第27回代数的組合せ論シンポジウム報告集

2010年6月21－23日

於　高知大学総合研究棟

平成22年度文部科学省科学研究費補助金基盤研究（B）

（課題番号　22340002　筑波大　宮本雅彦）

まえがき

この報告集は、平成２２年６月２１日（月）から２３日（水）にわたって、高知大学総合研究棟で行われた「第２７回代数的組合せ論シンポジウム」の講演記録です。研究集会には４９名の参加者がありました。

この報告集の作成は
科学研究費補助金 基盤研究 (B) 課題番号:22340002, 研究代表者 宮本雅彦 (筑波大)
から援助を受けました。また、旅費に関しまして、
科学研究費補助金 基盤研究 (B) 課題番号:19340002, 研究代表者 北詰正顕 (千葉大)
高知大学小駒基金
から援助を受けました。

講演者をはじめ、この集会の開催にご協力いただいた皆様に深く感謝いたします。

平成２２年１０月
大浦　学（高知大学理学部）

第27回代数的組合せ論シンポジウム

下記の要領で研究集会を催しますので、ご案内申し上げます。

世話人：大浦　学（高知大学理学部）

記

日時：平成22年6月21日(月)～23日(水)
場所：高知大学総合研究棟会議室1 (朝倉キャンパス)

6月21日（月）
10:00-10:50 前原濶 (琉球大名誉教授, 東海大), 桑田孝泰（東海大）
Lattice points on conics
11:05-11:55 坂内英一 (九州大名誉教授), 坂内悦子
Several remarks on the concepts of t-designs
14:00-14:50 藤沢潤 (高知大)
Hamiltonicity of 4-connected claw-free graphs
15:00-15:30 奥田隆幸 (東京大)
コンパクト Lie 群上のデザインと符号
15:30-16:00 三枝崎剛 (東北大)
4次直交群の有限部分群から構成される球面デザインについて
16:15-17:05 本間正明 (神奈川大)
Plane curves over finite fields with many points, and Sziklai's conjecture

6月22日（火）
10:00-10:50 中岡宏行 (東京大)
Categorical aspect of the Witt-Burnside construction
11:05-11:35 菅井智 (北海道大)
Abstract Mackey Functors
11:35-12:05 田上真 (東北大)
On the number of points in a lattice polytope
14:00-14:40 谷口浩朗 (香川高専)
On some quotients of dual hyperovals in $PG(d(d+3)/2, 2)$
14:50-15:30 平峰豊 (熊本大)
位数 n^2 の半正則自己同型群をもつ $\mathrm{TD}_2(2n, n)$ について
15:45-16:25 末竹千博 (大分大), 秋山献之 (福岡大), 田中正紀 (崇城大)
Generalized Hadamard matrices over $GF(4)$ and Hadamard matrices
16:35-17:25 Alexander Pott(Ott-von-Guerick-Univ.)
Almost perfect and perfect nonlinear functions: Differences and similarities
18:00- 懇親会 開始時刻が18時に変更されました。

6月23日（水）
10:00-10:50 原田耕一郎 (オハイオ州立大名誉教授)
シン／トンプソンの仕事から
11:05-11:55 宮本雅彦 (筑波大)
フリーボゾン型頂点作用素代数の自己同型による固定点空間の C_1-余有限性

詳しい情報は下記ホームページをご覧ください。
http://www.math.kochi-u.ac.jp/oura/27algcomb/index.html

The 27th Symposium on Algebraic Combinatorics

Dates: June 21(Mon) - June 23(Wed), 2010
Place: Kochi University, Asakura Campus
Organizer: M.Oura(Kochi Univ., email:oura@kochi-u.ac.jp)

June 21, Monday

10:00-10:50 H.Machara(Prof.Emer. at Univ. of the Ryukyus, Tokai Univ.), T.Kuwata(Tokai Univ.)
Lattice points on conics

11:05-11:55 E.Bannai(Prof.Emer. at Kyushu Univ.), E.Bannai
Several remarks on the concepts of t-designs

14:00-14:50 J.Fujisawa(Kochi Univ.)
Hamiltonicity of 4-connected claw-free graphs

15:00-15:30 T.Okuda(Univ. of Tokyo)
Designs and codes on compact Lie groups

15:30-16:00 T.Miezaki(Tohoku Univ.)
Spherical designs obtained from finite subgroups of the orthogonal group of degree 4

16:15-17:05 M.Homma(Kanagawa Univ.)
Plane curves over finite fields with many points, and Sziklai's conjecture

June 22, Tuesday

10:00-10:50 H.Nakaoka(Univ. of Tokyo)
Categorical aspect of the Witt-Burnside construction

11:05-11:35 T.Sugai(Hokkaido Univ.)
Abstract Mackey Functors

11:35-12:05 M.Tagami(Tohoku Univ.)
On the number of points in a lattice polytope

14:00-14:40 H.Taniguchi(Kagawa National College of Tech.)
On some quotients of dual hyperovals in $PG(d(d+3)/2, 2)$

14:50-15:30 Y.Hiramine(Kumamoto Univ.)
On $\mathrm{TD}_2(2n, n)$'s admitting semiregular automorphism groups of order n^2

15:45-16:25 C.Suetake(Oita Univ.), K.Akiyama(Fukuoka Univ.), M.Tanaka(Sojo Univ.)
Generalized Hadamard matrices over GF(4) and Hadamard matrices

16:35-17:25 Alexander Pott (Ott-von-Guerick-Univ.)
Almost perfect and perfect nonlinear functions: Differences and similarities

18:00- Banquet Time changed!

June 23, Wednesday

10:00-10:50 K.Harada(Professor Emeritus at Ohio State Univ.)
From the work of Sin and Thompson

11:05-11:55 M.Miyamoto(Univ. of Tsukuba)
C_1-cofiniteness of the fixed point subVOAs for VOAs of free bozon type

目　次

円錐曲線上の格子点

桑田孝泰 (Kuwata Takayasu) 前原　濶 (Maehara Hiroshi)
東海大学　教育開発研究所

1　はじめに

H. Steinhaus は 1957 年に「どんな整数 $n \geq 0$ についても，ちょうど n 個の格子点を含む円板が存在するか」という問題を提起した．格子点とは整数格子 $\mathbb{Z}^2 \subset \mathbb{R}^2$ の点のことである．この問題は [5] にも収録されている．W. Sierpinski [4] は点 $(\sqrt{2}, 1/3)$ を中心とするどんな半径の円も 2 個以上の格子点を通らないことを示すことによって，どんな $n \geq 0$ についても，ちょうど n 個の格子点を含む円板が存在することを証明した．

平面図形 F に関して，$\mathbb{N} \cup \{\infty\}$ の部分集合

$$\mathcal{S}(F) := \{|\varphi(F) \cap \mathbb{Z}^2| \ : \ \varphi \text{ は } \mathbb{R}^2 \text{ の相似変換で} \varphi(F) \cap \mathbb{Z}^2 \neq \emptyset\}$$

を F の **size-set** と呼ぶことにする．ここで，$|\cdot|$ は集合の要素の個数を表す．例えば，$\mathcal{S}$(円板) $= \mathbb{N}$ である．すると与えられた平面図形の size-set を求める問題は，Steinhaus の問題の一般化となっている．まず，円板に関する結果は次のように拡張できる．

▶ **1.1.** 平面上の任意のコンパクトな凸領域 Γ に対して $\mathcal{S}(\Gamma) = \mathbb{N}$ である．

問題 1. 単純閉曲線で囲まれた領域で，その size-set が $\mathbb{N}$ と異なるものがあるか．

曲線についてはどうだろうか．明らかに $\mathcal{S}$(直線) $= \{1, \infty\}$，$\mathcal{S}$(線分) $= \mathbb{N}$ である．円周についても，Schinzel [3], 前原・松本 [2] により，$\mathcal{S}$(円周) $= \mathbb{N}$ となることがわかっている．

定理 A[3,2]. 素数 p を $p \equiv 1 \pmod 8$ なる素数とすると，任意の $n > 0$ に対して円 $(4x-1)^2 + (4y)^2 = p^{n-1}$ はちょうど n 個の格子点を通る．従って $\mathcal{S}$(円周) $= \mathbb{N}$ である．　□

実は，坂内・三枝崎 [1] により，もっと一般的な次の結果が得られている．2次元格子 Λ は，任意の2つのベクトルの内積が整数となるとき，integral lattice という．

定理 B[1]. 2次元格子 Λ が integral lattice なら，任意の整数 $n \geq 0$ に対して，ちょうど n 個の Λ の点を通る円が存在する． □

では，円以外の円錐曲線の size-set はどうなるだろうか．円錐曲線はある定点からの距離とある直線からの距離の比 e（離心率）が一定となるような点の軌跡である．離心率 e が等しい2つの円錐曲線は互いに相似である．例えば，放物線の離心率は1で，放物線はすべて相似である．

▶ **1.2.** S(放物線) $= \{1, 2, 3, 4, \infty\}$.

楕円 $(x/a)^2 + (y/b)^2 = 1$ $(a > b > 0)$ の離心率は $e = \sqrt{1 - \lambda^2}$ $(\lambda = b/a)$ である．楕円や双曲線では，離心率は軸比 λ（長軸と短軸または主軸と副軸の長さの比）で決まる．例えば，双曲線 $(x/a)^2 - (y/b)^2 = 1$ $(a, b > 0)$ の離心率 e は軸比 $\lambda = b/a$ を用いて $e = \sqrt{1 + \lambda^2}$ と表される．以下，軸比が λ の楕円（と相似な楕円）を E_λ で，軸比が λ の双曲線を H_λ で表す．また，正の実数の集合 $\mathcal{R}$ を次のように定義する．

$$\mathcal{R} = \{|\alpha/\beta| : \alpha, \beta \text{は正則で対称な } 2 \times 2 \text{ 整数行列の固有値 }\}.$$

楕円，双曲線の size-set に関しては，次の表のような結果を得た．

▶ **1.3.** 楕円と双曲線の size-set:

	$\lambda \in \mathbb{Q}$	$\lambda \notin \mathbb{Q}$ $\lambda^2 \in \mathbb{Q}$	$\lambda^2 \in \mathcal{R} \setminus \mathbb{Q}$	$\lambda^2 \notin \mathcal{R}$
$S(E_\lambda)$	$\mathbb{N}$	$\mathbb{N}$	(1)	$\{1, 2, 3, 4\}$
$S(H_\lambda)$	$\mathbb{N} \cup \{\infty\}$ $(\lambda = 1)$ $\mathbb{N}$ $(\lambda \neq 1)$	(2)	(3)	$\{1, 2, 3, 4\}$

注 1.1. (1)(2)(3) は未定．いずれも $\{1, 2, 3, 4\}$ を含み，(2) は ∞ を含む．

問題 2. (1)(2)(3) を決定せよ．（表をさらに分割する必要があるか．）

問題 3. 3次曲線の size-set はどうなるか．（Siegel の定理により非特異な3次曲線の size-set は ∞ を含まない．）

2　コンパクト凸領域

定理 1. 平面上の任意のコンパクトな凸領域 Γ に対して，$\mathcal{S}(\Gamma) = \mathbb{N}$ である．つまり，どんな正整数 n についても，Γ と相似な図形 C で，$|C \cap \mathbb{Z}^2| = n$ なるものが存在する．

証明. 明らかに $1 \in \mathcal{S}(\Gamma)$ であり，また，Γ と相似な図形は有界であるから，$\infty \notin \mathcal{S}(\Gamma)$ である．ある整数 $m > 0$ について，Γ と相似な図形で，ちょうど m 個の格子点を含む図形 C_0 が存在し，ちょうど $m+1$ 個の格子点を含むような Γ と相似な図形は存在しないと仮定せよ．すると，

$$C \sim \Gamma \text{ (相似)},\ |\mathrm{Int}(C) \cap \mathbb{Z}^2| = m,\ \partial C \cap \mathbb{Z}^2 \neq \emptyset$$

を満たすような図形 C が存在する．ここで，$\mathrm{Int}(C)$ は C の内部を示し，∂C は C の境界を示す．(実際，C_0 を，ある内点を中心に徐々に相似拡大していくと，このような図形が得られる.) このような C の中で，$|\partial C \cap \mathbb{Z}^2|$ が最小となるものを C_1 とせよ．すると，ちょうど $m+1$ 個の格子点を含むものは存在しないと仮定したから，∂C_1 上には 2 個以上の格子点が乗ることになる．$P, Q \in \partial C_1 \cap \mathbb{Z}^2$ とせよ．このとき，

(1) $\overline{PQ}$ が C_1 の内部を通るなら，P を中心として C_1 をほんの少し相似縮小したものを C_2 とする．$Q \notin C_2$ である．

(2) $\overline{PQ} \subset \partial C_1$ なら，P を中心に C_1 を微小回転して Q を含まないようにしたものを C_2 とする．

すると，$|\mathrm{Int}(C_2) \cap \mathbb{Z}^2| = m$ で，$0 < |\partial C_2 \cap \mathbb{Z}^2| < |\partial C_1 \cap \mathbb{Z}^2|$ を満たし，C_1 の取り方に矛盾する．　□

注 2.1. 定理 1 とその証明は高次元に拡張できる．例えば，任意の凸体 $B \subset \mathbb{R}^3$ と任意の $n > 0$ に対して，B と相似な凸体 $B_n \subset \mathbb{R}^3$ で $|B_n \cap \mathbb{Z}^3| = n$ を満たすものが存在する．

平面領域は，その内部の特定の点から，領域内の任意の点に引いた線分が，全てその領域に含まれるとき星形領域（star shaped region）という．

注 2.2. コンパクトな星形領域の size-set は $\mathbb{N}$ となることが，定理 1 と同様にして証明できる．

3　放物線

▶ **3.1.** 5個以上の格子点を通る固有2次曲線は，整数係数の2次の方程式で表すことができる．

証明．$Ax^2+Bxy+Cy^2+Dx+Ey+F=0$ を5個の格子点 (x_i,y_i), $i=1,2,3,4,5$, を通る固有2次曲線とせよ．F は整数としてよい．A,B,C,D,E を未知数とみなすと，連立方程式

$$x^2A+x_iy_iB+y_i^2C+x_iD+y_iE=-F,\ i=1,2,3,4,5$$

は自明でない解をもつ．従って，有理数の解をもつ．よって，適当な整数をかけて，$A,B,\dots,F$ を整数にすることができる．　□

▶ **3.2.** 5個の格子点を通る放物線は無限個の格子点を通る．

証明．放物線 Γ が5個の格子点 $P_1,\dots,P_5$ を通るとせよ．(P_1 は原点としてよい．) すると Γ は係数がすべて整数の方程式で与えられる．点 P_3 を通り弦 P_1P_2 に平行な弦を P_3Q とすると，その傾きは有理数であるから，点 Q は有理点となる．従って，弦 P_1P_2 の中点と弦 P_3Q の中点を結ぶ直線 ℓ の傾きは有理数 b/a $(a,b\in\mathbb{Z})$ である．直線 ℓ は Γ の対称軸に平行であるから，対称軸の傾きも b/a となる．$\mathbb{R}^2$ の相似変換

$$\varphi:\begin{pmatrix}x\\y\end{pmatrix}\mapsto\begin{pmatrix}b&-a\\a&b\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix}$$

によって，点 (a,b) は y 軸上の点 $(0,a^2+b^2)$ に移されるから，$\varphi(\Gamma)$ は y 軸に平行な軸を持つ放物線となる．また，$\varphi(\mathbb{Z}^2)\subset\mathbb{Z}^2$ だから，$\varphi(\Gamma)$ 上には5個以上の格子点（その中の1点は原点）がある．よって，$\varphi(\Gamma)$ は係数がすべて整数の方程式 $Ay=Bx^2+Cx$ で表される．すると，

$$Q_n=(A(a^2+b^2)n,\ AB(a^2+b^2)^2n^2+C(a^2+b^2)n),\quad n\in\mathbb{Z}$$

はすべて $\varphi(\Gamma)$ 上の格子点となる．線形写像 φ の逆写像 φ^{-1} の行列は

$$\begin{pmatrix}b/(a^2+b^2)&a/(a^2+b^2)\\-a/(a^2+b^2)&b/(a^2+b^2)\end{pmatrix}$$

で与えられるから，点 $\varphi^{-1}(Q_n)$ はすべて格子点となる．これらは，すべて $\Gamma=\varphi^{-1}(\varphi(\Gamma))$ 上に載っている．従って，Γ は無限個の格子点を通る．　□

定理 2. $\mathcal{S}($ 放物線 $) = \{1, 2, 3, 4, \infty\}$.

証明. $y = \sqrt{2}x^2$ は唯 1 個の格子点を通り，$y = \sqrt{2}(x^2 - 1)$ は 2 個の格子点を通る．$(x - \sqrt{2}y)^2 = 2(x + y)$ は放物線で 3 個の格子点を通る．曲線

$$(6x + (-3 + \sqrt{15})y)^2 - 72x + (-24 + 6\sqrt{15})y = 0$$

は放物線で，4 つの格子点 $(0,0), (0,1), (2,0), (1,3)$ を通る．5 個以上の格子点を通る 2 次曲線は係数が整数の方程式で表わされるから，この放物線は 5 個以上の格子点を通らない．$y = x^2$ は無限個の格子点を通る． □

4 楕円

定理 3. 軸比 λ が有理数の楕円 E_λ の size-set は $\mathcal{S}(E_\lambda) = \mathbb{N}$ である．

証明. $\lambda = b/a$（既約分数）とし，p を $p \equiv 1 \pmod 8$ なる素数とする．a, b の少なくとも一方は奇数だから，a は奇数としよう．(b が奇数の場合もほぼ同様である.）このとき，楕円 $(4x/a - 1)^2 + (4y/b)^2 = p^{n-1}$ はちょうど n 個の格子点を通ることを示そう．$(x_0, y_0) \in \mathbb{Z}^2$ に対して

$$\begin{aligned} (4x_0/a - 1)^2 \quad &+ \quad (4y_0/b)^2 = p^{n-1} \\ &\Rightarrow \quad (4bx_0)^2 + (4ay_0)^2 = a^2b^2(p^{n-1} - 1) + 8ab^2x_0 \\ &\Rightarrow \quad 8b^2 \mid 16a^2y_0^2 \Rightarrow b \mid y_0 \Rightarrow 4x_0/a \in \mathbb{Z} \Rightarrow a \mid x_0 \end{aligned}$$

である．ゆえに，楕円 $(4x/a - 1)^2 + (4y/b)^2 = p^{n-1}$ 上の格子点の個数は $(4X - 1)^2 + (4Y)^2 = p^{n-1}$ の整数解 (X, Y) の個数に等しく，定理 A により，n に等しい． □

2 つのベクトル $(\sqrt{m}, 0), (0, \sqrt{n})$ で生成される 2 次元格子 Λ は integral lattice であるから，定理 B により，与えられた個数の Λ の点を通る円がある．この円は，Λ を $\mathbb{Z}^2$ に移す $\mathbb{R}^2$ の線形変換

$$\begin{pmatrix} x \\ y \end{pmatrix} \to \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} x/\sqrt{m} \\ y/\sqrt{n} \end{pmatrix}$$

で，$\lambda = \sqrt{n/m}$ の楕円に移る．よって，定理 3 より強い次の結果が得られる．

定理 4. $\lambda^2 \in \mathbb{Q}$ のとき，$\mathcal{S}(E_\lambda) = \mathbb{N}$ である． □

▶ **4.1.** 楕円 E_λ または双曲線 H_λ が5個以上の格子点を通るなら，$\lambda^2 \in \mathcal{R}$ である．

証明．曲線は整数係数の方程式 $ax^2+2hxy+by^2+2gx+2fy+c=0$ で表すことができる．これは座標の回転で $\alpha x^2+\beta y^2+2px+2qy+r=0$ に変わる．この場合，α, β は行列

$$\begin{pmatrix} a & h \\ h & b \end{pmatrix}$$

の固有値で，$|\alpha/\beta|$ が軸比の平方 λ^2 に等しいから，$\lambda^2 \in \mathcal{R}$ である． □

▶ **4.2.** $\lambda^2 \notin \mathbb{Q}$ なら，楕円 $\mathcal{S}(E_\lambda)$ (双曲線 $\mathcal{S}(H_\lambda)$) は $\{1,2,3,4\}$ を含む．

証明．$\xi = \pm\lambda^2$（楕円の場合は $+$，双曲線の場合は $-$）とし，τ を ξ と代数的に独立な超越数とする．まず，$\xi x^2+y^2+\tau x=0$ はただ1個の格子点 $(0,0)$ を通る．$\xi(x^2-1)+y^2+\tau y=0$ は格子点を2個だけ通る．また，$\xi x^2+y^2-1+(1-\xi)x=0$ はちょうど3個の格子点 $(0,\pm1),(1,0)$ を通る．$\xi x^2+y^2=\xi+1$ は4個の格子点 $(\pm1,\pm1)$ を通る． □

定理 5. $\lambda^2 \notin \mathcal{R} \Rightarrow \mathcal{S}(E_\lambda)\,(\mathcal{S}(H_\lambda)) = \{1,2,3,4\}$． □

5 双曲線

▶ **5.1.** $0<\lambda\in\mathbb{Q}$ のとき，$\begin{cases} \lambda\neq 1 \text{ なら } \infty \notin \mathcal{S}(H_\lambda) \\ \lambda = 1 \text{ なら } \infty \in \mathcal{S}(H_\lambda) \end{cases}$

証明．ペル方程式 $X^2-2Y^2=1$ は無限個の整数解を持つから，方程式 $(x+y)^2-2y^2=1$ も無限個の整数解を持つ．これは軸比 $\lambda=1$ の双曲線である．ゆえに $\lambda=1$ なら $\infty\in\mathcal{S}(H_\lambda)$ である．

以下，$1\neq\lambda\in\mathbb{Q}$ とし，H_λ は5個以上の格子点を通ると仮定しよう．H_λ の主軸，副軸の傾きが $0,\infty$ の場合，その方程式は

$$(ax-p)^2-(by-q)^2=c\ (a,b,c,p,q\in\mathbb{Z})$$

と表わされる．$c\neq 0$ で，c の約数の個数は有限個であり，

$$(ax-p)^2-(by-q)^2=(ax-by-p+q)(ax+by-p-q)$$

であるから，この双曲線は無限個の格子点を通ることはできない．

軸の傾きが $0, \infty$ でない場合，5 個以上の格子点を通る双曲線は整数係数の方程式 $ax^2 + 2hxy + by^2 + 2gx + 2fy + c = 0$ $(h \neq 0)$ で表される．$a + b = 0$ なら $\lambda = 1$ だから，$(a + b)h \neq 0$ である．このとき，$\begin{pmatrix} a & h \\ h & b \end{pmatrix}$ の固有値は有理数である．(さもないと，$\lambda^2 \notin \mathbb{Q}$ となることが容易に確かめられる．) 従って，この行列には整数成分の固有ベクトル $\begin{pmatrix} p \\ q \end{pmatrix}$ がある．すると，$\mathbb{R}^2$ の相似変換

$$\varphi : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} p & -q \\ q & p \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

によって双曲線は軸の傾きが $0, \infty$ のものに変換される．変換された双曲線の軸比は同じ λ であるから，その上に無限個の格子点は乗らない．また $\varphi(\mathbb{Z}^2) \subset \mathbb{Z}^2$ だから，もとの双曲線上にも無限個の格子点が乗ることはできない． □

定理 6. $0 < \lambda \in \mathbb{Q} \Rightarrow S(H_\lambda) = \begin{cases} \mathbb{N} & for\ \lambda \neq 1 \\ \mathbb{N} \cup \{\infty\} & for\ \lambda = 1 \end{cases}$

証明. $\lambda = b/a$ (既約分数) とし，p を $p \equiv 1 \pmod{6ab}$ なる素数とする．双曲線 $(3ax + 1)^2 - (3by)^2 = p^{n-1}$ 上にはちょうど n 個の格子点が乗ることを示そう．$(x_0, y_0) \in \mathbb{Z}^2$ に対して，

$$\begin{aligned} (3ax_0 + 1)^2 \quad - \quad & (3by_0)^2 = p^{n-1} \\ \Rightarrow \quad & (3ax_0 + 1 + 3by_0)(3ax_0 + 1 - 3by_0) = p^{n-1} \\ \Rightarrow \quad & \begin{cases} 6ax_0 + 2 = \pm(p^k + p^{n-1-k}) \\ 6by_0 = \pm(p^k - p^{n-1-k}) \end{cases} \qquad (0 \leqq k < n,\ \text{複合同順}) \end{aligned}$$

であるが，$6ax_0 + 2 \equiv 2, \pm(p^k + p^{n-1-k}) \equiv \pm 2 \pmod 6$ であるから「$-$」は適さない．ゆえに，$(3ax + 1)^2 - (3by)^2 = p^{n-1}$ 上の格子点の個数は n 個以下である．逆に，$p \equiv 1 \pmod{6ab}$ であるから，すべての $0 \leq k < n$ に対して，最後の 2 つの式 (符号 $+$ を選択した 2 つの式) を満たす整数 x_0, y_0 が存在し，双曲線 $(3ax + 1)^2 - (3by)^2 = p^{n-1}$ 上にはちょうど n 個の格子点が乗ることがわかる．従って $n \in S(H_\lambda)$ である．$S(H_\lambda)$ が ∞ を含むかどうかは 5.1 から出る． □

▶ **5.2.** $aX^2 - bY^2 = c$ $(a, b \in \mathbb{N},\ \sqrt{ab} \notin \mathbb{N},\ c \in \mathbb{Z})$ が整数解をもつなら，それは無限個の整数解をもつ．

証明. (x_0, y_0) を不定方程式 $a^2X^2 - abY^2 = ac$ の 1 つの整数解とすると，$(ax_0 - \sqrt{ab}y_0)(ax_0 + \sqrt{ab}y_0) = ac$ である．$\sqrt{ab} \notin \mathbb{N}$ より，ペル方程式 $x^2 - aby^2 = 1$ は無限個の整数解 (x_i, y_i), $i = 1, 2, 3, \ldots$ をもつ．(例えば，Steuding [6] を参照せよ.) すると

$$(ax_0 \pm \sqrt{ab}y_0)(x_i \pm \sqrt{ab}y_i) = a(x_0x_i + by_0y_i) \pm \sqrt{ab}(ax_0y_i + y_0x_i)$$

であるから，$(x_0x_i + by_0y_i, ax_0y_i + y_0x_i)$, $i = 1, 2, 3, \ldots$ が $a^2X^2 - abY^2 = ac$ の無限個の整数解を与える． □

▶ **5.3.** $\lambda^2 \in \mathbb{Q}$, $\lambda \notin \mathbb{Q}$ のとき，$\infty \in \mathcal{S}(H_\lambda)$. □

▶ **5.4.** 互いに素な正整数 m, n に対して，$\sqrt{t(1-t)(m-n)^2 + mn}$ が無理数となるような有理数 $t \in (0, 1)$ が存在する.

証明. $m > n$ と仮定し，$1/t = k(m-n)$ とおくと，

$$t(1-t)(m-n)^2 + mn = \frac{1}{k^2}(km-1)(kn+1)$$

となる．Dirichlet の算術定理により $\{km - 1 \mid k = 1, 2, 3, \ldots\}$ は無限個の素数を含む．$k > 2$ を $km - 1$ が素数 $(:= p)$ となるように定めることができる．すると，$p = km - 1 > kn + 1$ であるから，p^2 は $(km-1)(kn+1)$ を割り切らない．従って，$\sqrt{\frac{1}{k^2}(km-1)(kn+1)} \notin \mathbb{Q}$ である． □

▶ **5.5.** $\lambda \notin \mathbb{Q}$, $\lambda^2 \in \mathbb{Q} \Rightarrow \mathcal{S}(H_\lambda) \supset \{1, 2, 3, 4\}$.

証明. $\mathcal{S}(H_\lambda)$ が 1,2 を含むことは，4.2 と同じように証明できる．$\mathcal{S}(H_\lambda)$ が 3,4 を含むことを示すため，$\lambda^2 = m/n$ $(m, n \in \mathbb{N})$ とおく．すると，$\sqrt{m/n} \notin \mathbb{Q}$ である．まず，双曲線 $(m-n)(y^2 - 1 + x) + 2\sqrt{mn}\,xy = 0$ は軸比 $\sqrt{m/n}$ を持ち，ちょうど 3 つの格子点 $(0, 1), (0, -1), (1, 0)$ を通る．ゆえに，$3 \in \mathcal{S}(H_\lambda)$ である．次に，

$$\begin{aligned} f(x, y) &= tx^2 + (1-t)y^2 - t(y+1) - (1-t)(x+1), \\ K &= t(1-t)(m-n)^2 + mn \end{aligned}$$

とおき，$t = a/b\,(a < b,\ a, b \in \mathbb{N})$ を $\sqrt{K}$ が無理数となるようにとる．すると，$(m-n)\,f(x, y) + 2\sqrt{K}\,xy = 0$ は軸比 $\sqrt{m/n}$ の双曲線の方程式となることが確かめられる．また，この双曲線はちょうど 4 つの有理点

$$(0, -1),\ (0, \tfrac{b}{b-a}),\ (-1, 0),\ (\tfrac{b}{a}, 0)$$

を通ることがわかる．この双曲線を

$$\begin{cases} X = a(b-a)x \\ Y = a(b-a)y \end{cases}$$

と変数変換（相似変換）すると，変換後の双曲線は4つの格子点

$$(0, -a(b-a)),\ (0, ab),\ (-a(b-a), 0),\ (b(b-a), 0)$$

を通る． □

6 その他の結果

▶ **6.1.** M を正則な 2×2 の整数行列, $T = Tr(M^tM)$, $D = \det(M^tM)$ とする．このとき，$\lambda^2 = \frac{T^2-2D-T\sqrt{T^2-4D}}{2D}$ となる $\lambda > 0$ に対して，$\mathcal{S}(E_\lambda) = \mathbb{N}$ である．

証明. $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ とし，$f : \mathbb{R}^2 \to \mathbb{R}^2$ を

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

なる線形変換とする．$\Lambda := \Lambda[(a,b),(c,d)]$ を $(a,b),(c,d)$ で生成される格子とすると，$f : \mathbb{Z}^2 \to \Lambda$ は全単射である．Λ は integral lattice であるから，定理Bにより，任意の $n > 0$ に対して，ちょうど n 個の Λ の点を通る円 $(X-p)^2 + (Y-q)^2 = r^2$ がある．従って，楕円

$$(ax + cy - p)^2 + (bx + dy - q)^2 = r^2$$

はちょうど n 個の $\mathbb{Z}^2$ の点を通る．左辺を展開して，x, y の2次の項をまとめると，$(a^2+b^2)x^2 + 2(ac+bd)xy + (c^2+d^2)y^2$ となる．これから，軸比の平方を計算すると 6.1 の λ^2 に等しくなる． □

▶ **6.2.** $\mathcal{S}(E_\lambda) = \mathbb{N}$ となる $\lambda^2 \in \mathcal{R} \setminus \mathbb{Q}$ がある． □

▶ **6.3.** $\lambda^2 \in \mathcal{R} \setminus \mathbb{Q}$ で，$\infty \in \mathcal{S}(H_\lambda)$ となる λ が存在する．

証明. 整数行列 $\begin{pmatrix} a & h \\ h & b \end{pmatrix}$ を固有値の比の絶対値が $\lambda^2 \in \mathcal{R} \setminus \mathbb{Q}$ を満たし，しかも $d := h^2 - ab > 0$ で $\sqrt{d} \notin \mathbb{Q}$ なるものとする．例えば行列 $\begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}$ はこれらの条件を満足する．5.2により，$-dX^2 + Y^2 = -d + h^2$ は無限個の整数解をもつ．従って，双曲線 $-d(ax+hy+1)^2 + (-dy+h)^2 = -d+h^2$ は $\frac{1}{ad}\mathbb{Z}^2$ の無限個の点を通る．この双曲線の方程式は，$ax^2 + 2hxy + by^2 +$ (x, y の一次式) $= 0$ と書き換えられるから，その軸比の二乗は λ^2 である．この双曲線を原点を中心として，ad 倍に拡大すれば，無限個の格子点を通る双曲線で，$\lambda^2 \in \mathcal{R} \setminus \mathbb{Q}$ なるものが得られる． □

▶ **6.4.** $\begin{pmatrix} a & c \\ b & d \end{pmatrix}$ がunimodular行列のとき，軸比の平方が $\lambda^2 = \frac{S^2+2-S\sqrt{S^2+4}}{2}$ ($S = a^2 - b^2 + c^2 - d^2$) で，しかも $S(H_\lambda) \supset \mathbb{N}$ なるような双曲線 H_λ がある．

証明. unimodular行列の導く線形変換 f は $\mathbb{Z}^2$ の間の全単射となることと，定理6の証明に現れた双曲線 $(3X+1)^2 - (3Y)^2 = p^{n-1}$ （$a = b = 1$ の場合）はちょうど n 個の格子点を通ることから，$X = ax + by$, $Y = cx + dy$ と代入して，6.1のように計算していけば6.4が導かれる． □

参考文献

[1] E. Bannai, T. Miezaki, On a property of 2-dimensional integral Euclidean lattices, preprint.

[2] H. Maehara, M. Matsumoto, Is there a circle that passes through a given number of lattice points?, *European J. Combin.* 19 (1998) 591–592.

[3] A. Schinzel, Sur l'existence d'un cercle passant par un nombre donne de points aux cooronnees entieres, *Ensignement Math.* (2) 4 (1958) 71-72.

[4] W. Sirepinski, Sur quelques problemes concenant les points aus coordonnees entriers, *Ensignement Math.* (2) 4 (1958) 25–31.

[5] H. Steinhaus, *One Hundred Problems in Elementary Mathematics*, Dover Publications, Inc. 1964 New York.

[6] J. Steuding, *Diophantine Analysis*, Chapman & Hall/CRC 2005 London.

Several remarks on the concepts of t-designs

Eiichi Bannai and Etsuko Bannai
(bannai@math.kushu-u.ac.jp, et-ban@rc4.so-net.ne.jp)

1 Introduction

この講演では，実双曲空間で t-design を定義する事，その定義を球面 design およびユークリッド design と比較する事が一つの目標です．また，これ等の概念と Delsarte が定義したアソシエーションスキームに於ける relative t-design との関係を述べる事がもう一つの目標です．

先ず次の３つの空間を考えましょう．

$\mathbb{S}^n$	$\mathbb{R}^n$	$\mathbb{H}^n$
球面	ユークリッド空間	実双曲空間
正の定曲率空間	曲率 0 の定曲率空間	負の定曲率空間
$\mathbb{S}^n = SO(n+1)/SO(n)$	$\mathbb{R}^n = E(n)/O(n)$	$\mathbb{H}^n = SO^1(n+1)/SO(n)$
$(= O(n+1)/O(n))$	$(E(n) = \mathbb{R}^n \cdot O(n))$	$(= O^1(n+1)/O(n))$

これ等はいずれも Riemann 対称空間であり，さらに 2 point homogeneous 空間になっています．

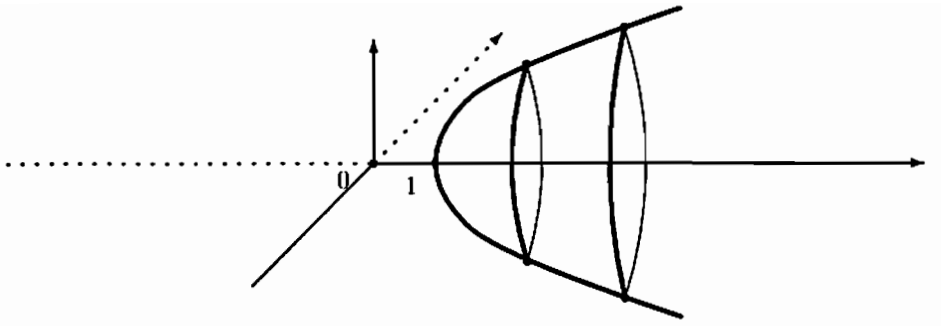
$\mathbb{S}^n$ における t-design の概念は Delsarte-Goethals-Seidel (1977) により定義されました．$\mathbb{R}^n$ における t-design の概念は Neumaier-Seidel (1988) (Delsarte-Seidel (1989)) により定義されました．$\mathbb{H}^n$ において t-design をどの様に定義するのが良いかをここで考えたいと思います．その前に，実双曲空間の定義を与えます．

$$\mathbb{H}^n = \{(x_0,\ x_1, \ldots, x_n) \in \mathbb{R}^{n+1} \mid x_0^2 - x_1^2 - \cdots - x_n^2 = 1,\ x_0 > 0\}$$

とし，$\mathbb{H}^n$ の２つの元 $x = (x_0,\ x_1, \ldots, x_n)$, $y = (y_0,\ y_1, \ldots, y_n)$ の間の距離は次で定義します．

$$d(x,\ y) = \operatorname{arccosh}(x_0y_0 - x_1y_1 - \cdots - x_ny_n)$$

ここで $\cosh(z) = \frac{e^z+e^{-z}}{2}$ です．この空間は Bolyai-Lobachevskii 空間と呼ばれる有名な非ユークリッド空間として知られています．



講演者（坂内英一）は $\mathbb{H}^n$ に対しても t-design の概念を定義したいと３０年ほど前に考えました．ことあるごとにこの問題に立ち返ったのですが，うまく行きませんでした．その理由については後述します．例えば，次の論文

Bannai-Blokhuis-Delsarte-Seidel: An addition theorem for hyperbolic spaces, J. of Combi. Teory (A) 36 (1984), 832-841.

では $\mathbb{H}^n$ 上での加法公式を見いだし，それを用いて $\mathbb{H}^n$ 上の s-距離集合 X については $|X| \leq \binom{n+1}{s}$ と言う結果を得ることができました．それが t-design の定義を導く事を期待していたのですが，どうしてもうまく行きませんでした．

2 球面上の t-design に関しての復習

球面 $\mathbb{S}^n$ は，

$$\mathbb{S}^n = \{(x_0,\ x_1, \ldots, x_n) \in \mathbb{R}^{n+1} \mid x_0^2 + x_1^2 + \cdots + x_n^2 = 1\}$$

と置き，$\mathbb{S}^n$ の２つの元 $x = (x_0,\ x_1, \ldots, x_n)$, $y = (y_0,\ y_1, \ldots, y_n)$ の間の距離は

$$d(x,\ y) = \arccos(x_0y_0 + x_1y_1 + \cdots + x_ny_n)$$

で定めます．

- **[球面 design の定義]**

  $X \subset \mathbb{S}^n$ が球面 $\mathbb{S}^n$ 上の t-design

  $$\Longleftrightarrow \frac{1}{|\mathbb{S}^n|}\int_{\mathbb{S}^n} f(x)d\sigma(x) = \frac{1}{|X|}\sum_{x\in X} f(x),\ {}^\forall f(x) = f(x_0, x_1, \ldots, x_n) : \text{多項式 } \deg(f) \leq t$$

  $$\Longleftrightarrow \sum_{x\in X} f(x) = 0,\ {}^\forall f(x) \in \mathrm{Harm}_k(\mathbb{R}^{n+1}),\ {}^\forall k = 1,\ 2, \ldots, t.$$

ここで，$\mathrm{Harm}_k(\mathbb{R}^{n+1})$ は次数 k の斉次の調和多項式全体の空間を表します．すなわち，$\Delta f(x) = 0$, $\Delta = \frac{\partial^2}{\partial x_0^2} + \frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_n^2}$, を満たす多項式です．また，$\dim \mathrm{Harm}_k(\mathbb{R}^{n+1}) = \binom{n+k}{k} - \binom{n+k-2}{k-2}$ です．

3 $\mathbb{H}^n$ で design を定義する事が何故難しいか

理由 1： $\int_{\mathbb{H}^n} f(x)dx$ は多項式 $f(x)$ に対して定義されない. (この状況は $\mathbb{R}^n$ においても同様です.)

理由 2： $\mathbb{H}^n$ 上において, 調和多項式の類似は定義出来ます. $\Delta^* = \frac{\partial^2}{\partial x_0^2} - \frac{\partial^2}{\partial x_1^2} - \cdots - \frac{\partial^2}{\partial x_n^2}$ とし,

$$f \in \mathrm{Harm}_k^*(\mathbb{R}^{n+1}) \iff f(x) \text{ は } k \text{ 次の斉次多項式で } \Delta^* f(x) = 0$$

と定義します. この時, もし

$$X \text{ が } \mathbb{H}^n \text{ の } t\text{-design} \Longleftrightarrow \sum_{x \in X} f(x) = 0,\ {}^\forall f(x) \in \mathrm{Harm}_k^*(\mathbb{R}^{n+1}),\ {}^\forall k = 1,\ 2, \ldots, t$$

で定義すると, 例えば

$$f(x) = nx_0^2 + x_1^2 + \cdots + x_n^2 \in \mathrm{Harm}_2^*(\mathbb{R}^{n+1})$$

に対して

$$\sum_{x \in X} f(x) > 0, \quad {}^\forall X \subset \mathbb{H}^n$$

となります. この事は 2-design が一切存在しない事になり, 望ましくありません. この定義を何らかの形で修正したかったのですがうまく行きませんでした.

4 $\mathbb{R}^n$ における t-design の概念の復習

ユークリッド空間 $\mathbb{R}^n$ 上の t-design の概念は Neumaier- Seidel (1988) によります. 解析の分野では, cubature formula として同様な概念が考えられていました. ユークリッド空間上のデザインは球面上のデザインの次の意味での2段階の拡張になっています. すなわち,

(1) $X \subset \mathbb{S}^{n-1}$ と言う条件を緩める.
(2) X 上の重さ関数を考える.

