(G) \otimes_{D_G(J)} D_G(J) \otimes_{D_G(L)} \text{Incl}_{L,g}(\mathbb{C}[L/L]) \\ &\cong D(G) \otimes_{D_G(L)} \text{Incl}_{L,g}(\mathbb{C}[L/L]), \end{aligned}$$

where $J = C_G(g)$. □

(3.10) Sub-Green functors. There is a sub-Green functor $X\Omega(*, G^c)_1$ which assigns to each subgroup H of G the subring $X\Omega(H, G^c)_1$ of $X\Omega(H, G^c)$ generated by the elements $(H/L)_{1_G}$. There is also a sub-Green functor $R_{\mathbb{C}}(D_G(*))_1$ which assigns to each subgroup H of G the subring $R_{\mathbb{C}}(D_G(H))_1$ of $R_{\mathbb{C}}(D_G(H))$ generated by $\text{Incl}_{H,1_G}(V)$'s, where $\text{Incl}_{H,1_G}$ is a functor embedding the category of $\mathbb{C}H$ -modules as a full subcategory of the category of $D_G(H)$ -modules (see, [Wi96] Section 1) and V is a $\mathbb{C}H$ -module. It is easy to see that $X\Omega(H, G^c)_1$ is isomorphic to the Burnside ring $\Omega(H)$ and $R_{\mathbb{C}}(D_G(H))_1$ is isomorphic to the ordinary character ring $R_{\mathbb{C}}(H)$. The homomorphism $\theta_{G^c} \downarrow_{X\Omega(H, G^c)_1}$ is the natural ring homomorphism from $\Omega(H)$ to $R_{\mathbb{C}}(H)$.

(3.11) Characters. Witherspoon pointed out the character of a $\mathbb{C}D(G)$ -module in [Wi96], that appeared in [Lu87]. For $g \in G$ and an irreducible character ρ of $C_G(g)$, a character $\chi_{g,\rho}$ of a $\mathbb{C}D(G)$ -module $U = \{U_h\}_{h \in G^c}$ is given by the formula

$$\chi_{g,\rho}(U) = \frac{1}{\text{deg } \rho} \sum_{h \in C_G(g)} \text{Tr}(g, U_h) \rho(h).$$

The characters of the crossed Burnside ring have been considered by Oda and Yoshida ([OY01], Section 5). For a subgroup H of G and an irreducible character θ of $C_G(H)$, the linear map $\omega_{H,\theta}$ of $X\Omega(G, G^c)$ to \mathbb{C} is the composite of Burnside homomorphism φ_H and a central character $\tilde{\omega}_{H,\theta}$: given a crossed G -set X over G^c , $H \leq G$, and an irreducible character ρ of the group algebra $\mathbb{C}C_G(H)$, $\omega_{H,\rho}(X) = \tilde{\omega}_{H,\rho} \circ \varphi_H(X)$.

For each $h \in G^c$ the h -component of the crossed G -set (X, α) is defined by

$$X[h] = \{x \in X \mid \alpha(x) = h\}.$$

(3.12) **Lemma.** *Let g be an element of G , ρ an irreducible character of $\mathbb{C}C_G(g)$, and θ_{G^c} the homomorphism from $X\Omega(G, G^c)$ to $R_{\mathbb{C}}(D(G))$. Then $\chi_{g,\rho}\theta_{G^c} = \omega_{(g),\rho}$, where $\langle g \rangle$ is the cyclic subgroup generated by g .*

PROOF: Let $(G/L)_s$ be a transitive crossed G -set over G^c . Then 3.11 shows that

$$\begin{aligned}
 \omega_{(g),\rho}((G/L)_s) &= \sum_{xL \in (G/L)^{(g)}} \frac{\rho(x)}{\rho(1_G)} \\
 &= \sum_{h \in C_G(g)} |G/L[h]^{(g)}| \cdot \frac{\rho(h)}{\rho(1_G)} \\
 &= \frac{1}{\deg \rho} \sum_{h \in C_G(g)} \#\{xL \in (G/L)^{(g)} \mid x^r s = h\} \rho(h) \\
 &= \frac{1}{\deg \rho} \sum_{h \in C_G(g)} \text{Tr}(g, ([G/L]_s)_h) \rho(h) \\
 &= \chi_{g,\rho}([G/L]_s) \\
 &= \chi_{g,\rho}(\theta_{G^c}((G/L)_s)).
 \end{aligned}$$

□

4 Induction theorems

The proof of the following theorem is similar to the proof of Theorem 3.5.2 in [Bo00].

(4.1) **Theorem.** *Let G be a finite group. Then*

$$\mathbb{C}R_{\mathbb{C}}(D(G)) = \sum_{H \in \mathcal{C}(G)} \text{Dind}_H^G \mathbb{C}R_{\mathbb{C}}(D_G(H)),$$

where $\mathcal{C}(G)$ is the family of cyclic subgroups of G . In other words, any complex character of $D(G)$ is a linear combination with rational coefficients of characters induced from cyclic groups of G .

PROOF: It suffices to show that the left hand side is contained in the right hand side. There is a natural homomorphism θ_{G^c} from the crossed Burnside ring $X\Omega(G, G^c)$ to the Grothendieck ring $R_{\mathbb{C}}(D(G))$ by Lemma 3.8. This extends to a homomorphism of \mathbb{C} -algebra from $\mathbb{C}X\Omega(G, G^c)$ to $\mathbb{C}R_{\mathbb{C}}(D(G))$.

Let H be a subgroup of G and s an element of G . Let $e_{H,\psi}$ be the primitive idempotent corresponding to a \mathbb{C} -irreducible character ψ of $C_G(H)$ (see Theorem 2.3). Since a character $\omega_{(s),\rho}$ of $\mathbb{C}X\Omega(G, G^c)$ is the composite of a central character $\tilde{\omega}_{(s),\rho}$ and a Burnside homomorphism $\varphi_{(s)}$ (see 3.11), $\omega_{(s),\rho}(e_{H,\psi}) = 0$ if H is not conjugate in G to the cyclic subgroup $\langle s \rangle$ generated by s . Lemma 3.12 implies that $\chi_{s,\rho}(\theta_{G^c}(e_{H,\psi})) = 0$, and it follows that $\theta_{G^c}(e_{H,\psi})$ in $\mathbb{C}R_{\mathbb{C}}(D(G))$ is zero unless H is cyclic. If H is cyclic, by Lemma 3.9, $\theta_{G^c}(e_{H,\psi})$ is a linear combination with coefficients of induced $\mathbb{C}D(G)$ -modules $D(G) \otimes_{D_{\mathbb{C}}(L)} \text{Incl}_{L,s}(\mathbb{C}[L/L])$, for a subgroup L of the cyclic group H . Let

$$(G/G)_{1_G} = \sum_{H \in \mathcal{C}(G \setminus \{G\})} \sum_{\psi \in \mathcal{N}_G(H) \setminus \text{Irr}(C_G(H))} e_{H,\psi}$$

be the decomposition of the unit element of $\mathbb{C}X\Omega(G, G^c)$. Then Lemma 3.8 shows that $\theta_{G^c}((G/G)_{1_G})$ is the unit of $\mathbb{C}R_{\mathbb{C}}(D(G))$ and $\theta_{G^c}((G/G)_{1_G})$ is a linear combination with \mathbb{C} -coefficients of such induced modules $D(G) \otimes_{D_G(L)} \text{Incl}_{L,g}(\mathbb{C}[L/L])$, which are induced from cyclic subgroups L of G . Then if U is any $D(G)$ -module

$$U \otimes \text{Incl}_{L,s}(\mathbb{C}[L/L]) \uparrow^{D_G(G)} \cong (U \downarrow_{D_G(L)} \otimes \text{Incl}_{L,s}(\mathbb{C}[L/L])) \uparrow^{D_G(G)}$$

by Lemma 5.2 of [Wi96]. Therefore, the theorem follows by the unitarity of θ_{G^c} . \square

The previous theorem and (3.10) show the following corollary.

(4.2) Corollary (Artin). *Let G be a finite group. Then*

$$\mathbb{Q}R_{\mathbb{C}}(G) = \sum_{H \in \mathcal{C}(G)} \text{Ind}_H^G \mathbb{Q}R_{\mathbb{C}}(H).$$

References

- [Bo97] S. BOUC, *Green functors and G-sets*, Lecture Notes in Mathematics, vol. 1671, Springer, 1997.
- [Bo00] S. BOUC, Burnside rings, in *Handbook of Algebra*, Vol. 2, Elsevier Science B.V. (2000), 439–804.
- [Bo03a] S. BOUC, Hochschild constructions for Green functors, *Comm. Algebra*, **31** (2003), 419–453.
- [Bo03b] S. BOUC, The p -blocks of the Mackey algebra, *Algebras and Representation Theory*, **6** (2003), 515–543.
- [Dr73] A.W.M. DRESS, *Contributions to the theory of induced representations*, Lecture Notes in Math., **342**, Springer-Verlag, Berlin, 1973, 183–240.
- [Dr86] V. G. DRINFEL'D, Quantum groups, in *Proceedings International Congress of Mathematicians*, Berkeley, pp. 798–820, American Mathematical Society, Providence, Rhode Island, 1986.
- [Lu87] G. LUSZTIG, Leading coefficients of character values of Hecke algebras, *Proc. Symp. Pure. Math.* **47** (1987), 235–262.
- [OY01] F. ODA AND T. YOSHIDA, Crossed Burnside rings I. The Fundamental Theorem, *J. Algebra* **236** (2001), 29–79.
- [OY04] F. ODA AND T. YOSHIDA, Crossed Burnside rings II. The Dress construction of a Green functor, *J. Algebra* **282** (2004), 58–82.
- [Ro95] M. ROSSO, Groupes quantiques et algèbres de battage quantiques, *C. R. Acad. Sc. Paris* **320** (1995), 145–148.
- [Th88] J. THÉVENAZ, Some remarks on G -functors and the Brauer morphism, *J. Reine Angew. Math.* **384** (1988), 24–56.

- [TW95] J. THÉVENAZ AND P. WEBB, The structure of Mackey functors, *Trans. Amer. Math. soc.* **347** (6) (1995), 1865–1961.
- [We00] P. WEBB, A guide to Mackey functor, In *Handbook of Algebra* Vol. 2, Elsevier Science B.V. (2000), 805–836.
- [Wi04] S.J.WITHERSPOON, Products in Hochschild cohomology and Grothendieck rings of group crossed products, *Adv. Math.* **185** (2004), 136–158.
- [Wi96] S.J.WITHERSPOON, The representation ring of the quantum double of a finite group, *J. Algebra* **179** (1996), 305–329.

Uniqueness of maximum three-distance sets in the three-dimensional Euclidean space

篠原雅史 (九州大学数理学府, COE 研究員)
shino@math.kyushu-u.ac.jp

1 序文

与えられた空間における有限個の点の配置として、どのようなものがよい配置であるかを考えることは、組合せ論における研究テーマの一つである。大雑把に言ってしまえば、符号理論においては多くの点をできるだけ最小距離が大きくなるように配置することを目標としていて、デザイン理論においては少ない点で空間を近似することを目標としている。同様に距離集合においては、多くの点をできるだけでくる距離（相異なる二点間の距離）の種類を少なくなるように配置することを目標としている。

まず始めに、距離集合 (distance set) に関する定義を与える。

\mathbb{R}^d を d 次元ユークリッド空間とする。 \mathbb{R}^d 上の有限部分集合 X に対し $A(X) = \{PQ : P, Q \in X, P \neq Q\}$ とする。ここで、 PQ は二点 P, Q 間のユークリッド距離を表す。 X が k -距離集合 (distance set) であるとは、 $|A(X)| = k$ のとき、つまり X の相異なる二点間の距離がちょうど k 種類ででくるときをいう。一つの k -距離集合が与えられたとき、それを平行移動・拡大・縮小・回転などの変換で移したのもまた k -距離集合となる。そのため、相似変換で移りあう二つの距離集合を同型とし、以後同一視して考える。

本報告書では、二節で距離集合について知られていることや予想などを紹介し、今回の主結果を述べる。三節で条件付きで今回の主結果が正しいことを見る。四節では有限部分集合に対し直径グラフ (diameter graph) を定義し、二次元・三次元における直径グラフの特徴付けを行う。五節で今後の研究課題、特に locally distance set について述べる。

2 距離集合

\mathbb{R}^d 上の k -距離集合の頂点数が上からバウンドされることは容易に確認できる。ここでその最大値を $g_d(k)$ とする。最大値の上限として次の定理が知られている。

k	1	2	3	4	5	6
$g_2(k)$	3	5	7	9	12	13(?)

平面上の k -距離集合の最大頂点数

d	1	2	3	4	5	6	7	8
$g_d(2)$	3	5	6	10	16	27	29	45

\mathbb{R}^d 上の 2-距離集合の最大頂点数

Theorem 1. (坂内-坂内-Stanton [3], Blokhuis [4], 1983)

$$g_d(k) \leq \binom{d+k}{k}.$$

$g_d(k)$ について, $g_1(k) = k + 1$, $g_d(1) = d + 1$ となっていることは容易に確かめられる. つまり $d = 1$ または $k = 1$ のときには上のバウンドの等号を満たす場合になっている.

$d = 2$ のとき $k \leq 5$ に対し, また $k = 2$ のとき $d \leq 8$ に対し最大値が求められている. (知られている最大値を上表に記す.) 分類についてはそれぞれ $k \leq 5$, $d \leq 7$ に対しなされている. ([2], [5], [9], [12], [13], [15], [16])

$d = 2$ のとき Erdős-Fishburn [9] は次の予想をしている.

Conjecture 1. (Erdős-Fishburn)

$g_2(6) = 13$ となる. また $k \geq 3$ とすると, $L_\Delta = \{a(1, 0) + b(1/2, \sqrt{3}/2) : a, b \in \mathbb{Z}\}$ の部分集合で $g_2(k)$ 点からなる k -距離集合が存在する. 特に $k \geq 7$ とすると, $g_2(k)$ 点からなる k -距離集合は L_Δ の部分集合に限られる.

このように $d \leq 2$ または $k \leq 2$ のときはいくつか知られている結果があるが, $d \geq 3$ かつ $k \geq 3$ の場合, 最小のケース $g_3(3)$ すら求められていない状況であった. このとき Einhorn-Schoenberg [7] は次のような予想をしていた.

Conjecture 2. (Einhorn-Schoenberg, 1966)

三次元ユークリッド空間上の 12 点からなる 3-距離集合は, 正二十面体の 12 点に限られる. 特に $g_3(3) = 12$.

この予想に対し次のような部分的な結果が得られていた.

Theorem 2. (篠原 [17])

(i) 三次元ユークリッド空間上の 14 点からなる 3-距離集合は存在しない. 特に $12 \leq g_3(3) \leq 13$.

(ii) 球面 S^2 上の 12 点からなる 3-距離集合は, 正二十面体の 12 点に限られる.

本報告書では [17] の方法を改良し, Einhorn-Schoenberg の予想を (肯定的に) 示すことを目標とする.

3 5 点からなる 2-距離集合を含む 3-距離集合

Einhorn-Schoenberg [7] は \mathbb{R}^3 上の 5 点からなる 2-距離集合を分類している. そのようなものは, 正五角形の 5 点 R_5 を含めて 27 個ある. (平面上の 5 点 2-距離集合は R_5 に限られる.) この節では 5 点からなる 2-距離集合を含む 12 点 3-距離集合について考える. 特に次の命題について紹介する.

Proposition 1. 三次元ユークリッド空間上の 12 点からなる 3-距離集合で, 5 点からなる 2-距離集合を含むものは, 正二十面体の 12 点に限られる.

この命題を確かめるためには, 27 個の 5 点 3-距離集合 Y それぞれに対して, Y を含むような 12 点 3-距離集合が存在するかどうか確かめればよい. $Candi(Y)$ で $Y \cup \{P\}$ が高々 3-距離集合であるような点 $Q \in \mathbb{R}^3$ 全体の集合とする. このとき次の補題が成り立つ.

Lemma 1. Y を \mathbb{R}^3 上の 5 点からなる 2-距離集合で $Y \neq R_5$ とする. このとき $Candi(Y)$ のすべての点は計算可能で, 特に $|Candi(Y)| < +\infty$.

Proof. $P \in Candi(Y)$ に対し, $Old(P) = \{Q \in Y \mid PQ \in A(Y)\}$, $New(P) = \{Q \in Y \mid PQ \notin A(Y)\}$, また $Type(P) = |New(P)|$ と定める. $Type(P)$ によって次のように場合わけして考える.

(i) $Type(P) \leq 2$ のとき $\{Q_1, Q_2, Q_3\} \subset Old(P)$ とする. このとき $PQ_i \in A(Y)$ より, このような P は高々 $2 \cdot 2^3$ 点ある.

(ii) $Type(P) = 3, 4$ のとき $\{Q_1, Q_2, Q_3\} \subset New(P)$, $Q' \in Old(P)$ とする. また L を三角形 $Q_1Q_2Q_3$ の外接円の中心を通り, 三点 Q_1, Q_2, Q_3 によって定まる平面に直行するような直線とする. このとき P は L 上にあり $PQ' \in A(Y)$ となっているので, そのような P は高々 4 点ある.

(iii) $Type(P) = 5$ のとき Y は同一平面上にないので P は Y のすべての点を通る球の中心になければならない. よってこのような P は高々 1 点ある.

以上により, $|Candi(Y)| \leq \binom{5}{3} \cdot 16 + \binom{5}{3} \cdot \binom{2}{1} \cdot 4 + 1$.

また $Candi(Y)$ のすべての点を計算することができることもわかる. □

最後に $Candi(Y)$ の点を組み合わせてどのような 12 点 3-距離集合ができるかを確かめれば, そのような 12 点 3-距離集合は正二十面体の 12 点になることがわかる. また $Y - R_5$ のときも上の場合に帰着できることが示せるので, 上の命題が成り立つことが確かめられる.

この命題により予想の解決のためには, 12 点からなる 3-距離集合が 5 点からなる 2-距離集合を含んでいることを示せばよいことがわかる.

次節でこのことを示す.

4 直径グラフ

直径グラフを定義する前にグラフに関する基本的な定義を復習する. ここでは単純グラフのみを扱う. C_n, P_n でそれぞれ n 点からなるサイクル, パスとする. グラフ G の頂点 $v \in V(G)$ に対し, $\Gamma_i(v) = \{w \in V(G) : d(v, w) = i\}$ と定める. ここで $d(v, w)$ は v と w の距離を表す. 特に $i = 1$ のとき $\Gamma(v)$ と省略し, $|\Gamma(v)|$ を頂点 v の次数といい $deg(v)$ で表す. 二点 $v, w \in V(G)$ が隣接しているとき $v \sim w$ と表す. $H \subset V(G)$ の任意の二点が隣接していないとき H を G の独立集合という. G における独立集合の頂点数の最大値を $\alpha(G)$ で表し, G の独立数という.

次に $X \subset \mathbb{R}^d$ に対し, 直径と直径グラフを定義する. $X \subset \mathbb{R}^d$ ($|X| < \infty$) に対し, $D(X) = \max A(X)$ とし X の直径とよぶ. X の直径グラフ $G = DG(X)$ を頂点集合を X 自身とし, 二点 P, Q 間の距離が X の直径となっているとき P, Q を結んだグラフ, つまり $V(G) = X, P, Q \in X$ に対し, $PQ = D(X)$ のとき $P \sim Q$ としたグラフとする.

Example. $R_n = \{\text{正 } n \text{ 角形の頂点}\}$ とする. このとき,

$$DG(R_{2m+1}) = C_{2m+1}, \quad DG(R_{2m}) = m \cdot P_2.$$

Remark 1. X を k -距離集合とする. $DG(X)$ の独立集合 Y に対し, 明らかに $A(Y) \subset A(X)$, 更に $D(X) \notin A(Y)$ となっているので, Y は高々 $(k-1)$ -距離集合となる.

平面上の直径グラフに対しては, 次の命題が成り立つ.

Proposition 2. $X \subset \mathbb{R}^2$ に対し $G = DG(X)$ とするとき,

- (i) G は偶数サイクル C_{2k} を含まない;
- (ii) G が奇数サイクル C_{2k+1} を含むとき, $V(G) \setminus V(C_{2k+1})$ の任意の二点は隣接していない.

特に, G は高々一つのサイクルを持つ.

上の命題より、平面上の直径グラフの独立数を次のように評価することができる。

Corollary 1. $X \subset \mathbb{R}^2$ ($|X| = n$) に対し $G = DG(X)$ とする。 $\alpha(G) \geq \lfloor \frac{n}{2} \rfloor$ となる。更に $G \neq C_n$ のとき、 $\alpha(G) \geq \lfloor \frac{n}{2} \rfloor$ となる。

三次元の場合、次の定理が知られている。

Theorem 3. (Dol'nikov [6])

X を \mathbb{R}^3 上の有限部分集合とし、その直径グラフを G とする。 G が異なる二つの奇数サイクル C, C' を含むとき、 C と C' は共通の頂点を持つ。つまり $V(G) \cap V(C') \neq \emptyset$ 。

この命題より明らかに次の系が成り立つ。

Corollary 2. $X \subset \mathbb{R}^3$, $|X| \geq 12$ に対し、 $G = DG(X)$ とする。 G が C_3 を含むとする。このとき $G - C_3$ は二部グラフになる。特に $\alpha(G) \geq 5$ 。

Remark 2. 上の系より、直径グラフとして 3-サイクルを含まないものを考えればよいことがわかる。 [17] では上の系を Dol'nikov とは独立に示した。この系によりラムゼー数 $R(3, 5) = 14$ を用いると、 $X \subset \mathbb{R}^3$ ($|X| \geq 14$) に対し $DG(X)$ が 3-サイクルを含まない場合についても $\alpha(DG(X)) \geq 5$ が成立する。このことにより Theorem 2 が示せることになる。Dol'nikov の定理より、更に三次元有限部分集合の直径グラフは相異なる二つの 5-サイクルを含まないことを用いると次の命題が示せる。

Proposition 3. $X \subset \mathbb{R}^3$, $|X| = 12$ とするとき、 $\alpha(DG(X)) \geq 5$ となる。

Proof. G を $|V(G)| = 12$ となるグラフで 3-サイクルを含まないとする。 $\alpha(G) < 5$ のとき、 G が相異なる二つの 5 サイクルを含むことを示せばよい。

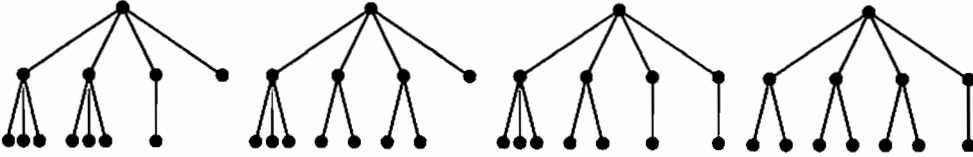
Claim 上の仮定のもとで次が成り立つ。

- (i) 任意の頂点 v に対して $3 \leq \deg(v) \leq 4$;
 - (ii) $\deg(v_0) = 4$ となる $v_0 \in V(G)$ が存在する。
- (Claim の証明は [17] を参考にして下さい。)

Claim より $\deg(v_0) = 4$ となる $v_0 \in V(G)$ が存在する。 $w \in \Gamma_3(v_0)$ となる $w \in V(G)$ が存在するとすると、 $\Gamma_2(v_0) \cup \{w\}$ は 5 点からなる独立集合になるので、 $\Gamma_3(v_0) = \emptyset$ 。よって $|\Gamma_2(v_0)| = 7$ 。ここで次のような 7 の分割を考える。 $m_1 + m_2 + m_3 + m_4 = 7$, $m_i \in \{0, 1, 2, 3\}$ ($m_1 \geq m_2 \geq m_3 \geq m_4$) とすると、 $(m_1, m_2, m_3, m_4) \in \{(3, 3, 1, 0), (3, 2, 2, 0), (3, 2, 1, 1), (2, 2, 2, 1)\}$ 。

よって G は下図のいずれかを部分グラフとして含む。

Case A (3, 3, 1, 0) Case B (3, 2, 2, 0) Case C (3, 2, 1, 1) Case D (2, 2, 2, 1)



ここでは Case A の場合のみ示す。

$\Gamma(v_0) = \{v_1, v_2, v_3, v_4\}$, $\Gamma_2(v_0) = \{v_5, v_6, \dots, v_{11}\}$ とする。更に $\{v_5, v_6, v_7\} \subset \Gamma(v_1)$, $\{v_8, v_9, v_{10}\} \subset \Gamma(v_2)$, $\{v_{11}\} \subset \Gamma(v_3)$ とする。

$\{v_2, v_3, v_5, v_6, v_7\}$ は独立集合ではないので, $v_3 \sim v_j$ となる $j \in \{5, 6, 7\}$ が存在する。よって一般性を失うことなく $v_3 \sim v_7$ としてよい。同様に $v_3 \sim v_8$ と仮定してよい。また $\{v_2, v_3, v_4, v_5, v_6\}$ は独立集合ではないので $v_4 \sim v_5$ とできる。同様に $v_4 \sim v_{10}$ と仮定してよい。 v_4 の次数は高々 4 なので, $v_4 \sim v_8, v_4 \sim v_9$ としてよい。

(a) $v_4 \sim v_{11}$ のとき, $\{v_1, v_4, v_8, v_9, v_{11}\}$ は独立集合ではないので, $v_9 \sim v_{11}$ となっている。また $\{v_0, v_5, v_6, v_7, v_{10}\}$ は独立集合でないので, $v_i \sim v_{10}$ となる $i \in \{6, 7\}$ が存在する。このとき共通頂点を持たない 2 つの 5-サイクル $v_0 \sim v_4 \sim v_{10} \sim v_i \sim v_1 \sim v_0$ と $v_3 \sim v_8 \sim v_2 \sim v_9 \sim v_{11} \sim v_3$ が存在する。

(b) $v_4 \sim v_{11}$ のとき, $\{v_0, v_5, v_6, v_7, v_{11}\}$ は独立集合でないので $v_6 \sim v_{11}$ となっている。また $\{v_0, v_5, v_7, v_8, v_{11}\}$ は独立集合でないので $v_5 \sim v_8$ 。このとき共通頂点を持たない 2 つの 5-サイクル $v_0 \sim v_4 \sim v_5 \sim v_8 \sim v_2 \sim v_0$ と $v_1 \sim v_7 \sim v_3 \sim v_{11} \sim v_6 \sim v_1$ が存在する。よって Case A のとき命題は正しい。

他の Case の場合にも同様に示せる。

□

この命題より次の系が成り立つ。

Corollary 3. 三次元ユークリッド空間上の 12 点からなる k -距離集合は, 5 点からなる $(k-1)$ 距離集合を含む。

5 最後に

三節と四節の命題により今回の主結果である次の定理が示せる。

Theorem 4. 三次元ユークリッド空間における 3-距離集合で 12 点からなるものは, 正二十面体の 12 点と同型である。特に, $g_3(3) = 12$ 。

一般に少ない頂点数の距離集合を分類する方が難しい問題となる。11 点の 3-距離集合についてこれまで知られているものは正二十面体の頂点の 11 点部分集合だけであるので、自然に次の問題が考えられる。

Problem 1. 三次元ユークリッド空間における 3-距離集合で 11 点からなるものは、正二十面体の 12 点の部分集合と同型になるか？

ここで距離集合の定義を拡張した *locally distance set* を次のように定義する。

$P \in X \subset \mathbb{R}^d$ に対し $(A(P) =) A_X(P) = \{PQ : Q \in X, P \neq Q\}$ とする。 X が *locally k -distance set* であるとは、任意の点 $P \in X$ に対して $|A_X(P)| \leq k$ のときをいう。定義より明らかに、 k -距離集合なら *locally k -distance set* となることがわかる。距離集合の場合と同様に \mathbb{R}^d 上の *locally k distance* の頂点数が上からバウンドされることは容易に確認できる。ここでその最大値を $g'_d(k)$ とする。

$k = 2$ の場合にはいくつか結果が得られている ([14])。

Theorem 5.

$$g'_d(2) \leq \max\{g_d(2), f(d)\}$$

ここで、

$$f(d) = \max_{1 \leq i \leq d-1} \{g_i(2) + g'_{d-i}(2)\}$$

この定理により、2-距離集合の結果を用いると、次の表のように $d \leq 8$ に対して最大値が求まる。ここで $d = 3$ の場合を除いては、2-距離集合の頂点数の最大値 $g_d(2)$ と一致していることに注意しておく。

d	1	2	3	4	5	6	7	8
$g'_d(2)$	3	5	7	10	16	27	29	45

また頂点数が十分大きいとき、次の系が成り立つ。

Corollary 4. $\binom{d+2}{2}$ 点以上持つような \mathbb{R}^d ($d \geq 2$) 上の *locally 2-distance set* は、2-距離集合になる。特に $g'_d(2) \leq \binom{d+2}{2}$ 。

Remark 3. 一般の k に対して *locally k -distance set* の頂点数の上限が、距離集合の場合と同様に $g'_d(k) \leq \binom{d+k}{k}$ で与えられると思われるが今のところ成功していない。

一方, 平面上の locally 3-distance set に対して, $g_2'(3) = 8$ となりその配置が一意に定まることが, Fishburn [11] より確かめられる.

Problem 2. 三次元ユークリッド空間における locally 3 distance set で 12 点からなるものは, 正二十面体の 12 点と同型であるか?

参考文献

- 1 E. Altman, On a problem of P. Erdős, Amer. Math. Monthly (1963) 148-157.
- 2 E. Bannai and E. Bannai, 球面上の代数的組合せ理論, シュプリンガー・フェアラーク東京, 1999.
- 3 E. Bannai, E. Bannai, and D. Stanton, An upper bound for the cardinality of an s -distance subset in real Euclidean space, II, Combinatorica 3 (1983), 147-152.
- 4 A. Blokhuis, Few-distance sets, Ph. D. thesis, Eindhoven Univ. of Technology (1983), (CWI Tract (7) 1984).
- 5 H. T. Croft, 9-point and 7-point configuration in 3-space, Proc. London. Math. Soc. (3), 12 (1962), 400-424.
- 6 V. Dol'nikov, Some properties of graphs of diameters, Discrete Comput. Geom. 24 (2000), 293-299.
- 7 S. J. Einhorn and I. J. Schoenberg, On Euclidean sets having only two distances between points I, II, Nederl Akad. Wetensch. Proc. Ser. A69=Indag. Math. 28 (1966), 479-504.
- 8 P. Erdős and P. Fishburn, Convex nonagons with five intervertex distance, Geometriae Dedicata 60 (1996) 317-332.
- 9 P. Erdős and P. Fishburn, Maximum planar sets that determine k distances, Discrete Math, 160 (1996) 115-125.
- 10 P. Fishburn, Convex polygons with few intervertex distance, Computation Geometry: Theory and Applications 5 (1995) 65-93.
- 11 P. Fishburn, A remarkable eight point planar configuration, Discrete Math, 252 (2002) 103-122.

- 12 L. M. Kelly, Elementary Problems and Solutions. Isosceles n -points, Amer. Math. Monthly, 54 (1947), 227-229.
- 13 P. Lisoněk, New maximal two-distance sets, J. Comb. Theory, Ser. A77 (1997), 318-338.
- 14 H. Nozaki and M. Shinohara, On locally distance sets, 準備中.
- 15 M. Shinohara, Classification of three-distance sets in two dimensional Euclidean space, Europ. J. Combinatorics, 25 (2004) 1039-1058.
- 16 M. Shinohara, Uniqueness of maximum planar five-distance sets, to appear in Discrete Math.
- 17 M. Shinohara, On three-distance sets in the three-dimensional Euclidean space, 第23回代数的組合せ論シンポジウム報告集, 301-305.

Galois Group on Elliptic Curves and Flavor Symmetry

松岡武夫（皇學館大学）

（服部忠・朗、松永守、中西健一氏との共同研究に基づく）

1 はじめに

現在、素粒子物理学における未解決の重要な課題としてフレーバー対称性とクォーク・レプトンの世代構造の解明がある。現在の素粒子物理学では、物質を構成する基本粒子は、クォーク、レプトン、ヒッグス粒子それにゲージ粒子と考えられている。これらの粒子が従う基本法則は、素粒子の標準模型、即ち、 $SU(3)_c \times SU(2)_L \times U(1)_Y$ ゲージ理論で記述されるとされている。実際、クォーク、レプトンとゲージ粒子との相互作用に関しては、現在までのところ標準模型から導かれる結果は高い精度で実験と一致しており、標準模型は成功している。ところが、ヒッグス粒子が関与する相互作用の特徴については、標準模型は予言能力を持たない。その特徴とは、まず、クォーク・レプトンの種類（フレーバーの自由度）とその質量スペクトルに関するものである。クォーク・レプトンにはそれぞれ2個づつ対になって3組あり、これを3世代というが、これらクォーク・レプトンの質量はニュートリノまで含めると、10桁以上の違いがあり、階層的な構造をしている。また、世代間には状態混合が起きており、この状態混合にも特別なパターンが見られる。これらの世代構造の背後には、特別な離散対称性があると考えられる。

一方、力の統一理論を目指した自然なモデルの構築を考えたとき、boson と fermion の対称性である超対称性の導入が求められる。ところが、超対称性を導入すると、そのままでは、陽子崩壊の問題など観測事実と矛盾する相互作用を導いてしまう。これを解決するには、Rパリティと呼ばれる Z_2 対称性を禁止則として追加する必要がある。これらの離散対称性をまとめて、フレーバー対称性という。現時点ではこのフレーバー対称性を解明するための理論的指導原理は未だ見いだされていない。今日までに、フレーバー対称性に関して多くの試みがあるが、それらはフレーバー対称性としてある対称性を試行的に導入し、実験事実に近い

結果を再現できるかどうかを個別に調べている段階に留まっている。そこで、我々はフレーバー対称性の解明の理論的指針を超弦理論の数論的構造に求める新しいアプローチを提案する。

超弦理論は、現時点で最も優れた統一理論である。この理論では、時空は10次元で、この内の4次元は我々の知る時空である。残る6次元空間は、プランク・サイズ (10^{-33}cm) 程度のコンパクト空間(余次元空間)と考えられる。超弦理論から導かれる低エネルギー有効理論が超対称性を持つとの要請から、この余次元空間はカラビ・ヤウ多様体や orbifold であろうと考えられる。この余次元空間の幾何学やトポロジーが、フレーバー対称性を含めた低エネルギー有効理論の構造に強く反映すると考えるのは自然であろう。

2 フレーバー対称性の起源

1987年に Gepner は超弦理論と2次元の有理共形場理論との関係、また、カラビ・ヤウ多様体の幾何学との関係も議論した。さらに、有理共形場理論は有限次代数体と密接な関係にある。実際、有理共形場理論における融合則はある可換環を与え、その可換環は融合則によって定まる代数体の整数環と同型となる。従って、カラビ・ヤウ多様体の幾何学は有限次代数体に関する数論を用いて調べることができる。

非摂動的弦理論においては、有理共形場理論は D-brane (boundary state , Cardy state) を自然に導く。この D-brane は、有理共形場理論に対応する幾何学を持ったカラビ・ヤウ多様体上の部分多様体として実現する。そこで、簡単なモデルとして、我々は2つの D-brane の交差する空間が $M_4 \times E_\Lambda$ であるとし、 $M_4 \times E_\Lambda$ 上の有効理論を考える。 M_4 は4次元時空、楕円曲線 E_Λ は余次元空間の部分である。ここで、格子 Λ は、基本周期を ω_1, ω_2 とする \mathbb{C} 上の格子である。

有理共形場理論はモジュラー変換性を通して楕円曲線と結び付いている。より具体的には、中心電荷 $c=2$ の2次元トーラス上の有理共形場理論を与えると、これに対応して2次元トーラスを表す楕円曲線が定まり、しかも、この楕円曲線は虚数乗法 (complex multiplication, CM) を持つ。(Gukov-Vafa) 従って、カラビ・ヤウ多様体が虚数乗法をもつ楕円曲線をその部分多様体として含んでいる時は、その楕円曲線の数論的

構造は有効理論の特徴に強く反映すると考えられる。こうして、虚数乗法をもつ楕円曲線の数論的構造を通してフレーバー対称性の起源とその特徴を解明する手掛かりも得られると期待できる。

$M_4 \times E_\Lambda$ 上の理論を考えたとき、D-brane 描像ではクォーク・レプトン超場とヒッグス超場は共に E_Λ 上に端点を持つ orientable の開いた弦として表される。このとき、開いた弦の端点は D-brane 内 (E_Λ 内) の方向には自由端であり、開いた弦は E_Λ から E_Λ への写像と見ることができる。ところで、 E_Λ 上には自己同型写像が存在する。そこで、我々は、 E_Λ から E_Λ への自己同型の自由度は物理的には開いた弦のフレーバーの自由度であるとの解釈を提案する。より具体的には、虚数乗法をもつ楕円曲線 E_Λ の自己同型群として、 E_Λ 上の m -torsion point : $E_\Lambda[m]$ から導かれるガロア群を考える。そして、このガロア群こそフレーバー対称性であると解釈する。

3 虚数乗法をもつ楕円曲線

格子 Λ と 1 対 1 に対応する楕円曲線 E_Λ は、次の複素解析的写像を通して定義される。

$$\mathbb{C}/\Lambda \longrightarrow E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \quad (1)$$

$$z \longmapsto (x, y) = (\wp(z; \Lambda), \wp'(z; \Lambda)) \quad (2)$$

ここで、 $\wp(z; \Lambda)$ は Weierstrass の \wp 関数である。 g_2, g_3 は Eisenstein 級数 $G_{2k}(\Lambda)$ で次のように書ける。

$$g_2(\Lambda) = 60 G_4(\Lambda), \quad g_3(\Lambda) = 140 G_6(\Lambda) \quad (3)$$

y を $2y$ と置き換え、 $g_2(\Lambda) = -4A$ 、 $g_3(\Lambda) = -4B$ と書くと、以下で楕円曲線の標準形として用いる次の形が得られる。

$$E_\Lambda : y^2 = f(x) = x^3 + Ax + B \quad (4)$$

格子 Λ に対して相似変換 $\Lambda \longrightarrow \lambda\Lambda$ 、 $\lambda \in \mathbb{C}^*$ を行ったとき、係数 A 、 B は $A \longrightarrow \lambda^{-4}A$ 、 $B \longrightarrow \lambda^{-6}B$ と変換される。よって、楕円曲線 E_Λ は、 \mathbb{C} 同型を用いて類別される。この類別された楕円曲線 $\{E\}$ の代表元として基底を正規化した格子 $\Lambda_\tau = \{\mathbb{Z} + \mathbb{Z}\tau\}$ で定まる楕円曲線を

採用することができる。ここで、2次元トーラスの complex structure moduli τ は複素平面の上半面 $H = \{\tau \in \mathbb{C}; \text{Im } \tau > 0\}$ で定義されるが、モジュラー変換の自由度があるために格子 Λ_τ を指定しても τ は一意的には定まらない。しかし、 H をモジュラー群で割った商空間、即ち、基本領域 $\mathcal{F} = \{\tau \in H; |\tau| \geq 1, |\text{Re } \tau| \leq \frac{1}{2}\}$ に τ の値をとれば、 τ と格子とは1対1に対応する。

次に、虚数乗法について述べる。一般に、同型 $\text{End}(E_\Lambda) \simeq \text{End}(\mathbb{C}/\Lambda)$ が成り立つので、 E_Λ 上の自己同型は、 \mathbb{C}/Λ 上のそれを通して調べることができる。有理共形場理論に対応する楕円曲線においては、共形場理論の rationality の結果として E_Λ 上の自己同型には、 m 倍写像 ($m \in \mathbb{Z}_+$) の他に、虚数乗法が存在する。即ち、 $\mu\Lambda \subset \Lambda$ を満たす複素数 $\mu (\notin \mathbb{R})$ が存在する。虚数乗法をもつ楕円曲線 E_Λ では、 τ は整係数の2次方程式の根であり、その2次方程式の判別式 D は負となる。そこで、有理数体 \mathbb{Q} の代数的拡大体として E_Λ に伴う虚2次体 $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\tau)$ が定義される。即ち、 E_Λ は K による虚数乗法を持つ。中心電荷 $c = 2$ の2次元トーラス上の有理共形場理論が定める楕円曲線 E_Λ は K による虚数乗法を持つだけでなく、2次元トーラスのサイズ・パラメーターである Kähler class moduli ρ も体 K に値をとる。

楕円曲線 E_Λ の標準モジュライ・パラメーター (重さ0のモジュラー関数) である j -不変量 $j(E_\Lambda)$ は τ だけの関数であるので、 $j(\tau)$ とも表される。虚数乗法を持つ楕円曲線 E_Λ においては、 $j(E_\Lambda)$ は代数的整数となり、 $\mathbb{Q}(j(E_\Lambda))$ が $\{E_\Lambda\}$ の最小定義体となる。楕円曲線 E_Λ の \mathbb{C} 同型による類別は、 $j(E_\Lambda)$ と1対1対応しており、さらに、虚2次体 K の整数環 R_K のイデアル類群と同型である。 R_K のイデアル類群の元の個数 h_K は K の類数と呼ばれ、 $\mathbb{Q}(j(E_\Lambda))/\mathbb{Q}$ の拡大次数は、類数 h_K に等しい。ここで、我々は

$$j(E_\Lambda) \in \mathbb{Q} \tag{5}$$

を仮定し、これを標準モジュライ・パラメーター $j(E_\Lambda)$ の量子仮説と呼ぶ。この量子仮説の下では、虚2次体 K の類数は1となる。このとき、適当な相似変換により楕円曲線 E_Λ は \mathbb{Q} 上で定義できて、標準形 $f(x)$ の係数は $A, B \in \mathbb{Z}$ ととれる。この仮説は楕円曲線 E_Λ の形の量子化に相当する。

4 楕円曲線上のガロア群

E_Λ の自己同型群は、 E_Λ のねじれ点を体 $K(j(E_\Lambda))$ に添加したガロア拡大体 L を導入することにより得られる。ところで、有理共形場理論は、その融合則が定める点の集合である fusion variety 上で定義され、有理共形場理論が定める余次元空間は楕円曲線 E_Λ 上の離散化された点の集合となる。そこで、我々は、楕円曲線 E_Λ 上のこの離散化された点の集合は E_Λ のねじれ点と解釈する。 E_Λ のねじれ点 $E_\Lambda[\mathfrak{a}]$ は、 R_K の整イデアル \mathfrak{a} に対応して

$$E_\Lambda[\mathfrak{a}] = \{ P \in E_\Lambda \mid \alpha \in \mathfrak{a}, \alpha P = \mathcal{O} \} \quad (6)$$

で定義され、 \mathcal{O} は楕円曲線 E_Λ 上の加法群の零元である。ここでは、 R_K の整イデアルとして $\mathfrak{a} = m R_K$ ($m \in \mathbb{Z}_+$) を採用し、 E_Λ の m ねじれ点 (m 等分点) $E_\Lambda[m]$ を考える。 $E_\Lambda[m]$ は2つの m 次巡回群の直和と同型である。この場合、余次元空間 E_Λ のサイズの最小単位は $m^{-1}\Lambda$ の基本平行四辺形で定まる空間である。この最小単位の空間のサイズは、弦理論の基本的スケール、即ち、プランク・スケール程度と考えるのが自然である。なお、上記の量子仮説 $j(E_\Lambda) \in \mathbb{Q}$ により $K(j(E_\Lambda)) = K$ である。

そこで、 E_Λ の全てのねじれ点 $E_\Lambda[m]$ の全ての座標で生成される K のガロア拡大体 $L = K(E_\Lambda[m])$ を考える。この拡大体 L は興味深い特殊な性質を持つ。実際、 L/K のガロア群 $H = \text{Gal}(L/K)$ を導き、 H はアーベル群となる。さらに、 L は \mathbb{Q} のガロア拡大体でもあり、 L/\mathbb{Q} のガロア群

$$G = \text{Gal}(L/\mathbb{Q}) \quad (7)$$

が導かれる。 G は核 H による $\mathbb{Z}_2 = \text{Gal}(K/\mathbb{Q})$ の拡大であり、 H は G の正規部分群である。 G は多くの場合、非アーベル群となる。開いた弦の自由度は E_Λ から E_Λ への自己同型の自由度、即ち、ガロア群 $G = \text{Gal}(L/\mathbb{Q})$ の元と対応関係を持つ。

次に L/K のガロア群 H の性質に注目する。 \mathbb{C}/Λ 上の m 等分点の内、加群に関して位数 m の点の個数を F とする。ここで、位数 m の点の集合は

$$\{ u \mid u \in \mathbb{C}/\Lambda, mu \in \Lambda, m'u \notin \Lambda \text{ for } m' < m \} \quad (8)$$

で与えられる。 H の任意の元は、 C/Λ 上の位数 m の点を位数 m の点に移す。 ここで、 $m = 2$ のとき $F = 3$ 、 $m > 2$ では $F = \text{even}$ である。 E_Λ 上の m 等分点の内の位数 m の点の x 座標は、 \mathbb{Q} 上の方程式

$$\psi_m(x) = \prod_u (x - \wp(u)) = 0 \quad (9)$$

の根として与えられる。 ここで、積は、 $m = 2$ のとき C/Λ 上の位数 2 の点 $F = 3$ 個についてとり、 $m > 2$ では Weierstrass の \wp 関数が偶関数であることから、 $F/2$ 個についてとる。 従って、この多項式 $\psi_m(x)$ の次数は、 $m = 2$ のとき 3、 $m > 2$ では $F/2$ である。

j -不変量と m を指定したとき、 \mathbb{Q} 上の楕円曲線 E_Λ を変えると、 K のアーベル拡大体 $L = K(E_\Lambda[m])$ が変わり、それに伴って L/K のガロア群 H も変化する。 このとき、ガロア群 H の位数 $\#H$ は、拡大次数 $[L : K]$ に等しく、その最大値は F である。 位数 $\#H$ が最大値 F をとるには、多項式 $\psi_m(x)$ が、 \mathbb{Q} 上で既約であることが必要である。 一般に、多項式 $\psi_m(x)$ が \mathbb{Q} 上で既約であるときは、 $(\#H) | F$ となる。 これに対して、 $\psi_m(x)$ が \mathbb{Q} 上で可約であるときは、 $\#H$ は F より小さいだけでなく、 $\#H$ は F の約数とは限らない。

虚数乗法をもつ楕円曲線の具体例として、 $-D = 1, 3$ 、即ち、 Λ_τ がガウスの整数環 $\mathbb{Z}[i]$ 、及び $\mathbb{Z}[\omega]$ である場合をとり、それぞれの場合について $E_\Lambda[m]$ から導かれるガロア群 G を調べる。 ここで、 $\omega = \exp(2\pi i/3)$ である。 この場合、 $g_3(\mathbb{Z}[i]) = 0$ 、 $g_2(\mathbb{Z}[\omega]) = 0$ であるので、 $j(E_\Lambda)$ の値は、其々 1728、0 である。 いずれも $j \in \mathbb{Q}$ であるから、 Λ_τ が $\mathbb{Z}[i]$ と $\mathbb{Z}[\omega]$ の E_Λ は \mathbb{Q} 上で定義された楕円曲線 $y^2 = x^3 + x$ 、 $y^2 = x^3 + 1$ にそれぞれ \mathbb{C} 同型である。 ガロア拡大体およびガロア群の構造を調べるために、以下では、 $y^2 = x^3 + x$ 、 $y^2 = x^3 + 1$ に \mathbb{C} 同型な \mathbb{Q} 上の次の楕円曲線を考える。

$$E_\Lambda : y^2 = x^3 + Ax, \quad A \in \mathbb{Z} \quad (10)$$

$$E_\Lambda : y^2 = x^3 + B, \quad B \in \mathbb{Z} \quad (11)$$

まず、楕円曲線 $E_\Lambda : y^2 = x^3 + 1$ 上の $m = 3$ ねじれ点 (3 等分点) を例にとり、この場合のガロア群 $\text{Gal}(K(E_\Lambda[3])/\mathbb{Q})$ を調べる。 この場合のガロア拡大体は $L = K(E_\Lambda[3]) = \mathbb{Q}(\omega, \sqrt[3]{4})$ 、 L/K のガロア群 H は $H = \mathbb{Z}_3$ となる。 $m = 3$ のとき $F = 8$ であるが、 $E_\Lambda : y^2 = x^3 + 1$

における $\psi_3(x)$ は \mathbf{Q} 上の可約な多項式である。その結果、 $\sharp H = 3$ 、 $(\sharp H) \nmid F$ となっている。ガロア表現 $Gal(K(E_\Lambda[3])/Q) \rightarrow GL_2(\mathbf{Z}/3\mathbf{Z})$ をとると、

$$\eta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod{3} \quad (12)$$

となる。このとき、関係式

$$\eta^2 = \sigma^3 = 1, \quad \eta\sigma\eta = \sigma^{-1}. \quad (13)$$

が成り立つので、ガロア群 G は

$$G = Gal(\mathbf{Q}(E_\Lambda[3])/Q) = \mathbf{Z}_2 \times \mathbf{Z}_3 = D_3 \quad (14)$$

である。

第2の例として楕円曲線 $E_\Lambda : y^2 = x^3 + x$ 上の $m = 3$ ねじれ点 (3等分点) のガロア群 $Gal(K(E_\Lambda[3])/Q)$ を調べる。ガロア拡大体は $L = K(E_\Lambda[3]) = \mathbf{Q}(i, \beta_{1-})$ 、 L/K のガロア群 H は $H = \mathbf{Z}_8$ となる。

ここで、 $\beta_{1-} = \sqrt{\sqrt{3}-1} (2/\sqrt{27})^{1/4}$ 。この場合、 $\psi_3(x)$ は \mathbf{Q} 上の既約多項式であり、 $\sharp H = F = 8$ である。ガロア表現 $Gal(K(E_\Lambda[3])/Q) \rightarrow GL_2(\mathbf{Z}/3\mathbf{Z})$ をとると、

$$\eta = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix} \pmod{3} \quad (15)$$

となる。このとき、関係式

$$\eta^2 = \sigma^8 = 1, \quad \eta\sigma\eta = \sigma^3 \quad (16)$$

が成り立つので、ガロア群 G は

$$G = Gal(\mathbf{Q}(E_\Lambda[3])/Q) = \mathbf{Z}_2 \times \mathbf{Z}_8 \quad (17)$$

である。

表1、2に、それぞれ $y^2 = x^3 + Ax$ 、 $y^2 = x^3 + B$ における $A, B = 1, 2$ 、 $m = 2, 3, 4$ の場合のガロア拡大体 $L = K(E_\Lambda[m])$ およびガロア群 $G = Gal(L/Q)$ をまとめた。ガロア群 G はアーベル群である H を核とした \mathbf{Z}_2 の拡大である。 \mathbf{Z}_2 の拡大として可能なガロア群には、多くのタイプがある。具体例で見たように、 G にはアーベル群の場合と非アーベル群の場合がある。ガロア群 G の可能な非アーベル群としては、2面体群 D_n ($n \geq 3$) はあるが、対称群 S_n ($n \geq 4$) の可能性はない。

表 1: Galois Groups on $E_\Lambda : y^2 = x^3 + Ax$

E_Λ	$y^2 = x^3 + x$	$y^2 = x^3 + 2x$
$L = K(E_\Lambda[2])$ $G = Gal(L/Q)$	$Q(i)$ Z_2	$Q(\sqrt{2}i)$ Z_2
$L = K(E_\Lambda[3])$ $G = Gal(L/Q)$	$Q(i, \beta_{1-})$ $Z_2 \times Z_8$	$Q(i, \beta_{2-})$ $Z_2 \times Z_8$
$L = K(E_\Lambda[4])$ $G = Gal(L/Q)$	$Q(i, \sqrt{2})$ $Z_2 \times Z_2$	$Q(i, \sqrt[4]{2})$ D_4

表 2: Galois Groups on $E_\Lambda : y^2 = x^3 + B$

E_Λ	$y^2 = x^3 + 1$	$y^2 = x^3 + 2$
$L = K(E_\Lambda[2])$ $G = Gal(L/Q)$	$Q(\omega)$ Z_2	$Q(\omega, \sqrt[3]{2})$ D_3
$L = K(E_\Lambda[3])$ $G = Gal(L/Q)$	$Q(\omega, \sqrt[3]{4})$ D_3	$Q(\omega, \sqrt{2})$ $Z_2 \times Z_2$
$L = K(E_\Lambda[4])$ $G = Gal(L/Q)$	$Q(\omega, \sqrt[4]{27}/\sqrt{2})$ D_4	$Q(\omega, \sqrt[3]{2}, \sqrt[4]{27})$ $Z_2 \times (Z_2 \times Z_2 \times Z_3)$

5 $SU(6) \times SU(2)_R$ 模型への適用

$H = Gal(L/K)$ の具体例として $Z_4 \times Z'_4 \times Z_N$ ($N = \text{odd}$) をとり、核 H による Z_2 の拡大である非可換のガロア群

$$G = Gal(L/Q) = Z_2 \times (Z_4 \times Z'_4) \times Z_N \quad (18)$$

をフレーバー対称性として採用する。ここで、ガロア群 G の生成子をそれぞれ $\tau, \sigma_1, \sigma_2, \omega$ と書くと、

$$\tau \sigma_i \tau = \sigma_i^{-1} \quad (i = 1, 2), \quad \tau \omega \tau = \omega, \quad (19)$$

で、 $\sigma_1, \sigma_2, \omega$ は互いに可換である。また、2種類の D-brane の一方は $SU(6)$ のゲージ自由度を持ち、他方の D-brane は $SU(2)_R$ のゲージ自

由度を持っているとする。そこで、上記のガロア群 G をフレーバー対称性として持つ $SU(6) \times SU(2)_R$ model を考える。

$SU(6) \times SU(2)_R$ model のゲージ対称性に関わる主な特徴は、以下の通りである。

1. ゲージ群 $SU(6) \times SU(2)_R$ は、 E_6 群の maximal subgroup の一つで、超弦理論から導くことができる。このゲージ群から標準模型ゲージ群への自発的破れは、高次元表現の場を追加せずに E_6 の基本表現の物質場だけを用いてヒッグス機構により実現する。
2. 物質場は、次のように3世代の E_6 の基本表現と一組の vector-like set から成る。

$$3 \times 27(\Phi_{1,2,3}) + (27(\Phi_0) + \overline{27}(\bar{\Phi})), \quad (20)$$

E_6 の基本表現 27 のカイラル超場 Φ は、次のように $G = SU(6) \times SU(2)_R$ の既約表現に分解される。

$$\Phi(27) = \begin{cases} \phi(15, 1) : & Q, L, g, g^c, S, \\ \psi(6^*, 2) : & (U^c, D^c), (N^c, E^c), (H_u, H_d), \end{cases} \quad (21)$$

クォークとレプトン、それにヒッグス粒子はここに含まれている。

物質超場のフレーバー対称性に関する charge assignment の議論に移る。まず、 $Gal(K/Q) = \mathbf{Z}_2$ を R パリティと同一視する。R パリティは、共役な対を持つ物質超場と持たない物質超場とを区別する量子数である。一方、虚数乗法をもつ楕円曲線上の共役な自己同型変換は、 K が虚 2 次体であることから、ガロア群 G の部分群である $Gal(K/Q) = \mathbf{Z}_2$ である。従って、 $Gal(K/Q) = \mathbf{Z}_2$ を R パリティと同一視する。

次に、 $Gal(L/K) = H = \mathbf{Z}_4 \times \mathbf{Z}'_4 \times \mathbf{Z}_N$ の部分の charge assignment に移る。quark/lepton の質量スペクトルと混合角の世代構造を再現する解は $N = 31$ 、 $N = 35$ などの場合に存在する。これらの解は、フレーバー対称性とゲージ対称性との mixed anomaly-free 条件をも満足するものである。表 3 に $N = 31$ の場合の charge assignment を掲げる。ここで、 q_θ は Grassmann 数 θ の charge である。 $N = 31$ の場合のガロア群 G を導く m ねじれ点は、 $m = 311$ のときである。また、 $N = 35$ の場合のガロア群 G を導く m ねじれ点は、 $m = 41$ のときである。これらの m の値は、超弦理論における基本的な長さを単位としたときのコンパクト空間 E_3 のサイズを表していると解釈される。

表 3: $\mathbf{Z}_2 \times (\mathbf{Z}_4 \times \mathbf{Z}'_4) \times \mathbf{Z}_N$ -charge $q_\theta = (-, 1, 1, 1)$

	$\phi(15, 1)$	$\psi(6^*, 2)$
Φ_0	(+, 0, 2, 18)	(+, 2, 1, 12)
$\bar{\Phi}$	(+, 0, 1, 18)	(+, 1, 0, 27)
Φ_1	(-, 0, 2, 0)	(-, 2, 2, 21)
Φ_2	(-, 0, 2, 20)	(-, 2, 2, 9)
Φ_3	(-, 0, 2, 29)	(-, 2, 2, 18)

6 まとめ

虚数乘法をもつ楕円曲線の数論的構造を通して、クオーク・レプトンの質量と混合角の世代構造の背後にあるフレーバー対称性を解明する新しいアプローチを提案した。有理共形場理論、代数的整数論、それに虚数乘法をもつ楕円曲線の間には非常に密接な関係がある。我々は、2種類の D-brane の intersection が $M_4 \times E_\Lambda$ を与え、開いた弦は E_Λ 上の自己同型を表しているとし、さらに、 E_Λ 上の自己同型群こそフレーバー対称性であるとの仮説を導入した。クオーク・レプトンの質量と混合角の世代構造を説明する具体的なフレーバー対称性として、ガロア群 $G = \mathbf{Z}_2 \times (\mathbf{Z}_4 \times \mathbf{Z}'_4) \times \mathbf{Z}_N$ を採用し、 $N = 31$ 、 $N = 35$ の場合に現実的な解を見出した。

参考文献

- D. Gepner, Phys. Lett. **B199** (1987) 380; Nucl. Phys. **B296** (1988) 757.
 S. Gukov and C. Vafa, Commun. Math. Phys. **246** (2004) 181.
 D. Gepner, hep-th/0606081 (2006).
 J. H. Silverman, "The Arithmetic of Elliptic Curves",
 Springer-Verlag, New York, 1986.
 J. H. Silverman, "Advanced Topics in the Arithmetic of Elliptic Curves",
 Springer-Verlag, New York, 1994.

Type II codes over Galois rings

上武大学・別宮耕・(Koichi Betsumiya)

1 導入

符号を分類する際、考えうる符号を列挙し、それらがすべてであることを数え上げ公式等で確認し、分類を完成させるという方法が一般的である。本講演では、ガロア環上の第二型符号の分類を完成させる際に必要な数え上げ公式について議論する。数え上げ公式の決定問題では、当然、特定の長さの数え上げ公式を完全に決定することが期待されるが、現時点では数え上げ公式は完成していない。ただし、符号の分類を完成させるためには、完全な数え上げ公式は必要でなく、ある種の条件を満たす部分集合ごとに個数が求まれば目的は達成できる。今回はその目的のために使える程度に定式化することができたため、そこまでを紹介することとする。

通常の符号と呼ばれているものは、素体上の符号が一般的である。その拡張として重要と考えられているものに、一般の有限体上の符号と、整数剰余環上の符号がある。講演者は、ガロア環上の符号について強い興味を持っているが、その理由として、これらの2つの一般化はガロア環上の符号として統合できることをあげることができる。

2 準備

2.1 ガロア環

p を素数とする。正の整数 m, f に対して、位数を p^{mf} 、標数を p^m とする主イデアル環の構造は一意に定まる。そのような環を $\text{GR}(p^m, f)$ と表わし、位数 p^{mf} 、標数 p^m のガロア環と呼ぶ。特に $m = 1$ のとき、 $\text{GR}(p, f)$ は位数 p^f の有限体 \mathbb{F}_{p^f} となり、 $f = 1$ のとき、 $\text{GR}(p^m, 1)$ は標数 p^m の整数剰余環 $\mathbb{Z}/p^m\mathbb{Z}$ となる。このことから分るとおり、ガロア環は有限体と標数が素数中の整数剰余環の概念を統合したものとなっている。

$\text{GR}(p^m, f)$ の部分集合 $\mathcal{T}(p^m, f) = \{x \in \text{GR}(p^m, f) \mid x^{p^f} = x\}$ を $\text{GR}(p^m, f)$ の Teichmüller 集合と呼ぶ。 $\mathcal{T}(p^m, f)$ は $\text{GR}(p^m, f)/p\text{GR}(p^m, f) \simeq \text{GR}(p, f) = \mathbb{F}_{p^f}$ の代表系となっており、任意の $u \in \text{GR}(p^m, f)$ に対して、 $u_0, \dots, u_{m-1} \in \mathcal{T}(p^m, f)$ が一意に定まり、 $u = u_0 + pu_1 + p^2u_2 + \dots + p^{m-1}u_{m-1}$ と表すことができる。

2.2 ガロア環上の符号

n 個のガロア環 $\text{GR}(p^m, f)$ の直和 $\text{GR}(p^m, f)^n$ は $\text{GR}(p^m, f)$ 加群であるが、その部分加群のことを長さ n の符号と呼ぶ。

整数剰余環上の符号と同様、ガロア環上の符号も、適当な座標の置換を施すことで、次のような生成行列を持つ。

$$\begin{pmatrix} I_{k_0} & A_{0,1,0} & A_{0,2,0} + pA_{0,2,1} & A_{0,3,0} + pA_{0,3,1} + p^2A_{0,3,2} & \dots & A_{0,t,0} + pA_{0,t,1} + \dots + p^{t-1}A_{0,t,t-1} \\ 0 & pI_{k_1} & pA_{1,2,1} & pA_{1,3,1} + p^2A_{1,3,2} & \dots & pA_{1,t,1} + \dots + p^{t-1}A_{1,t,t-1} \\ 0 & 0 & p^2I_{k_2} & p^2A_{2,3,2} & \dots & p^2A_{2,t,2} + \dots + p^{t-1}A_{2,t,t-1} \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & \dots & \dots & p^{t-1}A_{t-1,t,t-1} \end{pmatrix}$$

ただし、 I_{k_i} は k_i 次の単位行列で、 $A_{a,b,c}$ は成分を $T(p^m, f)$ とする $k_a \times k_b$ 行列とする。このような符号を $(k_0, k_1, \dots, k_{t-1}, k_t)$ 型の符号と呼ぶ。なお、 $k_t = n - \sum_{i=0}^{t-1} k_i$ とする。

2.3 自己双対符号、自己直交符号

$\text{GR}(p^m, f)^n$ の通常のユークリッド内積として $c = (c_1, \dots, c_n), d = (d_1, \dots, d_n)$ に対して、 $c \cdot d = c_1d_1 + \dots + c_nd_n$ と表すこととする。

符号 C に対して、 C の双対符号を $C^\perp = \{x \in \text{GR}(p^m, f)^n \mid x \cdot c = 0 \text{ for all } c \in C\}$ と定義し、 $C = C^\perp$ となるものを自己双対符号と呼び、 $C \subset C^\perp$ となるものを自己直交符号と呼ぶ。前述のような (k_0, k_1, \dots, k_t) 型符号の双対符号は次のような生成行列を持つ。

$$\begin{pmatrix} B_{0,t,0} + pB_{0,t,1} + \dots + p^{t-1}B_{0,t,t-1} & \dots & B_{0,3,0} + pB_{0,3,1} + p^2B_{0,3,2} & B_{0,2,0} + pB_{0,2,1} & B_{0,1,0} & I_{k_t} \\ pB_{1,t,1} + \dots + p^{t-1}B_{1,t,t-1} & \dots & pB_{1,3,1} + p^2B_{1,3,2} & pB_{1,2,1} & pI_{k_{t-1}} & 0 \\ p^2B_{2,t,2} + \dots + p^{t-1}B_{2,t,t-1} & \dots & p^2B_{2,3,2} & p^2I_{k_{t-2}} & 0 & 0 \\ \vdots & & & & & \vdots \\ p^{t-1}B_{t-1,t,t-1} & \dots & 0 & 0 & 0 & 0 \end{pmatrix}$$

すなわち、 C^\perp は $(k_t, k_{t-1}, \dots, k_1, k_0)$ 型符号となる。このことから、 (k_0, k_1, \dots, k_t) 型符号が自己双対符号となるためには、 $i = 0, \dots, t$ について、 $k_i = k_{t-i}$ となる必要がある。

2.4 ねじれ符号と剰余符号

まず、写像 ι, π を次のように定義する。

$$\begin{aligned} \iota : \text{GR}(p^{m-1}, f) &\rightarrow \text{GR}(p^m, f) \quad (x \mapsto px), \\ \pi : \text{GR}(p^m, f) &\rightarrow \text{GR}(p^{m-1}, f) \quad (\text{projection}) \end{aligned}$$

$\text{GR}(p^m, f)$ 上の符号 C に対して, $\iota^{-1}(C), \pi(C)$ は $\text{GR}(p^{m-1}, f)$ 上の符号となり, それぞれ, ねじれ符号, 剰余符号と呼ぶこととする. ι^{-1} と π は $\text{GR}(p^m, f)$ 上の符号の圏から $\text{GR}(p^{m-1}, f)$ 上の符号の圏への関手と見ることができ, 次が成立する.

Lemma 2.1. 関手 ι^{-1}, π は可換である. すなわち, $\iota^{-1} \circ \pi = \pi \circ \iota^{-1}$.

Lemma 2.2. $\text{GR}(p^m, f)$ 上の符号 C に対して, $\iota^{-1}(C)^\perp = \pi(C^\perp)$.

2.5 重偶符号, 第二型符号

$p = 2$ の場合, 次のように重偶符号を定義することができる.

Definition 1. $\text{GR}(2^m, f)$ 上の長さ n の符号 C が重偶符号であるとは, C のすべての元 $c = (c_1, c_2, \dots, c_n)$ に対して,

$$\sum_{1 \leq i < j \leq n} c_i c_j = 0$$

が成立することと定義する.

この定義と同値な定義を与えるため, 前述の自然な射影 π の逆像について考える. $u \in \text{GR}(2^m, f)$ に対して, $a, b \in \pi^{-1}(u)$ とすると, $a^2 = b^2 \in \text{GR}(2^{m+1}, f)$ となり, u のみによって決まる. そこで $\bar{u}^2 = a^2$ と表すこととする. この表記法を用いると, 前述の定義は次のように言い換えることができる.

Lemma 2.3. $\text{GR}(2^m, f)$ 上の符号 C が重偶であることと, 任意の元 $c \in C$ について, $\sum_{i=1}^n \bar{c}_i^2 = 0 \in \text{GR}(2^{m+1}, f)$ であることは同値である.

本講演のタイトルにある, 第二型符号とは, 重偶な自己双対符号をいう. [1]

3 主定理

本講演では, $\text{GR}(p^{m-1}, f)$ 上の 2 つの符号を与えられたとき, それらをねじれ符号と剰余符号としてもつような $\text{GR}(p^m, f)$ 上の符号の数を数え上げる公式を紹介している.

導出手法としては, Gaborit[2] の手法が有用である. $\text{GR}(p^m, f)$ 上の符号から $\text{GR}(p^{m-1}, f)$ 上のねじれ符号と剰余符号が構成する際, もとの符号には含まれていて, ねじれ符号と剰余符号には含まれていない情報は, 生成行列中の $\Lambda_{0,t,t-1}$ の部分のみである. つまり, 導出手法としては与えられたねじれ符号と剰余符号のもとで, 条件を満たす行列 $\Lambda_{0,t,t-1}$ の個数を求めればよい.

一般の符号について, 次が成立する.

Theorem 3.1. X, Y を $\text{GR}(p^{m-1}, f)$ 上の符号とし, $\iota^{-1}(X) = \pi(Y)$ をみたしているものとする. このとき, X, Y はそれぞれ $(k_0, k_1, \dots, k_{t-2}, k_{t-1} + k_t)$ 型と $(k_0 + k_1, \dots, k_{t-2}, k_{t-1}, k_t)$ 型と書くことができる.

そのとき, $\pi(C) = X, \iota^{-1}(C) = Y$ をみたす $\text{GR}(p^m, f)$ 上の符号 C の個数は, $p^{k_0 k_t}$ となる.

p が奇素数のとき、自己双対符号について、次が成立する。

Theorem 3.2. p は奇素数、 X を $\text{GR}(p^{m-1}, f)$ 上の自己直交符号とし、 $\iota^{-1}(X) = \pi(X^\perp)$ をみたしているものとする。また X は $(k_0, k_1, \dots, k_{t-2}, k_{t-1} + k_t)$ 型とする。

そのとき、 $\pi(C) = X$ 、 $\iota^{-1}(C) = X^\perp$ をみたす $\text{GR}(p^m, f)$ 上の自己双対符号 C の個数は、 $p^{\frac{k_0(k_0-1)}{2}}$ となる。

$p = 2$ のとき、自己双対符号について、次が成立する。

Theorem 3.3. X を $\text{GR}(2^{m-1}, f)$ 上の重偶な自己直交符号とし、 $\iota^{-1}(X) = \pi(X^\perp)$ をみたしているものとする。また X は $(k_0, k_1, \dots, k_{t-2}, k_{t-1} + k_t)$ 型とする。

そのとき、 $\pi(C) = X$ 、 $\iota^{-1}(C) = X^\perp$ をみたす $\text{GR}(2^m, f)$ 上の自己双対符号 C の個数は、 $2^{\frac{k_0(k_0+1)}{2}}$ となる。

$p = 2$ のとき、第二型符号について、次が成立する。

Theorem 3.4. X を $\text{GR}(2^{m-1}, f)$ 上の重偶な自己直交符号とし、 $\iota^{-1}(X) = \pi(X^\perp)$ をみたしているものとする。また X は $(k_0, k_1, \dots, k_{t-2}, k_{t-1} + k_t)$ 型とする。

そのとき、 $\pi(C) = X$ 、 $\iota^{-1}(C) = X^\perp$ をみたす $\text{GR}(2^m, f)$ 上の第二型符号 C の個数は、 $2^{1 + \frac{k_0(k_0-1)}{2}}$ となる。

4 最後に

本講演では、与えられたねじれ符号と剰余符号からを持つ符号の個数を評価することで、分類に有用な結果を得ることができた。このことは、条件を満たすねじれ符号と剰余符号の個数がわかれば、符号の数え上げ公式が完成することを意味している。そのためには、自己直交符号の個数や、重偶な自己直交符号の個数が評価が必要である。

また、ガロア環は標数が素数巾な整数剰余環が含まれるが、一般の標数のものは含まれない。ただ、一般標数のものも、中国剰余定理を用いて素数巾のものに分解して評価することができるので、これらを扱う際も本講演で扱った内容で十分適用できる。

参考文献

- [1] K. Betsuniya and Y. Choie. Jacobi forms over totally real fields and type II codes over Galois rings $\text{GR}(2^m, f)$. *European J. Combin.*, 25(4):475-486, 2004.
- [2] P. Gaborit. Mass formulas for self-dual codes over Z_4 and $\mathbf{F}_q + u\mathbf{F}_q$ rings. *IEEE Trans. Inform. Theory*, 42(4):1222-1228, 1996.

A generalization of the Frenkel-Zhu bimodule¹

安部 利之 (愛媛大学大学院理工学研究科)

1 序

頂点作用素代数の表現論において, Zhu 代数と呼ばれる結合代数は本質的な役割を果たし, 一般論においても, 具体的な模型の研究においても, その構造の研究が重要となる. 特に既約加群の分類においては, 多くの模型に対し, 分類に十分な情報を Zhu 代数から得ることができる. しかし加群の構造を研究するためには, Zhu 代数は不十分であり, Dong, Li 及び Mason は, [DLM] において Zhu 代数を高次に一般化し, 頂点作用素代数の有理性と関連について研究した. 一方, 頂点作用素代数の既約加群の間のフュージョン則 (intertwining 作用素のなす空間の次元) と呼ばれる量の決定もまた表現論における重要な問題である. Frenkel と Zhu は [FZ] において, Zhu 代数の両側加群を定義し, その空間と intertwining 作用素のなす空間との関連について研究した. 頂点作用素代数が有理的な場合には, Frenkel-Zhu-両側加群の構造によりフュージョン則は完全に決定できるが, そうでない場合には, 高次の両側加群の情報も必要となると思われる. そこで本報告では, Frenkel-Zhu 両側加群の高次への一般化について, その定義と性質について述べる.

2 頂点作用素代数とその加群

以下ベクトル空間は複素数体 \mathbb{C} 上のベクトル空間とする. 組 $V, Y(\cdot, x), 1, \omega$ が頂点作用素代数であるとは V は $\mathbb{Z}_{\geq 0}$ -次数付きベクトル空間 $V = \bigoplus_{n=0}^{\infty} V_n$ であって, $Y(\cdot, x) : V \rightarrow \text{End } V[x, x^{-1}]$, $a \mapsto Y(a, z) = \sum_{n \in \mathbb{Z}} a_{(n)} z^{-n-1}$ ($a \in V$) としたとき, 次の条件を満たすことを言う.

(1) 任意の $a, b \in V$ に対し, ある $N \in \mathbb{Z}_{\geq 0}$ が存在し, $a_{(n)} b = 0$ ($n \geq N$).

(2) (Borcherds 恒等式) 任意の $a, b, u \in V$, $p, q, r \in \mathbb{Z}$ に対し,

$$\sum_{i=0}^{\infty} \binom{q}{i} (a_{(p+i)} b)_{(q+r-i)} u = \sum_{i=0}^{\infty} (-1)^i \binom{p}{i} (a_{(p+q-i)} b_{(r+i)} - (-1)^p b_{(p+r-i)} a_{(q+i)}) u. \quad (2.1)$$

(3) 任意の $n \in \mathbb{Z}$ に対し, $1_{(n)} = \delta_{n,-1} \text{id}_V$. 任意の $a \in V$, $n \in \mathbb{Z}_{\geq 0}$ に対し, $a_{(n)} 1 = 0$.

(4) $\{L_n := \omega_{(n+1)} (n \in \mathbb{Z}), \text{id}_V\}$ は, V 上に中心電荷 $c_V \in \mathbb{C}$ の Virasoro 代数の表現を与える:

$$[L_m, L_n] = (m-n)L_{m+n} + \frac{m^3 - m}{12} c_V \text{id}_V \quad (m, n \in \mathbb{Z}).$$

¹2007年6月28日, 第24回代数的組み合わせ論研究集会

(5) 任意の $a \in V, n \in \mathbb{Z}$ に対し, $(L_{-1}a)_{(n)} = -na_{(n-1)}$.

(6) V_n は L_0 に関する固有値 n の有限次元固有空間.

頂点作用素代数 V に対し, その加群の圏がいろいろ知られているが, 本報告では logarithmic 加群の圏を考える. 組 $(M, Y(\cdot, x))$ が, logarithmic V -加群 (以下 log V -加群) であるとは, M は \mathbb{C} -次数付きベクトル空間; $M = \bigoplus_{\lambda \in \mathbb{C}} M_{(\lambda)}$ であつて, $Y(\cdot, x)$ は線形写像 $V \rightarrow \text{End } M[x, x^{-1}]$ であり, $a \mapsto Y(a, z) = \sum_{n \in \mathbb{Z}} a_{(n)} z^{-n-1}$ ($a \in V$) としたとき, 次を満たすことを言う.

(7) 任意の $a \in V, u \in M$ に対し, ある $N \in \mathbb{Z}_{\geq 0}$ が存在し, $a_{(n)}u = 0$ ($n \geq N$).

(8) (Borcherds 恒等式) 任意の $a, b \in V, u \in M, p, q, r \in \mathbb{Z}$ に対し, (2.1) が成立する.

(9) $1_{(n)} = \delta_{n,-1} \text{id}_M$.

(10) 任意の $\lambda \in \mathbb{C}$ に対し, $M_{(\lambda)}$ は L_0 に関する固有値 λ の有限次元広義固有空間で, ある $N \in \mathbb{Z}_{\geq 0}$ が存在し, $M_{(\lambda-n)} = 0$ ($n \geq N$).

logarithmic V -加群と呼ばれる由来は, 一般にその (擬) 指標の q -展開に \log の多項式が現れるからである.

いま $0 \neq u \in M_{(\lambda)}$ に対し, λ を $|u|$ と表すことにする. また任意の $\lambda \in \mathbb{C}$ に対し, $M_{(\lambda-n)} \neq 0$ かつ $M_{(\lambda-n-i)} = 0$ ($i \in \mathbb{Z}_{>0}$) を満たす n が存在する時, n を λ の M における次数と呼び $\text{deg}(\lambda)$ と表すことにする. 特に任意の $a \in V$ に対し, $|a| = \text{deg}(a)$ である.

線形写像 $a_{(n)} \in \text{End } M$ は, $a_{(n)}M_{(\lambda)} \subset M_{(\lambda+|a|-n-1)}$ を満たす. よつて

$$a[n] := a_{(|a|+n-1)}$$

と斉次元 $a \in V$ に対し定義し, 線形に V 上に拡張すると, $a \in V$ に対し

$$a[n]M_{(\lambda)} \subset M_{(\lambda-n)}$$

が成立する.

$p \in \mathbb{Z}$ に対し, $a[p+n]u = 0$ ($a \in V, n \in \mathbb{Z}_{\geq 0}$) を満たす M の元 u 全体の集合を $\Omega_p(M)$ と表すことにする. 定義より, $q \leq p$ ならば, $\Omega_q(M) \subset \Omega_p(M)$ が成り立ち, $\text{id}_M = 1[0]$ なので, $p < 0$ ならば, $\Omega_p(M) = 0$ となる. また log V -加群 M と任意の $\lambda \in \mathbb{C}$ に対し, $N = \bigoplus_{n \in \mathbb{Z}} M_{(\lambda+n)}$ は M の部分加群となる. 特に, $u \in M$ に対し, $\text{deg}(u) \leq p$ ならば, $u \in \Omega_p(M)$ が成り立つ.

3 Intertwining 作用素

M^1, M^2, M^3 を log V -加群とする. 型 $\begin{pmatrix} M^3 \\ M^1 & M^2 \end{pmatrix}$ の intertwining 作用素とは, 線形写像 $I(\cdot, x) : M^1 \rightarrow \text{Hom}(M^2, M^3)\{x\}$, $v \mapsto I(v, x) = \sum_{n \in \mathbb{C}} v_{(n)} x^{-n-1}$ ($v \in M^1$) であつて次を満たすものである.

(11) 任意の $v \in M^1, u \in M^2, n \in \mathbb{C}$ に対し, ある $N \in \mathbb{Z}_{\geq 0}$ が存在して, $v_{(n+i)}u = 0$ ($i \geq N$).

(12) 任意の $a \in V, v \in M^1, u \in M^2, p, q \in \mathbb{Z}$ 及び $r \in \mathbb{C}$ に対し, (2.1) において $b = v$ としたものが成立.

(13) 任意の $v \in M^1, n \in \mathbb{C}$ に対し, $(L_{-1}v)_{(n)} = -nv_{(n-1)}$ が成立.

各 M^i が $M^i = \bigoplus_{n=0}^{\infty} M_{(\lambda_i+n)}$ ($\lambda_i \in \mathbb{C}$) の形の加群であると仮定すると, 型 $\begin{pmatrix} M^3 \\ M^1 & M^2 \end{pmatrix}$ の intertwining 作用素 $I(\cdot, x)$ と $v \in M^1$ に対し, $I(v, x) \in \text{Hom}(M^2, M^3)[[x, x^{-1}]]x^{-\lambda_1-\lambda_2+\lambda_3}$ が成り立つことが知られている. そこで, $v \in M^1$ と $n \in \mathbb{Z}$ に対し,

$$I(v, x) = \sum_{n \in \mathbb{Z}} v_n x^{-n-1-\lambda_1-\lambda_2+\lambda_3}$$

によって $v_n \in \text{Hom}(M^2, M^3)$ を定めると $v_n M_{(\mu)}^2 \subset M_{(\mu+\deg v-n-1)}^3$ が成立する. 特に $Y(\cdot, x)$ を intertwining 作用素と見なした時, $a_n = a_{(n)}$ ($a \in V, n \in \mathbb{Z}$) となる. そこで任意の斉次元 $v \in M^1$ に対し, $v[n] = v_{\deg(v)+n-1}$ と定義し, M^1 上に線形に拡張すれば, 任意の $v \in M^1$ に対し, $v[n]M_{(\mu)}^2 \subset M_{(\mu-n)}^3$ が成り立つことがわかる.

今 intertwining 作用素の定義に用いた Borchers 恒等式をこの斉次な表記法で表すと, Borchers 恒等式は次のように表される: 任意の $a \in V, v \in M^1, u \in M^2, p, q, r \in \mathbb{Z}$ に対し,

$$\begin{aligned} & \sum_{i=0}^{\infty} \binom{|a|+p-1}{i} (a_{(q+i)}v)[p+q+r]u \\ &= \sum_{i=0}^{\infty} \binom{q}{i} (-1)^i (a[p+q-i]v[r+i]u - (-1)^q v[q+r-i]a[p+i]u). \end{aligned} \quad (3.1)$$

4 結合公式

M^1, M^2, M^3 を $\log V$ -加群とし, $I(\cdot, x)$ を型 $\begin{pmatrix} M^3 \\ M^1 & M^2 \end{pmatrix}$ の intertwining 作用素とする. このとき, 次の結合公式が成り立つ ([Li]): $a \in V, u \in M^1, v \in M^2, m \in \mathbb{Z}, n \in \mathbb{C}$ に対し,

$$a_{(m)}u_{(n)}v = \sum_{i=0}^l \sum_{j=0}^{\infty} \binom{m-k}{i} \binom{k}{j} (a_{(m-k-i+j)}u)_{(n+k+i-j)}v,$$

但し k は, 任意の $i \in \mathbb{Z}_{\geq 0}$ に対し, $a_{(k+i)}v = 0$ となる整数で, l は任意の $i \in \mathbb{Z}_{\geq 0}$ に対し, $u_{(l+n+1+i)}v = 0$ が成り立つ正の整数である. $p, q, r \in \mathbb{Z}_{\geq 0}$ に対し, $v \in \Omega_p(M^2)$ とし, $m = |a| + r - q - 1, n = \deg(u) + p - r - 1$ とすると, $l = r, k = |a| + p$ とおけば, このとき斉次記法で結合法則を表すと,

$$a[r-q]u[p-r]v = \sum_{i=0}^r \sum_{j=0}^{\infty} \binom{r-p-q-1}{i} \binom{|a|+p}{j} (a_{(r-p-q-1-i+j)}u)[p-q]v$$

を得る. 同様に,

$$\begin{aligned} & u[r-q]a[p-r]v \\ &= \sum_{i=0}^r \sum_{j=0}^{\infty} \binom{r-q-s-1}{i} (-1)^{r-q-s-i} \binom{|a|+p-r-1+i}{j} \\ & \quad \times (a_{(r-q-s-1+j-i)}u)[p-q]v \end{aligned}$$

が成り立つこと示すことができる.

これら二つの公式は $\Omega_p(M^2)$ 上においては, 合成

$$a[r-q]u[p-r] : \Omega_p(M^2) \rightarrow \Omega_r(M^3) \rightarrow \Omega_q(M^3)$$

及び

$$u[r-q]a[p-r] : \Omega_p(M^2) \rightarrow \Omega_r(M^2) \rightarrow \Omega_q(M^3)$$

が, それぞれ M^1 の一つのベクトル w が存在して $w[p-q]$ で与えられることを表している. そこで最初の合成を, V の M^1 への左作用, 後の合成を V の M^1 への右作用ととらえ, 両側加群を構成するのが基本的な考え方である. ただ表現から代数を構成しているので, 構成法が自然かどうかはわからないが, 今まで知られていた結果はほとんど復元することができる.

5 Zhu 代数と Frenkel-Zhu 両側加群

V を頂点作用素代数とし, M を $\log V$ -加群とする. 任意の斉次元 $a \in V$, $u \in M$, $p, q \in \mathbb{Z}$ に対し,

$$a \odot_q^p u = \sum_{i=0}^{\infty} \binom{|a|+p}{i} a_{(q+i)}u$$

と定義し, V 上線形に拡張する.

非負整数 $p, q \in \mathbb{Z}_{\geq 0}$ に対し, V の部分空間 $O_{q,p}(M)$ を

$$O_{q,p}(M) = \text{span}\{a \odot_{-p-q-2}^p u \mid a \in V, u \in M\}$$

によって定義し,

$$A_{q,p}(M) = M/O_{q,p}(M)$$

とおく. また $\Gamma \in \text{End } M$ を $\Gamma(u) = L_{-1}u + L_0u$ ($u \in M$) によって定義する. 公理 (5) より, 線形写像 Γ は次の性質を持つことが示される.

命題 5.1. $a \in V$, $u \in M$, $p, q \in \mathbb{Z}$ に対し,

(1) $\Gamma(a) \odot_q^p u = -qa \odot_{q-1}^p u - (p+q+1)a \odot_q^p u$,

(2) $\Gamma(a \odot_q^p u) = \Gamma(a) \odot_q^p u + a \odot_q^p \Gamma(u)$ が成り立つ.

特に, 任意の $p, q \in \mathbb{Z}_{\geq 0}$ に対し $\Gamma(O_{q,p}(M)) \subset O_{q,p}(M)$.

命題 5.1 (1) より, $p' \geq p$ かつ $q' \geq q$ ならば

$$O_{q',p'}(M) \subset O_{q,p}(M)$$

となることを示すことができる.

任意の $p, q, r \in \mathbb{Z}_{\geq 0}$ に対し, 双線形写像 $\triangleright_{q,p}^r: V \times M \rightarrow M$ と $\triangleleft_{q,p}^r: M \times V \rightarrow M$ を, $a \in V, u \in M$ に対し,

$$a \triangleright_{q,p}^r u = \sum_{i=0}^r \binom{r-p-q-1}{i} a \odot_{r-p-q-1-i}^p u$$

及び

$$u \triangleleft_{q,p}^r a = \sum_{i=0}^r \binom{r-q-p-1}{i} (-1)^{r-q-p-i} a \odot_{r-q-p-1-i}^{p-r-1+i} u$$

と定めることによって定義する. 直接計算によって, 次の命題を得る.

命題 5.2. $p, q, r \in \mathbb{Z}_{\geq 0}$ に対し, $r \leq p+q$ ならば,

$$\begin{aligned} O_{q,p}(M) &= \text{span}\{((\Gamma+r-q)a) \triangleright_{q,p}^r u \mid a \in V, u \in M\} \\ &= \text{span}\{u \triangleleft_{q,p}^r ((\Gamma+p-r)a) \mid a \in V, u \in M\} \end{aligned}$$

が成り立つ.

Remark 5.3. M^2, M^3 を $\log V$ -加群とし, $I(\cdot, x)$ を型 $\begin{pmatrix} M^3 \\ M & M^2 \end{pmatrix}$ の intertwining 作用素とすれば, 任意の $v \in \Omega_p(M^2)$ に対し,

$$a[r-q]u[p-r]v = (a \triangleright_{q,p}^r u)[p-q]v, \quad u[r-q]a[p-r]v = (u \triangleleft_{q,p}^r a)[p-q]v$$

が成立する. 命題 5.2 より, $u \in O_{q,p}(M), v \in \Omega_p(M)$ ならば $u[q-p]v = 0$ であることがわかる.

結合則については, 次が成立する.

命題 5.4. 任意の $a, b \in V, u \in M$ に対し,

- (1) $a \triangleright_{q,p}^q (b \triangleright_{q,p}^q u) \equiv (a \triangleright_{q,q}^q b) \triangleright_{q,p}^q u \pmod{O_{q,p}(M)}$.
- (2) $(u \triangleleft_{q,p}^p a) \triangleleft_{q,p}^p a \equiv u \triangleleft_{q,p}^p (a \triangleleft_{p,p}^p a) \pmod{O_{q,p}(M)}$.
- (3) $a \triangleright_{q,p}^q (u \triangleleft_{q,p}^p b) \equiv (a \triangleright_{q,p}^q u) \triangleright_{q,p}^p b \pmod{O_{q,p}(M)}$.

上の設定を含むもっと一般的な状態で, 結合則は成り立つが, 複雑なのでここでは省略する.

加群 M が頂点作用素代数自身の時には, 更にいくつかの性質が成り立つ.