• [ユークリッド design の定義]

$X \subset \mathbb{R}^n$, $|X| < \infty$, $w : X \longrightarrow \mathbb{R}_{>0}$ とします.

$$\begin{aligned}&(X,\ w) \text{ が } \mathbb{R}^n \text{ の } t\text{-design}\\ \Longleftrightarrow &\sum_{i=1}^{p} \frac{w(X_i)}{|\mathbb{S}^{n-1}(r_i)|} \int_{\mathbb{S}^{n-1}(r_i)} f(x)d\sigma_i(x) = \frac{1}{|X|} \sum_{x \in X} w(x)f(x),\\ &{}^\forall f(x) = f(x_1, \ldots, x_n) : \text{多項式 } \deg(f) \le t\end{aligned}$$

ここで,
$S^{n-1}(r)$ は原点を中心とする半径 r の球面を表します.
$\{r_1,\ r_2, \ldots, r_p\} = \{r \in \mathbb{R}_{>0} \mid X \cap S^{n-1}(r) \neq \emptyset\}$
$X_i = X \cap S^{n-1}(r_i)$ $i = 1,\ 2, \ldots, p$

$w(X_i) = \sum_{x \in X_i} w(x)$
とします．この $\mathbb{R}^n$ 上の t-design の定義は次と同値です．

$$\iff \sum_{x \in X} w(x)\|x\|^{2j} f(x) = 0,\ {}^\forall f(x) \in \mathrm{Harm}_k(\mathbb{R}^n),$$
$1 \leq k,\ 0 \leq j,\ k+2j \leq t,$（$\|x\|$ は通常のノルム）

$\iff X$ の高々 t 次までの任意のモーメントは直交変換によって不変である．

最後の条件を言い直すと

$$\sum_{x \in X} w(x) f(x) = \sum_{x \in X} w(x) f(\sigma(x))$$

が任意の高々 t 次の多項式 $f(x) = (x_1, \ldots, x_n)$ と任意の $\sigma \in O(n)$ に対して成り立つことになります．

注意：この最後の定義は，球面 $\mathbb{S}^{n-1}$ 上の t-デザインの定義としてそっくりそのまま成り立ちます．従ってこの最後の定義は球面上の t-デザインとユークリッド空間上の t-デザインの統一した定義を与える良い定義であると考えています．

5 $\mathbb{H}^n$ における t-design の定義の提唱

$\mathbb{H}^n = \{(x_0,\ x_1, \ldots, x_n) \in \mathbb{R}^{n+1} \mid x_0^2 - x_1^2 - \cdots - x_n^2 = 1,\ x_0 > 0\}$ であった事を思い出しましょう．

$\mathrm{Isom}(\mathbb{H}^n) \cong O^1(n+1)$ であり，
$z_0 = (1, 0,\ 0, \ldots, 0) \in \mathbb{H}^n$に対して z_0 の固定部分群は $O(n)$ と同型です．

一方，

$\mathrm{Isom}(\mathbb{R}^n) \cong E(n) (= \mathbb{R}^n \cdot O(n))$ であり，
$z_0 = (0,\ 0, \ldots, 0) \in \mathbb{R}^n$に対して z_0 の固定部分群は $O(n)$ と同型です．

定義 [$\mathbb{H}^n$ **上の** t-**design の定義**]
$X \subset \mathbb{H}^n$, $|X| < \infty$, $w : X \longrightarrow \mathbb{R}_{>0}$ とします．
$(X,\ w)$ が特別な点 z_0 に関して $\mathbb{H}^n$ の t-design であるとは，変数 $x_1,\ x_2, \ldots, x_n$ に対する X の高々 t 次のモーメントが $x_1,\ x_2, \ldots, x_n$ に関する直交変換群 $O(n)$（$= \mathrm{Isom}(\mathbb{H}^n)$ の中の z_0 の固定部分群） の任意の元 σ によって不変である事です．

幾つかの注意

(1) ユークリッド空間上の t-design との類似はこの節のはじめに述べた事から明らかです．

(2) 球面上の t-design に関しても特別な点 $z_0 \in S^n$ に関する t-design が次の様に定義出来ます．

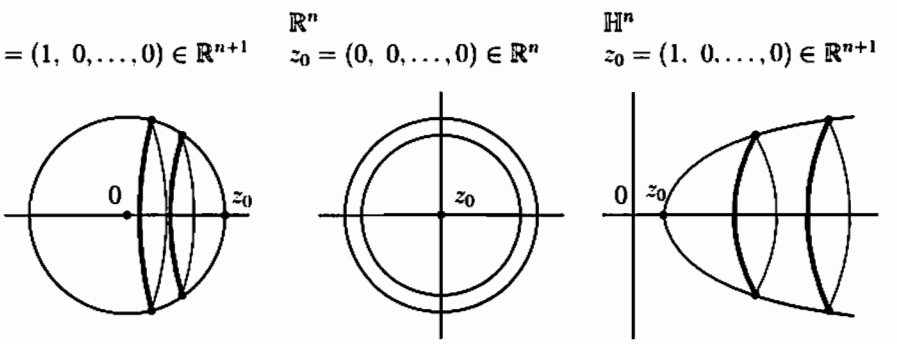
$X \subset \mathbb{S}^n$, $|X| < \infty$, $w : X \longrightarrow \mathbb{R}_{>0}$ (ここで, $\mathrm{Isom}(\mathbb{S}^n) \cong O(n+1)$, $z_0 \in \mathbb{S}^n$ の固定部分群 $\cong O(n)$ に注意.)

• (X, w) が特別な点 $z_0 = (1,\ 0,\ 0, \ldots, 0) \in \mathbb{S}^n$ $(\subset \mathbb{R}^{n+1})$ に関する t-design であるとは変数 $x_1,\ x_2, \ldots, x_n$ に対する X の高々 t 次のモーメントが $x_1,\ x_2, \ldots, x_n$ に関する直交変換群 $O(n)$ $(= O(n+1)$ の中の z_0 の固定部分群$)$ の任意の元 σ によって不変である事です.

この特別な z_0 に関する $\mathbb{S}^n$ 上の t-design の定義は $\mathbb{S}^n$ 上の通常の t-design の定義に比べて遥かに弱い. 何故ならば, 通常の t-design の定義は, 変数 $x_0,\ x_1, \ldots, x_n$ に関する X の高々 t 次の任意のモーメントが $O(n+1)$ の任意の元によって不変であったからです.

(3) 3つの空間 $\mathbb{S}^n$, $\mathbb{R}^n$ および $\mathbb{H}^n$ の上の t-design の間の関係.

以下 X を上に挙げた3つの空間の内のどれかの部分空間とし, $w : X \longrightarrow \mathbb{R}_{>0}$ を考える.



一つの場合に t-design が存在すれば本質的に残り2つの場合にも存在する. この事は次の写像達を考えれば説明がつきます.

$$x = (x_0,\ x_1, \ldots, x_n) \longrightarrow (x_1, \ldots, x_n) \longleftarrow x = (x_0,\ x_1, \ldots, x_n)$$
$$(\sqrt{1 - x_1^2 - \cdots - x_n^2},\ x_1, \ldots, x_n) \longleftarrow (x_1, \ldots, x_n) \longrightarrow x = (\sqrt{1 + x_1^2 + \cdots + x_n^2},\ x_1, \ldots, x_n)$$

上で, 本質的にと言う言葉を使ったのは, $\mathbb{S}^n$ においては $x_1^2 + x_2^2 + \cdots + x_n^2 \leq 1$ が成り立っていなければならないのですが, 必ずしもそれが成り立っていないからです. しかし $\mathbb{R}^n$ において拡大・縮小をしてもユークリッドデザインとして同型なので適当に縮小すればその条件が成り立つ様に出来るからです. この事は, t-design に対する Fisher 型不等式とか tight t-design の定義, tight t-design の分類も含めて全ての事が全く同様である事を物語っています. この様に全く同様になってしまうと言うことは, ある意味では面白くないと考える人も居るかもしれませんが, 逆にこの design の定義が自然であり意味のある事を示唆していると思います. 個人的にはこのことによってユークリッドデザインの定義が良いものであると言うことをここで初めて納得出来ました. いずれにしてもコンパクトでない, 無限に広がる空間を, 有限個の点で近似すると言う形で t-design を考えることはもともと無理な事なのかもしれません. ここで考えた $\mathbb{R}^n$ 上あるいは $\mathbb{H}^n$ 上の t-design は1点を特別視して全体を近似すると言う意味で, 自己中心的あるいは地動説的なデザインの概念と言えるでしょう.

6 Q-多項式スキームにおける relative t-design との関係

2010 年 3 月の神戸学院大に於ける代数的組合せ論ミニ集会において講演者はここで定義した $\mathbb{R}^n$ および $\mathbb{H}^n$ 上の t-design の概念をそっくり Q-多項式スキームの t-design に対して考えると面白いと言うことを述べました．それに対して田中太初氏は， Delsarte の論文

Pairs of vectors in the space of association schemes,
Philips Res. Repts. 32, (1977), 373–411.

に現れる relative t-design の概念がそれでないかと指摘しました．実際にそうでした．

Delsarte の relative t-design について少し説明を加えると次の様になります．

$\mathfrak{X} = (X, \{R_i\}_{0\le i\le d})$ を Q-多項式スキームとし，E_0, $E_1, \ldots, E_d$ を付随した原始ベキ等行列とします．$u \in X$ を固定し，
$X_i = \Gamma_i(u) (= \{x \in X \mid (x,u) \in R_i\})$
$Y \subset X$ に対して X 上の特性関数（vector）ψ_Y を

$$\psi_Y(x) = \begin{cases} 1 & x \in Y \text{ の時} \\ 0 & x \notin Y \text{ の時} \end{cases}$$

と定義します．$v \in X$ に対して $E_j\psi_{\{v\}}$ は E_j の v 列ベクトルです．
$L_j(X)$ を $\{E_j\psi_{\{v\}} \mid v \in X\}$ で生成されるベクトル空間とします．（これは球面の場合の j 次の斉次調和多項式の空間 $\mathrm{Harm}_j(\mathbb{S}^{n-1})$ に対応します．）$\psi : X \longrightarrow \mathbb{R}_{\ge 0}$ X 上の任意の非負関数とします．以下にでは，記号を濫用して X 上の関数と X で張られるベクトル空間のベクトルを同一視し同じ記号で表します．

• **[Delsarte による Q-多項式スキームに於ける relative t-design の定義]**
X 上の非負関数 ψ が点 $u \in X$ に関する relative t-design

$\Longleftrightarrow$ $E_j\psi$ と $E_j\psi_u$ 一次従属である事が $j = 1, 2, \ldots, t$ に対して成り立つ

$\Longleftrightarrow$ $E_j\psi$ と $E_j\overline{\psi}$ 一次従属である事が $j = 1, 2, \ldots, t$ に対して成り立つ

ここで $\overline{\psi}(x)$ ($x \in X_i = \Gamma_i(u)$ の時 $\frac{1}{|X_i|}\sum_{y\in X_i}\psi(y)$ で与えられる．)

$\Longleftrightarrow$

$Y = \psi$ の support, $w = \psi|_Y$ とすると (Y, w) が次の式を満たす

$$\sum_{i=1}^{p} \frac{W_{\nu_i}}{|X_{\nu_i}|} \sum_{x\in X_{\nu_i}} f(x) = \sum_{y\in Y} w(y)f(y)$$

が任意の $f \in L_0(X) \perp L_1(X) \perp \cdots L_t(X)$ に対して成り立つ．
ここで $\{\nu_1, \nu_2, \ldots, \nu_p\} = \{\nu \mid Y \cap X_\nu \neq \emptyset\}$ です．

注意： $E_j\psi_{X_i}$ と $E_j\psi_{\{u\}}$ は任意の i, j $(0 \le i, j \le d)$ に対して一次従属です．従って各 X_i 上で一定の値をとる関数は任意の t に対して u に関する relative t-design です．この

様なものを自明な relative t-design と呼びます．また，$\psi_{\{u\}}$ と $\overline{\psi}$ は一次独立です．

我々はユークリッドデザインの研究の類似として次の結果を得ることができました．

定理　$(Y,\ w)$ を Q-多項式スキームにおける点 $u \in X$ に関する自明でない relative $2e$-design とする．この時次の Fisher 型不等式が成り立つ．

$$|Y| \geq \dim(L_0(S) + L_1(S) + \cdots + L_e(S))$$

ここで $S = X_{\nu_1} \cup X_{\nu_2} \cup \cdots \cup X_{\nu_p}$ であり $L_i(S)$ は $L_i(X)$ の定義域を S に制限したものである．

注意：ユークリッド $2e$-design $(X,\ w)$ の場合の Fisher 型不等式は

$$|X| \geq \dim(\mathrm{Hom}_0(S) + \mathrm{Hom}_1(S) + \cdots + \mathrm{Hom}_e(S)$$

ここで $S = S^{n-1}(r_1) \cup S^{n-1}(r_2) \cup \cdots \cup S^{n-1}(r_p)$ です．

上の定理に対応して tight な relative t-design の概念を種々の Q-多項式スキームに対して適用して，それ等の構成・分類を考える事は非常に興味のある問題であると思います．

References

[1] E. Bannai and E. Bannai,　球面上の代数的組合せ理論シュプリンガー・東京 (1999).

[2] Et. Bannai and Et. Bannai, *A survey on spherical designs and algebraic combinatorics on spheres*, European J. Combin., 30 (2009), 1392–1425.

[3] E. Bannai, A. Blokhuis, Ph. Delsarte, and J. J. Seidel, *An addition formula for hyperbolic space*, J. Combin. Theory Ser. A 36 (1984), no. 3, 332–341.

[4] P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. 10 (1973).

[5] P. Delsarte, *Pairs of vectors in the space of association schemes*, Philips Res. Repts. 32, (1977), 373–411.

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

[7] P. Delsarte and J. J. Seidel, *Fisher type inequalities for Euclidean t-designs*, Linear Algebra Appl. 114-115 (1989), 213–230.

[8] 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), no. 3, 321–334.

Hamiltonicity of 4-connected claw-free graphs

藤沢　潤 (Fujisawa Jun)
高知大学

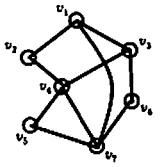
Hamiltonicity of 4-connected
claw-free graphs

藤沢　潤 (高知大学理学部)

joint work with
太田　克弘 (慶應義塾大学)

グラフとは

グラフ…ある頂点集合Vとその2元部分集合の族（辺集合）Eの組(V,E)で定義される離散構造。



$V(G) = \{v_1, v_2, v_3, v_4, v_5, v_6, v_7\}$
$E(G) = \{v_1v_2, v_1v_3, v_1v_7, v_2v_4, v_3v_4, v_3v_6, v_4v_5, v_4v_7, v_5v_7, v_6v_7\}$

$V(G)$…頂点集合、 $E(G)$…辺集合

グラフG

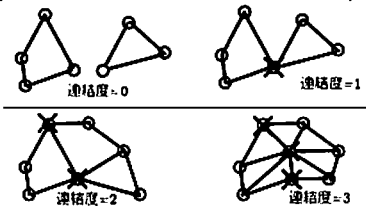
今日の話題

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

キーワード
- 4-連結
- claw-freeグラフ
- ハミルトンサイクル

連結度

連結度…グラフの「各頂点間の結びつき」の強さ。
(何点取り除いたら、グラフが非連結になるか？？)



n-連結グラフ=連結度がn以上のグラフ

今日の話題

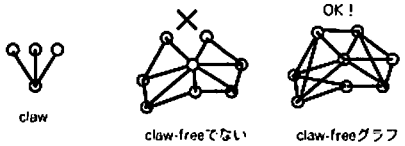
予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

キーワード
- 4-連結
- claw-freeグラフ
- ハミルトンサイクル

---

claw-freeグラフ

GがHを誘導部分グラフとして持つ
…GがHを、辺の非隣接の関係も考慮に入れた上で含む
clawを誘導部分グラフとして持たないグラフを
claw-freeグラフと呼ぶ。



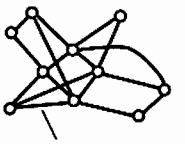
今日の話題

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

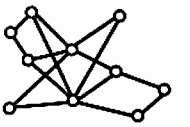
キーワード
- 4-連結
- claw-freeグラフ
- ハミルトンサイクル

ハミルトンサイクル

同じ頂点を二度通らないように辺を辿っていき、元の頂点に戻る回路をサイクルと呼び、全ての頂点を通るサイクルをハミルトンサイクルと呼ぶ。



ハミルトンサイクル

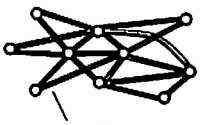


ハミルトンサイクルを持たない

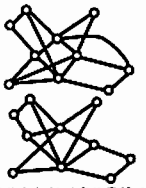
ハミルトンサイクル

同じ辺を二度通らないように辺を辿っていき、全ての辺を通って元の頂点に戻る回路…オイラー回路

オイラー回路の存在の判定は簡単だが、ハミルトンサイクルの存在の判定は難しい。(NP完全)



オイラー回路



ハミルトンサイクルを持つ？
持たない？？

既存の結果

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

定理 (Broersma et al, 2001)
4-連結claw-free, Hourglass-freeグラフは
ハミルトンサイクルを持つ。

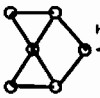
claw

hourglass

既存の結果

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

定理 (Kaiser et al., 2005)
4-連結claw-freeグラフが Hourglass-propertyを満たす時
ハミルトンサイクルを持つ。

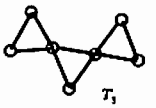


Hourglass-property …
ーこのような頂点がどのhourglassにも存在

既存の結果

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

定理 (Pfender, 2005)
4-連結claw-free, T_3-freeグラフはハミルトンサイクルを持つ。



T_3

Thomassen予想

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

一方、Thomassenは次の予想を提起している。

予想 (Thomassen, 1986)
4-連結lineグラフはハミルトンサイクルを持つ。

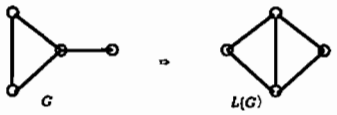
15

Thomassen予想

予想 (Thomassen, 1986)
4-連結lineグラフはハミルトンサイクルを持つ。

グラフGのlineグラフ$L(G)$は、次のようにして定義される。

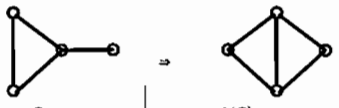
- $L(G)$の頂点集合 = Gの辺集合
- $L(G)$の2頂点 e_1 e_2は、Gにおいてそれらが隣接している時 $L(G)$において辺で結ぶ。



16

Thomassen予想

予想 (Thomassen, 1986)
4-連結lineグラフはハミルトンサイクルを持つ。



G	$L(G)$
辺	頂点
頂点	完全グラフ
次数	完全グラフの頂点数

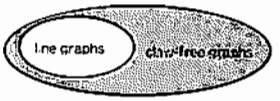
17

Thomassen予想

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

予想 (Thomassen, 1986)
4-連結lineグラフはハミルトンサイクルを持つ。

lineグラフはclaw-freeグラフになるので、Thomassen予想の仮定はMatthews and Sumnerの予想の仮定より強い。



18

Ryjacek closure

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

予想 (Thomassen, 1986)
4-連結lineグラフはハミルトンサイクルを持つ。

lineグラフはclaw-freeグラフになるので、Thomassen予想の仮定はMatthews and Sumnerの予想の仮定より強い。

しかしながら、この2つの予想が同値であることが示された。

19

Ryjacek closure

予想 (Matthews and Sumner, 1984)
4-連結claw-freeグラフはハミルトンサイクルを持つ。

予想 (Thomassen, 1986)
4-連結lineグラフはハミルトンサイクルを持つ。

lineグラフはclaw-freeグラフになるので、Thomassen予想の仮定はMatthews and Sumnerの予想の仮定より強い。
しかしながら、この2つの予想が同値であることが示された。

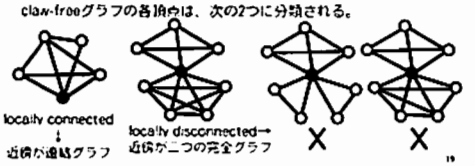
定理 (Ryjacek, 1997)
全ての4-連結lineグラフがハミルトンサイクルを持つ時、
全ての4-連結claw-freeグラフはハミルトンサイクルを持つ。

20

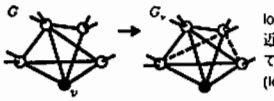
Ryjacek closure

定理 (Ryjacek, 1997)
全ての4-連結lineグラフがハミルトンサイクルを持つ時、
全ての4-連結claw-freeグラフはハミルトンサイクルを持つ。

証明には、Ryjacek 閉包 (closure) と呼ばれるグラフの変形操作を用いる。
claw-freeグラフの各頂点は、次の2つに分類される。



Ryjacek closure

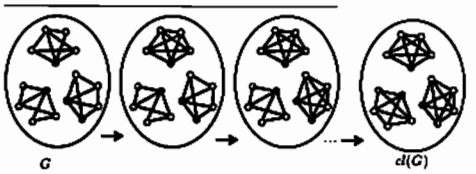


locally connected vertex v の近傍間全てに辺を加えてできるグラフをG_vとする。
(local completion操作)

定理 (Ryjacek, 1997)
G: claw-free, v: locally connected vertex とする。
G_vがハミルトンサイクルを持つならば、Gはハミルトンサイクルを持つ。

一般的には辺を加えると新たなハミルトンサイクルが生じる可能性があるが、この操作においてはそのようなことは起きない。

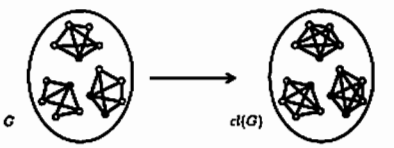
Ryjacek closure



定理 (Ryjacek, 1997)
G: claw-freeのとき、そのclosure $cl(G)$は一意に定まる。
さらに、あるtriangle-freeグラフHが存在して、
$cl(G)=L(H)$ となる。

(closureはline graphになる。)

Ryjacek closure



G… 4-連結 claw-free graph　　$cl(G)$… 4-連結 line graph

ハミルトンサイクルを持つ ⟵ ハミルトンサイクルを持つ

定理 (Ryjacek, 1997)
全ての4-連結lineグラフがハミルトンサイクルを持つ時、
全ての4-連結claw-freeグラフはハミルトンサイクルを持つ。

dominating closed trail

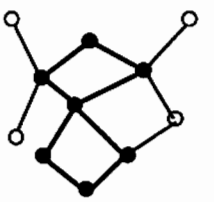
以上の議論より、lineグラフのハミルトン性を調べればよいことがわかった。

lineグラフのハミルトン性を調べる際に、次の定理が非常に有用である。

定理 (Harary and Nash-Williams, 1965)
グラフGがdominating closed trail を持つ。
⇔ $L(G)$がハミルトンサイクルを持つ。

dominating closed trail

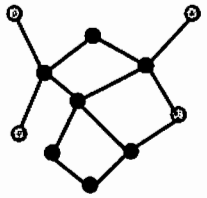
定理 (Harary and Nash-Williams, 1965)
グラフGがdominating closed trail を持つ。
⇔ $L(G)$がハミルトンサイクルを持つ。



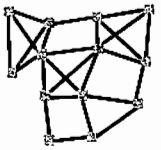
closed trail…同じ辺を二度通らないように辺を辿っていき、元の頂点に戻る回路。
(全ての辺を通らなくてもよい)

dominating
… 「全ての辺が接している」

dominating closed trail



G



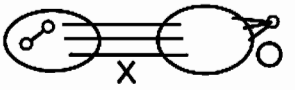
L(G)

essentially 4-辺連結 ⟷ 4-連結
dominating closed trail ⟷ ハミルトンサイクル

25

essential edge-connectivity

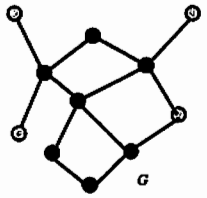
グラフ*G*がessentially 4-辺連結
⇔どの3辺(以下)を取り除いても、どちらも辺を持つような2つのグラフに分断されない。



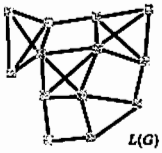
(次数3以下の点の存在が許されるような4-辺連結グラフ)

26

dominating closed trail



G



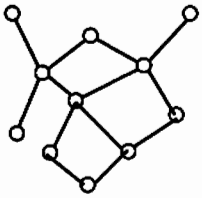
L(G)

dominating closed trail ⟷ ハミルトンサイクル
essentially 4-辺連結 ⟷ 4-連結

全てのessentially 4-辺連結グラフがdominating closed trailを持つことが示されれば、予想の解決になる。

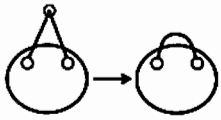
27

core



essentially 4-辺連結グラフを扱う上で、次数1や2の点は扱いにくい。
→消してしまおう！

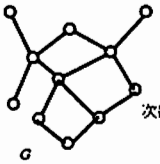
次数1の点…除去



次数2の点…縮約

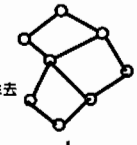
28

core



G

次数1の点…除去



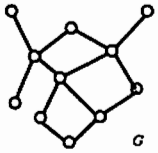
次数2の点…縮約

※*core*(*G*)は、点の除去・辺の縮約の順番に関わらず一意に定まる。

core(*G*)

29

core



G

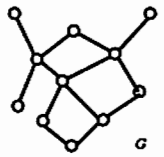
core(*G*)

essentially 4-辺連結
dominating closed trail ⟵
essentially 4-辺連結、最小次数3以上
spanning closed trail

spanning closed trail…全ての頂点を通る closed trail

30

core



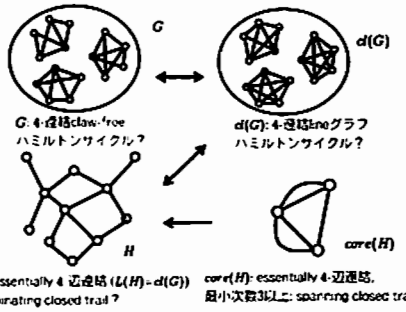
essentially 4-辺連結

dominating closed trail ←

essentially 4-辺連結、
最小次数3以上
spanning closed trail

全ての最小次数3以上のessentially 4-辺連結グラフがspanning closed trailを持つことが示されれば、予想の解決になる。

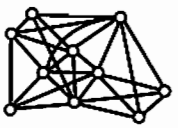
ここまでの話のまとめ



Edge-disjoint spanning trees

少し話題を変えて…

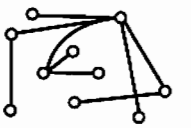
- tree … サイクルを持たないグラフ
- グラフのspanning tree
  … 全ての頂点を覆うtree

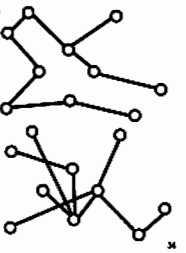


Edge-disjoint spanning trees

少し話題を変えて…

- tree … サイクルを持たないグラフ
- グラフのspanning tree
  … 全ての頂点を覆うtree

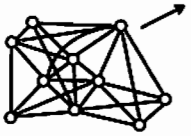




Edge-disjoint spanning trees

少し話題を変えて…

- tree … サイクルを持たないグラフ
- グラフのspanning tree
  … 全ての頂点を覆うtree



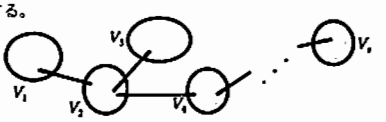
3つのedge-disjoint
spanning trees を持つ

一般に、グラフがk個の
edge-disjoint spanning trees を
持つための条件は？

Edge-disjoint spanning trees

グラフがk個の edge-disjoint spanning trees を持つための条件

頂点集合を、適当にs個に分割したものを$S=V_1 \cup V_2 \cup \cdots \cup V_s$
とする。



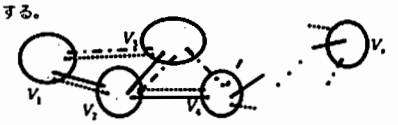
Tをこのグラフのspanning tree とすると、どのV_iにおいても
V_iと他のV_jとを結ぶTの辺が存在する。

Tの辺のうち、Sをまたぐ辺は$s-1$本以上。

Edge-disjcint spanning trees

グラフがk個の edge-disjoint spanning trees を持つための条件

頂点集合を、適当にs個に分割したものを$S=V_1 \cup V_2 \cup \cdots \cup V_s$とする。



Tの辺のうち、Sをまたぐ辺は$s-1$本以上。

グラフがk個のedge-disjointなspanning treeを持つ時、
Sをまたぐ辺は必ず$k(s-1)$本以上存在。→自明な必要条件

Edge-disjoint spanning trees

グラフがk個のedge-disjointなspanning treeを持つ時、
Sをまたぐ辺は必ず$k(s-1)$本以上存在。→自明な必要条件

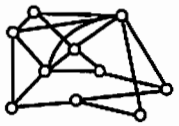
この自明な必要条件が、実は十分条件になる。

定理 (Nash-Williams and Tutte, 1961)
グラフがk個のedge-disjoint spanning treesを持つための
必要十分条件は、そのグラフの任意の分割S ($|S|=s$)に対し
Sをまたぐ辺が$k(s-1)$本以上存在することである。

Edge-disjoint spanning trees

spannning closed trail と edge-disjoint spanning trees の関係は？

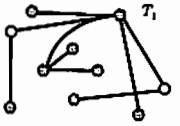
グラフが2個のedge-disjoint spanning treesを持つ時、
そのグラフはspanning closed trail を持つ。

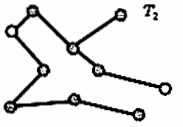


Edge-disjoint spanning trees

spannning closed trail と edge-disjoint spanning trees の関係は？

グラフが2個のedge-disjoint spanning treeを持つ時、
そのグラフはspanning closed trail を持つ。





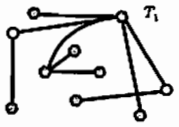
赤…次数が奇数の点

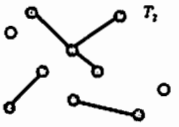
うまく辺を除くと、赤点のみ
次数を奇数にできる

Edge-disjoint spanning trees

spannning closed trail と edge-disjoint spanning trees の関係は？

グラフが2個のedge-disjoint spanning treeを持つ時、
そのグラフはspanning closed trail を持つ。





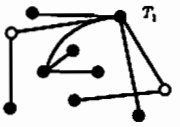
赤…次数が奇数の点

うまく辺を除くと、赤点のみ
次数を奇数にできる

Edge-disjoint spanning trees

spannning closed trail と edge-disjoint spanning trees の関係は？

グラフが2個のedge-disjoint spanning treeを持つ時、
そのグラフはspanning closed trail を持つ。

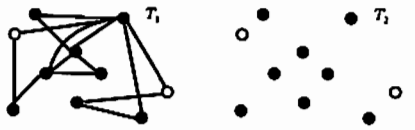


どの頂点も次数が偶数なので
spanning closed trailを持つ

Edge-disjoint spanning trees

spannning closed trail と edge-disjoint spanning trees の関係は？

グラフが2個のedge-disjoint spanning treeを持つ時、
そのグラフはspanning closed trail を持つ。



どの頂点も次数が偶数なので
spanning closed trailを持つ

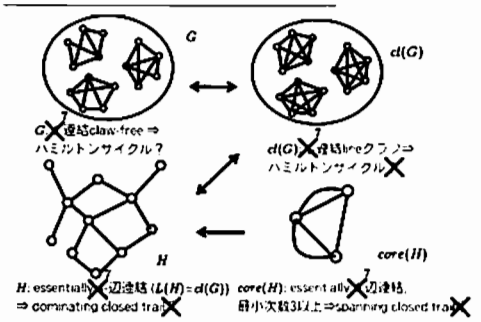
Edge-disjoint spanning trees

グラフが2個のedge-disjoint spanning treeを持つ時、
そのグラフはspanning closed trail を持つ。

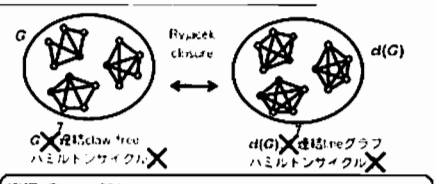
定理 (Nash-Williams and Tutte, 1961)
グラフがk個のedge disjoint spanning treesを持つための
必要十分条件は、そのグラフの任意の分割S ($|S|=s$)に対し
Sをまたぐ辺が$k(s-1)$本以上存在することである。

きちんと計算すると…
Essentially 7-edge connected, 最小次数3以上のグラフは
任意の分割Sに対し、Sをまたぐ辺が$2(s-1)$本以上存在。
→spanning closed trail を持つ。 [Zhan, 1991]

Hamiltonicity of 7-connected claw-free graphs



Hamiltonicity of 7-connected claw-free graphs



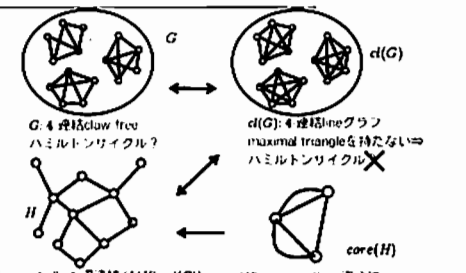
定理 (Zhan, 1991)
7-連結 line グラフはハミルトンサイクルを持つ。

定理 (Ryjacek, 1997)
7-連結 claw-free グラフはハミルトンサイクルを持つ。

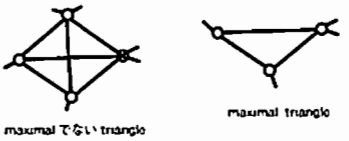
4-connected claw-free graphs without maximal triangles

同様に、きちんと計算すると…
Essentially 4-edge-connected, 最小次数4以上のグラフは
任意の分割Sに対し、Sをまたぐ辺が$2(s-1)$本以上存在。
→spanning closed trail を持つ。

4-connected claw-free graphs without maximal triangles



4-connected claw-free graphs without maximal triangles

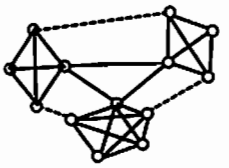


Fact.
Maximal triangle を持たない 4-連結 lineグラフは
ハミルトンサイクルを持つ。

予想の解決に近づくためには、Maximal triangle の周囲の
構造に着目することは自然。

49

New Result



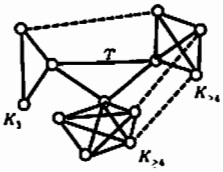
Maximal triangle と隣接する頂点は、3つの完全グラフから
成る。

今回得られた成果…
その3つの完全グラフの間に、ある程度辺があれば
そのようなグラフはハミルトンサイクルを持つ。

50

New Result

定理 (Fujisawa and Ota, 2010+)
G を4-連結 claw-freeグラフとする。
G の任意のMaximal triangle Tに対し、$G[N_G(T)]$が
cyclically-3-connectedの時、Gはハミルトンサイクルを持つ。



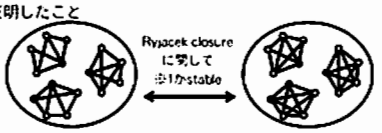
$G[N_G(T)]$が
cyclically-3-connected …
K_3は他の完全グラフに1辺以上
$K_{>4}$は他の完全グラフに2辺以上
辺を出す。

51

New Result

定理 (Fujisawa and Ota, 2010+)
G を4-連結 claw-freeグラフとする。
G の任意のMaximal triangle Tに対し、$G[N_G(T)]$が
cyclically-3-connectedの時、Gはハミルトンサイクルを持つ。
※1

証明したこと



G: 4-連結claw-free
※1を満たす⇒
ハミルトンサイクル?

cl(G): 4-連結lineグラフ
※1を満たす⇒
ハミルトンサイクル

52

New Result

証明したこと

必要十分ではない

dominating closed trail ← spanning closed trail
essentially 4-辺連結 essentially 4-辺連結、
最小次数3以上

必ずしもspanning closed trailは
必要ないので、そのgapをうまく利用した。

53

New Result

定理 (Fujisawa and Ota, 2010+)
G を4-連結 claw-freeグラフとする。
G の任意のMaximal triangle Tに対し、$G[N_G(T)]$が
cyclically-3-connectedの時、Gはハミルトンサイクルを持つ。

定理 (Kaiser et al., 2005)
4-連結claw-freeグラフがHourglass-propertyを満たす時
ハミルトンサイクルを持つ。

定理 (Pfender, 2005)
4-連結claw-free, T_3-freeグラフはハミルトンサイクルを持つ。

54

コンパクト Lie 群上のデザインと符号

奥田 隆幸

1 序

球面上のデザインと符号の理論として知られている理論を, 球面の代わりに別のコンパクト対称空間を舞台として展開できるかというテーマについて考える. 本報告では, 舞台となるコンパクト対称空間として, コンパクト Lie 群を考えた場合に得られた結果を紹介する.

球面上の理論においては, 以下の定理が重要であった.

Fact 1.1 (Delsarte–Goethals–Seidel [6]). d-次元単位球面 S^d 上の有限部分集合 X と自然数 s について, 次のことが成り立つ:

(1) $X \subset S^d$ が $2s$-design なら

$$|X| \geq \binom{d+s}{s} + \binom{d+s-1}{s-1}$$

であり, 等号成立は X が s-distance set であることと同値である.

(2) $X \subset S^d$ が s-distance set なら

$$|X| \leq \binom{d+s}{s} + \binom{d+s-1}{s-1}$$

であり, 等号成立は X が $2s$-design であることと同値である.

球面以外のコンパクト対称空間に対しても, その有限部分集合について design と distance set に対応する概念を定義することによって, この定理の類似と考えられる結果がいくつか知られている. まず, ランク が 1 のコンパクト対称空間に対しては, 球面と平行した理論が展開できることが知られている (Bannai–Hoggar [4] など). ランク が 1 ではない場合については, 実グラスマン多様体上の理論として, Bachoc–Bannai–Coulangeon

[2] において Fact 1.1 に対応する結果が示されている. また, 複素グラスマン多様体での結果 (三浦 [8], Roy [9]) や, ユニタリ群上の結果 (Roy [10]) も知られている.

本報告では, ランクが 1 とは限らないコンパクト対称空間として, 一般のコンパクト Lie 群 G を考えた場合に, その有限部分集合 $X \subset G$ について design と class set の概念を定義することによって, Fact 1.1 の類似の結果が成り立つことを報告する. 特に, これまでに知られていた結果と異なる点として, 自然数 t や s の代わりに, $\widehat{G}$ (G の有限次元既約ユニタリ表現の同型類全体の集合) の有限部分集合 T や S に対して, T-design と S-class set という概念を導入した (§3) ことが挙げられる. 本報告の主結果は以下の定理である:

主定理 (4.2). G をコンパクト Lie 群とする. G の有限部分集合 X と, $\widehat{G}$ の有限部分集合 S に対して, 次のことが成り立つ:

(i) X が $S \otimes S^{-}$-design なら,

$$|X| \geq \sum_{\sigma \in S} (\dim \sigma)^2.$$

ここで等号成立は, X が S-class set となることと同値である.

(ii) X が S-class set であるなら,

$$|X| \leq \sum_{\sigma \in S} (\dim \sigma)^2.$$

ここで等号成立は, X が $S \otimes S^{-}$-design となることと同値である.

本報告の構成を述べておこう. まず, §2 で, コンパクト Lie 群 G の有限次元既約ユニタリ表現 $\sigma \in \widehat{G}$ に付随する行列要素の定義と類関数の定義を述べる. 次に, §3 において, G の有限部分集合 X と $\widehat{G}$ の有限部分集合 T, S に対して, X が T-design, S-class set であることの定義を導入する. §4 で, 本報告の主定理を述べる. 続く §5 では 主定理の証明に必要な準備をし, §6 で, 主定理の証明を述べる. 最後に §7 において, G の共役から, X に可換なアソシエーションスキームの構造が入るための十分条件を述べる.

なお, 本報告の全編を通じて, コンパクト Lie 群の代わりに一般のコンパクトな Hausdorff 位相群を考えても, 全ての結果は同様に成り立つ.

2 行列要素と類関数

G を一般のコンパクト Lie 群とする. この章では, G 上の関数空間についての記号を定義する. この章の内容については, 詳しくは 小林–大島 [7] を参照.

G 上の複素数値連続関数全体の集合を $C(G)$ と書く. 直積群 $G \times G$ の $C(G)$ への作用 $L \times R$ を以下のように定義する:

$(g, g') \in G \times G$, $f \in C(G)$ に対して,

$$(L \times R)(g, g')f : G \to \mathbb{C},\ x \mapsto f(g^{-1}xg') \quad (x \in G)$$

この作用を $G \times G$ の**正則表現**と呼ぶ. また, 正規化された G 上の両側 Haar 測度 を μ とし, μ が誘導する $C(G)$ 上の (エルミート) 内積を

$$\langle f, f' \rangle := \int_G f(x) \cdot \overline{f'(x)}\, d\mu(x) \quad (f, f' \in C(G))$$

によって定義する. このとき $G \times G$ の $C(G)$ への正則表現 $L \times R$ は内積 $\langle\ ,\ \rangle$ を保つ.

$\widehat{G}$ と書いたら, G の有限次元既約ユニタリ表現の同型類全体の集合を表すことにする. 任意の G の既約ユニタリ表現は有限次元であることが知られているから, $\widehat{G}$ は G の既約ユニタリ表現の同型類全体の集合でもある.

2.1 行列要素

G の有限次元既約ユニタリ表現の同型類 $\sigma \in \widehat{G}$ に対応する関数空間 $H^\sigma(G) \subset C(G)$ を, 以下のように定義する.

定義 2.1 (行列要素). $\sigma \in \widehat{G}$ の実現として, 表現空間 V をとり, その正規直交基底 $(v_1, \ldots, v_{\dim \sigma})$ を考える. $x \in G$ について, $\sigma(x)$ を $(v_1, \ldots, v_{\dim \sigma})$ によって行列表示したときの (i, j)-成分を $\sigma_{ij}(x)$ と書くことにすると, $\sigma_{ij} \in C(G)$ である. このような関数を σ の**行列要素**と呼ぶ. また, $\sigma \in \widehat{G}$ に対応する関数空間 $H^\sigma(G) \subset C(G)$ を

$$H^\sigma(G) := \mathbb{C}\text{-span}\{\, \sigma_{ij} \mid 1 \le i, j \le \dim \sigma \,\} \subset C(G)$$

と定義する.

このように定義された関数空間 $H^\sigma(G) \subset C(G)$ は, 実現 V やその正規直交基底 $(v_1, \ldots, v_{\dim \sigma})$ のとり方によらず, 表現の同型類 $\sigma \in \widehat{G}$ のみによって定まる.

このとき, 次の Fact が知られている.

Fact 2.2. 任意の $\sigma \in \widehat{G}$ に対して,

$$\dim H^{\sigma}(G) = (\dim \sigma)^2$$

である. また, 異なる二つの $\sigma, \rho \in \widehat{G}$ について, $H^{\sigma}(G)$ と $H^{\rho}(G)$ は直交する.

Fact 2.3. 各 $\sigma \in \widehat{G}$ に対して、関数空間 $H^{\sigma}(G) \subset C(G)$ は, 正則表現 $L \times R$ で保たれる. この $G \times G$ の $H^{\sigma}(G)$ への表現は $\sigma \boxtimes \overline{\sigma}$ と同型である.

Remark 2.4. 本報告では直接は用いないが, Peter–Weyl の定理により, $\bigoplus_{\sigma \in \widehat{G}} H^{\sigma}(G)$ は $C(G)$ の稠密部分集合であることが知られている. 特に $G \times G$ の $C(G)$ への正則表現 $L \times R$ は無重複である.

2.2 類関数

$C(G)$ の部分空間 $C(G)^{\mathrm{Ad}}$ を

$$C(G)^{\mathrm{Ad}} := \{ F \in C(G) \mid F(gxg^{-1}) = F(x) \ ({}^{\forall}x \in G, \ {}^{\forall}g \in G) \}$$

として定義する. $C(G)^{\mathrm{Ad}}$ の元を**類関数**と呼ぶ. $F \in C(G)$ が類関数であることと, F が G の各共役類上で一定であることは同値である.

$x \in G$ の共役類を $[x] := \{ gxg^{-1} \mid g \in G \} \subset G$ と書くことにし, G の共役類全体の集合を $G/\sim := \{ [x] \mid x \in G \}$ で表すことにする. このとき, 自然な全射

$$G \to G/\sim, \ x \mapsto [x]$$

から, $G/\sim$ に商位相を定義し, $G/\sim$ 上の複素数値連続関数全体のなす空間 $C(G/\sim)$ を考えると, 各類関数 $F \in C(G)^{\mathrm{Ad}}$ に対して, $\tilde{F} : G/\sim \to \mathbb{C}$ を, 任意の $x \in G$ について $\tilde{F}([x]) = F(x)$ と定めることによって, $C(G)^{\mathrm{Ad}}$ は $C(G/\sim)$ と同一視される.

上で定義した類関数の空間 $C(G)^{\mathrm{Ad}}$ の部分空間として, $\sigma \in \widehat{G}$ に関する類関数の空間 $H^{\sigma}(G)^{\mathrm{Ad}} \subset C(G)^{\mathrm{Ad}}$ を次のように定義する.

定義 2.5. $\sigma \in \widehat{G}$ に対して, $H^{\sigma}(G)$ に属する類関数を σ に関する類関数と呼び,

$$H^{\sigma}(G)^{\mathrm{Ad}} := H^{\sigma}(G) \cap C(G)^{\mathrm{Ad}}$$

と書くことにする.

このように定義したとき, $\sigma \in \widehat{G}$ に関する類関数は, 指標 χ_{σ} の定数倍のものしかないことが知られている.

Fact 2.6. 任意の $\sigma \in \widehat{G}$ に対して, $\sigma \in \widehat{G}$ の指標を χ_σ と書けば, $\chi_\sigma \in H^\sigma(G)^{\mathrm{Ad}}$ であり,

$$H^\sigma(G)^{\mathrm{Ad}} = \mathbb{C} \cdot \chi_\sigma$$

が成り立つ. 特に $\dim H^\sigma(G)^{\mathrm{Ad}} = 1$ である.

3 コンパクト Lie 群上の design, code 及び class set の定義

コンパクト Lie 群 G に対して, G の有限次元既約ユニタリ表現の同型類全体の集合を $\widehat{G}$ としていた. この章の目的は, G の有限部分集合 X と, $\widehat{G}$ の有限部分集合 T, S をとったとき, X が T-design であることの定義 (3.2) と, X が S-class set であることの定義 (3.7) を与えることである.

3.1 Design の定義

定義 2.1 において, $\sigma \in \widehat{G}$ に対応する関数空間 $H^\sigma(G) \subset C(G)$ を定義したが, ここでは $\widehat{G}$ の有限部分集合 T について, 以下のように関数空間 $H^T(G) \subset C(G)$ を定める.

定義 3.1. 有限部分集合 $T \subset \widehat{G}$ に対して,

$$H^T(G) := \bigoplus_{\tau \in T} H^\tau(G)$$

とする. このとき, 命題 2.2 より, 上の直和は直交直和であり,

$$\dim H^T(G) = \sum_{\tau \in T} (\dim \tau)^2$$

である.

$\widehat{G}$ の有限部分集合 T について, G の有限部分集合 X が T-design であるということを次のように定義する.

定義 3.2 (T-design). $\widehat{G}$ の有限部分集合 T に対して, G 上の関数空間 $H^T(G)$ を考える (see 定義 3.1). G の有限部分集合 X が T-design であるとは,

$$\int_G f(x)\, d\mu(x) = \frac{1}{|X|} \sum_{x \in X} f(x) \quad (^\forall f \in H^T(G))$$

が成り立つことと定義する.

この定義と同値な条件を述べておく．証明は $H^T(G)$ の定義 (3.1) と命題 2.2 から従う．

命題 3.3. G の 1-次元自明表現を 1_G と書くことにする．有限集合 $X \subset G$, $T \subset \widehat{G}$ に対して，以下の条件は同値である．

(a) X は T-design.

(b) 任意の $\tau \in T \setminus \{1_G\}$, $f_\tau \in H^\tau(G)$ に対して

$$\sum_{x \in X} f_\tau(x) = 0.$$

(c) 任意の $\tau \in T \setminus \{1_G\}$ に対して，その実現を適当にとって，表現空間を V とすると，

$$\sum_{x \in X} \tau(x)v = 0 \quad ({}^\forall v \in V).$$

例 3.4. G としてユニタリ群 $U(2)$ を考える．$U(2)$ を行列群として定義し，$\sigma_0 \in \widehat{G}$ を $U(2)$ の $\mathbb{C}^2$ への自然表現とする．G の有限部分集合 X と，$\widehat{G}$ の有限部分集合 T を

$$X := \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} \}$$

$$T := \{ \tau \in \widehat{G} \mid \tau \text{ は } \sigma_0 \otimes \overline{\sigma_0} \text{ の既約分解に現れる } \}$$

とする．ここで，$U(2)$ の $\mathfrak{sl}(2,\mathbb{C})$ への随伴表現 ($\mathfrak{u}(2)$ への随伴表現の複素化) を $(\mathrm{Ad}_{U(2)})_{\mathbb{C}}$ とすると，$\sigma_0 \otimes \overline{\sigma_0}$ の既約分解は

$$\sigma_0 \otimes \overline{\sigma_0} = 1_{U(2)} \oplus (\mathrm{Ad}_{U(2)})_{\mathbb{C}}$$

となる．X は $(\mathrm{Ad}_{U(2)})_{\mathbb{C}}$ に対して，命題 3.3 の (c) を満たすことが示せるから，X は T-design である．

Remark 3.5. 球面上の理論においては，d-次元単位球面 S^d の有限部分集合 X が，自然数 t に対して t-design であることを，

$$\frac{1}{|S^d|} \int_{S^d} f(x)dx = \frac{1}{|X|} \sum_{x \in X} f(x) \quad ({}^\forall f \in \bigoplus_{i=0}^{t} \mathrm{Harm}_i(S^d))$$

としていた (ただし，$\mathrm{Harm}_i(S^d)$ は $\mathbb{R}^{d+1}$ 上の斉 i 次調和多項式を制限して得られる S^d 上の連続関数全体のなす関数空間としている)．この場合，指定された自然数 t 対して，関数空間 $\bigoplus_{i=0}^{t} \mathrm{Harm}_i(S^d)$ を考えていることになるが，今回の G 上の design の定義においては，自然数 t の代わりに $\widehat{G}$ の部分集合 T を指定し，T に対応する関数空間として，$H^T(G) := \bigoplus_{\tau \in T} H^\tau(G)$ を考えていることになる．

3.2 Code 及び class set の定義

定義 2.5 において, $\sigma \in \widehat{G}$ に関する類関数の集合 $H^{\sigma}(G)^{\mathrm{Ad}}$ を定義したが, $\widehat{G}$ の有限部分集合 S に対して, S に関する類関数の集合を以下のように定義する.

定義 3.6. $\widehat{G}$ の有限部分集合 S に対して, S に関する類関数の集合 $H^{S}(G)^{\mathrm{Ad}}$ を

$$H^{S}(G)^{\mathrm{Ad}} := \bigoplus_{\sigma \in S} H^{\sigma}(G)^{\mathrm{Ad}} \subset H^{S}(G)$$

として定義する ($H^{S}(G)$ の定義については, 定義 3.1 を参照). 特に Fact 2.6 より

$$H^{S}(G)^{\mathrm{Ad}} = \mathbb{C}\text{-span}\{\, \chi_{\sigma} \mid \sigma \in S \,\}$$

である.

類関数 $F \in H^{S}(G)^{\mathrm{Ad}}$ と, $\widehat{G}$ の有限部分集合 S について, 有限集合 $X \subset G$ が F-code であることと, S-class set であることを, 以下のように定義する.

定義 3.7 (F-code, S-class set). 類関数 $F \in C(G)^{\mathrm{Ad}}$ (see 定義 2.5) に対して, G の有限部分集合 X が F-code であるとは,

$$F(x^{-1}y) = |X| \cdot \delta_{xy} \quad ({}^{\forall}x, y \in X)$$

となることとする (ただし δ_{xy} はクロネッカーのデルタとしている). 更に, $\widehat{G}$ の有限部分集合 S に対して, X が S-class set であるとは, ある S についての類関数 $F \in H^{S}(G)^{\mathrm{Ad}}$ (see 定義 3.6) が存在して, X が F-code であることと定義する.

例 3.8. G としてユニタリ群 $U(2)$ を考える. $U(2)$ を行列群として定義し, $\sigma_0 \in \widehat{G}$ を $U(2)$ の $\mathbb{C}^2$ への自然表現とする. G の有限部分集合 X と $\widehat{G}$ の有限部分集合 S を,

$$X := \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} \}$$
$$S := \{ \sigma_0 \}$$

とする. このとき, 類関数 $F = 2 \cdot \chi_{\sigma_0} = 2 \cdot \mathrm{Trace}_{U(2)} \in H^{\sigma_0}(U(2))$ を考えれば X は F-code であり, 従って S-class set である.

この定義について少し補足しておく. いま, G の共役類全体の集合を $G/\sim$ としていた (see §2.2). G の有限部分集合 X に対して, $G/\sim$ の有限部分集合 $A(X)$ を

$$A(X) := \{\, [x^{-1}y] \in G/\sim \mid x, y \in X,\ x \neq y \,\}$$

とすれば, $F \in C(G)^{\mathrm{Ad}}$ に対して X が F-code であることは, $A(X)$ が $\tilde{F} \in C(G/\sim)$ (see §2.2) の零点集合に含まれていて, $\tilde{F}([e]) = |X|$ となることに他ならない.

Remark 3.9. 球面上の理論において, d-次元単位球面 S^d 上の有限部分集合 X が, 自然数 s に対して s-distance set であるとは, 閉区間 $[-1,1]$ の有限部分集合 $A(X)$ を

$$A(X) := \{ \langle x,y \rangle_{\mathbb{R}^{d+1}} \mid x,y \in X,\ x \neq y \} \quad (\langle\ ,\ \rangle_{\mathbb{R}^{d+1}} \text{は } \mathbb{R}^{d+1} \text{ の標準内積としている})$$

としたとき, $|A(X)| = s$ であることとして定義される. このとき, $A(X)$ の零化関数 $\tilde{F}$ ($[-1,1]$ 上の関数で, $A(X)$ を零点集合に含むもの) として, s-次多項式 $\tilde{F}$ が存在する. 今回の G 上の S-class set の定義においては,

$$\langle x,y \rangle_{\mathbb{R}^{d+1}} \in [-1,1] \quad (x,y \in S^d)$$

の代わりに

$$[x^{-1}y] \in G/\sim \quad (x,y \in G)$$

を考える (単位球面 S^d への $O(d)$ の自然な左作用を考えたとき, その商空間は閉区間 $[-1,1]$ と同一視できることに注意). 更に, $[-1,1]$ 上の s-次多項式 $\tilde{F}$ の代わりに, $F \in H^S(G)^{\mathrm{Ad}}$ が誘導する $G/\sim$ 上の関数 $\tilde{F}$ を考え, "$A(X) \subset G/\sim$ の零化関数 $\tilde{F}$ で, $F \in H^S(G)^{\mathrm{Ad}}$ から誘導されるものが存在する" ということとして, S-class set を定義している.

4 主定理

G をコンパクト Lie 群とし, $\widehat{G}$ を G の有限次元既約ユニタリ表現の同型類全体の集合とする. 本報告の主定理を述べるために, $\widehat{G}$ の有限部分集合の族について, 以下のように共役とテンソルを定義しておく:

定義 4.1. $\widehat{G}$ の有限部分集合 $S \subset \widehat{G}$ について, その共役 $S^- \subset \widehat{G}$ を,

$$S^- := \{ \overline{\sigma} \mid \sigma \in S \}$$

と表す (ただし $\overline{\sigma} \in \widehat{G}$ は $\sigma \in \widehat{G}$ の共役表現としている). また, 二つの有限部分集合 $S_1, S_2 \subset \widehat{G}$ に対して, そのテンソル $S_1 \otimes S_2 \subset \widehat{G}$ を,

$$S_1 \otimes S_2 := \{ \tau \in \widehat{G} \mid {}^{\exists}\sigma_1 \in S_1,\ {}^{\exists}\sigma_2 \in S_2 \ \text{ s.t. } \tau \text{ は } \sigma_1 \otimes \sigma_2 \text{ の既約分解に現れる} \}$$

と書くことにする.

この定義における $S^-, S_1 \otimes S_2 \subset \widehat{G}$ は有限集合であり, 定義 3.1 の意味で, 関数空間 $H^{S^-}(G)$ や $H^{S_1 \otimes S_2}(G)$ などが定義される (これらの関数空間の性質については, 命題 5.1 を参照).

本報告の主定理を述べる.

主定理 4.2. X を G の有限部分集合とし, S を $\widehat{G}$ の有限部分集合とする. このとき以下の事が成り立つ.

(i) X が $S \otimes S^-$-design (see 定義 3.2 and 定義 4.1) なら,

$$|X| \geq \sum_{\sigma \in S} (\dim \sigma)^2.$$

ここで等号成立は, X が S-class set (see 定義 3.7) となることと同値である.

(ii) X が S-class set であるなら,

$$|X| \leq \sum_{\sigma \in S} (\dim \sigma)^2.$$

ここで等号成立は, X が $S \otimes S^-$-design となることと同値である.

例 4.3. 例 3.8 において, $G = U(2)$ に対して, 有限集合 $X \subset G$, $S \subset \widehat{G}$ を,

$$X := \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} \}$$
$$S := \{ \sigma_0 \}$$

としていた (ただし, $\sigma_0 \in \widehat{G}$ を $U(2)$ の $\mathbb{C}^2$ への自然表現とする). このとき $S \otimes S^-$ は, 例 3.4 における $T \subset \widehat{G}$ と一致するから, X は $S \otimes S^-$-design かつ S-class set となる. この S に対して $\sum_{\sigma \in S} (\dim \sigma)^2 = 4 = |X|$ であるから, 主定理における等号が成立していることが分かる.

Remark 4.4. 球面上の理論においては, d-次元単位球面 S^d の有限部分集合 $X \subset S^d$ と自然数 s について, Fact 1.1 が成り立つのであった. Fact 1.1 の不等式の等号が成立している場合, つまり $X \subset S^d$ が $2s$-design かつ s-distance set である場合 (このような $2s$-design は tight と呼ばれる) には, S^d の距離から, X に可換な Q-多項式アソシエーションスキームの構造が入ることが知られている (Delsarte–Goethals–Seidel [6], 坂内–坂内 [1, 第 7 章] にも詳しい解説がある). しかし, 今回の主定理においての不等式の等号が成立している場合, つまり $X \subset G$ が $S \otimes S^-$-design かつ S-distance set である場合

に, G の共役から, X にアソシエーションスキームの構造が入るかについては分かっていない. このことに関連して, X に可換なアソシエーションスキームの構造が入るための十分条件を §7 で述べる.

5 主定理の証明の準備

この章では, 主定理 4.2 の証明の準備として, $\widehat{G}$ の有限部分集合についての共役, テンソル (see 定義 4.1) に対応する関数空間についての命題 (後述の命題 5.1) を述べ, また, 各 $\sigma \in \widehat{G}$ に対して, ある性質を満たす関数 $K^\sigma \in H^\sigma(G)$ を定義し, それの性質 (後述の命題 5.7, 命題 5.4) について述べる. なお, この章の命題の詳しい証明は省略する.

$\widehat{G}$ の有限部分集合について, 定義 3.1 で対応する関数空間を定義した. また, 定義 4.1 では有限部分集合の間の共役とテンソルを定義していた. これらについて, 次の命題が成り立つ:

命題 5.1. 有限集合 $S \subset \widehat{G}$ に対して

$$H^{S^-}(G) = \{\overline{f} \mid f \in H^S(G)\}$$

が成り立つ (ただし, $\overline{f}$ は関数としての複素共役としている). また, 二つの有限集合 $S_1, S_2 \subset \widehat{G}$ に対して,

$$H^{S_1 \otimes S_2}(G) = \mathbb{C}\text{-span}\{f_1 \cdot f_2 \mid f_1 \in H^{S_1}(G),\ f_2 \in H^{S_2}(G)\}$$

が成り立つ (ただし, $f_1 \cdot f_2$ は関数としての積としている).

Remark 5.2. この命題の証明の難しい点は, 後半の等式において, 左辺が右辺を張ることを示すことである. このことの証明は, 行列要素の定義から直接得ることもできるが, 指標の性質

$$\chi_{\sigma \otimes \rho} = \chi_\sigma \cdot \chi_\rho$$

に注目することによっても証明できる (ここでは省略する).

各 $\sigma \in \widehat{G}$ に対して, 行列要素の張る関数空間 $H^\sigma(G) \subset C(G)$ を定義したが, この $H^\sigma(G)$ に属する G 上の関数 K^σ を次のように定義する.

定義 5.3. $\sigma \in \widehat{G}$ に対して, $K^\sigma \in H^\sigma(G)$ を

$$(f^\sigma, K^\sigma) = f^\sigma(e) \quad (^\forall f^\sigma \in H^\sigma(G))$$

を満たすものとして定める ($H^\sigma(G)$ は有限次元内積空間なので, このような K^σ は一意的に存在する). また, $\widehat{G}$ の有限部分集合 S に対して,

$$K^S := \sum_{\sigma \in S} K^\sigma$$

と定める.

次の命題でみるように, 各 $\sigma \in \widehat{G}$ に対して, K^σ は類関数である.

命題 5.4. 任意の $\sigma \in \widehat{G}$ に対して, $K^\sigma \in H^\sigma(G)$ は類関数であり,

$$K^\sigma = (\dim \sigma) \cdot \chi_\sigma$$

が成り立つ. 特に, $H^\sigma(G)^{\mathrm{Ad}} = \mathbb{C} \cdot K^\sigma$ となる.

次の系は上の命題から直ちに従う.

系 5.5. 任意の $\sigma \in \widehat{G}$ に対して, $K^\sigma(e) = (\dim \sigma)^2$.

ここで, 一般の類関数 $F \in C(G)^{\mathrm{Ad}}$, $x \in G$ に対して, $F_x \in C(G)$ を次のように定義しておく.

定義 5.6. 類関数 $F \in C(G)^{\mathrm{Ad}}$ を固定する. $x \in G$ に対して, $(g, g') \in G \times G$ を

$$g \cdot (g')^{-1} = x$$

となるようにとる. ここで $F_x \in C(G)$ を, 正則表現 $L \times R$ を用いて

$$F_x = (L \times R)(g, g')F \in H^\sigma(G)$$

と定義する.

このとき, $F_x \in C(G)$ は $g \cdot (g')^{-1} = x$ となる $(g, g') \in G \times G$ のとり方によらないことと, 任意の $x, y \in G$ に対して, $F_x(y) = F(x^{-1}y)$ であることを注意しておく.

この定義を用いて, $\sigma \in \widehat{G}$, $x \in G$ に対して K^σ_x を考えれば, K^σ_x は $H^\sigma(G)$ の関数に x を代入させる性質を持つ.

命題 5.7 (K^σ の reproducing property). 任意の $\sigma \in \widehat{G}$, $x \in G$ に対して, $K^\sigma_x \in H^\sigma(G)$ (see 定義 5.6) を考える. このとき,

$$\langle f^\sigma, K^\sigma_x \rangle = f^\sigma(x) \quad ({}^\forall f^\sigma \in H^\sigma(G))$$

が成り立つ. また $\rho \in \widehat{G}$ が $\rho \neq \sigma$ なら,

$$\langle f^\rho, K_x^\sigma \rangle = 0 \quad (^\forall f^\rho \in H^\rho(G))$$

である.

上の命題は, 正則表現 $L \times R$ が内積を保つこと, $\sigma \in \widehat{G}$ に対する $K^\sigma \in H^\sigma(G)^{\mathrm{Ad}}$ の定義, $\sigma, \rho \in \widehat{G}$ に対して $H^\sigma(G)$ と $H^\rho(G)$ が直交する (see 命題 2.2) ことから得られる.

この命題から次の系が従う.

系 5.8. 有限部分集合 $S \subset \widehat{G}$ に対して, $K^S := \sum_{\sigma \in S} K^\sigma$ としていたが, 任意の $x \in G$ に対して

$$\langle f, K_x^S \rangle = f(x) \quad (^\forall f \in H^S(G))$$

が成り立つ.

6 主定理の証明

この章では主定理の証明を述べる.

設定と記号を整理しておこう.

設定 6.1. G を一般のコンパクト Lie 群, X を G の有限部分集合とする. また G の有限次元既約ユニタリ表現の同型類全体のなす集合を $\widehat{G}$ と書き, S を $\widehat{G}$ の有限部分集合とする.

これまでに定義した記号をまとめておく:

- μ : 正規化された G 上の両側 Haar 測度.
- $C(G)$: G 上の C^∞ 級複素数値関数全体のなす集合.
- $\langle\ ,\ \rangle : C(G) \times C(G) \to \mathbb{C}$: μ から誘導される $C(G)$ 上の内積.
- $H^\sigma(G) \subset C(G)$: $\sigma \in \widehat{G}$ の行列要素の張る G 上の関数空間 (see 定義 2.1).
- $H^\sigma(G)^{\mathrm{Ad}} \subset H^\sigma(G)$: $\sigma \in \widehat{G}$ に関する類関数の空間 (see 定義 2.5).
- $K^\sigma \in H^\sigma(G)^{\mathrm{Ad}}$ (see 定義 5.3)
- $K_x^\sigma \in H^\sigma(G)$ (see 定義 5.3 and 定義 5.6).
- $H^S(G) := \bigoplus_{\sigma \in S} H^\sigma(G) \subset C(G)$: $S \subset \widehat{G}$ に対応する関数空間 (see 定義 3.1).
- $H^S(G)^{\mathrm{Ad}} := \bigoplus_{\sigma \in S} H^\sigma(G)^{\mathrm{Ad}} \subset H^S(G)$: $S \subset \widehat{G}$ に関する類関数の空間 (see 定義 3.6).

- $K^S := \sum_{\sigma \in S} K^\sigma \in H^S(G)^{\mathrm{Ad}}$ (see 定義 5.3).

6.1 主定理の証明のアイディア

まず, 有限集合 X 上の関数空間 $C(X)$ を次のように定義する.

定義 6.2. 有限集合 X について, X 上の複素数値関数全体の集合を

$$C(X) := \mathrm{Map}(X, \mathbb{C})$$

と書くことにする. $x \in X$ に対して $\delta_x \in C(X)$ を

$$\delta_x : X \to \mathbb{C},\ y \mapsto \delta_{xy}$$

と定義する (ただし, δ_{xy} はクロネッカーのデルタとしている) と, $\{\, \delta_x \mid x \in X \,\}$ は $C(X)$ の基底を成す. 特に $C(X)$ は $|X|$-次元複素ベクトル空間である. また, $C(X)$ 上の (エルミート) 内積を

$$(\xi, \eta)_{C(X)} := \frac{1}{|X|} \sum_{x \in X} \xi(x) \cdot \overline{\eta(x)} \quad (\xi, \eta \in C(X))$$

によって定義する.

設定 6.1 において, $H^S(G)$ と $C(X)$ の間の線形写像 $r : H^S(G) \to C(X)$ と, $F \in H^S(G)^{\mathrm{Ad}}$ に対して, 線形写像 $q^F : C(X) \to H^S(G)$ を以下のように定義する.

定義 6.3. 関数空間 $H^S(G)$ から $C(X)$ への制限写像を

$$r : H^S(G) \to C(X),\ f \mapsto f|_X \quad (f \in H^S(G))$$

と書くことにする. また S に関する類関数 $F \in H^S(G)^{\mathrm{Ad}}$ に対して, $C(X)$ から $H^S(G)$ への線形写像 q^F を

$$q^F : C(X) \to H^S(G),\ \xi \mapsto \frac{1}{|X|} \sum_{x \in X} \xi(x) \cdot F_x \quad (\xi \in C(X))$$

として定義する ($F_x \in H^S(G)$ の定義については, 定義 5.6 を参照).

このとき次の三つの命題 6.4, 6.5, 6.6 が成り立つ.

命題 6.4. 設定 6.1 において, 以下の三条件は同値である:

(D-1) X は $S \otimes S^{-}$-design.
(D-2) 制限写像 $r : H^S(G) \to C(X)$ は内積を保つ.
(D-3) $q^{K^S} \circ r = \mathrm{id}_{C(G)}$.

特に, 上記の条件を満たすとき, 制限写像 $r : H^S(G) \to C(X)$ は単射である.

命題 6.5. 設定 6.1 において, S についての類関数 $F \in H^S(G)^{\mathrm{Ad}}$ について, 以下の二条件は同値である:

(C-1) X は F-code.
(C-2) $r \circ q^F = \mathrm{id}_{C(X)}$.

特に, 上記の条件を満たすとき, 制限写像 $r : H^S(G) \to C(X)$ は全射である.

命題 6.6. 設定 6.1 において, S に関する類関数 $F \in H^S(G)^{\mathrm{Ad}}$ について, $q^F : C(X) \to H^S(G)$ が $r : H^S(G) \to C(X)$ の逆写像になるなら, $F = K^S$ である.

これら命題 6.4, 6.5, 6.6 を用いて主定理を証明しよう.

主定理 4.2 の証明. まず, $\dim H^S(G) = \sum_{\sigma \in S} (\dim \sigma)^2$ (see 定義 3.1), $\dim C(X) = |X|$ (see 定義 6.2) であることに注意しておく.

(i), (ii) の不等式の証明

X が $S \otimes S^{-}$-design であれば, 命題 6.4 より, $r : H^S(G) \to C(X)$ は単射であるから

$$\dim H^S(G) \leq \dim C(X).$$

が成り立つ (特に, 等号が成立する事と, r が q^{K^S} の逆写像になることは同値). 従って $\sum_{\sigma \in S} (\dim \sigma)^2 \leq |X|$ である. また, X が S-class set とすると, 定義より X が F-code となる $F \in H^S(G)^{\mathrm{Ad}}$ が存在する. 命題 6.5 より, $r : H^S(G) \to C(X)$ は全射であるから,

$$\dim H^S(G) \geq \dim C(X).$$

が成り立つ (特に, 等号が成立する事と, r が q^F の逆写像になることは同値). 従って $\sum_{\sigma \in S} (\dim \sigma)^2 \geq |X|$ である.

(i), (ii) の等号成立条件の証明. 主定理の等号成立条件の主張は, $X \subset G$, $S \subset \widehat{G}$ についての次の三つの条件

- X が $S \otimes S^{-}$-design.
- X が S-class set.

- $|X| = \sum_{\sigma \in S} (\dim \sigma)^2$.

の内, どれか二つが成り立つなら, 残ったもう一つの条件も自動的に成り立つということである. これを証明しよう. まず, X が $S \otimes S^-$-design かつ S-class set なら, 上で示した二つの不等式より $|X| = \sum_{\sigma \in S} (\dim \sigma)^2$ である. また X が $S \otimes S^-$-design かつ $|X| = \sum_{\sigma \in S} (\dim \sigma)^2$ であれば, 上記の一つ目の不等式の証明より, q^{K^S} は r の逆写像でなければならない. 従って補題 6.5 から X は K^S-code である. 特に X は S-class set となる. 最後に, X が S-class set かつ $|X| = \sum_{\sigma \in S} (\dim \sigma)^2$ が成立しているとする. S-class set の定義より, X が F-code となる $F \in H^S(G)^{\mathrm{Ad}}$ が存在するが, 上記の二つ目の不等式の証明より, q^F が r の逆写像でなければならない. 従って命題 6.6 より $F = K^S$ であるから, 補題 6.4 から X が $S \otimes S^-$-design となることが分かる. □

従って, 命題 6.4, 6.5, 6.6 を示せば, 主定理の証明が完成する.

6.2 命題 6.4, 命題 6.5 の証明

これより命題 6.4, 6.5 の証明を行う. 命題 6.6 については §6.3 で証明のアイディアを述べる.

命題 6.4 の証明. (D-1) ⇔ (D-2) の証明.

命題 5.1 から, X が $S \otimes S^-$-design であることと, 任意の $f, f' \in H^S(G)$ について

$$\int_G (f \cdot \overline{f'})(x)\, d\mu(x) = \frac{1}{|X|} \sum_{x \in X} (f \cdot \overline{f'})(x)$$

となることは同値である. $H^S(G)$ と $C(X)$ の内積の定義を考えれば, これは制限写像 $r : H^S(G) \to C(X)$ が内積を保つことと同値である.

(D-2) ⇔ (D-3) の証明.

一般に, $f \in H^S(G)$ に対して $(q^{K^S} \circ r) f = \frac{1}{|X|} \sum_{x \in X} f(x) \cdot K_x^S$ である事と, 系 5.8 に注意すると, 任意の $f' \in H^S(G)$ に対して

$$\langle (q^{K^S} \circ r)(f), f' \rangle = \langle r(f), r(f') \rangle_{C(X)}$$

が成り立つことが分かる. 従って $q^{K^S} \circ r = \mathrm{id}_{H^S(G)}$ と, 任意の $f, f' \in H^S(G)$ に対して

$$\langle f, f' \rangle = \langle r(f), r(f') \rangle_{C(X)}$$

となることは同値であり, つまり制限写像 $r : H^S(G) \to C(X)$ が内積を保つことと同値である. □

命題 6.5 の証明. 一般に, $x, y \in X$ に対して,

$$(r \circ q^F)(\delta_x)(y) = \frac{1}{|X|} F(x^{-1}y)$$

であることに注意する (see 定義 5.6). $\{\, \delta_x \mid x \in X \,\}$ が $C(X)$ の基底をなすことに注意すると, $r \circ q^F = \mathrm{id}_{C(X)}$ が成り立つことと, X が F-code であること, すなわち任意の $x, y \in X$ に対して

$$\delta_x(y) = \frac{1}{|X|} F(x^{-1}y)$$

が成り立つことは同値である. □

これで, 主定理の証明を完成させるには, 命題 6.6 を示せばよいことになった. 命題 6.6 の証明については次の §6.3 でアイディアを述べる.

6.3 命題 6.6 の証明のアイディア

この章では, 以降は次の設定で考える:

設定 6.7. 設定 6.1 に加え, S に関する類関数 $F \in H^S(G)^{\mathrm{Ad}}$ について, X が $r \circ q^F = \mathrm{id}_{C(X)}$ であるとする.

一般に $\sigma \in S$ に対して, $H^\sigma(G)^{\mathrm{Ad}} = \mathbb{C} \cdot K^\sigma$ であった (see 命題 5.4). 従って $F \in H^S(G)^{\mathrm{Ad}}$ に対して, $c_\sigma \in \mathbb{C}$ $(^\forall \sigma \in S)$ が存在して,

$$F = \sum_{\sigma \in S} c_\sigma K^\sigma$$

と書ける. 命題 6.6 の主張は, 設定 6.7 において, 更に $q^F \circ r = \mathrm{id}_{H^S(G)}$ を仮定すると, 任意の $\sigma \in S$ に対して $c_\sigma = 1$ となるということに他ならない.

命題 6.6 の証明には, 以下の補題 6.8, 6.9 を用いる.

補題 6.8. 設定 6.7 において, 全ての $\sigma \in S$ に対して c_σ が非負実数なら,

$$0 \leq c_\sigma \leq 1 \quad (^\forall \sigma \in S).$$

補題 6.9. 設定 6.7 において, 更に $q^F \circ r = \mathrm{id}_{H^S(G)}$ ならば, 任意の $\sigma \in S$ に対して, c_σ は非負実数である.

この二つの補題の証明はここでは省略する. これらを用いて命題 6.6 の証明を述べる.

命題 6.6 の証明. まず設定 6.7 において, $F(e)$ を二通りの方法で計算しよう (ただし $e \in G$ は G の単位元としている). 任意の $x \in X$ に対して, $F(e) = F_x(x)$ であること (see 定義 5.6), $|X| \cdot q^F(\delta_x) = F_x$ であること (see 定義 6.3), 更に $r \circ q^F = \mathrm{id}_{C(X)}$ の仮定に注意すれば, $F(e) = |X|$ が分かる. また, $F = \sum_{\sigma \in S} c_\sigma K^\sigma$ と書いたが, 一般に $\sigma \in \widehat{G}$ について $K^\sigma(e) = (\dim \sigma)^2$ である (see 系 5.5) ことから, $F(e) = \sum_{\sigma \in S} c_\sigma \cdot (\dim \sigma)^2$ となる. すなわち

$$|X| = \sum_{\sigma \in S} c_\sigma \cdot (\dim \sigma)^2$$

となることが分かった. 特に $|X| = \dim C(X)$ と, $(\dim \sigma)^2 = \dim H^\sigma(G)$ $({}^\forall \sigma \in S)$ に注意すれば,

$$\dim C(X) = \sum_{\sigma \in S} c_\sigma \cdot \dim H^\sigma(G)$$

である. ここで $q^F \circ r = \mathrm{id}_{H^S(G)}$ を仮定すれば, $r : H^S(G) \to C(X)$ は単射であるから,

$$\sum_{\sigma \in S} \dim H^\sigma(G) = \dim H^S(G) \leq \dim C(X)$$

となって,

$$\sum_{\sigma \in S} \dim H^\sigma(G) \leq \sum_{\sigma \in S} c_\sigma \cdot \dim H^\sigma(G)$$

が成り立つ (実際には, 命題 6.5 から等号が成立していることも分かる). いま, 補題 6.9, 6.8 から

$$0 \leq c_\sigma \leq 1 \quad ({}^\forall \sigma \in S)$$

であるから $c_\sigma = 1$ $({}^\forall \sigma \in S)$ でなければならない. 従って $F = \sum_{\sigma \in S} K^\sigma = K^S$ である. □

7 アソシエーションスキームについて

有限集合 $X \subset G$, $S \subset \widehat{G}$ について, X が $S \otimes S^-$-design である ($S \otimes S^-$-design については定義 3.2 と定義 4.1 を参照) としよう. 球面上の理論と比較した場合, 主定理 4.2 (i) の不等式において等号が成立している場合には, X にアソシエーションスキームが付随することが期待されるが, 今のところ証明は出来ておらず, 反例も見つけられなかった. この章では, X が $S \otimes S^-$-design であるとき, X に可換なアソシエーションスキームが付随するための十分条件を述べる (後述の定理 7.1, この条件は主定理 4.2 (i) における等号成立よりも真に強い条件である).

G の有限部分集合 X に対して, $G/\sim$ の有限部分集合 $A(X)$ を,

$$A(X) := \{\, [x^{-1}y] \mid x, y \in X,\ x \neq y \,\}$$

として定義していた ($[x^{-1}y]$ は $x^{-1}y \in G$ の共役類を表している). これに単位元 $e \in G$ の共役類も加えた集合を

$$A'(X) := A(X) \sqcup \{[e]\} \subset G/\sim$$

と表す. これに付随して, $X \times X$ の部分集合 R_α ($\alpha \in A'(X)$) を

$$R_\alpha := \{\, (x, y) \in X \times X \mid [x^{-1}y] = \alpha \,\} \quad (\alpha \in A'(X))$$

として定義すると,

$$X \times X = \bigsqcup_{\alpha \in A'(X)} R_\alpha$$

は $X \times X$ の分割を表す.

このとき $\mathfrak{X} := (X, \{R_\alpha\}_{\alpha \in A'(X)})$ がクラス $|A(X)|$ の可換なアソシエーションスキームであるための十分条件として, 次の定理が成り立つ:

定理 7.1. 有限集合 $X \subset G$, $S \subset \widehat{G}$ について, X は $S \otimes S^-$-design であるとする. このとき,

$$|S| \leq |A'(X)| \ (\dot{=} |A(X)| + 1)$$

が成り立つ. 更に, この等号が成立するとき, $S = S^-$ であって, X は K^S-code であり, $\mathfrak{X} = (X, \{R_\alpha\}_{\alpha \in A'(X)})$ は, クラス $|A(X)|$ の可換なアソシエーションスキームである.

この定理 7.1 の等号が成立する例を挙げておく.

例 7.2. コンパクト Lie 群として, ユニタリ群

$$U(1) := \{\, z \in \mathbb{C} \mid |z| = 1 \,\}$$

を考え, $G = U(1)$ としておく ($U(1)$ は円周 S^1 と Lie 群としては同じものであるが, S^1 を 1-次元球面と思う場合には, 作用する群が異なる (1-次元球面には $O(2)$ が作用する, $U(2)$ には $U(2) \times U(2)$ が作用する) ので, 別の空間として考えている). 整数 k に対して

$$\chi_k : U(1) \to \mathbb{C}^\times,\ z \mapsto z^k$$

を定義すると, χ_k は $U(1)$ の 1-次元ユニタリ表現である (このとき $\widehat{G} = \{\chi_k \mid k \in \mathbb{Z}\}$ である). 自然数 $2n+1$ を固定して, G の有限部分集合 X と $\widehat{G}$ の有限部分集合 S を

$$X := \{ e^{2\pi\sqrt{-1}\frac{k}{2n+1}} \mid 0 \geq k \geq 2n \} \quad (\text{正 } 2n+1 \text{ 角形})$$
$$S := \{ \chi_l \mid -n \leq l \leq n \}$$

とする. $S \otimes S^- = \{ \chi_l \mid -2n \leq l \leq 2n \} \subset \widehat{G}$ であることに注意すると, このとき X は $S \otimes S^-$-design であることが分かる. 更に,

$$A(X) = \{ [e^{2\pi\sqrt{-1}\frac{k}{2n+1}}] \in G/\sim \mid 1 \leq k \leq 2n \} \subset G/\sim$$

となるから $|A(X)| = 2n$ である. 従って $|S| = |A(X)| + 1$ が成立している. 実際この場合, $S = S^-$ かつ X は S-code であって, X には, クラス $2n$ の可換なアソシエーションスキーム (可換群 $\mathbb{Z}/(2n+1)\mathbb{Z}$ の群アソシエーションスキームと同じもの) が付随している.

この定理の不等式での等号が成立していれば, 特に X は S-code でもあるから, 主定理 4.2 から $|X| = \sum_{\sigma \in S} (\dim \sigma)^2$ が分かる. 従って, この定理における不等号の等号成立:

"X は $S \otimes S^-$-design であって, $|S| = |A(X)| + 1$"

という条件は, 主定理 4.2 における不等号の等号成立:

"X は $S \otimes S^-$-design であって, $|X| = \sum_{\sigma \in S} (\dim \sigma)^2$ "

という条件より強い. 実際には, 次の例が示すように上の条件は下の条件より真に強い.

例 7.3. 例 4.3 ($G = U(2)$ の例) では, X は $S \otimes S^-$-design であって, 主定理 4.2 における等号

$$|X| = \sum_{\sigma \in S} (\dim \sigma)^2$$

が成立しているのであった. しかし, この場合の $A(X) \subset G/\sim$ は

$$A(X) = \{ [\begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}] \} \subset U(2)/\sim$$

であるから, $|S| = 1$, $|A(X)| + 1 = 2$ となって,

$$|S| \leq |A(X)| + 1$$

の等号は成立しない. また, $A(X)$ が一点集合であることから, $\mathfrak{X} := (X, \{R_\alpha\}_{\alpha \in A'(X)})$ は, 自動的にクラス 1 の対称なアソシエーションスキームとなる.

最後に定理 7.1 の証明のアイディアを述べる.

定理 7.1 の証明のアイディア. 証明の方針を大まかに述べると, R_α $(\alpha \in A'(X))$ の隣接行列の張る空間を調べるということである.

Step1: X を添え字集合とする正方行列のなす多元環を

$$M(X,\mathbb{C}) := \{\, A : X \times X \to \mathbb{C} \,\}$$

と書く. $M(X,\mathbb{C})$ には行列としての積の構造と, $X \times X$ 上の関数としての積の構造 (アダマール積と呼ばれる) が入る. 一方, 複素ベクトル空間 $C(X)$ に対して, $\mathrm{End}\, C(X)$ を考える. $\mathrm{End}\, C(X)$ は合成による積構造によって, $\mathbb{C}$-代数の構造を持つ. ここで, 各 $A \in \mathrm{End}\, C(X)$ に対して, $C(X)$ の正規直交基底 $\{\, \sqrt{|X|}\cdot\delta_x \mid x \in X \,\}$ についての行列表示をすることで, $M(X,\mathbb{C})$ の元とみなせる. この対応によって, $M(X,\mathbb{C})$ と $\mathrm{End}\, C(X)$ を同一視すると, $M(X,\mathbb{C})$ での転置共役は, $\mathrm{End}\, C(X)$ でのエルミート共役と一致し, $M(X,\mathbb{C})$ での行列としての積は, $\mathrm{End}\, C(X)$ での合成による積一致する.

Step2: 各 $\alpha \in A'(X)$ に対して, 隣接行列 $A_\alpha \in M(X,\mathbb{C})$ を

$$A_\alpha(x,y) := \begin{cases} 1 & ((x,y) \in R_\alpha) \\ 0 & ((x,y) \notin R_\alpha) \end{cases} \qquad ({}^\forall x, y \in X)$$

と定義して $M(X,\mathbb{C})$ の部分空間 $\mathfrak{A}$ を

$$\mathfrak{A} := \mathbb{C}\text{-span}\{\, A_\alpha \mid \alpha \in A'(X) \,\}$$

とする. $\mathfrak{A}$ はアダマール積で閉じており, $\{\, A_\alpha \mid \alpha \in A'(X) \,\}$ がアダマール積についての原始冪等元全体の集合である. また, $\dim \mathfrak{A} = |S|$ であることも分かる. 定義から, $A_{[e]}$ が単位行列であることと, $\mathfrak{A}$ が複素共役で閉じることも注意しておく.

Step3: 制限写像 $r : H^S(G) \to C(X)$ に対して, $H^\sigma(G)$ の像 $r(H^\sigma(G)) \subset C(X)$ を考え, $C(X)$ から $r(H^\sigma(G))$ への直交射影を, $p_\sigma : C(X) \to r(H^\sigma(G))$ で表すことにする. $\mathrm{End}\, C(X)$ の部分空間 $\mathfrak{P}$ を

$$\mathfrak{P} := \mathbb{C}\text{-span}\{\, p_\sigma \mid \sigma \in S \,\}$$

と定義する. いま, X は $S \otimes S^-$-design であると仮定していたから, 命題 6.4 より, $r : H^S(G) \to C(X)$ は内積を保つ. 従って, $C(X)$ の部分空間の族 $r(H^\sigma(G))$ $(\sigma \in S)$ は互いに直交しており, p_σ $(\sigma \in S)$ 達は互いに可換な射影作用素である. 特に, $\mathfrak{P} \subset \mathrm{End}\, C(X)$ はエルミート共役で閉じる可換な部分代数であり, $\{\, p_\sigma \mid \sigma \in S \,\}$ が合成に関する原始冪等元全体の集合である. また, $\dim \mathfrak{P} = |S|$ であることも分かる.

Step4: $\mathfrak{P} \subset \mathrm{End}\, C(X)$ を Step 1 の対応において, $\mathfrak{P} \subset M(X, \mathbb{C})$ とみなせば, $\mathfrak{P}$ は転置共役で閉じていて, 行列の積に関して可換な部分代数をなす. このとき, 任意の $\sigma \in S$ に対して, p_σ の $M(X, \mathbb{C})$ の元としての (x, y)-成分を調べると,

$$p_\sigma(x, y) = \frac{1}{|X|} K_\sigma(x, y) \quad ((x, y) \in X \times X)$$

となることが示せる. 特に K_σ が類関数であることと, $\mathfrak{A}$ の性質を合わせて考えると, $\mathfrak{P} \subset \mathfrak{A}$ が言える.

Step5: Step 4 で $\mathfrak{P} \subset \mathfrak{A}$ が分かったので, 特に両辺の次元を考えれば,

$$|S| \geq |A'(X)|$$

が成り立つ. ここでの等号成立条件は, $\mathfrak{P} = \mathfrak{A}$ となることである. $\mathfrak{P} = \mathfrak{A}$ の場合には, 特に $\mathfrak{A} \subset M(X, \mathbb{C})$ が, 転置, 複素共役, アダマール積で閉じていて, 行列としての積で可換な部分代数をなし, さらに単位行列を含むことになるから, $\mathfrak{X}$ は可換なアソシエーションスキームであることが示せる. また, この場合, $\mathfrak{P}$ は単位行列を含んでいるので, 制限写像 $r : H^S(G) \to C(X)$ は内積を保つ全単射でなければならず, 特に命題 6.4, 命題 6.5 から, X は K^S-code となる. 更に, このとき $\mathfrak{P} = \mathfrak{A}$ が複素共役で閉じることから, $S = S^-$ も証明することが出来る. □

参考文献

[1] 坂内英一・坂内悦子. 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.