命題 5.5. $a, b \in V, p, q, r \in \mathbb{Z}_{\geq 0}$ に対し,

$$a \triangleright_{q,p}^r b - a \triangleleft_{q,p}^r b \in (\Gamma+p-q)(V).$$

特に $a \triangleright_{p,p}^p b \equiv a \triangleleft_{p,p}^p b \pmod{\Gamma(V)}$.

従って

$$A_p(V) := V/(O_{p,p}(V) + \Gamma(V))$$

において、 $\triangleright_{p,p}^p = \triangleleft_{p,p}^p$ が成り立ち、これを $*$ と表すと、命題 5.2 より、 $*$ は well-defined な積 $A_p(V) \times A_p(V) \rightarrow A_p(V)$ を定義する。更に命題 5.4 により、この積は結合的であることがわかる。

上で構成した結合代数は [DLM] において導入された p -th Zhu 代数と全く同様の物であり、 $1 + O_{p,p}(V) + \Gamma(V)$ が単位元を与え、 $\omega + O_{p,p}(V) + \Gamma(V)$ が中心の元となる。

一般の $\log V$ -加群に戻る。命題 5.2 と 5.4 を組み合わせると次のことがわかる。

補題 5.6. $p, q \in \mathbb{Z}_{\geq 0}$ とする。このとき

$$(O_{q,q}(V) + \Gamma(V)) \triangleright_{q,p}^q M \subset O_{q,p}(M), \quad M \triangleleft_{q,p}^p (O_{p,p}(V) + \Gamma(V)) \subset O_{q,p}(M)$$

及び

$$V \triangleright_{q,p}^q O_{q,p}(M) \subset O_{q,p}(M), \quad O_{q,p}(M) \triangleleft_{q,p}^p V \subset O_{q,p}(M)$$

が成り立つ。

この補題により $\triangleright_{q,p}^q$ と $\triangleleft_{q,p}^p$ はそれぞれ、 $A_{q,p}(M)$ 上に左から $A_q(V)$ 、右から $A_p(V)$ の作用を誘導することがわかる。命題 5.4 により、この作用が $A_{q,p}(M)$ に $A_q(V) - A_p(V)$ -両側加群の構造を与えることが示される。

定理 5.7. 左作用 $\triangleright_{q,p}^q$ 、右作用 $\triangleleft_{q,p}^p$ によって $A_{q,p}(M)$ は $A_q(V) - A_p(V)$ -両側加群の構造をもつ。

$p = q = 0$ の時、Frenkel と Zhu により導入された $A(V)$ -両側加群 $A(M)$ と一致する。

6 Borchers 恒等式と $A_{q,p}(M)$

最後に intertwining 作用素の Borchers 恒等式に対応する両側加群の恒等式を挙げる。前に Borchers 恒等式を、斉次な表記法で表すと (3.1) の様になると述べた。積 \odot を用いると、この恒等式 (3.1) の左辺は $(a \odot_q^{p-1} v)[p+q+r]u$ となることがわかる。一方、恒等式 (3.1) の右辺において $u \in \Omega_s(M^2)$ とすれば、 $s \geq p+q+r$ のとき、結合公式を用いて

$$\begin{aligned} & \sum_{i=0}^{\infty} \binom{q}{i} (-1)^i (a[p+q-i]v[r+i]u - (-1)^q v[q+r-i]a[p+i]u) \\ &= \sum_{i=0}^{\infty} \binom{q}{i} (-1)^i \left((a \triangleright_{s-p-q-r,s}^{s-r-i} v)[p+q+r]u - (-1)^q (v \triangleleft_{s-p-q-r,s}^{s-p-i} a)[p+q+r]u \right), \end{aligned}$$

但し $a, b \in \mathbb{Z}_{\geq 0}$, $c < 0$ の時、 $\triangleright_{a,b}^c = \triangleleft_{a,b}^c = 0$ と定義した。ここで p, q, r, s をそれぞれ $r-q, k, p-r-k, p$ に置き換えると、任意の $p, q \in \mathbb{Z}_{\geq 0}$ 及び $r, k \in \mathbb{Z}$ に対し、

$$\begin{aligned} & (a \odot_k^{r-q-1} v)[p-q]u \\ &= \sum_{i=0}^{\infty} \binom{k}{i} (-1)^i \left((a \triangleright_{q,p}^{r+k-i} v)[q-r]u - (-1)^k (v \triangleleft_{q,p}^{p+q-r-i} a)[q-r]u \right) \end{aligned}$$

が成り立つことがわかる。この等式は $A_{q,p}(M)$ において、

$$a \odot_k^{r-q-1} u = \sum_{i=0}^{\infty} \binom{k}{i} (-1)^i \left(a \triangleright_{q,p}^{r+k-i} u - (-1)^k u \triangleleft_{q,p}^{p+q-r-i} a \right)$$

が成り立つことを、示唆しているが、実際に次の定理を得る。

定理 6.1. 任意の $a \in V$, $u \in M$, $r \in \mathbb{Z}$, $p, q \in \mathbb{Z}_{\geq 0}$ 及び $r, k \in \mathbb{Z}$ 対し, 恒等式

$$a \odot_k^{r-q-1} u \equiv \sum_{i=0}^{\infty} \binom{k}{i} (-1)^i \left(a \triangleright_{q,p}^{r+k-i} u - (-1)^k u \triangleleft_{q,p}^{p+q-r-i} a \right) \quad (6.1)$$

が $O_{q,p}(M)$ を法として成り立つ。

参考文献

- [DLM] C. Dong, H.-S. Li and G. Mason, Vertex operator algebras and associative algebras, *J. Algebra* **206** (1998), no. 1, 67–96.
- [FHL] I. Frenkel, Y.-Z. Huang and J. Lepowsky, On axiomatic approaches to vertex operator algebras and modules, *Mem. Amer. Math. Soc.* **104** (1993).
- [FZ] I. Frenkel and Y. Zhu, Vertex operator algebras associated to representations of affine and Virasoro algebras, *Duke Math. J.* **66** (1992), 123–168.
- [Li] H.-S. Li, The regular representation, Zhu’s $A(V)$ -theory and induced modules, *J. Algebra*, **238** (2001), 159–193.
- [MN] A. Matsuo and K. Nagatomo, Axioms for a Vertex Algebra and the Locality of Quantum Fields, *MSJ Memoirs* **4**, Mathematical Society of Japan, (1999).
- [Mil] A. Milas, Weak modules and logarithmic intertwining operators for vertex operator algebras in Recent developments in infinite-dimensional Lie algebras and conformal field theory (Charlottesville, VA, 2000), 201–225, *Contemp. Math.*, **297**, Amer. Math. Soc., Providence, RI, 2002.
- [Z] Y.-C. Zhu, Modular invariance of characters of vertex operator algebras, *J. Amer. Math. Soc.* **9** (1996), 237–302.

Subalgebras of lattice vertex operator algebras and W-algebras

山田裕理

一橋大学大学院経済学研究科

1 はじめに

ℓ を 2 以上の整数とする. レベル ℓ の $A_1^{(1)}$ 型アフィン単純頂点作用素代数 $L(\ell, 0)$ には, 中心電荷 1 の共形元の commutant として, 中心電荷 $\frac{2(\ell-1)}{\ell+2}$ の W -代数 $W(\frac{2(\ell-1)}{\ell+2})$ が含まれることが知られている. この W -代数は, 主として物理の方面から研究されてきた (cf. [2]). 一方 $W(\frac{2(\ell-1)}{\ell+2})$ は, $A_{\ell-1}$ 型ルート格子を $\sqrt{2}$ 倍した格子に付随する頂点作用素代数 $V_{\sqrt{2}A_{\ell-1}}$ にも含まれる (cf. [9]). この観点から, 筆者は C. Dong 氏, C. H. Lam 氏と共同で, $W(\frac{2(\ell-1)}{\ell+2})$ の既約加群の分類について考察してきた. 本稿では, ℓ が小さい場合に得られた結果を紹介する.

講演では, $\ell \leq 7$ の場合には既約加群の分類ができること述べたが, その後, 安部利之氏, 荒川知幸氏, 松尾厚氏により, 議論の一部に不備があることが指摘された. 本稿では, この不備を修正した上で, $\ell = 5$ の場合の既約加群の分類および Zhu 代数について説明する. $\ell = 2, 3, 4$ のときには, $W(\frac{2(\ell-1)}{\ell+2})$ は退化して良く知られた頂点作用素代数になる.

第 2 節では, $W(2, 3, 4, 5)$ について説明する. $W(\frac{2(\ell-1)}{\ell+2})$ はこれの準同型像であるが, ある種の特異ベクトルは $W(2, 3, 4, 5)$ の元として計算する必要がある. 第 3 節では, 一般の ℓ について $W(\frac{2(\ell-1)}{\ell+2})$ の性質をまとめておく. 主結果は第 4 節で述べる.

2 $W(2, 3, 4, 5)$

$\{h, e, f\}$ を sl_2 -triple, すなわち

$$\begin{aligned} [e, f] &= h, & [h, e] &= 2e, & [h, f] &= -2f, \\ \langle h, h \rangle &= 2, & \langle e, f \rangle &= 1, & \langle h, e \rangle &= \langle h, f \rangle = \langle e, e \rangle = \langle f, f \rangle = 0 \end{aligned}$$

とする. $V(\ell, 0)$ を, $A_1^{(1)}$ 型アフィンリー代数 $\widehat{sl}_2 = sl_2 \otimes \mathbb{C}[t, t^{-1}] \oplus \mathbb{C}c$ のレベル ℓ , 最高ウェイト 0 の Verma 加群とし, その最高ウェイトベクトルを 1 で表す. 以下, $\ell = 2, 3, 4, \dots$ の場合だけを考える. 1 には, $sl_2 \otimes \mathbb{C}[t]$ は 0 として作用し, c は ℓ として作用する. $V(\ell, 0)$ は, $sl_2 \otimes \mathbb{C}[t^{-1}]t^{-1}$ -加群としては 1 で生成される自由加群である. $h \otimes t^n, e \otimes t^n, f \otimes t^n$ の $V(\ell, 0)$ への作用を, それぞれ $h(n), e(n), f(n)$ と表す. 次のような $V(\ell, 0)$ のウェイト 2 の元を考える.

$$\begin{aligned}\omega_{\text{aff}} &= \frac{1}{2(\ell+2)} \left(-h(-2)1 + \frac{1}{2}h(-1)^2 1 + 2e(-1)f(-1)1 \right), \\ \omega_\gamma &= \frac{1}{4\ell} h(-1)^2 1, \\ \omega &= \frac{1}{2\ell(\ell+2)} \left(-\ell h(-2)1 - h(-1)^2 1 + 2\ell e(-1)f(-1)1 \right).\end{aligned}$$

$\omega = \omega_{\text{aff}} - \omega_\gamma$ である。 ω_{aff} は頂点作用素代数 $V(\ell, 0)$ のヴィラソロ元で、その中心電荷は $3\ell/(\ell+2)$ である。 また、 ω_γ は中心電荷 1 の共形元である。 ω も共形元で、その中心電荷は $3\ell/(\ell+2) - 1 = 2(\ell-1)/(\ell+2)$ である。 [1] において、 $\text{Vir}(\omega_\gamma)$ の $V(\ell, 0)$ における commutant として $W(2, 3, 4, 5)$ が定義された。

$$W(2, 3, 4, 5) = \{v \in V(\ell, 0) \mid (\omega_\gamma)_n v = 0 \text{ for all } n \geq 0\}.$$

以下、簡単のため $W(2, 3, 4, 5)$ を \widetilde{W} と書くことにする。 ここで、 $\text{Vir}(\omega_\gamma)$ は ω_γ で生成される部分頂点作用素代数を表す。 \widetilde{W} は、 ω をヴィラソロ元とする頂点作用素代数である。

$$\begin{aligned}W^3 &= \ell^2 h(-3)1 + 3\ell h(-2)h(-1)1 + 2h(-1)^3 1 - 6\ell h(-1)e(-1)f(-1)1 \\ &\quad + 3\ell^2 e(-2)f(-1)1 - 3\ell^2 e(-1)f(-2)1\end{aligned}$$

とおく。

\widetilde{W} は頂点作用素代数として 1 個の元 W^3 で生成されるが、作用素積展開を記述するためには、次のウエイト 4 の元 W^4 およびウエイト 5 の元 W^5 が必要になる。

$$\begin{aligned}W^4 &= -2\ell^2(\ell^2 + \ell + 1)h(-4)1 - 8\ell(\ell^2 + \ell + 1)h(-3)h(-1)1 - \ell(5\ell^2 - 6)h(-2)^2 1 \\ &\quad - 2\ell(11\ell + 6)h(-2)h(-1)^2 1 - (11\ell + 6)h(-1)^4 1 + 4\ell^2(6\ell - 5)h(-2)e(-1)f(-1)1 \\ &\quad + 4\ell(11\ell + 6)h(-1)^2 e(-1)f(-1)1 - 4\ell^2(5\ell + 11)h(-1)e(-2)f(-1)1 \\ &\quad + 4\ell^2(5\ell + 11)h(-1)e(-1)f(-2)1 + 8\ell^2(\ell - 3)(\ell - 2)e(-3)f(-1)1 \\ &\quad - 4\ell^2(3\ell^2 - 3\ell + 8)e(-2)f(-2)1 - 2\ell^2(6\ell - 5)e(-1)^2 f(-1)^2 1 \\ &\quad + 8\ell^2(\ell^2 + \ell + 1)e(-1)f(-3)1,\end{aligned}$$

$$\begin{aligned}
W^5 = & -2\ell^3(\ell^2 + 3\ell + 5)h(-5)1 - 10\ell^2(\ell^2 + 3\ell + 5)h(-4)h(-1)1 - 5\ell^2(3\ell^2 - 4)h(-3)h(-2)1 \\
& - 5\ell(7\ell^2 + 12\ell + 16)h(-3)h(-1)^2 1 - 15\ell(3\ell^2 - 4)h(-2)^2 h(-1)1 \\
& - 5\ell(19\ell + 12)h(-2)h(-1)^3 1 - 2(19\ell + 12)h(-1)^5 1 \\
& + 10\ell^2(4\ell^2 - 7\ell + 8)h(-3)e(-1)f(-1)1 + 20\ell^2(10\ell - 7)h(-2)h(-1)e(-1)f(-1)1 \\
& + 10\ell(19\ell + 12)h(-1)^3 e(-1)f(-1)1 - 5\ell^2(11\ell^2 - 14\ell + 12)h(-2)e(-2)f(-1)1 \\
& - 5\ell^2(17\ell + 64)h(-1)^2 e(-2)f(-1)1 + 15\ell^2(3\ell^2 - 4)h(-2)e(-1)f(-2)1 \\
& + 5\ell^2(17\ell + 64)h(-1)^2 e(-1)f(-2)1 + 30\ell^2(\ell - 4)(\ell - 3)h(-1)e(-3)f(-1)1 \\
& - 40\ell^2(\ell^2 + 3\ell + 5)h(-1)e(-2)f(-2)1 - 10\ell^2(10\ell - 7)h(-1)e(-1)^2 f(-1)^2 1 \\
& + 10\ell^2(3\ell^2 + 19\ell + 8)h(-1)e(-1)f(-3)1 - 10\ell^3(\ell - 4)(\ell - 3)e(-4)f(-1)1 \\
& + 20\ell^3(\ell - 4)(\ell - 3)e(-3)f(-2)1 + 5\ell^3(10\ell - 7)e(-2)e(-1)f(-1)^2 1 \\
& - 10\ell^3(2\ell^2 - 4\ell + 17)e(-2)f(-3)1 - 5\ell^3(10\ell - 7)e(-1)^2 f(-2)f(-1)1 \\
& + 10\ell^3(\ell^2 + 3\ell + 5)e(-1)f(-4)1.
\end{aligned}$$

たとえば、 $W_1^3 W^3$ および $W_1^3 W^4$ は

$$\begin{aligned}
W_1^3 W^3 = & -(162\ell^3(\ell - 2)(\ell + 2)(3\ell + 4)/(16\ell + 17))\omega_{-3}1 \\
& + (288\ell^3(\ell - 2)(\ell + 2)^2(3\ell + 4)/(16\ell + 17))\omega_{-1}\omega \\
& + (36\ell(2\ell + 3)/(16\ell + 17))W^4,
\end{aligned}$$

$$\begin{aligned}
W_1^3 W^4 = & (1248\ell^2(\ell - 3)(\ell + 2)(2\ell + 1)(2\ell + 3)/(64\ell + 107))\omega_{-1}W^3 \\
& - (48\ell^2(\ell - 3)(2\ell + 1)(2\ell + 3)(2\ell + 7)/(64\ell + 107))W_{-3}^3 1 \\
& - (12\ell(3\ell + 4)(16\ell + 17)/(64\ell + 107))W^5
\end{aligned}$$

となる。

$W_n^i W^j$, $3 \leq i \leq j \leq 5$, $n \geq 0$ は、[1] において計算されている。ただし、[1] の記述では Virasoro descendant が省略されている。このような省略のない形で、筆者も独自に $W_n^i W^j$ を計算した。 $W_n^i W^j$, $3 \leq i \leq j \leq 5$, $n \geq 0$ は、すべてヴィラソロ元 ω および W^3 , W^4 , W^5 を用いて記述できる。すなわち、 \widetilde{W} は ω , W^3 , W^4 , W^5 で閉じている。

W^3 , W^4 , W^5 は、それぞれウエイト 3, 4, 5 の $\text{Vir}(\omega_\gamma)$ に関する最高ウエイトベクトルとして、スカラー倍を除いて一意的に定まる。 $W(2, 3, 4, 5)$ の 3, 4, 5 は、それぞれ W^3 , W^4 , W^5 に対応し、2 はヴィラソロ元 ω に対応する。この意味で、 ω を W^2 と書いても良い。

注意 上記の W^3 , W^4 , および W^5 は、[1, Appendix A] の W_3 , W_4 , W_5 と次の関係にある。

ただし [1] では、ここでの ℓ を k と表記している。

$$\begin{aligned} W^3 &= \frac{1}{2}W_3, \\ W^4 &= \frac{16\ell + 17}{144\ell(2\ell + 3)}W_4, \\ W^5 &= -\frac{64\ell + 107}{3456\ell^2(2\ell + 3)(3\ell + 4)}W_5. \end{aligned}$$

$L(n) = \omega_{n+1}$, $W^3(n) = W_{n+2}^3$, $W^4(n) = W_{n+3}^4$, $W^5(n) = W_{n+4}^5$ とおく。これらは、ウェイトが $-n$ の作用素である。 $W_n^i W^j$ の具体的な形から、次のことがわかる。

補題 2.1 \widetilde{W} は、ベクトル空間として次の形の元で張られる。

$$\begin{aligned} L(-i_1) \cdots L(-i_p) W^3(-j_1) \cdots W^3(-j_q) \\ W^4(-m_1) \cdots W^4(-m_r) W^5(-n_1) \cdots W^5(-n_s) 1, \end{aligned} \quad (2.1)$$

$i_1 \geq \cdots \geq i_p \geq 2$, $j_1 \geq \cdots \geq j_q \geq 3$, $m_1 \geq \cdots \geq m_r \geq 4$, $n_1 \geq \cdots \geq n_s \geq 5$.

$h \mapsto -h$, $e \mapsto f$, $f \mapsto e$ で定まるリー代数 sl_2 の位数 2 の自己同型は、自然に次のような頂点作用素代数 \widetilde{W} の位数 2 の自己同型 θ に拡張できる。

$$\theta\omega = \omega, \quad \theta W^3 = -W^3, \quad \theta W^4 = W^4, \quad \theta W^5 = -W^5.$$

特に、 θ は (2.1) の形の元を $(-1)^{q+s}$ 倍する。 $\widetilde{W}^\pm = \{v \in \widetilde{W} \mid \theta v = \pm v\}$ とおく。自己同型 θ を考慮することにより、様々な計算の見通しが良くなる。

$$W_5^3 W^3 = 12\ell^3(\ell - 2)(\ell - 1)(3\ell + 4)1$$

および \widetilde{W} が W^3 で生成される頂点作用素代数であることから、次の定理が得られる。

定理 2.2 $\ell \geq 3$ のとき、 \widetilde{W} の全自己同型群は θ で生成される位数 2 の群である。

$\ell = 2$ の場合は、 W^3 で生成される真のイデアルが存在し、 \widetilde{W} の極大イデアルによる剰余代数は、ヴィラソロ頂点作用素代数 $\text{Vir}(\omega) \cong L(1/2, 0)$ に同型になる。これの自己同型は自明なものだけである。

次に、 \widetilde{W} の Zhu 代数 $A(\widetilde{W})$ を考える。補題 2.1 により、 $A(\widetilde{W})$ はベクトル空間として

$$[u]^p * [W^3]^{q*} * [W^4]^{r*} * [W^5]^{s*}, \quad p, q, r, s \geq 0$$

で張られることがわかる。ここで、 $[u]^p$ は $[u]$ の Zhu 代数における p 個の積を表す。Zhu 代数の性質により、 $[u]$ は $A(\widetilde{W})$ の中心に含まれるが、さらに

$$\begin{aligned} [W^3] * [W^4] - [W^4] * [W^3] &= [W_0^3 W^4 + 2W_1^3 W^4 + W_2^3 W^4] = 0, \\ [W^3] * [W^5] - [W^5] * [W^3] &= [W_0^3 W^5 + 2W_1^3 W^5 + W_2^3 W^5] = 0, \\ [W^4] * [W^5] - [W^5] * [W^4] &= [W_0^4 W^5 + 3W_1^4 W^5 + 3W_2^4 W^5 + W_3^4 W^5] = 0 \end{aligned}$$

が計算により確かめられる。したがって、次の補題が成り立つ。

補題 2.3 \widetilde{W} の Zhu 代数 $A(\widetilde{W})$ は可換である.

この補題により、 $A(\widetilde{W})$ は 4 変数多項式環の準同型像であることがわかる. 実際、 w_2, w_3, w_4, w_5 を変数とする 4 変数多項式環 $\mathbb{C}[w_2, w_3, w_4, w_5]$ に対して、 $w_2 \mapsto [\omega], w_3 \mapsto [W^3], w_4 \mapsto [W^4], w_5 \mapsto [W^5]$ により、 $\mathbb{C}[w_2, w_3, w_4, w_5]$ から $A(\widetilde{W})$ への全準同型が得られる.

次に、 \widetilde{W} の特異ベクトルを考える. \widetilde{W} の特異ベクトルは、

(a) \widetilde{W} の null vector

(b) $V(\ell, 0)$ の極大イデアルに含まれるもの

の 2 種類がある. $V(\ell, 0)$ の極大イデアルは次節で扱うこととし、ここでは \widetilde{W} の null vector を調べる.

[1, (2.1.8)] により、 \widetilde{W} の指標は

$$\frac{\sum_{r \geq 0} (-1)^r q^{r(r+1)/2} - q \sum_{r \geq 0} (-1)^r q^{r(r+3)/2}}{\prod_{n \geq 1} (1 - q^n)^2}$$

である. 最初のいくつかの項を具体的に書くと、

$$1 + q^2 + 2q^3 + 4q^4 + 6q^5 + 11q^6 + 16q^7 + 27q^8 + 40q^9 + 63q^{10} + 92q^{11} + \dots$$

となる. 一方、ウエイト m の (2.1) の形の元の個数を q^m の係数とする母関数は、

$$\frac{(1-q)^4(1-q^2)^3(1-q^3)^2(1-q^4)}{\prod_{n \geq 1} (1-q^n)^4}$$

であり、最初のいくつかの項は

$$1 + q^2 + 2q^3 + 4q^4 + 6q^5 + 11q^6 + 16q^7 + 29q^8 + 44q^9 + 72q^{10} + 108q^{11} + \dots$$

となる. 両者の差は

$$2q^8 + 4q^9 + 9q^{10} + 16q^{11} + \dots$$

であるが、ここに現れる $2q^8$ は、ウエイト 8 の (2.1) の形の元 29 個は線型独立ではなく、2 つの非自明な線型関係があることを意味する. このような非自明な線型関係を null vector と呼ぶ. ウエイト 9 以上についても、同様である. ウエイトが 7 以下の null vector は存在しない. ウエイトの小さい (たとえば 11 以下) の null vector は、任意の ℓ について具体的な形を求めることができる.

3 $W\left(\frac{2(\ell-1)}{\ell+2}\right)$

$\ell = 2, 3, \dots$ なので、 $V(\ell, 0)$ は単純ではない. 実際、 $V(\ell, 0)$ は唯一つの極大イデアル \mathcal{J} を持ち、それは $e(-1)^{\ell+1}1$ で生成される (cf. [6, 10]). 剰余代数 $L(\ell, 0) = V(\ell, 0)/\mathcal{J}$ は単純な頂点作用素代数であり、その基本的な性質は詳しく研究されている. \widetilde{W} についても同様に、唯一つの極大イデアル $\widetilde{\mathcal{I}}$ が存在する. $\mathcal{W} = \widetilde{W}/\widetilde{\mathcal{I}}$ とおく. $\mathcal{W} \cong W\left(\frac{2(\ell-1)}{\ell+2}\right)$ である. $\text{Vir}(\omega_r)$ の $V(\ell, 0)$ における commutant \widetilde{W} は、 $e(-1)^{\ell+1}1$ を含まない. 次の命題は C. H. Lam [8] による.

命題 3.1 $f(0)^{\ell+1}e(-1)^{\ell+1} \in \tilde{I}$ である.

$W \cong W(\frac{2(\ell-1)}{\ell+2})$ は、ある種の格子に付随する頂点作用素代数の部分代数として記述できる. また、それを用いて $W(\frac{2(\ell-1)}{\ell+2})$ のいくつかの既約加群が構成できる (cf. [4]). ここで、その概略を説明する.

$L = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_\ell$, $(\alpha_p, \alpha_q) = 2\delta_{pq}$ とする. L は、 ℓ 個の A_1 型ルート格子の直交和にほかならない. L の双対格子は、 $L^\perp = \mathbb{Z}\frac{1}{2}\alpha_1 + \cdots + \mathbb{Z}\frac{1}{2}\alpha_\ell$ である. L に付随する頂点作用素代数 V_L 、およびその加群 V_{L^\perp} を考える. 今の場合、 L の通常の群環 $\mathbb{C}[L]$ を用いて、 $V_L = M(1) \otimes \mathbb{C}[L]$ と表せることに注意する. V_L は、 $\beta_1(-n_1) \cdots \beta_r(-n_r)e^\alpha$, $\beta_i \in \{\alpha_1, \dots, \alpha_\ell\}$, $\alpha \in L$, $n_1 \geq \cdots \geq n_r \geq 1$ で張られる. 格子 L の各元を -1 倍する L の自己同型から引き起こされる V_L の位数 2 の自己同型を、 θ で表す.

$$H = \alpha_1(-1)1 + \cdots + \alpha_\ell(-1)1, \quad E = e^{\alpha_1} + \cdots + e^{\alpha_\ell}, \quad F = e^{-\alpha_1} + \cdots + e^{-\alpha_\ell}$$

とおく. $\gamma = \alpha_1 + \cdots + \alpha_\ell$ とおくと、 $H = \gamma(-1)1$ となる. $\theta H = -H$, $\theta E = F$, $\theta F = E$ に注意する. H, E, F の成分作用素 H_n, E_n, F_n (これらは、 $\text{End } V_L$ の元あるいは $\text{End } V_{L^\perp}$ の元である) は、

$$\begin{aligned} [H_m, H_n] &= 2m\ell\delta_{m+n,0}, \\ [H_m, E_n] &= 2E_{m+n}, \\ [H_m, F_n] &= -2F_{m+n}, \\ [E_m, F_n] &= H_{m+n} + m\ell\delta_{m+n,0}, \\ [E_m, E_n] &= [F_m, F_n] = 0 \end{aligned}$$

をみます. すなわち、 $H_n \leftrightarrow h(n)$, $E_n \leftrightarrow e(n)$, $F_n \leftrightarrow f(n)$ は、 \widehat{sl}_2 のレベル ℓ の表現を与える. また、 $0 \leq j \leq \ell$ について

$$(E_{-1})^j 1 = j! \sum_{\substack{I \subset \{1,2,\dots,\ell\} \\ |I|=j}} e^{\alpha_I}, \quad (F_{-1})^j 1 = j! \sum_{\substack{I \subset \{1,2,\dots,\ell\} \\ |I|=j}} e^{-\alpha_I}$$

であり、 $(E_{-1})^{\ell+1}1 = (F_{-1})^{\ell+1}1 = 0$ となる. ここで、 $\alpha_I = \sum_{p \in I} \alpha_p$ である. 特に、 $(E_{-1})^\ell 1 = \ell!e^\gamma$, $(F_{-1})^\ell 1 = \ell!e^{-\gamma}$ である. さらに、群環 $\mathbb{C}[L]$ において

$$e^{-\gamma} \cdot (E_{-1})^j 1 = \frac{j!}{(\ell-j)!} (F_{-1})^{\ell-j} 1, \quad e^\gamma \cdot (F_{-1})^j 1 = \frac{j!}{(\ell-j)!} (E_{-1})^{\ell-j} 1$$

が成り立つ.

H, E, F で生成される V_L の部分代数を V^{aff} 、 e^γ と $e^{-\gamma}$ で生成される部分代数を V^γ とおく. $V_L \supset V^{\text{aff}} \supset V^\gamma$ で、 $V^{\text{aff}} \cong L(\ell, 0)$ および $V^\gamma \cong V_{\mathbb{Z}\gamma}$ である. ここで、 $V_{\mathbb{Z}\gamma}$ は格子 $\mathbb{Z}\gamma$ に付随する頂点作用素代数を表す. V^γ は、 $(e^\gamma)_{2\ell-2}e^{-\gamma} = \gamma(-1)1 = H$ を含むことに注意する. θ を V^{aff} に制限したものは、第 2 節の θ から引き起こされる $L(\ell, 0)$ の位数 2 の自己同型に等しい. 格子に付随する頂点作用素代数の有理性、既約加群の分類な

どは良く知られている。 $\langle \gamma, \gamma \rangle = 2\ell$ なので、 V_{Z_γ} の既約加群は $V_{Z_\gamma+n\gamma/2\ell}$, $0 \leq n \leq 2\ell-1$ のいずれかに同型である。 V^{aff} を既約 V_γ -加群の直和に分解することを考える。 $v \in V_{L_\perp}$ で生成される V_{L_\perp} の部分 V_{Z_γ} -加群を、 $V_\gamma \cdot v$ で表す。 $V_\gamma \cdot v = \text{span}\{u_n v \mid u \in V_\gamma, n \in \mathbb{Z}\}$ である。 $V_\gamma \cdot (E_{-1})^j 1$ (あるいは $V_\gamma \cdot (F_{-1})^j 1$) は、 V_{Z_γ} -加群 $V_{Z_\gamma+j\gamma/2\ell}$ (あるいは $V_{Z_\gamma-j\gamma/2\ell}$) に同型である。 $M^{0j} = \{v \in V^{\text{aff}} \mid H_0 v = -2jv\}$ とおくと、次が成立する。

補題 3.2 V_γ -加群として、 $V^{\text{aff}} = \bigoplus_{j=0}^{\ell-1} (V_\gamma \cdot (F_{-1})^j 1) \otimes M^{0j}$ である。

いいかえると、 V_{Z_γ} -加群として $L(\ell, 0) = \bigoplus_{j=0}^{\ell-1} V_{Z_\gamma-j\gamma/2\ell} \otimes M^{0j}$ である。これより、 $M^{0,0}$ は V_{Z_γ} の $L(\ell, 0)$ における commutant で、 $M^{0,0} = W\left(\frac{2(\ell-1)}{\ell+2}\right)$ であることがわかる。

次に、 V_L -加群 V_{L_\perp} に含まれる既約 $M^{0,0}$ -加群を考える。 $0 \leq i \leq \ell, 0 \leq j \leq i$ について、

$$v^i = \sum_{\substack{I \subset \{1, 2, \dots, \ell\} \\ |I|=i}} e^{\alpha_I/2}, \quad v^{ij} = \frac{1}{j!} (F_0)^j v^i$$

とおく。 v^{ij} は、具体的には

$$v^{ij} = \frac{1}{j!} \sum_{\substack{I \subset \{1, 2, \dots, \ell\} \\ |I|=i}} \sum_{\substack{p_1, \dots, p_j \in I \\ p_1, \dots, p_j \text{ distinct}}} e^{\alpha_I/2 - \alpha_{p_1} - \dots - \alpha_{p_j}}$$

と書くことができる。

$$\begin{aligned} H_0 v^{ij} &= (i - 2j)v^{ij}, \\ E_0 v^{ij} &= \begin{cases} 0 & \text{if } j = 0, \\ (i - j + 1)v^{ij-1} & \text{if } 1 \leq j \leq i, \end{cases} \\ F_0 v^{ij} &= \begin{cases} (j + 1)v^{ij+1} & \text{if } 0 \leq j \leq i - 1, \\ 0 & \text{if } j = i, \end{cases} \end{aligned}$$

および $H_n v^{ij} = E_n v^{ij} = F_n v^{ij} = 0$, $n \geq 1$ が成り立つ。

$H_0 \leftrightarrow h(0)$, $E_0 \leftrightarrow e(0)$, $F_0 \leftrightarrow f(0)$ は sl_2 の表現を与え、 $U^i = \text{span}\{v^{ij} \mid 0 \leq j \leq i\}$ は $i+1$ 次元の既約 sl_2 -加群となる。また V_{L_\perp} の中で、 v^i で生成される部分 V^{aff} -加群 $V^{\text{aff}} \cdot v^i$ は、既約 $L(\ell, 0)$ -加群 $L(\ell, U^i)$ に同型である。 $M^{ij} = \{v \in V^{\text{aff}} \cdot v^i \mid H_0 v = (i - 2j)v\}$, $0 \leq i \leq \ell, 0 \leq j \leq \ell - 1$ とおく。 $V^{\text{aff}} \cdot v^i$ を既約 V_γ -加群の直和に分解することで、次の補題が得られる。

補題 3.3 V_{Z_γ} -加群として、 $L(\ell, U^i) = \bigoplus_{j=0}^{\ell-1} V_{Z_\gamma+(i-2j)\gamma/2\ell} \otimes M^{ij}$ である。

M^{ij} に関して、次のことがわかる (C. Dong [3] による)。

(1) M^{ij} は既約 $M^{0,0}$ -加群である。

(2) 群環の部分に $e^{-\gamma/2}$ をかける操作は $M^{0,0}$ の作用と可換で、この操作は $M^{0,0}$ -加群の同型 $M^{i,j} \cong M^{\ell-i, \ell-i+j}$ を引き起こす。ここで $0 \leq m \leq \ell-1$ について、 $M^{i, \ell+m} = M^{i,m}$ とする。

(3) $M^{i,j}$, $0 \leq i \leq \ell$, $0 \leq j \leq i$ は、 $M^{i,i} \cong M^{\ell-i,0}$ を除いて、互いに非同型である。これにより、 $\ell(\ell+1)/2$ 個の非同型な既約 $M^{0,0}$ -加群が得られる。

(4) $M^{0,0}$ の位数 2 の自己同型 θ は、既約 $M^{0,0}$ -加群の置換 $M^{i,j} \mapsto M^{i,i-j}$ を引き起こす。

(5) $M^{i,j}$, $0 \leq i \leq \ell$, $0 \leq j \leq i$ のトップレベルは 1 次元 $\mathbb{C}v^{i,j}$ で、 $o(\omega) = \omega_1$ および $o(W^3) = W_2^3$ は $\mathbb{C}v^{i,j}$ に次のように作用する。

$$o(\omega)v^{i,j} = \frac{1}{2\ell(\ell+2)} \left(\ell(i-2j) - (i-2j)^2 + 2\ell(i-j+1)j \right) v^{i,j},$$

$$o(W^3)v^{i,j} = \left(\ell^2(i-2j) - 3\ell(i-2j)^2 + 2(i-2j)^3 - 6\ell(i-2j)(i-j+1)j \right) v^{i,j}.$$

4 ℓ が小さい場合

$\ell = 2, 3, 4, 5$ の場合に、 $\mathcal{W} \cong W\left(\frac{2(\ell-1)}{\ell+2}\right)$ の既約加群の分類について述べる。 $\ell \leq 4$ の場合、 \mathcal{W} は良く知られた頂点作用素代数になる。

$\ell = 2$ のとき W^3 は $f(0)^{\ell+1}e(-1)^{\ell+1}1$ のスカラー一倍で、 W^3, W^4, W^5 は \mathcal{W} において 0 になり、 \mathcal{W} は中心電荷 $1/2$ のヴィラソロ頂点作用素代数 $L(1/2, 0)$ に同型である。これの既約加群は 3 個である。

$\ell = 3$ のとき W^4 は $f(0)^{\ell+1}e(-1)^{\ell+1}1$ のスカラー一倍で、 W^4, W^5 は \mathcal{W} において 0 になり、 \mathcal{W} は $L(4/5, 0) \oplus L(4/5, 3)$ に同型である。これの既約加群は 6 個である (cf. [7])。

$\ell = 4$ のとき W^5 は $f(0)^{\ell+1}e(-1)^{\ell+1}1$ のスカラー一倍で、 \mathcal{W} において 0 になり、 \mathcal{W} は $V_{\mathbb{Z}\beta}^+$ に同型である。ここで、 $\langle \beta, \beta \rangle = 6$ で、 $V_{\mathbb{Z}\beta}^+$ の既約加群は 10 個である (cf. [5])。

上記 3 つの場合、 \mathcal{W} の既約加群は $M^{i,j}$ に限る。

$\ell = 5$ のとき \mathcal{W} の既約加群が 15 個で、 $M^{i,j}$ のいずれかに同型であることを、以下の方針で証明することができる。 $\widetilde{\mathcal{W}}$ の特異ベクトルのうち、 $\widetilde{\mathcal{W}}$ の null vector については、ウエイト 8 のもの v^0 と、ウエイト 9 のもの v^1 をとる。ウエイト 8 の null vector は 2 個あり、そのうちの 1 個は $\widetilde{\mathcal{W}}^+$ 、他の 1 個は $\widetilde{\mathcal{W}}^-$ に含まれる。 v^0 は、 $\widetilde{\mathcal{W}}^+$ に含まれるウエイト 8 の null vector として、定数倍を除いて一意的に定まる。 v^0 と v^1 を (2.1) の形の元の線型結合として表し、それらの $\mathcal{W} = \widetilde{\mathcal{W}}/\widetilde{\mathcal{I}}$ の Zhu 代数における像 $[v^0], [v^1]$ を $w_2 = [\omega]$, $w_3 = [W^3]$, $w_4 = [W^4]$, $w_5 = [W^5]$ の多項式として表す。次に、 $\widetilde{\mathcal{W}}$ の特異ベクトルのうち $V(\ell, 0)$ の極大イデアル \mathcal{J} に含まれるものを考える。 $\ell = 5$ のときの $f(0)^{\ell+1}e(-1)^{\ell+1}1$ を u^0 とおく。命題 3.1 により、 $u^0 \in \widetilde{\mathcal{I}}$ である。 $u^m = (W_1^3)^m u^0$, $m = 0, 1, 2, 3$ について、同様に $[u^0], [u^1], [u^2], [u^3]$ を w_2, w_3, w_4, w_5 の多項式として表す。

上記の6個の多項式で生成される $\mathbb{C}[w_2, w_3, w_4, w_5]$ のイデアル \mathcal{P} の Gröbner 基底は、次の5個の多項式からなる。

$$\begin{aligned} P_1 &= w_2(5w_2 - 6)(5w_2 - 4)(7w_2 - 6)(7w_2 - 2) \\ &\quad (35w_2 - 23)(35w_2 - 17)(35w_2 - 3)(35w_2 - 2), \\ P_2 &= w_3(5w_2 - 6)(5w_2 - 4)(35w_2 - 23)(35w_2 - 17)(35w_2 - 3)(35w_2 - 2), \\ P_3 &= p(w_2) + 564841728w_3^2, \\ P_4 &= q(w_2) + 14685884928w_4, \\ P_5 &= r(w_2)w_3 + 5575284w_5. \end{aligned}$$

$p(w_2), q(w_2), r(w_2)$ は w_2 の多項式で、次数はそれぞれ 8, 8, 5 である。また、 $p(w_2)$ と P_1 の共通因子は $w_2(7w_2 - 6)(7w_2 - 2)$ 、 $q(w_2)$ と P_1 の共通因子は w_2 で、 $r(w_2)$ と P_1 は互いに素である。

$w_2 \mapsto [\omega], w_3 \mapsto [W^3], w_4 \mapsto [W^4], w_5 \mapsto [W^5]$ により、 $\mathbb{C}[w_2, w_3, w_4, w_5]$ から $A(\mathcal{W})$ への結合代数の全準同型が得られる。 \mathcal{W} において $u^0 = u^1 = u^2 = u^3 = v^0 = v^1 = 0$ なので、 \mathcal{P} はこの全準同型の核に含まれる。一方、Gröbner 基底の形から、 $\mathbb{C}[w_2, w_3, w_4, w_5]/\mathcal{P}$ は 15 次元で $w_2^m + \mathcal{P}, 0 \leq m \leq 8, w_2^n w_3 + \mathcal{P}, 0 \leq n \leq 5$ はその基底である。さらに、次のこともわかる。

(1) $P_1 = 0$ より、 w_2 の値は 0, 6/5, 4/5, 6/7, 2/7, 23/35, 17/35, 3/35, 2/35 のいずれかである。

(2) $P_2 = P_3 = 0$ より、(1) の w_2 の値のうち、 $w_3 = 0$ となるのは $w_2 = 0, 6/7, 2/7$ の場合に限る。また、 w_3 の 0 以外の値は、± のペアで現れる。

(3) $P_4 = P_5 = 0$ より、 w_4, w_5 は w_2 あるいは w_2 と w_3 で表せる。

また、連立方程式 $P_1 = P_2 = P_3 = P_4 = P_5 = 0$ の解 (w_2, w_3, w_4, w_5) は 15 個であり、それらの (w_2, w_3) は、既知の 15 個の既約加群 $M^{i,j}$ のトップレベルへの $o(\omega)$ と $o(W^3)$ の作用の値の組 $(o(\omega), o(W^3))$ に一致する。

以上により、次の定理が得られる。

定理 4.1 $\ell = 5$ のとき、 \mathcal{W} の Zhu 代数 $A(\mathcal{W})$ は $[\omega]^m, 0 \leq m \leq 8, [\omega]^n * [W^3], 0 \leq n \leq 5$ を基底とする 15 次元の可換結合代数で、 $\mathbb{C}[w_2, w_3, w_4, w_5]/\mathcal{P}$ と同型である。また、 \mathcal{W} の既約加群は $M^{i,j}, 0 \leq i \leq 5, 0 \leq j \leq i$ (ただし $M^{i,i} \cong M^{5-i,0}$) の 15 個に限る。

最後に、 $\ell = 5$ のときの $o(\omega)$ と $o(W^3)$ の $M^{i,j}, 0 \leq i \leq 5, 0 \leq j \leq i$ のトップレベルへの作用の値の表を添付する。 $M^{i,i} \cong M^{5-i,0}$ に注意する。 θ により $M^{i,j} \mapsto M^{i,i-j}$ であり、 $\theta W^3 = -W^3$ なので、 $o(W^3)$ の $M^{i,i-j}$ のトップレベルへの作用は、 $M^{i,j}$ のトップレベルへの作用の -1 倍である。特に、 $M^{i,j} \cong M^{i,i-j}$ となる場合、 $M^{i,j}$ のトップレベルに $o(W^3)$ は 0 として作用する。

(i, j)	$o(\omega)$	$o(W^3)$	(i, j)	$o(\omega)$	$o(W^3)$
(0, 0)	0	0	(4, 0)	2/35	-12
(1, 0)	2/35	12	(4, 1)	23/35	-234
(1, 1)	2/35	-12	(4, 2)	6/7	0
(2, 0)	3/35	6	(4, 3)	23/35	234
(2, 1)	2/7	0	(4, 4)	2/35	12
(2, 2)	3/35	-6	(5, 0)	0	0
(3, 0)	3/35	-6	(5, 1)	4/5	-456
(3, 1)	17/35	-78	(5, 2)	6/5	-228
(3, 2)	17/35	78	(5, 3)	6/5	228
(3, 3)	3/35	6	(5, 4)	4/5	456
			(5, 5)	0	0

参考文献

- [1] R. Blumenhagen, W. Eholzer, A. Honecker, K. Hornfeck and R. Hübel, Coset realization of unifying W algebras, *Internat. J. Modern Physics A* **10** (1995), 2367-2430.
- [2] A. Cappelli, L. S. Georgiev, I. T. Todorov, Parafermion Hall states from coset projections of abelian conformal theories, *Nuclear Physics B* **599** (2001), 499-530.
- [3] C. Dong, personal communication.
- [4] C. Dong and J. Lepowsky, The algebraic structure of relative twisted vertex operators, *J. Pure and Applied Algebra* **110**(1996), 259-295.
- [5] C. Dong and K. Nagatomo, Representations of vertex operator algebra V_L^+ for rank one lattice L , *Comm. Math. Phys* **202** (1999), 169-195.
- [6] V. G. Kac, *Infinite-dimensional Lie Algebras* 3rd ed., Cambridge University Press, Cambridge, 1990.
- [7] M. Kitazume, M. Miyamoto and H. Yamada, Ternary codes and vertex operator algebras, *J. Algebra*, **223** (2000), 379-395.
- [8] C. H. Lam, personal communication.
- [9] C. H. Lam and H. Yamada, Decomposition of the lattice vertex operator algebra $V_{\sqrt{2}A_1}$, *J. Algebra* **272** (2004), 614-624.
- [10] J. Lepowsky and H.-S Li, *Introduction to Vertex Operator Algebras and Their Representations*, Birkhäuser, Boston, 2004.

Verlinde 予想の証明に対する一考察 (群論的、高次元結晶的考察)

宮本雅彦 (筑波大学数理物質科学研究科)
近畿大学ノーベンバーホールにて

平成19年6月29日

序文

Verlinde 公式とはある種の物理模型に対する公式であり、非常に簡潔な公式である。ここでは、Verlinde 公式の本当の意味を理解するために、Huang が証明した設定を広げてどのような現象が起こるかを代数の立場から簡単に考察しよう。

代数 V とその既約加群 $W^1 \cong V, \dots, W^k$ の集合があり、加群のテンソル積 $W^i \otimes W^j = \bigoplus_{r=1}^k N_{ij}^r W^r$ (N_{ij}^r は重複度でフュージョン規則と呼ばれる) が定義されており、また加群の指標関数 (またはトレース関数) $\text{ch}_{W^i}(\tau)$ 達の張る空間がモジュラー不変性を持つ、例えば、モジュラー群の元 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ の与える変換 $\tau \rightarrow -1/\tau$ によって指標関数を変換したものが $\text{ch}_{W^j}(\tau)$ の線形和

$$\text{ch}_{W^i}(-1/\tau) = \sum S_i^j \text{ch}_{W^j}(\tau)$$

となっているとき、Verlinde 公式とは、フュージョン規則と上の変換の係数に関係があることを示すもので、 N_{ij}^r を S_a^b 達を使って表示する公式である。特に、注目された性質としては、行列 $S = (S_{ij})$ によって $N(a) = (N_{ai}^j)$ が対角化されることが多い。

Verlinde 公式

$S_1^a \neq 0$ であり、

$$N_{ij}^r = \sum_{s=1}^k \frac{S_i^s S_j^s S_s^r}{S_1^s}$$

これまで知られている結果を簡単に述べると、

個々の物理モデル(共形場理論)に対しては色々な場合に計算されており、

上屋-山田-上野、Beauville-Laszlo、Faltings、Kumar-Narasimhan-Ramanathan ... などの結果がある。

ごく最近、上の結果達を含む形で、幾つかの条件を仮定するが、頂点作用素代数の公理から一般論として Verlinde 公式が Yi-Zhi Huang によって証明された。Vertex operator algebras and the Verlinde conjecture, math.QA/0406291.

条件は、

- (1) 頂点作用素代数 V が不変内積を持ち、
- (2) C_2 -有限条件を満たし、かつ
- (3) すべての加群が完全可約、このような頂点作用素代数を有理と呼ぶ。(これらの用語の説明は後で述べる)

これからの問題への考察:

Point 1: 頂点作用素代数が C_2 -有限と呼ばれる条件を満たしていれば、有理性の条件がなくても、テンソル積も自然に定義され、モジュラー不変性も満たされている [Mi1]。Huang の証明は本質的に直接計算だが、 S -変換の行列 S_{ij}^g によって N_{ij} が対角化されることを示しており、そこでの本質はテンソル積とモジュラー不変性である。それ故、 C_2 -有限条件の下で Verlinde 公式の類似したものが存在していて不思議はない。

Point 2: C_2 -有限だけでは有理ではないので、対角化出来ないと考えるのが自然である。その場合、Verlinde 予想に対応するものはどのようなものになるだろうか? N_{ij}^g と S_{ij}^g の間に関係があるだろうか? 現在のところ、Verlinde 予想を拡張した形のものも与えられていない。それゆえ、新しい解釈を与える可能性がある。

理由は、テンソル積が既約加群の直和でない場合、[Mi1]におけるモジュラー変換の証明でつかった pseudo-trace 関数と同様に、 $\log z$ 型の項に対応するある種の新しい因子を考える必要がある。ただ、[Mi2]で示したように、射影加群は各既約加群に対応して一意的に決まり、これが大きな役割を果たすと期待できる。

Point 3: Verlinde 公式の分母 S_{11}^g に対して $S_{11}^g \neq 0$ が証明できるか?

これが出来れば、加群のテンソル積の平坦性が出てくる。

Point 4: Huang の論文の Key Point は3次対称群と同型な自己同型群 S_3 と交絡作用素の積の結合性との関係である。ただ、Huang の論文は非常に長い直接計算で、あまり読みやすいものでない。タイプミスや計算間違いもかなりあるが、本質的な誤りはないと判断できる。それ故、この部分をわかり易くすることが今後の展開にとって必要となる。

講演の内容

I. 準備

II. 3次対称群の交絡作用素への作用

III. 交絡作用素の積に作用する群と正三角形の張り合わせ?

I. 準備

I-1. 元: 量子作用素

ベクトル空間 W 上の線形変換 $\{a_n \in \text{End}(W), n \in \mathbb{Z}\}$ を係数とする無限級数

$$a(z) = \sum a_n z^{-n-1}$$

が量子作用素であるとは、任意の $w \in W$ に対して、 $a(z)w$ が下に有界な Laurent 級数になっていること、即ち、ある整数 N があって、 $n > N$ となるすべての n に対して $a_n w = 0$ となることである。

I-2. 積: 正規積 上の量子作用素同士の間無限個の積 (n -th 正規積と呼ぶ) が定義できる。

W 上の量子作用素 $a(z), b(z)$ と整数 $n \in \mathbb{Z}$ に対して、

$$a(z) *_{n} b(z) = \text{Res}_x \{(x-z)^n a(x)b(z) - (-z+x)^n b(z)a(x)\}$$

を定義すると、これも量子作用素となる。ここで、 Res_x は x^{-1} の係数をとる作用 (留数のようなもの) であり、また

$$(-z+x)^n = \sum_{i=0}^{\infty} \binom{n}{i} (-z)^{n-i} x^i, \quad \binom{n}{i} = \frac{n(n-1)\cdots(n-i+1)}{i!}$$

である。

特に、十分大きな n に対して、 $a(z) *_{n} b(z) = 0$ となる簡単な条件として、ある N があって

$$(x-z)^N \{a(x)b(z) - b(z)a(x)\} = 0$$

となることがある。この条件を局所可換とよぶ。

I-3 代数: 頂点作用素代数

○ N -次数付きのベクトル空間 (次数をウェイトと呼ぶ) $W = \bigoplus_{n=0}^{\infty} W_n$ 上に

○ 無限個の積 $v, u \in V, m \in \mathbb{Z} \Rightarrow v_m u \in V$ (i.e. $v_m \in \text{End}(V)$) を持ち、

$$v \in V_{\text{wt}(v)}, u \in V_{\text{wt}(u)} \Rightarrow v_n u \in V_{\text{wt}(v) + \text{wt}(u) \cdot n - 1}$$

母関数 $Y(v, z) = \sum v_n z^{-n-1}$ で表示する。 v の頂点作用素と呼ぶ。 これらが互いに局所可換な量子作用素となっていること。

本質的な性質：互いに局所可換, i.e. $v, u, w \in V$ に対して、 $z_1 \neq z_2$ 上で関数として

$$\langle v', Y(v, z_1)Y(u, z_2)w \rangle = \langle v', Y(u, z_2)Y(v, z_1)w \rangle$$

ここで、 $\langle v', * \rangle \in \text{Hom}(V, \mathbb{C})$

○ 次数作用素 ω_1 を与える特別な元 (ヴィラソロ元) $\omega \in V_2$ がある。

ヴィラソロ元とは、 $L(n) = \omega_{1+n}$ と置くと、ヴィラソロ関係式

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

を満たしている。

微分作用素 $\omega_0 = L(-1)$ は $Y(L(-1)v, z) = \frac{d}{dz} Y(v, z)$ を満たしている。

1-4. 加群： V -加群

次数付きベクトル空間の直和

$$W = \bigoplus_{n=0}^{\infty} W_{r+n} \quad \exists r \in \mathbb{Q}$$

$$v \in V, n \in \mathbb{Z}, \Rightarrow \exists v_n \in \text{End}(W^i)$$

母関数 $Y^W(v, z) = \sum v_n z^{-n-1}$ で表示し、加群への頂点作用素と呼ぶ。

互いに局所可換で、代数として V の表現となっている。

制限双対空間 (重要な player)

$$W' = \bigoplus_{n=0}^{\infty} \text{Hom}(W_{r+n}, \mathbb{C})$$

を考え、 $W' \times W$ 上の自然な内積

$$\langle \cdot, \cdot \rangle : W' \times W \rightarrow \mathbb{C}$$

を使って、

$$\langle Y^{W'}(v, z)w', w \rangle = \langle w', Y^W(\dots v, 1/z)w \rangle$$

で $Y^{W'}$ を考えると、 W' も V -加群となる。

1-5. 有限条件： V に適切な有限条件 (C_2 -有限など) を付け加えることで、かなり自然なものを対象とする。

○ 既約加群の同型類の個数は有限 $V = W^1, \dots, W^k$

○ ウェイトはすべて有理数

○ 下で説明するモジュラー不変性が成り立っている。

例えば、Zhu が技術的な理由で導入した条件であるが、

定義 部分空間として、 $\langle a_n b \mid n \leq -2, a, b \in V \rangle$ が V の中で有限余次元を持つとき、 V は C_2 -有限条件を満たすと呼ぶ。

この時、上の条件はすべて満たしており、知られている有限型の頂点作用素代数はすべて C_2 -有限条件を満たしている。

○ Huang の証明を説明するために、 V は C_2 -有限条件を満たし、さらに有理型であると仮定する。即ち、加群はすべて完全可約（既約加群の直和）と仮定する。

1-6. モジュラー不変：

$v \in V_n$ と $W = \bigoplus_{n=0}^{\infty} W_{n+r}$ に対して、

$$\begin{aligned} S_W(v, \tau) &:= \text{tr}_W \rho(v) q^{\tau(\alpha(v)-c/24)} \\ &= \text{tr}_{W_{r+n}} v_{n-1} e^{2\pi i(r+n-c/24)\tau} \end{aligned}$$

は上半平面 (τ の虚部 > 0) 上で絶対収束する関数となる。

しかも、モジュラー不変性がある。

$$\begin{aligned} PSL_2(\mathbb{Z}) &= \langle \tau \rightarrow \tau + 1, \tau \rightarrow -1/\tau \rangle \\ S(v, \tau + 1) &= e^{2\pi i(r-c/24)} S(v, \tau) \\ \left(\frac{1}{\tau}\right)^{\text{wt}(v)} S_{W'}(v, -1/\tau) &= \sum S_i^j S_{W_j}(v, \tau) \end{aligned}$$

係数 S_i^j が出てくる。 $S = (S_i^j)$ は $k \times k$ -行列である。

1-7. 交絡作用素とテンソル積：

V -加群 W, U, T に対して、

$$w \in W, m \in \mathbb{Q} \text{ に対して } w_m \in \text{Hom}(U, T)$$

$I(w, z) = \sum_{m \in \mathbb{Q}} w_m z^{-m-1}$ で表示し、 w の交絡作用素とよぶ。

これは V のすべての元の作用（頂点作用素）と局所可換であり、かつ $L(-1)$ -微分性と結合性を満たしている。

$L(-1)$ -微分性とは、 $I(L(-1)w, z) = \frac{d}{dz} I(w, z)$ であり、

結合性とは、 $I(v_n w, z) = Y(v, z) \cdot_n I(w, z)$ がすべての $v \in V, w \in W, n \in \mathbb{Z}$ に対して成り立つことである。

$$\langle w_m u \mid w \in W, u \in U \rangle = T$$

となるとき I を全射と呼ぶ。

W^i, W^j を固定すると、交絡作用素 $I(W^i \times W^j \rightarrow T)$ で全射となるようなものがある T の中に (同型を無視して) 最大のものがある。この時の T を $W^i \boxtimes W^j$ で表す。

加群が完全可約なので、

$$W^i \boxtimes W^j = \bigoplus_{r=1}^k N_{ij}^r W^r$$
 N_{ij}^r は重複度で、これをフージョン規則と呼んでいます。

II. 交絡作用素の積への群の作用 (Huang)

有限生成 V -加群 W, U, T と交絡作用素 $\mathcal{Y} \in I(W \times U \rightarrow T)$ に対して、 σ_{12}, σ_{23} を次のように定義する。

○ $\sigma_{12}(\mathcal{Y}) \in I(U \times W \rightarrow T)$ を skew-symmetry を使って

$$\sigma_{12}(\mathcal{Y})(u, z)w := e^{\pi i(\text{wt}(U) + \text{wt}(W) - \text{wt}(T))} e^{zL_{-1}} \mathcal{Y}(w, e^{\pi i} z)u$$

ここで、 $w \in W, u \in U$ で、 $\text{wt}(U)$ 等は U の最小ウエイトを表す。

$e^{\pi i}$ は -1 の事で、以下 -1 で表す。ただ、 z は整数べきとは限らないことに注意。

○ $\sigma_{13}(\mathcal{Y}) \in I(W \times T' \rightarrow U')$ を制限双対加群の交絡作用素を使って、

$$\langle \sigma_{13}(\mathcal{Y})(w, x)l', u \rangle = \langle l', \mathcal{Y}(e^{xL(1)}(e^{-\pi i} x^{-2})^{L(0)} w, x^{-1})u \rangle$$

w, u, l' が singular vectors 即ち、 $L(1)w = L(1)u = L(1)l' = 0$ なら

$$\langle \sigma_{23}(\mathcal{Y})(w, x)l', u \rangle = e^{-\pi i \text{wt}(w)} x^{-2\text{wt}(w)} \langle l', \mathcal{Y}(w, x^{-1})u \rangle$$

補題 [Huang] σ_{12}, σ_{23} は (12), (23) $\in S_3$ の表現となっている。

III. 交絡作用素の積への置換

III-1. 置換 τ の定義 : $\mathcal{Y}^2 \in I(B \times A \rightarrow F), \mathcal{Y}^1 \in I(C \times F \rightarrow D)$ に対して、

$$P(d', c, b, a; z_1, z_2) = \langle d', \mathcal{Y}^1(c, z_1) \mathcal{Y}^2(b, z_2) a \rangle$$

が考えられる。

$\exists k$ s.t. $z_2^k P(d', c, b, a; z_1, z_2)$ は一変数 $z = z_1/z_2$ 関数と見ることができ、確定特異点型の微分方程式を満たし、 $|z_1| > |z_2| > 0$ の範囲で絶対収束する。

この関数を $|z_2| > |z_1 - z_2| > 0$ の範囲で展開すると、 $\mathcal{Y}^3, \mathcal{Y}^4$ があって、

$$P(d', c, b, a; z_1, z_2) = \langle d', \mathcal{Y}^3(\mathcal{Y}^4(c, z_1 - z_2)b, z_2) a \rangle$$

積に置換 σ_{12} を作用せると、

$$P(d', c, b, a; z_1, z_2) = \langle d', \mathcal{Y}^1(c, z_1 - z_2) \sigma_{12}(\mathcal{Y}^2)(a, -z_2) b \rangle$$

先の結合展開を置換として見る。

$$\begin{aligned}
& P(d', c, b, a; z_1, z_2) \\
&= \langle d', \mathcal{Y}^1(c, z_1) \mathcal{Y}^2(b, z_2) a \rangle \\
&= \langle d', \mathcal{Y}^3(\mathcal{Y}^4(c, z_1 - z_2) b, z_2) a \rangle \\
&= \langle d', \sigma_{12}(\mathcal{Y}^3)(a, -z_2) \mathcal{Y}^4(c, z_1 - z_2) b \rangle
\end{aligned}$$

この置換を τ で表す。

$$\begin{aligned}
\langle d', \mathcal{Y}^1(c, z_1) \mathcal{Y}^2(b, z_2) a \rangle &= \langle d', \tau_1(\mathcal{Y}^1 \mathcal{Y}^2)(a, -z_2) \tau_2(\mathcal{Y}^1 \mathcal{Y}^2)(c, z_1 - z_2) b \rangle \\
\sigma_{12} \tau_1(\mathcal{Y}^1 \mathcal{Y}^2) &= \mathcal{Y}^3, \quad \tau_2(\mathcal{Y}^1 \mathcal{Y}^2) = \mathcal{Y}^4 \\
a, b, c \text{ に対する置換も位数 } 3, \text{ 変数の変換 } &\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \text{ も位数 } 3 \text{ なので,}
\end{aligned}$$

Lemma $\tau^3 = 1.$

III-2. Huang の証明と (穴あき) 正 8 面体:

交絡作用素全体を $\oplus W^i$ から $\oplus W^i$ への交絡作用素とみて、そのベクトル空間の基底を $\{\mathcal{Y}_s : s \in X\}$ を決め $\mathcal{Y}^3(\mathcal{Y}^4)$ 達を $\mathcal{Y}_s \mathcal{Y}_t$ 達の線形和

$$\mathcal{Y}^3(\mathcal{Y}^4) = \sum_{s,t} F(\mathcal{Y}^1 \mathcal{Y}^2 : \mathcal{Y}_s \mathcal{Y}_t) \mathcal{Y}_s \mathcal{Y}_t$$

の形で表示している。すると、 F は $|X|^2$ 次の正則行列となる。その逆行列を F^{-1} で表している。

○ 例えば、Huang の論文の (3.5) 式

$$F^{-1}(\mathcal{Y}^1 \mathcal{Y}^2 : \mathcal{Y}_s \mathcal{Y}_t) = F(\sigma_{12}(\mathcal{Y}^1) \sigma_{12}(\mathcal{Y}^2) : \sigma_{12}(\mathcal{Y}_s) \sigma_{12}(\mathcal{Y}_t))$$

基底は $\sigma_{12}(\mathcal{Y}_s)$ で展開

これは τ が σ_{12} を b に作用することで invert されることと同値

○ Huang の論文の (3.12) 式

$$F(\mathcal{Y}^1 \otimes \mathcal{Y}^2; \mathcal{Y}^3 \otimes \mathcal{Y}^4) = F(\sigma_{12} \sigma_{13}(\mathcal{Y}^2) \sigma_{13} \sigma_{12}(\mathcal{Y}^1); \sigma_{13} \sigma_{12}(\mathcal{Y}^4) \sigma_{12} \sigma_{13}(\mathcal{Y}^3))$$

これは正 8 面体 (の 4 つの面だけ残したもの) を使って説明すると、自然であることがわかる。

正 8 面体の (回転) 自己同型群はよく知られているように、4 次対称群 S_4 である。 S_4 はもう一つの 3 次元既約表現を持っているが、この表現は余り良く扱われていない。頂点作用素代数における上の 3 点関数に対する作用として出てくる群 S_4 の表現はこのもう一つの 3 次元既約表現である。正 8 面体の 8 つの面から交互に面を取り除くと、辺では隣接していない 4 つの面が残る。この 4 つの面だけ残した正 8 面体の自己同型は 4 次交代群である。新しい位数 2 の自己同型として、この頂点だけでつながった 4 つの面を裏返しにする操作を加えると、4 つの面だけ残した正 8 面体の自己同型群も 4 次対称群となる。

講演では正 8 面体 (の 4 つの面だけ残したもの) を利用して説明したが、これを図で表示して説明するのは困難なので、省略する。

可換代数から構成される頂点代数の 加群について

田辺顕一郎 (北海道大学大学院理学研究科)

1 動機と準備

頂点代数とは1986年に Borchers[1] によって導入された無限個の積を持つ代数系である。まず定義を紹介する。以下 x は変数とする。

定義. (頂点代数) 次の条件を満たす三つ組み $(V, Y, 1)$ を頂点代数という。

- (1) V は \mathbb{C} 上のベクトル空間.
- (2) $Y(\cdot, x)$ は V から $(\text{End } V)[[x, x^{-1}]]$ への線型写像. $a \in V$ に対して $Y(a, x) = \sum_{i \in \mathbb{Z}} a_i x^{-i-1}$ とする.
- (3) $a \in V, u \in V$ に対して $Y(a, x)u \in V((x))$.
- (4) $1 \in V$ で $Y(1, x) = \text{id}_V = 1_{-1}x^{-(-1)-1}$.
- (5) $a \in V$ に対して $a_n 1 = 0, n \geq 0$, と $a_{-1} 1 = a$.
- (6) (Borchers 恒等式) $a, b \in V, u \in V, l, m, n \in \mathbb{Z}$ に対して

$$\sum_{i=0}^{\infty} \binom{m}{i} (a_{l+i} b)_{m+n-i} u = \sum_{i=0}^{\infty} \binom{l}{i} (-1)^i (a_{l+m-i} b_{n+i} + (-1)^{l+1} b_{l+n-i} a_{m+i}) u.$$

頂点代数に、Virasoro 元と呼ばれる特別な元の存在とさらにいくつかの条件を課したものを頂点作用素代数という。有名なムーンシャイン予想に登場するムーンシャイン頂点作用素代数はその代表例である。ただし今回扱うものは頂点作用素代数ではなく頂点代数である。

頂点代数 V に対して線型写像 $D: V \rightarrow V (u \mapsto u_{-2} 1)$ を定める。次が成り立つ。

命題 1. $a \in V$ に対して $Y(Da, x) = \frac{d}{dx} Y(a, x)$.

Proof. $l = -2, m = 0$ として Borcherds 恒等式を用いる.

$$\begin{aligned}
 (Da)_n &= (a_{-2}1)_n = \sum_{i=0}^{\infty} \binom{-2}{i} (-1)^i (a_{-2-i}1_{n+i} + (-1)^{-2+1}1_{-2+n-i}a_i) \\
 &= \sum_{i=0}^{\infty} (i+1)a_{-2-i}\delta_{n+i,-1} - \sum_{i=0}^{\infty} (i+1)\delta_{-2+n-i,-1}a_i \\
 &= \sum_{i=0}^{\infty} (i+1)a_{-2-i}\delta_{n,-i-1} - \sum_{i=0}^{\infty} (i+1)\delta_{n,i+1}a_i \\
 &= \sum_{i<0}^{\infty} (-i-1)a_i\delta_{n,i+1} - \sum_{i=0}^{\infty} (i+1)\delta_{n,i+1}a_i = \sum_{i \in \mathbb{Z}} (-i-1)a_i\delta_{n,i+1} = -na_{n-1}.
 \end{aligned}$$

□

Borcherds[1] は \mathbb{C} 上の可換代数とその上の微分を用いて頂点代数が構成できること、さらにそのようにして構成できる頂点代数の特徴付けを与えた. ここで \mathbb{C} 上の可換代数 A 上の微分 D とは $D(ab) = (Da)b + a(Db)$ を満たす線型写像 $D: A \rightarrow A$ のことである.

命題 2. (Borcherds)

(1) A を \mathbb{C} 上の可換代数、 D を A 上の微分とする.

$$a, b \in A \text{ に対して } Y(a, x)b = \sum_{i=0}^{\infty} \left(\frac{D^i}{i!}a\right)bx^i \in (\text{End } V)[[x]].$$

と定めると、 $(A, Y, 1_A)$ は頂点代数となる. ここで 1_A は A の単位元.

(2) 任意の $u \in V$ に対して $Y(u, x) \in (\text{End } V)[[x]]$ となる頂点代数 $(V, Y, 1)$ が与えられたとする. V 上の積と、写像 $D: V \rightarrow V$ を次で定める.

$$(\text{積}) \quad u, v \in V \text{ に対して } u \cdot v = u_{-1}v. \quad (\text{写像}) \quad D: V \rightarrow V \quad (u \mapsto u_{-2}1)$$

この時、 V は 1 を単位元とする \mathbb{C} 上の可換代数、 D は V 上の微分となる.

(1),(2) は互いに逆構成を与えていることに注意する. また (A, D) から構成された頂点代数 $(A, Y, 1_A)$ に対して $Da = Da$ ($a \in A$) となっている. 命題の証明は微分の性質を用いて直接計算で与えられるので省略する. 可換代数 A とその上の微分 D から構成される頂点代数は、 A が有限次元かつ $D = 0$ の場合を除いて頂点作用素代数とはならない.

次に頂点代数の加群を考える. 以下 V は頂点代数をあらわすこととする.

定義. (頂点代数の加群) 次の条件を満たす組み (M, Y_M) を V 加群という.

- (1) M は \mathbb{C} 上のベクトル空間.
- (2) $Y_M(\cdot, x)$ は V から $(\text{End } M)[[x, x^{-1}]]$ への線型写像. $a \in V$ に対して $Y_M(a, x) = \sum_{i \in \mathbb{Z}} a_i x^{-i-1}$ とする.
- (3) $a \in V, u \in M$ に対して $Y_M(a, x)u \in M((x))$.
- (4) $Y_M(1, x) = \text{id}_M$.
- (5) (Borcherds 恒等式) $a, b \in V, u \in M, l, m, n \in \mathbb{Z}$ に対して

$$\sum_{i=0}^{\infty} \binom{m}{i} (a_{l+i}b)_{m+n-i}u = \sum_{i=0}^{\infty} \binom{l}{i} (-1)^i (a_{l+m-i}b_{n+i} + (-1)^{i+1} b_{l+n-i}a_{m+i})u.$$

以下 A を \mathbb{C} 上の可換代数, D を A 上の微分とする. 可換代数から頂点代数を構成したのと同じ方法で, 代数としての A 加群から頂点代数としての A 加群を構成することが出来る.

命題 3. (Borcherds)

- (1) M を代数としての A 加群とする.

$$a \in A, u \in M \text{ に対して } Y_M(a, x)u = \sum_{i=0}^{\infty} \left(\frac{D^i}{i!} a \right) u x^i \in (\text{End } M)[[x]].$$

と定めると, (M, Y_M) は頂点代数としての A 加群となる.

- (2) 任意の $a \in A$ に対して $Y_M(a, x) \in (\text{End } M)[[x]]$ となる頂点代数としての A 加群 (M, Y_M) が与えられたとする. A の M 上の作用を

$$(\text{作用}) \quad a \in A, u \in V \text{ に対して } a \cdot u = a_{-1}u$$

と定める. この時, M は代数としての A 加群となる.

命題 2 と同様に (1), (2) は互いに逆構成を与えている. ここで, 命題 2 と 3 は頂点代数としての A 加群が代数としての A 加群から全て得られることを保証していないことに注意しなければならない. この点は既に Borcherds 自身によって指摘されている. しかしながら可換代数から構成される頂点代数は, 一般に頂点作用素代数にならない為, その加群についての詳しい研究はこれまでおこなわれてこなかったようである. 可換代数 A に対して, 代数としての加群と頂点代数としての加群との違いを調べるのが今回の研究の動機である.

以下, 頂点代数としての A 加群と, 代数としての A 加群を表示

A 加群_(VA) (頂点代数としての加群), A 加群_(Alg) (代数としての加群).

を用いて区別することにする。今回は A が一変数多項式環 $\mathbb{C}[t]$ の場合に、 $\mathbb{C}[t]$ 加群 (Alg) から構成されない有限次元 $\mathbb{C}[t]$ 加群 (VA) を分類することが出来たので報告する。実際、特定の微分に対してはそのような有限次元 $\mathbb{C}[t]$ 加群 (VA) が存在する。したがって A 加群 (VA) の研究は、一般の頂点代数の表現の考察に役立つものと期待出来る。

$\mathbb{C}[t]$ 加群 (VA) を考察するために次のよく知られた結果 (cf. [2, Proposition 4.8]) を用いる。

補題 4. \mathbb{C} 上のベクトル空間 M と、 V から $(\text{End } M)[[x, x^{-1}]]$ への線型写像 $Y_M(\cdot, x)$ が与えられたとする。この時、 (M, Y_M) が V 加群となるための必要十分条件は、次の 5 つの条件が満たされることである：

$$(M1) \quad u \in V, w \in M \text{ に対して } Y_M(u, x)w \in M((x)).$$

$$(M2) \quad Y_M(1, x) = \text{id}_M.$$

$$(M3) \quad u, v \in V, i, j \in \mathbb{Z} \text{ に対して } [u_i, v_j] = \sum_{k=0}^{\infty} \binom{i}{k} (u_k v)_{i+j-k}.$$

$$(M4) \quad u, v \in V \text{ に対して,}$$

$$Y_M(u_{-1}v, x_1) = \text{Res}_x \left((x_1 - x)^{-1} Y_M(u, x_1) Y_M(v, x) - (-x + x_1)^{-1} Y_M(v, x) Y_M(u, x_1) \right).$$

$$(M5) \quad u \in V \text{ に対して } Y_M(Du, x) = \frac{d}{dx} Y_M(u, x).$$

2 頂点代数としての有限次元 $\mathbb{C}[t]$ 加群

今回調べるのは有限次元 $\mathbb{C}[t]$ 加群 (VA) であるので補題 4 の判定条件は次のように簡単になる。

補題 5. M を \mathbb{C} 上の有限次元ベクトル空間、 $T(x) = \sum_{i \in \mathbb{Z}} T_{(i)} x^i \in (\text{End } M)[[x, x^{-1}]]$ とする。この時、 $Y_M(t, x) = T(x)$ となる $\mathbb{C}[t]$ 加群 (VA) が存在するための必要十分条件は $T(x)$ が次の三つの条件を満たすことである：

$$(i) \quad T(x) \in (\text{End } M)((x)).$$

$$(ii) \quad i, j \in \mathbb{Z} \text{ に対して } T_{(i)} T_{(j)} = T_{(j)} T_{(i)}.$$

$$(iii) \quad \frac{d}{dx} T(x) = f(T(x)).$$

この場合、 $P(t) \in \mathbb{C}[t]$ に対して $Y_M(P(t), x) = P(Y_M(t, x))$ となる。特に (M, Y_M) は $Y_M(t, x) = T(x)$ から一意的に決まる。また (M, Y_M) が A 加群 (Alg) から構成されないための必要十分条件は $T(x) \notin (\text{End } M)[[x]]$ である。

$\mathbb{C}[t]$ 上の任意の微分 D は $D = f(t)\frac{d}{dt}$, $f(t) \in \mathbb{C}[t]$, の形に表すことが出来ることに注意しておく. 補題 5 を用いて次のように有限次元 $\mathbb{C}[t]$ 加群 (VA) を分類することが出来る.

主定理. $D = f(t)\frac{d}{dt}$, $f(t) \in \mathbb{C}[t]$, を $\mathbb{C}[t]$ 上の微分とする. $\mathbb{C}[t]$ 加群 (Alg) から構成されない有限次元 $\mathbb{C}[t]$ 加群 (VA) が存在する為の必要十分条件は $f(t) \neq 0$ かつ $\deg f(t) = 2$ である.

$f(t) = c(t - \alpha)(t - \beta)$, $c \neq 0$ とする. 任意の正の整数 n に対してそのような n 次元直既約 $\mathbb{C}[t]$ 加群 (VA) は, $Y_{M_n}(t, x)$ が以下で定められる $\mathbb{C}[t]$ 加群 (VA) (M_n, Y_{M_n}) に同型である:

(1) $\alpha = \beta$ の場合. $M_n = \mathbb{C}^n$ で

$$\begin{aligned} Y_{M_n}(t, x) &= \alpha - \frac{1}{c}x^{-1}(E_n - x^{-1}J_n)^{-1} \\ &= \alpha - \frac{1}{c} \sum_{i=0}^{\infty} J_n^i x^{-i-1}. \end{aligned}$$

(2) $\alpha \neq \beta$ の場合. $M_n = \mathbb{C}^n$ で

$$\begin{aligned} Y_{M_n}(t, x) &= \alpha + (\alpha - \beta)(-1 + \exp(-c(\alpha - \beta)x))^{-1} \\ &\quad \times \left(E_n - \frac{\exp(-c(\alpha - \beta)x)}{-1 + \exp(-c(\alpha - \beta)x)} J_n \right)^{-1}. \end{aligned}$$

ここで E_n は n 次単位行列, J_n は

$$J_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & & & \ddots & 1 \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix}.$$

である.

参考文献

- [1] R. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster, *Proc. Nat. Acad. Sci. U.S.A.* **83** (1986), 3068-3071.
- [2] V. G. Kac, *Vertex Algebras for Beginners*, University Lecture Series, Vol. 10, Amer. Math. Soc., 1997.

On Ising vectors in the VOAs associated with lattices

島倉 裕樹 (Hiroki Shimakura)

千葉大学大学院理学研究科
Graduate School of Science, Chiba University
e-mail: shima@math.s.chiba-u.ac.jp

序

本稿では偶格子 L に付随する頂点作用素代数 (VOA) である V_L^+ のイジング元について述べる. この研究は国立成功大学の Ching Hung Lam 氏との共同研究 [LS] の一部である. ここで考える頂点作用素代数 V は複素数体上であり, $V = \bigoplus_{n=0}^{\infty} V_n$ としたときに $V_0 = \mathbf{C}1$ かつ $V_1 = 0$ である.¹ VOA の定義の詳細は [Bo86, FLM88] を参照していただきたい.

1 準備

1.1 イジング元

この節ではイジング元について述べる.

定義 1.1. V_2 の元 e がイジング元であるとは e が生成する部分頂点代数 $VA(e)$ が中心電荷 $1/2$ の単純ヴィラソロ VOA $L(1/2, 0)$ と同型であって, e がそのヴィラソロ元となることである.

このイジング元は VOA の構造, 表現論, 自己同型群等を調べるのに有用である. ここでは自己同型との関係について述べよう. e を VOA V のイジング元とする. $VA(e) \cong L(1/2, 0)$ の既約加群は $L(1/2, h)$ ($h = 0, 1/2, 1/16$) の 3 つのいずれかと同型であり, また, 有理的であるので, 任意の $L(1/2, 0)$ -加群は既約加群の直和に分解する. そこで, $V(h)$ で V の既約 $VA(e)$ -部分加群で $L(1/2, h)$ と同型なもの全体の成す V の部分加群を表すとする. すると, V は $VA(e)$ -加群として

$$V = V(0) \oplus V(1/2) \oplus V(1/16)$$

¹ $V_1 = 0$ の仮定がなくてもイジング元を考えることは出来る. しかし, $V_1 \neq 0$ の場合は V_1 の元の 0-積から作られる自己同型群が無限群になることが多く, その作用によって無限個のイジング元が存在することが多い. よって, イジング元の特徴付けを考えようとする際には難しくなると思われる.

と分解される. そこで, V 上の線形写像 τ_e を

$$\tau_e = \begin{cases} 1 & \text{on } V(0) \oplus V(1/2), \\ -1 & \text{on } V(1/16), \end{cases}$$

と定めると分岐則から V の VOA としての自己同型となる ([Mi96a]). また V の τ_e による固定部分 VOA $V^{\tau_e} = V(0) \oplus V(1/2)$ 上の線形写像 σ_e を

$$\sigma_e = \begin{cases} 1 & \text{on } V(0), \\ -1 & \text{on } V(1/2), \end{cases}$$

と定めるとやはり分岐則から σ_e は V^{τ_e} の自己同型となる ([Mi96a]). 本稿では $\tau_e \neq 1$ のとき e を τ -型, $\tau_e = 1$ の時に σ -型と呼ぶ.

次は基本的かつ重要な問題である.

問題 1.2. VOA のイジング元を分類せよ.

もちろん, 一般の VOA に対して考えるのは難しいが, いくつかの例ではイジング元が特徴付けられている.

(例 1) ([La99, LSY07])² C を長さ n の二元偶符号で, 重さ 2 の符号語を持たないとする. このとき C に付随する VOA³ M_C のイジング元は $16N + n$ 個ある. ただし, N は $[8, 4, 4]$ -ハミング符号の C への埋め込みの総数である. もう少し詳しく述べると, n 個のイジング元は M_C を定義する際に用いる $L(1/2, 0)^{\otimes n}$ に含まれるものであり, また C のハミング符号と同型なそれぞれの部分符号 H に対して, M_C の部分 VOA M_H がさらに 16 個イジング元を含む.

(例 2) ([Co85, Mi96a]) ムーンシャイン加群 V^\natural の自己同型群はモンスター単純群である. V^\natural のイジング元とモンスターの共役類 $2A$ に含まれる元との間の写像 $e \mapsto \tau_e$ は 1:1 対応である.⁴

そこで, この問題を偶格子 L に付随する V_L^+ に対して考えたい. ただし, $V_1 = 0$ の条件を満たすように L は長さ 2 の元を含まないものを考える.

²講演中は [LSY07] で書かれていると述べたが, 本質的な部分は [La99] で行われたと指摘を受けたので注意しておきます.

³ M_C の定義等は [Mi96b] 参照.

⁴これで特徴付けられているとはいえ, モンスターの全ての $2A$ の元の V^\natural への作用が具体的に記述されているわけではなく, またイジング元も具体的に記述されているわけでない. 単射性を意味する [Co85] の結果にはモンスターに関する深い群論 (例えば $2A$ の中心化群の構造など) が用いられていることを注意しておく.

1.2 頂点作用素代数 V_L^+

この節では簡単に V_L^+ について述べておく。詳細は [FLM88] 等を参照していただきたい。 L を正定値内積を持つ偶格子とし、 $L(n)$ で長さ n の元全体の集合を表すとす。このとき、 L に付随する格子 VOA V_L が構成できる。この VOA は格子の自己同型の持ち上げを自己同型としてもっていて、特に -1 倍する L の自己同型の持ち上げ θ を考える。そして、 V_L^+ で θ による固定点全体の集合を表すことにする。明らかに V_L^+ は V_L の部分 VOA となっている。

2 V_L^+ のイジング元

この章では V_L^+ のイジング元について考察する。

まず、次の二つの形のイジング元が存在することは知られていることに注意する。

- ([DMZ94]) L の長さ 4 の元 α に対して

$$\omega(\alpha)^\pm = \frac{1}{16}\alpha(-1)^{2\mathbf{1}} \pm \frac{1}{4}(e^\alpha + \theta(e^\alpha))$$

は V_L^+ のイジング元である。

- ([DLMN98]) E を $\sqrt{2}E_8$ と同型な L の部分格子として、 $\varphi \in \text{Hom}(E, \mathbb{Z}_2)$ とする。このとき、

$$e_{E,\varphi} = \frac{1}{16}\omega_{V_E^+} + \frac{1}{32} \sum_{\alpha \in E(4)/\{\pm 1\}} (-1)^{\varphi(\alpha)}(e^\alpha + \theta(e^\alpha))$$

は V_L^+ のイジング元である。

[LSY07] で次の予想が述べられている⁵。

予想 2.1. 長さ 2 の元を持たない偶格子 L に付随する V_L^+ のイジング元は $\omega(\alpha)^\pm$ と $e_{E,\varphi}$ で尽くされる。

実際に (例 1) に帰着させることで次が示されている。

命題 2.2. [LSY07] R をルート格子とする。このとき $L = \sqrt{2}R$ に対して、予想 2.1 は正しい。

そして、[LS] では次の結果が得られた。⁶

定理 2.3. リーチ格子 Λ に付随する VOA V_Λ^+ に対して、予想 2.1 は正しい。

⁵この予想が成り立つかどうかは未解決である。

⁶[LSY07, 注意 4.7] では私が定理 2.3 を示したとコメントされているが、その時点での証明は (例 2) の対応を用いて、モンスターの詳論を用いて得たものである。今回の証明は (例 2) の対応 (モンスターの性質) を用いずに VOA の理論と Conway 群の性質から得られた。

さて、この定理の証明の概略を述べよう。まず、次の補題を思い出す。

補題 2.4. [LSY07] V を $V_0 = \mathbb{C}1$ と $V_1 = 0$ を満たす VOA とする。 e, f を V のイジング元とし、 e が σ -型と仮定する。 このとき、 $e \in V^{\tau}$ 、すなわち e は τ_f で固定される。

定理 2.3 は次の方針で証明する。 $e \in V$ をイジング元としたとき、 e は V^{τ_e} では σ -型である。 よって、 V^{τ_e} に含まれるイジング元に付随する τ -型の自己同型が生成する群を A とした時に、 e は A で固定される。 よって、もし V^{τ_e} の A による固定部分 VOA が “既にイジング元が分類されている VOA” と同型になるなら、 e はどのような元かわかる。 実際に V_{Λ}^+ の場合には命題 2.2 に帰着出来るわけである。 もう少し詳しく述べよう。

一般の偶格子 L で議論できる箇所はそのまま述べる。 e を V_L^+ のイジング元とする。 このとき e を V_L のイジング元と見ること、 $\tau_e \in H = C_{\text{Aut}(V_L)}(\theta)/\langle \theta \rangle$ となることがわかる (cf. [Sh04]). また、 [FLM88] より

$$1 \rightarrow \text{Hom}(L, \mathbb{Z}_2) \rightarrow H \rightarrow \text{Aut}(L)/\langle -1 \rangle \rightarrow 1$$

は完全列である。 よって二つの場合にわけて考える。

$\tau_e \in \text{Hom}(L, \mathbb{Z}_2)$ の場合は、ある L の部分格子 L' があって $V_L^{+\tau_e} = V_{L'}^+$ となる。 そこで、 L' の長さ 4 の元に付随する $V_{L'}^+$ のイジング元から作られる τ -型の自己同型による固定点を計算すると命題 2.2 に帰着出来る。

$\tau_e \notin \text{Hom}(L, \mathbb{Z}_2)$ の場合は τ_e は $\text{Aut}(L)/\langle \pm 1 \rangle$ の位数 2 の元である。 $L = \Lambda$ の場合には Conway_1 の対合とその元の (Conway_0 への持ち上げの) Λ への作用が良く知られているので、 $V_{\Lambda}^{+\tau_e}$ が具体的にわかり、命題 2.2 に帰着出来る。⁷ もう少し詳しく述べる。 τ_e の共役類は ATLAS の記号で $2A$ または $2C$ である。 なぜなら共役類 $2B$ の元は Conway_0 への持ち上げの位数が 4 となるので τ_e の位数が V_L 上で 2 に反する。 よって、 Λ の τ_e の ± 1 固有ベクトルで生成される部分格子は $2A, 2C$ の場合にそれぞれ $\sqrt{2}E_8 \oplus \text{BW}_{16}, \sqrt{2}D_{24}^+$ である。 これらに対応する V_L^+ のイジング元の τ -型の自己同型による固定部分 VOA をそれぞれの場合において計算することで、それぞれ e は $V_{\sqrt{2}E_8 \oplus 2\text{BW}_{16}}^+, V_{\sqrt{2}D_{24}^+}^+$ に含まれることがわかる。 これらの VOA のイジング元は命題 2.2 からわかるので、定理 2.3 は証明できる。

特に次のことがわかる。

系 2.5. V_{Λ}^+ のイジング元は全て τ -型である。

また、 V_{Λ}^+ の自己同型群のイジング元への作用の軌道は次の通りである。

系 2.6. V_{Λ}^+ のイジング元全体の集合は自己同型群の作用によって二つの軌道に分かれ、それぞれの代表元は $\omega(\alpha)^{\pm}$ と $e_{E, \varphi}$ である。

⁷他の格子でも位数 2 の自己同型の格子への作用が良くわかっていれば、同様に V_L^+ のイジング元の分類を行うことが出来るかもしれない。

最後に、ムーンシャイン加群への応用を考えよう。 $V^h = V_\Lambda^+ \oplus V_\Lambda^{T,+}$ となるので、 V^h は V_Λ^+ を部分 VOA として含んでいる。また、 V_Λ^+ 上 1 、 $V_\Lambda^{T,+}$ 上 -1 として作用する線形写像 z は V^h の自己同型になる。そして、次が成立することは知られている (cf. [Mi04])。実際に V^h が $\alpha \in \Lambda(4)$ に対して $\omega^\pm(\alpha)$ を含むヴィラソロ枠を持ち、正則かつ $V_1^h = 0$ であることから示せる。

命題 2.7. $\alpha \in \Lambda(4)$ に対して $\tau_{\omega^+(\alpha)}\tau_{\omega^-(\alpha)} = z$ である。

すると次のことが示せる。⁸

命題 2.8. V^h のイジング元は全て τ -型である。

証明. $e \in V^h$ を σ -型のイジング元とする。すると、補題 2.4 と命題 2.7 から

$$e \in V^{h, (\tau_{\omega^+(\alpha)}, \tau_{\omega^-(\alpha)})} \subset V_\Lambda^+$$

である。しかし、これは系 2.5 に矛盾する。 □

この命題で得た結果は次への応用が期待される。

予想 2.9. $V = \bigoplus_{n=0}^{\infty} V_n$ を正定値不変内積を持つ正則な VOA とする。 $V_0 = \mathbf{C}1$ 、 $V_1 = 0$ であり、 V のイジング元は全て τ -型であると仮定する。このとき、イジング元から自己同型群への写像 $e \mapsto \tau_e$ は単射である。

参考文献

- [Bo86] R.E. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster, *Proc. Nat'l. Acad. Sci. U.S.A.*, **83** (1986), 3068–3071.
- [Co85] J.H. Conway, A simple construction for the Fischer-Griess monster group, *Invent. Math.* **79** (1985), 513–540.
- [DLMN98] C. Dong, H. Li, G. Mason and S.P. Norton, Associative subalgebras of Griess algebra and related topics, Proc. of the Conference on the Monster and Lie algebra at the Ohio State University, May 1996, ed. by J. Ferrar and K. Harada, Walter de Gruyter, Berlin - New York, 1998.
- [DMZ94] C. Dong, G. Mason and Y. Zhu, Discrete series of the Virasoro algebra and the moonshine module, *Pro. Symp. Pure. Math., American Math. Soc.* **56** II (1994), 295–316.