[2] C. Bachoc, E. Bannai, and R. Coulangeon. Codes and designs in Grassmannian spaces. *Discrete Mathematics*, 277(1-3):15–28, 2004.

[3] C. Bachoc, R. Coulangeon, and G. Nebe. Designs in Grassmannian spaces and lattices. *Journal of Algebraic Combinatorics*, 16(1):5–19, 2002.

[4] E. Bannai and S. G. Hoggar. On tight t-designs in compact symmetric spaces of rank one. *Proc. Japan Acad. Ser. A Math. Sci.*, 61(3):78–82, 1985.

[5] E. Bannai and S. G. Hoggar. Tight t-designs in projective spaces, and Newton polygons. *Ars Combin.*, 20(A):43–49, 1985. Tenth British combinatorial conference (Glasgow, 1985).

[6] P. Delsarte, J. Goethals, and J. Seidel. Spherical codes and designs. *Geom. Dedicata*, 6(3):363–388, 1977.

[7] 小林俊行・大島利雄. リー群と表現論. 岩波書店, 2005.

[8] 三浦佳子. Codes and designs in complex Grassmannian spaces. 九州大学修士論文, 2004.

[9] A. Roy. Bounds for codes and designs in complex subspaces. *Journal of Algebraic Combinatorics*, 31(1):1–32, 2010.

[10] A. Roy and A. Scott. Unitary designs and codes. *Designs, Codes and Cryptography*, 53(1):13–31, 2009.

4次直交群の有限部分群から構成される球面デザインについて

三枝崎 剛 Tsuyoshi Miezaki *

この原稿は, 2010年6月の第27回「代数的組合せ論シンポジウム」(高知大学) の三枝崎による上の題での講演の記録です. タイトルの英訳は "Spherical designs obtained from finite subgroups of the orthogonal group of degree 4" であり, プレプリント [5](投稿準備中) に基づいています.

1 序

球面デザインの概念は, Delsarte-Goethals-Seidel [3] によります.

定義 1.1. 正整数 t, 単位球面上の有限集合 X が球面 t-デザイン (以下 t-デザインと書きます) とは次の条件を満たす事です:

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

が, 全ての次数 t 以下の多項式 $f(x) = f(x_1, x_2, \cdots, x_{d+1})$ に関して成立する.

ここで, 右辺は球面上での積分を意味し, $|S^d|$ で球 S^d の表面積を表します. 半径 r の球上の有限集合 X について, 正規化した集合 X/r が t-デザインの時, X を t-デザインと呼ぶ事にします.

一般に, t-デザインの構成は非常に難しい問題ですが, 直交群の有限部分群を用いて, ある程度高い t の t-デザインを構成する事が出来ます. 例えば, 任意の点 $x \in S^7$ に対して, E_8 型ワイル群の軌道 $x^{W(E_8)}$ は 7-デザインになります. (特別な点を選ぶと 11-デザインになります.) 群 G がこのような性質「任意の点 $x \in S^d$ に対して, x^G は t-デザインになる」を持つ時, G は t-均質群と呼ばれ, 次が成立します.

*東北大学 大学院情報科学研究科 数学教室, e-mail: miezaki@math.is.tohoku.ac.jp.

定理 1.1 (cf. [1, page 112]). Gを$O(d+1)$の有限部分群，$\rho_i(i=0,1,2,\ldots)$を$O(d+1)$のi次球表現とする．このとき次の条件は互いに同値である．

1. Gはt-均質な部分群である．

2. $\mathrm{Harm}_i(S^d)^G=0$が$1\leq i\leq t$を満たす任意のiに対して成り立つ．

3. $1\leq i\leq t$を満たす任意のiに対して$(\rho_0,\rho_i)_G=0$.

また，t-重可移群の類似として$O(d+1)$の有限部分群Gに対してt-重群という概念があります．

定義 1.2 (cf. [1, page 118]). $O(d+1)$の有限部分群Gは，$i+j\leq t$を満たす任意のi,jに対して$(\rho_i,\rho_i)_G=\delta_{i,j}$のときに$t$-重群であるという．

この時，次が予想されています．

予想 1.1. $t\geq 11$とする．この時Gがt-均質群であれば，Gがt-重群である．

予想 1.2. Gがt-均質群であれば，$t\leq 11$.

特に予想1.1はt-重可移群に関するLivingstone-Wagnerの定理の類似です．

筆者は最近，4次直交群の有限部分群はConway-Smith[2]により分類されている事を知りました．その分類を用い，4次直交群の有限部分群に関して上の予想を確かめようと思ったのが，この研究の始まりです．

2 結果

先に述べた様に，4次直交群はConway-Smith[2]により分類されています．その各々に対して，i次球表現の指標を用い，t-重群だが$t+1$-重群でない，t-均質群だが$t+1$-均質群でないtの値を決定し，それにより上の予想を確かめました．

ここで，i次球表現の指標は以下の様にして計算できます．行列$A\in O(4)$に対して，

$$\sum_{k=0}^{\infty}H_k(A)t^k=\frac{1}{\det(I_n-tA)}$$

とおきます．

定理 2.1 (cf. [4, page 230]). 直交群 $O(4)$ の i 次球表現の指標 ρ_i は,

$$\rho_i(A) = H_i(A) - H_{i-2}(A)$$

となる. ここで $k < 0$ のとき, $H_k = 0$ と約束する.

特別な場合のみ, 計算結果を与えます. 詳しくは, [5] を見て下さい.

表 1: Chiral I type

No.	群	生成元	t-均質	t-重
1	$\pm[I \times O]$	$[i_I, 1], [\omega, 1], [1, i_O], [1, \omega]$;	11	11
2	$\pm[I \times T]$	$[i_I, 1], [\omega, 1], [1, i], [1, \omega]$;	11	11
3	$\pm[I \times D_{2n}]$	$[i_I, 1], [\omega, 1], [1, e_n], [1, j]$;	11	11
4	$\pm[I \times C_n]$	$[i_I, 1], [\omega, 1], [1, e_n]$;	11	11
5	$\pm[O \times T]$	$[i_O, 1], [\omega, 1], [1, i], [1, \omega]$;	7	7
6	$\pm[O \times D_{2n}]$	$[i_O, 1], [\omega, 1], [1, e_n], [1, j]$;	7	7
7	$\pm\frac{1}{2}[O \times D_{2n}]$	$[i, 1], [\omega, 1], [1, e_n]; [i_O, j]$	5	5
8	$\pm\frac{1}{2}[O \times \overline{D}_{4n}]$	$[i, 1], [\omega, 1], [1, e_n], [1, j]; [i_O, e_{2n}]$	7	7
9	$\pm\frac{1}{6}[O \times D_{6n}]$	$[i, 1], [j, 1], [1, e_n]; [i_O, j], [\omega, e_{3n}]$	5	5
10	$\pm[O \times C_n]$	$[i_O, 1], [\omega, 1], [1, e_n]$;	7	7
11	$\pm\frac{1}{2}[O \times C_{2n}]$	$[i, 1], [\omega, 1], [1, e_n]; [i_O, e_{2n}]$	7	7
12	$\pm[T \times D_{2n}]$	$[i, 1], [\omega, 1], [1, e_n], [1, j]$;	7	5
13	$\pm[T \times C_n]$	$[i, 1], [\omega, 1], [1, e_n]$;	5	5
14	$\pm\frac{1}{3}[T \times C_{3n}]$	$[i, 1], [1, e_n]; [\omega, e_{3n}]$	5	5
15	$\pm\frac{1}{2}[D_{2m} \times \overline{D}_{4n}]$	$[e_m, 1], [1, e_n], [1, j]; [j, e_{2n}]$	3	3
16	$\pm[D_{2m} \times C_n]$	$[e_m, 1], [j, 1], [1, e_n]$;	3	3
17	$\pm\frac{1}{2}[D_{2m} \times C_{2n}]$	$[e_m, 1], [1, e_n]; [j, e_{2n}]$	3	3
18	$+\frac{1}{2}[D_{2m} \times C_{2n}]$	$-, -; +$	1	1
19	$\pm\frac{1}{2}[\overline{D}_{4m} \times C_{2n}]$	$[e_m, 1], [j, 1], [1, e_n]; [e_{2m}, e_{2n}]$	3	3

最後になりましたが, 講演の機会を頂き, また旅費を援助して下さりました大浦学氏に感謝いたします.

参考文献

[1] Ei. Bannai and Et. Bannai, 球面上の代数的組合せ理論, Springer–Verlag, Tokyo 1999.

[2] J. H. Conway and D. A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*, A K Peters, Ltd., Natick, MA, 2003.

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

[4] S. Okada, 古典群の表現論と組合せ論〈下〉(数理物理シリーズ), 培風館 2006.

[5] T. Miezaki, *Classification of t-homogeneous subgroups of the orthogonal group of degree* 4, in preparation.

有限体上の平面代数曲線とSziklai予想*

本間正明 (神奈川大学工学部)

1 有限体上の平面代数曲線–組合せ論的視点から

Weil [21] によれば，整数係数多項式 $f(x,y)$ について，素数 p を法とする方程式 $f(x,y)=0$ の解がいくつあるあるかというタイプの問題はGauss にまでさかのぼる．この問題は多項式を斉次化し「$F(X,Y,Z)=0$ の解を有限体 $\mathbb{F}_p$ 上の射影空間 $\mathbb{P}^2(\mathbb{F}_p)$ の中で数えること」と幾何学的にとらえなおすことができる．

以下では，素数 p のみに限らず，その冪も許し，それを q とする．$\mathbb{F}_q$ 上定義された射影空間 $\mathbb{P}^2$ の斉次座標 X,Y,Z を固定し，$Z\neq 0$ となるアフィン空間の座標を $x=X/Z$, $y=Y/Z$ であらわす．

また $\mathbb{F}_q$ 上の 重複因子を持たない 斉次多項式 $F(X,Y,Z)$ が与えられたとき，$\{F=0\}$ でその $\mathbb{F}_q$ の代数的閉包上の解集合をあらわし，これを $\mathbb{F}_q$ 上の曲線とよぶ．

$C=\{F=0\}$ のとき，$C(\mathbb{F}_q)=\{(\alpha,\beta,\gamma)\in\mathbb{P}^2(\mathbb{F}_q)|F(\alpha,\beta,\gamma)=0\}$ とあらわし，$C(\mathbb{F}_q)$ の元の個数を $N_q(C)$ であらわす．

さらに，C の次数，すなわち $F(X,Y,Z)$ の次数を d とする．

以上の状況の下で，

$N_q(C)$ の d,q による良い上限を見出せ

という問題を考えたい．

1.1 自明な上限

$C(\mathbb{F}_q)\subset\mathbb{P}^2(\mathbb{F}_q)$ なので，

$$N_q(C)\leq q^2+q+1 \tag{1}$$

である．

*講演時のタイトルは Plane curves over finite fields, and Sziklai's conjecture だったが，報告を書くに当って日本語の題名に変更した．なお，これは Seon Jeong KIM (Gyeongsang National University, Korea) との共同研究である．

補題 1.1 C が $\mathbb{F}_q$-直線を既約成分に持たないとき，言い換えれば，どんな $\mathbb{F}_q$ 係数の 1 次式でも $F(X,Y,Z)$ が割り切れないとき，

$$N_q(C) \leq (q+1)(d-1)+1 = dq+1-(q+1-d). \tag{2}$$

証明. $d \geq q+1$ のときは (1) より明らか．ゆえ，$d < q+1$ とする．$P_0 \in C(\mathbb{F}_q)$ を固定する．P_0 を通る $\mathbb{F}_q$-直線 l について，$(C(\mathbb{F}_q) \cap l) \setminus \{P_0\}$ の個数は高々 $(d-1)$. □

$\mathbb{F}_q$-直線を既約成分に持つことも許した任意の C について，d にも依存する自明な上限として，

命題 1.2

$$N_q(C) \leq dq+1. \tag{3}$$

さらに，等号が成立するのは，C がある $\mathbb{F}_q$-点を通る d 本の $\mathbb{F}_q$-直線からなる場合に限る．

証明. $d \geq q+2 \Rightarrow dq+1 > q^2+q+1 \geq N_q(C)$ であるから，$d \leq q+1$ として良い．

(i) $d = q+1$ の場合．このとき (3) の右辺は $q^2+q+1 = {}^{\#}\mathbb{P}^2(\mathbb{F}_q)$ であるから，不等式の成立は明らか．さらに等号が成立すれば，$C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)$ となる．

$\mathbb{P}^2(\mathbb{F}_q)$ のイデアルは $X^qY - XY^q$, $Y^qZ - YZ^q$, $Z^qX - ZX^q$ で生成されるから，C の方程式は，$d = q+1$ ゆえ $F = \alpha(X^qY - XY^q) + \beta(Y^qZ - YZ^q) + \gamma(Z^qX - ZX^q)$ (ただし，$\alpha, \beta, \gamma \in \mathbb{F}_q$) の形．これは点 (β, γ, α) を通る $q+1$ 本の直線の和である．

よって，以下では $d < q+1$ とする．$\mathbb{F}_q$-直線で C の既約成分となるものの個数を i とする．$i = 0$ であれば，補題 1.1 で済んでいる．

(ii) $i = 1$ とする．C の既約成分となる $\mathbb{F}_q$-直線を l_0 として，$C = l_0 \cup C'$ と置くと，$\deg C' = d-1$ であり，補題 1.1 より，$N_q(C') \leq (q+1)(d-2)+1$. ゆえ

$$\begin{aligned} N_q(C) &\leq N_q(C') + q + 1 \leq (q+1)(d-2) + 1 + q + 1 \\ &\leq (q+1)(d-1) + 1 = dq + 1 - (q+1-d) \leq dq+1. \end{aligned}$$

$d < q+1$ であるから等号はとりえない．

(iii) 次に $i \geq 2$ とする．C の既約成分となる，ふたつの $\mathbb{F}_q$-直線の交点を $P_0 \in C(\mathbb{F}_q)$ とする．

P_0 を通る $\mathbb{F}_q$-直線で C の既約成分となるものを $l_1, \ldots, l_j$ とする．$j \geq 2$ である．l を P_0 を通る $\mathbb{F}_q$-直線で $l \neq l_i$ $(i = 1, \ldots, j)$ とすれば，$(C(\mathbb{F}_q) \cap l) \setminus \{P_0\}$ の個数は高々 $(d-j)$. ゆえに，

$$N_q(C) \leq (q+1-j)(d-j) + jq + 1 \leq dq + 1 - (j-1)(d-j) \leq dq+1.$$

$j \geq 2$ であるから，等号は $j = d$ のときに限る． □

1.2 Segre 上限と Sziklai 予想

平面曲線 $C = \{F = 0\}$ として，最初に述べた $F(X, Y, Z)$ が重複因子を持たないという条件だけで考えれば，命題 1.2 が最良の上界を与える．このような自明な状況を排除するため，以下では，

> $C = \{F = 0\}$ は $\mathbb{F}_q$-直線を既約因子に持たない，すなわち，
> どんな $\mathbb{F}_q$ 係数の 1 次式も $F(X, Y, Z)$ を割り切らない

と仮定する．

この状況下では (2) が，ひとつの上限を与える．これを次のような形で書いておく．

$$N_q(C) \leq (d-1)q + d. \tag{4}$$

しかし，この上限はあまり良くない．

実際 Beniamino Segre は 1959 年の長大な論文 [15] の中で

$$N_q(C) \leq (d-1)q + \left\lfloor \frac{d}{2} \right\rfloor \tag{5}$$

という評価を得ている．

Segre 上限 (5) は (4) に比べ末尾の項が大幅に改善されているとはいえ，これを到達する曲線は conic 位しか見当たらないという意味で改善の余地がある．

2008 年に至って，Peter Sziklai は $N_q(C)$ の大きそうな曲線の例をいくつか計算した上で，次の予想を提出した [17]:

Sziklai 予想 $N_q(C) \leq (d-1)q + 1$.

2 既約平面曲線についての既知の上限と Sziklai 予想

Sziklai 予想は既約な曲線について確認すれば十分である．実際，

命題 2.1 (i) C が $\mathbb{F}_q$ 上可約ならば $N_q(C) < (d-1)q$.

(ii) C が $\mathbb{F}_q$ 上定義されていない既約成分を持つならば $N_q(C) \leq (d-1)q$.

(iii) $C(\mathbb{F}_q) \cap \operatorname{Sing} C \neq \emptyset$ ならば $N_q(C) \leq (d-1)q$.

が成り立つ [11, Sec.2]．ただし，上の命題中の $\operatorname{Sing} C$ は C の特異点全体の集合を意味する．

既約な平面曲線 C についての $N_q(C)$ について知られている上限と Sziklai 予想とを比較してみる．

2.1 Hasse-Weil の上限

まず，特異点を持たない (必ずしも平面曲線とは限らない) 曲線についてのHasse-Weil の上限を復習する．

定理 2.2 (Hasse-Weil) Y を 種数 g の $\mathbb{F}_q$ 上定義された非特異曲線とする．このとき，$N_q(Y) \leq q+1+2g\sqrt{q}$ が成り立つ．

$g=1$ のときが Hasse[2, 3, 4]，一般の genus の場合は Weil[20] に帰せられている．

系 2.3 $\mathbb{F}_q$ 上の (必ずしも非特異とは限らない) 平面既約曲線 C について，その次数が d であるとき，

$$N_q(C) \leq q+1+(d-1)(d-2)\sqrt{q}$$

が成り立つ．

証明. $\pi : Y \to C$ を正規化とする．Y は $\mathbb{F}_q$ 上定義される．その種数を g とする．各 $P \in \mathrm{Sing}\, C$ について，重複度を m_P とする．$g \leq \frac{1}{2}(d-1)(d-2) - \sum \frac{1}{2} m_P(m_P-1)$. また，$N_q(C) \leq N_q(Y) + \sum m_P$. この 2 つの不等式と Hasse-Weil の上限を合わせれば良い． □

2.2 Stöhr-Voloch 上限

次数 d の $\mathbb{F}_q$ 上の平面既約曲線 C の定義式を $F(X,Y,Z)=0$ とする．D を

$$\tilde{F}(X,Y,Z) := F_X(X,Y,Z)X^q + F_Y(X,Y,Z)Y^q + F_Z(X,Y,Z)Z^q = 0$$

で定まる曲線とする．ここで，$F_X(X,Y,Z)$, $F_Y(X,Y,Z)$, $F_Z(X,Y,Z)$ は $F(X,Y,Z)$ のそれぞれ X, Y, Z による偏微分である．

$P=(\alpha,\beta,\gamma) \in C(\mathbb{F}_q)$ とする．$\alpha,\beta,\gamma \in \mathbb{F}_q$ として良い．このとき，$\alpha^q=\alpha,\ldots$ であるから，$\tilde{F}(\alpha,\beta,\gamma) = dF(\alpha,\beta,\gamma) = 0$, すなわち，$P=(\alpha,\beta,\gamma) \in C \cap D$.

また，P が C の非特異点ならば，接線の方程式は

$$F_X(\alpha,\beta,\gamma)X + F_Y(\alpha,\beta,\gamma)Y + F_Z(\alpha,\beta,\gamma)Z = 0,$$

である．一方，

$$\begin{aligned} \tilde{F}_X(\alpha,\beta,\gamma) &= F_{XX}(\alpha,\beta,\gamma)\alpha + F_{YX}(\alpha,\beta,\gamma)\beta + F_{ZX}(\alpha,\beta,\gamma)\gamma \\ &= (d-1)F_X(\alpha,\beta,\gamma) \\ \ldots &\quad \text{etc} \end{aligned}$$

であるから，P が D の非特異点なら接線は C へのそれと一致する．よって C と D との P における交点数は 2 以上．また，P が C または D の特異点であれば自動的に C と D との P における交わりの重複度 $i(C,D;P)$ は 2 以上ある．$\deg D = d-1+q$ であるから

$$N_q(C) \leq \sum_{P \in C(\mathbb{F}_q)} \frac{1}{2} i(C,D;P) \leq \frac{1}{2}(C.D) = \frac{1}{2} d(d-1+q).$$

ここで，$(C.D)$ は C と D との交点数の総和である．

上で述べた議論はこのままでは正しくない．$\tilde{F}(X,Y,Z)$ が恒等的に 0，あるいは C が D の成分となってしまうような場合にはこの議論は通用しない．つまり，

$\forall Q = (a,b,c) \in C$ について，

$$F(a,b,c) = 0 \Rightarrow F_X(a,b,c)a^q + F_Y(a,b,c)b^q + F_Z(a,b,c)c^q = 0$$

となる場合を除いて上の議論は正しい．

$\mathbb{F}_q$ 上の平面既約曲線 C がこの除外すべき性質を持つとき，C は **q-Frobenius nonclassical** であるという．q-Frobenius classical はもちろん q-Frobenius nonclassical ではないことを意味する．

したがって，上の議論によって得られた結論は

定理 2.4 (Stöhr-Voloch [16]) $\mathbb{F}_q$ 上の次数 d の平面既約曲線 C が *q-Frobenius classical* のとき，$N_q(C) \leq \frac{1}{2} d(d-1+q)$.

一方，q-Frobenius nonclassical の場合にはあまり良い上限が知られていなかった．しかし C が非特異であれば，$N_q(C)$ は，はっきりと定まる．

定理 2.5 (Hefez-Voloch [5]) $\mathbb{F}_q$ 上の次数 d の平面非特異 *q-Frobenius nonclassical* 曲線 C について，$N_q(C) = d(q+2-d)$.

2.3 上限の比較と例

これらの上限の相互関係は図 1 のようになっている．ただし，この図で水平方向の座標軸は d を，垂直方向の座標軸は $N_q(C)$ を表している．

また Sziklai 上限の直線上に印した • は例が存在することを示す．

Example 2.6 $d = 2$ とする．すべての $\mathbb{F}_q$ 上の既約 2 次曲線は $q+1$ 個の有理点を持つ．

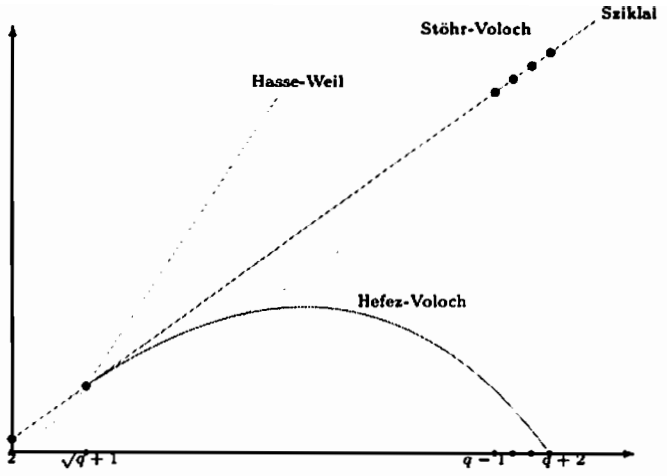


図 1: 上限の比較

Example 2.7 q が平方数のとき，$d=\sqrt{q}+1$ とする．Hermitian 曲線 $Y^{\sqrt{q}}Z+YZ^{\sqrt{q}}=X^{\sqrt{q}+1}$ は $\sqrt{q}^3+1=(d-1)q+1$ 個の有理点を持つ．これは非特異曲線である．$F(X,Y,Z)=X^{\sqrt{q}+1}-Y^{\sqrt{q}}Z-YZ^{\sqrt{q}}$ とおくと，

$$\begin{aligned}\tilde{F}(X,Y,Z) &= X^{q+\sqrt{q}}-Y^qZ^{\sqrt{q}}-Y^{\sqrt{q}}Z^q \\ &= (X^{\sqrt{q}+1}-Y^{\sqrt{q}}Z-YZ^{\sqrt{q}})^{\sqrt{q}}\end{aligned}$$

であるから，q-Frobenius nonclassical である．

Example 2.8 (Sziklai[17]) $d=q-1$ とする．$\alpha,\beta\in\mathbb{F}_q$ を $\alpha\beta(\alpha+\beta)\neq 0$ を満たすものとする．このとき，$C_{\alpha,\beta}:\alpha(X^{q-1}-Z^{q-1})+\beta(Y^{q-1}-Z^{q-1})=0$ は $\forall(a,b,c)\in\mathbb{P}^2(\mathbb{F}_q)$ $(abc\neq 0)$ を有理点として持つ．ゆえ，$N_q(C_{\alpha,\beta})=(q-1)^2=(q-2)q+1$.

Example 2.9 $d=q$ とする．$C:X^q-XZ^{q-1}+X^{q-1}Y-Y^q=0$ について，$C(\mathbb{F}_q)=\mathbb{P}^2(\mathbb{F}_q)\setminus(\{Z=0\}\cup\{(0,b,1)|b\neq 0\})$. ゆえ，$N_q(C)=(q-1)^2+q=(q-1)q+1$.

Example 2.10 $d=q+1$ とする．$C:X^{q+1}-X^2Z^{q-1}+Y^qZ-YZ^q=0$ について，$C(\mathbb{F}_q)=\mathbb{P}^2(\mathbb{F}_q)\setminus\{(1,b,0)|b\in\mathbb{F}_q\}$. ゆえ，$N_q(C)=q^2+q+1-q=(q+1-1)q+1$.

3 反例と予想の変形

Sziklai 予想に立ち返る．実はこの予想には反例がある．

Example 3.1 $\mathbb{F}_4$ 上で

$$K : X^4+Y^4+Z^4+X^2Y^2+Y^2Z^2+Z^2X^2+X^2YZ+XY^2Z+XYZ^2=0$$

で定義される曲線を考える．これは非特異曲線であり，7 本の $\mathbb{F}_2$-直線が K の複接線となり 2 つの接点は互いに $\mathbb{F}_2$ 上共役な $\mathbb{F}_4$-点となっている．したがって少なくとも 14 個の $\mathbb{F}_4$-点を持つ．どんな $\mathbb{F}_2$-点も K 上にないことは容易に確かめられる．すなわち $N_4(K)=14$. ところが $d=q=4$ なので $(d-1)q+1=13$ である．

しかし，$d=q=4$ で $N_4(C)=14$ となる曲線は，この K に $\mathbb{F}_4$ 上の射影変換で移る [10]．すなわち，$d=q=4$ の場合でも，この K を除けば予想は正しい．そこで，やや安易に映るかもしれないが，

Sziklai 予想の変形 $C \neq K$ について，$N_q(C) \leq (d-1)q+1$.

と変形した問題を考える[1].

最近 Seon Jeong Kim との共同研究により，この形でなら Sziklai 上限が正しいことを確認した [10, 11, 12]．その証明の概略を次節で述べる．

Remark 3.2 例 3.1 の曲線について若干付言する．定義式から明らかなように，この曲線は $\mathbb{F}_2$ 上定義されるが，$N_2(C)=0$. この曲線を $\mathbb{F}_8$ 上で考えると Kline quartic $x^3y+y^3+x=0$ に射影同値であり $N_8(C)=24$. これは Hasse-Weil 上限の Serre による改良 $N_q(Y) \leq q+1+g\lfloor 2\sqrt{q} \rfloor$ の等号を到達する例である．C は種数 3 の $\mathbb{F}_2$ 上定義される非特異曲線であるから $N_2(C)=0, N_{2^2}(C)=14, N_{2^3}(C)=24$ から L-多項式が計算できる：

$$L(t)=1-3t+9t^2-13t^3+18t^4-12t^5+8t^6.$$

この双対曲線も興味深い．それは次数 6 で 7 つの通常 2 重点を特異点にもち，それらは丁度 $\mathbb{P}^2(\mathbb{F}_2)$ に一致する．

4 証明の概略

証明は 3 つの部分に分かれ，それらは概ね [10], [11], [12] に対応する．
(I) 目的の上限より緩やかな不等式を証明する．

補題 4.1 $N_q(C) \leq \left(q-1+\frac{3}{q+2}\right)d$.

これを $2 \leq \deg C \leq q+1$ の範囲で考えれば

[1] われわれにとって，当初は予想というより作業仮説に近いものだった．

系 4.2 $2 \leq d \leq q+1$ のとき，$N_q(C) \leq (d-1)q + (q+2-d)$.

を得る．ここで $d = q+1$ とすれば，この場合の Sziklai 上限を得る．

Remark 4.3 $q = d = 4$ のとき，例 3.1 の曲線は系 4.2 の上限を到達する．

(II) $d = q$ の場合 (I) より，$N_q(C) \leq (q-1)q + 2$ となるので，$N_q(C) = (q-1)q + 2$ なる C の非存在を示せばよい．

C の方程式を具体的に書き下すことにより，可能な点配置を調べ $N_q(C) = (q-1)q + 2$ は起こり得ないことを示す．

(III) $3 \leq d \leq q-1$ のとき，図 1 から明らかなように C が q-Frobenius classical であれば証明すべきことはない[2]．

よって，次数 d の既約曲線 C は q-Frobenius nonclassical であり，$C(\mathbb{F}_q)$ には特異点がないとして良い (命題 2.1)．

これらの仮定の下で，

補題 4.4 (Hirschfeld-Korchmáros [7])

$$N_q(C) \leq \frac{1}{2} d \left(p^i (d-3) + q + 2 \right).$$

が成り立つ．

ここで，p^i は以下のような数である：既約曲線 C が q-Frobenius nonclassical であると，C の一般の点 Q における接線と C との Q における交わりの重複度は p の冪となる．それを p^i とした．

さらに，補題 4.1 の変形

補題 4.5

$$N_q(C) \leq \left(q - p^i + \frac{p^{2i} + p^i + 1}{q + p^i + 1} \right) d.$$

も示すことができる．

やや煩雑な計算をすると，これら 2 つの上限のうち少なくとも一方が $(d-1)q + 1$ より小さいこと[3]が分かり証明が終わる．

5 まとめに代えて

記号をいくつか用意する．

---

[2]同じ図より，q-Frobenius nonclassical であっても非特異でありさえすれば成立する．
[3]どちらが小さいかは d に依存する．

$\mathcal{C}_d(\mathbb{F}_q)$ を $\mathbb{F}_q$ 上の次数が d で，$\mathbb{F}_q$-直線を既約成分に持たない平面曲線全体の成す集合，$\mathcal{C}_d^i(\mathbb{F}_q) = \{C \in \mathcal{C}_d(\mathbb{F}_q) | C$: 既約 $\}$，$\mathcal{C}_d^s(\mathbb{F}_q) = \{C \in \mathcal{C}_d(\mathbb{F}_q) | C$: 非特異 $\}$ とする．

さらに，$M_q(d) := \max\{N_q(C) \mid C \in \mathcal{C}_d(\mathbb{F}_q)\}$，$M_q^i(d) := \max\{N_q(C) \mid C \in \mathcal{C}_d^i(\mathbb{F}_q)\}$，$M_q^s(d) := \max\{N_q(C) \mid C \in \mathcal{C}_d^s(\mathbb{F}_q)\}$ と定める．

明らかに，$M_q(d) \geq M_q^i(d) \geq M_q^s(d)$ であるが，これらの真の値はどうなるのであろうか？

われわれが示したことは

(i) $(q,d) \neq (4,4)$ ならば $(d-1)q+1 \geq M_q(d)$

(ii) $M_4(4) = M_4^i(4) = M_4^s(4) = 14$

(iii) $d \geq q+2$ ならば $M_q(d) = q^2+q+1$ [10]

(iv) $M_q(q+1) = M_q^i(q+1) = M_q^s(q+1) = q^2+1$

(v) $M_q(q) = M_q^i(q) = M_q^s(q) = (q-1)q+1$

(vi) $M_q(q-1) = M_q^i(q-1) = M_q^s(q-1) = (q-2)q+1$

等々にすぎない．

また，[18] および [9] によれば

(vii) $M_q(q+2) = M_q^i(q+2) = M_q^s(q+2) = q^2+q+1$

である．

(iii)-(vii) を見ると「各 $d \geq q+3$ に対し $C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)$ となる非特異曲線 C は存在するか？」という問いは，そう不自然ではない．無数の d について存在することは Gabber[1], Poonen[13] で知られている．

参考文献

[1] O. Gabber, *On space filling curves and Albanese varieties*, Geom. Funct. Anal. 11 (2001), 1192–1200.

[2] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper I. Die Struktur der Gruppe der Divisorenklassen endlicher Ordnung*, J. Reine Angew. Math. 175 (1936), 55–62.

[3] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper II. Automorphismen und Meromorphismen. Das Additionstheorem*, J. Reine Angew. Math. 175 (1936), 69–88

[4] H. Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper* III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung, J. Reine Angew. Math. 175 (1936), 193–208

[5] A. Hefez and J. F. Voloch, *Frobenius nonclassical curves*, Arch. Math. (Basel) 54 (1990) 263–273; Correction, Arch. Math. (Basel) 57 (1991) 416.

[6] J. W. P. Hirschfeld, Projective geometries over finite fields (second edition), Oxford University Press, Oxford, 1998.

[7] J. W. P. Hirschfeld and G. Korchmáros, *On the number of solutions of an equation over a finite field*, Bull. London Math. Soc. 33 (2001) 16–24.

[8] J. W. P. Hirschfeld, G. Korchmáros and F. Torres, Algebraic curves over a finite field, Princeton Univ. Press, Princeton, NJ, 2008.

[9] M. Homma and S. J. Kim, *Nonsingular plane filling curves of minimum degree over a finite field and their automorphism groups: Supplements to a work of Tallini*, `arXiv:0903.1918`, 2009.

[10] M. Homma and S. J. Kim, *Around Sziklai's conjecture on the number of points of a plane curve over a finite field*, Finite Fields Appl. 15 (2009) 468-474.

[11] M. Homma and S. J. Kim, *Sziklai's conjecture on the number of points of a plane curve over a finite field* II, in: G. McGuire, G.L. Mullen, D. Panario, I.E. Shparlinski (Eds.), Finite Fields: Theory and Applications, in: Contemp. Math., vol. 518, AMS, Providence, RI, 2010, 225–234. (An earlier version is available at `arXiv:0907.1325`.)

[12] M. Homma and S. J. Kim, *Sziklai's conjecture on the number of points of a plane curve over a finite field* III, Finite Fields Appl., in press. (doi:10.1016/j.ffa.2010.05.001)

[13] B. Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) 160 (2004), 1099–1127.

[14] J. P. Serre, *Nombres de points des courbes algébriques sur* $\mathbb{F}_q$, Sem. de Théorie des Nombres de Bordeaux 1982–1983, exp. 22; Oeuvres III, No. 129, 664–668.

[15] B. Segre, Le geometrie di Galois, Ann. Mat. Pura Appl. (4) 48 (1959) 1–96

[16] K.-O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) 52 (1986) 1–19.

[17] P. Sziklai, *A bound on the number of points of a plane curve*, Finite Fields Appl. 14 (2008) 41–43.

[18] G. Tallini, *Sulle ipersuperficie irriducibili d'ordine minimo che contengono tutti i punti di uno spazio di Galois* $S_{r,q}$, Rend. Mat. e Appl. (5) 20 (1961) 431–479.

[19] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, `http://www.science.uva.nl/~geer/` `http://www.manypoints.org/`

[20] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg 7 (1945). Hermann et Cie., Paris, 1948.

[21] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. AMS 55 (1949) 497–508.

CATEGORICAL ASPECT OF THE WITT-BURNSIDE CONSTRUCTION

HIROYUKI NAKAOKA

ABSTRACT. By definition, the *Witt-Burnside ring* is a composant of the Witt ring and the Burnside ring. In this talk, we introduce how Tambara functors describe the structure of the Witt-Burnside ring.

For an arbitrary group G, a (semi-)Mackey functor is a pair of covariant and contravariant functors from the category of 'G-sets'. More precisely, if we are given a *Mackey system* $(\mathcal{C}, \mathcal{O})$ on G, then subcategories of the category of G-sets ${}_G\mathit{Set}_{\mathcal{C}}$ and ${}_G\mathit{Set}_{\mathcal{C},\mathcal{O}}$ are associated, and a *Mackey functor* is defined as a pair $M = (M^*, M_\bullet)$ of a covariant functor $M_\bullet\colon {}_G\mathit{Set}_{\mathcal{C},\mathcal{O}} \to \mathit{Ab}$ and an additive contravariant functor $M^*\colon {}_G\mathit{Set}_{\mathcal{C}} \to \mathit{Ab}$. If G is finite, this agrees with an ordinary (semi-)Mackey functor on G.

For a finite group G, a (semi-)Mackey functor is regarded as a G-bivariant analog of a commutative (semi-)group. In fact if G is trivial, the category of (semi-)Mackey functors are canonically equivalent to the category of commutative (semi-)groups. In this view, a G-bivariant analog of a (semi-)ring is a *(semi-)Tambara functor*. A Tambara functor is firstly defined by Tambara, which he called a TNR-functor, for any finite group G. As shown by Brun, a Tambara functor plays a natural role in the Witt-Burnside construction.

It will be a natural question if there exist sufficiently many examples of Tambara functors, compared to the wide range of Mackey functors. In this talk, we give a general construction of a Tambara functor from any Mackey functor, on an arbitrary group G. In fact, we construct a functor from the category of semi-Mackey functors to the category of semi-Tambara functors. More precisely, in Theorem 1, for any Tambara system $(\mathcal{C}, \mathcal{O}_{\mathcal{C}}, \mathcal{O}_\bullet)$ on G, we construct a functor

$$\mathcal{S}\colon \mathit{SMack}_{(\mathcal{C},\mathcal{O}_\bullet)} \to \mathit{STam}_{(\mathcal{C},\mathcal{O}_\bullet)},$$

where $\mathit{SMack}_{(\mathcal{C},\mathcal{O}_\bullet)}$ and $\mathit{STam}_{(\mathcal{C},\mathcal{O}_\bullet)}$ are appropriately defined categories of semi-Mackey and semi-Tambara functors, respectively.

Theorem 1. Let $(\mathcal{C}, \mathcal{O}_{\mathcal{C}}, \mathcal{O}_\bullet)$ be a Tambara system on G. There exists a functor

$$\mathcal{S}\colon \mathit{SMack}_{(\mathcal{C},\mathcal{O}_\bullet)} \to \mathit{STam}_{(\mathcal{C},\mathcal{O}_\bullet)}.$$

Composing $\mathcal{S}$ with other known functors, we obtain functors

$$\begin{aligned} \mathcal{T}\colon \mathit{SMack}_{(\mathcal{C},\mathcal{O}_\bullet)} &\to \mathit{Tam}_{(\mathcal{C},\mathcal{O}_\bullet)}, \\ \mathit{Mack}_{(\mathcal{C},\mathcal{O}_\bullet)} &\to \mathit{STam}_{(\mathcal{C},\mathcal{O}_\bullet)}, \\ \mathit{Mack}_{(\mathcal{C},\mathcal{O}_\bullet)} &\to \mathit{Tam}_{(\mathcal{C},\mathcal{O}_\bullet)}, \end{aligned}$$

where $\mathit{Mack}_{(\mathcal{C},\mathcal{O}_\bullet)}$ and $\mathit{Tam}_{(\mathcal{C},\mathcal{O}_\bullet)}$ are the categories of Mackey and Tambara functors, respectively.

Moreover in Theorem 2, we show $\mathcal{T}$ is left adjoint to the forgetful functor $Tam_{(\mathcal{C},\mathcal{O}_\bullet)} \to SMack_{(\mathcal{C},\mathcal{O}_\bullet)}$. Thus $\mathcal{T}$ can be regarded as a G-bivariant analog of the monoid-ring functor.

Theorem 2. Let $(\mathcal{C}, \mathcal{O}_\mathcal{C}, \mathcal{O}_\bullet)$ be any Tambara system on G. The functor constructed in Theorem 1

$$\mathcal{S}\colon SMack_{(\mathcal{C},\mathcal{O}_\bullet)} \to STam_{(\mathcal{C},\mathcal{O}_\bullet)}$$

is left adjoint to the forgetful functor $STam_{(\mathcal{C},\mathcal{O}_\bullet)} \to SMack_{(\mathcal{C},\mathcal{O}_\bullet)}$.

When G is finite, we denote the category of Mackey functors simply by $Mack(G)$, and so on. For any commutative monoid Q, we can associate a constant valued semi-Mackey functor $\mathcal{C}$, defined by

$$\mathcal{C}_Q(G/H) = Q, \quad \mathrm{res}^H_K = [H:K], \quad \mathrm{ind}^H_K = \mathrm{id}_Q, \quad c^g_H = \mathrm{id}_Q,$$
$$^\forall K \leq {}^\forall H \leq G, \quad {}^\forall g \in G.$$

This gives a functor $\mathcal{C}\colon Mon \to SMack(G)$, which is left adjoint to the 'G-invariant evaluation' functor

$$\mathrm{ev}_1\colon SMack(G) \to Mon\ ;\ M \to M(G/e)^G.$$

Besides by Brun's theorem, the functor taking the Witt-Burnside ring

$$\mathbb{W}_G\colon Ring \to Tam(G)$$

is left adjoint to G-invariant evaluation functor

$$\mathrm{ev}_1\colon Tam(G) \to Ring\ ;\ T \to T(G/e)^G.$$

Thus, each functor in the diagram

$$\begin{array}{ccc} Mon & \xrightarrow{\mathbb{Z}[-]} & Ring \\ {\scriptstyle \mathcal{C}}\downarrow & & \downarrow{\scriptstyle \mathbb{W}_G} \\ SMack(G) & \xrightarrow[\mathcal{T}]{} & Tam(G) \end{array}$$

is left adjoint to the corresponding functor in the following commutative diagram of functors.

$$\begin{array}{ccc} Mon & \xleftarrow{\text{forgetful}} & Ring \\ {\scriptstyle ev_1}\uparrow & \circlearrowleft & \uparrow{\scriptstyle ev_1} \\ SMack(G) & \xleftarrow[\text{forgetful}]{} & Tam(G) \end{array}$$

Thus by the uniqueness of the left adjoint functor, we obtain an isomorphism of functors

$$\mathbb{W}_G \circ \mathbb{Z}[-] \cong \mathcal{T} \circ \mathcal{C}.$$

Graduate School of Mathematical Sciences, The University of Tokyo 3-8-1 Komaba, Meguro, Tokyo, 153-8914 Japan
E-mail address, Hiroyuki NAKAOKA: deutsche@ms.u-tokyo.ac.jp

Abstract Mackey Functors

菅井 智 (Tomo Sugai)
joint work with T.Yoshida

2010.6.22

1 introduction

1971 年に Green [1] によって，指標環や相対 Grothendieck 群，G-代数，群のコホモロジーなど対する注目すべき公理的な取り扱いが導入された．それは上に上げた群にかかわる代数的構造に共通する 3 つの写像 transfer(induction)，restriction，conjugation をその基本的性質 (特に，Mackey Decomposition や Frobenius 相互律) を保存するように定義される Mackey functor の概念である．Mackey functor に関しては，Thevenaz・Webb [2, 3] や吉田 [4, 5] などで詳細に研究されている．それらの研究の成果として，群のコホモロジーにおいてよく知られた transfer theorem の一般化などがある．Mackey functor は有限 G 集合の圏に基づいており，有限群に対してのみ適用できる概念であるが，より一般の圏に関して同様の結果を得ようとするのは自然な試みであろう.Burnside 環に関する同様の一般化の試みは吉田 [6] で行われている (Abstract Burnside ring)．本稿では，Mackey functor の理論をより一般の圏に適用することを可能とする Abstract Mackey functor の定義を与えた．また，Mackey functor の理論で用いられるいくつかの付随する概念の定義様与えた．

2 Abstract Burnside rings

Abstract Mackey functor(以後，AMF) を定義するために必要となる概念，Abstract Burnside ring(以後，ABR) の定義を与える．なお，ABR の定義・定理は吉田 [6] による．

以後 Γ を finite category(f.cat と略す) とする．

$i \in \Gamma/\cong$ に対し，

$$\mathbf{Z}\Gamma := \{ \sum_{j \in \Gamma/\cong} a_j[j] \mid a_j \in \mathbf{Z} \}$$

$$\mathbf{Z}^{\Gamma} := \mathrm{Map}(\Gamma/\cong, \mathbf{Z})$$

(ただし $\mathbf{Z}^{\Gamma} \cong \prod_{i \in \Gamma/\cong} \mathbf{Z}$ と同一視.)

と定義する．

また，簡単のため $\Gamma(i, j) := \hom_{\Gamma}(i, j)$ と定める．

このとき，$\mathbf{Z}$-準同型 $\varphi := \prod_{i \in \Gamma/\!\sim} \varphi_i : \mathbf{Z}\Gamma \to \mathbf{Z}^{\Gamma}$ を

$$\begin{array}{rccccccc} \varphi_i & : & \mathbf{Z}\Gamma & \to & \mathbf{Z} & ; & [f] & \mapsto & |\Gamma(i,\ j)| \\ \varphi := \prod_{i \in \Gamma/\!\sim} \varphi_i & : & \mathbf{Z}\Gamma & \to & \mathbf{Z}^{\Gamma} & ; & [f] & \mapsto & (|\Gamma(i,\ j)|)_{i \in \Gamma/\!\sim} \end{array}$$

と定める．

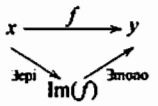
この φ を Burnside homomorphism と呼ぶ．次が ABR の定義である．

Definition 2.1 (Definition of ABR)

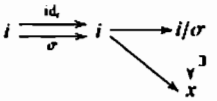
φ が $\mathbf{Z}\Gamma$ のある環構造に対して injective ring hom となるとき $\mathbf{Z}\Gamma$ は Abstract Burnside Ring(ABR) であるという．

特に Γ が次の条件 (F)，(C) を満たせば $\mathbf{Z}\Gamma$ は ABR となる．

(F)Γ は同型を除いて一意な epi-mono 分解をもつ



(C) 各 $i \in \Gamma$ において，任意の $\sigma \in \mathrm{Aut}(i)$ は coequalizer $i/\sigma \in \Gamma$ をもつ



Example 2.2 G を有限群とし，$C(G)$=[部分群の共役類] とする．

Γ として可移有限 G-set からなる圏をとる．

また，G-set X，部分群 $S \leq G$ に対し，X^S は S-fixed point set と表すこととする．

このとき，$\mathbf{Z}\Gamma$ は積

$$[G/H][G/K] = \sum_{gK \in [H\backslash G/K]} [G/H^g \cap K]$$

により

$$\varphi : \begin{array}{ccc} \mathbf{Z}\Gamma & \to & \mathbf{Z}^{\Gamma} = \mathbf{Z}^{C(G)} \\ \sum_{H \in C(G)} a_H [G/H] & \mapsto & \sum_{H \in C(G)} |(G/H)^S| \end{array}$$

は injective ring hom となる．

このとき $\mathbf{Z}\Gamma = \Omega(G)$ は"普通の"Burnside 環である．

次に，$\mathbf{Z}$-加群 $\mathrm{Obs}(\Gamma)$ を

$$\mathrm{Obs}(\Gamma) := \prod_{i \in \Gamma/\!\sim} (\mathbf{Z}/|\mathrm{Aut}(i)|\mathbf{Z})$$

と定める. また, Z-linear hom ψ を

$$\begin{aligned} \psi : \ \mathbf{Z}^{\Gamma} &\to \mathrm{Obs}(\Gamma) \\ \chi &\mapsto \left(\sum_{\sigma \in \mathrm{Aut}(i)} \chi(i/\sigma) \mod |\mathrm{Aut}(i)| \right)_{i \in \Gamma/\cong} \end{aligned}$$

と定める. これらの概念を用いて, ABR の基本定理を次のように述べることができる.

Theorem 2.3 (ABR の基本定理)
Γ が条件 (F), (C) を満たすとき次はアーベル群の完全系列である.

$$0 \to \mathbf{Z}\Gamma \xrightarrow{\varphi} \mathbf{Z}^{\Gamma} \xrightarrow{\psi} \mathrm{Obs}(\Gamma) \to 0$$

Γ を (F),(C) を満たす f.cat として Γ^{κ} を対象は Γ と同じで, 射は Γ のエピ射のみからなる圏とする. このとき,

$$\begin{array}{ccccccccc} 0 & \to & \mathbf{Z}\Gamma^{\kappa} & \xrightarrow{\varphi'} & \mathbf{Z}^{\Gamma} & \xrightarrow{\psi} & \mathrm{Obs}(\Gamma) & \to & 0 \\ & & \exists_{\gamma} & & \| & & \| & & \\ 0 & \to & \mathbf{Z}\Gamma & \xrightarrow{\varphi} & \mathbf{Z}^{\Gamma} & \xrightarrow{\psi} & \mathrm{Obs}(\Gamma) & \to & 0 \end{array}$$

を可換にする $\mathbf{Z}\Gamma^{\kappa} \longrightarrow \mathbf{Z}\Gamma$ (Z-hom) が存在する.
これより, $\mathbf{Z}\Gamma \cong \mathbf{Z}\Gamma^{\kappa}$ (Z-alg iso) となり, はじめから Γ はエピ射のみからなる圏と仮定してよいことがわかる.

3 Abstract Mackey functors

以後, Γ を射はすべてエピ, 条件 (C) を満たす f.cat とする.

AMF を定義するため, Mackey functor の定義であらわれるスパンに対応する概念を定義する.

$\Gamma/x,y$ を対象, 射として

$$\mathrm{Obj}(\Gamma/x,y) = \{[x \xleftarrow{f} a \xrightarrow{g} y] \mid f,g \text{ in } \Gamma\}$$

$$\mathrm{hom}_{\Gamma/x,y}([x \leftarrow a \rightarrow y],[x \leftarrow b \rightarrow y]) = \left\{ h : a \to b \;\middle|\; \begin{array}{ccccc} & & a & & \\ & \swarrow & \downarrow h & \searrow & \\ x & \leftarrow & b & \rightarrow & y \end{array} \right\}$$

を持つ圏とする.
ただし,

$$[x \xleftarrow{f} a \xrightarrow{g} y] = [x \xleftarrow{f'} a' \xrightarrow{g'} y] \overset{\text{def}}{\Leftrightarrow} \begin{array}{ccccc} x & \xleftarrow{f} & a & \xrightarrow{g} & y \\ \| & & \downarrow \exists \sigma & & \| \\ x & \xleftarrow[f']{} & a' & \xrightarrow[g']{} & y \end{array} \qquad \sigma \in \mathrm{Iso}(a,a')$$

と定める.
Γ が f.cat であり条件 (F), (C) を満たすので, $\Gamma/x,y$ も f.cat でありこれもまた条件 (F), (C) を満たす.
ABR の基本定理より次は完全系列である.

$$0 \to \mathbf{Z}\Gamma/x,y \to \mathbf{Z}^{\Gamma/x,y} \to \mathrm{Obs}(\Gamma/x,y) \to 0$$

$\mathbf{Z}\Gamma/x,y$ に関しては次の同一視が成り立つ.

$$\mathbf{Z}\Gamma/x,y \cong \bigoplus_{i\in\Gamma/\cong} \mathbf{Z}(\Gamma(i,x)\times\Gamma(i,y)/\mathrm{Aut}(i))$$
$$\mathbf{Z}^{\Gamma/x,y} \cong \prod_{i\in\Gamma/\cong} (\mathbf{Z}^{\Gamma(i,x)\times\Gamma(i,y)})^{\mathrm{Aut}(i)}$$
$$\cong \prod_{i\in\Gamma/\cong} \mathrm{Mat}(\Gamma(i,x)\times\Gamma(i,y);\mathbf{Z})^{\mathrm{Aut}(i)}$$

この同一視により行列の積で

$$\mathbf{Z}^{\Gamma/x,y}\times\mathbf{Z}^{\Gamma/y,z} \to \mathbf{Z}^{\Gamma/x,z}$$

を与える.

Theorem 3.1 $[x \leftarrow a \to y] \in \Gamma/x,y$, $[y \leftarrow b \to z] \in \Gamma/y,z$ とする.
また, φ, ψ は前述と同様とする. このとき

$$\varphi([x \leftarrow a \to y])\,\varphi([y \leftarrow b \to z]) \in \mathrm{Ker}\,\psi$$

が成立する.

この定理は ABR の基本定理から出る. これより双線形写像

$$\mathbf{Z}\Gamma/x,y \times \mathbf{Z}\Gamma/y,z \longrightarrow \mathbf{Z}\Gamma/x,z$$

が定義される.
特に Γ が Pull Back を持つときにはこの積は Pull Back によって記述される.
この定理を用いることにより, Γ に関するスパンを次のように定義することができる.

$$\mathrm{Sp}(\Gamma):\quad \mathrm{Obj}(\mathrm{Sp}(\Gamma)) = \mathrm{Obj}(\Gamma)$$
$$\hom_{\mathrm{Sp}(\Gamma)}(y,\ x) = \left\{ [x \xleftarrow{f} a \xrightarrow{g} y] \mid a \in \Gamma,\ f,\ g \text{ in } \Gamma \right\}$$

ただし, 射の合成は先に与えた積で与える.
有限 G 集合の圏のスパンから Mackey functor を定義したのと同様にして, Γ のスパンから AMF を定義する.
一般の前加法圏 C に対して hom 集合を R-係数拡大した圏を RC と記す. 次が AMF の定義である.

Definition 3.2 (Definition of AMF)
Γ を (C) を満たし, 射がすべてエピである f.cat とする. また, R を 環とする.
M は圏 Γ 上の Abstract Mackey Functor(AMF)
$:\Leftrightarrow_{\mathrm{def}} M : R\,\mathrm{Sp}(\Gamma)^{\mathrm{op}} \to R\text{-}\mathrm{mod} : R$-additive functor

以後，$\mathrm{Mack}_R(\Gamma) := \mathrm{Func}(\mathrm{Sp}(\Gamma)^{op}, R\text{-mod})$ (functor category) と記す．また，$\mu_R(\Gamma)$ と書いて，$R\,\mathrm{Sp}(\Gamma)$ の path algebra とする．特に $\mathrm{Mack}_R(\Gamma) = \mu_R(\Gamma)\text{-mod}$ である．

Example 3.3 (Mackey Functor)
Γ を可移有限 G-集合からなる圏とする．
$\mathbf{Z}\Gamma$ は Burnside 環となり，このとき，AMF は普通の Mackey Functor と一致し，$\mathrm{Sp}(\Gamma)$ は MF の表現カテゴリーである．

Example 3.4 Γ を一点のみの対象とその恒等射からなる圏とする．
このとき，$\mathbf{Z}\Gamma = \mathbf{Z}$，$\mathbf{Z}^{\Gamma} = \mathbf{Z}$ となり $\mathrm{Sp}(\Gamma)$ は $\mathbf{Z}$ 行列の圏と一致する．また，AMF は R 加群である．

4 Decomposition of Abstract Mackey functor

C を圏としたとき C の中心 $\mathrm{Z}(C)$ を

$$\mathrm{Z}(C) := \mathrm{EndNat}(I_C)$$
$$= \left\{ (\omega_x : x \to x)_{x \in C} \;\middle|\; \begin{array}{ccc} x & \xrightarrow{\omega_x} & x \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ y & \xrightarrow{\omega_y} & y \end{array} (\forall x, y, \forall f : x \to y) \right\}$$

と定める．C が前加法圏のときは和積を

$$\omega + \sigma := (\omega_x + \sigma_x)_{x \in C},\quad \omega \cdot \sigma := (\omega_x \cdot \sigma_x)_{x \in C}$$

と定めることによって中心 $\mathrm{Z}(C)$ は環となる．

群 G と環 R に対して圏 $\mathrm{Hec}(G; R)$ を

$$\mathrm{Obj}(\mathrm{Hec}(G;\ R)) = \{\text{finite } G\text{-set}\}$$
$$\mathrm{Hec}(G;\ R)(Y,\ X) = \{\, X \times Y \text{ 型の } R \text{ 上の } G\text{-matrix} \,\}$$

とする．ただし，$(a_{x,y})_{x \in X,\ y \in Y}$ が G-matrix であるとは，$a_{gx,\ gy} = a_{x,\ y} (\forall g \in G)$ が成立することである．
R を torsion free commutative ring とし，$i \in \Gamma$ とする．
このとき

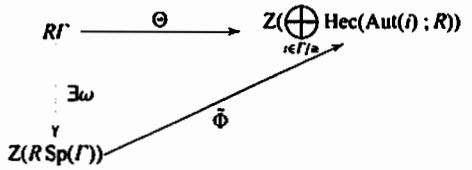
$$\begin{array}{rccc} \Phi_i : & R\,\mathrm{Sp}(\Gamma) & \longrightarrow & \mathrm{Hec}(\mathrm{Aut}(i); R) \\ & a & \longmapsto & \Gamma(i, a) \\ & [x \leftarrow a \to y] & \longmapsto & (|\Gamma/x, y|([x \xleftarrow{\lambda} i \xrightarrow{\mu} y], [x \leftarrow a \to y])) \\ \Phi = (\Phi_i)_{i \in \Gamma/\!\sim} : & R\,\mathrm{Sp}(\Gamma) & \longrightarrow & \displaystyle\bigoplus_{i \in \Gamma/\!\sim} \mathrm{Hec}(\mathrm{Aut}(i); R) \end{array}$$

$$\begin{array}{rccc} \Theta_i : & R\Gamma & \longrightarrow & Z(\mathrm{Hec}(\mathrm{Aut}(i); R)) \\ & [a] & \longmapsto & \Theta_i([a])_X = (|\Gamma(i,\ a)|\delta_{x,\ y})_{x,\ y \in X} \\ \Theta = (\Theta_i)_{i \in \Gamma/\!\sim} : & R\Gamma & \longrightarrow & \displaystyle\bigoplus_{i \in \Gamma/\!\sim} \mathrm{Hec}(\mathrm{Aut}(i); R) \end{array}$$

によって，関手 Φ，Θ を定める．
また，$\tilde{\Phi} : \mathrm{Z}(R\,\mathrm{Sp}(\Gamma)) \to \mathrm{Z}(\bigoplus_{i \in \Gamma/\!\sim} \mathrm{Hec}(\mathrm{Aut}(i); R))$ を $\tilde{\Phi}(\lambda)_i\ (\lambda \in \mathrm{Z}(R\,\mathrm{Sp}(\Gamma)))$ が $\mathrm{Aut}(i)$ コンポーネントが $\Phi_i(\lambda_i)$ で

あるような元とする.
特に, $Z(\bigoplus_{i\in\Gamma} \mathrm{Hec}(\mathrm{Aut}(i);R))$ の元は各 i 直和因子の $\mathrm{Aut}(i)$ コンポーネントの値によって完全に定まる.

Theorem 4.1 R を torsion free c.ring とし,Φ, $\tilde{\Phi}$, Θ を前述と同様とする.
このとき次が成り立つ.
(i)Φ は faithful.
(ii) ある $\omega : R\Gamma \to Z(R\,\mathrm{Sp}(\Gamma))$ が存在して



を可換にする.

$Q\Gamma$ における中心的原始べき等元は吉田 [6] によって具体的な記述が与えられている. その中心的原始べき等元分解 $1 = \sum_{i\in\Gamma} e_i$ に対し, $\varepsilon_i := \omega(e_i) = (\varepsilon_{ix})_{x\in\Gamma}$ とすれば $1 = \sum_{i\in\Gamma} \varepsilon_i$ を得る.
圏 $\varepsilon_i Q\,\mathrm{Sp}(\Gamma)$ を Γ と同じ対象を持ち, 射として

$$\hom_{\varepsilon_i Q\,\mathrm{Sp}(\Gamma)}(x,y) = \{f \in Q\,\mathrm{Sp}(\Gamma)(x,y) \mid f = f \circ \varepsilon_{ix}\}$$

を持つカテゴリーとする.

Theorem 4.2 次が成り立つ.

$$Q\,\mathrm{Sp}(\Gamma) \overset{M}{\sim} \bigoplus_{i\in\Gamma} \varepsilon_i Q\,\mathrm{Sp}(\Gamma) \text{ (森田同値)}$$

特に定理の場合のように $R = Q$ のときには Φ は fully faithful となり

$$\varepsilon_i Q\,\mathrm{Sp}(\Gamma) \cong \mathrm{Hec}(\mathrm{Aut}(i) ; Q) \text{(圏同値)}$$

が成り立つ. さらに $Z(\mathrm{Hec}(G;Q)) \cong Z(QG)$ から

$$\left|\{\text{c.p.i of } Q\,\mathrm{Sp}(\Gamma)\}\right| = \sum_{i\in\Gamma/\cong} \left|\{\text{conjugacy class of } \mathrm{Aut}(i)\}\right|$$

がわかる.

5 induction, restriction

最後に, induction functor, restriction functor のコンマ圏を用いた一般化を与える.
$a \in \Gamma$ に対して, 自然に環準同型 $\mu_R(\Gamma/a) \to \mu_R(\Gamma)$ を定義される.

Definition 5.1 M : AMF of Γ, $a \in \Gamma$
(i) 関手 ind_a を

$$\begin{array}{rccc} \mathrm{ind}_a : & \mathrm{Mack}_R(\Gamma/a) & \to & \mathrm{Mack}_R(\Gamma) \\ & M & \mapsto & \mu_R(\Gamma) \otimes_{\mu_R(\Gamma/a)} M \end{array}$$

と定め，これを induction と呼ぶ．

(ii) 関手 res_a を

$$\begin{array}{rccc} \mathrm{res}_a : & \mathrm{Mack}_R(\Gamma) & \to & \mathrm{Mack}_R(\Gamma/a) \\ & N & \mapsto & N \end{array}$$

と定め，これを restriction と呼ぶ．

特に ind_a は res_a の左随伴である．

参考文献

[1] Andreas W. M. Dress. Contributions to the theory of induced representations. In *Algebraic K-theory, II: "Classical" algebraic K-theory and connections with arithmetic (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972)*, pp. 183–240. Lecture Notes in Math., Vol. 342. Springer, Berlin, 1973.

[2] Jacques Thévenaz. Some remarks on G-functors and the Brauer morphism. *J. Reine Angew. Math.*, Vol. 384, pp. 24–56, 1988.

[3] Jacques Thévenaz and Peter Webb. The structure of Mackey functors. *Trans. Amer. Math. Soc.*, Vol. 347, No. 6, pp. 1865–1961, 1995.

[4] Tomoyuki Yoshida. On G-functors. I. Transfer theorems for cohomological G-functors. *Hokkaido Math. J.*, Vol. 9, No. 2, pp. 222–257, 1980.

[5] Tomoyuki Yoshida. On G-functors. II. Hecke operators and G-functors. *J. Math. Soc. Japan*, Vol. 35, No. 1, pp. 179–190, 1983.

[6] Tomoyuki Yoshida. On the Burnside rings of finite groups and finite categories. In *Commutative algebra and combinatorics (Kyoto, 1985)*, Vol. 11 of *Adv. Stud. Pure Math.*, pp. 337–353. North-Holland, Amsterdam, 1987.

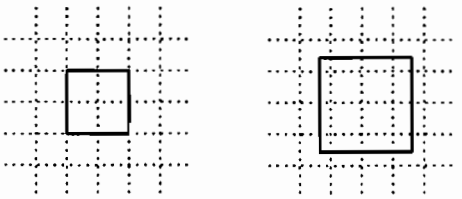
On the number of integer points in a lattice polytope

田上　真
東北大学大学院理学研究科数学専攻
e-mail: tagami@math.tohoku.ac.jp

1　序文

この研究は Arseniy Akopyan(University of Texas at Brownsville) との共同研究で、問題は Rom Pinchasi(Israel Institute of Technology) に依るものです。

P を $\mathbb{R}^d$ の中の d 次元 polytope、即ち有限個の点で張られる convex hull とします。この時、P が *lattice polytope* であるとはその頂点が全て $\mathbb{Z}^d$ の元である時を言います。以下 $\mathbb{Z}^d$ の元を lattice points と言う事にします。例えば



左は lattice polytope ですが、右は lattice polytope ではありません。このように相似変換によって polytope は lattice polytope であるかどうかは変わります。この報告で考えたい問題は lattice polytope を自然数倍で拡大した時に、その中の lattice points の数を勘定すると言うもので、この種の問題は Ehrhart 理論と呼ばれ、多くの研究者によって研究されています (Ehrhart 理論については [2] とその中の references を参照の事)。特に考えたい問題は次です:

問題 1. *Lattice polytope* を自然数倍した時に、その中にある *lattice points* の数の *parity* について何か規則性はあるか？

P を lattice polytope、t を自然数とします。この時、$tP := \{tx \mid x \in P\}$ とします。

上記の問題に対して、例えば 1 次元の場合に、端点が lattice points である長さ n の線分 L を考えると、

$$\sharp(L \cap \mathbb{Z}) = n + 1,$$

$$\sharp(2L \cap \mathbb{Z}) = 2n + 1.$$

となります。この事から 1 次元の lattice polytope を 2 倍すると必ず奇数個の lattice points を含んでいる事が解ります。次に 2 次元の場合を考えます。

よって2次元 lattice polytope を2倍してもその中にある lattice points の数は奇数個とは限らない事が解ります。一方、2次元 lattice polygon (頂点が lattice points である polygon) について、次の有名な定理があります。

定理 1 (Pick). *P を2次元 lattice polygon とする。A をその area、I で P の内部にある lattice points の数、B で P の境界上にある lattice points の数を表すとする。この時、次の等式が成り立つ:*

$$A = I + \frac{1}{2}B - 1.$$

A'、I'、B' をそれぞれ $4P$ の area、その内部にある lattice points の数、境界上の lattice points の数を表すとします。この時、Pick's theorem より、

$$A' = I' + \frac{1}{2}B' - 1$$

となり、$A' = 16A = 16I + 8B - 16 \in 2\mathbb{Z}$、$B' = 4B$、$\sharp(4P \cap \mathbb{Z}^2) = I' + B'$ であるので、

$$\sharp(4P \cap \mathbb{Z}^2) = A' + \frac{1}{2}B' + 1 \in 2\mathbb{Z} + 1$$

となります。この事から lattice polygon を4倍すると必ず奇数個の lattice points を含んでいる事が解ります。この事を一般化して次の問題を考えます。

問題 2. *(i)* 3次元でも *lattice polytope* を4倍すると必ず奇数個の *lattice points* を含むのか？

(ii) parity ではなく一般の素数 p に対して、*lattice points* (mod p) について何か規則性はあるか？

これらの問題に対して一般的な定式化を与える為に、いくつかの準備をします。

定義 1 (Simplicial complex). *T を $\mathbb{R}^d$ の中の simplices の集合で、その simplices の最大次元は d であるとします。この時、T が d 次元 simplicial complex であるとは次が成り立つ時を言う:*

(i) T の任意の simplex の face はまた T に属している。

(ii) 任意の σ_1、$\sigma_2 \in T$ に対して、$\sigma_1 \cap \sigma_2$ は σ_1、σ_2 両方の *face* である。

定義 2 (Euler characteristic). *T を d 次元 simplicial complex、f_i を T の i 次元 simplex の数とする。この時、T の Euler characteristic $\chi(T)$ を次で定義する:*

$$\chi(T) := \sum_{i=0}^{d} (-1)^i f_i = f_0 - f_1 + f_2 - f_3 + \cdots.$$

$\chi(T)$ が位相不変量であることはよく知られています。例えば、P を polytope とすると、P は単体分割できるので、P は simplicial complex と見ることができます。また P は明らかに d 次元球 B^d と同相であるので、d 次元単体 σ_d の Euler characteristic $\chi(\sigma_d)$ と一致します。よって

$$\chi(P) = \chi(\sigma_d) = 1.$$

また、もし simplicial complex T が $(d-1)$ 次元球面 S^{d-1} と同相ならば、

$$\chi(T) = 1 - (-1)^d$$

となります。次が主定理です:

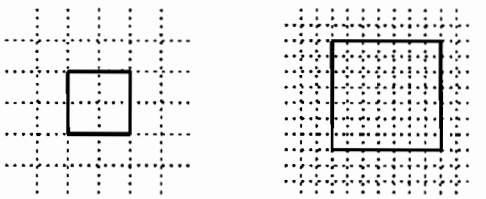
定理 2. 任意の自然数 d、n $(n > 1)$ が与えられた時、ある自然数 t が存在し、任意の d 次元 *simplicial complex* T でその頂点が *lattice points* であるものに対して、tT の中の *lattice points* の数は $\pmod n$ で $\chi(T)$ になる。

2 Ehrhart 多項式と定理 2 の証明

定理 2 を証明するために、いくつか準備をします。$S \subset \mathbb{R}^d$ として、

$$L_S(t) := \sharp(tS \cap \mathbb{Z}^d)$$

と置きます。例えば



P $\qquad\qquad$ kP

とすると、$L_P(k) = (2k+1)^2$ となり、$L_P(k)$ は k についての 2 次多項式になります。実際には一般に次の定理が知られています:

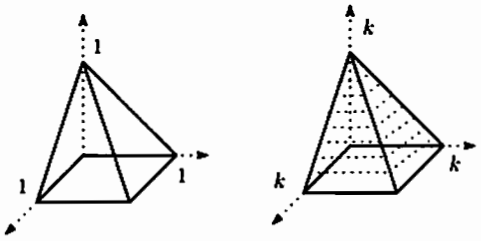
定理 3 (Ehrhart [3]). P を d 次元 *lattice polytope* とする。この時、$L_P(k)$ は k についての d 次の多項式になる。

注意. 1. 定理 3 の多項式を P の *Ehrhart* 多項式と言います。$L_P(k)$ の定数項は必ず 1 になり、最高次の係数は $vol(P)$、また係数は整数とは限りませんが、それらは有理数で $\frac{1}{d!}\mathbb{Z}$ に含まれていることが知られています。

例 1.

$$P = \{(x_1, x_2, \ldots, x_d) \in \mathbb{R}^d \mid 0 \leq x_1, x_2, \ldots, x_{d-1} \leq 1 - x_d \leq 1\}$$

とおくと、P は d 次元 *lattice polytope* で、特に $d = 3$ の場合を描いてみると、次の様なピラミッド型になります:



層毎に *lattice point* の数を数える事と冪和の公式より、

$$L_P(k) = 1^2 + 2^2 + \cdots + (k+1)^2 = \frac{1}{3}B_3(k+2) = \frac{1}{3}k^3 + \frac{3}{2}k^2 + \frac{13}{6}k + 1$$

となります。ここで $B_3(x)$ は 3 次の *Bernoulli* 多項式を表しています。一般に k 次の *Bernoulli* 多項式 $B_k(x)$ は次の母関数で与えられます:

$$\frac{ze^{xz}}{e^z - 1} = \sum_{k\geq 0} \frac{B_k(x)}{k!} z^k.$$

また一般の次元の場合には

$$L_P(k) = \frac{1}{d}\{B_d(k+2) - B_d\}$$

となっています。ここで、B_d は d 番目の *Bernoulli* 数です。

次に Ehrhart 級数を導入します。

$$\mathrm{Ehr}_P(z) := 1 + \sum_{k\geq 1} L_P(k) z^k.$$

この形式的冪級数を P の Ehrhart 級数と言います。$L_P(k)$ が d 次の多項式であることから、$s \leq d$ に対して

$$\mathrm{Ehr}_P(z) = \frac{a_0 + a_1 z + \cdots + a_s z^s}{(1-z)^{d+1}}$$

と有理関数の形に一意的に書けます。$a_0(P) = 1$、$a_1(P) = L_P(1) - (d+1)$、$a_d(P) = L_{P^\circ}(1)$ (P° は P の内部を表す) 等が知られています。

2 次元の場合に考えた Pick の定理 は Ehrhart の定理から次の様にして出てきます。P を 2 次元 lattice polytope とすると Ehrhart 級数は

$$\mathrm{Ehr}_P(z) = \frac{1 + a_1 z + a_2 z^2}{(1-z)^3} = \sum_{t\geq 0} L_P(t) z^t$$

という形になります。よって展開して、Ehrhart 多項式 $L_P(t)$ は次のように表されます:

$$L_P(t) = 1 + \frac{1}{2}(3 + a_1 - a_2)t + \frac{1}{2}(1 + a_1 + a_2)t^2.$$

ここで $a_1 = L_P(1) - 3 = I + B - 3$, $a_2 = L_{P^\circ}(1) = I$ であり、注意 1 で述べたように $L_P(t)$ の 2 次の係数は P の area であるので、次の Pick の定理を得ることができます:

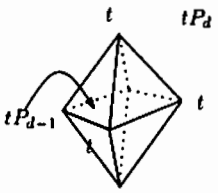
$$area(P) = I + \frac{1}{2}B - 1.$$

一般に次の事が知られています。

定理 4 (Stanley [4]). 任意の *Ehrhart series* の a_i は全て非負整数である。

例 2. 次の d 次元 *cross polytope* を考えます:

$$P_d := \left\{(x_1,\dots,x_d) \in \mathbb{R}^d \mid |x_1| + \cdots + |x_d| \le 1\right\}.$$



また層毎に *lattice points* の数を数えることにより、

$$L_{P_d}(t) = 2 + 2L_{P_{d-1}}(1) + \cdots + 2L_{P_{d-1}}(t-1) + L_{P_{d-1}}(t).$$

よってその *Ehrhart* 級数は

$$\mathrm{Ehr}_{P_d}(z) = \frac{1+z}{1-z}\mathrm{Ehr}_{P_{d-1}}(z) = \cdots = \frac{(1+z)^d}{(1-z)^{d+1}}$$

となり、特に $a_i = \binom{d}{i}$ となります。またこれから逆に *Ehrhart* 多項式は次で与えられることが解ります:

$$L_{P_d}(t) = \sum_{k=0}^{d} \binom{d}{k}\binom{t-k+d}{d}.$$

定理 2 の証明に入ります。

補題 1. $P \subset \mathbb{R}^d$ を d 次元 *lattice polytope*、p を任意の素数とする。$l := \lfloor \log_p d \rfloor$、$[x]$ は x を超えない最大の整数とする。この時任意の整数 $k > l$ に対して、

$$L_P(p^k) = \sharp(p^k P \cap \mathbb{Z}^d) \equiv 1 \pmod{p^{k-l}}.$$

Proof. 定理 4 より、

$$L_P(t) = \binom{t+d}{d} + a_1\binom{t+d-1}{d} + \cdots + a_{d-1}\binom{t+1}{d} + a_d\binom{t}{d},$$

a_i 達は非負整数と書ける。

$t = p^k$、$m \le d \le p^{l+1} - 1$ として、$m = p^{\alpha_m} m'$, $\alpha_m \le l$, $(m', p) = 1$ と置く。この時、

$$\frac{m + p^k}{p^{\alpha_m}} \equiv \frac{m}{p^{\alpha_m}} = m' \pmod{p^{k-l}}$$

となる。よって、

$$\binom{t+d}{d} = \frac{(t+d)(t+d-1)\cdots(t+1)}{d!} = \prod_{m=1}^{d} \frac{m+p^k}{m} \equiv 1 \pmod{p^{k-l}}.$$

次に $\binom{t+d-i}{d}$ $(1 \le i \le d)$ を $\pmod{p^{k-l}}$ で評価する。次の補題が知られている:

補題 2 (Kummer's theorem ([1] Theorem 10.2.2)). 非負整数 $n \geq m \geq 0$ が与えられた時、$\binom{n}{m}$ に現れる p の最大冪は m、$n-m$ を p 進展開で表して、和を取った時の繰り上がりの数と等しい。

例 3. 補題 2 を用いて $\binom{2010}{622}$ の 5 冪を計算してみましょう。$2010-622$、622 をそれぞれ 5 進展開して、

$$2010 - 622 = 2 \cdot 5^4 + 1 \cdot 5^3 + 0 \cdot 5^2 + 2 \cdot 5 + 3 = 21023\ (5),$$

$$622 = 4 \cdot 5^3 + 4 \cdot 5^2 + 4 \cdot 5 + 2 = 4442\ (5).$$

$21023 + 4442$ (5) において 4 回の繰り上がりが起こるので、$\binom{2010}{622} = 5^4 \cdot m'$、$(m', 5) = 1$ と言う事が解ります。

$i = 1, 2, \ldots, d$ に対して、$\binom{t+d-i}{d}$ の p 冪を考える。

$$d = c_l p^l + c_{l-1} p^{l-1} + \cdots + c_0,\ (0 \leq c_i \leq p-1,\ c_l \neq 0) \tag{1}$$

また

$$\begin{aligned}(t+d-i) - d = t - i &= p^k - (s_l p^l + \cdots + s_0) \\ &= (p-1)p^{k-1} + (p-1)p^{k-2} + \cdots + (p-1)p^{l+1} + \cdots. \end{aligned} \tag{2}$$

$$t + d - i = p^k + t_l p^l + \cdots + t_1 p + t_0 \tag{3}$$

(1)、(2)、(3) より、$(t-i)+d$ の 5 進展開における演算には少なくとも $k-l$ 回の繰り上がりが起こる。よって補題 2 より、$i = 1, \ldots, d$ に対して

$$\binom{t+d-i}{d} \equiv 0 \pmod{p^{k-l}}.$$

以上より、

$$\begin{aligned} L_P(t) &= \binom{t+d}{d} + a_1 \binom{t+d-1}{d} + \cdots + a_{d-1} \binom{t+1}{d} + a_d \binom{t}{d} \\ &\equiv 1 \pmod{p^{k-l}}. \end{aligned}$$

□

Theorem 2. 任意の自然数 d, n $(n > 1)$ が与えられた時、ある自然数 t が存在し、任意の d 次元 simplicial complex T でその頂点が lattice points であるものに対して、tT の中の lattice points の数は $\pmod n$ で $\chi(T)$ になる。

Proof.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

と素因数分解する。この時、

$$\beta_i = \alpha_i + [\log_{p_i} d],$$

$$t = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} \cdots p_s^{\beta_s}$$

とする。

Δ を頂点が lattice point にある simplex とする。この時、Lemma 1 より $i=1,\dots,s$ に対して、

$$\sharp(t\Delta\cap\mathbb{Z}^d)\equiv 1 \pmod{p_i^{\alpha_i}}.$$

よって中国剰余定理より、

$$\sharp(t\Delta\cap\mathbb{Z}^d)\equiv 1 \pmod{n}.$$

T を一般の d 次元 simplicial complex としてその頂点が lattice point にあるものとする。この時、$\chi(T)$ は simplex 上で 1 の値を取る simplicial complex 上の additive function になっている。また上記の simplex の場合より、lattice points の数 (mod n) もそれぞれの simplex 上で 1 の値を取る additive function になっている。よってそれらは一致しなければならず、

$$\sharp(tT\cap\mathbb{Z}^d)\equiv\chi(T) \pmod{n}.$$

□

Theorem 2 の証明から解るように、$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$、$\beta_i=\alpha_i+[\log_{p_i}d]$ として、

$$t=p_1^{\beta_1}p_2^{\beta_2}p_3^{\beta_3}\cdots p_s^{\beta_s}$$

と取れば十分であることが解ります。また内部の lattice points の数についても次のように同様の事が言えます:

Cororally 1. *P を d 次元 lattice polytope、P° をその内部、$n>1$ を自然数とする。この時、ある自然数 t が存在し、*

$$\sharp(tP^\circ\cap\mathbb{Z}^d)\equiv(-1)^d \pmod{n}.$$

Proof. ∂P で P の境界を表すとする。P 及び ∂P はそれぞれ B^d, S^{d-1} と同相であるから、

$$\chi(P)=1,\chi(\partial P)=1-(-1)^d.$$

Theorem 2 の t を取ってくると、

$$\sharp(tP^\circ\cap\mathbb{Z}^d)=\sharp(tP\cap\mathbb{Z}^d)-\sharp(t\partial P\cap\mathbb{Z}^d)$$

$$\equiv\chi(P)-\chi(\partial P)=(-1)^d \pmod{n}.$$

□

例 4 (semimagic squares). 正方行列が *Semimagic square* であるとはその成分が非負整数で、その任意の行和と列和が同じである時を言います。

3	0	0
0	1	2
0	2	1

普通考えられている *magic square* は各成分を $1\sim n^2$ から異なるように取り、対角線の和も同じでなければいけませんが、ここでは簡単の為、*semimagic square* だけを考えます。n 次の *semimagic square* でその行

和、列和が t のものを $H_n(t)$ と書きます。実際に $H_n(t)$ はある *lattice polytope* の *Ehrhart* 多項式になっている事が次の様にして解ります。n 次の *Birkhoff-von Neumann polytope* を取ります:

$$B_n := \left\{ \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ & \cdots & \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} \in \mathbb{R}^{n^2} : x_{jk} \geq 0, \sum_j x_{jk} = 1 \textit{ for all } 1 \leq k \leq n, \sum_k x_{jk} = 1 \textit{ for all } 1 \leq j \leq n \right\}.$$

B_n は *lattice polytope* で

$$tB_n := \left\{ \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ & \cdots & \\ x_{n1} & \cdots & x_{nn} \end{pmatrix} \in \mathbb{R}^{n^2} : x_{jk} \geq 0, \sum_j x_{jk} = t \textit{ for all } 1 \leq k \leq n, \sum_k x_{jk} = t \textit{ for all } 1 \leq j \leq n \right\}.$$

よって

$$H_n(t) = \sharp(tB_n \cap \mathbb{Z}^{n^2}) = L_{B_n}(t).$$

$\dim B_n = (n-1)^2$ が知られているので、定理 2 または補題 1 より $l = \lceil \log_p (n-1)^2 \rceil$ とすると、$k > l$ に対して、

$$H_n(p^k) \equiv 1 \pmod{p^{k-l}}.$$

例えば $n = 11$ とすると、$k > 2$ に対して

$$H_{11}(5^k) \equiv 1 \pmod{5^{k-2}}.$$

参考文献

[1] T. Andreescu and D. Andrica, *Number Theory: Structures, Examples and Problems*, Birkhaeuser Boston, 2009.

[2] M. Beck and S. Robins, *Computing the Continuous Discretely*, Springer, 2006.

[3] E. Ehrhart, Sur les polyedres rationnels homothétiquesan dimensions. *CR Acad. Sci. Paris*, 254:616-618, 1962.

[4] R.P. Stanely, Decompositions of rational convex polytopes. *Annals of Discrete Mathematics*, 6:333-342, 1980.

On some quotients of d-dimensional dual hyperovals in $PG(d(d+3)/2, 2)$

香川高専　谷口浩朗 (Hiroaki Taniguchi)*
Kagawa National College of Technology

1　はじめに

射影空間 $PG(m, 2)$ 内の高次元双対超卵形 (dimensional dual hyperoval, DHO) は C. Huybrechts と A. Pasini [5] により以下のように定義された.

定義 1 ($GF(q)$ 上の DHO). m-次元射影空間 $PG(m, q)$ における d-次元部分空間の集合 S が, $PG(m, q)$ における d-次元双対超卵形であるとは, 以下のことが成り立つことである:
(1) S に属するどの 2 個の d-部分空間も 1 点で交わり,
(2) S に属するどの異なる 3 個の d-部分空間も共通点を持たず,
(3) S に属する d-部分空間達は $PG(m, q)$ を生成し,
(4) S は $q^d + q^{d-1} + \cdots + q + 2$ 個の d-部分空間から成る.

本稿では $GF(2)$ 上の高次元双対超卵形のみを考察するが, $q > 2$ の場合の双対超卵形も同様に研究されている. (有名なものとしては, M_{22} が作用する $PG(5, 4)$ における 2 次元双対超卵形の例がある.) $GF(2)$ 上の d-次元の双対超卵形が生成する射影空間の次元 n については, $2d \leq n \leq d(d+3)/2 + 2$ が示されている [12] が, 本当は $2d \leq n \leq d(d+3)/2$ であろうと予想されている. その最大の次元と考えられる $PG(d(d+3)/2, 2)$ には, 現在
（1） Huybrechts' DHO [4],
（2） Buratti-Del Fra's DHO [1],[13],
（3） Veronesean DHO [10], [12],
（4） Veronesean DHO の変形 [9],
の 4 種類の（同型でない）双対超卵形が構成されている.

*E-mail address: taniguchi@dg.kagawa-nct.ac.jp

ここでは, $d \geq 3$ の場合, (ある $n \geq d+1$ にたいし有限体 $GF(2^n)$ のガロア群 $Gal(GF(2^n)/GF(2))$ の生成元 σ を用いて,) 「(4)Veronesean DHO の変形」の quotient である d-次元双対超卵形 T_σ を $PG(3d,2)$ に構成する. さらに 2 個のガロア群の生成元 σ, τ にたいし, T_σ が T_τ と同型であるならば, 部分体 $GF(2^d)$ において $\sigma = \tau$ または $\sigma = \tau^{-1}$ となることを説明する. このことより, $PG(3d,2)$ には「(4)Veronesean DHO の変形」の quotient である同型でない高次元双対超卵形が多く存在することがわかる. (quotient の正確な定義については A. Psini [6], 8.2 および 8.3 をご覧下さい.)

2 「Veronesean DHO の変形」型の DHO

$n \geq d+1 \geq 3$ とし, $H \subset GF(2^n)$ を $d+1$ 次元ベクトル空間とする. 以下のことが簡単に分かる.

命題 1. $s,t \in H^\times$ にたいし $b(s,t) \in GF(2^n) \oplus GF(2^n)$ を次を満たすように定める.
(b1) $b(s,s) = (s^2, 0)$,
(b2) $b(s,t) = b(t,s)$,
(b3) $b(s,t) \neq (0,0)$,
(b4) $b(s,t) = b(s',t')$ *if and only if* $\{s,t\} = \{s',t'\}$,
(b5) $\{b(s,t) \mid t \in H^\times\} \cup \{(0,0)\}$ *is a vector space over* $GF(2)$, *and*

このとき, $X(s) := \{b(s,t) \mid t \in H \backslash \{0\}\}$ および $X(\infty) := \{b(s,s) \mid s \in H \backslash \{0\}\}$ は $PG(GF(2^n) \oplus GF(2^n))$ の d-次元部分空間であり $S = \{X(s) \mid s \in H^\times\} \cup \{X(\infty)\}$ は d-次元双対超卵形となる.

例 1 ((3) Veronesean DHO). n を十分大きい整数, $GF(2^n)$ の $(d+1)$-次元 $GF(2)$-ベクトル空間 H を「その 1 つの基底 $\{e_0, e_1, \ldots, e_d\}$ が $\{e_i e_j \mid 0 \leq i \leq j \leq d\}$ が一次独立になる」ようにとる. σ をガロア群 $Gal(GF(2^n)/GF(2))$ の生成元とする. $s,t \in H^\times$ にたいし, 次のように $b(s,t)$ を定める.

$$b(s,t) := (st, s^\sigma t + s t^\sigma).$$

このとき, $b(s,t)$ は $(b1)$ - $(b5)$ を満たし, この $\{b(s,t)\}$ を用いて 命題 *1* より d-次元双対超卵形 S が構成される. R を $\{(e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma) \mid 0 \leq i \leq j \leq d\}$ で生成されたベクトル空間とするとき S は $PG(d(d+3)/2, 2) = PG(R)$ を張ることがわかる. (*[9]* および *[13].*) S は *Thas, Van Maldeghem [10]* によって構成された「*(3) Veronesean DHO*」と同型であることが吉荒 *[13]* によって証明されている.