⁸ V^h のイジング元とモンスターの $2A$ 元との $1:1$ 対応 (モンスターの詳論) を用いるとわかることだが (cf. [Mi96a]), それを用いずにも証明できたわけである。

- [FLM88] I. Frenkel, J. Lepowsky and A. Meurman, Vertex operator algebras and the Monster, Pure and Appl. Math., Vol.134, Academic Press, Boston, 1988.
- [La99] C.H. Lam, Code vertex operator algebras under coordinates change, *Comm. Algebra* **27** (1999), 4587-4605.
- [LSY07] C.H. Lam, S. Sakuma and H. Yamauchi, Ising vectors and automorphism groups of commutant subalgebras related to root systems, *Math. Z.* **255** (2007), 597-626.
- [LS] C.H. Lam and H. Shimakura, Ising vectors in the vertex operator algebra V_{Λ}^+ associated with the Leech lattice Λ , preprint.
- [Mi96a] M. Miyamoto, Griess algebras and conformal vectors in vertex operator algebras, *J. Algebra* **179** (1996), 523-548.
- [Mi96b] M. Miyamoto, Binary codes and vertex operator (super)algebras, *J. Algebra* **181** (1996), 207-222.
- [Mi04] M. Miyamoto, A new construction of the Moonshine vertex operator algebra over the real number field, *Ann. of Math.* **159** (2004), 535-596.
- [Sh04] H. Shimakura, The automorphism group of the vertex operator algebra V_L^+ for an even lattice L without roots, *J. Algebra* **280** (2004), 29-57.

回転不変な積分のクラスに関する求積公式について

名古屋大学大学院情報科学研究科 澤 正憲
名古屋大学大学院情報科学研究科 平尾 奨剛

1 求積公式

$\Omega \subset \mathbb{R}^d$ と重み関数 W に対して,

$$I[f] = \int_{\Omega} f(x)W(x)dx, \quad f \in L^2(\Omega, W), \quad (1)$$

という積分を考える. 積分領域 Ω と重み関数 W を明記する必要のない場合, 単に $\int f$ のように表記する. 例えば, $(\Omega, W) = (\mathbb{R}^d, e^{-\|\mathbf{x}\|^2})$ や $(B^d, 1)$ 等は様々な分野でよく扱われる組である. このような組に対して, 与えられた関数の積分値を直接求めることは大抵の場合困難であるため, \mathbb{R}^d の有限個の点における関数値を用いて積分値を近似したい. しかも, 得られた値はできるだけ真の積分値に近づけるという都合の良いことを考えよう.

$X = \{\mathbf{x}_1, \dots, \mathbf{x}_N\} \subset \mathbb{R}^d$ とし, X 上で定義される正值重み関数を λ とする. X の元と λ を用いて, 関数 f の積分値を次のように近似する:

$$I[f] \approx \frac{I[1]}{\sum_{i=1}^N \lambda(\mathbf{x}_i)} \sum_{i=1}^N \lambda(\mathbf{x}_i) f(\mathbf{x}_i). \quad (2)$$

係数 $\frac{I[1]}{\sum_{i=1}^N \lambda(\mathbf{x}_i)}$ は, 例えば $f \equiv 1$ に対して近似式に誤差が生じないようにするために必要となる. (2) のような式はデザインあるいは求積公式 (積分近似公式) とよばれている. 点集合 X のことをデザインあるいは求積公式とよぶこともある.

n 次以下の全ての多項式に対して, 誤差が 0 の正確な等式となる時, 求積公式 (2) の次数は k であるという. 多項式にこだわるのには特別な理由がある. すなわち, Ω をコンパクトな積分領域とすると, Weierstrass の定理によって, 任意の連続関数 P と任意の正数 ϵ に対して,

$$|P(\mathbf{x}) - f_P(\mathbf{x})| < \epsilon$$

が Ω 上の任意の点 \mathbf{x} において成り立つような多項式 f_P が存在する. この定理によって, Ω 上の連続関数は好きな精度で多項式近似できる. 多項式でない連続関数 f に対して, 近似精度を高くすればするほど, すなわち ϵ を小さく

すればするほど、近似多項式 f_P の次数は大きくならなければならない。従って、求積公式の次数は高いほどよい。また、実計算上の都合により $|X|$ の値はできるだけ小さくするのが望ましい。特に、 $|X|$ に関するある下界が達成される時、求積公式は直交多項式と密接な関係にある。これについては3節で詳しく述べる。まずは次節で直交多項式に関する事実を述べよう。

2 直交多項式と再生核

Ω, W, \mathcal{I} は前節と同じ表記を用いる。 Ω 上 n 次以下の d 変数多項式が張る線型空間を $\mathcal{P}_n^d(\Omega)$ とおく。 n 次多項式 f が、任意の $n-1$ 次以下の多項式 g に対して、

$$\mathcal{I}[fg] = 0$$

を満たす時、 f を W に関する n 次直交多項式という。特に、 $\mathcal{I}[f^2] = 1$ を満たす f を正規直交多項式という。 $r_n^d = \dim\{f \in \mathcal{P}_n^d(\Omega) \mid \deg f = n\}$ とおくと、 Ω 上互いに独立な n 次直交多項式は r_n^d 個存在する。線型独立な n 次正規直交多項式 $P_{n,i}$ ($i = 1, \dots, r_n^d$) を成分とする列ベクトルを $\mathbb{P}_n = (P_{n,1}, \dots, P_{n,r_n^d})^T$ と表そう。この時、 $n+1$ 次多項式列 $x_i \mathbb{P}_n$ ($i = 1, \dots, d$) が $\mathbb{P}_1, \dots, \mathbb{P}_{n+1}$ の一次結合として表されることは明らかである。直交性によって、実は $n-2$ 次以下の多項式列は上で述べた一次結合に必要なことがよく知られている。

定理 2.1. (三項関係式). 非負整数 n に対して、行列 $A_{n,i} \in M_{r_n^d \times r_{n+1}^d}(\mathbb{R})$, $B_{n,i} \in M_{r_n^d}(\mathbb{R})$, $C_{n,i} \in M_{r_n^d \times r_{n-1}^d}(\mathbb{R})$ で次を満たすものが存在する:

$$x_i \mathbb{P}_n = A_{n,i} \mathbb{P}_{n+1} + B_{n,i} \mathbb{P}_n + C_{n,i} \mathbb{P}_{n-1}, \quad i = 1, \dots, d. \quad (3)$$

ただし、

$$A_{n,i} = \int x_i \mathbb{P}_n \mathbb{P}_{n+1}^T, \quad B_{n,i} = \int x_i \mathbb{P}_n \mathbb{P}_n^T, \quad C_{n,i} = \int x_i \mathbb{P}_n \mathbb{P}_{n-1}^T.$$

正規直交多項式列 \mathbb{P}_k ($k = 0, \dots, n$) に対して、関数

$$K_n(\mathbf{x}, \mathbf{y}) = \sum_{k=0}^n \mathbb{P}_k^T(\mathbf{x}) \mathbb{P}_k(\mathbf{y}) \quad (4)$$

を考える。 $\mathcal{P}_n^d(\Omega)$ の任意の元 f に対して、

$$f(\mathbf{x}) = \sum_{k=0}^n \mathcal{I}[f(\mathbf{y}) \mathbb{P}_k(\mathbf{y})]^T \mathbb{P}_k(\mathbf{x}) = \mathcal{I}[K_n(\mathbf{x}, \mathbf{y}) f(\mathbf{y})] \quad (5)$$

が成り立つ。この性質により、 $K_n(\cdot, \cdot)$ は n 次再生核と呼ばれる。明らかに、 $K_n(\cdot, \cdot)$ は \mathbb{P}_k の選び方に依らず定まる。再生核は、数ある積分核の中でも様々な性質をもち、フーリエ解析をはじめ多くの分野における主要な研究対象の一つである。

定理 2.2. (Christoffel-Darboux 公式). $\{\mathbb{P}_k \mid k = 0, \dots\}$ を直交多項式列からなる集合とする。この時、任意の非負整数 n 及び相異なる $x = (x_1, \dots, x_d), y = (y_1, \dots, y_d) \in \mathbb{R}^d$ に対して、次の関係式が成り立つ:

$$\sum_{k=0}^n \mathbb{P}_k^T(x) \mathbb{P}_k(y) = \frac{[A_{n,i} \mathbb{P}_{n+1}(x)]^T \mathbb{P}_n(y) - \mathbb{P}_n^T(x) [A_{n,i} \mathbb{P}_{n+1}(y)]}{x_i - y_i}, \quad 1 \leq i \leq d, \quad (6)$$

$$\sum_{k=0}^n \mathbb{P}_k^T(x) \mathbb{P}_k(x) = \mathbb{P}_n^T(x) [A_{n+1,i} \partial_i \mathbb{P}_{n+1}(x)] - [A_{n+1,i} \mathbb{P}_{n+1}(x)]^T \partial_i \mathbb{P}_n(x), \quad 1 \leq i \leq d. \quad (7)$$

Christoffel-Darboux 公式は、再生核における n 次以下の各直交多項式の積の和の計算を、ある n 次直交多項式と $n+1$ 次直交多項式の積の和の計算に帰着させるという意義をもつが、その計算は依然として困難である。幾つかの具体的な (Ω, W) に対して、より明快な再生核の表現公式が知られている。例えば、 $(\Omega, W) = (S^{d-1}, 1)$ において、

$$K_n(x, y) = \sum_{k=0}^n Q_k(\langle x, y \rangle)$$

は、加法公式としてよく知られている [1, 12]。ここで、 $Q_k(\cdot)$ は k 次 Gegenbauer 多項式である。この他にも、 Ω が B^d に等しい場合 [14] あるいは d 次元単体の場合 [15] に、各々特定の重み関数に対して実計算に向けた扱いやすい再生核の表現公式が知られている。いずれの表現公式も、 $(S^{d-1}, 1)$ に対する加法公式と密接な関係にある [16]。

積分領域 Ω 及び重み関数 W がともに $O(d)$ -不変である、すなわち、 $O(d)$ の任意の元 σ に対して、

$$\Omega^\sigma = \Omega, \quad W(x^\sigma) = W(x)$$

が成り立つ時、 (Ω, W) に関する直交多項式を $O(d)$ -不変であるという。定義より、 $K_n(\cdot, \cdot)$ は $O(d)$ の作用に関して不変であるから、 $O(d)$ -不変直交多項式に対する再生核もまた $O(d)$ -不変であるということにしよう。 $O(d)$ -不変な再生核は、一般の積分と比較して容易に計算可能である。それについては 4 節で明らかにする。次節では、再生核の求積公式への応用について議論する。

3 再生核と求積公式

次数 n のデザインを X とおく. $|X| < \dim \mathcal{P}_{\lfloor \frac{n}{2} \rfloor}^d(\Omega)$ と仮定すると, X の全ての点で零となるような $\mathcal{P}_{\lfloor \frac{n}{2} \rfloor}^d(\Omega)$ の非零元が少なくとも 1 つ存在する. これは積分 I の正定値性に反するから, $|X|$ に関して次の不等式が成り立つ:

$$|X| \geq \dim \mathcal{P}_{\lfloor \frac{n}{2} \rfloor}^d(\Omega). \quad (8)$$

(8) において等号を達成する求積公式はガウス求積公式あるいはタイトデザインとよばれる.

次数 $2n-1$ のガウス求積公式と n 次直交多項式全体の共通根の間には密接な関係がある.

定理 3.1. [7]. $X = \{\mathbf{x}_1, \dots, \mathbf{x}_{\dim \mathcal{P}_{n-1}^d(\Omega)}\} \subset \mathbb{R}^d$ と積分 I に関する n 次直交多項式全体からなる集合 \mathbb{P}_n に対して, X が次数 $2n-1$ のガウス求積公式をなすための必要十分条件は, \mathbb{P}_n が $\dim \mathcal{P}_{n-1}^d(\Omega)$ 個の共通根をもつことである.

n 次直交多項式全体は高々 $\dim \mathcal{P}_{n-1}^d(\Omega)$ 個の共通根をもつ. しかし, ちょうど $\dim \mathcal{P}_{n-1}^d(\Omega)$ 個の共通根をもつような積分 I の存在はほとんど知られておらず, ガウス求積公式の存在もほとんど知られていない [4]. なお, 各点 \mathbf{x}_k の重みは再生核 $K_n(\cdot, \cdot)$ を用いて,

$$\lambda(\mathbf{x}_k) = \frac{1}{K_n(\mathbf{x}_k, \mathbf{x}_k)}$$

と表されることがよく知られている. 従って, $K_n(\cdot, \cdot)$ の対称性により $\lambda(\mathbf{x}_k)$ は常に正値をとる.

X が $O(d)$ -不変な次数 $2n-1$ のデザインであるとしよう. n と同じ偶奇をもつ多項式全体が張る $\mathcal{P}_n^d(\Omega)$ の部分空間を $\mathcal{P}_n^{d*}(\Omega)$ とおく. この時, $|X|$ に関する次の不等式がよく知られている:

$$|X| \geq \begin{cases} 2 \dim \mathcal{P}_{n-1}^{d*}(\Omega) - 1 & \text{if } 0 \in X \text{ and } n \text{ is an even integer,} \\ 2 \dim \mathcal{P}_{n-1}^{d*}(\Omega) & \text{otherwise.} \end{cases} \quad (9)$$

(9) を達成するとき, 求積公式あるいはデザインをタイトであるという. この不等式は Möller ([5]) あるいは Mysovskikh ([6]) によって独立に示されたが, 一般に Möller lower bound とよばれている. この所以は, Möller が (9) を導くとともに等号成立の場合をより詳しく調べ, 当分野において重要な結果を示したことによる. 条件

$$\mathbf{x} \in X \Rightarrow -\mathbf{x} \in X$$

を満たす点集合 $X \subset \mathbb{R}^d$ は極対的であるという.

定理 3.2. [5]. デザイン X が (9) において等号を達成するとしよう. この時, $0 \in X$ かつ n が偶数である, あるいは n が奇数であるならば, X は極対的である.

以下, $0 \in X$ かつ n が偶数である場合に, (9) において等号を達成するデザイン X を考えよう. 定理 3.2 より, そうしたデザインは,

$$I[f] = 2\lambda(0)f(0) + \sum_{k=1}^{\dim \mathcal{P}_n^{d^*}(\Omega)-1} \lambda(\mathbf{x}_k)\{f(\mathbf{x}_k) + f(-\mathbf{x}_k)\} \quad (10)$$

のように表すことができる.

\mathcal{P}_n^* 上に制限された再生核 $\bar{K}_n(\cdot, \cdot)$ を考える. すなわち, $\bar{K}_n(\cdot, \cdot)$ は

$$f(\mathbf{y}) = \int_{\Omega} f(\mathbf{x})\bar{K}_n(\mathbf{x}, \mathbf{y})W(\mathbf{x})d\mathbf{x}, \quad f \in \mathcal{P}_n^{d^*}(\Omega) \quad (11)$$

という性質をもつ. $\bar{K}_n(\cdot, \cdot)$ は変形 n 次再生核とよばれる. 上述のデザイン X と変形 n 次再生核は密接な関係にある.

定理 3.3. [7]. 求積公式 (10) が存在するための必要十分条件は,

- (i) $\bar{K}_n(\mathbf{x}_i, \mathbf{x}_j) = 0, \quad i \neq j, i, j = 0, \dots, \dim \mathcal{P}_n^{d^*}(\Omega) - 1;$
- (ii) $\lambda(\mathbf{x}_i) = \frac{1}{2\bar{K}_n(\mathbf{x}_i, \mathbf{x}_i)}, \quad i = 0, \dots, \dim \mathcal{P}_n^{d^*}(\Omega) - 1.$

次数 $2n$ のガウス求積公式と直交多項式の間に関連性については本稿では触れない. 次節では, $O(d)$ -不変な次数 5 の求積公式に関する最近の結果を紹介する.

4 次数 5 の求積公式

$O(d)$ -不変な n 次直交多項式は, n の偶奇に依って偶多項式あるいは奇多項式をなす. Weyl-Brauer による $O(d)$ -不変多項式の基本定理を用いれば, $\bar{K}_n(\cdot, \cdot)$ は $\|\mathbf{x}\|, \|\mathbf{y}\|, \langle \mathbf{x}, \mathbf{y} \rangle$ によって一意的に表現されることがわかる. $\bar{K}_n(\cdot, \cdot)$ は対称式であるから, $\bar{K}_n(\mathbf{x}, \mathbf{y})$ は,

$$\bar{K}_n(\mathbf{x}, \mathbf{y}) = a\langle \mathbf{x}, \mathbf{y} \rangle^2 + b\|\mathbf{x}\|^2\|\mathbf{y}\|^2 + c(\|\mathbf{x}\|^2 + \|\mathbf{y}\|^2) + d, \quad a, b, c, d \in \mathbb{R}, \quad (12)$$

のように表される.

さて、領域 $\Omega \subset \mathbb{R}^d$ が $\dot{\Omega} \neq \emptyset$ を満たすという仮定のもとで、5次の求積公式について考えよう。この場合、

$$\dim \mathcal{P}_2^{d*}(\Omega) = \binom{d+1}{2} \quad (13)$$

であることが容易にわかる。

補題 4.1. 領域 $\Omega \subset \mathbb{R}^d$ が $\dot{\Omega} \neq \emptyset$ とする。任意の $\mathbf{x}, \mathbf{y} \in \mathbb{R}^d$ に対して、 $O(d)$ -不変直交多項式に関する変形再生核 $\bar{K}_n(\cdot, \cdot)$ は、

$$\bar{K}_n(\mathbf{x}, \mathbf{y}) = a\langle \mathbf{x}, \mathbf{y} \rangle^2 + b\|\mathbf{x}\|^2\|\mathbf{y}\|^2 + c(\|\mathbf{x}\|^2 + \|\mathbf{y}\|^2) + d, \quad (14)$$

のように表される。ただし、

$$\begin{aligned} a &= \frac{d(d+2)}{2|S^{d-1}| \int_p^q r^{d+3} W(r) dr}, \\ b &= \frac{1}{|S^{d-1}| \int_p^q r^{d+3} W(r) dr} \times \left\{ -\frac{n+2}{2} \frac{\int_p^q r^{d+1} W(r) dr}{\int_p^q r^{d+3} W(r) dr} \right. \\ &\quad \left. - \frac{\int_p^q r^{d-1} W(r) dr \int_p^q r^{d+1} W(r) dr}{(\int_p^q r^{d+1} W(r) dr)^2 - \int_p^q r^{d+3} W(r) dr \int_p^q r^{d-1} W(r) dr} \right\}, \\ c &= \frac{1}{|S^{d-1}|} \frac{\int_p^q r^{d-1} W(r) dr \int_p^q r^{d+1} W(r) dr}{(\int_p^q r^{d+1} W(r) dr)^2 - \int_p^q r^{d+3} W(r) dr \int_p^q r^{d-1} W(r) dr}, \\ d &= -\frac{1}{|S^{d-1}|} \frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d+1} W(r) dr} c, \end{aligned}$$

であり、 p, q は $\Omega = \{\mathbf{x} \in \mathbb{R}^d \mid p \leq \|\mathbf{x}\| \leq q\}$ によって定められる正の実数であるとする。

証明. (5) を用いる。□

補題 4.2. [8]. 領域 $\Omega \subset \mathbb{R}^d$ が $\dot{\Omega} \neq \emptyset$ とする。求積公式 (10) が存在するならば、次の形で与えられる:

$$\lambda_0 f(\mathbf{0}) + \lambda_1 \sum_{k=1}^{d(d+1)/2} \{f(\mathbf{x}_k) + f(-\mathbf{x}_k)\}. \quad (15)$$

ただし, λ_0, λ_1 は次で定められる:

$$\lambda_0 = 1 - \frac{(\int_p^q r^{d+1} W(r) dr)^2}{\int_p^q r^{d-1} W(r) dr \int_p^q r^{d+3} W(r) dr}, \quad (16)$$

$$\lambda_1 = \frac{1}{d(d+1)} \frac{(\int_p^q r^{d+1} W(r) dr)^2}{\int_p^q r^{d-1} W(r) dr \int_p^q r^{d+3} W(r) dr}, \quad (17)$$

$$\|\mathbf{x}_k\| = \sqrt{\frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d+1} W(r) dr}}, \quad \mathbf{x}_k \neq \mathbf{0}. \quad (18)$$

証明. 定理 3.3 (ii) より, (16) 及び (17) が成り立つ. 定理 3.3 (i) より, 任意の $k = 1, \dots, d(d+1)$ に対して,

$$\bar{K}_2(\mathbf{0}, \mathbf{x}_k) = 0$$

となる. 従って, 補題 4.1 より, (18) が成り立つ. \square

定理 4.3. 領域 $\Omega \subset \mathbb{R}^d$ が $\Omega \neq \emptyset$ とする. $X = \{\mathbf{x}_1, \dots, \mathbf{x}_{d(d+1)}\} \subset S^{d-1}$ がタイト球 5 デザインであるための必要十分条件は, $\{\mathbf{0}\} \cup \{\sqrt{\frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d+1} W(r) dr}} \mathbf{x}_k \mid k = 1, \dots, d(d+1)\}$ が求積公式 (15) をなすことである.

証明. $X = \{\mathbf{x}_1, \dots, \mathbf{x}_{d(d+1)}\} \subset S^{d-1}$ をタイト球 5 デザインとする. この時, 補題 4.2 より \mathcal{I} に対する非零モーメントは次のように表される.

$$\begin{aligned} \mathcal{I}[x_k^2] &= \frac{1}{d} \cdot \frac{\int_p^q r^{d+1} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\ &= \mathcal{I}_S[x_k^2] \frac{\int_p^q r^{d+1} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\ &= \left(\frac{1}{d(d+1)} \sum_{l=1}^{d(d+1)} q_{k,l}^2 \right) \frac{\int_p^q r^{d+1} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\ &= \lambda_1 \sum_{l=1}^{d(d+1)} \left(\sqrt{\frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d+1} W(r) dr}} q_{k,l} \right)^2. \end{aligned}$$

$$\begin{aligned}
\mathcal{I}[x_k^4] &= \frac{3}{d(d+2)} \cdot \frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\
&= \mathcal{I}_S[x_k^4] \frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\
&= \left(\frac{1}{d(d+1)} \sum_{l=1}^{d(d+1)} q_{k,l}^4 \right) \frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\
&= \lambda_1 \sum_{l=1}^{d(d+1)} \left(\sqrt{\frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d+1} W(r) dr}} q_{k,l} \right)^4.
\end{aligned}$$

$$\begin{aligned}
\mathcal{I}[x_k^2 x_l^2] &= \frac{1}{d(d+2)} \cdot \frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\
&= \mathcal{I}[x_k^2 x_l^2] \frac{\int_p^q r^{d+1} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\
&= \left(\frac{1}{d(d+1)} \sum_{m=1}^{d(d+1)} q_{m,k}^2 q_{m,l}^2 \right) \frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d-1} W(r) dr} \\
&= \lambda_1 \sum_{m=1}^{d(d+1)} \left(\sqrt{\frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d+1} W(r) dr}} q_{m,k} \cdot \sqrt{\frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d+1} W(r) dr}} q_{m,l} \right)^2.
\end{aligned}$$

一般に,

$$\mathcal{I}[1] = \lambda_0 + \lambda_1 \sum_{l=1}^{d(d+1)} 1 = \frac{1}{d(d+1)} \sum_{l=1}^{d(d+1)} 1$$

が成り立つ。従って, $\{\mathbf{0}\} \cup \left\{ \sqrt{\frac{\int_p^q r^{d+3} W(r) dr}{\int_p^q r^{d+1} W(r) dr}} \mathbf{x}_k \mid k = 1, \dots, d(d+1) \right\}$ は求積公式 (15) をなす。命題の逆方向も同様に示される。□

$(\Omega, W) = (B^d, 1)$ のとき, 定理 4.3 は Noskov-Schmid の定理 [8] に一致する。 $\Omega \neq \emptyset$ とすると, Schwarz の不等式より,

$$\left(\int_p^q r^{d+1} W(r) dr \right)^2 - \int_p^q r^{d+3} W(r) dr \int_p^q r^{d-1} W(r) dr < 0 \quad (19)$$

が成り立つ。従って、 $O(d)$ -不変デザインの各点は領域 Ω 内に含まれる。そのような求積公式は内部公式とよばれており、応用上重要な意義をもつ。

S^{d-1} 上の 5 デザイン X について、次の結果がよく知られている [2]:

$$|X| \geq \begin{cases} d(d+1)+1 & \text{if } d=1, 2, 3, \\ d(d+1)+2 & \text{if } d=4, 5, 6, \end{cases} \quad \begin{matrix} d=(2\ell+1)^2-2, \\ 6 < d \neq (2\ell+1)^2-2. \end{matrix} \quad (20)$$

ここで、 ℓ は任意の自然数とする。 $S^{(2\ell+1)^2-2}$ 上のタイト 5 デザインの存在問題は未解決である。坂内-宗政-Venkov [3] により幾つかの $d=(2\ell+1)^2-2$ に対してタイト 5 デザインの非存在が示されているが、未解決な部分が多く。 $O((2\ell+1)^2-2)$ -不変なタイト 5 デザインの存在問題も未解決である。一方、上の不等式は $1 \leq d \leq 7$ および $d=23$ のとき達成されることがよく知られている。7次元のタイト 5 デザインの存在は Reznick [9] によって示されている。

定理 4.4. $\Omega \neq \emptyset$ を満たす $O(d)$ -不変な領域を $\Omega \subset \mathbb{R}^d$ とし、 $O(d)$ -不変な重み関数を W とおく。 $d \in \{1, 2, 3, 4, 5, 6, 7, 23\}$ ならば、 (Ω, W) に関する \mathbb{R}^d 上タイト 5 デザインが存在する。

本稿では 5 デザインの結果のみ紹介させていただいた。一般に、次数 $4k+1$ の $O(d)$ -不変タイトデザインの存在性に関する結果として、 $d=2$ の場合に $(\Omega, W) = (\mathbb{R}^2, e^{-\alpha\|\mathbf{x}\|^2})$ 等の特別な組に対するタイトデザインの非存在が示されている [13]。 $d \geq 3$ かつ $k \geq 2$ の場合に、そうしたデザインの存在性についてはほとんど知られていない。

References

- [1] E. Bannai and E. Bannai, Algebraic Combinatorics on Spheres, Springer Tokyo, 1999 (in Japanese).
- [2] E. Bannai, R. M. Damerell, Tight spherical designs, II. *J. London Math. Soc. (2)* **21** (1980), no. 1, 13–30.
- [3] E. Bannai, A. Munemasa, B. Venkov, The nonexistence of certain tight spherical designs. With an appendix by Y.-F. S. Petermann. *Algebra i Analiz* **16** (2004), no. 4, 1–23; translation in *St. Petersburg Math. J.* **16** (2005), no. 4, 609–625.
- [4] H. Berens, H. J. Schmid, Y. Xu, Multivariate Gaussian cubature formulae. *Arch. Math.* **64** (1995), 26–32.

- [5] H. M. Möller, Lower bounds for the number of nodes in cubature formulas, in: G. Hämmerlin (Ed.), *Numerische Integration*, ISNM, Vol. 45, Birkhäuser, Basel, 1979, pp. 221–230.
- [6] I. P. Mysovskikh, Construction of cubature formulae, *Vopr. Vycisl. i Prikl. Mat. Tashkent* **32** (1975), 85–98 (in Russian).
- [7] I. P. Mysovskikh, Interpolatory cubature formulas, Nauka, Moscow, 1981 (in Russian), Interpolatorische Kubaturformeln, Institut für Geometrie und Praktische Mathematik der RWTH Aachen, Aachen 1992, Bericht No.74 (in German).
- [8] M. V. Noskov, H. J. Schmid, On the number of nodes in n -dimensional cubature formulae of degree 5 for integrals over the ball. *J. Comp. Appl. Math.* **169** (2004), 247–254.
- [9] B. Reznick, Some constructions of spherical 5-designs, *Linear Algebra Appl.* **226/228** (1995), 163–196.
- [10] A. H. Stroud, Some fifth degree integration formulas for symmetric regions, II, *Numer. Math.* **9** (1967), 460–468.
- [11] A. H. Stroud, *Approximate Calculation of Multiple Integrals*, Prentice-Hall, Englewood Cliffs, NJ, 1971.
- [12] G. Szegő, *Orthogonal polynomials*, 4th ed., Amer. Math. Soc. Colloq. Publ. vol.23, Providence, RI, 1975.
- [13] P. Verlinden, R. Cools, On cubature formulae of degree $4k + 1$ attaining Moller's lower bound for integrals with circular symmetry. *Numer. Math.* **61** (1992), no. 3, 395–407.
- [14] Xu, Y, Summability of Fourier orthogonal series for Jacobi weight on a ball in \mathbb{R}^d . *Trans. Amer. Math. Soc.* **351** (1999), 2439–2458.
- [15] Xu, Y, Summability of Fourier orthogonal series for Jacobi weights on the simplex in \mathbb{R}^d . *Proc. Amer. Math. Soc.* **126** (1998), 3027–3036.
- [16] Xu, Y, Orthogonal polynomials and cubature formulae on spheres and on balls. *SIAM J. Math. Anal.* **29** (1998), 779–793.

Nilpotent, solvable, and monomial schemes

花木 章秀 (信州大学理学部)

1 はじめに

アソシエーションスキームは有限群をある意味で一般化したものであり、したがって有限群について成り立つ性質がアソシエーションスキームに対してどの程度、どのように一般化されるかを考えることは自然なことである。昨年、竹ヶ原-吉田 [5] によるべき零群の研究のあと、竹ヶ原 [4] によってべき零スキームが定義された。その後、講演者によって竹ヶ原による定義をいくらか一般化した定義が与えられた [1]。次に可解スキームを考えることは自然な流れである。しかし (べき零群についてもそうであるが) 可解群を特徴付ける性質はたくさんあり、それぞれに対してアソシエーションスキームへの一般化が考えられる。しかしそれらは必ずしも同値な条件とはならず、どれを採用するのが適当であるかを判断することはできない。今回はあえて可解スキームを定義せず、それに関連する性質などを考える。

有限群論において、べき零と可解の間にあるものとして M -群というものがある。すなわちべき零群は M -群であり (Blichfeldt の定理)、 M -群は可解群である (竹田の定理)。今回はこれに注目して、アソシエーションスキームへの拡張の可能性を考えた。結果として、竹田の定理はある程度納得できる形で拡張されるが、Blichfeldt の定理はうまくいかないことが分かった。竹田の定理の拡張を考えるためには closed subset からの指標の誘導を考える必要があるが、これは重複度をうまく扱うことによって処理できることが分かった。

2 準備

ここでは必要な定義とよく知られた結果について簡単に解説する。 (X, S) がアソシエーションスキーム、あるいは簡単にスキーム、であるとは次の条件が成り立つこととする。

- X は有限集合、

- S は $X \times X$ の分割、

$$X \times X = \bigcup_{s \in S} s \quad (\text{disjoint})$$

- $1 := \{(x, x) \mid x \in X\} \in S$,
- $s \in S$ ならば $s^* := \{(y, x) \mid (x, y) \in s\}$,
- $s, t, u \in S$ 対して $p_{st}^u \geq 0$ が存在して、 $(x, y) \in u$ であるならば

$$p_{st}^u = \#\{z \in X \mid (x, z) \in s, (z, y) \in t\}$$

となる。

$s \in S$ について p_{ss}^1 を s の **valency** といい n_s と書く。 $n_s = 1$ である $s \in S$ は **thin** であるといわれる。 $T \subset S$ が **thin** であるとは、任意の $t \in T$ が thin であることとする。 S 自身が thin であるとき、スキーム (X, S) は本質的に有限群と同じものであり、逆に任意の有限群は thin スキームを定める。アソシエーションスキームが有限群の一般化であるというのはこのことによる。 $T \subset S$ について $n_T = \sum_{t \in T} n_t$ とおく。

$s, t \in S$ に対して、その **complex product** を

$$st = \{u \in S \mid p_{st}^u > 0\}$$

で定める。 $A, B \subset S$ に対して、その **complex product** を

$$AB = \bigcup_{s \in A} \bigcup_{t \in B} st$$

で定める。 S の空でない部分集合 T が $TT = T$ をみたすとき、 T を S の **closed subset** という。 Closed subset T が **normal** であるとは、任意の $s \in S$ について $sT = Ts$ が成り立つこととする。 Closed subset T が **strongly normal** であるとは、任意の $s \in S$ について $sTs^* = T$ が成り立つこととする。 Strongly normal ならば normal であるが、一般に逆は成り立たない。 S の closed subset T は (一意ではないが) **subscheme** を定め、また **quotient scheme** $S//T$ を定める。 Quotient scheme $S//T$ が thin であることと T が S で strongly normal であることは同値である。

$s \in S$ に対して隣接行列を σ_s と書く。 すなわち σ_s は行、列、ともに集合 X で添え字付けられた $\{0, 1\}$ を成分にもつ行列で

$$(\sigma_s)_{xy} = \begin{cases} 1 & \text{if } (x, y) \in s, \\ 0 & \text{otherwise} \end{cases}$$

で定まるものである。\$R\$ を単位元をもつ可換環とする。\$\{\sigma_s \mid s \in S\}\$ を \$R\$ 上の行列の集合と見て、その \$R\$-一次結合の全体を考えれば、アソシエーションスキームの定義により、それは積で閉じていて、環になる。これを \$(X, S)\$ の \$R\$ 上の隣接代数といい \$RS\$ と書く。\$S\$ の closed subset \$T\$ に対して、\$T\$ で生成される \$R\$ の \$R\$-部分加群 \$RT\$ は \$RS\$ の部分代数をなす。ここでは特に係数環として複素数体 \$\mathbb{C}\$ を考える。

$$CS = \bigoplus_{s \in S} \mathbb{C}\sigma_s$$

\$CS\$ が可換環であるときスキーム \$(X, S)\$ は可換であるという。よく知られているように \$CS\$ は半単純代数であり、したがっていくつかの全行列環の直和に同型である。

$$CS \cong \bigoplus_{i=1}^r M_{n_i}(\mathbb{C})$$

ここで各直和因子への射影を \$\pi_i : CS \to M_{n_i}(\mathbb{C})\$ とする。すると \$\{\pi_i \mid i = 1, 2, \dots, r\}\$ は \$CS\$ の既約表現の同値類の完全代表系である。\$\chi_i\$ を \$\pi_i\$ の指標、すなわちトレース、とする。\$\text{Irr}(S) = \{\chi_i \mid i = 1, 2, \dots, r\}\$ とおく。特に \$1_S : \sigma_s \to n_s\$ とすると \$1_S \in \text{Irr}(S)\$ である。これを \$S\$ の自明な指標という。

写像 \$\Gamma_S : \sigma_s \to \sigma_s\$ は \$CS\$ の行列表現で、これを \$S\$ の標準表現という。対応する指標を \$\gamma_S\$ と書いて標準指標という。標準指標 \$\gamma_S\$ の既約分解

$$\gamma_S = \sum_{\chi \in \text{Irr}(S)} m_\chi \chi$$

における \$\chi \in \text{Irr}(S)\$ の重複度 \$m_\chi\$ を単に \$\chi\$ の重複度という。一般に \$\chi(1) \leq m_\chi\$ であることが知られている。

3 Commutators

スキームに対して可解群に相当するようなものを考えるために commutator を定義する。

\$t, u \in S\$ に対して

$$[t, u] = t \cdot u \cdot tu$$

とにおいて、これを \$t\$ と \$u\$ の commutator という。\$T, U \subset S\$ に対しては

$$[T, U] = \langle [t, u] \mid t \in T, u \in U \rangle$$

とする。ここで右辺は元の commutator をすべて含む最小の closed subset の意味である。 S の closed subset T に対して $D(T) = [T, T]$ とおく。すると $D(T)$ は $T//D(T)$ が可換かつ thin となる最小の closed subset である。 $D^0(S) = S$ とし、帰納的に $D^{i+1}(S) = D(D^i(S))$ を定める。これは群論における交換子群などの定義の拡張となっている。

ここで自然な疑問として、各 $D^i(S)$ は S の normal closed subset か、という問題が考えられるが、実はこれは成り立たない。 $D^i(S)$ に関する簡単な命題を一つ示しておく。

Proposition 3.1. (X, S) は closed subset の列

$$1 = S_0 \subset S_1 \subset \cdots \subset S_r = S$$

で、各 $S_{i+1}//S_i$ が可換かつ thin であるものをもつとする。このとき $D^r(S) = 1$ である。

4 Inductions and restrictions

指標、あるいは加群の誘導と制限について簡単に説明する。Frobenius 相互律が成り立つことが、基本的ではあるが重要である。

(X, S) をスキーム、 T をその closed subset とする。 K を体とし L を右 KT -加群とする。このとき KS を自然に左 KT -加群として

$$L \uparrow^S = L \otimes_{KT} KS$$

とすれば、これは右 KS -加群となる。これを L の S への誘導加群という。 M を右 KS -加群とすれば、作用を制限することによって M は右 KT -加群にもなる。これを M の T への制限加群といい $M \downarrow_T$ と書く。これらに対応する指標を誘導指標、制限指標といい、同様の記号を用いる。

Frobenius 相互律は指標の言葉を使うと次のように表される。 $\chi \in \text{Irr}(S)$ とし、 η を既約とは限らない S の指標とする。 η における χ の重複度を $m(\chi \text{ in } \eta)$ と表すことにする。このとき $\chi \in \text{Irr}(S)$ と $\varphi \in \text{Irr}(T)$ について

$$m(\chi \text{ in } \varphi \uparrow^S) = m(\varphi \text{ in } \chi \downarrow_T)$$

が成り立つ。

5 Multiplicities

有限群 G とその部分群 H を考える。このとき H の指標 φ について、その誘導指標を考えれば $\varphi \uparrow^G(1) = |G:H|\varphi(1)$ が成り立つ。これは CG が左 CH -加群として自由であることによる。同様のことをアソシエーションスキーム (X, S) とその closed subset T で考えても CS は一般に自由 CT -加群ではなく、うまくはいかない。しかし指標の重複度を考えれば同様の議論が可能になることを示す。Thin スキーム、すなわち有限群、の場合には既約指標 χ の次数 $\chi(1)$ と重複度 m_χ は一致するので、これは不思議なことではない。

一般に重複度は既約指標に対してのみ定義されているので、まずはこれを一般の指標 η について以下のように定義する。

$$m_\eta = \sum_{\chi \in \text{Irr}(S)} m(\chi \text{ in } \eta) m_\chi$$

すると有限群の場合の指標の次数に関する式と同じような結果が得られる。

Theorem 5.1. (X, S) をスキーム、 T をその closed subset とする。 T の指標 φ に対して

$$m_{\varphi \uparrow S} = \frac{n_S}{n_T} m_\varphi$$

が成り立つ。

Proof. $\varphi \in \text{Irr}(T)$ について示せば十分である。Frobenius 相互律と指標の直交関係を用いれば

$$\begin{aligned} m_{\varphi \uparrow S} &= \sum_{\chi \in \text{Irr}(S)} m(\chi \text{ in } \varphi \uparrow^S) m_\chi = \sum_{\chi \in \text{Irr}(S)} m(\varphi \text{ in } \chi \downarrow_T) m_\chi \\ &= \sum_{\chi \in \text{Irr}(S)} m_\chi \frac{m_\varphi}{n_T \varphi(1)} \sum_{t \in T} \frac{1}{n_t} \varphi(\sigma_t) \chi(\sigma_{t^*}) \\ &= \frac{m_\varphi}{n_T \varphi(1)} \sum_{t \in T} \frac{1}{n_t} \varphi(\sigma_t) \sum_{\chi \in \text{Irr}(S)} m_\chi \chi(\sigma_{t^*}) \\ &= \frac{m_\varphi}{n_T \varphi(1)} \sum_{t \in T} \frac{1}{n_t} \varphi(\sigma_t) \gamma_S(\sigma_{t^*}) = \frac{m_\varphi}{n_T \varphi(1)} \varphi(1) n_S = \frac{n_S}{n_T} m_\varphi. \end{aligned}$$

である。 □

6 Monomial representations

アソシエーションスキームについての M -群に対応する概念を考えよう。このためには単項表現を考える必要がある。有限群については単項表現はある部分群の 1 次の表現からの誘導表現として定義される。そして、有限群のすべての既約表現が単項表現と同型であるとき、その群を M -群 (monomial group) という。これをそのままアソシエーションスキームに適用すると、任意の可換スキームについて、そのすべての既約表現は 1 次なので、それは monomial になる。しかし、例えば単純群から得られる群アソシエーションスキームは感覚的に可解とは考え難い。そこで定義を見直すことになる。表現の次数が 1 のものを考えるのではなく、重複度 1 のもの考えるのである。このとき次数も 1 となる。

(X, S) をスキームとする。 S の指標 χ に対して、ある closed subset T とその重複度 1 の指標 φ が存在して $\chi = \varphi \uparrow^S$ となるとき χ を単項指標という。すべての既約指標が単項指標であるようなスキームを単項スキーム (monomial scheme) という。次の定理が主定理である。

Theorem 6.1. (X, S) が単項スキームであるとする。任意の i について $D^i(S)$ が S の normal closed subset であると仮定する。このとき、ある ℓ があって $D^\ell(S) = 1$ である。

証明は、指標の次数の代わりに重複度を用いることによって M -群のとき、例えば [3, Theorem 5.12]、とほぼ同じようにできるが、指標の核などに関する説明が必要となるため、ここには書かない。単項スキームであって normal でない $D^i(S)$ をもつようなものの例は見つかっていない。したがって $D^i(S)$ が normal であるという仮定は外せるのかもしれない。

7 An Example

ここでは我々のホームページ [2] の as32, No.10851 について調べる。その指標表は

	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	m_{χ_i}
χ_1	1	1	2	4	4	4	4	4	4	4	1
χ_2	1	1	2	4	4	4	-4	-4	-4	-4	1
χ_3	1	1	2	-4	0	0	-A	A	A	-A	2
χ_4	1	1	2	-4	0	0	A	-A	-A	A	2
χ_5	1	1	2	4	-4	-4	0	0	0	0	2
χ_6	2	0	-2	0	2	-2	0	0	0	0	8
χ_7	1	-1	0	0	-2	2	0	0	0	0	8

である。ここで $A = 2\sqrt{-2}$ である。 $D^i(S)$ は以下のようになる。

$$\begin{aligned} S &= \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9\}, \\ D(S) &= \{s_0, s_1, s_2, s_3, s_4, s_5\}, \\ D^2(S) &= \{s_0, s_1, s_2, s_3\}, \\ D^3(S) &= \{s_0, s_1, s_2\}, \\ D^4(S) &= \{s_0, s_1\}, \\ D^5(S) &= \{s_0\}. \end{aligned}$$

これについて以下のことが確かめられる。

- S の closed subset は $D^i(S)$ ($i = 0, 1, 2, 3, 4, 5$) のみである。
- $D^4(S)$ は S で normal ではない。
- S は単項スキームではない。
- $D(S)$ は可換、べき零であるが、単項スキームではない。

これによって、簡単な修正では Blichfeldt の定理が成り立ちそうもないことが分かる。

References

- [1] A. Hanaki, *Nilpotent schemes and group-like schemes*, to appear in J. Combin. Theory Ser. A.
- [2] A. Hanaki and I. Miyamoto, *Classification of association schemes with small vertices*, published on web (<http://kissme.shinshu-u.ac.jp/as/>).
- [3] I. M. Isaacs, *Character theory of finite groups*, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976.
- [4] Y. Takegahara, *Nilpotent association schemes*, preprint.
- [5] Y. Takegahara and T. Yoshida, *On character theoretical aspects of nilpotency class*, preprint.