$d=2$ の場合は，$GF(2)$ 上の DHO は Del Fra [2] により完全に分類されているので，以下 $d\geq 3$ とする．$(d+1)$-次元ベクトル空間 H の 0 でない元 u にたいし，$Supp(u)$ を基底 $\{e_0,e_1,\ldots,e_d\}$ の部分集合 M で $u=\sum_{e_i\in M}e_i$ となっているものとする．$H'\subset H$ を $\{e_1,e_2,\ldots,e_d\}$ で生成されたベクトル空間とし

$$H\ni s=\sum_{i=0}^{d}\alpha_i e_i\mapsto \bar{s}=\sum_{i=1}^{d}\alpha_i e_i\in H' \tag{1}$$

を自然な射影とする．ここに $\alpha_i\in GF(2)$ $(0\leq i\leq d)$ である．

定義 2 ([9])．χ を H' において定義された「部分集合 $H'\backslash\{0\}$ の特性関数」とする，また $u\in H$ にたいし $J(u)$ を，$\bar{u}=0$ の場合は $\{0\}$，それ以外は $Supp(\bar{u})$ と定める．これにより関数 $H\times H\ni(s,t)\mapsto x_{s,t}\in GF(2)$ が以下のように定義される．

$$x_{s,t}:=\chi(\bar{s}+\bar{t})+\sum_{w\in J(t)}\chi(\bar{s}+w).$$

このとき次の条件が成り立っている：([9] の Section 7 参照.)

$(x1)$ $x_{s,t}=x_{s,t+e_0}=x_{s+e_0,t}=x_{s+e_0,t+e_0}$,

$(x2)$ $x_{s,w}=0$ for $w\in\{0,e_0,e_1,\ldots,e_d\}$,

$(x3)$ $x_{s,t}=x_{w,t}$ for $w\in Supp(\bar{s})\backslash Supp(\bar{t})$,

$(x4)$ $x_{s,t}+x_{t,s}=x_{w,s}+x_{w,t}$ for $w\in Supp(\bar{s})\cap Supp(\bar{t})$,

$(x5)$ $x_{s,s}=x_{w,s}$ for $w\in Supp(\bar{s})$, and

$(x6)$ $x_{s,t}+x_{s,s}=x_{s,s+t}$.

この $\{x_{s,t}\}$, を用いて $s,t\in H$ に対して $b(s,t)$ を次のように定義する．

定義 3 (「Veronesean DHO の変形」型の DHO を定める $b(s,t)$)．σ をガロア群 $Gal(GF(2^n)/GF(2))$ の生成元とする．$GF(2^n)\oplus GF(2^n)$ において，$s,t\in H^{\times}$ にたいし $b(s,t)$ を

$$\begin{aligned} b(s,t) &= (st,s^{\sigma}t+st^{\sigma}) \\ &+ x_{s,t}\sum_{w\in Supp(s)}(we_0+w^2,w^{\sigma}e_0+we_0^{\sigma}) \\ &+ \sum_{w\in Supp(t)}x_{w,s}(we_0+w^2,w^{\sigma}e_0+we_0^{\sigma}) \end{aligned} \tag{2}$$

と定め、 $s=0$ または $t=0$ の場合 $b(s,t)=(0,0)$ と定める．

このとき $\{b(s,t) \mid s,t \in H^\times\}$ は条件 (b1), (b2), (b5) とさらに 次の条件 (b6) を満たすことがわかる. さらに以下の和公式 (3) も満たす.

命題 2. 上記, 定義 *3*により定まる $\{b(s,t) \mid s,t \in H^\times\}$ は次の条件を満たす:

(b1) $b(s,s) = (s^2, 0)$,

(b2) $s, t \in H^\times$ にたいし $b(s,t) = b(t,s)$,

(b5) $\{b(s,t) \mid t \in H^\times\} \cup \{(0,0)\}$ は $GF(2)$ 上のベクトル空間,

(b6) $w, w' \in \{e_0, e_1, \ldots, e_d\}$ にたいし $b(w,w') = (ww', w^\sigma w' + ww'^\sigma)$.

さらに, $H^\times$ の元 s, t_1, t_2 (ただし $t_1 \neq t_2$) にたいし, **和公式**

$$b(s,t_1) + b(s,t_2) = b(s, t_1 + t_2 + \alpha\{s,t_1,t_2\}(s + e_0)) \tag{3}$$

が成り立つ. ここに $\bar{t_1} \neq 0$, $\bar{t_2} \neq 0$, $\bar{s} \neq \bar{t_1} + \bar{t_2}$ のとき $\alpha\{s,t_1,t_2\} = \chi(\bar{s} + \bar{t_1}) + \chi(\bar{s} + \bar{t_2}) + \chi(\bar{t_1} + \bar{t_2})$ と定め, それ以外は $\alpha\{s,t_1,t_2\} = 0$ と定める.

例 2 ((4) Veronesean DHO の変形). n を十分大きい整数とし, $GF(2^n)$ の $(d+1)$-次元 $GF(2)$-ベクトル空間 H を「その 1 つの基底 $\{e_0, e_1, \ldots, e_d\}$ が $\{e_i e_j \mid 0 \leq i \leq j \leq d\}$ が一次独立になる」ようにとる. σ をガロア群 $Gal(GF(2^n)/GF(2))$ の生成元とする. このとき $s,t \in H^\times$ にたいし, 定義 *3* によって定められた $b(s,t)$ は命題 *1* の条件 (b1) - (b5) をみたし さらに命題 *2* (b6) も満たしている. よって双対超卵形 S が命題 *1* より構成される. R を $\{(e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma) \mid 0 \leq i \leq j \leq d\}$ で生成されたベクトル空間とするとき この S は $PG(d(d+3)/2, 2) = PG(R)$ を張ることがわかる. (*[9].*)

3 quotient T_σ の構成

$l \geq 3$ とし, $e_0 \in GF(2^{dl})$ を, $GF(2^d)$ 上 e_0 が $GF(2^{dl})$ を体として生成するように選んでおく. $GF(2^d)$ の基底 $\{e_1, e_2, \ldots, e_d\}$ も固定しておく. この節では, 第 2 節のベクトル空間 H を $H := \langle GF(2^d), e_0 \rangle$ と固定して議論を進める. このとき $H' = GF(2^d)$ となっている. また σ をガロア群 $Gal(GF(2^{dl})/GF(2))$ の生成元とする. $GF(2^{dl}) \oplus GF(2^{dl})$ 内でベクトル空間 U を次のように定義する.

$$U := \{(s+t, s^\sigma t + s t^\sigma) \mid s,t \in GF(2^d)\}.$$

同様ベクトル空間 V を次のように定義する.

$$V := \langle (e_0e_1 + e_1^2, e_0^\sigma e_1 + e_0e_1^\sigma), (e_0e_2 + e_2^2, e_0^\sigma e_2 + e_0e_2^\sigma), \\ (e_0e_3 + e_3^2, e_0^\sigma e_3 + e_0e_3^\sigma), \ldots, (e_0e_d + e_D^2, e_0^\sigma e_d + e_0e_d^\sigma)\rangle.$$

ベクトル空間 W も $W := \langle (e_0^2, 0)\rangle$ と定義する. このとき $U = GF(2^d) \oplus GF(2^d)$ であることがわかる. さらに, e_0 の取り方により, V は d-次元ベクトル空間であり

$$U \oplus V \oplus W \subset GF(2^{dl}) \oplus GF(2^{dl})$$

となっていることもわかる. また, 以下の式から $b(s+e_0, t+e_0) \in U \oplus V \oplus W$ がわかる.

$$\begin{aligned} b(s+e_0, t+e_0) &= b(s,t) + (s^2+t^2, 0) \\ &\quad + (e_0(s+t) + (s+t)^2, e_0^\sigma(s+t) + e_0(s+t)s^\sigma) + (e_0^2, 0) \\ &= (st, s^\sigma t + st^\sigma) + (s^2+t^2, 0) \\ &\quad + (x_{s,t}+1) \sum_{w \in Supp(s)} (we_0 + w^2, w^\sigma e_0 + we_0^\sigma) \\ &\quad + \sum_{w \in Supp(t)} (x_{w,s}+1)(we_0 + w^2, w^\sigma e_0 + we_0^\sigma) + (e_0^2, 0). \end{aligned}$$

同様にして $b(s,t) \in U \oplus V \oplus W$, $b(s, t+e_0) \in U \oplus V \oplus W$, $b(s+e_0, t) \in U \oplus V \oplus W$ などが成り立つので, $s, t \in H^\times$ に対して $b(s,t)$ 達が生成する空間が $U \oplus V \oplus W$ に含まれることが分かる. さらに生成する空間が本当に $U \oplus V \oplus W$ に等しいことも簡単に確かめられる. 次に, 射影 π を

$$\pi : U \oplus V \oplus W \to U \oplus W = \{(x,y) \mid x, y \in GF(2^d)\} \oplus \langle (e_0^2, 0)\rangle$$

と定義すると, $s, t \in GF(2^d)$ に対して, 次が成り立つことがわかる.

$$\begin{aligned} &\pi(b(s,t)) = (st, s^\sigma t + st^\sigma) \in U, \\ &\pi(b(s+e_0, t)) = (st, s^\sigma t + st^\sigma) + (t^2, 0) \in U, \\ &\pi(b(s, t+e_0)) = (st, s^\sigma t + st^\sigma) + (s^2, 0) \in U, \\ &\pi(b(s+e_0, t+e_0)) = (st, s^\sigma t + st^\sigma) + (s^2+t^2, 0) + (e_0^2, 0) \in U \oplus W. \end{aligned}$$

このことを用いて, $(b3)$, $(b4)$ が成り立つことが証明される.

命題 3. $s, t \in H^\times = \langle GF(2^d), e_0\rangle^\times$ とすると, 定義 *3* の $\{b(s,t)\}$ にたいして, 命題 *1* の $(b3)$, $(b4)$ が成り立つ.

これらのことより，以下の T_σ が DHO であることがわかる．$s \in H^\times$ にたいし $X_\sigma(s) := \{b(s,t) \mid t \in H^\times\}$ とし，さらに $X_\sigma(\infty) := \{b(s,s) \mid s \in H^\times\}$ とする．$\{b(s,t) \mid s,t \in H^\times\}$ は (b3), (b4) を満たすので，命題 1 より，$T_\sigma := \{X_\sigma(s) \mid s \in H^\times\} \cup \{X_\sigma(\infty)\}$ は d-次元 DHO になる．また T_σ は $PG(U \oplus V \oplus W) = PG(3d,2)$ を生成することもわかる．さらに例 2 の S と T_σ は同じ和公式 (3) を満たすので，T_σ は「(4)Veronesean DHO の変形」の quotient であることもわかる．

4 $\{T_\sigma\}$ 達の同型問題について

σ および τ を $GF(2^{dl})$ 上ガロア群の生成元とする．この節では，T_σ と T_τ が同型であるとき，σ と τ の満たす条件を考察する．ベクトル空間 V_σ と V_τ を

$$V_\sigma := \langle (e_0e_1 + e_1^2, e_0^\sigma e_1 + e_0 e_1^\sigma), (e_0e_2 + e_2^2, e_0^\sigma e_2 + e_0 e_2^\sigma), \\ (e_0e_3 + e_3^2, e_0^\sigma e_3 + e_0 e_3^\sigma), \ldots, (e_0e_d + e_D^2, e_0^\sigma e_d + e_0 e_d^\sigma)\rangle.$$

および

$$V_\tau := \langle (e_0e_1 + e_1^2, e_0^\tau e_1 + e_0 e_1^\tau), (e_0e_2 + e_2^2, e_0^\tau e_2 + e_0 e_2^\tau), \\ (e_0e_3 + e_3^2, e_0^\tau e_3 + e_0 e_3^\tau), \ldots, (e_0e_d + e_D^2, e_0^\tau e_d + e_0 e_d^\tau)\rangle.$$

と定める．T_σ の生成空間は $PG(U \oplus V_\sigma \oplus W)$ であり，T_τ の生成空間は $PG(U \oplus V_\tau \oplus W)$ である．また，$X_\sigma(t) := \{b_\sigma(s,t) \mid s,t \in H^\times\}$, $X_\sigma(\infty) := \{b_\sigma(s,s) \mid s \in H^\times\}$, $X_\tau(t) := \{b_\tau(s,t) \mid s,t \in H^\times\}$, $X_\tau(\infty) := \{b_\tau(s,s) \mid s \in H^\times\}$ などと定める．線形同型写像 $\Phi : PG(U \oplus V_\sigma \oplus W) \to PG(U \oplus V_\tau \oplus W)$ によって $T_\sigma = \{X_\sigma(t) \mid t \in H^\times\} \cup \{X_\sigma(\infty)\}$ から $T_\tau = \{X_\tau(t) \mid t \in H^\times\} \cup \{X_\tau(\infty)\}$ への同型が導かれるとする．このとき，1 対 1 写像 $\rho : H^\times \cup \{\infty\} \to H^\times \cup \{\infty\}$ があって $\Phi(X_\sigma(t)) = X_\tau(\rho(t))$ と表せる．そうすると，ρ は実は $H := \langle GF(2^d), e_0\rangle$ 上の線形写像で，さらに $\rho(\infty) = \infty$ および $\rho(e_0) = e_0$ を満たすことが証明できる．([8] の Proposition 2 および Cororally 3 参照.) さらに $s, t_1, t_2 \in H^\times$ に対して以下が成り立つことが分かる．

$$\rho(t_1 + t_2 + \alpha\{s, t_1, t_2\}(s + e_0)) \\ = \rho(t_1) + \rho(t_2) + \alpha\{\rho(s), \rho(t_1), \rho(t_2)\}(\rho(s) + e_0).$$

これらより $\Phi(V_\sigma \oplus W) \subset V_\tau \oplus W$ となることがわかり，以下の線形同型写像 $\bar{\Phi} : U = GF(2^d) \oplus GF(2^d) \to GF(2^d) \oplus GF(2^d) = U$ が定義できる．

$$\bar{\Phi} : U \cong (U \oplus V_\sigma \oplus V)/(V_\sigma \oplus W) \to (U \oplus V_\tau \oplus W)/(V_\tau \oplus W) \cong U.$$

ここで，線形写像 F, G, M, L を用いて $\bar{\Phi}$ を以下のように表す．

$$\bar{\Phi} : U \ni (x, y) \mapsto (F(x) + G(y), M(x) + L(y)) \in U.$$

すると，(先の注意より，今の場合)ρ は線形写像で $\rho(\infty) = \infty$ であることより，

$$\Phi((s^2, 0)) = \Phi(X_\sigma(t) \cap X_\sigma(\infty)) = X_\tau(\rho(t)) \cap X_\tau(\infty) = (\rho(t)^2, 0).$$

なので $t \in GF(2^d)$ に対して $F(t^2) = \overline{\rho(t)}^2$ となり $M = 0$ となることがわかる．さらに L は線形同型写像であることなどもわかる．よって，$s, t \in GF(2^d)$ に対して

$$L(st, s^\sigma t + st^\sigma) = \bar{\rho}(s)^\tau \bar{\rho}(t) + \bar{\rho}(s)\bar{\rho}(t)^\tau$$

が成り立つ．($\bar{\rho}(s), \bar{\rho}(t)$ は，それぞれ $\rho(t), \rho(t)$ の射影 (1) による像である．) この等式より，$\sigma = \tau$ または $\sigma = \tau^{-1}$ であることが以下のようにしてわかる．

[証明]

$X_1(t) := \{(x, x^\sigma t + xt^\sigma) \mid x \in GF(2^d)^\times\} \subset GF(2^d) \oplus GF(2^d)$ とし，双対超卵形 S_1 を $S_1 := \{X_1(t) \mid t \in GF(2^d)\}$ と定める．また $X_2(t) := \{(x, x^\tau t + xt^\tau) \mid x \in GF(2^d)^\times\} \subset GF(2^d) \oplus GF(2^d)$ とし，双対超卵形 S_2 を $S_2 := \{X_2(t) \mid t \in GF(2^d)\}$ と定める．(S_1, S_2 は吉荒 [?] によって研究された DHO である.) このとき線形同型写像 $\Psi : GF(2^d) \oplus GF(2^d) \to GF(2^d) \oplus GF(2^d)$ を

$$\Psi : (x, y) \mapsto (\bar{\rho}(x), L(y))$$

と定めると

$$\Psi : X_1(t) \ni (x, x^\sigma t + xt^\sigma) \mapsto (\bar{\rho}(x), \bar{\rho}(x)^\tau \bar{\rho}(t) + \bar{\rho}(x)\bar{\rho}(t)^\tau) \in X_2(\bar{\rho}(t))$$

より $t \in GF(2^d)$ にたいし $\Psi(X_1(t)) = X_2(\bar{\rho}(t))$ となることがわかる．よって S_1 と S_2 は同型になり，[11] の Proposition 11 より $\sigma = \tau$ または $\sigma = \tau^{-1}$ であることがわかる． □

上記の証明について，筆者は当初込み入った長い証明を持っていたが，吉荒氏によりこのように簡略化された．

References

[1] M. Buratti and A. Del Fra, Semi-Boolean quadruple systems and dimensional dual hyperovals, Advances in Geometry. 3 (2003), 245–253.

[2] A. Del Fra, On d-Dimensional Dual Hyperovals, Geometriae Dedicata, 79 (2000), 157–178.

[3] A. Del Fra and S. Yoshiara, Dimensional dual hyperovals associated with Steiner systems, European Journal of Combinatorics. 26 (2005), 173–194.

[4] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AC^*$ geometries, Discrete Mathematics. 255 (2002), 503–532.

[5] C. Huybrechts and A. Pasini, Frag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40. (1999), 503–532.

[6] A. Pasini, Diagram Geometries, Oxford Science Publications, Clarendon Press, Oxford. (1994).

[7] H. Taniguchi, On a family of dual hyperovals over $GF(q)$ with q even, European Journal of Combinatorics, 26 (2005), 195–199.

[8] H. Taniguchi, On automorphism of some dual hyperovals in $PG(d(d+3)/2, 2)$, Graphs and Combinatorics, 24. (2008), 229–236.

[9] H. Taniguchi, A new family of dual hyperovals in $PG(d(d+3)/2, 2)$ with $d \geq 3$, Discrete Mathematics, 309(2009), 418–429.

[10] J. Thas and H. van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, The Quarterly Journal of Mathematics, Oxford. 55 (2004), 99–113.

[11] S. Yoshiara, A Family od d-dimensional Dual Hyperovals in $PG(2d+1, 2)$, European Journal of Combinatorics, 20 (1999), 589–603.

[12] S. Yoshiara, Ambient spaces of dimensional dual arcs, Journal of Algebraic Combinatorics. 19 (2004), 5–23.

[13] S. Yoshiara, Notes on Taniguchi's dimensional dual hyperovals, European Journal of Combinatorics, 28 (2007), 674–684.

On $\mathrm{TD}_2(2n, n)$'s admitting semiregular automorphism groups of order n^2

Yutaka Hiramine

Department of Mathematics, Faculty of Education,
Kumamoto University,
Kurokami, Kumamoto, Japan
hiramine@gpo.kumamoto-u.ac.jp

1 Introduction

A *transversal design* $\mathrm{TD}_\lambda(k, u)$ $(u > 1, k = u\lambda)$ is an incidence structure $\mathcal{D} = (\mathbb{P}, \mathbb{B})$, where

(i) $\mathbb{P}$ is a set of uk points partitioned into k classes (called *point classes*), each of size u,

(ii) $\mathbb{B}$ is a collection of k-subsets of $\mathbb{P}$ (called blocks),

(iii) Any two distinct points in the same point class are incident with no block and any two points in distinct point classes are incident with exactly λ blocks.

A transversal design $\mathrm{TD}_\lambda(k, u)$ is said to be *symmetric* and denoted by $\mathrm{STD}_\lambda(k, u)$ if its dual structure is also a transversal design with the same parameters as $\mathrm{TD}_\lambda(k, u)$.

A transversal design $\mathcal{D}$ is called *class regular* with respect to U if U is an automorphism group of $\mathcal{D}$ acting regularly on each point class, which is necessarily symmetric by a result of Jungnickel (Corollary 6.9 of [5]).

Let $\mathcal{D}$ be an $\mathrm{STD}_\lambda(k, u)$. If $\mathcal{D}$ is class regular with respect to U, then there exists a *generalized Hadamard matrix* $[d_{i,j}]$ of order k with entries from U (for short $\mathrm{GH}(u, \lambda)$) such that whenever $i \neq \ell$ the set of differences $\{d_{ij}d_{\ell j}^{-1} \mid 1 \leq j \leq k\}$ contains each element of U exactly λ times. Conversely, from a generalized Hadamard matrix $\mathrm{GH}(u, \lambda)$ over a group U of order u, one can construct an $\mathrm{STD}_\lambda(k, u)$ which admits U as a class regular automorphism group (Theorem 3.6 of [1]).

In [4] we give a modification of generalized Hadamard matrices. Let H be a group of order su. For subsets D_{ij} $(1 \leq i, j \leq t, st = u\lambda)$ of H, a matrix

$$[D_{ij}] = \begin{bmatrix} D_{11} & D_{12} & \cdots & D_{1t} \\ D_{21} & D_{22} & \cdots & D_{2t} \\ \vdots & & & \vdots \\ D_{t1} & D_{t2} & \cdots & D_{tt} \end{bmatrix}$$

is called a *modified generalized Hadamard matrix* with respect to subgroups $U_1, \cdots, U_t$ of H of order u if the following two conditions are satisfied.

$$|D_{ij}| = s, \ 1 \leq i, j \leq t \tag{1}$$

$$\sum_{1 \leq j \leq t} D_{ij} D_{\ell j}^{(-1)} = \begin{cases} k + \lambda(H - U_i) & \text{if } i = \ell, \\ \lambda H & \text{otherwise.} \end{cases} \tag{2}$$

For short, we say $[D_{ij}]$ is a $GH(s, u, \lambda)$ *matrix with respect to subgroups* $U_1, \cdots, U_t$ and the subgroups are called *forbidden subgroups.* Clearly any $\mathrm{GH}(1, u, \lambda)$ matrix is an ordinary generalized Hadamard matrix $\mathrm{GH}(u, \lambda)$ and a $\mathrm{GH}(u\lambda, u, \lambda)$ matrix with respect to U is a $(u\lambda, u, u\lambda, \lambda)$-difference set relative to U (see [1]).

A transversal design $\mathrm{TD}_\lambda(k, u)$ is obtained from a $\mathrm{GH}(s, u, \lambda)$ matrix. For a $t \times t$ $\mathrm{GH}(s, u, \lambda)$ matrix $[D_{ij}]$ $(st = u\lambda)$, we define a set of points $\mathbb{P}$ and a set of blocks $\mathbb{B}$ in the following way.

$$\mathbb{P} = \{1, 2, \cdots, t\} \times H, \quad \mathbb{B} = \{B_{jh} : 1 \leq j \leq t, \ h \in H\}, \tag{3}$$
$$\text{where } B_{jh} = \bigcup_{1 \leq i \leq t} (i, D_{ij}h) \ (= \bigcup_{1 \leq i \leq t} \{(i, dh) : 1 \leq i \leq t, \ d \in D_{ij}\}).$$

Then we have

Result 1.1. ([4]) Let $[D_{ij}]$ be a $t \times t$ $\mathrm{GH}(s, u, \lambda)$ matrix over a group H of order su with respect to subgroups U_i $(1 \leq i \leq t)$, where $t = u\lambda/s$. If we define $\mathbb{P}$ and $\mathbb{B}$ by (3), then the following holds.

(i) $(\mathbb{P}, \mathbb{B})$ is a transversal design $\mathrm{TD}_\lambda(k, u)$ $(k = u\lambda)$.

(ii) For each i $(1 \leq i \leq t)$ and $x \in H$, set $\mathbb{P}_{i,U,x} = \{(i, wx) : w \in U_i\}$ $(1 \leq i \leq t, x \in H)$. Then $\mathbb{P}_{i,U_i x}$ is a point class of $(\mathbb{P}, \mathbb{B})$.

(iii) If we define the action of H on $(\mathbb{P}, \mathbb{B})$ by $(i, c)^x = (i, cx), (B_{j,d})^x = B_{j,dx}$, then H is an automorphism group of $(\mathbb{P}, \mathbb{B})$ acting semiregularly both on $\mathbb{P}$ and on $\mathbb{B}$ and each (i, H) is an H-orbit on $\mathbb{P}$ for each i $(1 \leq i \leq t)$.

(iv) For every $x \in H$, $x^{-1}U_i x$ acts regularly on a point class $\mathbb{P}_{i,U_i x}$ $(1 \leq i \leq t)$.

(iv) $(\mathbb{P}, \mathbb{B})$ is symmetric if and only if $[D_{ij}{}^{(-1)}]^T$ is $\mathrm{GH}(s, u, \lambda)$-matrix.

Let $(\mathbb{P}, \mathbb{B})$ a $\mathrm{TD}_\lambda(k, u), k = u\lambda$ and let G be an automorphism group of $(\mathbb{P}, \mathbb{B})$. From now on we say that G semiregular if G is semiregular both on $\mathbb{P}$ and on $\mathbb{B}$. We say that G is *class-transitive* if G acts on the set of point classes transitively. In this case, clearly $|G| = u\lambda s$ for some $s \mid u$. Set $T_t = \{1, 2, \cdots, t\}$ for $t \in \mathbb{N}$. We show the following.

Theorem 3.1. *Let* $(\mathbb{P}, \mathbb{B})$ *a* $TD_\lambda(k, u), k = u\lambda$. *If a semiregular automorphism group* G *of* $(\mathbb{P}, \mathbb{B})$ *of order* $u\lambda s$ *is class transitive, then there exist subsets* D_{ij} $(1 \leq i, j \leq t)$, *where* $t = u/s$ *and a subgroup* U *of* G *of order* s *satisfying the following.*

$$(*) \quad \sum_{1\le j\le t} D_{ij}D_{\ell j}^{(-1)} = \begin{cases} k+\lambda(G-U) & \text{if } i=\ell, \\ \lambda(G-U) & \text{otherwise} \end{cases}$$

and $|D_{i1}|+\cdots+|D_{it}| = |D_{1j}|+\cdots+|D_{tj}| = u\lambda$ *for any* $i,j \in T_t$.

We call the above $t\times t$-matrix $[D_{ij}]$ satisfying $(*)$ a $\mathrm{CT}(s,u,\lambda)$-matrix over G relative to U. We show that from a given $\mathrm{CT}(s,u,\lambda)$-matrix a $\mathrm{TD}_\lambda(\lambda u,u)$ can be constructed (Theorem 3.6). We also show that if a $\mathrm{TD}_\lambda(\lambda u,u)$ admits a semiregular automorphism group then it is isomorphic to one of the two types of $\mathrm{TD}_\lambda(\lambda u,u)$ (Theorem 4.1). As an application, we show the following.

Theorem 5.1. Let $\mathcal{D}$ be a symmetric $\mathrm{TD}_2(2u,u)$. If $\mathcal{D}$ admits a semiregular automorphism group G of order u^2 and the square free part of u is not 2, then G contains a class regular subgroup, say U, of order u. In particular, there exist u-subsets D_{ij} $(1\le i,j\le 2)$ of G such that $[D_{ij}]$ is a $\mathrm{GH}(u,u,2)$-matirx of order 2 relative to U.

We also give a class of examples of $\mathrm{TD}_2(2u,u)$ satisfying the condition of Theorem 5.1 (Proposition 6.1).

2 Preliminaries

Result 2.1. ([4]) Let $(\mathbb{P},\mathbb{B})$ be a transversal design $\mathrm{TD}_\lambda[k;u]$ and let H be a semiregular automorphism group of $(\mathbb{P},\mathbb{B})$ order su such that each H-orbit on $\mathbb{P}$ is a union of some point classes. Then, there exist s-subsets D_{ij} $(1\le i,j\le t=u\lambda/s)$ of H and subgroups U_i of H of order u satisfying

$$\sum_{j=1}^{t} D_{ij}D_{\ell j}{}^{(-1)} = \begin{cases} k+\lambda(H-U_i) & \text{if } i=\ell, \\ \lambda H & \text{otherwise.} \end{cases}$$

Result 2.2. ([9]) Let G be an abelian group and let $z\in\mathbb{Z}[G]$. If $\chi(z)=0$ for any character $\chi\neq\chi_0$, where χ_0 is a principal character of G, then $z=\frac{\chi_0(z)}{|G|}G$.

Proposition 2.3. *Let* U_1,U_2 *and* V *are subgroups of an abelian group* G. *If* $V\not\subseteq U_1,U_2$, *then there exists a character* χ *of* G *satisfying* $\chi|_V=\chi_0$ *and* $\chi|_{U_1}\neq\chi_0$, $\chi|_{U_2}\neq\chi_0$.

3 Class-transitive automorphism groups

Let $(\mathbb{P},\mathbb{B})$ a $\mathrm{TD}_\lambda(k,u), k=u\lambda$ and let G be an automorphism group of $(\mathbb{P},\mathbb{B})$. We say that G is *class-transitive* if G acts on the set of point classes transitively. In this case, clearly $|G|=u\lambda s$ for some $s\mid u$. Set $T_t=\{1,2,\cdots,t\}$ for $t\in\mathbb{N}$.

Theorem 3.1. *Let $(\mathbb{P}, \mathbb{B})$ a $TD_\lambda(k,u), k = u\lambda$. If a semiregular automorphism group G of $(\mathbb{P}, \mathbb{B})$ of order $u\lambda s$ is class transitive, then there exist subsets D_{ij} $(1 \le i,j \le t)$, where $t = u/s$ and a subgroup U of G of order s satisfying the following.*

$$\sum_{1 \le j \le t} D_{ij} D_{\ell j}^{(-1)} = \begin{cases} k + \lambda(G-U) & \text{if } i = \ell, \\ \lambda(G-U) & \text{otherwise} \end{cases} \tag{4}$$

and $|D_{i1}| + \cdots + |D_{it}| = |D_{1j}| + \cdots + |D_{tj}| = u\lambda$ for any $i, j \in T_t$.

Proof. Let $\mathcal{C}$ be a point class of $(\mathbb{P}, \mathbb{B})$ and let $\{\mathbb{P}_1, \mathbb{P}_2, \cdots, \mathbb{P}_t\}$ and $\{\mathbb{B}_1, \mathbb{B}_2, \cdots, \mathbb{B}_t\}$ be the se of G-orbits on $\mathbb{P}$ and $\mathbb{B}$, respectively. Fix $P_i \in \mathbb{P}_i \cap \mathcal{C}$ and $B_i \in \mathbb{B}_i$ for each $i \in T_t$. For each $i, j \in T_t$, we define a subset D_{ij} of G as follows.

$$D_{ij} = \{g \in G \mid P_i^g \in B_j\} \tag{5}$$

Since $\mathbb{P}_i$ is a G-orbit on $\mathbb{P}$, $P_i^{D_{ij}} = \mathbb{P}_i \cap B_j$. In particular, $|D_{ij}| = |\mathbb{P}_i \cap B_j|$. Hence

$$|D_{1j}| + |D_{2j}| + \cdots + |D_{tj}| = u\lambda \tag{6}$$

Denote by (P_i) the set of blocks of $\mathbb{B}$ through P_i. As $D_{ij}^{(-1)} = \{g \in G \mid B_j^g \ni P_i\}$ and (P_i) is a direct sum of $\mathbb{B}_j \cap (P_i)$'s with $j \in T_t$, by a similar argument as in (6), we have the following.

$$|D_{i1}| + |D_{i2}| + \cdots + |D_{it}| = u\lambda \ (i \in T_t) \tag{7}$$

Set $U = G_{\mathcal{C}}$. Then $U = \{g \in G \mid P_i^g \in \mathcal{C}\}$ for each $i \in T_t$ as G acts on the set of point classes. As $[G : G_{\mathcal{C}}] = u\lambda$, U is a subgroup of G of order s. We show that

$$D_{i1} D_{i1}^{(-1)} + D_{i2} D_{i2}^{(-1)} + \cdots + D_{it} D_{it}^{(-1)} = u\lambda + \lambda(G-U) \tag{8}$$

Fix $i \in T_t$ and let $c \in G, c \neq 1$. Then

$$\begin{aligned} c = ab^{-1}, a, b \in D_{ij} (\exists j \in T_t) &\iff a = cb, P_i^a, P_i^b \in B_j, (\exists j \in T_t) \\ &\iff a = cb, P_i^c, P_i \in B_j^{b^{-1}}, (\exists j \in T_t) \end{aligned}$$

Then there exist exactly λ such pairs (j, b) if $c \notin U$, and no such pairs otherwise. This, together with (7), gives (8).

We now show that for $i, \ell \in T_t, i \neq \ell$

$$D_{i1} D_{\ell 1}^{(-1)} + D_{i2} D_{\ell 2}^{(-1)} + \cdots + D_{it} D_{\ell t}^{(-1)} = \lambda(G-U) \tag{9}$$

Let $c \in G$. Then

$$\begin{aligned} c = ab^{-1}, a \in D_{ij}, b \in D_{\ell j} (\exists j \in T_t) &\iff a = cb, P_i^a, P_\ell^b \in B_j, (\exists j \in T_t) \\ &\iff a = cb, P_i^c, P_\ell \in B_j^{b^{-1}}, (\exists j \in T_t) \end{aligned}$$

Then there exist exactly λ such pairs (j, b) if $c \notin U$, and no such pairs otherwise. Thus (9) holds. □

Definition 3.2. Let G be a group of order $su\lambda$ with $s \mid u$. Let D_{ij} $(i,j \in T_t, t = u/s)$ be subsets of G and U a subgroup of G of order s. A $t \times t$ matrix $[D_{ij}]$ is called a $CT(s,u,\lambda)$-*matrix* over a group G relative to U if it satisfies (4).

Lemma 3.3. *Let notations be as in Theorem 3.1. Set $m_{ij} = |D_{ij}|$ for $i,j \in T_t$. Then, a $t \times t$ matrix $M = [m_{ij}]$ satisfies $MM^T = M^TM = (\alpha-\beta)I+\beta J$, where $\alpha = u\lambda + \lambda(u\lambda s - s), \beta = \lambda(u\lambda s - s)$ and J is a all one matrix.*

Proof. By (6) and (7) $MJ = JM$. On the other hand, $\det(MM^t) = (\alpha + (t-1)\beta)(\alpha-\beta)^{t-1} = (u\lambda)^{t+1} \neq 0$. Hence, by a standard argument, $M^T = M^{-1}((\alpha-\beta)I+\beta J) = ((\alpha-\beta)I+\beta J)M^{-1}$. Thus $M^TM = (\alpha-\beta)I+\beta J$. □

Proposition 3.4. *Let $q = p^e$ be a power of a prime p and let G be an elementary abelian p-group of order q^2. Let $S = \{H_1, \cdots, H_{q+1}\}$ be a spread of G. Set $r = q/p$ $(= p^{e-1})$ and*

$$\begin{aligned} A_i &= H_{ir+1} + H_{ir+2} + \cdots + H_{(i+1)r} - r \quad (0 \le i \le p-2), \\ A_{p-1} &= H_{(p-1)r+1} + H_{(p-1)r+2} + \cdots + H_{pr+1} - r. \end{aligned}$$

Let $L = [n_{ij}]$ be an arbitrary Latin square of order p with entries from $\{0,1,\cdots,p-1\}$. Then the following is a $CT(1,p,p^{2e-1})$ matrix, which gives a $TD_{p^{2e-1}}(p^{2e},p)$.

$$\begin{bmatrix} A_{n_{11}} & A_{n_{12}} & \cdots & A_{n_{1,p-1}} \\ A_{n_{2,1}} & A_{n_{2,2}} & \cdots & A_{n_{2,p}} \\ \vdots & \vdots & \vdots & \\ & & & A_{n_{p-1,p}} \\ A_{n_{p,1}} & \cdots & A_{n_{p,p-1}} & A_{n_{p,p}} \end{bmatrix}$$

Proof. Set $S_i = H_{ir+1} + H_{ir+2} + \cdots + H_{(i+1)r}, 0 \le i \le p-2$ and $S_{p-1} = H_{(p-1)r+1} + H_{(p-1)r+2} + \cdots + H_{pr+1}$. Then, $A_i = S_i - r$ and $A_i^{(-1)} = A_i$ for each $i \in \{0,1,\cdots,p-1\}$. Hence $\sum_{0\le i\le p-1} A_iA_i^{(-1)} = \sum_{0\le i\le p-1}(S_i-r)^2 = \sum_{0\le i\le p-2} S_i^2 + S_{p-1}^2 - 2r\sum_{0\le i\le p-1} S_i + pr^2 = (p-1)r(r-1)G + q\sum_{0\le i\le p-2} S_i + (r+1)rG + qS_{p-1} - 2r\sum_{0\le i\le p-1} S_i + qr = (qr-q+2r)G + (q-2r)\sum_{0\le i\le p-1} S_i + qr = (qr-q+2r)G + (q-2r)(G+q) + qr = q^2 + qr(G-1)$.

Assume $i \neq \ell$. Then,

$$S_iS_\ell = \begin{cases} r^2G & \text{if } i,\ell \neq p-1, \\ r(r+1)G & \text{otherwise.} \end{cases}$$

Hence

$$A_iA_\ell = \begin{cases} r^2G - r(S_i+S_\ell) + r^2 & \text{if } i,\ell \neq p-1, \\ r(r+1)G - r(S_i+S_\ell) + r^2 & \text{otherwise.} \end{cases}$$

Thus, if $i \neq \ell$, then $\sum_{1\le j\le p} A_{n_{ij}}A_{n_{\ell j}}^{(-1)} = r^2p - 2r\sum_{0\le i\le p-1} S_i + (p-2)r^2G + 2(r^2+r)G = -rq + rqG = rq(G-1)$. Therefore the proposition holds. □

Example 3.5. Let G be a group of order $4m^2$. Suppose C and D are any $(4m^2, 2m^2 - m, m^2 - m)$ and $(4m^2, 2m^2 + m, m^2 + m)$ difference sets of G, respectively. Then we can verify that $CC^{(-1)} + DD^{(-1)} = 4m^2 + 2m^2(G-1)$ and $C(G-C)^{(-1)} + D(G-D)^{(-1)} = 2m^2(G-1)$. Thus $\begin{bmatrix} C & D \\ G-C & G-D \end{bmatrix}$ is a CT-$(1, 2, 2m^2)$ matrix.

The converse of Theorem 3.1 is true as we show below.

Theorem 3.6. *Let G be a group of order $u\lambda s$ with $s \mid u$. Let $[D_{ij}]$ be a $CT(s, u, \lambda)$-matrix over a group G relative to U, then an incidence structure $\mathcal{D}(\mathbb{P}, \mathbb{B})$ defined by the following is a $TD_\lambda(k, u)$ admitting G as a semiregular and class-transitive automorphism group under the action $(i, w)g = (i, wg)$ for $i \in \{1, \cdots, t\}$ and $w, g \in G$.*

$$\mathbb{P} = \{1, 2, \cdots, t\} \times G \qquad \mathbb{B} = \{B_{j,g} \mid 1 \le j \le t,\ g \in G\}, t = u/s \qquad (10)$$
$$\text{where } B_{j,g} = \sum_{1 \le i \le t} (i, D_{ij}g)$$

Moreover, the point classes of $\mathcal{D}$ are $C_j (j, 1 \le j \le k)$, where $C_j = \cup_{1 \le i \le t}(i, Ux_j)$.

Proof. Set $B_j = B_{j,1}$ for $j \in \{1, \cdots, t\}$. Then

$$(*) \qquad B_j^g = B_{j,g} \text{ for } g \in G.$$

Let (i, a) and (ℓ, b) be distinct points of $\mathbb{P}$ and denote by $[(i, a), (\ell, b)]$ the number of blocks containing them. We show that

$$[(i, a), (\ell, b)] = \begin{cases} \lambda & \text{if } ab^{-1} \notin U, \\ 0 & \text{if } ab^{-1} \in U. \end{cases} \qquad (11)$$

We have

$$\begin{aligned} &(i, a), (\ell, b) \in B_{j,g} \\ &\quad \Longleftrightarrow \quad (i, ag^{-1}), (\ell, bg^{-1}) \in B_j \\ &\quad \Longleftrightarrow \quad ag^{-1} \in D_{ij},\ bg^{-1} \in D_{\ell j} \\ &\quad \Longleftrightarrow \quad ag^{-1} = d_1,\ bg^{-1} = d_2\ (\exists d_1 \in D_{ij}, \exists d_2 \in D_{\ell,j}) \\ &\quad \Longleftrightarrow \quad ab^{-1} = d_1 d_2^{-1},\ g = d_1^{-1}a\ (\exists d_1 \in D_{ij}, \exists d_2 \in D_{\ell,j}) \qquad (12) \end{aligned}$$

We note that $a \neq b$ if $i = \ell$. Hence (12) together with (4) implies (11).

Let $G = Ux_1 \cup Ux_2 \cup \cdots \cup Ux_k$ be the decomposition of G into the right cosets of U in G. Set $C_j = \cup_{1 \le i \le t}(i, Ux_j)$ for $j \in T_t$. Then, by (11), $(\mathbb{P}, \mathbb{B})$ is a TD$\lambda(uk, u)$ with point classes $C_j (j, 1 \le j \le k)$ and G acts on $(\mathbb{P}, \mathbb{B})$ as a semiregular class-transitive automorphism group. □

We use the notation B_j^g $(j \in T_t, g \in G)$ defined in $(*)$.

Lemma 3.7. *In Theorem 3.6, for two distinct (j, a) and (ℓ, b) of $T_t \times G$, $|B_j^a \cap B_\ell^b|$ is the coefficient of ab^{-1} in $\sum_{1 \le i \le t} D_{ij}^{(-1)} D_{i\ell}$.*

Proof. Let B_j^a and B_ℓ^b be any two distinct blocks. Then

$$B_j^a \cap B_\ell^b = \cup_{i\in T_t}(i, D_{ij}a) \cap \cup_{i\in T_t}(i, D_{i\ell}b)$$
$$= \{(i,g) \mid i \in T_t, d_{ij}^{-1}d_{i\ell} = ab^{-1}, g = d_{ij}a\}$$

Thus the lemma holds. □

Hypothesis 3.8. Under the hypothesis Theorem 3.1 we assume that $(\mathbb{P}, \mathbb{B})$ is symmetric.

Lemma 3.9. *Assume Hypothesis 3.8.*

(i) *There exist s-subsets $W_{j\ell}(j, \ell \in T_t)$ of G such that*

$$\sum_{1\le i\le t} D_{ij}^{(-1)} D_{i\ell} = \begin{cases} k + \lambda(G - W_{jj}) & \text{if } j = \ell, \\ \lambda(G - W_{j\ell}) & \text{otherwise.} \end{cases} \tag{13}$$

(ii) *Each W_{jj} is a subgroup of G of order s.*

(iii) *Let $\mathcal{B}_j$ be the block class containing B_j. Then $G_{\mathcal{B}_j} = W_{jj}$.*

Proof. By assumption $(\mathbb{P}, \mathbb{B})$ is symmetric. Hence $|B_j^a \cap B_\ell^b| \in \{0, \lambda\}$. Applying Lemma 3.7, we have (13). By Lemma 3.3, we can easily check that $|W_{j\ell}| = s$ for any $j, \ell \in T_t$.