量子信号処理における代数的組合せ論*

城本 啓介

愛知県立大学 情報科学部

keisuke@ist.aichi-pu.ac.jp

1 Introduction

One of the main problem in the study of quantum signals is the maximization problem of the mutual information of the quantum channel for a classical information. That is, for the quantum signals in a quantum communication system, the problem is to compute several quantities in quantum information theory, such as the minimum error probability and the maximum mutual information.

Let \mathcal{H} be a finite dimensional Hilbert space over the complex field \mathbb{C} . And let $A = \{x_i : i = 0, 1, \dots, M - 1\}$ be an input alphabet of (classical) information source. For a classical input information $x_i \in A$, there corresponds a quantum signal $|\psi_i\rangle \in \mathcal{H}$ which is transmitted at a transmitter.

In this note, we assume that the quantum signals are *group covariant signals* defined as follows (cf. [1]):

Definition 1 Let G be a finite group. A set of signals $\{|\psi_a\rangle \in \mathcal{H} : a \in G\}$ is called *group covariant* if there exist unitary operators U_b such that

$$U_b|\psi_a\rangle = |\psi_{ba}\rangle, \quad \forall a, b \in G.$$

In [5], the following necessary and sufficient condition for the group covariancy was proved.

Proposition 2 A set of quantum signals $\{|\psi_a\rangle \in \mathcal{H} : a \in G\}$ are group covariant if and only if

$$\langle \psi_{cb} | \psi_{ca} \rangle = \langle \psi_b | \psi_a \rangle, \quad \forall a, b, c \in G.$$

For a finite group G and a set of quantum signals $\{|\psi_a\rangle \in \mathcal{H} : a \in G\}$, we consider the *Gram matrix* Γ given by

$$\Gamma = [(\langle \psi_a | \psi_b \rangle)]_{(a,b) \in G \times G}.$$

The main purpose of this research is to find some equations on the square-root of the Gram matrix. In [6], the case of $G = \mathbb{F}_p^n$ has been discussed, where p is prime.

*白田 毅氏 (愛知県立大学・情報) との共同研究

2 The Main Result

Throughout this section, let G be a finite group. Define that $\Delta_G = \{x \in G : x^2 = 1\}$. Consider a map $f : G \rightarrow \mathbb{C}$ such that $f(\Delta_G) \subseteq \mathbb{R}$ and $f(x^{-1}) = \overline{f(x)}$ for any $x \in G \setminus \Delta$. Then we define the matrix Γ_G as follows:

$$\Gamma_G = [f(a^{-1}b)]_{(a,b) \in G \times G}.$$

Let $\text{Irr}(G) = \{\chi_1, \chi_2, \dots, \chi_k\}$ be the set of irreducible characters of G and let C_1, C_2, \dots, C_k be the conjugacy classes of G . From the *first orthogonality relation* (cf. [2]), we have the following lemma which is essential:

Lemma 3 For any $\chi_i, \chi_j \in \text{Irr}(G)$,

$$\frac{1}{|G|} \sum_{g \in G} \chi_i(g) \chi_j(g^{-1}) = \delta_{ij}.$$

Now we shall consider the eigenvalues and eigenvectors of the matrix Γ_G .

Theorem 4 For any element $g \in G$,

$$\begin{aligned} \lambda_g &= \sum_{a \in G} \chi_i(a) f(a) \\ \text{and} \\ \lambda_g &= \frac{1}{\sqrt{|G|}} [\chi_i(b)]_{b \in G}, \end{aligned}$$

are eigenvalues and the corresponding eigenvectors of the matrix Γ_G , respectively, if $g \in C_i$.

Proof. We shall prove the equation $\Gamma_G \lambda_g = \lambda_g \lambda_g$ for any $g \in G$. For any i and any $g \in C_i$, it follows that

$$\begin{aligned} \Gamma_G \lambda_g &= \frac{1}{\sqrt{|G|}} \left[\sum_{b \in G} f(a^{-1}b) \chi_i(b) \right]_{a \in G} \\ &= \frac{1}{\sqrt{|G|}} \left[\sum_{c \in G} f(c) \chi_i(ac) \right]_{a \in G} \end{aligned}$$

On the other hand, we have the following equation.

$$\begin{aligned} \lambda_g \lambda_g &= \frac{1}{\sqrt{|G|}} \left[\sum_{a \in G} \chi_i(a) f(a) \chi_i(b) \right]_{b \in G} \\ &= \frac{1}{\sqrt{|G|}} \left[\sum_{a \in G} \chi_i(ab) f(a) \right]_{b \in G} \end{aligned}$$

The theorem follows. □

The orthogonality of the eigenvectors of Γ_G follows.

Lemma 5 For any $a, b \in G$,

$$\lambda_a \cdot \lambda_b = \begin{cases} 1 & (a \text{ is conjugate to } b) \\ 0 & (\text{otherwise}) \end{cases}$$

Proof. We assume that $a \in C_i$ and $b \in C_j$. By Proposition 3, we have that

$$\begin{aligned} \lambda_a \cdot \lambda_b &= \frac{1}{|G|} \sum_{c \in G} \chi_i(c) \overline{\chi_j(c)} \\ &= \frac{1}{|G|} \sum_{c \in G} \chi_i(c) \chi_j(c^{-1}) \\ &= \delta_{ij} \end{aligned}$$

□

Using the above results, we have the following proposition:

Proposition 6 Let G be a finite abelian group. Then

$$[(\Gamma_G)^{1/2}]_{(a,b) \in G \times G} = \left[\frac{1}{|G|} \sum_{c \in G} \chi_{ab^{-1}}(c) \sqrt{\sum_{d \in G} \chi_c(d) f(d)} \right]_{(a,b) \in G \times G}.$$

3 An Application to Linear Codes

Let \mathbb{F}_q be a finite field of q elements with characteristic p . Let C be an $[n, r]$ code over \mathbb{F}_q (cf. [4]). Since C is also an additive group, we now consider the case $G = C$. For any vector $\mathbf{v} = (a_1, a_2, \dots, a_n)$, we consider the corresponding quantum signal

$$|\mathbf{v}\rangle = |a_1\rangle \otimes |a_2\rangle \otimes \cdots \otimes |a_n\rangle \in \mathcal{H},$$

where \mathcal{H} is the q^n -dimensional Hilbert space over the complex field \mathbb{C} . For any vectors $\mathbf{v} = (a_1, a_2, \dots, a_n), \mathbf{w} = (b_1, b_2, \dots, b_n) \in \mathbb{F}_q^n$, define the inner product

$$\langle \mathbf{v}, \mathbf{w} \rangle = a_1 \cdot b_1 + a_2 \cdot b_2 + \cdots + a_n \cdot b_n \in \mathbb{F}_q.$$

Set $C = \{\mathbf{v}_0 = \mathbf{0}, \mathbf{v}_1, \dots, \mathbf{v}_{q^r-1}\}$. We consider the Gram matrix $\Gamma_C = [\langle \mathbf{v}_i | \mathbf{v}_j \rangle]_{i,j}$. Now we consider the *absolute trace function* from \mathbb{F}_q to \mathbb{F}_p which is defined by

$$\text{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{m-1}}$$

for any $\alpha \in \mathbb{F}_q$, where $q = p^m$. Then, for any codewords $\mathbf{v}_j, \mathbf{v}_l \in C$, it is known that $\chi_j(l) = e^{2\pi i \text{Tr}(\langle \mathbf{v}_j, \mathbf{v}_l \rangle) / p}$ is an irreducible character of C as an additive group (cf. [3]). Therefore we have the following result from Theorem 4 and Lemma 5.

Proposition 7 For any $[n, r]$ code over \mathbb{F}_q , the vectors

$$\lambda_i = \frac{1}{\sqrt{|G|}} \begin{bmatrix} \chi_i(0) \\ \chi_i(1) \\ \vdots \\ \chi_i(q^r - 1) \end{bmatrix}, \quad i = 0, 1, \dots, q^r - 1$$

are the orthonormal eigenvectors of Γ_C .

So we have the following result for any linear code.

Corollary 8

$$[(\Gamma_C)^{1/2}]_{i,j} = \left[\frac{1}{q^r} \sum_{l=0}^{q^r-1} \chi_{i-j}(l) \sqrt{\sum_{s=0}^{q^r-1} \chi_l(s) \langle v_0 | v_s \rangle} \right]_{i,j},$$

where $i - j$ denotes the index of the vector $v_i - v_j$.

For any positive integer m , we denote the ring of integers modulo m by \mathbb{Z}_m . Let D be a linear code of length n over \mathbb{Z}_m , that is, a \mathbb{Z}_m -submodule of \mathbb{Z}_m^n (cf. [4]). Assume that $|D| = d$ and set $D = \{w_0 = 0, w_1, \dots, w_{d-1}\}$. Then, for any codewords $w_j, w_l \in D$, it is known that $\chi_j(l) = e^{2\pi i \langle w_j, w_l \rangle / m}$ is an irreducible character of D as an additive group, where $\langle w_j, w_l \rangle$ denotes the inner product between w_j and w_l over \mathbb{Z}_m .

By the same argument as linear codes over a finite field, we have the similar result.

Corollary 9 For any linear code D of order d over \mathbb{Z}_m ,

$$[(\Gamma_D)^{1/2}]_{i,j} = \left[\frac{1}{d} \sum_{l=0}^{d-1} \chi_{i-j}(l) \sqrt{\sum_{s=0}^{d-1} \chi_l(s) \langle w_0 | w_s \rangle} \right]_{i,j},$$

where $i - j$ denotes the index of the vector $w_i - w_j$.

Acknowledgements

The author gratefully thanks Professor Yutaka Hiramine for his helpful comments.

References

- [1] E. B. Davies, Information and quantum measurement, *IEEE Trans. Inform. Theory* **24** (1978), pp. 596–599.
- [2] I. M. Isaacs, *Character theory of finite groups*, Academic Press, New York-London, 1976.
- [3] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge, 2003.

- [4] V. Pless, *Introduction to the Theory of Error-Correcting Codes* (Third Edition), Wiley-Interscience, 1998.
- [5] T. S. Usuda and I. Takumi, Group covariant signals in quantum information theory, *Quantum Communication, Computing, and measurement 2*, Plenum, New York, 2000, pp. 37–42.
- [6] T. S. Usuda, S. Usami, I. Takumi and M. Hata, Superradditivity in capacity of quantum channel for q -ary linear dependent real symmetric-state signals, *Physics Letters A* **305** (2002), pp. 125–134.

On d -dimensional dual hyperovals in $PG(2d, 2)$ coming from finite translation affine planes

谷口 浩朗 (詫間電波高専)

July 25, 2007

1 Introduction

Let $GF(q)$ be finite field with q elements. Let d, m be integers with $d \geq 2$ and $m > d$. Let $PG(m, 2)$ be an n -dimensional projective space over the binary field $GF(2)$.

Definition 1. A family S of d -dimensional subspaces of $PG(m, 2)$ is called a d -dimensional dual hyperoval in $PG(m, 2)$ if it satisfies the following conditions;

1. any two distinct members of S intersect in a projective point,
2. any three mutually distinct members of S intersect in the empty projective set,
3. all members of S generate $PG(m, 2)$, and
4. there are exactly 2^{d+1} members of S .

In Example 2. 5 and Theorem 6. 1 of [1] (also see Proposition 3. 1 of [2]), Cooperstein and Thas showed that each d -dimensional dual hyperoval in $PG(2d, 2)$ is obtained as a dual of a partition of $PG(2d, 2) \setminus PG(d, 2)$.

Theorem 1 (Example 2. 5 and Theorem 6. 1 of [1]). *Let $PG(d, 2)$ be a d -dimensional subspace of $PG(2d, 2)$. Consider a partition of $PG(2d, 2) \setminus PG(d, 2)$*

into 2^{d+1} $(d-1)$ -dimensional subspaces. Then the set S of the dual subspaces of these $(d-1)$ -dimensional subspaces in $PG(2d, 2)$ is a d -dimensional dual hyperoval in $PG(2d, 2)$. The converse also holds.

This family is called as Cooperstein-Thas's family in [2]. In [5] (also see [6]), Yoshiara constructed a family of d -dimensional dual hyperovals in $PG(2d, 2)$ in a different way, as follows.

Theorem 2 (Proposition 3 of [5]). *Let σ be a generator of the automorphism group of $GF(2^{d+1})$ over $GF(2)$. Inside $GF(2^{d+1}) \oplus GF(2^{d+1})$, let us define $X_Y(t)$ for $t \in GF(2^{d+1})$ as:*

$$X_Y(t) := \{(x, x^\sigma t + xt^{\sigma^{-1}}) | x \in GF(2^{d+1}) \setminus \{0\}\}.$$

Then $S_Y := \{X_Y(t) | t \in GF(2^{d+1})\}$ is a d -dimensional dual hyperoval in $PG(2d, 2)$.

Then, it is quite natural to ask whether the all members of the Cooperstein-Thas's family are the Yoshiara's dual hyperovals or not. In this paper, we will give a negative answer to this question.

Definition 2 ([3]). Let Π be a vector space over $GF(q)$. A spread T of Π is a collection of at least two subspaces of Π which satisfies the following conditions:

1. two distinct elements of T are isomorphic subspaces,
2. every point except $\{0\}$ of Π is on exactly one subspace in T , and
3. for any $U_1, U_2 \in T$ with $U_1 \neq U_2$, Π is a direct (vector space) sum of U_1 and U_2 .

It is known that the vector space Π has even dimension $2m$ with $m > 0$. Moreover, the cardinality of the spread $|T| = q^m + 1$. (See [3] or [4].)

From spreads of the vector space $V \oplus V$, where V is a $(d+1)$ -dimensional vector space over $GF(2)$, we are able to construct d -dimensional dual hyperovals as follows:

Theorem 3. *Let $V := GF(2)^{d+1}$ be a $(d+1)$ -dimensional vector space over $GF(2)$, and $T := \{K_0, K_1, \dots, K_{2^{d+1}}\}$ a spread of $V \oplus V$. Let v be a non-zero element of $V \oplus V$. We may assume that v is contained in K_0 . Let*

$$\pi : V \oplus V \ni x \mapsto \bar{x} \in \overline{V \oplus V} := (V \oplus V) / \langle v \rangle$$

be a $GF(2)$ -linear mapping with the kernel $\{0, v\}$ (which we denote by $\langle v \rangle$), and the image $(V \oplus V)/\langle v \rangle$. We regard $PG((V \oplus V)/\langle v \rangle) = PG(2d, 2)$. Then,

$$S := \{\pi(K_1) \setminus \{0\}, \pi(K_2) \setminus \{0\}, \dots, \pi(K_{2^{d+1}}) \setminus \{0\}\}$$

is a d -dimensional dual hyperovals in $PG(2d, 2)$.

We will give the proof of this theorem in the following section. We refer the relations among spreads, quasifields and translation affine planes to Kallaher [3] or Lüneburg [4].

Example . We regard $V := GF(2^{d+1})$ as a $(d+1)$ -dimensional vector space over $GF(2)$. Let σ be a generator of the galois group $Gal(GF(2^{d+1})/GF(2))$. Let

$$\pi' : GF(2^{d+1}) \oplus GF(2^{d+1}) \ni (x, y) \mapsto (x, y^\sigma + y) \in GF(2^{d+1}) \oplus GF(2^{d+1}).$$

Then it is easy to see that the kernel of π' is $\{(0, 0), (0, 1)\}$, and the image of π' is $W := \{(x, y) | Tr(y) = 0\}$, which is a $(2d+1)$ -dimensional vector space over $GF(2)$, where Tr is a trace function from $GF(2^{d+1})$ to $GF(2)$.

In $V \oplus V$, let $K_\infty := \{(0, x) | x \in GF(2^{d+1})\}$ and $K_a := \{(x, xa) | x \in GF(2^{d+1})\}$ for $a \in GF(2^{d+1})$. Then, $T := \{K_\infty\} \cup \{K_a | a \in GF(2^{d+1})\}$ is a spread of $V \oplus V$. (It is well known that the translation affine plane constructed from this spread is a Desarguesian affine plane.) Let $S' := \{\pi'(K_a) \setminus \{0\} | a \in GF(2^{d+1})\}$. Then, by Theorem 3, S' is a d -dimensional dual hyperoval in $PG(2d, 2) = PG(W)$.

Proposition 1. S' is isomorphic to the Yoshiara's dual hyperoval S_Y .

Proof. We have $\pi'(K_a) \setminus \{0\} = \{(x, (ax)^\sigma + ax) | x \in GF(2^{d+1}) \setminus \{0\}\}$. If we put $a^\sigma := t$, then $a = t^{\sigma^{-1}}$, hence we have

$$\{(x, (ax)^\sigma + ax) | x \in GF(2^{d+1}) \setminus \{0\}\} = \{(x, x^\sigma t + xt^{\sigma^{-1}}) | x \in GF(2^{d+1}) \setminus \{0\}\}.$$

Therefore, we have $\pi'(K_a) \setminus \{0\} = X_Y(t)$, where $X_Y(t)$ is as in Theorem 2. Consequently, we have $S' = \{\pi'(K_a) \setminus \{0\} | a \in GF(2^{d+1})\} = \{X_Y(t) | t \in GF(2^{d+1})\} = S_Y$ □ □

Now, we will use quasifields Q to construct spreads of $Q \oplus Q$.

Definition 3 ([3],[4]). An algebraic structure $(Q; +, \circ)$ is called a quasifield if it satisfies the following conditions:

1. Q is an abelian group under $+$ with identity 0 ,
2. for $a, c \in Q$ with $a \neq 0$, there exists exactly one $x \in Q$ such that $a \circ x = c$,
3. for $a, b, c \in Q$ with $a \neq b$, there exists exactly one $x \in Q$ such that $x \circ a - x \circ b = c$,
4. for all $a \in Q$, $a \circ 0 = 0 \circ a = 0$,
5. there exists an element $1 \in Q \setminus \{0\}$ such that $1 \circ a = a \circ 1 = a$ for all $a \in Q$, and
6. for all $a, b, c \in Q$, $(a + b) \circ c = a \circ c + b \circ c$.

A nearfield is a quasifield N in which the multiplication \circ is associative; that is, in which $(N \setminus \{0\}, \circ)$ is a group. A semifield is a quasifield S in which the left distributive law

$$a \circ (b + c) = a \circ b + a \circ c$$

holds for all $a, b, c \in S$.

In $Q \oplus Q$, we define $K_\infty := \{(0, y) | y \in Q\}$ and $K_a := \{(x, x \circ a) | x \in Q\}$ for $a \in Q$. Then it is known that $\{K_\infty\} \cup \{K_a | a \in Q\}$ is a spread of $Q \oplus Q$.

Example . [2. 1 and 2. 3 of [9]] Consider the field $GF(q^n)$ where $n \geq 1$ and $q = p^s$ with p a prime and $s \geq 1$. Let $\lambda : GF(q^n) \rightarrow I_n = \{0, 1, \dots, n-1\}$ be a mapping satisfying; (i) $\lambda(0) = \lambda(1) = 0$, and (ii) given $a, b \in GF(q^n) \setminus \{0\}$ there exists $x \neq 0$ with

$$x^{q^{\lambda(a)}} a = x^{q^{\lambda(b)}} b$$

if and only if $a = b$. We define $x \circ y := x^{q^{\lambda(y)}} y$. Then $(GF(q^n), +, \circ)$ is a quasifield called a generalized André system.

Consider also the field $GF(q^n)$ and $q = p^s$ with p a prime and $s \geq 1$, and assume every prime divisor of n divides $q - 1$. Also assume $n \not\equiv 0 \pmod{4}$ if $q \equiv 3 \pmod{4}$. Choosing a primitive element ω of $GF(q^n)$, define $\lambda : GF(q^n) \setminus \{0\} \rightarrow I_n = \{0, 1, \dots, n-1\}$ by

$$(q^{\lambda(a)} - 1)(q - 1)^{-1} \equiv i \pmod{n}, \text{ where } a = \omega^i \in GF(q^n).$$

With $\lambda(0) = 0$, the mapping λ satisfies the conditions (i) and (ii) for a generalized André system. This system, denoted by $N(q, n)$, is a nearfield and is called a regular nearfield (or a Dickson nearfield).

Proposition 2 (Theorem 7.3 and Theorem 7.4 of [4]). *The group $(N(q, n) \setminus \{0\}, \circ)$ in Example is a non-abelian metacyclic group. Moreover, there exist $\phi(n)/m$ non-isomorphic $N(q, n)$'s, where ϕ is a Euler function and m is the order of $p \bmod n$.*

Moreover, it is known that, in $GF(2^{d+1})$, using a natural addition of $GF(2^{d+1})$, we are able to define more multiplications \circ so that we have some semifields, such as Knuth semifields, Kantor semifields or Albert semifields, and so on. (See [3].)

Definition 4 (dual hyperoval S_K). Let $(GF(2^{d+1}), +, \circ)$ be a quasifield, and regard $V := GF(2^{d+1})$ as a vector space over $GF(2)$. In $V \oplus V$, we define $K_\infty := \{(0, x) | x \in GF(2^{d+1})\}$ and $K_a := \{(x, x \circ a) | x \in GF(2^{d+1})\}$ for $a \in GF(2^{d+1})$. Then, $T := \{K_\infty\} \cup \{K_a | a \in GF(2^{d+1})\}$ is a spread of $V \oplus V$. Let σ be a generator of the galois group $Gal(GF(2^{d+1})/GF(2))$. Let π' be a $GF(2)$ -linear mapping defined by

$$\pi' : GF(2^{d+1}) \oplus GF(2^{d+1}) \ni (x, y) \mapsto (x, y^\sigma + y) \in GF(2^{d+1}) \oplus GF(2^{d+1}).$$

Then, as in Example, the image of π' is $W := \{(x, y) | Tr(y) = 0\}$, which is a $2d + 1$ -dimensional vector space over $GF(2)$. We note that the kernel of π' , $\{(0, 0), (0, 1)\}$, is contained in K_∞ . We define $X_K(a) := \pi'(K_a) \setminus \{0\}$. Then, by Theorem 3, $S_K := \{X_K(a) | a \in GF(2^{d+1})\}$ is a d -dimensional dual hyperovals in $PG(2d, 2) = PG(W)$, where

$$X_K(a) = \{(x, (x \circ a)^\sigma + x \circ a) | x \in GF(2^{d+1}) \setminus \{0\}\}.$$

Then we have the following proposition.

Proposition 3. *If the algebraic system $(GF(2^{d+1}), +, \circ)$ is a regular nearfield, then, the automorphism group G_K of the dual hyperoval S_K contains the following subgroup $N := \{n_b | b \in GF(2^{d+1}) \setminus \{0\}\}$ with $n_b(X_K(t)) = X_K(b \circ t)$ defined by*

$$n_b((x, y)) := (x \circ b', y),$$

where b' is an element which satisfies that $b' \circ b = 1$. N is isomorphic to the group $(GF(2^{d+1}) \setminus \{0\}, \circ)$, and so, by Proposition 2, N is a non-abelian metacyclic group with the cardinality $|N| = 2^{d+1} - 1$. If the algebraic system $(GF(2^{d+1}), +, \circ)$ is a semifield, then, the automorphism group G_K of the

dual hyperoval S_K contains the following subgroup $T := \{t_a | a \in GF(2^{d+1})\}$ with $t_a(X_K(t)) = X_K(t + a)$, defined by

$$t_a((x, y)) := (x, y + (x \circ a)^\sigma + x \circ a).$$

T is isomorphic to $GF(2^{d+1})$ as an additive group.

Proof. Since the multiplication \circ is associative in the regular nearfield, we have

$$n_b(X_K(t)) = \{(x \circ b', ((x \circ b') \circ (b \circ t))^\sigma + (x \circ b') \circ (b \circ t))\} = X_K(b \circ t)$$

for $b \in GF(2^{d+1}) \setminus \{0\}$, and hence

$$n_{b_2}(n_{b_1}(X_K(t))) = n_{b_2}(X_K(b_1 \circ t)) = X_K((b_2 \circ b_1) \circ t) = n_{b_2 \circ b_1}(X_K(t))$$

for $b_1, b_2 \in GF(2^{d+1}) \setminus \{0\}$. Therefore $N := \{n_b | b \in GF(2^{d+1}) \setminus \{0\}\}$ is isomorphic to the group $(GF(2^{d+1}) \setminus \{0\}, \circ)$. Since the multiplication \circ has left distributive law in the semifield, we also have

$$t_a(X_K(t)) = \{(x, (x \circ t)^\sigma + x \circ t + (x \circ a)^\sigma + x \circ a)\} = X_K(t + a),$$

hence we have $T \cong GF(2^{d+1})$ as an additive group. □ □

By Theorem 1 (also see 1. 2. Examples (a) of [2]), the complement of the points on the members of the dual hyperoval in $PG(2d, 2)$, that is,

$$PG(2d, 2) \setminus \cup \{\text{the points on the members the dual hyperoval}\}$$

is a $(d - 1)$ -dimensional subspace. Hence we have the following lemma.

Lemma 1. *Let $U := \{(0, y) | y \in GF(2^{d+1}), Tr(y) = 0\}$. Note that $U \subset W := \{(x, y) | x, y \in GF(2^{d+1}), Tr(y) = 0\}$. Then, in $PG(2d, 2) = PG(W)$, the $(d - 1)$ -dimensional subspace $PG(U)$ is the complement of the set $\cup X_K(a)$ of the points which are on some members of the dual hyperoval S_K in Definition 4, that is,*

$$PG(U) = PG(W) \setminus \cup_{a \in GF(2^{d+1})} X_K(a).$$

In section 3, we will prove the following Theorem, hence we give a negative answer to the previous question.

Theorem 4. *Let the algebraic system $(GF(2^{d+1}), +, \circ)$ in Example be regular nearfield. Then, a d -dimensional dual hyperoval S_K in $PG(2d, 2)$ in Definition 4 is not isomorphic to the Yoshiara's dual hyperoval S_Y .*

2 Proof of Theorem 3

Since $K_i \not\cong v$ for $1 \leq i \leq 2^{d+1}$, $\pi(K_i) \setminus \{0\}$ is a d -dimensional subspace in $PG(2d, 2) = PG((V \oplus V)/\langle v \rangle)$ for $1 \leq i \leq 2^{d+1}$. Let $\pi(K_i) \setminus \{0\}$ and $\pi(K_j) \setminus \{0\}$ have a common point $\pi(x_i) = \pi(x_j)$ for $x_i \in K_i \setminus \{0\}$ and $x_j \in K_j \setminus \{0\}$ with $1 \leq i < j \leq 2^{d+1}$. Then, since $\pi(x_i + x_j) = 0$, we have $x_i + x_j = v$. However, since $V \oplus V$ is a direct sum of K_i and K_j by 3 of Definition 2, there exist unique $x_i \in K_i \setminus \{0\}$ and unique $x_j \in K_j \setminus \{0\}$ which satisfies that $x_i + x_j = v$. Thus, we have proved that $\pi(K_1) \setminus \{0\}$ and $\pi(K_1) \setminus \{0\}$ have only one common point. Assume that $\pi(K_s) \setminus \{0\}$, $\pi(K_t) \setminus \{0\}$ and $\pi(K_u) \setminus \{0\}$ have a common point $\pi(x_s) = \pi(x_t) = \pi(x_u)$ for $x_s \in K_s \setminus \{0\}$, $x_t \in K_t \setminus \{0\}$ and $x_u \in K_u \setminus \{0\}$ with $1 \leq s < t < u \leq 2^{d+1}$. Then, since $\pi(x_s + x_t) = 0$, we have $x_s + x_t = v$. We also have $x_s + x_u = v$. However, we have $x_t = x_u$ from these equations, which contradicts 2 of Definition 2. Hence $\pi(K_s) \setminus \{0\}$, $\pi(K_t) \setminus \{0\}$ and $\pi(K_u) \setminus \{0\}$ with $1 \leq s < t < u \leq 2^{d+1}$ have no common point. Since the cardinality

$$|S| := |\{\pi(K_1) \setminus \{0\}, \pi(K_2) \setminus \{0\}, \dots, \pi(K_{2^{d+1}}) \setminus \{0\}\}| = 2^{d+1},$$

S is a d -dimensional dual hyperoval in $PG(2d, 2) = PG((V \oplus V)/\langle v \rangle)$.

3 Proof of Theorem 4

We consider the dual hyperovals inside the projective space

$$PG(2d, 2) = \{(x, y) | (x, y) \in GF(2^{d+1}) \oplus GF(2^{d+1}) \setminus \{(0, 0)\}, Tr(y) = 0\}.$$

We recall that an automorphism of the dual hyperoval S in $PG(2d, 2)$ is a linear transformation which permute the members of S . We also define an isomorphism of the dual hyperovals S to S' as a linear transformation of $PG(2d, 2)$ which sends each member of S to that of S' .

Let $d + 1 = sn$ with $s \geq 1$, and assume every prime divisor of n divides $2^s - 1$. (for example, $(s, n) = (4, 3)$, etc.) Then, by Example , we are able to define a multiplication \circ of $GF(2^{d+1})$ such that $(GF(2^{d+1}), +, \circ)$ is a regular near field. Hence, by Definition 4, we have a dual hyperoval $S_K = \{X_K(t) | t \in GF(2^{d+1})\}$, where

$$X_K(t) := \{(x, (x \circ t)^s + x \circ t) | x \in GF(2^{d+1}) \setminus \{0\}\}.$$

By Proposition 3, the automorphism group G_K of the dual hyperoval S_K contains a subgroup $N := \{n_b | b \in GF(2^{d+1}) \setminus \{0\}\}$ with $n_b(X_K(t)) = X_K(bot)$ defined by

$$n_b((x, y)) := (x \circ b', y),$$

where $b' \circ b = 1$. By Proposition 2, N is a non-abelian metacyclic group with the cardinality $|N| = 2^{d+1} - 1$.

We recall that the automorphism group G_Y of Yoshiara's dual hyperoval S_Y is generated by the group T , M and F , where $T = \{t_a | a \in GF(2^{d+1})\}$ with $t_a(X_Y(t)) = X_Y(t + a)$ defined by

$$t_a : (x, y) \mapsto (x, x^\sigma a + xa^{\sigma^{-1}} + y),$$

$M = \{m_b | b \in GF(2^{d+1}) \setminus \{0\}\}$ with $m_b(X_Y(t)) = X_Y(bt)$ defined by

$$m_b : (x, y) \mapsto (xb^{-1}, y),$$

and $F = \{f_\tau | \tau \in Gal(GF(2^{d+1})/GF(2))\}$ with $f_\tau(X_Y(t)) = X_Y(t^\tau)$ defined by

$$f_\tau : (x, y) \mapsto (x^\tau, y^\tau).$$

We also have $G_Y = T : (M : F)$. Hence G_Y is doubly transitive on the members of S_Y . (See Proposition 7 of [5].) We note that M is a cyclic group with the cardinality $|M| = 2^{d+1} - 1$. The following lemma is easily obtained from the expressions of T , M and F and the fact that $G_Y = T : (M : F)$. Hence we omit the proof.

Lemma 2. *Let $g \in G_Y$ with the action $g : (x, y) \mapsto (g_1(x, y), g_2(x, y))$, where g_1 and g_2 are $GF(2)$ -linear mapping. If $g_2(x, y) = y$ for any $(x, y) \in GF(2^{d+1}) \oplus GF(2^{d+1})$ with $Tr(y) = 0$, then we have $g \in M$.*

We assume to the contrary that there exists an isomorphism i from S_K to S_Y . Since G_Y is doubly transitive on the members of S_Y , we may assume that $i(X_K(0)) = X_Y(0)$, that is, i maps $\{(x, 0) | x \in GF(2^{d+1})\}$ onto itself. On the other hand, since i is an isomorphism from $S_K = \{X_K(t) | t \in GF(2^{d+1})\}$ to $S_Y = \{X_Y(t) | t \in GF(2^{d+1})\}$, we have

$$i(\cup_{t \in GF(2^{d+1})} X_K(t)) = \cup_{t \in GF(2^{d+1})} X_Y(t).$$

Hence, by Lemma 1, we have

$$i(U) = i(PG(2d, 2) \setminus \cup_{t \in GF(2^{d+1})} X_K(t)) = PG(2d, 2) \setminus \cup_{t \in GF(2^{d+1})} X_Y(t) = U$$

which means that i maps $\{(0, y) | y \in GF(2^{d+1}), Tr(y) = 0\}$ onto itself. Therefore, there exist $GF(2)$ -linear mapping f and g such that the isomorphism i is expressed as follows:

$$i((x, y)) = (f(x), g(y)). \quad (1)$$

Now, we have $i(N) = \{i(n_b) | b \in GF(2^{d+1}) \setminus \{0\}\} \cong N$ as a subgroup of G_Y with the action $i(n_b)(X_Y(t)) = i(n_b(i^{-1}(X_Y(t))))$ for $X_Y(t) \in S_Y$. Then, by (1), the action of $i(n_b)$ is

$$i(n_b) : (x, y) \mapsto (f(f^{-1}(x) \circ b), y).$$

Hence, by Lemma 2, $i(N)$ is a subgroup of $M \subset G_Y$. However, the cardinality $|i(N)| = |M| = 2^{d+1} - 1$. Moreover, N is a non-abelian metacyclic group and M is a cyclic group. This is impossible. Hence, we have a contradiction. Therefore, we finally have that the dual hyperoval S_K is not isomorphic to the Yoshiara's dual hyperoval S_Y .

References

- [1] B. N. Cooperstein and J. A. Thas, On Generalized k -Arcs in $PG(2n, q)$, *Annals of Combinatorics*. 5 (2001), 141–152.
- [2] A. del Fra, On d -dimensional dual hyperovals, *Geometriae Dedicata* 26 (2000), 157–178.
- [3] M. Kallaher, Translation Planes, *Handbook of Incidence Geometry*, Elsevier Science B. V. (1995), 137–192.
- [4] H. Lüneburg, *Translation Planes*, Springer-Verlag (1980).
- [5] S. Yoshiara, A family of d -dimensional dual hyperovals in $PG(2d + 1, 2)$. *European J. Combin.* 20 (1999), no. 6, 589–603.
- [6] H. Taniguchi and S. Yoshiara, On dimensional dual hyperovals $S_{\sigma, \phi}^{d+1}$. *Innov. Incidence Geom.* 1 (2005), 197–219.

A characterization of some distance-regular graphs

平木 彰 (大阪教育大学) Akira HIRAKI (Osaka Kyoiku University)

1. Definition.

Let $\Gamma = (V\Gamma, E\Gamma)$ be a connected graph with usual shortest path distance ∂_Γ . Let d be the diameter of Γ (i.e., the maximal distance of two vertices in Γ). Set

$$\Gamma_j(x) = \{ y \in V\Gamma \mid \partial_\Gamma(x, y) = j \}.$$

For $x, y \in V\Gamma$ with $\partial_\Gamma(x, y) = i$, let

$$A(x, y) = \Gamma_i(x) \cap \Gamma_1(y), B(x, y) = \Gamma_{i+1}(x) \cap \Gamma_1(y), C(x, y) = \Gamma_{i-1}(x) \cap \Gamma_1(y).$$

Definition 1. Let i be an integer with $0 \leq i \leq d$.

- (i) We say $c_i(\Gamma)$ -exists if $c_i(\Gamma) = |C(x, y)|$ is constant whenever $\partial_\Gamma(x, y) = i$.
- (ii) We say $a_i(\Gamma)$ -exists if $a_i(\Gamma) = |A(x, y)|$ is constant whenever $\partial_\Gamma(x, y) = i$.
- (iii) We say $b_i(\Gamma)$ -exists if $b_i(\Gamma) = |B(x, y)|$ is constant whenever $\partial_\Gamma(x, y) = i$.

A connected graph Γ of diameter d is said to be *distance-regular* if $c_i(\Gamma)$ -exists and $b_i(\Gamma)$ -exists for $i = 0, \dots, d$. Then Γ is a regular graph of valency $k = k(\Gamma) = b_0(\Gamma)$ and that $a_i(\Gamma)$ -exists with $a_i(\Gamma) = k(\Gamma) - c_i(\Gamma) - b_i(\Gamma)$ for $i = 0, \dots, d$. The constants $c_i(\Gamma), a_i(\Gamma)$ and $b_i(\Gamma)$ ($i = 0, \dots, d$) are called the *intersection numbers* of Γ .

For more background information about distance-regular graphs we refer the reader to [1, 2].

Let Γ be a distance-regular graph of diameter $d = d(\Gamma) \geq 2$ and valency $k = k(\Gamma) \geq 3$. We write c_i, a_i and b_i for the intersection numbers $c_i(\Gamma), a_i(\Gamma)$ and $b_i(\Gamma)$ of Γ .

Let Δ be a subset of vertices in Γ . We identify Δ with the induced subgraph on it. Let $x \in \Delta$. Δ is called *strongly closed* (resp. *geodetically closed*) with respect to x if $C(x, y) \cup A(x, y) \subseteq \Delta$ (resp. $C(x, y) \subseteq \Delta$) for any $y \in \Delta$. Δ is called *strongly closed* (resp. *geodetically closed*) if it is strongly closed (resp. geodetically closed) with respect to x for any $x \in \Delta$. It is clear that a strongly closed subgraph is geodetically closed.

Definition 2. We say *the condition $(SC)_m$ holds* if for any pair of vertices at distance m there exists a strongly closed subgraph of diameter m containing them.

The Odd graphs, the doubled Odd graphs, the doubled Grassmann graphs, the Hamming graph and the dual polar graph satisfy the condition $(SC)_{d-1}$, where d is the diameter.

Our problem is to classify distance-regular graph of diameter d satisfying the condition $(SC)_{d-1}$. In this note we give some results which are partial answers of this problem.

2. Strongly closed subgraphs.

In this section we recall known facts for strongly closed subgraphs.

The Hamming graph $H(d, n)$ is a graph with

$$V\Gamma = (\mathbb{Z}_n)^d \quad \text{and} \quad (u, v) \in E\Gamma \Leftrightarrow \#\{i \mid u_i \neq v_i\} = 1.$$

Then

$$\partial_\Gamma(u, x) = j \Leftrightarrow \#\{i \mid u_i \neq x_i\} = j$$

(i.e., Hamming distance). It is known that $H(d, n)$ is distance-regular with

$$\begin{Bmatrix} c_i \\ a_i \\ b_i \end{Bmatrix} = \begin{Bmatrix} * & 1 & \cdots & j & \cdots & d \\ 0 & (n-2) & \cdots & j(n-2) & \cdots & d(n-2) \\ d(n-1) & (d-1)(n-1) & \cdots & (d-j)(n-1) & \cdots & * \end{Bmatrix}.$$

Let (x, y) be a pair of vertices at distance t in $H(d, n)$. Then $\#\{i \mid u_i \neq x_i\} = j$ and thus $\#\{i \mid u_i = x_i\} = d - j$. We set $\Lambda = \{i \mid u_i = x_i\}$ and

$$\Delta = \Delta(x, y) = \{z \in (\mathbb{Z}_n)^d \mid z_i = x_i = y_i \text{ for all } i \in \Lambda\}.$$

It is not hard to see that Δ is a strongly closed subgraph of $H(d, n)$ which is isomorphic to $H(t, n)$. This implies that the Hamming graph $H(d, n)$ satisfies the condition $(SC)_t$ for $t = 1, \dots, d - 1$. In particular, any strongly closed subgraph is also a Hamming graph. Similarly it can be shown that the dual polar graphs of diameter d satisfy the condition $(SC)_t$ for $t = 1, \dots, d - 1$ and any strongly closed subgraph is also the dual polar graph.

Let Δ be a geodetically closed subgraph of Γ with diameter $m = d(\Delta)$. For any vertices x and y in Δ , a shortest path between x and y in Γ is contained in the subgraph Δ . So the distance in Δ coincides with the distance in Γ . Then $c_i(\Delta)$ -exists with $c_i(\Delta) = c_i$ for $i = 1, \dots, m$. Moreover if Δ is strongly closed, then $a_i(\Delta)$ -exists with $a_i(\Delta) = a_i$ for $i = 1, \dots, m$. Hence if Δ is a regular graph of valency $k(\Delta)$, then $b_i(\Delta)$ -exists with $b_i(\Delta) = k(\Delta) - c_i - a_i$ for $i = 1, \dots, m$. and thus Δ is distance-regular. However there exist several examples of non-regular strongly closed subgraphs in a distance-regular graph.

- Suppose Γ is either the doubled Grassmann graph, the doubled Odd graph, or the Odd graph. The it satisfies the condition $(SC)_t$ for $t = 1, \dots, d - 1$, where $d = d(\Gamma)$. Any strongly closed subgraph of odd diameter $2m + 1 \leq d - 1$ is a doubled Grassmann graph, or a doubled Odd graph But any strongly closed subgraph of even diameter $2m \leq d - 1$ is non-regular distance-biregular graph (see [4]).
- For any pair of vertices at distance 6 in the Foster graph there exists a 2-subdivision graph of the Peterson graph (the graph obtained from the Peterson graph by replacing each edge by a path of length 2) containing them as a strongly closed subgraph (see [9]).
- For any pair of vertices at distance 5 in the Biggs-Smith graph there exists a 3-subdivision graph of the complete graph K_4 (the graph obtained from the complete graph K_4 by replacing each edge by a path of length 3) containing them as a strongly closed subgraph (see [9]).

The next results are direct consequences of [3, Theorem 1], [9, Theorem 1.1], [4, Proposition 4.5] (see also [5, Corollary 7]).

Proposition 3. *Let Γ be a distance-regular graph of diameter $d \geq 3$ and valency $k \geq 3$. Let m be an integer with $1 \leq m \leq d - 1$. Suppose the condition $(SC)_m$ holds. Then the following hold.*

- (i) *The condition $(SC)_j$ holds for all j with $1 \leq j \leq m$.*
- (ii) *Any strongly closed subgraph of diameter m satisfies the condition $(SC)_j$ for all j with $1 \leq j \leq m - 1$.*
- (iii) *Let $r = r(\Gamma) := \max\{i \mid (c_i, a_i, b_i) = (c_1, a_1, b_1)\}$. Then one of the following holds.*
 - (a) $m \leq r$.
 - (b) $m = r + 2 \in \{5, 8\}$, $a_1 = 0$ and $(c_{r+1}, a_{r+1}, b_{r+1}) = (c_{r+2}, a_{r+2}, b_{r+2}) = (1, 1, k - 2)$.
 - (c) $r = 4$, $m = 6$, $a_1 = \dots = a_6 = 0$, $c_5 = c_6 = 2$ and $k \in \{3, 57\}$.
 - (d) Γ is either the doubled Grassmann graph, the doubled Odd graph, or the Odd graph.
 - (e) $b_{m-1} > b_m$ and any strongly closed subgraph of diameter m is distance-regular.

Since a strongly closed subgraph of diameter 1 is a clique of size $a_1 + 2$, it is straightforward to see the following fact.

Lemma 4. *The following conditions are equivalent.*

- (i) Γ contains no induced subgraph $K_{2,1,1}$.
- (ii) Each edge lies on a clique of size $a_1 + 2$.
- (iii) The condition $(SC)_1$ holds.

Let Γ be a distance-regular graph of diameter $d \geq 3$. Suppose the condition $(SC)_{d-1}$ holds. Then Proposition 3 implies that the condition $(SC)_j$ holds for all $j = 1, \dots, d - 1$. We can obtain the following fact (see [5]).

Lemma 5. *Suppose the condition $(SC)_m$ holds. Then for any integer i with $1 \leq i \leq m$ the following hold.*

- (i) *For any vertex u in Γ the subgraph induced by $\Gamma_1(u)$ is a disjoint union of $\frac{b_0}{1 + a_1}$ cliques of size $1 + a_1$.*
- (ii) *For any pair (x, y) of vertices at distance i the subgraph induced by $B(x, y)$ is a disjoint union of $\frac{b_i}{1 + a_1}$ cliques of size $a_1 + 1$.*
- (iii) *For any pair (w, z) of vertices at distance $i + 1$ the subgraph induced by $C(w, z)$ is a coclique of size c_{i+1} . In particular, $a_{i+1} \geq c_{i+1}a_1$.*

3. Results.

In this section we introduce some results which are partial answers of our problem. We refer the reader to papers [5, 6, 7, 8] for the proofs.

Theorem 6. ([5]) *Let Γ be a distance-regular graph of diameter $d \geq 3$ and valency $k \geq 3$. Suppose $b_{d-1} = a_1 + 1$ and the condition $(SC)_{d-1}$ hold. Then Γ is either the Pappus graph, the Coxeter graph, the doubled Odd graph $2O_k$ or the Hamming graph $H(d, a_1 + 2)$.*

Lemma 5 shows that if the condition $(SC)_{d-1}$ holds, then for any pair (x, y) of vertices at distance $d - 1$ the subgraph induced by $B(x, y)$ is disjoint union of cliques of size $1 + a_1$. Hence the case $b_{d-1} = a_1 + 1$ is the extremal case.

Theorem 7. ([6]) *Let Γ be a distance-regular graph of diameter $d \geq 4$ and valency $k \geq 3$ such that $b_{d-2} > b_{d-1}$. Suppose the condition $(SC)_{d-1}$ holds. Let $q = \frac{b_{d-1}}{b_{d-2} - b_{d-1}}$. Then $c_2 \leq q + 1$. Moreover the following conditions are equivalent.*

- (i) $c_2 = q + 1$.
- (ii) Γ has classical parameters $(d, q, 0, a_1 + 1)$.
- (iii) Γ is either the Hamming graph or the dual polar graph.

Proposition 8. ([7]) *Let Γ be a distance-regular graph of diameter $d \geq 3$ and valency $k \geq 3$. Let t be a positive integer with $t \leq d - 1$. Suppose the condition $(SC)_t$ holds. Then for any positive integers i and j with $i + j \leq t + 1$, the following hold.*

$$(c_i - c_{i-1})(c_{j+1} - c_j) \leq c_{i+j} - c_{i+j-1}, \quad (1)$$

$$(a_i - a_{i-1})(c_{j+1} - c_j) \leq a_{i+j} - a_{i+j-1}, \quad (2)$$

$$(b_{i-1} - b_i)(c_{j+1} - c_j) \leq b_{i+j-1} - b_{i+j}, \quad (3)$$

$$c_i(c_{j+1} - c_j) \leq c_{i+j} - c_j, \quad (4)$$

$$a_i(c_{j+1} - c_j) \leq a_{i+j} - a_j, \quad (5)$$

$$(b_0 - b_i)(c_{j+1} - c_j) \leq b_j - b_{i+j}, \quad (6)$$

$$(c_i - c_{i-1})c_{j+1} \leq c_{i+j} - c_{i-1}, \quad (7)$$

$$(a_i - a_{i-1})c_{j+1} \leq a_{i+j} - a_{i-1}, \quad (8)$$

$$(b_{i-1} - b_i)c_{j+1} \leq b_{i-1} - b_{i+j}. \quad (9)$$

Moreover the following hold.

- (i) The equality holds in (3) if and only if the equalities hold in both of (1) and (2).
- (ii) The equality holds in (6) if and only if the equalities hold in both of (4) and (5).
- (iii) The equality holds in (9) if and only if the equalities hold in both of (7) and (8).

We are interested in the case that the equalities hold for those inequalities in Proposition 8.

Theorem 9. ([7]) *Let Γ be a distance-regular graph of diameter $d \geq 4$ and valency $k \geq 3$. Suppose the condition $(SC)_{d-1}$ holds. Then*

$$(b_{i-1} - b_i)(c_{j+1} - c_j) \leq b_{i+j-1} - b_{i+j}, \quad (10)$$

$$(b_0 - b_i)(c_{j+1} - c_j) \leq b_j - b_{i+j} \quad (11)$$

and

$$(b_{i-1} - b_i)c_{j+1} \leq b_{i-1} - b_{i+j} \quad (12)$$

hold for any positive integers i and j with $i + j \leq d$. Moreover, the following hold.

(i) *Suppose $c_2 = 1$ and one of the following conditions holds. Then Γ is either the Odd graph, the doubled Odd graph or the doubled Grassmann graph.*

(i-a) *The equality in (11) holds for some i and j such that $i \geq 3$ and $c_{j+1} > c_j$.*

(i-b) *The equality in (12) holds for some i and j such that $i \geq 2$, $j \geq 2$ and $b_{i-1} > b_i$.*

(ii) *Suppose $c_2 > 1$. Then the following 5 conditions are equivalent.*

(ii-a) *The equality in (10) holds for some i and j such that $i \geq 2$ and $i + j = d$.*

(ii-b) *The equality in (11) holds for some i and j such that $i \geq 2$ and $i + j = d$.*

(ii-c) *The equality in (12) holds for some i and j such that $i \geq 2$ and $i + j = d$.*

(ii-d) *The equalities in (10),(11),(12) hold for all i and j .*

(ii-e) *Γ is either the Hamming graph or the dual polar graph.*

Proposition 10. ([8]) *Let Γ be a distance-regular graph with $d \geq 5$. Let q and m be integers with $q > 1$ and $4 \leq m \leq d - 1$. Suppose for any three distinct vertices, the number of common neighbors of them are 0, 1 or $q + 1$. Then the following conditions are equivalent:*

(i) *$c_i = 1 + q + \dots + q^{i-1}$ and $a_i = 0$ for all i with $1 \leq i \leq m$.*

(ii) *The condition $(SC)_m$ holds. Moreover q is a prime power and any strongly closed subgraph of diameter m is the dual polar graph on $[D_m(q)]$.*

These results are partial answers of our problem.

References

- [1] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin-Cummings, California, 1984.
- [2] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer Verlag, Berlin, Heidelberg, 1989.
- [3] A. Hiraki, A distance-regular graph with strongly closed subgraphs, *J. Alg. Combin.* **14** (2001), 127–131.
- [4] A. Hiraki, A characterization of the doubled Grassmann graphs, the doubled Odd graphs, and the Odd graphs by strongly closed subgraphs, *Europ. J. Combin.* **24** (2003), 161–171.
- [5] A. Hiraki, A characterization of the Hamming graph by strongly closed subgraphs, preprint
- [6] A. Hiraki, A characterization of the Hamming graph and the dual polar graph by strongly closed subgraphs, preprint
- [7] A. Hiraki, A characterization of some distance-regular graphs by strongly closed subgraphs, preprint
- [8] A. Hiraki, Strongly closed subgraphs in a distance-regular graph with $c_2 > 1$, preprint
- [9] H. Suzuki, On strongly closed subgraphs of highly regular graphs, *Europ. J. Combin.* **16** (1995), 197–220.

超幾何多項式の積公式

吉田知行 (北大・理)

YOSHIDA, Tomoyuki

yoshidat@math.sci.hokudai.ac.jp

1 ${}_2F_0$ 型超幾何級数

一般超幾何級数とは次のような級数のことである：

$${}_pF_q(\alpha_1, \dots, \alpha_p; \beta_1, \dots, \beta_q; z) = \sum_{k=0}^{\infty} \frac{(\alpha_1)_k \cdots (\alpha_p)_k}{(\beta_1)_k \cdots (\beta_q)_k} \frac{z^k}{k!}$$

ここで $(\alpha)_k := \alpha(\alpha+1)\cdots(\alpha+k-1) = (-1)^k \binom{-\alpha}{k} k!$ と書いた。とくに ${}_2F_1(\alpha, \beta; \gamma; z)$ を Gauss の超幾何級数, ${}_1F_1(\alpha; \beta; z)$ を合流型超幾何級数という。一般超幾何級数のうちで, ${}_2F_0$ 型超幾何級数

$${}_2F_0(\alpha, \beta; z) = \sum_{k=0}^{\infty} \frac{(\alpha)_k (\beta)_k}{k!} z^k = \sum_{k=0}^{\infty} \binom{-\alpha}{k} \binom{-\beta}{k} k! z^k$$

はほとんど研究されていないようである。実際, α, β のどちらかが非負整数の場合(そのときは多項式になる)を除けば, その収束半径はゼロであり, したがって形式的整級数としての意味しかない。この級数は, 特異性の強い微分方程式

$$z^2 y'' + ((1 + \alpha + \beta) - z)y' + \alpha\beta y = 0 \quad (1)$$

の解であり, 微分漸化式

$$\frac{d}{dz} {}_2F_0(\alpha, \beta; z) = \alpha\beta {}_2F_0(\alpha + 1, \beta + 1; z) \quad (2)$$

を満たす. 他の超幾何関数と同様に, ${}_2F_0$ 型超幾何級数についても, 次のような積公式が知られている (Chaundy, 1943) :

$${}_2F_0(\alpha, \beta; pz) {}_2F_0(\alpha', \beta'; qz) = \sum_{n=0}^{\infty} \frac{(\alpha)_n (\beta)_n (pz)^n}{n!} {}_3F_2 \left[\begin{matrix} \alpha', \beta', -n \\ 1-\alpha-n, 1-\beta-n \end{matrix}; -q/p \right] \quad (3)$$

これから紹介するのは, この積公式とは違ったタイプのもので, 確率統計の分野と関係している. 以下では, 非負整数 a, b に対し, ${}_2F_0$ 型超幾何多項式について, 記号

$$F_{a,b}(z) := {}_2F_0(-a, -b; z) = \sum_{k \geq 0} \binom{a}{k} \binom{b}{k} k! z^k \quad (4)$$

を用いることにする.

以下, $\mathbf{a} = (a_1, \dots, a_m), \mathbf{b} = (b_1, \dots, b_m)$ は, $\sum_i a_i = \sum_j b_j = n$ を満たす非負整数ベクトルとし,

$$\text{TAB}(\mathbf{a}, \mathbf{b}) := \{ \mathbf{x} = (x_{ij}) \mid x_{ij} \geq 0, \sum_j x_{ij} = a_i, \sum_i x_{ij} = b_j \} \quad (5)$$

と定義する. $\text{TAB}(\mathbf{a}, \mathbf{b})$ の元 \mathbf{x} は, 整数計画法に輸送方程式の解である.

主定理 (積公式)
$$\prod_{i=1}^m F_{a_i, b_i}(z) = \sum_{\mathbf{x} \in \text{TAB}(\mathbf{a}, \mathbf{b})} F_{n, \text{Tr}(\mathbf{x})}(z)$$
 (6)

この定理は次のようにも書き換えられる.

$$\prod_{i=1}^m F_{a_i, b_i}(z) = \sum_{\mathbf{x} \in \text{TAB}(\mathbf{a}, \mathbf{b})} p(r) F_{n,r}(z) \quad (7)$$

ここで,

$$p(r) := \sum_{\text{Tr}(\mathbf{x})=r} H(\mathbf{x}), \quad H(\mathbf{x}) := \frac{\mathbf{a}! \mathbf{b}!}{n! \mathbf{x}!} = \frac{\prod_i a_i! \times \prod_j b_j!}{n! \prod_{ij} x_{ij}!} \quad (8)$$

ここに現れた $H(\mathbf{x})$ ($\mathbf{x} \in \text{TAB}(\mathbf{a}, \mathbf{b})$) の確率論的意味を述べておく. 容易に分かるように, $H(\mathbf{x})$ は $\text{TAB}(\mathbf{a}, \mathbf{b})$ 上の確率分布である. すなわ

ち $0 \leq H(\mathbf{x}) \leq 1$ で, $\sum_{\mathbf{x}} H(\mathbf{x}) = 1$. これより, $0 \leq p(r) \leq 1$ で, $\sum p(r) = 1$.

$|N| = n, |M| = m$ なる集合 N と M を取る. データセット $[f]$ とは, 単に写像 $f: N \rightarrow M$ のことである. 非負整数ベクトル

$$\text{type}[f] := (|f^{-1}(i)|)_{i \in M}$$

を $[f]$ の度数分布表という. ここでは単に型とよんでおく. 型 \mathbf{a} を持つデータセットの全体を

$$\text{DS}(\mathbf{a}) := \{[f] \mid f: N \rightarrow M, \text{type}[f] = \mathbf{a}\}$$

で表す. このとき

$$|\text{DS}(\mathbf{a})| = \frac{n!}{\mathbf{a}!} = \frac{n!}{\prod_i a_i!}$$

である.

$$\text{DS}(\mathbf{a}, \mathbf{b}) := \text{DS}(\mathbf{a}) \times \text{DS}(\mathbf{b})$$

の元 $[f, g]$ のことを2次元データセットという. このとき写像

$$\text{tab}: \text{DS}(\mathbf{a}, \mathbf{b}) \rightarrow \text{TAB}(\mathbf{a}, \mathbf{b}); [f, g] \mapsto (|f^{-1}(i) \cap g^{-1}(j)|)_{ij}$$

がある. $\text{tab}[f, g]$ をデータセット $[f, g]$ の分割表という.

$\mathbf{x} = (x_{ij}) \in \text{TAB}(\mathbf{a}, \mathbf{b})$ に対し,

$$|\text{tab}^{-1}(\mathbf{x})| = \#\{[f, g] \in \text{DS}(\mathbf{a}, \mathbf{b}) \mid \text{tab}[f, g] = \mathbf{x}\} = \frac{n!}{\mathbf{x}!} = \frac{n!}{\prod_{i,j} x_{ij}!}$$

である. とくに $[f, g] \in \text{DS}(\mathbf{a}, \mathbf{b})$ が $\text{tab}[f, g] = \mathbf{x}$ を満たす確率は

$$\text{Prob}(\text{tab}[f, g] = \mathbf{x}) = \frac{\mathbf{a}! \mathbf{b}!}{n! \mathbf{x}!} = H(\mathbf{x})$$

となる. つまり周辺和が \mathbf{a}, \mathbf{b} であるような分割表として \mathbf{x} が現れる確率が $H(\mathbf{x})$ である. $H(\mathbf{x})$ は多項超幾何確率と呼ばれることがある.

2 積公式の証明

たくさんの証明がある. ここでは純粋に組合せ論的で短いものの概略を紹介する. 積公式の左辺の積は

$$\prod_{j=1}^m F_{a_j, b_j}(z) = \prod_{j=1}^m \sum_{k_j \geq 0} \binom{a_j}{k_j} \binom{b_j}{k_j} k_j! z^{k_j} = \sum_{k \geq 0} \left[\sum_{\sum k_j = k} \prod_j \binom{a_j}{k_j} \binom{b_j}{k_j} k_j! \right] z^k$$

と展開される。右辺は

$$\sum_{k \geq 0} \sum_{\mathbf{x} \in \text{TAB}(\mathbf{a}, \mathbf{b})} H(\mathbf{x}) \binom{n}{k} \left(\frac{\text{Tr}(\mathbf{x})}{k} \right)^k z^k$$

なので、結局

$$\sum_{\sum k_j = k} \prod_j \binom{a_j}{k_j} \binom{b_j}{k_j} k_j! = \sum_{\mathbf{x} \in \text{TAB}(\mathbf{a}, \mathbf{b})} H(\mathbf{x}) \binom{n}{k} \left(\frac{\text{Tr}(\mathbf{x})}{k} \right)^k k! \quad (9)$$

すなわち

$$\mathbb{E}_{\mathbf{x}} \left[\binom{\text{Tr}(\mathbf{x})}{k} \right] = \frac{1}{(n)_k} \sum_{\sum k_i = k} \prod_j \binom{a_i}{k_i} \binom{b_i}{k_i} k_i! \quad (10)$$

を示せばよい。 $\mathbb{E}_{\mathbf{x}}$ は $\text{TAB}(\mathbf{a}, \mathbf{b})$ 上の平均値で、 $(n)_k := n(n-1)\cdots(n-k+1)$ である。左辺は

$$\mathbb{E}_{[f,g]} \left[\binom{x_0[f,g]}{k} \right] = \frac{1}{|\text{DS}(\mathbf{a}, \mathbf{b})|} \sum_{[f,g]} \binom{x_0[f,g]}{k}$$

に等しいことに注意しておく。ここで $\mathbb{E}_{[f,g]}$ は $\text{DS}(\mathbf{a}, \mathbf{b})$ 上の平均値で、 $x_0[f,g]$ は一致数である。

まず $k=1$ に対する (10) を示そう。この場合、次を示せばよい。

$$\mathbb{E}_{[f,g]}(x_0[f,g]) = \frac{1}{n} \sum_j a_j b_j \quad (11)$$

すなわち

$$\frac{1}{|\text{DS}(\mathbf{a}, \mathbf{b})|} \sum_{[f,g] \in \text{DS}(\mathbf{a}, \mathbf{b})} \#\{i \in N \mid f(i) = g(i)\} = \frac{1}{n} \sum_j a_j b_j$$

左辺の和の部分は、次のようになる。

$$\begin{aligned} \# &:= \#\{(f, g, c) \mid [f, g] \in \text{DS}(\mathbf{a}, \mathbf{b}), c \in N, f(c) = g(c)\} \\ &= \sum_{c \in N} \#\{[f, g] \in \text{DS}(\mathbf{a}, \mathbf{b}) \mid f(c) = g(c)\} \\ &= \sum_{c \in N} \sum_{i=1}^m \#\{[f, g] \in \text{DS}(\mathbf{a}, \mathbf{b}) \mid f(c) = g(c) = i\} \\ &= \sum_{c \in N} \sum_{i=1}^m \#\{[f] \in \text{DS}(\mathbf{a}) \mid f(c) = i\} \times \#\{[g] \in \text{DS}(\mathbf{b}) \mid g(c) = i\} \end{aligned}$$

$f: N \rightarrow L$ で, $f(c) = i, |f^{-1}(j)| = a_j (\forall j)$ を満たすものの個数は

$$\frac{(n-1)!}{(a_i-1)! \prod_{j \neq i} a_j!} = \frac{a_i}{n} |DS(\mathbf{a})|$$

なので, 結局

$$\# = \sum_{c \in N} \sum_{i=1}^m \frac{a_i b_i}{n^2} |DS(\mathbf{a}, \mathbf{b})| = \frac{1}{|DS(\mathbf{a}, \mathbf{b})|} \sum_{i=1}^m a_i b_i$$

を得る.

一般の k については, N の代わりに, 相異なる k 個の元の組の集合 N_k を使えば, $k=1$ の場合に帰着される.

3 群論からのアプローチ

対称群との関係を少し述べておく. 容易に分かるように, 次で定義される対称群 S_n の $DS(\mathbf{a})$ 上の作用は可移である.

$$DS(\mathbf{a}) \times S_n \rightarrow DS(\mathbf{a}); ([f], \pi) \mapsto [f \circ \pi]$$

したがって $S_n \times S_n$ は $DS(\mathbf{a}) \times DS(\mathbf{a})$ に可移に作用している.

$[f_0, g_0] \in DS(\mathbf{a}, \mathbf{b}) := DS(\mathbf{a}) \times DS(\mathbf{b})$ を適当に取っておく (例えば 2 次元観測データ). このとき写像

$$\begin{aligned} S_n \times S_n &\rightarrow DS(\mathbf{a}, \mathbf{b}) \rightarrow \text{TAB} \\ (\sigma, \tau) &\mapsto [f_0 \circ \sigma, g_0 \circ \tau] \mapsto \text{tab}[f_0 \circ \sigma, g_0 \circ \tau] \end{aligned} \quad (12)$$

を得る. 容易に分かるように $\text{tab}[f_0 \circ \sigma, g_0 \circ \tau] = \text{tab}[f_0, g_0 \circ \tau \sigma^{-1}]$ なので,

$$\text{tab}' : S_n \rightarrow \text{TAB}(\mathbf{a}, \mathbf{b}); \tau \mapsto \text{tab}[f_0, g_0 \circ \tau] \quad (13)$$

も全射で, 対称群 S_n に一様確率分布を与えておくと, この全射による商確率分布はまさに多項超幾何分布 $H(\mathbf{x})$ になる. とくに一様分布に収束するような対称群上のランダムサンプリングは, 上の全射によって, 多項超幾何分布 $H(\mathbf{x})$ にしたがう $\text{TAB}(\mathbf{a}, \mathbf{b})$ 上のランダムサンプリングに収束する.

現代 (コンピュータによる大量データ処理の時代) の統計学では, 与えられた周辺度数 \mathbf{a}, \mathbf{b} を持つ分轄表の大量生成が必要になる. 群論的には

この問題は、対称群の元の大量発生と同じである。対称群の場合、互換をランダムに取って次々と掛けて対称群の元を作るといような自然なマルコフ鎖がある。これに対応する分轄表の上のマルコフ鎖が得られることになる。このマルコフ鎖は、与えられている分轄表に

$$\begin{array}{c|cc} & j & j' \\ \hline i & +1 & -1 \\ i' & -1 & +1 \end{array}$$

を(適当な確率で)加えることに相当する。

ところで n 個のデータを対称群でかき混ぜることは、統計学的には Fisher の並べ替え検定のアイデアである。また対称群上のマルコフ鎖の収束性や収束の速さの評価には対称群の表現論が使われている。もう一つ別の重要なリサンプリング法のひとつにブートストラップ法がある。これはデータをランダムに選んで行くのだが、データの復元抽出であるところが並べ替え検定と違うところである。この場合は、対称群の代わりに対称半群とその表現が現れる。興味深いことに対称半群の既約表現は対称群の既約表現から決まる。これについては別の機会に述べたい。

4 分轄表の一致率検定への応用

$M \times M$ 型の正方分割表 $\mathbf{x} = (x_{jk}) \in DS(a) \times DS(b)$ の一致率検定とは、対角和 $\text{Tr}(\mathbf{x})$ が期待値よりはずれているかどうかを見るための検定である。Cohen のカッパ検定法がよく知られている。 $0 \leq r \leq n$ に対し、

$$p(r) := \text{Prob}(\text{Tr}(\mathbf{x}) = r) = \sum_{\text{Tr}(\mathbf{x})=r} H(\mathbf{x})$$

$$P(r) := \text{Prob}(\text{Tr}(\mathbf{x}) \geq r) = \sum_{k \geq r} p(k) = \sum_{\text{Tr}(\mathbf{x}) \geq r} H(\mathbf{x})$$

と置く。Fisher の正確確率法の考えでは、分割表 \mathbf{x} をすべて列挙し、それらの $H(\mathbf{x})$ を足し合わせることによって、確率 $p(r)$ や上側確率 $P(r)$ を求める。一般に正確確率法は、分割表のサイズ m が大きいとすぐ計算の限界に達する。しかしこの講演で示した超幾何級数の積公式を使えば、ある程度のサイズまで可能である。計算量は $O(m)$ 程度。ただし超多倍長 ($n!$ 程度) の整数係数を持つたかだか n 次の多項式計算が必要である。必要なメモリサイズは $O(n^2 \log n)$ 。

前と同じように,

$$F_{a,b}(z) = \sum_{k \geq 0} \binom{a}{k} \binom{b}{k} k! z^k$$

と置く. 積公式により, 問題の確率 $\{p(r)\}_{r=0,1,\dots,n}$ は次の等式を満たす:

$$\sum_{r \geq 0} p(r) F_{n,r}(z) = \prod_{i=1}^m F_{a_i, b_i}(z) =: F(z) \quad (14)$$

ここで, 多項式 $F(z)$ の次数は $\sum_i \min(a_i, b_i) \leq n$ である.

定理. $F(z) = \sum_{k \geq 0} \binom{n}{k} k! q(k) z^k$ と展開する. このとき

$$\begin{aligned} \sum_{r=0}^n p(r) z^r &= \sum_{r=0}^n q(r) (z-1)^r \\ \sum_{r=0}^n P(r) z^r &= 1 + z \sum_{r=1}^n q(r) (z-1)^{r-1} \end{aligned}$$

したがって, 超多倍長整数係数の多項式計算が出来るソフト (Asir/Risa でなくとも Maple, Mathematica 程度でも) を使えば上側確率 $P(x_0)$ の正確な値の計算が可能となる.

比較言語学からの計算例をあげておこう. これは基礎 200 語による上古 (奈良時代) 日本語 (J) と中期 (15 世紀李氏朝鮮時代) 朝鮮語 (K) との語頭音一致数の検定である. 音韻対応表は次で与えられる.

J \ K	k	m	n	p	r	t	w	y	-	
k	9	6	6	9	3	11	0	0	4	48
m	7	4	1	4	2	5	0	1	1	25
n	3	4	3	3	1	2	0	0	1	17
p	6	3	7	10	0	6	0	0	1	33
r	0	0	0	0	0	2	0	0	0	2
t	4	5	8	11	1	27	0	1	0	57
w	1	0	3	2	1	3	0	0	0	10
y	1	1	2	2	0	1	0	0	1	8
-	0	0	0	0	0	0	0	0	0	0
	31	23	30	41	8	57	0	2	8	200

これより一致数は対角和 $x_0 = 53$ で与えられる。この一致数が偶然得られる上側確率の正確な値 $P_{\text{ex}}(53)$ は次のようになる。

$$\frac{971072955976527370489065992048363534695258683180916330016972}{623729162842170272509552467370904366650977071823270606663} \\ \frac{621808756731104460234413202960802888298370454841707272110637}{520765525658472228904396826948279002883680647387345546300000}$$

分母は 120 桁、分子は 117 桁である。

なお(正規分布による)Cohen のカッパ検定では、 $P_n(53) = 0.0005086$ であり、(二項分布による)二項検定では $P_b(53) = 0.00238$ である。

$$P_n(53) = 0.0005086 < P_{\text{ex}}(53) = 0.00156169 < P_b(53) = 0.00238.$$

カッパ検定の有意確率は、正確な確率のほぼ $1/3$ であり、日本語と朝鮮語の近さを過大評価している。つまり、無関係な二言語を関係ありと判断する(第一種の過誤)の可能性が強くなる。反対に二項検定は第一種の過誤の可能性は少なくなるが、反対に二言語が関係を持つのに、関係なしと判断する(第二種の過誤)の可能性が強くなる。

これら三種類の検定方式での有意確率の大小関係はさまざまで、上の不等式の向きが逆になることもある。いずれにせよ、安全かつ計算が楽なのは二項検定である。正確確率法はもっとも信頼できるが、計算量が膨大という欠点を持つ。

5 一般化など

(A) 未解決問題.

いろいろな「一致数」が統計の応用分野に現れている。これまで見てきたところでは、何らかの「一致数」のモメント公式があれば、それから何らかの「超幾何多項式」の積公式が得られる、という仕組みになっている。残念ながらほとんど何の結果もないが、若干のコメントを追加しておきたい。

(1) 3次元以上の分割表とその一致数。これについても、同様の結論が成り立つ。例えば、 ${}_3F_0$ 型超幾何多項式の積公式がある。また、3次元立方分割表の一致数検定への応用がある。ただし、考える分割表 (x_{ijk}) は1次元周辺和 $x_{i++}, x_{+j+}, x_{++k}$ を固定したものだけを考える。2次元周辺和

$x_{+jk}, x_{i+k}, x_{ij+}$ を固定した分割表については難しい。ただこれこそが現代の代数統計の分野でもっともやりたいことである。

(2) q アナログ. 超幾何分布 \sim 超幾何関数 $\sim q$ アナログ, と来ると, 超幾何分布の q アナログを考えたい。例えば, 次のような 2times2 型分割表 $x = (x_{ij})$:

	1	2	計
1	$x (= x_{11})$	$a - x$	a
2	$b - x$	$n - a - b + x$	$n - a$
計	b	$n - b$	n

は $x_{11} = x$ を決めれば他の成分はすべて決まる。生起確率は超幾何分布

$$H(x) = \frac{a!b!(n-a)!(n-b)!}{n!x!(a-x)!(b-x)!(n-a-b+x)!}$$

である。これの q アナログは,

$$H_q(x) = \frac{(q)_a(q)_b(q)_{n-a}(q)_{n-b}}{(q)_n(q)_x(q)_{a-x}(q)_{b-x}(q)_{n-a-b+x}} q^{x(a+b-n+x)}$$

と考えられる。ここで $(q)_k = (1-q)(1-q^2)\cdots(1-q^k)$ である。

これについても ${}_3\phi_0$ 型基本超幾何関数の積公式がある。ただ, $H_q(x)$ が確率や統計に現れるかどうかは知らない。

(3) 重み付き一致数 $x_w[f, g] = \sum_{ij} w_{ij} |f^{-1}(i) \cap g^{-1}(j)|$. 重み付きカップ係数は Cohen らによって研究されてきたが, 高次のモーメント公式はあると思う。どのような超幾何多項式がそれに関係しているかや, 積公式があるかも分からない。

(4) ふたつの写像の族同士の一致数. $N = \{1, 2, \dots, n\}$ から M への写像の族 $\{f_\alpha\}$ と $\{g_\beta\}$ 同士の一致数

$$x_0 = \sum_{\alpha, \beta} x_0[f_\alpha, g_\beta]$$

については平均と分散の公式は得られている。高次モーメント公式, 関連する超幾何多項式の積公式は不明。次の一致数は実用上研究の価値がある:

$$x_0 := \#\{c \in N \mid \exists \alpha, \beta; f_\alpha(c) = g_\beta(c)\}$$

ヨを \forall にしたものも価値がある。しかしこれらについては平均さえ簡単な公式が内容である。

(5) 系統樹とは、葉にラベル $(1, 2, \dots, n)$ の付いた根つき二分木をいう。このとき対称群 S_{2n} がそのような系統樹の集合 T_n に可移に作用している。したがって、系統樹の何かの不変量 $T_n \rightarrow \mathbb{N}_0$ (正方分割表の対角和に相当) についても、モメント公式や超幾何多項式もどきの積公式があるかもしれない。

(B) 将来性.

(高次元) 分割表の検定はもっともよく使われている統計的手法である。現代の統計学では、そのために余次元1の周辺和を固定した分割表を大量に(百万単位で)生成する必要がある。そのための手法として、マルコフ鎖モンテカルロ法(MCMC法)が発展してきた。最近では、グレブナー基底を用いて、分割表のマルコフ鎖を作ることが活発に研究されている。

ここで述べた一致数検定法は、対称群の元のランダムサンプリングから2次元分割表のランダムサンプリングが出来ることを意味している。フィッシャーの並べ替え検定と正確確率法両方の流れを組む方法である。この方法の利点は、対称群の理論(古典的な指標理論、ヘッケ環の理論など)を使えることである。それによれば、現在使われている2次元分割表の生成法(Diaconisなど)は、対称群の言葉では、ランダムに互換を取って次々に乗じて行くことで対称群の元、したがって分割表の生成を行う。指標理論によれば、この収束性はきわめて悪い。もっとも収束が早いのは、互換の代わりに長さ $n-1$ のサイクルを乗じて行くことである(n はサンプルサイズ)。「計算代数統計」という新しい分野に、有限群の表現論が応用される日も近い。そのときのために、若い人には、分割表の検定とグレブナー基底の勉強をしておいて欲しい。

参考論文

[1] P.Diaconis, S.P.Holmes, Random walks on trees and matchings, *Electric J. of Probability*, 7(2002), no 6, 1-17.

[2] P.Diaconis, "Group Representations in Probability and Statistics," *Inst. Math. Stat.*, 1988.

[3] 日比孝之編 「グレブナー基底の現在」 数学書房 2006.

ユークリッド空間のデザインについて

坂内悦子 (Etsuko Bannai)

九大・数理

(Faculty of Mathematics, Graduate School
Kyushu University)

1 はじめに

ユークリッド空間のデザインの概念は Neumaier - Seidel ([12]) によって球デザインの拡張として 1988 年に定義された. Delsarte-Seidel ([8]) により $2e$ -デザインの場合及び antipodal な場合の $(2e+1)$ -デザインに含まれる点の個数の下界が与えられ, tight なデザインの定義が与えられた. 当初は tight なものはほとんど存在しないのではないかと考えられていたが, その後の Bajnok, 坂内-坂内, 坂内悦子 等の研究により面白い, 重要な例がいくつか構成され, 部分的な分類についての結果が得られている ([1, 2, 5, 6, 3, 4]). その後平尾 将剛, 澤 正憲などとの交流の中でユークリッド空間の $(2e+1)$ -デザインの自然な下界が Möller によりすでに 1976 年により一般的な形で与えられていた事を教えてもらった ([10, 11]). この講演では Möller の与えた下界を用いて, ユークリッド空間の tight なデザインの定義を与え直し, tight な 7-デザイン 9-デザインの分類問題について特にデザインをサポートする球面の個数が 2 個の場合について最近得られた結果を紹介する.

デザインが tight であると言う性質は, 球面上のデザインの場合と同様に, 自然な意味で究極な性質であり, 存在する事は稀である. そして, 存在が確かめられたものは色々な良い性質を満たしている. また, 一般にデザインについての存在定理は知られているが具体的に構成しようとするとそう簡単ではない. この講演の後半では, Hamming scheme $H(d, q)$ を使ったユークリッド空間の 4-デザインの構成について解説を与えた.

この研究は坂内英一との共同研究である.

2 基本的な定義と Möller の結果

ユークリッド空間 \mathbb{R}^n の単位球面を $S^{n-1} = \{\mathbf{x} \in \mathbb{R}^n \mid \|\mathbf{x}\| = 1\}$ とする. \mathbb{R}^n の有限部分集合を X とする. この報告の中で用いる記号を次に与えておく.

$\{\|\mathbf{x}\| \mid \mathbf{x} \in X\} = \{r_1, \dots, r_p\}$ とし各 i ($1 \leq i \leq p$) に対して $S_i = \{\mathbf{x} \in \mathbb{R}^n \mid \|\mathbf{x}\| = r_i\}$, $X_i = S_i \cap X$ とする. この時 X は $S = \cup_{i=1}^p S_i$ でサポートされているとか p 個の同心球面でサポートされているなどと表現する. σ_i, σ_i ($1 \leq i \leq p$) は S^{n-1} および S_i の Haar 測度とし $|S^{n-1}| = \int_{S^{n-1}} d\sigma(\mathbf{x})$, $|S_i| = \int_{S_i} d\sigma_i(\mathbf{x}) = r_i^{n-1}|S^{n-1}|$ が成り立っているとす.

$r_i = 0$ の場合は $\frac{1}{|S_i|} \int_{S_i} f(\mathbf{x}) d\sigma_i(\mathbf{x}) = f(0)$ と定義する. X 上には正の weight function $w: X \rightarrow \mathbb{R}_{>0}$ が定義されているとする. さらに次の記号を用いる. $\mathcal{P}(\mathbb{R}^n) = \mathbb{R}[x_1, \dots, x_n]$ を n 変数の多項式が作る実係数ベクトル空間. $\text{Hom}_i(\mathbb{R}^n)$ を次数 i の斉次多項式の作る部分空間. $\mathcal{P}_i(\mathbb{R}^n) = \bigoplus_{i=0}^i \text{Hom}_i(\mathbb{R}^n)$, $\mathcal{P}_i^*(\mathbb{R}^n) = \bigoplus_{\substack{i \equiv t \pmod{2} \\ 0 \leq t \leq i}} \text{Hom}_t(\mathbb{R}^n)$. $\mathcal{P}(S)$, $\mathcal{P}_i(S)$, $\mathcal{P}_i^*(S)$ 等はは多項式の定義域を S に制限した時に得られるベクトル空間連とする.

定義 2.1 (Neumaier-Seidel, 1988 [12]) \mathbb{R}^n の有限部分集合と正の weight function w の組 (X, w) は自然数 t について次の条件が成り立つ時にユークリッド空間の t -デザインと呼ばれる.

$$\sum_{i=1}^p \frac{w(X_i)}{|S_i|} \int_{S_i} f(\mathbf{x}) d\sigma_i(\mathbf{x}) = \sum_{\mathbf{x} \in X} w(\mathbf{x}) f(\mathbf{x})$$

が全ての $f \in \mathcal{P}_t(\mathbb{R}^n)$ に対して成り立つ. ここで, $w(X_i) = \sum_{\mathbf{x} \in X_i} w(\mathbf{x})$ である.

Neumaier-Seidel の論文においてはユークリッド空間のデザインは原点 0 を含まない形で定義が与えられていたが, 論文 [3] では原点を含めた定義を与えている. ユークリッド空間のデザインとして, さらには解析学の研究者達が考える cubature formula との関連に於いても原点を含めて考える方が自然であろう.

Möller が cubature formula に関してもっと一般的な形で証明した定理をユークリッド空間の t -デザインについて応用すると次の定理が得られる.

定理 2.2 (Möller, 1976 [10] ([11] も参照))

(i) ユークリッド空間の $2e$ -デザイン X に対して次の不等式が成り立つ.

$$|X| \geq \dim(\mathcal{P}_e(S)).$$

(ii) ユークリッド空間の $(2e+1)$ -デザイン X に対して次の不等式が成り立つ.

(n) e が奇数の時, または, e が偶数で $0 \notin X$ の時

$$|X| \geq 2 \dim(\mathcal{P}_e^*(S)).$$

(b) e が偶数で $0 \in X$ の時

$$|X| \geq 2 \dim(\mathcal{P}_e^*(S)) - 1.$$

注意 1 ユークリッド空間の $2e$ -デザイン X の点の個数の下界については [8] にも独立に与えられている. ユークリッド空間の $(2e+1)$ -デザインの下限については *antipodal* かつ $w(-x) = w(x)$ を満たすという条件をつけて [8, 5] で下界が与えられている (すなわち X^* を $X = X^* \cup (-X^*)$, $X^* \cap (-X^*) = \{0\}$ 又は \emptyset で定義すると $|X^*| \geq \dim(\mathcal{P}_e^*(S))$ が成り立つ). 組合せ論の研究者達は最近まで Möller の結果に気が付かずに行った.

Möller はさらに次の結果を得ている (実際はもっと一般的な形で述べている).

定理 2.3 (Möller, [10, 11]) X をユークリッド空間の $(2e + 1)$ - デザインとし定理 2.2 (ii) の不等式の等号が成立していると仮定する. この時さらに, e が奇数であるか, または偶数で $0 \in X$ を満たしていれば X は *antipodal* であり *weight* 関数 w は原点に関して対称である, すなわち, $w(-x) = w(x)$ が成り立つ.

Möller は e が偶数で $0 \notin X$ を満たしている場合については何も述べていなかったが Möller の手法を用いるとつぎの定理が得られる.

定理 2.4 定理 X をユークリッド空間の $(2e + 1)$ - デザインとし定理 2.2 (ii) の不等式の等号が成立していると仮定する. さらに e が偶数, $0 \notin X$ とする. この時 $p \leq \frac{e}{2} + 1$ であれば X は *antipodal* であり *weight* 関数 w は原点に関して対称である.

tight 性の定義

球面上のデザインと同様にユークリッド空間のデザインについても tight 性を定義したかったのであるが, これまで l が奇数の場合にユークリッド空間の l - デザインの自然な下界の証明を知らなかった事により条件付きの定義しかできなかった. 上述の Möller の結果を踏まえて下記の様に定義する.

定義 2.5 (tight デザイン)

定理 2.2 の不等号において等号が成り立つ時に X を p 個の同心球面 S 上の *tight* な $2e$ - または $(2e + 1)$ - デザインと呼ぶ. さらに $\dim(\mathcal{P}_e(S)) = \dim(\mathcal{P}_e(\mathbb{R}^n))$ が成り立つならば X をユークリッド空間の *tight* な $2e$ - または $(2e + 1)$ - デザインと呼ぶ.

注意 2 定理 2.4 より, e が奇数の場合 p 個の同心球面 S 上の *tight* な $(2e + 1)$ - デザインは原点を含まないことがわかる.

注意 3 p 個の同心球面上での *tight* $2e$ - または $(2e + 1)$ - デザインの定義は明確であるが, ユークリッド空間の $2e$ - または $(2e + 1)$ - デザインとして *tight* であると言う事を定義する時に, デザイン X をサポートする同心球面の和集合 S に対して S がユークリッド空間を代表していると言うニュアンスを与えたいと考えた. その意味で $\dim(\mathcal{P}_e(S)) = \dim(\mathcal{P}_e(\mathbb{R}^n))$ と言う条件を付けたのである. 是等の等式を満たす球面の個数の最小値はどうなっているかを調べてみる. まず, S が原点を含む時に $\varepsilon_S = 1$, 含まない時に $\varepsilon_S = 0$ と定めておく. $\dim(\mathcal{P}_e(S)) = \dim(\mathcal{P}_e(\mathbb{R}^n))$ を満たす最小の p の値は $\lceil \frac{e+1}{2} \rceil + 1$ である事がわかる.

定義 2.5 及び定理 2.3, 定理 2.4 から次の定理が得られる.

定理 2.6 (X, w) を p 個の同心球面上の *tight* $(2e + 1)$ - デザインとする. この時次が成り立つ.

- (i) e が奇数であるか, または, e が偶数で $0 \in X$ を満たすならば X は *antipodal* かつ w は原点に関して対称である.
- (ii) e が偶数で $0 \notin X$ かつ, $p \leq \frac{e}{2} + 1$ であれば X は *antipodal* かつ w は原点に関して対称である.