Set $W = W_{jj}$. Clearly $1 \in W$. Let $a \in W \setminus \{1\}$. Then, as $B_j^a \cap B_j = \emptyset$, $B_j \cap B_j^a = \emptyset$. Hence $a^{-1} \in W$ by Lemma 3.7. Let $a, b \in W \setminus \{1\}$. Then, again by Lemma 3.7, $B_j^a \cap B_j = \emptyset$ and $B_j^b \cap B_j = \emptyset$. Since $(\mathbb{P}, \mathbb{B})$ is symmetric, this implies that $B_j^a \cap B_j^b = \emptyset$. Thus $ab^{-1} \in W$. Therefore (ii) holds.

By Lemma 3.7, $\mathbb{B}_j^a \in \mathcal{B}_j$ for each $a \in W$. Thus $W \subset G_{\mathcal{B}_j}$. The converse implication is clear by Lemma 3.7. Therefore $W = G_{\mathcal{B}_j}$. □

Corollary 3.10. *Assume Hypothesis 3.8. Then G is also transitive on the set of block classes.*

Proof. By (i) and (iii) of Lemma 3.9 $[G : G_{\mathcal{B}_j}] = [G : W_{jj}] = u\lambda$. Thus we have the corollary. □

We say two blocks B_j^a and B_ℓ^b are *parallel* and denoted by $B_j^a \parallel B_\ell^b$ if $(j,a) = (\ell,b)$ or $B_j^a \cap B_\ell^b = \emptyset$.

Lemma 3.11. *Let notations be as in Lemma 3.9. For each $j \in T_t$ set $\mathcal{B}_j = B_1^{W_{1j}} \cup B_2^{W_{2j}} \cup \cdots \cup B_t^{W_{tj}}$. Then $\mathcal{B}_j$ is a block class. Moreover each $W_{\ell j}$ is a left coset of W_{jj} in G.*

Proof. By Lemmas 3.7 3.9, $B_j^a \parallel B_\ell^b$ if and only if $(j,a) = (\ell,b)$ or $ab^{-1} \in W_{j\ell}$. Hence all blocks in $B_\ell^{W_{tj}}$ are parallel to B_j. Since $B_\ell^{W_{tj}} \parallel B_j^{W_{jj}}$, $W_{\ell j}W_{jj}^{(-1)} \subset W_{\ell j}$. Thus each $W_{\ell j}$ is a left coset of W_{jj} in G. □

Theorem 3.12. *Assume Hypothesis 3.8. Then there exist elements $c_1, c_2, \cdots, c_t$ of G and a subgroup W of G of order s satisfying*

$$\sum_{1\le i\le t} D_{ij}^{(-1)} D_{i\ell} = \begin{cases} k+\lambda(G-c_jWc_\ell^{-1}) & \text{if } j=\ell, \\ \lambda(G-c_jWc_\ell^{-1}) & \text{otherwise.} \end{cases} \tag{14}$$

Proof. Set $W = W_{11}$. By Lemma 3.11, there exist elements $c_1, c_2, \cdots, c_t$ of G such that $W_{11} = c_1W, W_{21} = c_2W, \cdots, W_{t1} = c_tW$ and $c_1 = 1$. Then $B_1^{c_1} \parallel B_2^{c_2} \parallel \cdots \parallel B_t^{c_2}$ and $\mathbb{B} = B_1^G \cup B_2^G \cup \cdots B_t^G$. Set $C_{ij} = \{x \in G \mid (B_i^{c_i})^x \ni P_j\}$. Since $(\mathbb{P}, \mathbb{B})$ is symmetric, applying Theorem 3.1,

$$\sum_{1\le j\le t} C_{ij}C_{\ell j}^{(-1)} = \begin{cases} k+\lambda(G-W) & \text{if } i=\ell, \\ \lambda(G-W) & \text{otherwise} \end{cases} \tag{15}$$

As $C_{ij} = \{x \in G \mid P_j^{x^{-1}c_i^{-1}} \in B_i\}$, $C_{ij} = c_i^{-1}D_{ji}^{(-1)}$ $(i, j \in T_t)$. Hence,substituting these into 15, we have

$$\sum_{1\le j\le t} d_i^{-1}D_{ji}^{(-1)}(c_\ell^{-1}D_{j\ell}^{(-1)})^{(-1)} = \begin{cases} k+\lambda(G-W) & \text{if } i=\ell, \\ \lambda(G-W) & \text{otherwise} \end{cases}$$

Therefore (15) holds. □

Theorem 3.13. *Let $[D_{ij}]$ be a $CT(s,u,\lambda)$-matrix over a group G of order $su\lambda$ relative to a subgroup U of G of order s. If there exist elements $c_1, c_2, \cdots, c_t$ of G and a subgroup W of G of order s satisfying (14). Then the $TD_\lambda(u\lambda, u)$ defined by (10) is a symmetric.*

Proof. Set $\mathcal{C} = B_1^{c_1W} \cup B_2^{c_1W} \cup \cdots \cup B_t^{c_1W}$. Let $a = c_jw_1$ and $b = c_\ell w_2$. Then $ab^{-1} = c_jw_1w_2^{-1}c_\ell^{-1}$. By (14), $B_j^a \parallel B_\ell^b$. Hence all blocks of $\mathcal{C}$ are parallel. Let $G = Wd_1 \cup Wd_2 \cup \cdots \cup Wd_k$ be the decomposition of G into the right cosets of W in G. Obviously all blocks in $\mathcal{C}^g$ are parallel for any $g \in G$. We consider $B_j^a \in \mathcal{C}^{d_p}$ and $B_\ell^b \in \mathcal{C}^{d_q}, p \ne q$. Then $a = c_jw_1d_p$ and $b = c_\ell w_2 d_q$, where $j, \ell, p, q \in T_t, p \ne q$ and $w_1, w_2 \in W$. Then $ab^{-1} = c_j(w_1d_pd_q^{-1}w_2^{-1})c_\ell^{-1}$. Hence, if $ab^{-1} \in c_jWc_\ell^{-1}$, then $d_pd_q^{-1} \in W$ and so $d_p = d_q$, a contradiction. Thus $|B_j^a \cap B_\ell^b| = \lambda$ by (14). Therefore $(\mathbb{P}, \mathbb{B})$ is a symmetric $\mathrm{TD}_\lambda(u\lambda, u)$ with block classes $\mathcal{C}^{d_1}, \mathcal{C}^{d_2}, \cdots, \mathcal{C}^{d_k}$. □

4 Large semiregular automorphism groups

In this section we show the following.

Theorem 4.1. *Let $\mathcal{D} = (\mathbb{P}, \mathbb{B})$ be a $TD_\lambda(k,u)$ $(k = u\lambda)$ and let G be a semiregular automorphism group of $\mathcal{D}$ of order $u^2\lambda/2$. Then one of the following occurs.*

(i) *There exist subgroups U_1 and U_2 of G of order u and $u\lambda/2$-subsets D_{ij} $(1 \le i,j \le 2)$ of G such that $\mathcal{D}$ is isomorphic to the $TD_\lambda(k,u)$ obtained from the $GH(u\lambda/2,u,\lambda)$-matrix $\begin{bmatrix} D_{11} & D_{12} \\ D_{21} & D_{22} \end{bmatrix}$ relative to U_1 and U_2.*

(ii) *$2 \mid u$, $u\lambda = 4m^2$ for an integer m and G acts transitively on the set of point classes. There exist a subgroup U of G of order $u/2$ and susets D_{ij} $(1 \le i,j \le 2)$ satisfying*

(1) $|D_{11}| = |D_{22}|, |D_{12}| = |D_{21}|, \{|D_{11}|, |D_{22}|\} = \{2m^2 \pm m\}$

(2) $[D_{ij}]$ is a $CT(u/2,u,\lambda)$-matrix relative to U, that is,

$$\sum_{1\le j\le 2} D_{ij}D_{\ell j}^{(-1)} = \begin{cases} k+\lambda(G-U) & \text{if } i=\ell, \\ \lambda(G-U) & \text{otherwise.} \end{cases} \tag{16}$$

Proof. Let $\mathcal{D} = (\mathbb{P},\mathbb{B})$ be a $TD_\lambda(k,u)$ $(k = u\lambda)$ and let G be a semiregular automorphism group of $\mathcal{D}$ of order $u^2\lambda/2$. Let $\mathcal{C}$ be a point class of $\mathcal{D}$ and . $\{\mathbb{P}_1,\mathbb{P}_2\}$ the set of G-orbits on $\mathbb{P}$. We note that $|\mathbb{P}_1| = |\mathbb{P}_2| = u^2\lambda/2$. Let Ω be the set of point classes of $\mathcal{D}$. Then $|\Omega| = u\lambda$ and G induces a permutation group on Ω. Let $\mathcal{C} \in \Omega$. Then, as G is semiregular on $\mathbb{P}$, $|G_\mathcal{C}| \mid |\mathcal{C}| = u$ and so $|G|/u \mid [G : G_\mathcal{C}]$. Hence the length of G each G-orbit on Ω is divided by $u\lambda/2$. Thus one of the following occurs.

(1) There exist G-orbits Ω_1 and Ω_2 on Ω such that $\Omega = \Omega_1 \cup \Omega_2$ and $|\Omega_1| = |\Omega_2| = u\lambda/2$.

(2) G acts transitively on Ω and $|G_\mathcal{C}| = u/2$ for each point class $\mathcal{C}$.

If (1) occurs, then clearly each $\mathbb{P}_i$ with $i \in \{1,2\}$ is a union of $u\lambda/2$ parallel classes of $\mathcal{D}$. Therefore, by ResultHDij, $\mathcal{D}$ is isomorphic to the $TD_2(2n,n)$ constructed from the $GH(n,n,2)$-matrix M over G.

Assume (2). By Theorem 3.1, There exist subsets D_{ij} $(1 \le ij \le 2)$ and a subgroup U of order s such that

$$\sum_{1\le j\le 2} D_{ij}D_{\ell j}^{(-1)} = \begin{cases} k+\lambda(H-U) & \text{if } i=\ell, \\ \lambda(H-U) & \text{otherwise.} \end{cases} \tag{17}$$

Set $m_{ij} = |D_{ij}|$ $(1 \le ij \le 2)$. Then, for each $i \in \{1,2\}$

$$m_{i1} + m_{i2} = u\lambda \tag{18}$$

$$m_{i1}{}^2 + m_{i2}{}^2 = u^2\lambda^2/2 + u\lambda/2 \tag{19}$$

$$m_{11}m_{21} + m_{12}m_{22} = u^2\lambda^2/2 - u\lambda/2 \tag{20}$$

By (18)-(20), we have

$$m_{i1}m_{i2} = (u^2\lambda^2 - u\lambda)/4 \ (1 \le i \le 2) \tag{21}$$

$$(m_{11} - m_{21})^2 + (m_{12} - m_{22})^2 = 2u\lambda \tag{22}$$

Therefore, by (18), (21),(22), we have (ii). □

We give examples of Theorem 4.1(i)(ii)

Example 4.2. (i) Let $G = \langle a, b \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ be a group of order 9 and set

$$M = \begin{bmatrix} 1 + ab + a^2b & 1 + ab + a^2b \\ 1 + ab + ab^2 & 1 + b + ab^2 \end{bmatrix}$$

Then M is a GH(3, 3, 2)-matrix relative to $\langle a \rangle$ and $\langle b \rangle$ and the resulting $TD_2(6, 3)$ is non-symmetric.

(ii) Let $G = \langle a \rangle \simeq \mathbb{Z}_4$ be a group of order 4 and set

$$M = \begin{bmatrix} 1 & a + a^2 + a^3 \\ a + a^2 + a^3 & 1 \end{bmatrix}$$

Then M is a CT(3, 3, 2)-matrix relative to $\langle a^2 \rangle$ and the corresponding transversal design is a $TD_2(4, 2)$. G is class-transitive, but contains no class regular group.

Remark 4.3. Let D be a $(u\lambda, u, u\lambda, \lambda)$-difference set in a group G relative to a subgroup U of G of order u. Then the following holds.

(i) The 1×1 matrix $[D]$ is a CT(u, λ, u)-matrix relative to U.

(ii) If a subgroup H of G satisfies $[G : H] = [U : U \cap H]$, then H is a semiregular class-transitive of the $TD_\lambda(u\lambda, u)$ corresponding to D.

Remark 4.4. Let $\mathcal{D} = (\mathbb{P}, \mathbb{B})$ be a $TD_\lambda(u\lambda, u)$ with $\lambda \in \{1, 2\}$. If $\lambda = 1$ and $TD_1(u, u)$ admits an abelian semiregular automorphism group of order u^2 then u is a power of a prime ([2],[7]). If $\lambda = 2$, $TD_2(2p, p)$ admits no semiregular automorphism group of order $2p^2$ ([6]). Recently, it is shown that $TD_2(2u, u)$ admits an abelian semiregular automorphism group of order $2u^2$ only if $u = 2^m$ for some m under a certain additional conditions ([3]). On the other hand, several authors constructed $TD_2(2u, u)$'s for an odd prime power u admitting class regular automorphism groups of order u by using GH$(u, 2)$-matrices ([8], [10],[11],[12]).

In connection with Remark 4.4 we would like to raise the following question.

Question 4.5. What can we say about u if $TD_(2u, u)$ admits a semiregular automorphism group of order u^2

It is conjectured that u is a power of a prime for any $TD_\lambda(u\lambda, u)$. Hence, it is conceivable that u in Question 4.5 is also a power of a prime.

In the rest of this article we consider $TD_2(2u, u)$ admitting semiregular automorphism group of order u^2.

5 Symmetric $TD_2(2u, u)$'s

We have seen in Example 4.2 that a $TD_2(2u, u)$ admitting semiregular automorphism group of order u^2 is not always symmetric $TD_2(2u, u)$.

Let u^* denote the square free part of a positive integer u. In this section we prove the following.

Theorem 5.1. *Let $\mathcal{D}$ be a symmetric $TD_2(2u,u)$. If $\mathcal{D}$ admits a semiregular automorphism group G of order u^2 and $u^* \neq 2$, then G contains a class regular subgroup, say U, of order u. In particular, there exist u-subsets D_{ij} $(1 \leq i,j \leq 2)$ of G such that $[D_{ij}]$ is a $GH(u,u,2)$-matrix of order 2 relative to U.*

Question 5.2. Is each D_{ij} always a $(u,u,u,1)$-difference set ?

As far as we know, D_{ij}'s are $(u,u,u,1)$-difference sets. If this is always true, u is a power of a prime applying the results of [2] and [7].

Proof of Theorem 5.1

Set $cD = (\mathbb{P},\mathbb{B})$. Applying Theorem 4.1 to $\lambda = 2$, there exist u-subsets D_{ij} $(1 \leq i,j \leq 2)$ of G and subgroups U_1, U_2 of G of order u such that $[D_{ij}]$ is a $\mathrm{GH}(u,u,2)$-matrix relative to U_1, U_2. Set $D_1 = D_{11}, D_2 = D_{12}, D_3 = D_{21}, D_4 = D_{22}$. Then,

$$D_1 D_1^{(-1)} + D_1 D_2^{(-1)} = 2u + 2(G - U_1) \tag{23}$$

$$D_3 D_3^{(-1)} + D_4 D_4^{(-1)} = 2u + 2(G - U_2) \tag{24}$$

$$D_1 D_3^{(-1)} + D_2 D_4^{(-1)} = 2G \tag{25}$$

If we show that $U_1 = U_2$, then $U_1 (= U_2)$ is class regular and so the theorem holds. Suppose $U_1 \neq U_2$. By assumption, $(\mathbb{P},\mathbb{B})$ is a symmetric $\mathrm{TD}_2(2u,u)$ and so by Result 1.1(iv), there exist subgroups V, W of G of order u satisfying

$$D_1 D_1^{(-1)} + D_3 D_3^{(-1)} = 2u + 2(G - V) \tag{26}$$

$$D_2 D_2^{(-1)} + D_4 D_4^{(-1)} = 2u + 2(G - W) \tag{27}$$

If $V \neq U_1, U_2$, by Proposition 2.3, we can take a character χ of G such that $\chi|_V = \chi_0$ and $\chi|_{U_i} \neq \chi_0$ $(1 \leq i \leq 2)$. By (26), $|\chi(D_1)|^2 + |\chi(D_3)|^2 = 0$. Hence, $\chi(D_1) = \chi(D_3) = 0$. On the other hand, using (23) and (24), $|\chi(D_1)|^2 + |\chi(D_2)|^2 = |\chi(D_3)|^2 + |\chi(D_4)|^2 = 2n$. it follows that $|\chi(D_2)|^2 = |\chi(D_4)|^2 = 2u$. However, by (25), $\chi(D_1)\overline{\chi(D_3)} + \chi(D_2)\overline{\chi(D_4)} = 0$, a contradiction. Thus either $V = U_1$ or $V = U_2$. Similarly, we have either $W = U_1$ or $W = U_2$. As $U_1 \neq U_2$, we may assume $V = U_1, W = U_2$. Then, by (23) and (26), $D_2 D_2^{(-1)} = D_3 D_3^{(-1)}$ and similarly by (24) and (27), $D_1 D_1^{(-1)} = D_4 D_4^{(-1)}$. Therefore $U_1 = U_2$.

6 Examples satisfying Theorem 4.1

In this section we first construct a class of $\mathrm{STD}_2(2q,q)$'s satisfying the condition of Theorem 4.1(i). Let q be a power of an odd prime and set $K = GF(q)$. Let $G = K \times K$ be an abelian group of order q^2. Let $\begin{bmatrix} D_1 & D_2 \\ D_3 & D_4 \end{bmatrix}$ be a $\mathrm{GH}(n,n,2)$-matrix over G. We assume that each D_i is a $(q,q,q,1)$-difference set in G relative to $U = 0 \times K$ (see Question 5.2) and construct a class of $\mathrm{STD}_2(2q,q)$'s satisfying

the condition of Theorem 4.1(i). We further assume that each D_i is obtained from quadratic polynomial over K.

Proposition 6.1. *Let q be a power of an odd prime. Set $K = GF(q)$ and $G = K \times K$. A matrix M over $\mathbb{Z}[G]$ given by*

$$M = \begin{bmatrix} \bigcup_{x\in K} (x, a_1x^2 + b_1x) & \bigcup_{x\in K} (x, a_2x^2 + b_2x) \\ \bigcup_{x\in K} (x, a_3x^2 + b_3x) & \bigcup_{x\in K} (x, a_4x^2 + b_4x + c) \end{bmatrix}$$

is a $GH(q, q, 2)$-matrix if and only if $a_i, b_i \in K$ $(1 \le i \le 4)$ and $c \in K$ satisfy the following condition.

$$a_1a_2a_3a_4 \in K \setminus K^2, \qquad \frac{1}{a_1} + \frac{1}{a_4} = \frac{1}{a_2} + \frac{1}{a_3}$$
$$(a_1 - a_3)(a_2b_4 - a_4b_2) + (a_2 - a_4)(a_1b_3 - a_3b_1) = 0$$
$$c = \frac{(b_1 - b_3)^2}{4(a_1 - a_3)} - \frac{(b_2 - b_4)^2}{4(a_2 - a_4)},$$

where $K \setminus K^2$ denotes the set of non-square elements of K. The symmetric $TD_2(2u, u)$ corresponding to M admits G as a semiregular automorphism group of order q^2.

Remark 6.2. Set $b_1 = b_2 = b_3 = b_4 = 0$. Then, applying Proposition 6.3 of [4], we have the following $\mathrm{GH}(q, 2)$-matrix of order $2q$.

$$\begin{bmatrix} a_1(\ell - m)^2 & a_2(\ell - m)^2 \\ a_3(\ell - m)^2 & a_4(\ell - m)^2 \end{bmatrix}_{\ell,m\in K},$$

where $K = GF(q)$ and a_1, a_2, a_3 and a_4 satisfy the following.

$$a_1a_2a_3a_4 \in K \setminus K^2, \qquad \frac{1}{a_1} + \frac{1}{a_4} = \frac{1}{a_2} + \frac{1}{a_3}$$

We now construct a class of $\mathrm{STD}_2(2q, q)$'s satisfying the condition of Theorem 4.1(ii), where $q = 2^e$.

Lemma 6.3. *Set $K = GF(2^e)$ and let f_K be a bijective additive map from K to K. We define a 2-group $G_{f_K} = K \times K$ of order q^2 as follows.*

$(x_1, y_1)(x_2, y_2) = (x_1 + x_2, y_1 + y_2 + x_1f(x_2))$ $((x_1, y_1), (x_2, y_2) \in G)$

Then the following holds.

(i) $R = F \times 0$ is a $(2^e, 2^e, 2^e, 1)$-difference set relative to $U = 0 \times F$.

(ii) G_{f_K} is abelian if and only if $af(b) = bf(a)$ for any $a, b \in K$.

We will construct examples of Theorem 4.1(ii) using G when it is non abelian.

Using Lemma 6.3, we construct a class of examples satisfying Theorem 4.1(ii).

Lemma 6.4. *Let $K = GF(2^{2m})$ and $f(x) = x^{2^m}$. Then G_f has a subgroup H satisfying*

$$[G_f : H] = 2, \quad H \geq (0 \times GF(2)), \quad H \not\geq 0 \times F$$

In particular, setting $\overline{G}_f = G_f/0 \times GF(2)$, a subset $\overline{F \times 0}$ of $\overline{G}_f$ is a $(2^{2m}, 2^{2m-1}, 2^{2m}, 2)$-difference set relative to $\overline{0 \times F}$. Moreover, the $TD_2(2^{2m}, 2^{2m-1})$ corresponding the difference set admits $\overline{H}$ as a semiregular automorphism group of order 2^{2m-2} and contains no class regular subgroup.

Corollary 6.5. *For any odd power q of 2, there exists a $TD_2(2q, q)$ admitting semiregular class-transitive automorphism of order q^2.*

As an application of the results we have

Proposition 6.6. *Let G be a group of order $2u^2$ for an odd integer u and assume that a Hall $2'$-subgroup of G is abelian. If G contains a $(2u, u, 2u, 2)$-difference set relative to U, then U is a normal subgroup of G.*

Proposition 6.7. *Let G be a group of order $2u^2$ for an integer u and assume that $u^* \neq 2$. If G contains a $(2u, u, 2u, 2)$-difference set relative to U, then U is a subgroup of $\langle g^2 \mid g \in G \rangle$.*

References

[1] T. Beth, D. Jungnickel and H. Lenz, "Design Theory" Volume I, Second Edition, Cambridge University Press, 1999.

[2] A. Blokhuis, D. Jungnickel and B. Schmidt, Proof of the prime power conjecture for projective planes of order n with abelian collineation groups, Proc. Amer. Math.

[3] Y. Hiramine, On abelian $(2n, n, 2n, 2)$-difference set, JCTA 101 (2010), 281-284.

[4] Y. Hiramine, Modified generalized Hadamard matrices and constructions for transversal designs, Designs, Codes and Cryptography, Vol.56, 2010, 21–33.

[5] D. Jungnickel, On automorphism groups of divisible designs, Canad. J. Math. Vol. 34, 1982, 257–297.

[6] T. Feng and Q. Xiang, Semi-regular relative difference sets with large forbidden subgroups, J. of Combinatorial Theory, Ser. A, Vol. 115 (2008), 1456-1473.

[7] M. J. Ganley, On a paper of Dembowski and Ostrom, Arch. Math. Vol. 27 (1976), 93-98.

[8] D. Jungnickel, On difference matrices, resolvable transversal designs and generalized Hadamard matrices, Math. Z. Vol. 167(1979), 49-60.

[9] B. Schmidt, *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Mathematics 1797, Springer-Verlag, Berlin Heiderberg (2002)

[10] Zhang Wen Liu, A difference scheme $D(14, 14, 7, 2)$ generating orthogonal array $\mathrm{OA}(98, 15, 7, 2)$, Kexue Tangbao Vol.22 (1977) 31.

[11] M. Masuyama, Construction of difference sets for $\mathrm{OA}(2p^2, 2p+1, p, 2)$ p being an odd prime, Rep. Statist. Appl. Res. Un. Japan. Sci.Engrs. vol.16 (1969), 1-9.

[12] Cheng Xu Xu, Construction of orthogonal arrays $L_{2p^u}(p^{1+\sum_{i=1}^{u-1} 2p^i})$ with p odd prime, Acta Math.Appl. Sinica 2 (1979), 92-97.

Generalized Hadamard matrices over $GF(4)$ and Hadamard matrices

K. Akiyama(Fukuoka University; akiyama@sm.fukuoka-u.ac.jp)
C. Suetake(Oita University; suetake@csis.oita-u.ac.jp)
M. Tanaka(Sojo University; mtanaka@ed.sojo-u.ac.jp)

§1. Definitions

Definition 1.1 A **symmetric transversal design** $\mathrm{STD}_\lambda[k;u]$ (STD) is an incidence structure $\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ satisfying the following three conditions:
(i) Each block contains exactly k points.
(ii) The point set $\mathcal{P}$ is partitioned into k point sets $\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}$ of equal size u such that any two distinct points are incident with exactly λ blocks or no block according as they are contained in different $\mathcal{P}_i$'s or not. $\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}$ are said to be the **point classes** of $\mathcal{D}$.
(iii) The dual structure of $\mathcal{D}$ also satisfies the above conditions (i) and (ii). The point classes of the dual structure of $\mathcal{D}$ are said to be the **block classes** of $\mathcal{D}$. (From the definition of a STD, $k=\lambda u$.)

Definition 1.2 Let $\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ be an STD. Let Ω and Δ be the set of point classes of $\mathcal{D}$ and the set of block classes of $\mathcal{D}$, respectively. Let $W\leq \mathrm{Aut}\mathcal{D}$. Then W is called an **elation group** of $\mathcal{D}$ and any non-identity element of W is called an **elation**, if $W^\Omega=1$ and $W^\Delta=1$. (In this case it is known that W acts semiregularly on each point class and on each block class.) Moreover $\mathcal{D}$ is called **class regular** with respect to W, if $|W|=u$.

Definition 1.3 Let $u(\geq 2),\lambda\in\mathbb{N}$ and $k=\lambda u$. Let U be a group of order u. Then, a $k\times k$ matrix

$$H=\begin{pmatrix} \varphi_{00} & \varphi_{01} & \cdots & \varphi_{0,k-1} \\ \varphi_{10} & \varphi_{11} & \cdots & \varphi_{1,k-1} \\ \vdots & \vdots & & \vdots \\ \varphi_{k-1,0} & \varphi_{k-1,1} & \cdots & \varphi_{k-1,k-1} \end{pmatrix}$$

with entries from U is called a **generalized Hadamard matrix** of order k over U, $\mathrm{GH}(U,\lambda)$, if $\displaystyle\sum_{j=0}^{k-1}\varphi_{i_1,j}\varphi_{i_2,j}{}^{-1}=\lambda\sum_{\tau\in U}\tau\ (\in\mathbb{Z}[U])$ for $0\leq i_1\neq i_2\leq k-1$.

Remark 1.4 Any class regular $\mathrm{STD}_\lambda[k;u]$ $\mathcal{D}$ with respect to a group U

corresponds to some GH(U, λ) H.

Example 1.5 Consider $GF(4)$ as an additive group. Let $GF(4) = \{0, 1, 2, 3\}$, where 0 is the zero element and $1+2 = 2+1 = 3$, $1+3 = 3+1 = 2$, $2+3 = 3+2 = 1$. Then the following 4×4 matrix over $GF(4)$

$$H = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 \\ 0 & 2 & 3 & 1 \\ 0 & 3 & 1 & 2 \end{pmatrix}$$

is a GH$(GF(4), 1)$.

Let $0 \longmapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $1 \longmapsto \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$, $2 \longmapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$, $3 \longmapsto \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.

Then from H we get an incidence matrix S of a class regular $\mathrm{STD}_1[4; 4]$ $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ with respect to $(GF(4), +)$.

$$S = \left(\begin{array}{c|c|c|c} 1000 & 1000 & 1000 & 1000 \\ 0100 & 0100 & 0100 & 0100 \\ 0010 & 0010 & 0010 & 0010 \\ 0001 & 0001 & 0001 & 0001 \\ \hline 1000 & 0010 & 0100 & 0001 \\ 0100 & 0001 & 1000 & 0010 \\ 0010 & 1000 & 0001 & 0100 \\ 0001 & 0100 & 0010 & 1000 \\ \hline 1000 & 0100 & 0001 & 0010 \\ 0100 & 1000 & 0010 & 0001 \\ 0010 & 0001 & 0100 & 1000 \\ 0001 & 0010 & 1000 & 0100 \\ \hline 1000 & 0001 & 0010 & 0100 \\ 0100 & 0010 & 0001 & 1000 \\ 0010 & 0100 & 1000 & 0001 \\ 0001 & 1000 & 0100 & 0010 \end{array}\right).$$

where $\mathcal{P}_i = \{p_i, p_{i+1}, p_{i+2}, p_{i+3}\}$ and $\mathcal{B}_i = \{B_i, B_{i+1}, B_{i+2}, B_{i+3}\}$ $(i \in \{0, 1, 2, 3\})$ are the point classes and the block classes of $\mathcal{D}$, respectively.

de Launey conjectured that there is a GH$(\mathrm{EA}(4), \lambda)$ for any positive integer λ (Conjecture 5.18 in [CD]). There are studies of generalized Hadamard matrices of order 16 by M. Harada, C. Lam, and V. D. Tonchev [HLT] and P. B. Gibbons and R. Mathon [GM]. But, little is known about the orders for which there exist a generalized Hadamard matrix over $\mathrm{EA}(2^t)$ for $t \geq 2$ (Remark 5.17 in [CD]). For example, when $\lambda < 25$, the existence of a GH$(\mathrm{EA}(4), \lambda)$ for $\lambda \in \{5, 6, 7, 10, 11, 13, 15, 17, 18, 19, 20, 21, 22, 23\}$ is not known (Table 5.13 in [CD]).

In this note, we construct a GH$(GF(4), 6)$ and a GH$(GF(4), 10)$ and give a conjecture about generalized Hadamard matrices over $GF(4)$. We also state about Hadamard matrices with a interesting form related these generalized Hadamard matrices.

§2 Hadamard matrices

Definition 2.1 Let n be a positive integer. Let H be a $n \times n$ matrix with entries from $\{1, -1\}$. Then H is said to be a **Hadamard matrix** of order n, if $HH^T = nI$.

Remark 2.2 If H is a Hadamard matrix of order n, then $n \in \{1, 2\}$ or $n \equiv 0 \pmod 4$.

Definition 2.3 Let n be a positive integer. For $a_0, a_1, \cdots, a_{n-1} \in \{1, -1\}$, set

$$((a_0, a_1, \cdots, a_{n-1})) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-3} & a_{n-2} & a_{n-1} \\ -a_{n-1} & a_0 & a_1 & \cdots & a_{n-4} & a_{n-3} & a_{n-2} \\ -a_{n-2} & -a_{n-1} & a_0 & \cdots & a_{n-5} & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ -a_3 & -a_4 & -a_5 & \cdots & a_0 & a_1 & a_2 \\ -a_2 & -a_3 & -a_4 & \cdots & -a_{n-1} & a_0 & a_1 \\ -a_1 & -a_2 & -a_3 & \cdots & -a_{n-2} & -a_{n-1} & a_0 \end{pmatrix}.$$

This matrix is said to be a (-1)-**circulant matrix** of order n over $\{1, -1\}$.

Example 2.4 $((1,1,1,1,-1,1)) =$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & -1 & 1 \\ -1 & 1 & 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 & 1 & 1 \\ -1 & -1 & 1 & -1 & 1 & 1 \\ -1 & -1 & -1 & 1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} + & + & + & + & - & + \\ - & + & + & + & + & - \\ + & - & + & + & + & + \\ - & + & - & + & + & + \\ - & - & + & - & + & + \\ - & - & - & + & - & + \end{pmatrix}$$

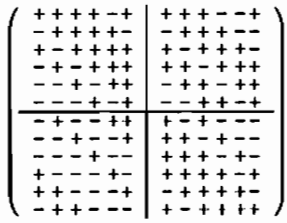
From now on, we use $+$ and $-$ instead of 1 and -1, respectively.

Lemma 2.5 *Let* $a_0, a_1, \cdots, a_{n-1}, b_0, b_1, \cdots, b_{n-1} \in \{1, -1\}$.
Then $((a_0, a_1, \cdots, a_{n-1}))((b_0, b_1, \cdots, b_{n-1})) = ((b_0, b_1, \cdots, b_{n-1}))((a_0, a_1, \cdots, a_{n-1}))$.

Lemma 2.6 *Let* m *be a positive integer. For* $a_0, a_1, \cdots, a_{2m-1}, b_0, b_1, \cdots, b_{2m-1} \in \{1, -1\}$, *let* $A = ((a_0, a_1, \cdots, a_{2m-1}))$ *and* $B = ((b_0, b_1, \cdots, b_{2m-1}))$. *Set* $[A, B] = \begin{pmatrix} A & B \\ -B^T & A^T \end{pmatrix}$. *Then* $[A, B]$ *is a Hadamard matrix of order* $4m$ *if and only if* $-a_0a_i - a_1a_{i+1} - \cdots - a_{2m-1-i}a_{2m-1}$
$+a_{2m-i}a_0 + a_{2m+1-i}a_1 + \cdots + a_{2m-1}a_{i-1}$
$= b_0b_i + b_1b_{i+1} + \cdots + b_{2m-1-i}b_{2m-1}$
$-b_{2m-i}b_0 - b_{2m+1-i}b_1 - \cdots - b_{2m-1}b_{i-1}$ *for* $m + 1 \leq i \leq 2m - 1$.

Proposition 2.7 *For any positive integer* m *with* $m \leq 21$, *there exists a Hadamard matrix of order* $4m$ *with the form stated in Lemma* 2.6.

Example 2.8 $[((+\,+\,+\,+\,-\,+)),\ ((+\,+\,+\,-\,-\,+))] =$



is a Hadamard matrix of order 12.

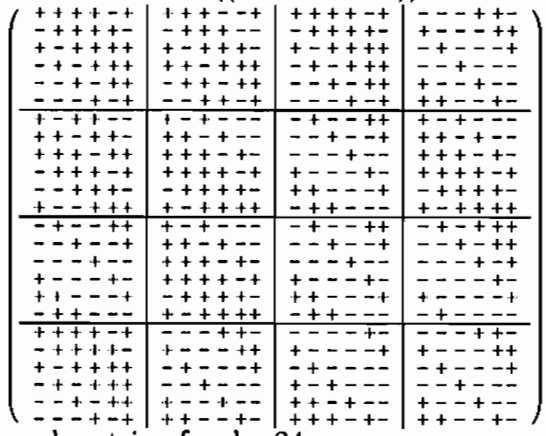
Lemma 2.9 *Let m be a positive integer. For $a_0, a_1, \cdots, a_{2m-1}, b_0, b_1, \cdots, b_{2m-1} \in \{1, -1\}$, let $A = ((a_0, a_1, \cdots, a_{2m-1}))$ and $B = ((b_0, b_1, \cdots, b_{2m-1}))$.*
Set

$$[A, B, A, -B] = \begin{pmatrix} A & B & A & -B \\ B^T & A^T & -B^T & A^T \\ -B^T & A^T & -B^T & -A^T \\ A & -B & -A & -B \end{pmatrix}.$$

Then, the following three statements are equivalent.
(i) $[A, B, A, -B]$ *is a Hadamard matrix of order* $8m$.
(ii) $[A, B] = \begin{pmatrix} A & B \\ -B^T & A^T \end{pmatrix}$ *is a Hadamard matrix of order* $4m$.
(iii) $-a_0a_i - a_1a_{i+1} - \cdots - a_{2m-1-i}a_{2m-1} + a_{2m-i}a_0 + a_{2m+1-i}a_1 + \cdots + a_{2m-1}a_{i-1}$
$= b_0b_i + b_1b_{i+1} + \cdots + b_{2m-1-i}b_{2m-1} - b_{2m-i}b_0 - b_{2m+1-i}b_1 - \cdots - b_{2m-1}b_{i-1}$
for $m + 1 \leq i \leq 2m - 1$.

Example 2.10 Let $A = ((+\,+\,+\,+\,-\,+))$ and $B = ((+\,+\,+\,-\,-\,+))$. Then

$[A, B, A, -B] =$



is a Hadamard matrix of order 24.

§3 Generalized Hadamard matrices over $GF(4)$

Hypothesis 3.1 For a positive integer n let

$$G = \langle \sigma,\ \tau |\ \sigma^{2n} = \tau^4 = 1,\ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle.$$

Therefore G is a meta cyclic group of order $8n$. Set $U = \langle \sigma^n,\ \tau^2 \rangle$. Then U is a normal subgroup of G, $|U| = 4$, and $U \leq Z(G)$, where $Z(G)$ is the center of G. Let $\mathcal{D} = (\mathcal{P}, \mathcal{B})$ be a class regular $\mathrm{STD}_n[4n; 4]$ with respect to U which G acts semiregularly on the point set and the block set.

Let $\{p, q\}$ be the set of base points of $\mathcal{D}$ and $\{B, C\}$ the set of base blocks of $\mathcal{D}$. Set $\alpha = \sigma^n$, $\beta = \tau^2$, and $\gamma = \alpha\beta = \sigma^n\tau^2$. Consider the following correspondences.

$$1 \longleftrightarrow 0,\ \alpha \longleftrightarrow 1,\ \beta \longleftrightarrow 2,\ \gamma \longleftrightarrow 3.$$

Then $GF(4) = \{0, 1, 2, 3\}$, where 0 is the zero element of $GF(4)$ and

$$1 + 2 = 2 + 1 = 3,\ 1 + 3 = 3 + 1 = 2,\ 2 + 3 = 3 + 2 = 1.$$

Set for $0 \leq i \leq n - 1$
$\mathcal{P}_i = \{p^{\sigma^i}, p^{\sigma^i\alpha}, p^{\sigma^i\beta}, p^{\sigma^i\gamma}\}$, $\mathcal{P}_{n+i} = \{p^{\tau\sigma^i}, p^{\tau\sigma^i\alpha}, p^{\tau\sigma^i\beta}, p^{\tau\sigma^i\gamma}\}$,
$\mathcal{P}_{2n+i} = \{q^{\sigma^i}, q^{\sigma^i\alpha}, q^{\sigma^i\beta}, q^{\sigma^i\gamma}\}$, and $\mathcal{P}_{3n+i} = \{q^{\tau\sigma^i}, q^{\tau\sigma^i\alpha}, q^{\tau\sigma^i\beta}, q^{\tau\sigma^i\gamma}\}$.
Set for $0 \leq j \leq n - 1$
$\mathcal{B}_j = \{B^{\sigma^j}, B^{\sigma^j\alpha}, B^{\sigma^j\beta}, B^{\sigma^j\gamma}\}$, $\mathcal{B}_{n+j} = \{B^{\tau\sigma^j}, B^{\tau\sigma^j\alpha}, B^{\tau\sigma^j\beta}, B^{\tau\sigma^j\gamma}\}$,
$\mathcal{B}_{2n+j} = \{C^{\sigma^j}, C^{\sigma^j\alpha}, C^{\sigma^j\beta}, C^{\sigma^j\gamma}\}$, and $\mathcal{B}_{3n+j} = \{C^{\tau\sigma^j}, C^{\tau\sigma^j\alpha}, C^{\tau\sigma^j\beta}, C^{\tau\sigma^j\gamma}\}$.

Then $\mathcal{P}_0,\ \mathcal{P}_1, \cdots,\ \mathcal{P}_{4n-1}$ is the point classes of $\mathcal{D}$ and $\mathcal{B}_0,\ \mathcal{B}_1, \cdots, \mathcal{B}_{4n-1}$ is the block classes of $\mathcal{D}$.

When we do the labeling of points and blocks of $\mathcal{D}$ by the above order, let H_{4n} be the generalized Hadamard matrix of order $4n$ over $GF(4)$ corresponding to $\mathcal{D}$.

We use the same notation as in Definition 2.3 for a matrix over $GF(4)$.

Definition 3.2 Let n be a positive integer. Let $a_0, a_1, \cdots, a_{n-1} \in GF(4) = \{0, 1, 2, 3\}$. A $n \times n$ matrix $((a_0, a_1, \cdots, a_{n-1}))$ on $GF(4)$ are defined as follows.

$$((a_0, a_1, \cdots, a_{n-1})) = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-3} & a_{n-2} & a_{n-1} \\ a_{n-1}+1 & a_0 & a_1 & \cdots & a_{n-4} & a_{n-3} & a_{n-2} \\ a_{n-2}+1 & a_{n-1}+1 & a_0 & \cdots & a_{n-5} & a_{n-4} & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ a_3+1 & a_4+1 & a_5+1 & \cdots & a_0 & a_1 & a_2 \\ a_2+1 & a_3+1 & a_4+1 & \cdots & a_{n-1}+1 & a_0 & a_1 \\ a_1+1 & a_2+1 & a_3+1 & \cdots & a_{n-2}+1 & a_{n-1}+1 & a_0 \end{pmatrix}.$$

Lemma 3.3 *H_{4n} is a* GH$(GF(4), n)$ *with the form*

$$H_{4n} = \left(\begin{array}{cc|cc} A_n & B_n & C_n & D_n \\ {B_n}^T + J(2)_n & {A_n}^T & {D_n}^T + J(2)_n & {C_n}^T \\ \hline P_n & Q_n & R_n & S_n \\ {Q_n}^T + J(2)_n & {P_n}^T & {S_n}^T + J(2)_n & {R_n}^T \end{array}\right),$$

where $A_n = ((a_0, a_1, \cdots, a_{n-1}))$, $B_n = ((b_0, b_1, \cdots, b_{n-1}))$,
$C_n = ((c_0, c_1, \cdots, c_{n-1}))$, $D_n = ((d_0, d_1, \cdots, d_{n-1}))$,
$P_n = ((p_0, p_1, \cdots, p_{n-1}))$, $Q_n = ((q_0, q_1, \cdots, q_{n-1}))$,
$R_n = ((r_0, r_1, \cdots, r_{n-1}))$, $S_n = ((s_0, s_1, \cdots, s_{n-1}))$, *and*

$$J(2)_n = \begin{pmatrix} 2 & \cdots & 2 \\ \vdots & & \vdots \\ 2 & \cdots & 2 \end{pmatrix}.$$

Definition 3.4 A mapping $f : GF(4) = \{0, 1, 2, 3\} \longrightarrow \{1, -1\}$ is defined as follows.

$$f(0) = f(2) = 1 \text{ and } f(1) = f(3) = -1.$$

For a matrix $H = (h_{ij})$ over $GF(4)$ a matrix $\widetilde{H}$ over $\{1, -1\}$ is defined by $\widetilde{H} = (f(h_{ij}))$.

Lemma 3.5 *$\widetilde{H_{4n}}$ is a Hadamard matrix of order $4n$ with the form*

$$\widetilde{H_{4n}} = \left(\begin{array}{cc|cc} {A_n}' & {B_n}' & {C_n}' & {D_n}' \\ {B_n}'^T & {A_n}'^T & {D_n}'^T & {C_n}'^T \\ \hline {P_n}' & {Q_n}' & {R_n}' & {S_n}' \\ {Q_n}'^T & {P_n}'^T & {S_n}'^T & {R_n}^T \end{array}\right),$$

where ${A_n}' = ((a_0', a_1', \cdots, a_{n-1}'))$, ${B_n}' = ((b_0', b_1', \cdots, b_{n-1}'))$,
${C_n}' = ((c_0', c_1', \cdots, c_{n-1}'))$, ${D_n}' = ((d_0', d_1', \cdots, d_{n-1}'))$,
${P_n}' = ((p_0', p_1', \cdots, p_{n-1}'))$, ${Q_n}' = ((q_0', q_1', \cdots, q_{n-1}'))$,
${R_n}' = ((r_0', r_1', \cdots, r_{n-1}'))$, *and* ${S_n}' = ((s_0', s_1', \cdots, s_{n-1}'))$.
Here each entry of $\widetilde{H_{4n}}$ is 1 *or* -1 *and the notation* (( )) *is the one defined by Definition* 2.3.