注意 4 一般に p 個の同心球面上の tight な $(2e+1)$ -デザイン X において e が偶数で X が原点を含まない場合は球面の個数が多くなると antipodal になる保証はないのであるが、かといって antipodal でない tight な $(2e+1)$ -デザインの存在も知られていない。これまでに見つかった tight な例においてほとんどの場合が、球面の個数は $\dim(\mathcal{P}_e(S)) = \dim(\mathcal{P}_e(\mathbb{R}^n))$ を満たす最小の p の値にほぼ等しくなっている。

次の補題は [3], [5] で証明されている。

補題 2.7

- (1) X を S 上の tight $2e$ -デザインとすると次の事が成り立つ。
- (i) w は各 X_i ($1 \leq i \leq p$) 上で一定の値をとる。
 - (ii) 各 X_i ($1 \leq i \leq p$) は高々 e -距離集合である。
 - (iii) 特に $p = 2$ かつ $X_i \neq \{0\}$ であれば X_i は球面上の $(2e-2)$ -デザインである。
- (2) X を S 上の tight $(2e+1)$ -デザインとする。さらに X が antipodal かつ $w(x)$ が原点に対して対称であれば次の事が成り立つ。
- (i) w は各 X_i ($1 \leq i \leq p$) 上で一定の値をとる。
 - (ii) 各 X_i^* ($1 \leq i \leq p$) は高々 e -距離集合である。
 - (iii) 各 X_i ($1 \leq i \leq p$) は高々 $(e+1)$ -距離集合である。
 - (iv) 特に $p = 2$ かつ $X_i \neq \{0\}$ であれば X_i は球面上の $(2e-1)$ -デザインである。
- ここで、 X_i^* は $X_i = X_i^* \cup (-X_i^*)$, $X_i^* \cap (-X_i^*) = \{0\}$ または \emptyset を満たす集合である。

補題 2.7 (2) は Möller の定理により一層重要になった。

3 ユークリッド空間の tight 7-デザイン

X をユークリッド空間の tight な 7-デザインとする。定義より $|X| = 2 \dim(\mathcal{P}_3^*(S)) = 2 \dim(\mathcal{P}_3^*(\mathbb{R}^n)) = \frac{1}{3}n(n^2 + 3n + 8)$ 。この場合 $e = 3$ であるので X は antipodal であり原点を含まない。また $\dim(\mathcal{P}_3(S)) = \dim(\mathcal{P}_3(\mathbb{R}^n))$ が成り立っていることより $p \geq 2$ である。

$p = 2$ の場合。

補題 2.7 により X_1, X_2 は球面上の 5-デザインでありかつ高々 4-距離集合である。従って各 X_i は球面上の tight な 5-デザインであるかまたは 5-デザインかつ 4-距離集合のいずれかである。後者の場合は X_i を実射影空間に射影すると Delsarte-Goethals-Seidel [7], Hoggar [9] の実射影空間 $P^{n-1}(\mathbb{R})$ 上のデザインに関する定理を適用することができる。すなわち、 X_i の実射影空間へに射影を X_i^* とすると、 X_i^* は $P^{n-1}(\mathbb{R})$ の 3-デザインであり 2-距離集合である。ここで X_i^* の距離は $A^2(X_i^*) = \{(x \cdot y)^2 \mid x, y \in X_i^*\}$ と定義される。Hoggar の結果により X_i^* は \mathbb{Q} -多項式スキームの構造を持ち、 $A^2(X_i^*)$ の元の逆数が有理整数でなければならないことが証明されている。正の実数 $0 < \alpha, \beta < 1$ が存在して $A(X_1) \subset \{0, \pm\alpha, -1\}$, $A(X_2) \subset \{0, \pm\beta r^2, -r^2\}$ となっている。これらの考察をもとに、論文 [3, 5] で用いた方法を用いることにより二つの球面でサポートされるユークリッド空間の tight 7-デザインは次の 3 つのどれかと同型であることが証明できた。

n	$ X $	$ X_1 $	$ X_2 $	$A(X_1)$	$A(X_2)$	w
2	12	6(tight)	6(tight)	$\pm\frac{1}{2}, -1$	$\pm\frac{1}{2}r^2, -r^2$	$\frac{1}{r}$
4	48	24	24	$0, \pm\frac{1}{2}, -1$	$0, \pm\frac{1}{2}r^2, -r^2$	$\frac{1}{r}$
7	182	56(tight)	126	$\pm\frac{1}{3}, -1$	$0, \pm\frac{1}{2}r^2, -r^2$	$\frac{32}{27r}$

上の表で X_1 上の weight は 1, X_2 上の weight は w である. 上の表で $n = 2$ の場合 X_1 と X_2 は正 6 角形である. $n = 4$ の場合は X_1 と X_2 は互いに相似で \mathbb{R}^4 の kissing 数を与える配置になっている. $n = 7$ の場合は X_1 は球面上の tight 5-デザインである. X_2 は F_7 型のルートで与えられる点集合である. 集合としては知られていたがユークリッド空間の tight 7-デザインとしては初めて認識されたものである.

$p \geq 3$ の場合.

各 X_i は $p = 3$ の場合は, 球面上の 3-デザインであり, $p = 4$ の場合は 1-デザインである. 各 X_i は高々 5-距離集合なのでアソシエーションスキームの構造を持つと言う保証はない. $p \geq 5$ の場合は各 X_i はデザインになっている保証はない. 以上の理由からは是等の場合は今のところ分類はそれほど容易とは思われない.

4 ユークリッド空間の tight 9-デザイン

この場合は $e = 4$ で偶数である. $\dim(\mathcal{P}_1(\mathbb{R}^n)) = \frac{1}{24}n(n+1)(n^2+5n+18)+1$.

$0 \in X$ の場合

$0 \in X$ と仮定すると X がユークリッド空間の tight-9 デザインであるためには $|X| = \frac{1}{12}n(n+1)(n^2+5n+18)+1$, 従って $p = 3$ でなければならない. すなわち $X = \{0\} \cup X_1 \cup X_2$ となっている. $X_1 \cup X_2$ はユークリッド空間の 9-デザインであるから, 問題は半径が正の 2つの同心球面上の tight 9-デザインの分類に同値となる. この時 X_1, X_2 は球面上の 7-デザインでありかつ高々 5-距離集合である. 従って X_i は球面上の tight 7-デザインであるかまたは X_i は 5-距離集合である. 従って X_i は tight 7-デザインでなければ $A(X_1) = \{\pm\alpha_1, \pm\alpha_2, -1\}$, $A(X_2) = \{\pm\beta_1 r^2, \pm\beta_2 r^2, -r^2\}$ となる正の実数 $0 < \alpha_1, \alpha_2, \beta_1, \beta_2 < 1$ が存在する. ここでは詳しく述べないが, $n \geq 3$ であれば α_i および β_i は有理数でなければならないことが証明できる. そのことを使って $n \leq 50$ を満たす全ての n に対して検証したところ $0 \in X$ を満たす tight 9-デザインは \mathbb{R}^2 の時だけ存在することがわかった. すなわち $|X| = 17$, X_1, X_2 は正 8 角形に相似で X_1 上で $w(x) = 1$ とすると X_2 上では $w(x) = \frac{1}{3}$ である. 一般の $n \geq 50$ に対して原点を含む tight 9-デザインの非存在が予想されるが, 証明法はまだ見つかっていない.

$0 \notin X$ の場合

この場合 X がユークリッド空間の tight な 9-デザインであるためには $p \geq 3$ でなければならない. $p \geq 4$ の場合は antipodal である保証はないが, $p = 3$ の場合は各 X_i は antipodal な 5-デザインであり高々 5-距離集合である. $n = 2$ の場合には $|X| = 18$ であり Bajnok ([1]) により与えられた正 6 角形 3 個を組合せたものだけである. 一般の n についても $p = 3$ の場合の分類問題は解ける可能性があると考えている.

5 Hamming scheme $H(d, q)$ から得られるユークリッド空間の 4-デザイン

ユークリッド空間の t -デザインは含まれる点の個数が十分大きければいつでも存在する事が証明されている. 例え tight でなくても t -デザインを具体的に構成することは簡単ではない. Bajnok ([2]) は B_n 型 Weyl 群の軌道を使った構成を試みているが, ここでは Hamming scheme $H(d, q)$ を使ったユークリッド空間の 4-デザインの構成法について解説する.

$F = \{1, 2, \dots, q\}$ とする. Δ を \mathbb{R}^{q-1} の regular simplex とする. $\Delta = \{u_1, \dots, u_q\}$ とおくと各 u_i は単位ベクトルであり異なる二つのベクトル間の内積は $u_i \cdot u_j = -\frac{1}{q-1}$ ($i \neq j$) となっている. 次に $\Delta_k = \{0\} \times \dots \times \{0\} \times \Delta \times \{0\} \times \dots \times \{0\} \subset \mathbb{R}^{q-1} \times \mathbb{R}^{q-1} \times \dots \times \mathbb{R}^{q-1} = \mathbb{R}^{d(q-1)}$ と置く. すなわち Δ_k は regular simplex Δ を $\mathbb{R}^{d(q-1)}$ に埋め込んだものであり異なる二つの Δ_i, Δ_j に含まれるベクトルは互いに直交している. 次に $X_1 = \Delta_1 \cup \Delta_2 \cup \dots \cup \Delta_d$, $X_2 = \{-(u_{i_1}, u_{i_2}, \dots, u_{i_d}) \mid (i_1, i_2, \dots, i_d) \in F^d\}$ と定義すると X_1 は $\mathbb{R}^{d(q-1)}$ の単位球面上にあり X_2 は半径 \sqrt{d} の球面上にある 2-距離集合となっている. さらに X_2 は Hamming scheme $H(d, q)$ の構造を持っている. 従って X_1 と X_2 はそれぞれ球面上の 2-デザインとなっている. $X = X_1 \cup X_2$ とし X 上の weight を $x \in X_1$ に対して $w(x) = 1$, $x \in X_2$ に対して $w(x) = q^{-(d-1)}$ と定義すると (X, w) は $\mathbb{R}^{d(q-1)}$ の 4-デザインとなる.

証明

X は $\mathbb{R}^{d(q-1)}$ の 2-デザインであるから

$$\sum_{x \in X} w(x) \|x\|^{2j} \varphi_l(x) = 0$$

が $2j+l \leq 4, 0 \leq j, 1 \leq l \leq 4$ を満たす任意の j, l に対する l 次の調和多項式 φ_l について成立することを示せば良い. $\mathbb{R}^{d(q-1)}$ の 3 次の調和多項式は $x_1 x_2 x_3, x_1^3 - 3x_1 x_2^2, x_1(x_2^2 - x_3^2)$ およびこれらの添字を対称群 $S_{d(q-1)}$ の元で動かしたもので生成される. また $\mathbb{R}^{d(q-1)}$ の 4 次の調和多項式は $x_1 x_2 x_3 x_4, x_1^3 x_2 - 3x_1 x_2 x_3, x_1 x_2(x_3^2 - x_4^2), x_1^4 - 3x_1^2 x_2^2 + 3x_2^2 x_3^2 - 3x_3^2 x_1^2, (x_1 - x_2^2)(x_3 - x_4^2)$ およびこれらの添字を対称群 $S_{d(q-1)}$ の元で動かしたもので生成される. 従って X の対称性を利用することによって X が $\mathbb{R}^{d(q-1)}$ の 4-デザインであることが初等的な計算で確かめられる.

References

- [1] B. BAJNOK, *On Euclidean designs*, Advances in Geometry 6 (2006), no. 3, 423-438.
- [2] B. BAJNOK, *Orbits of the hyperoctahedral group as Euclidean designs*, J. Algebraic Combin. 25 (2007), no. 4, 375-397.
- [3] EI. BANNAI AND ET. BANNAI, *On Euclidean tight 4-designs*, J. Math. Soc. Japan 58 (2006), 775-804.

- [4] EI. BANNAI, ET. BANNAI AND D. SUPRIANTO, *On the strong non-rigidity of certain tight Euclidean designs*, to appear in European J. Combin.
- [5] ET. BANNAI *On antipodal Euclidean tight $(2c + 1)$ -designs*. J. Algebraic Combin. 24 (2006), no. 4, 391-414.
- [6] ET. BANNAI *New examples of Euclidean tight 4-designs*, preprint.
- [7] P. DELSARTE, J. M. GOETHALS AND J. J. SEIDEL, *Bounds for systems of lines and Jacobi polynomials*. Philips Research Reports 30 (1975).
- [8] P. DELSARTE AND J. J. SEIDEL, *Fisher type inequalities for Euclidean t -designs*, Linear Algebra Appl. 114-115 (1989), 213-230.
- [9] S. G. HOGGAR, *Tight 4- and 5-designs in projective spaces*. Graphs Combin. 5 (1989), no. 1, 87-94.
- [10] H. M. MÖLLER, *Kubaturformeln mit minimaler Knotenzahl*, Numer. Math. 25 (1975/76), no. 2, 185-200.
- [11] H. M. MÖLLER, *Lower bounds for the number of nodes in cubature formulae*, Numerische Integration (Tagung, Math. Forschungsinst., Oberwolfach, 1978), 221-230, Internat. Ser. Numer. Math., 45, Birkhäuser, Basel-Boston, Mass., 1979.
- [12] A. NEUMAIER AND J. J. SEIDEL, *Discrete measures for spherical designs, eutactic stars and lattices*. Nederl. Akad. Wetensch. Proc. Ser. A 91=Indag. Math. 50 (1988), 321-334.

Terwilliger algebras of subsets with minimal width and dual width

Ric Hosoya
International Christian University
E-mail: hrie@nt.icu.ac.jp

1 Introduction

Terwilliger algebras are introduced by Terwilliger to study Q -polynomial distance-regular graphs [13, 14, 15]. Recently Brouwer-Godsil-Koolen-Martin introduced two parameters width and dual width, which are the parameters of a subset in a Q -polynomial distance-regular graph Γ and are expected to play an important role in the study of local structures of Γ [3].

In this paper, we study irreducible modules of the Terwilliger algebra \mathcal{T} with respect to a subset with minimal width and dual width. Here, we use the generalized Terwilliger algebra introduced by Suzuki [9]. This paper consists of two parts:

- (i) On the relation between the irreducible \mathcal{T} -modules of endpoint 0 and tight vectors.
- (ii) On the irreducible \mathcal{T} -modules of Hamming graphs and Doob graphs.

2 Preliminaries

In this section, we give definitions needed for the later discussion. We refer the reader to [1] and [2] for basic terminology and properties of distance-regular graphs.

2.1 Distance-regular graphs

Let $\Gamma = (X, R)$ be a connected graph with distance ∂ . Let D be the diameter of Γ . For $x \in X$, let $\Gamma_i(x) := \{y \in X \mid \partial(x, y) = i\}$. For $x, y \in X$ with $\partial(x, y) = i$, let

$$c_i = |\Gamma_{i-1}(x) \cap \Gamma_1(y)|,$$

$$a_i = |\Gamma_i(x) \cap \Gamma_1(y)|,$$

$$b_i = |\Gamma_{i+1}(x) \cap \Gamma_1(y)|.$$

Γ is called a *distance-regular graph* if c_i, a_i, b_i depend only on i .

Let Γ be a distance-regular graph. Let $A_0, A_1, \dots, A_D \in \text{Mat}_X(\mathbb{C})$ denote distance matrices of Γ , i.e.,

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

Let $\mathcal{M} := \mathbb{C}[A_1] \subset \text{Mat}_X(\mathbb{C})$. \mathcal{M} is called the *Bose-Mesner algebra* of Γ . Let E_0, E_1, \dots, E_D be primitive idempotents of \mathcal{M} . Then it is known that \mathcal{M} has two bases:

$$\mathcal{M} = \text{Span}_{\mathbb{C}}\{A_0, \dots, A_D\} = \text{Span}_{\mathbb{C}}\{E_0, \dots, E_D\}.$$

Let P and Q be the base change matrices, i.e.,

$$(A_0, \dots, A_D) = (E_0, \dots, E_D)P,$$

$$(E_0, \dots, E_D) = \frac{1}{|X|}(A_0, \dots, A_D)Q.$$

The matrices P and Q are called the *first eigenmatrix* and the *second eigenmatrix* of Γ , respectively.

The distance matrix A_i is expressed as a polynomial in A_1 of degree i under the ordinary matrix multiplication. This is called the *P-polynomial property*. Dually, Γ is said to be *Q-polynomial* with ordering E_0, \dots, E_D if E_i is expressed as a polynomial in E_1 of degree i under the Hadamard multiplication.

For the rest of the paper, we assume Γ is *Q-polynomial* with ordering E_0, \dots, E_D .

2.2 Terwilliger algebras with respect to subsets

Let C be a proper subset of X . For $y \in X$, let

$$\partial(y, C) := \min\{\partial(y, z) \mid z \in C\}$$

and

$$\Gamma_i(C) := \{y \in X \mid \partial(y, C) = i\}.$$

For $y \in X$ with $\partial(y, C) = i$, let

$$\gamma_i = |\Gamma_{i-1}(C) \cap \Gamma_1(y)|,$$

$$\alpha_i = |\Gamma_i(C) \cap \Gamma_1(y)|,$$

$$\beta_i = |\Gamma_{i+1}(C) \cap \Gamma_1(y)|.$$

A subset C is called a *completely regular code* if $\gamma_i, \alpha_i, \beta_i$ depend only on i .

Let $E_i^* \in \text{Mat}_X(\mathbb{C})$ be the projection matrix from X to $\Gamma_i(C)$, i.e.,

$$(E_i^*)_{xx} = \begin{cases} 1 & \text{if } x \in \Gamma_i(C) \\ 0 & \text{otherwise.} \end{cases}$$

Let $T = T(C) := \mathbb{C}[A_1, E_0^*, \dots, E_D^*]$. T is called the *Terwilliger algebra of Γ with respect to C* . This definition is introduced by Suzuki [9]. If we set $C = \{x\}$ for a vertex $x \in X$, $T(C)$ coincides with the ordinary Terwilliger algebra $T(x)$. T is a non-commutative, semisimple algebra.

Let $V = \mathbb{C}^X$ be the standard module and $\langle u, v \rangle := u^T v$ for $u, v \in V$. Since V is semisimple, V is expressed as a sum of the irreducible T -modules. Let W be an irreducible T -module. Let $r := \min\{i \mid E_i^* W \neq 0\}$ be the *endpoint* of W . and $d := |\{i \mid E_i^* W \neq 0\}| - 1$ be the *diameter* of W . Then we have

$$W = E_r^* W + \dots + E_{r+d}^* W. \quad (\text{orthogonal direct sum})$$

W is called *thin* if $\dim E_i^* W \leq 1$ for all i .

A graph Γ with thin modules has nice combinatorial properties. Let $T\chi$ be the *primary module* of T , where χ is the characteristic vector of C . The following theorem connects the primary module and a completely regular code.

Theorem 1 (Suzuki [9]) *The primary module is thin if and only if C is a completely regular code.*

2.3 Width and dual width

Let $C \subset X$ and χ the characteristic vector of C , i.e., the vector whose x th coordinate is 1 if $x \in C$ and 0 otherwise.

The *width* of C is defined as follows:

$$w := \max\{i \mid \chi^T A_i \chi \neq 0\},$$

i.e., the maximal distance between two vertices in C . Dually, the *dual width* of C is defined as follows:

$$w^* := \max\{i \mid \chi^T E_i \chi \neq 0\}.$$

Theorem 2 (Brouwer-Godsil-Koolen-Martin [3]) *We have $w + w^* \geq D$. If $w + w^* = D$, C is a completely regular code and induces a Q -polynomial scheme. Moreover if the induced scheme is primitive, it is P -polynomial as well.*

Remarks. When $w + w^* = D$ holds, w and w^* take the minimal values respectively.

Remarks. Recently, Tanaka showed that except for few cases, C with $w + w^* = D$ induces a Q -polynomial distance-regular graph [12].

3 $T(C)$ -modules of endpoint 0 and tight vectors

Let $C \subset X$ and $T = T(C)$. Let W be a thin irreducible T -module of endpoint 0.

Proposition 3 (Suzuki [9]) *There exists $v \in E_0^* V$ such that $W = \mathcal{M}v$.*

By the above proposition, we have $W = \mathcal{M}v = \text{Span}\{E_0 v, \dots, E_D v\}$. Hence

$$\dim W = |\{E_i \mid E_i v \neq 0\}| = D + 1 - |\{E_i \mid E_i v = 0\}|.$$

The dimension of W can be bounded using the following:

Proposition 4 (Suzuki [9])

$$|\{E_i \mid E_i v = 0\}| \leq w, \dots (*)$$

where w is the width of C .

The vector v is called *tight* with respect to C if equality holds in $(*)$. The irreducible $\mathcal{T}(C)$ -modules of endpoint 0 for C with $w + w^* = D$ are characterized by tight vectors as follows.

Proposition 5 (H.-Suzuki [7]) *Suppose C satisfies $w + w^* = D$. Then every endpoint 0 module W is thin, and*

$$W = E_j W + \cdots + E_{j+w^*} W$$

for some $0 \leq j \leq w$. Moreover, let $W = \mathcal{M}v$ for $v \in E_0^* W$. Then v is tight and $E_i v = 0$ if $i < j$ or $j + w^* < i$.

We can interpret the above proposition in terms of the eigenmatrices:

Theorem 6 (H.-Suzuki [7]) *Suppose C satisfies $w + w^* = D$. Let \tilde{P} be the first eigenmatrix of the induced scheme of C . Then*

$$\sum_{i=0}^w \tilde{P}_{ji} Q_{ii} = 0 \text{ if } i < j \text{ or } j + w^* < i.$$

Solving the above system of equations, where \tilde{P} is unknown and Q is given, the parameters of C are determined by parameters of Γ and w (or w^*). See also [12].

On the classification of subsets with $w + w^* = D$, there are a lot of examples by Brouwer et.al. [3] and by Tanaka [11] [12]. Our next project is to investigate the irreducible $\mathcal{T}(C)$ -modules of endpoint $\tau > 0$ for these examples.

4 Irreducible $\mathcal{T}(C)$ -modules of Hamming graphs and Doob graphs

We will determine every irreducible $\mathcal{T}(C)$ -modules, other than endpoint 0, where C is a subset with $w + w^* = D$ in a Hamming graph or a Doob graph.

4.1 Subsets with $w + w^* = D$ in Hamming graphs

Let $\Gamma = H(D, q)$ be the Hamming graph, i.e., the direct product of D copies of complete graphs K_q on q vertices:

$$\Gamma = \Gamma^1 \times \cdots \times \Gamma^D,$$

where $\Gamma^i = K_q$. See [2] for the definition of the direct product of graphs.

Theorem 7 (Brouwer et.al. [3]) *Suppose $C \subset \Gamma$ satisfies $w + w^* = D$. Then $C = C^1 \times \cdots \times C^D$ where $C^i = K_q$ or $|C^i| = 1$, i.e., the induced subgraph on C is isomorphic to $H(w, D)$.*

For example, the subset

$$\{(x_1, \dots, x_w, 1, \dots, 1) \in \Gamma \mid x_i \in K_q = \{1, \dots, q\}\}$$

satisfies $w + w^* = D$.

Note that the coset graph $\tilde{\Gamma} = \Gamma/C$ is isomorphic to $H(w^*, q)$. Later we will show irreducible $\mathcal{T}(C)$ -modules of Γ can be obtained from irreducible modules of ordinary Terwilliger algebra $\tilde{\mathcal{T}}$ of $\tilde{\Gamma}$. Go determined irreducible $\tilde{\mathcal{T}}$ -modules for binary Hamming graphs [5]. Following Tanabe's method on Doob graphs [10], we can determine irreducible $\tilde{\mathcal{T}}$ -modules for Hamming graphs in general. By using these results, we can determine irreducible $\mathcal{T}(C)$ -modules.

4.2 Subsets with $w + w^* = D$ in Doob graphs

Let Γ be the Doob graph, i.e., the direct product

$$\Gamma = \Gamma^1 \times \dots \times \Gamma^{D_1+D_2},$$

where Γ^i ($1 \leq i \leq D_1$) is the Shrikhande graph and Γ^i ($D_1 + 1 \leq i \leq D_1 + D_2$) is K_4 .

Theorem 8 (Tanaka [12]) *Suppose $C \subset \Gamma$ satisfies $w + w^* = D$. Then $C = C^1 \times \dots \times C^{D_1+D_2}$ where $C^i = \Gamma^i$ or $|C^i| = 1$.*

The coset graph Γ/C is isomorphic to a Doob graph and similar property as Hamming graphs holds.

4.3 The quotient graph of a completely regular partition

As we have mentioned, Terwilliger algebras of Γ and the coset graph $\tilde{\Gamma}$ are related to each other. In fact, if we consider the quotient graph of a special partition, we do not necessarily assume the group action, we obtain some relations between Terwilliger algebras of Γ and the quotient graph.

In general, a partition $\Pi = \{C_1, \dots, C_n\}$ of a distance-regular graph Γ is called a *completely regular partition* if Π is an equitable partition of X where each C_i is completely regular with same parameters. The *quotient graph* Γ/Π has vertex set Π and for $C_i, C_j \in \Pi$, C_i is adjacent to C_j if $C_i \neq C_j$ and there exists an edge joining a vertex in C_i to a vertex in C_j .

Theorem 9 (BCN: Thm 11.1.6 [2]) *Γ/Π is distance-regular if and only if Π is a completely regular partition.*

Suppose Π is a completely regular partition. Let $\tilde{\Gamma} = \Gamma/\Pi$. Fix $C \in \Pi$. Note that C is a subset in Γ while it is a vertex in $\tilde{\Gamma}$. Let $\mathcal{T} = \mathcal{T}(C)$ be the Terwilliger algebra of Γ with respect to a subset C , and $\tilde{\mathcal{T}} = \tilde{\mathcal{T}}(C)$ the Terwilliger algebra of $\tilde{\Gamma}$ with respect to a vertex C .

Let K be the $|X| \times |\Pi|$ -matrix defined as

$$(K)_{xC_i} = \begin{cases} 1 & \text{if } x \in C_i \\ 0 & \text{otherwise} \end{cases}$$

The matrix K connects two algebras \mathcal{T} and $\tilde{\mathcal{T}}$ as follows.

Lemma 10 (c.f. BCN: Thm 11.1.6 [2]) $\mathcal{T}K = K\tilde{\mathcal{T}}$.

Proposition 11 (H. [6], Martin-Taylor [8]) *Let W be an irreducible \mathcal{T} -module. Then $W = KU$ for some irreducible $\tilde{\mathcal{T}}$ -module U , or $K^T W = 0$.*

We would like to determine W with $K^T W = 0$. We can determine them when Γ is a Hamming graph or a Doob graph.

4.4 Irreducible modules of a Hamming graph and a Doob graph

Let Γ be a Hamming graph or a Doob graph. Let C be a subset with $w+w^* = D$. Let $\bar{\Gamma}$ be the coset graph Γ/C and $\hat{\Gamma}$ be the induced subgraph on C . Then $\Gamma \cong \bar{\Gamma} \times \hat{\Gamma}$. Let v_0, \dots, v_w be eigenvectors of $\bar{\Gamma}$ for distinct eigenvalues where $v_0 = \chi$, i.e., the characteristic vector of C . Let $K_i = v_i \otimes I$ where I denotes the identity matrix of size $|\hat{\Gamma}|$. Obviously, $K = K_0$.

Theorem 12 (H. [6]) *Let W be an irreducible T -module of Γ . Then $W = K_i U$ for some irreducible \bar{T} -module U of $\bar{\Gamma}$ and for some $0 \leq i \leq w$.*

4.5 Concluding remarks

- (1) Unlike the case of endpoint 0, for the case of endpoint $\tau > 0$, there exist non-thin irreducible $T(C)$ -modules in a Doob graph.
- (2) Let \bar{V} be the standard module of \bar{T} . Let $\varphi : V \rightarrow \bar{V}$ be the homomorphism defined by $\varphi(\mathbf{u}) = K^T \mathbf{u}$ for $\mathbf{u} \in V$. Proposition 11 implies the exact sequence $0 \rightarrow V \rightarrow \bar{V} \rightarrow 0$ is split.

References

- [1] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin/Cummings, California, 1984.
- [2] A. E. Brouwer, A. M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer Verlag, Berlin, Heidelberg, 1989.
- [3] A. E. Brouwer, C. D. Godsil, J. H. Koolen and W. J. Martin, Width and dual width of subsets in polynomial association schemes, *J. Combin. Th. (A)* 102 (2003), 255-271.
- [4] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Research Reports Supplements* 10 (1973).
- [5] J. T. Go, The Terwilliger algebra of the Hypercube, *Europ. J. Combin.* 23 (2002), 399-430.
- [6] R. Hosoya, On the Terwilliger algebra with respect to a subset with minimal width and dual width, in preparation.
- [7] R. Hosoya and H. Suzuki, Tight distance-regular graphs with respect to subsets, *European J. Combin.* 28 (2007), 61-74.
- [8] W. J. Martin and T. Taylor, On the subconstituent algebra of a completely regular code, preprint.
- [9] H. Suzuki, The Terwilliger algebra associated with a set of vertices in a distance-regular graph, *J. Algebraic Combinatorics* 22 (2005), 5-38.

- [10] K. Tanabe, The irreducible modules of the Terwilliger algebras of Doob Schemes, *J. Alg. Combin.* 6 (1997), 173-195.
- [11] H. Tanaka, Classification of subsets with minimal width and dual width in Grassmann, bilinear forms and dual polar graphs, *J. Combin. Theory (A)* 113 (2006), 903-910.
- [12] H. Tanaka, On subsets with minimal width and dual width in Q -polynomial distance-regular graphs, in preparation.
- [13] P. Terwilliger, The subconstituent algebra of an association schemes, (part I), *J. Alg. Combin.* 1 (1992), 363-388.
- [14] P. Terwilliger, The subconstituent algebra of an association schemes, (part II), *J. Alg. Combin.* 2 (1993), 73-103.
- [15] P. Terwilliger, The subconstituent algebra of an association schemes, (part III), *J. Alg. Combin.* 2 (1993), 177-210.

The Nonexistence of Projective Planes of Order 12 with a Collineation Group of Order 8

秋山 献之 (福岡大学理学部)
(akiyama@sm.fukuoka-u.ac.jp)
末竹 千博 (大分大学工学部)
(suetake@csis.oita-u.ac.jp)

§1 準備

この報告は [1] で書かれた内容の要約である。
扱う集合は有限集合とする。

1.1 定義 (有限射影平面)

$\pi = (\mathcal{P}, \mathcal{L}, I)$: 結合構造

\mathcal{P} の元を点, \mathcal{L} の元を直線という。

$\forall a \in \mathcal{P}, (a) := \{X \in \mathcal{L} \mid aIX\}$

$\forall A \in \mathcal{L}, (A) := \{x \in \mathcal{P} \mid xIA\}$

π が以下の条件を満たすとき, π を (有限) 射影平面という。

(i) $\forall a, b (\neq) \in \mathcal{P}, |(a) \cap (b)| = 1$

(ii) $\forall A, B (\neq) \in \mathcal{L}, |(A) \cap (B)| = 1$

(iii) $\exists a, b, c, d (\neq) \in \mathcal{P}: \forall \{x, y, z\} \subseteq \{a, b, c, d\}, |(x) \cap (y) \cap (z)| = 0$

1.2 注意

• 1.1 定義において, 次が成り立つ。

$|(a)| = |(A)| = (\text{一定}) \geq 3$

$(\forall a \in \mathcal{P}, \forall A \in \mathcal{L})$

この値を $n + 1$ とおき, n を π の位数という。

この場合, $|\mathcal{P}| = |\mathcal{L}| = n^2 + n + 1$ となる。

• 任意の素数べき q に対して, 位数 q の射影平面が存在する。

• 位数が素数べきでない射影平面の存在は知られていない。

1.3 問題

位数が素数べきでない射影平面は存在するか?

1.4 定理 (Bruck and Ryser (1949))

$n \equiv 1 \text{ or } 2 \pmod{4}$

$n = x^2 + y^2$ となる整数解 x, y は存在しない。

このとき

位数 n の射影平面は存在しない。

• Bruck-Ryser の定理で非存在が言える位数 (n)

$n = 6, 14, 21, 22, 30, 33, 38, 42, 46, \dots$

• Bruck-Ryser の定理で非存在がわからない位数 (n)

$n = 10, 12, 15, 18, 20, 24, 26, 28, \dots$

• Lam, Thiel and Swierz(1989)

位数 10 の射影平面は非存在

この講演では位数 12 の射影平面に興味がある。

• これまでの研究

Janko and Trng (1980-1982 12 編 (\leq) の論文)

Horvatic-Baldasari, Kramer and Matulic-Bedenic(1986,1987)

Suetake(2004)

• 得られている結果

G を位数 12 の射影平面の任意の自己同型群とすると, $|G| \equiv 8$ または $|G| \equiv 9$ 前者の場合, G は cyclic または quaternion である。

1.5 定義

$\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ を結合構造とする。

(i) $\forall B \in \mathcal{B}, |B| = k$

(ii) $\mathcal{P} = \mathcal{P}_0 \cup \mathcal{P}_1 \cup \dots \cup \mathcal{P}_{k-1}$ は \mathcal{P} の分割で次の条件を満たす。

$|\mathcal{P}_i| = u \quad (0 \leq \forall i \leq k-1)$

$p, q (\neq) \in \mathcal{P}, P \in \mathcal{P}_i, q \in \mathcal{P}_j$

$(0 \leq i, j \leq k-1)$ とするとき,

$i = j$ ならば p, q を通る block はない。

$i \neq j$ ならば p, q を通る blocks は丁度 λ 個ある。

$(\mathcal{P}_0, \mathcal{P}_1, \dots, \mathcal{P}_{k-1})$ を \mathcal{D} の point classes という。))

(iii) \mathcal{D} の双対構造も (i), (ii) を満たす。 (\mathcal{D} の双対構造の point classes を \mathcal{D} の block classes という。)

このとき,

\mathcal{D} を対称横断デザイン (symmetric transversal design) $\text{STD}_\lambda[k; u]$ という

($k = \lambda u$ が成り立つ。)

次の定理を証明する。

1.6 定理

G を位数 12 の射影平面の任意の自己同型群とすると, $|G| \equiv 4$ または $|G| \equiv 9$ 前者の場合, G は cyclic である。

1.7 補題

位数 8 の自己同型群を持つ位数 12 の射影平面が存在するならば, 点集合とブロック集合の上で半正則に作用する位数 4 の自己同型群を持つ $STD_2[12; 6]$ が存在する

証明 $\pi = (\mathcal{P}, \mathcal{L}, I)$ を位数 12 の射影平面とする。 $G \leq \text{Aut} \pi$, $|G| = 8$ とする。

G は cyclic または quaternion

$\therefore G$ は位数 2 の元を唯一つ持つ。それを φ とする。 φ は elation

φ の center を P_∞ , axis を l_∞ とする。

$P_\infty H_\infty$

$H := \langle \varphi \rangle$

Γ ; $\mathcal{P} - (l_\infty)$ 上の H -orbits の全体

Φ ; $\mathcal{L} - (P_\infty)$ 上の H -orbits の全体

$|\Gamma| = |\Phi| = 72$

$R \in \Gamma, S \in \Phi$

$RP'S \stackrel{\text{def}}{\iff} \exists p \in R, \exists l \in S \text{ s.t. } p \perp l$

とすると, $\mathcal{D} := (\gamma, \Phi, P')$ は $STD_2[12; 6]$ となり, G は Γ と Φ の上で半正則に作用する位数 4 の自己同型群 \tilde{G} を induce する。

次の§で補題 1.7 を満たす $STD_2[12; 6]$ が存在しないことを証明する。

このことを示せば定理が証明される

§2 位数 4 の半正則自己同型群を持つ $STD_2[12; 6]$ の非存在

次の補題は $STD_\lambda[k; u]$ の自己同型群の点とブロック上の作用を決めるのに有効

2.1 補題

$\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$; $STD_\lambda[k; u]$

Ω ; \mathcal{D} の point classes の集合

Δ ; \mathcal{D} の block classes の集合

$G \leq \text{Aut} \mathcal{D}$

t_X ; G の X 上の orbits の個数

($X = \mathcal{P}, \mathcal{B}, \Omega, \Delta$)

このとき

$$t_{\mathcal{P}} + t_{\Delta} = t_{\mathcal{B}} + t_{\Omega}$$

この§では次の定理を証明する。

2.2 定理

任意の $\text{STD}_2[12; 6]$ は点集合とブロック集合の上で半正則に作用する位数 1 の自己同型群を持たない。

証明

(1) $\mathcal{D} = (\mathcal{P}, \mathcal{B})$; $\text{STD}_2[12; 6]$.

$\Omega = \{\mathcal{P}_0, \dots, \mathcal{P}_{11}\}$; \mathcal{D} の point classes

$\Delta = \{\mathcal{B}_0, \dots, \mathcal{B}_{11}\}$; \mathcal{D} の block classes

$\mathcal{P}_0 = \{p_0, \dots, p_5\}, \dots, \mathcal{P}_{11} = \{p_{66}, \dots, p_{71}\}$

$\mathcal{B}_0 = \{B_0, \dots, B_5\}, \dots, \mathcal{B}_{11} = \{B_{66}, \dots, B_{71}\}$

G ; \mathcal{D} の位数 1 の自己同型群. \mathcal{P} と \mathcal{B} 上半正則に作用する。

(2) G は Ω と Δ 上同じ軌道構造を持ち、次のいずれかである。

(補題 2.1 を使う)

(i) サイズ 2:6 個, サイズ 4:0 個.

G は cyclic でない. (平峰, 末竹)

(ii) サイズ 2:4 個, サイズ 4:1 個

(iii) サイズ 2:2 個, サイズ 4:2 個

(iv) サイズ 2:0 個, サイズ 4:3 個

(3) $\mathcal{Q}_0, \dots, \mathcal{Q}_{17}$; G -orbits on \mathcal{P}

$\mathcal{C}_0, \dots, \mathcal{C}_{17}$; G -orbits on \mathcal{B}

$0 \leq i, j \leq 17$ に対して

$q_i := p_r, r = \min\{k | p_k \in \mathcal{Q}_i\}$

$C_j := B_s, s = \min\{l | B_l \in \mathcal{C}_j\}$

$\therefore q_i \in \mathcal{Q}_i, C_j \in \mathcal{C}_j$

$m_{ij} := |\mathcal{Q}_i \cap (C_j)|$

$D_{ij} := \{a \in G | q_i^a \in (C_j)\}$

$m_{ij} = |D_{ij}|$ が成立

$M := (m_{ij})_{0 \leq i, j \leq 17}$.

(4) H : G の subset に対して

$$\widehat{H} := \sum_{h \in H} h \in \mathbf{Z}[G]$$

$$H^{-1} := \{h^{-1} | h \in H\}$$

G は cyclic または elementary abelian なので, (2) より $1 + 3 \times 2 = 7$ 通り (正確には, G の点とブロック上の作用の仕方を考えて 16 通り) の場合を考えればよい

例えば (2) の (ii) が起こり, G が cyclic のとき, φ の \mathcal{P} と B 上の作用を具体的に決めると, $\mathbf{Z}[G]$ 上の次の 5 つの関係式を得る。

(5) (i) もし $i, j(\neq) \in \{k, k+1, k+2\}$ for some $k \in \{0, 3, 6, 9\}$ ならば

$$\sum_{0 \leq j \leq 17} \widehat{D}_{ij} \widehat{D}_{rj}^{-1} = 2\{\widehat{G} - (1 + \varphi^2)\}$$

(ii) もし $i \in \{0, 1, \dots, 11\}$ ならば

$$\sum_{0 \leq j \leq 17} \widehat{D}_{ij} \widehat{D}_{rj}^{-1} = 12 + 2\{\widehat{G} - (1 + \varphi^2)\}$$

(iii) もし $i, j(\neq) \in \{12, 13, \dots, 17\}$ ならば

$$\sum_{0 \leq j \leq 17} \widehat{D}_{ij} \widehat{D}_{rj}^{-1} = 2(\widehat{G} - 1)$$

(iv) もし $i \in \{12, 13, \dots, 17\}$ ならば

$$\sum_{0 \leq j \leq 17} \widehat{D}_{ij} \widehat{D}_{rj}^{-1} = 12 + 2(\widehat{G} - 1)$$

(v) もし $i, j(\neq)$ が (i), (ii), (iii), (iv) をいずれも満たさないならば

$$\sum_{0 \leq j \leq 17} \widehat{D}_{ij} \widehat{D}_{rj}^{-1} = 2\widehat{G}$$

これらの等式に G の自明な指標を作用させて, 次の 5 つの \mathbf{Z} 上の等式を得る

(6) (i) もし $i, j(\neq) \in \{k, k+1, k+2\}$ for some $k \in \{0, 3, 6, 9\}$ ならば

$$\sum_{0 \leq j \leq 17} m_{ij} m_{rj} = 4$$

(ii) もし $i \in \{0, 1, \dots, 11\}$ ならば

$$\sum_{0 \leq j \leq 17} m_{ij}^2 = 16$$

(iii) もし $i, i' (\neq) \in \{12, 13, \dots, 17\}$ ならば

$$\sum_{0 \leq j \leq 17} m_{ij} m_{i'j} = 0$$

(iv) もし $i \in \{12, 13, \dots, 17\}$ ならば

$$\sum_{0 \leq j \leq 17} m_{ij}^2 = 18$$

(v) もし $i, i' (\neq)$ が (i), (ii), (iii), (iv) をいずれも満たさないならば

$$\sum_{0 \leq j \leq 17} m_{ij} m_{i'j} = 8$$

$$(7) \sum_{0 \leq j \leq 17} m_{ij} = 12 \text{ for } 0 \leq i \leq 17$$

は m_{ij} の定義から明らか。

M の最初の 6 行が存在しないことを示す。

$$(8) \sum_{0 \leq i < 2} m_{ij} = \sum_{3 \leq i \leq 5} m_{ij} = 2$$

$$(0 \leq j \leq 17)$$

\therefore (7) と (5)(i)

(9) a_0, a_1, \dots, a_{17} : 非負整数

$$\sum_{0 \leq j \leq 17} a_j = 12, \quad \sum_{0 \leq j \leq 17} a_j^2 = 16$$

このとき、

a_0, a_1, \dots, a_{17} は順序を無視すると、次のように 1 通りに決まる。

$$\underbrace{0, \dots, 0}_8, \underbrace{1, \dots, 1}_8, \underbrace{2, 2}_2$$

(順序を無視してこのような形になる a_0, a_1, \dots, a_{17} を C 型のベクトルと呼ぶことにする)

次がコンピュータを使って示される

(10) $C = (c_{ij})_{0 \leq i \leq 5, 0 \leq j \leq 17}$

C の各行は C 型のベクトル

任意の $0 \leq j \leq 17$ に対して

$$\sum_{0 \leq i \leq 2} c_{ij} = 2, \quad \sum_{3 \leq i \leq 5} c_{ij} = 2$$

$0 \leq r \neq s \leq 5$ に対して

$$\sum_{0 \leq j \leq 17} c_{rj} c_{sj} = \begin{cases} 4 & \text{もし } 0 \leq r \neq s \leq 2 \text{ または } 3 \leq r \neq s \leq 5, \\ 8 & \text{otherwise} \end{cases}$$

このとき

C は存在しない。

(11) 従って、(2)の(ii)で G がcyclicの場合は起こらない。(残りの15通り：似た議論で潰せる。)

なお、 M の最後の6行が起こることを示しておく。この議論は他のcaseを考えるとときに必要。

(12) a_0, a_1, \dots, a_{17} : 非負整数

$$\sum_{0 \leq j \leq 17} a_j = 12, \quad \sum_{0 \leq j \leq 17} a_j^2 = 18$$

このとき、

a_0, a_1, \dots, a_{17} は順序を無視すると、次の2つの場合のいずれかである

$$\underbrace{0, \dots, 0}_8, \underbrace{1, \dots, 1}_9, 3$$

$$\underbrace{0, \dots, 0}_9, \underbrace{1, \dots, 1}_6, \underbrace{2, 2, 2}_3$$

(順序を無視してこのような形になる a_0, a_1, \dots, a_{17} をそれぞれA型、B型のベクトルと呼ぶことにする。)

(13) $k \in \{1, 2, \dots, 6\}$ とする。

$$\Omega_k := \left\{ X = \begin{pmatrix} x_{00} & x_{01} & \cdots & x_{017} \\ \vdots & \vdots & & \vdots \\ x_{k-1,0} & x_{k-1,1} & \cdots & x_{k-1,17} \end{pmatrix} \mid X \text{の各行はA型またはB型} \right\}$$

任意の $0 \leq u \neq v \leq k-1$ に対して

$$\sum_{0 \leq j \leq 17} x_{uj} x_{vj} = 6, \quad \text{任意の } 0 \leq j \leq 17 \text{ に対して } \sum_{0 \leq i \leq k-1} x_{ij} \leq 4$$

$\Omega_k(A) := \{X \in \Omega_k \mid X \text{ の各行は } A \text{ 型}\},$

$\Omega_k(B) := \{X \in \Omega_k \mid X \text{ の各行は } B \text{ 型}\}$

$R, S \in \Omega_k$ (resp. $\Omega_k(A), \Omega_k(B)$) とする。

このとき、

R の行と列を適当に入れ替えると S になるとき、 R は S に同値であるといひ、 $R \sim S$ とかく。(この \sim は、明らかに Ω_k (resp. $\Omega_k(A), \Omega_k(B)$) における同値関係である。)

コンピュータを使って次が示される。

(14) (i) $|\Omega_6(A)/\sim| = 2$

(ii) $|\Omega_6(B)/\sim| = 2623$

(iii) $\Omega_6 = \Omega_6(A) \cup \Omega_6(B)$

(iv) $\Omega_6(A)$ のそれぞれの行列に対して、その行列のすべての行との内積が 8 である A 型、 B 型のベクトルは存在しない。

(v) $\Omega_6(B)$ のそれぞれの行列に対して、その行列のすべての行との内積が 8 である B 型のベクトルは存在しない。

(15) (5) のような $\mathbb{Z}[G]$ 上の等式たちの cases は全部で 16 通りあるが、対応する (6) のような整数条件たちの cases は全部で 4 個に減少する。

References

[1] K. Akiyama, and C. Suetake.

The nonexistence of projective planes of order 12 with a collineation group of order 8, submitted.

[2] Y. Hiramine, and C. Suetake.

A contraction of square transversal designs, to appear.