Example 3.6

$$H_4 = \left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 2 & 0 & 2 & 1 \\ \hline 0 & 1 & 2 & 2 \\ 3 & 0 & 0 & 2 \end{array}\right)$$

Proposition 3.7 *A* GH$(GF(4), n)$ H_{4n} *stated in Lemma* 3.3 *exists for* $n = 1$, *but does not exist for any odd integer with* $3 \leq n \leq 11$.

Conjecture 3.8 *If* n *is an odd integer with* $n \geq 3$, *there does not exist* GH$(GF(4), n)$ H_{4n} *stated in Lemma* 3.3.

Example 3.9 We consider whether there exists a GH$(GF(4), 2m)$ $H_{4n} = H_{8m}$ $(n = 2m)$ such that $\widetilde{H_{4n}} = \widetilde{H_{8m}}$ has the form $[A, B, A, -B]$ stated in Lemma 3.6 or not for a small positive integer m.

(i) Let $m = 1$, $A = ((++))$, and $B = ((++))$.Then the Hadamard matrix

$$\widetilde{H_8} = [A, B, A, -B] = \left(\begin{array}{c|c|c|c} ++ & ++ & ++ & -- \\ -+ & -+ & -+ & +- \\ \hline +- & +- & -+ & +- \\ ++ & ++ & -- & ++ \\ \hline -+ & +- & -+ & -+ \\ -- & ++ & -- & -- \\ \hline ++ & -- & -- & -- \\ -+ & +- & +- & +- \end{array}\right)$$

of order 8 is extended to the following GH$(GF(4), 2)$.

$$H_8 = \left(\begin{array}{cc|cc|cc|cc} 0 & 0 & 0 & 0 & 0 & 2 & 1 & 3 \\ 1 & 0 & 1 & 0 & 3 & 0 & 2 & 1 \\ \hline 2 & 3 & 0 & 1 & 3 & 0 & 0 & 3 \\ 2 & 2 & 0 & 0 & 1 & 3 & 2 & 0 \\ \hline 1 & 2 & 0 & 3 & 3 & 2 & 3 & 2 \\ 3 & 1 & 2 & 0 & 3 & 3 & 3 & 3 \\ \hline 2 & 0 & 1 & 3 & 1 & 1 & 3 & 3 \\ 1 & 2 & 2 & 1 & 0 & 1 & 2 & 3 \end{array}\right).$$

(ii) Let $m = 2$, $A = ((+++-))$, and $B = ((++-+))$.
Then the Hadamard matrix

$\widetilde{H_{16}} = [A, B, A, -B] =$

$$\left(\begin{array}{c|c|c|c} +++- & ++-+ & +++- & --+- \\ -+++ & -++- & -+++ & +--+ \\ --+- & +--+ & --+- & -+-- \\ ---+ & -+-+ & ---+ & +-+- \\ \hline +-+- & +--- & -+-+ & +--- \\ +--+ & ++-- & --+- & ++-- \\ ++-+ & +++- & +---+ & ++++ \\ -++- & +++- & -+-- & +++- \\ \hline -+-+ & +--- & -+-+ & -+++ \\ --+- & ++-- & --+- & --++ \\ +--+ & +++- & +--+ & ---+ \\ -++- & +++- & -+-- & ---- \\ \hline +++- & ---+ & ---- & --+- \\ -+++ & +--+ & +--- & +--+ \\ --++ & -+-- & ++-- & -+-- \\ ---+ & +-+- & +++- & +-+- \end{array}\right).$$

of order 16 is extended to the following GH($GF(4), 4$).

$$H_{16} = \left(\begin{array}{cccc|cccc|cccc|cccc}
0&0&0&0&0&2&1&2&0&2&2&0&1&3&2&1\\
1&0&0&0&3&0&2&1&1&0&2&2&0&1&3&2\\
1&1&0&0&0&3&0&2&3&1&0&2&3&0&1&3\\
1&1&1&0&3&0&3&0&3&3&1&0&2&3&0&1\\
\hline
2&1&2&1&0&1&1&1&3&2&1&0&0&1&3&3\\
0&2&1&2&0&0&1&1&1&3&2&1&2&0&1&3\\
3&0&2&1&0&0&0&1&0&1&3&2&2&2&0&1\\
0&3&0&2&0&0&0&0&3&0&1&3&0&2&2&0\\
\hline
1&0&3&2&0&1&3&3&1&2&1&2&1&0&0&0\\
3&1&0&3&2&0&1&3&3&1&2&1&1&1&0&0\\
2&3&1&0&2&2&0&1&0&3&1&2&1&1&1&0\\
1&2&3&1&0&2&2&0&3&0&3&1&1&1&1&1\\
\hline
2&0&0&2&1&3&2&1&3&3&3&3&1&3&0&3\\
3&2&0&0&0&1&3&2&2&3&3&3&2&1&3&0\\
1&3&2&0&3&0&1&3&2&2&3&3&1&2&1&3\\
1&1&3&2&2&3&0&1&2&2&2&3&2&1&2&1
\end{array}\right).$$

(iii) Let $m = 3$, $A = \widetilde{((+++-+))}$, and $B = ((+++--+))$. Then the Hadamard matrix $\widetilde{H_{24}} = [A, B, A, -B]$ of order 24 is extended to the following GH($GF(4), 6$).

$$H_{24} = \left(\begin{array}{cccccc|cccccc|cccccc|cccccc}
0&0&0&0&1&2&0&2&0&1&3&0&0&0&0&2&3&2&1&1&3&0&2&1\\
3&0&0&0&0&1&1&0&2&0&1&3&3&0&0&0&2&3&0&1&1&3&0&2\\
0&3&0&0&0&0&2&1&0&2&0&1&2&3&0&0&0&2&3&0&1&1&3&0\\
1&0&3&0&0&0&0&2&1&0&2&0&3&2&3&0&0&0&1&3&0&1&1&3\\
1&1&0&3&0&0&1&0&2&1&0&2&1&3&2&3&0&0&2&1&3&0&1&1\\
1&1&1&0&3&0&3&1&0&2&1&0&1&1&3&2&3&0&0&2&1&3&0&1\\
\hline
2&3&0&2&3&1&0&3&0&1&1&1&3&2&1&3&0&2&0&3&2&3&1&1\\
0&2&3&0&2&3&0&0&3&0&1&1&3&3&2&1&3&0&0&0&3&2&3&1\\
2&0&2&3&0&2&0&0&0&3&0&1&1&3&3&2&1&3&0&0&0&3&2&3\\
3&2&0&2&3&0&0&0&0&0&3&0&2&1&3&3&2&1&2&0&0&0&3&2\\
1&3&2&0&2&3&1&0&0&0&0&3&0&2&1&3&3&2&3&2&0&0&0&3\\
2&1&3&2&0&2&2&1&0&0&0&0&3&0&2&1&3&3&2&3&2&0&0&0\\
\hline
1&2&1&1&0&2&0&1&2&3&3&1&3&0&3&3&0&2&3&2&3&2&0&2\\
3&1&2&1&1&0&0&0&1&2&3&3&3&3&0&3&3&0&3&3&2&3&2&0\\
1&3&1&2&1&1&2&0&0&1&2&3&1&3&3&0&3&3&1&3&3&2&3&2\\
0&1&3&1&2&1&2&2&0&0&1&2&2&1&3&3&0&3&3&1&3&3&2&3\\
0&0&1&3&1&2&3&2&2&0&0&1&2&2&1&3&3&0&2&3&1&3&3&2\\
3&0&0&1&3&1&0&3&2&2&0&0&1&2&2&1&3&3&3&2&3&1&3&3\\
\hline
2&2&0&0&1&2&1&3&1&0&0&3&1&1&3&1&0&1&3&3&1&2&2&1\\
3&2&2&0&0&1&2&1&3&1&0&0&0&1&1&3&1&0&0&3&3&1&2&2\\
0&3&2&2&0&0&1&2&1&3&1&0&1&0&1&1&3&1&3&0&3&3&1&2\\
1&0&3&2&2&0&1&1&2&1&3&1&0&1&0&1&1&3&3&3&0&3&3&1\\
1&1&0&3&2&2&0&1&1&2&1&3&2&0&1&0&1&1&0&3&3&0&3&3\\
3&1&1&0&3&2&2&0&1&1&2&1&0&2&0&1&0&1&2&0&3&3&0&3
\end{array}\right).$$

(iv) Let $m = 4$, $A = ((+++++-++))$, and $B = ((+++-+-++))$. Then the Hadamard matrix $\widetilde{H_{32}}$ of order 32 is extended to a GH($GF(4), 8$).

(v) Let $m = 5$, $A = ((+++++++--++))$, and $B = ((+++-+-++-+))$. Then the Hadamard matrix $\widetilde{H_{40}}$ of order 40 is extended to a GH($GF(4), 10$).

Theorem 3.10 *For any even positive integer n with $2 \leq n \leq 10$, there exists a* GH($GF(4), n$) *with the form stated in Lemma* 3.3.

Corollary 3.11 *For any even positive integer n with $2 \leq n \leq 10$, there exists an* $\mathrm{STD}_n[4n; 4]$ *with respect to $U = \langle \sigma^n, \tau^2 \rangle$ which the meta cyclic group*

$$G = \langle \sigma, \tau | \ \sigma^{2n} = \tau^4 = 1, \ \tau^{-1}\sigma\tau = \sigma^{-1} \rangle$$

of order $8n$ acts semiregularly on the point set and the block set as an automorphism group.

Remark 3.12 A GH($GF(4), 6$) and a GH($GF(4), 10$) given in Theorem 3.10 have new parameters as generalized Hadamard matrices (see Table 5.13 by de Launey in [CD]).

Conjecture 3.13 *For any even positive integer n, there exists a* GH($GF(4), n$) *with the form stated in Lemma* 3.3.

References

[CD] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, Second Edition, Chapman & Hall/CRC Press, Boca Raton (2007).

[GM] P. B. Gibbons and R. Mathon, Enumeration of generalized Hadamard matrices of order 16 and related designs, *J. Combin. Designs* **17**(2009), 119–135.

[HLT] M. Harada, C. Lam, and V. D. Tonchev, Symmetric $(4, 4)$-nets and generalized Hadamard matrices over group of order 4, *Des. Codes Cryptgr.* **34**(2005), 71–87.

A difference set description of dimensional dual hyperovals

Alexander Pott

Department of Mathematics, Otto-von-Guericke-University
Magdeburg, D-39016 Magdeburg, Germany

Abstract. Almost perfect nonlinear functions F may be viewed as difference set type representations of certain semi-biplanes, see [1]. If F is quadratic, these semi-biplanes can be also described via dimensional dual hyperovals. In this note we show that certain non-commutative dimensional dual hyperovals can be described by a non-abelian version of almost perfect nonlinear functions.

A **semi-biplane** Π is an incidence structure of points and lines with the following two properties:

- Any two different points are joined by 0 or 2 lines.
- Any two lines intersect in 0 or 2 points.

With each incidence structure consisting of points and lines, we may associate a graph: The vertices of the graph are the points, and two points are adjacent if and only if the two points are joined by a line. The incidence structure is called **connected** if this graph is connected. In the literature, connectivity of the semi-biplane is usually part of the definition. However, in this note we also consider non-connected semi-biplanes. We indicate explicitely if the incidence structure is connected.

One can show that for finite connected semi-biplanes, there is a number k such that any line consists of k points, and through any point there are precisely k lines. Moreover, if v is the number of points, then v is also the number of lines. We say that (v, k) are the **parameters** of the semi-biplane.

Example 1. Take the vertices of an icosahedron as the points, and the neighbors of each vertex as blocks. Then we have a semi-biplane with $v = 12$ and $k = 5$.

The semi-biplanes relevant in this paper can be constructed as follows: Let $U_i, i \in I$, be a collection of n-dimensional subspaces in V, where V is a vector space over $\mathbb{F}_2$. We call this collection $\mathcal{D}$ of subspaces a **dimensional dual hyperoval** if the following two properties hold:

- $\dim(U_i \cap U_j) = 1$ for all $i \neq j$.
- There is no element $v \neq 0$ contained in three of the U_i.

The vector space generated by the subspaces U_i is called the **ambient space**. It is easy to construct a semi-biplane $\Pi(\mathcal{D})$ from $\mathcal{D}$: The points are the elements in V, and the lines are the cosets of the U_i. Note that the mappings $\tau_v : V \to V$ with $\tau(x) := x+v$

are automorphisms of $\Pi(\mathcal{D})$, therefore we call the semi-biplane a **translation semi-biplane** (Yoshiara also used the term elation semi-biplane).

The line graph of this semi-biplane has a nice representation: Define the set $D := \bigcup_{i \in I} U_i$. Then two different points v and w are connected by a line if and only if $v - w \in D$. Therefore, the incidence structure is connected if and only if V is the ambient space. Otherwise the incidence structure splits into isomorphic copies.

We note that all this is well known, see [2], for instance.

The semi-biplanes in this note have parameters $v = 2^{2n}$ and $k = 2^n$. They can be constructed as follows: Take a set T_i, $i = 1, \ldots, 2^n - 1$, of linear mappings $\mathbb{F}_2^n \to \mathbb{F}_2^n$. Assume that all the T_i have rank $n - 1$. We define 2^n subspaces U_i, $i = 0, \ldots, 2^n - 1$, of dimension n as follows:

$$U_i := \{(x, T_i(x)) \ : \ x \in \mathbb{F}_2^n\},$$
$$U_0 := \{(x, 0) \ : \ x \in \mathbb{F}_2^n\}.$$

These subspaces of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ form a dimensional dual hyperoval. The ambient space is $\mathbb{F}_2^{2n}$ or $\mathbb{F}_2^{2n-1}$. We note that if $n = 1$, the ambient space is just $\mathbb{F}_2^1$.

Motivated by the analogy to translation planes, we consider the following types of linear mappings T_i: We assume that the index set can be taken as the set of nonzero elements in $\mathbb{F}_2^n$, and we take T_0 to be the zero mapping indexed by $0 \in \mathbb{F}_2^n$. We assume that $T_{v+w} = T_v + T_w$ holds for all $v, w \in \mathbb{F}_2^n$. In other words, the set of linear transformations itself have the structure of an $\mathbb{F}_2$-vector space. In the situation of projective planes, we call such a structure a semifield and the plane a semi-field plane. Therefore, we call these semi-biplanes of **semifield type**.

Example 2. We consider the additive group of the finite field $\mathbb{F}_{2^n}$ as our vector space $\mathbb{F}_2^n$. The set of linear mappings

$$\begin{aligned} T_v : \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n} \\ x &\mapsto x^2 v + v^2 x \end{aligned}$$

has the property $T_{v+w} = T_v + T_w$. Moreover, the rank of T_v is $n-1$ since $T_v(x) = 0$ is a quadratic equation. We have $U_v \cap U_w = \{0, x\}$, where $T_v(x) = T_w(x)$, equivalently $T_{v+w}(x) = 0$, $x \neq 0$. If $T_v(x) = T_w(x) = T_u(x)$ for different u, v, w, then (due to the symmetry $T_v(x) = T_x(v)$) we also have $T_x(v) = T_x(w) = T_x(u)$. This is possible only if $v + w = u$, otherwise $v + w$ and u generate a 2-dimensional subspace in the kernel of T_x.

Before we state our main theorem, let us briefly recall the description of incidence structures (designs) using difference sets. We refer to [3] for an excellent encyclopedic book on designs. To this end, let Γ be an incidence structure consisting of v points and v blocks. Assume that Γ admits an automorphism group G acting regularly on points and blocks: By regular action on a set S we mean that for two arbitrary elements $s, t \in S$, there is precisely one group element g mapping s to t, denoted by s^g. Obviously, we must have $|G| = v$. We choose a base point p_0 and a base block B_0. A point p may be identified with the group element g mapping p_0 to p. Let $p_1, \ldots, p_k$ be the points incident with B_0. Then we may identify B_0 with the set D of group elements

corresponding to the p_i. What are the blocks through arbitrary points p_0^g and p_0^h? These are the blocks B_0^k such that $d + k = g$ and $d' + k = h$ for suitable $d, d' \in D$, i.e. $d' - d = h - g$. Therefore, the number of blocks through p_0^g and p_0^h is the number of ways to write $h - g$ as a difference with elements from D. This concept goes back to Singer [4], therefore the regular group is sometimes called a **Singer group**. The sets corresponding to base blocks are called **difference sets**. We refer the reader to [3] for a modern treatment of difference sets.

We may recover the incidence structure Γ easily from its difference set: The group elements in G are the points of an incidence structure, the translates $D + g := \{d + g : g \in G\}$ the blocks. This incidence structure is isomorphic to the one that has been used to construct the difference set D in the Singer group G.

Sometimes it is easy to construct a "difference set" (without using the incidence structure) and then use the difference set to construct the design. The "difference properties" directly translate into a property about the numbers of blocks through two points.

The "classical" difference sets D in G are those where every non-zero element in G has the same number λ of difference representations $d - d' = g$ with $d, d' \in D$. We say that these difference sets have parameters $(v, k, \lambda$, where $v = |G|$ and $k = |D|$. A difference set corresponding to a semi-biplane is a subset D of G such that every non-zero g has 0 or 2 such difference representations. As far as I know, there is no systematic investigation of possible difference representations of semi-biplanes. This note is a first step in this direction.

A large class of semi-biplanes can be constructed from relative difference sets: A relative (m, n, k, λ) difference set in a group G relative to a subgroup N is a k-subset of G such that every element in $G \setminus N$ has exactly λ representations as a difference with elements from R, and no non-zero element in N has such a representation. Here mn is the size of G, and $|N| = n$. Constructions of $(m, m, m, 1)$ relative difference sets are well known if m is a prime power, and via "projections" one may construct $(m, n, m, m/n)$-RDS's. If $m/n = 2$, we obtain semi-biplanes. We do not want to go into details here, but refer to [5–7].

In the next theorem we show that dimensional dual hyperovals of semifield type give rise to semi-biplanes that admit many (not necessarily abelian) Singer groups. We emphasize that the construction is quite similar to those presented in [7], which goes back to Hughes [8], see also [9].

Theorem . *Let U_v ($v \in \mathbb{F}_2^{2n}$) be a dimensional dual hyperoval in $\mathbb{F}_2^{2n}$ such that $U_v := \{(x, T_v(x)) : x \in \mathbb{F}_2^n\}$ and $T_v + T_w = T_{v+w}$ for all $v, w \in \mathbb{F}_2^n$. Moreover, let T_0 be the zero linear mapping, and all the other linear mappings T_v with $v \neq 0$ have rank $n - 1$. Then the corresponding semi-biplane has an automorphism group of order at least 2^{3n}, which is the semidirect product of an elementary abelian group of order 2^{2n} and an elementary abelian group of order 2^n. This group contains a subgroup acting regular on points and lines of the corresponding semi-biplane. In particular, there is a group H of size 2^{2n} and a subset D of size 2^n such that the list of differences $d - d'$, $d, d' \in D$, cover every non-zero element in H precisely 0 or 2 times. This group H contains an elementary abelian normal subgroup N of size 2^n. No non-zero element in N has a difference representation with elements from D.*

Proof. The translations

$$\begin{aligned} \tau_{u,v} : \mathbb{F}_2^n \times \mathbb{F}_2^n &\to \quad \mathbb{F}_2^n \times \mathbb{F}_2^n \\ (x,y) &\mapsto (x+u, y+v) \end{aligned}$$

form a subgroup of order 2^{2n}. The mappings

$$\begin{aligned} \sigma_m : \mathbb{F}_2^n \times \mathbb{F}_2^n &\to \quad \mathbb{F}_2^n \times \mathbb{F}_2^n \\ (x,y) &\mapsto (x, y+T_m(x)) \end{aligned}$$

are permutations on the point set of the semi-biplane, and they preserve incidence: It is obvious that σ_m is injective, hence bijective. Now assume that $(x,y) \in U_v + (a,b)$, i.e. $y = T_v(x+a)+b$. Note that $\sigma_m(x,y) = (x, y+T_m(x))$. Since $y + T_m(x) = T_v(x+a)+b+T_m(x) = T_{v+m}(x+a)+T_m(a)+b$, we have $\sigma_m(x,y) \in U_{v+m}+(a, T_m(a)+b)$.

Obviously, the σ_m form a group of order 2^n disjoint from the translation subgroup, and the translations from a normal subgroup in the group generated by the σ_m and the translations. This gives us the group G of order 2^{3n} acting on the semi-biplane.

Now we may identify a regular subgroup H in G. We consider the mappings

$$\begin{aligned} \delta_{m,v} : \mathbb{F}_2^n \times \mathbb{F}_2^n &\to \quad \mathbb{F}_2^n \times \mathbb{F}_2^n \\ (x,y) &\mapsto (x+m, y+T_m(x)+v). \end{aligned}$$

These mappings form a group of order 2^{2n}:

$$\delta_{m,v} \circ \delta_{n,u}(x,y) = (x+n+m, y+T_n(x)+u+T_m(x)+T_m(n)+v) = \delta_{n+m,u+v+T_m(n)}.$$

The stabilizer of $(0,0)$ is $\delta_{0,0}$. This shows that the group acts regular on points. Since in the semi-biplane any two points are joined by 0 or 2 lines, the set of nonzero differences formed by elements of D covers every group element 0 or 2 times. Moreover, no element in the subgroup $\{\delta_{0,v} : v \in \mathbb{F}_2^n\}$ is covered by a difference.

□

Remark 1. The group H is abelian if and only if $T_v(w) = T_w(v)$ for all $v, w \in \mathbb{F}_2^n$. Every element has order 2 provided that $T_v(v) = 0$ for all $v \in \mathbb{F}_2^n$ (in which case the group H is obviously abelian). It is not clear whether $T_v(v) = 0$ has to be true for all v in order that H is abelian.

Remark 2. The subgroup $\{\delta_{0,v} : v \in \mathbb{F}_2^n\}$ is a normal subgroup of G.

Remark 3. If the ambient space is $\mathbb{F}_2^n \times U$ for some subspace $U < \mathbb{F}_2^n$ of dimension $n-1$, almost the same construction as in our theorem gives a subset $D \subset \langle\{\delta_{m,v} : m \in \mathbb{F}_2^n, v \in U\}\rangle$ $(:= H)$ in a smaller group of size only 2^{2n-1}. The size of D is, as before, 2^n. Counting the differences one immediately sees that now every element in $H \setminus \{\delta_{0,v} : v \in U\}$ can be expressed in precisely two ways as a difference with elements from D, hence D is a relative $(2^n, 2^{n-1}, 2^n, 2)$ difference set with "forbidden subgroup" $\{\delta_{0,v} : v \in U\}$.

Remark 4. There are many possible ways to index the subspaces U_v by vectors from V such that $T_{v+w} = T_v + T_w$. Therefore, we may construct a difference set type description of the semi-biplane in many different ways, even in non-isomorphic groups!

Example 3. An example for the situation described in Remark 3 is contained in [10]: The linear mappings

$$\begin{aligned} T_v : \mathbb{F}_{2^n} &\to \mathbb{F}_{2^n} \\ x &\mapsto v^{2^m} x + x^{2^h} v \end{aligned}$$

give rise to a semi-biplane of semifield type if $m, h < n$ and m, h relatively prime to n. If $m + h = n$, the ambient space is $\{(x, y) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \ : \ \text{trace}(y) = 0\}$, otherwise the ambient space has dimension $2n$. One may view this example as an $\mathbb{F}_2$-analogue of Albert semifields, see [11], for instance.

Quadratic APN mappings give rise to semi-biplanes of semifield type: We call a mapping $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ **almost perfect nonlinear** (for short APN) if $F(x + a) + F(x) = b$ has 0 or 2 solutions for all $a \neq 0$ and all b. We say that F is quadratic if $x \mapsto F(x + a) + F(x) + F(a) + F(0)$ is linear for all v. Then the mappings

$$\begin{aligned} T_v : \mathbb{F}_2^n &\to \mathbb{F}_2^n \\ x &\mapsto F(x + v) + F(x) + F(v) + F(0) \end{aligned}$$

are linear with 1-dimensional kernel, and they form a dimensional dual hyperoval, as explained before. A nice characterization of hyperovals which can be described by such APN mappings has been given by Edel [12]. For background on APN functions we refer to [13].

Example 4. The "classical" examples of APN functions are the power mappings x^{2^i+1} on $\mathbb{F}_{2^n}$, where $\gcd(i, n) = 1$. The linear mappings are defined by

$$T_v(w) = v^{2^i} w + w^{2^i} v$$

We note that our main theorem shows that we may easily transform a description of the semifield type semi-biplane using an abelian regular group into a non-abelian one. The group is abelian if and only if $T_v(w) = T_w(v)$. We may easily destroy this property by the application of a linear mapping φ to the v's: The mappings $T_{\varphi(v)}$ still define a semi-biplane, however the corresponding Singer group G which acts regular on points and lines is not abelian any more.

From a geometric point of view the interesting objects are the semi-biplanes or, if we move to the more special cases, the translation semi-biplanes described by dimensional dual hyperovals, or those where the corresponding linear mappings form a vector space, i.e. semi-biplanes of semifield type. In the latter case, the interesting algebraic object is the group of order 2^{3n}, which contains many point-line regular automorphism groups. Some of them are, in my opinion incidentally, elementary abelian, so they give rise to APN mappings.

It may be possible (this is speculation) and even easier to construct many semifield type semi-biplanes using the non-abelian description. Some of these non-abelian examples may turn out to contain a hidden elementary abelian Singer group, which then gives rise to an APN function (perhaps an interesting one).

References

1. Göloğlu, F., Pott, A.: Almost perfect nonlinear functions: A possible geometric approach. In Nikova, S., Preneel, B., Storme, L., Thas, J., eds.: Coding Theory and Cryptography II, Koninklijke Vlaamse Academie van België voor Wetenschappen en Kunsten (2007) 75–100
2. Yoshiara, S.: Dimensional dual arcs—a survey. In: Finite geometries, groups, and computation. Walter de Gruyter GmbH & Co. KG, Berlin (2006) 247–266
3. Beth, T., Jungnickel, D., Lenz, H.: Design Theory. 2 edn. Cambridge University Press, Cambridge (1999)
4. Singer, J.: A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. **43**(3) (1938) 377–385
5. Pott, A.: Finite Geometry and Character Theory. Volume 1601 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, Heidelberg (1995)
6. Pott, A.: A survey on relative difference sets. In Arasu, K.T., Dillon, J., Harada, K., Sehgal, S., Solomon, R., eds.: Groups, Difference Sets, and the Monster. Proceedings of a Special Research Quarter at the Ohio State University, Spring 1993, Berlin, Walter de Gruyter (1996) 195–232
7. Jungnickel, D.: On automorphism groups of divisible designs. Canad. J. Math. **34**(2) (1982) 257–297
8. Hughes, D.R.: Partial difference sets. Amer. J. Math. **78** (1956) 650–674
9. Ghinelli, D., Jungnickel, D.: Finite projective planes with a large abelian group. In: Surveys in combinatorics, 2003 (Bangor). Volume 307 of London Math. Soc. Lecture Note Ser., Cambridge, Cambridge Univ. Press (2003) 175–237
10. Yoshiara, S.: A family of d-dimensional dual hyperovals in $\mathrm{PG}(2d+1,2)$. European J. Combin. **20**(6) (1999) 589–603
11. Kantor, W.M.: Commutative semifields and symplectic spreads. J. Algebra **270**(1) (2003) 96–114
12. Edel, Y.: On quadratic APN functions and dimensional dual hyperovals. Des., Codes, Cryptogr. **57**(1) (2010) 35–44
13. Carlet, C.: Vectorial boolean functions for cryptography. In Crama, Y., Hammer, P., eds.: Boolean Methods and Models. Cambridge University Press (to appear) http://www-roc.inria.fr/secret/Claude.Carlet/chap-vectorial-fcts.pdf.

The convergence of $\psi(s)$ (preliminary report)

By Koichiro Harada

In the papers of Sin and Thompson [1,2], a Dirichlet series denoted by $\psi(s)$ is introduced. The series $\psi(s)$ emerges naturally from a representation ρ of $SL(2,\mathbb{Z})$ on an infinite dimensional vector space $D[[s]]$ over $\mathbb{C}$ consisting of (formal) Dirichlet series with a (formal) variable s. The details of their investigation may best be obtained from [1]. Here in this note, we mention only the following. $D[[s]] \cong \mathbb{C}^\infty$ is a commutative ring under the product

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} \cdot \sum_{n=1}^{\infty} \frac{b_n}{n^s} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

where $c_n = \sum_{ij=n} a_i b_j$. The ring $D[[s]]$ possesses an identity

$$1 = \frac{1}{1^s} = (1,0,0,\ldots,).$$

Here our basis of $D[[s]]$ is an obvious set $\{\frac{1}{1^s}, \frac{1}{2^s}, \ldots, \frac{1}{n^s}, \ldots\}$. The group $SL(2,\mathbb{Z})$ is generated by two elements S and T where

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

By the explicit construction of the representation ρ in [1], we have

$$\rho(T) = D = (d_{ij}), \quad d_{ij} = 1 \text{ if } i|j \text{ and } d_{ij} = 0 \text{ otherwise.}$$

This $\infty \times \infty$ matrix D is called the divisor matrix in [1]. The matrices of $\rho(SL(2,\mathbb{Z}))$ act on the left on the vector space $D[[s]]$ viewed as the

space of row vectors $\mathbb{C}^\infty$. Considering the action of $\rho(T) = D$ on the identity $\mathbf{1}$ in particular, we obtain the Riemann zeta function:

$$\zeta(s) = \mathbf{1} \cdot \rho(T) = \mathbf{1} \cdot D = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

since the first row of the matrix D is $(1, 1, 1, \dots,)$. The Dirichlet series $\psi(s)$ is likewise obtained by:

$$\psi(s) = \mathbf{1} \cdot \rho(-S).$$

As for the convergence of the series $\psi(s)$, it is mentioned in [1] only that $\psi(s)$ converges in a half plane of the complex plane $\mathbb{C}$ with a sufficiently large real part.

In this note, we shall show that the series $\psi(s)$ converges absolutely in $P = \{s \in \mathbb{C} \mid \Re(s) > 4.3571\}$.

Let us first recall a few facts about $\psi(s)$. Write

$$\psi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Here the coefficient a_n is defined as follows:

$$a_n = \alpha_1(n) + \sum_{l \geq 4} (-1)^l \alpha_{l-1}(n) \sum_{k=2}^{[\frac{l}{2}]} b_k \binom{l-k-2}{k-2}.$$

The relevant quantities are define below. Define firstly:

$$\alpha_k(n) = |A_k(n)|$$

where

$$A_k(n) = \{(n_1, n_2, \dots, n_k) \in (\mathbb{N} \backslash \{1\})^k | n_1 n_2 \cdots n_k = n\}.$$

Obviously then $\alpha_k(n) = 0$ if $2^k > n$, equivalently if $\alpha_k(n) \neq 0$ then $k \leq [\log_2 n]$ where $[\cdot]$ is the Gaussian symbol. Therefore, the first summation notation in the expression of the coefficient a_n may be written

$$\sum_{l \geq 4} = \sum_{l=4}^{1+[\log_2 n]} .$$

We note that the value of a_n depends only on the factorization of n into the product of powers of primes. Hence, if $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is the factorization, then a_n is a function of only on powers $e_1, e_2, \ldots, e_r$ but not on primes $p_1, p_2, \ldots, p_r$. We also note that $\alpha_1(1) = 0$ and $\alpha_1(n) = 1$ if $n > 1$.

Secondly let

$$b_0 = b_1 = 1, \quad b_n = - \sum_{i,j \geq 1, i+j=n} b_i b_j, n \geq 2.$$

It can then be shown, for $n > 1$:

$$b_n = \frac{(-1)^{n-1}}{n} \binom{2n-2}{n-1}.$$

Note that $C_n = \frac{1}{n+1}\binom{2n}{n}$ is the so-called Catalan number. Listed below are values of a_n for $1 \leq n \leq 200$ (computation done by Naoki Chigira. He actually computed up to $n = 100,000$.) Observe that the values of a_n are not 'large' as compared with n.

0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, −2, 1, 1, 1, −1, 1, −2, 1, −2,
1, 1, 1, −4, 1, 1, 0, −2, 1, −5, 1, 0, 1, 1, 1, −5, 1, 1, 1, −4,
1, −5, 1, −2, −2, 1, 1, 4, 1, −2, 1, −2, 1, −4, 1, −4, 1, 1, 1, −8,
1, 1, −2, 3, 1, −5, 1, −2, 1, −5, 1, 12, 1, 1, −2, −2, 1, −5, 1, 4,
−1, 1, 1, −8, 1, 1, 1, −4, 1, −8, 1, −2, 1, 1, 1, 18, 1, −2, −2, −5,

$1, -5, 1, -4, -5, 1, 1, 12, 1, -5, 1, 4, 1, -5, 1, -2, -2, 1, 1, 28,$

$1, 1, 1, -2, 0, -8, 1, 3, 1, -5, 1, -8, 1, 1, -4, -4, 1, -5, 1, -8,$

$1, 1, 1, 39, 1, 1, -2, -2, 1, -8, 1, -4, -2, -5, 1, -8, 1, 1, 1, 18,$

$1, 4, 1, -2, -5, 1, 1, 28, 1, -5, -2, -2, 1, -5, -2, 4, 1, 1, 1, 46,$

$1, -5, 1, -4, 1, -5, 1, -2, -4, -5, 1, 3, 1, 1, -5, -5, 1, -8, 1, 12.$

Let us first deduce the formula for b_n mentioned above (proof taken from [1].) As defined above, $\{b_n \mid n \geq 0\}$ is determined recursively by

$$b_0 = b_1 = 1, b_n + \sum_{i,j \geq 1,\ i+j=n} b_i b_j = 0 \quad \text{for all } n \geq 2.$$

Let $\mathbb{C}[[t]]$ be the ring of formal power series and let $g(t) \in \mathbb{C}[[t]]$ be defined by

$$1 + g(t) = \sum_{k=0}^{\infty} b_k t^k.$$

We compute:

$$g(t)^2 = \left(\sum_{k=1}^{\infty} b_k t^k\right)^2 = t - \sum_{k=1}^{\infty} b_k t^k = t - g(t).$$

Therefore,

$$g(t)^2 + g(t) - t = 0$$

and, noting $g(0) = 0$,

$$g(t) = \frac{-1 + \sqrt{1 + 4t}}{2}$$

where

$$\sqrt{1 + 4t} = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} (4t)^k = 1 + 2t + \sum_{k=2}^{\infty} \binom{\frac{1}{2}}{k} (4t)^k.$$

Now, we have

$$\binom{\frac{1}{2}}{k} 4^k = \frac{(\frac{1}{2})(\frac{1}{2} - 1)(\frac{1}{2} - 2) \cdots (\frac{1}{2} - k + 1)}{k(k-1)(k-2) \cdots 2 \cdot 1} 4^k = \frac{2(-1)^{k-1}}{k} \binom{2k-2}{k-1} \quad \text{if } k \geq 2.$$

Therefore,

$$g(t) = -1 + 1 + t + \sum_{k=2}^{\infty} b_k t^k = t + \sum_{k=2}^{\infty} \frac{(-1)^{k-1}}{k} \binom{2k-2}{k-1} t^k$$

Hence the formula. (We also compute that $\lim_{k\to\infty} \frac{|b_{k+1}|}{|b_k|} = \frac{1}{4}$ and so the power series $g(t)$ actually converges if $t < \frac{1}{4}$.)

§2 Absolute Convergence of ψ

We next attempt to obtain perhaps a very crude estimate of the abscissa of absolute convergence of $\psi(s)$. Let us recall

$$\psi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

with

$$a_n = 1 + \sum_{l=4}^{1+[\log_2 n]} (-1)^l \alpha_{l-1}(n) \sum_{k=2}^{[\frac{l}{2}]} b_k \binom{l-k-2}{k-2}.$$

Using the value of b_k given earlier, we have

$$|a_n| \leq 1 + \sum_{l=4}^{1+[\log_2 n]} \alpha_{l-1}(n) \sum_{k=2}^{[\frac{l}{2}]} \frac{1}{k} \binom{2k-2}{k-1} \binom{l-k-2}{k-2}.$$

Theorem. If $|a_n| = O(n^r)$ for some constant r, then the Dirichlet series $f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges absolutely on the half plane $\{s \in \mathbb{C} \mid \Re(s) > r + 1\}$.

Theorem ([1]). There exists a constant $1 < c < 2$ such that $|\alpha_k(m)| \leq m^c$.

Proof. Induct on k. We have

$$\left(\frac{1}{2^s} + \frac{1}{3^s} + \cdots\right)^k = \sum_{m=2}^{\infty} \frac{\alpha_k(m)}{m^s}$$

Therefore

$$\alpha_k(m) = \sum_{d|m} \alpha(m) = \sum_{d|m} \alpha(\frac{m}{d}), \quad d \neq 1, m.$$

By induction on k, we compute

$$\alpha_k(m) \leq m^c \sum_{1 \neq d|m} \frac{1}{d^c} \leq m^c(\zeta(c) - 1).$$

If we choose c so that $\zeta(c) = 2$, then the proof completes. Since $\zeta(2) = \pi^2/6 = 1.645...$ and so we may choose $1 < c < 2$.

We next consider the second summation of the expression of a_n. We need to estimate the growth of

$$\frac{1}{k}\binom{2k-2}{k-1}\binom{l-k-2}{k-2} = \frac{(2k-2)!}{k!(k-1)!} \cdot \frac{(l-k-2)!}{(k-2)!(l-2k)!}.$$

The main tool is the following asymptotic formula due to Stirling.

$$n! = n(n-1)(n-2)\cdots 2 \cdot 1 \sim \sqrt{2\pi n} \cdot n^n e^{-n}.$$

We do not need it here but the following expansion is also known:

$$\frac{n!}{\sqrt{2\pi n} \cdot n^n e^{-n}} = 1 + \frac{1}{12}\frac{1}{n} + \frac{1}{288}\frac{1}{n^2} - \frac{139}{51840}\frac{1}{n^3} + \cdots.$$

We here use the following estimate (see Goursat [3, p.291]):

$$n! = \sqrt{2n} \cdot n^n e^{-n} \left\{ \sqrt{\pi} + \frac{\omega}{\sqrt{2n}} \right\},$$

for all $n > 0$ where $-1 < \omega < 1$.

In particular, for all $n > 0$

$$1.79\sqrt{n} \cdot n^n e^{-n} \leq n! \leq 3.23\sqrt{n} \cdot n^n e^{-n},$$

Now, we conclude from the estimate given above,

$$\frac{1}{k}\frac{(2k-2)!}{(k-1)!^2}\cdot\frac{(l-k-2)!}{(k-2)!(l-2k)!} = O\left(\frac{1}{k}\sqrt{\frac{l-k-2}{(k-1)(k-2)(l-2k)}}\cdot\frac{2^{2k}(l-k-2)^{l-k-2}}{(k-2)^{k-2}(l-2k)^{l-2k}}\right),$$

where $2 \le k \le \left[\frac{l}{2}\right]$.

Let us first evaluate

$$C_k = \frac{2^{2k}(l-k-2)^{l-k-2}}{(k-2)^{k-2}(l-2k)^{l-2k}}.$$

Viewing k as a real value and differentiating $\log C_k$ with respect to k, we obtain

$$(\log C_k)' = 2\log 2 - \log(l-k-2) - 1 - \log(k-2) - 1 + 2\log(l-2k) + 2.$$

Therefore, $(\log C_k)' = 0$ implies $4(l-2k)^2 = (l-k-2)(k-2)$ and so $17k^2 - 17kl + 4l^2 + 2l - 4 = 0$. Solving for k, we obtain

$$k = \frac{17l \pm (l-4)\sqrt{17}}{34}.$$

Since $2 \le k \le \left[\frac{l}{2}\right]$, C_k takes on the extremal values either at the end points or at

$$k_0 = \frac{(17-\sqrt{17})l + 4\sqrt{17}}{34} \sim 0.3787l + 0.4851.$$

By taking the second derivative of C_k, we see that C_k is an increasing function from $k = 2$ to $k = k_0$. Therefore it takes on the unique local maximal value at k_0 where $2 \le k \le \left[\frac{l}{2}\right]$. Note, however, that if $l = 5, 7$, then k_0 does not fall in this allowed range of k. But we can still use C_{k_0} for the cases $l = 5, 7$ also as an upper bound.

We compute

$$C_{k_0} = 2^{2\alpha l + 2\beta}\left(\frac{1-\alpha-\frac{\beta+2}{l}}{\alpha+\frac{\beta-2}{l}}\right)^{\alpha l+\beta-2}\cdot\left(\frac{1-\alpha-\frac{\beta+2}{l}}{1-2\alpha-\frac{2\beta}{l}}\right)^{l-2\alpha l-2\beta},$$

where $\alpha = 0.3787$ and $\beta = 0.4851$. Noting

$$\lim_{x\to\infty}\left(1+\frac{A}{x}\right)^{x} = e^{A},$$

we obtain

$$C_{k_0} = O\left(4^{\alpha l}\cdot\left(\frac{1-\alpha}{\alpha}\right)^{\alpha l+\beta-2}\cdot\left(\frac{1-\alpha}{1-2\alpha}\right)^{l-2\alpha l-2\beta}\right)$$

$$= O\left(4^{\alpha l}\cdot\left(\frac{1-\alpha}{\alpha}\right)^{\alpha l}\cdot\left(\frac{1-\alpha}{1-2\alpha}\right)^{(1-2\alpha)l}\right).$$

Replacing α by 0.3787 we obtain

$$C_{k_0} = O(2.5615^{l})$$

$$= O(2^{1.3570l}).$$

Next let us evaluate

$$D_k = \frac{1}{k}\sqrt{\frac{l-k-2}{(k-1)(k-2)(l-2k)}}.$$

Note that $k-1$ and $k-2$ comes from $(k-1)!$ and $(k-2)!$ respectively, and so we should understand those values to be 1 if $k=1$ or $k=2$. It is easy to see, $D_k = O\left(\sqrt{\frac{l-k-2}{l-2k}}\right)$ and $\frac{l-k-2}{l-2k}$ is an increasing function and so $D_k = O(\sqrt{l})$. Therefore,

$$C_k D_k = O(\sqrt{l}\cdot 2^{1.3570l})$$

Therefore,

$$|a_n| \le 1 + \sum_{l\ge 4}\alpha_{l-1}(n)\sum_{k=2}^{[\frac{l}{2}]}\frac{1}{k}\binom{2k-2}{k-1}\binom{l-k-2}{k-2}.$$

$$= O\Big(\sum_{l=4}^{1+\log_2 n} n^{c}\cdot\sum_{k=2}^{[\frac{l}{2}]}\cdot\sqrt{l}\cdot 2^{1.3570l}\Big)$$

$$= O(\log_2 n \cdot n^c \cdot \log_2 n \cdot \sqrt{\log_2 n} \cdot n^{1.3570})$$

$$= O(n^{c+1.3571}).$$

Here we used the facts that $\alpha_l(n) = 0$ if $l > 1 + [\log_2 n]$ and that $\log_2 n = O(n^\epsilon)$ for any $\epsilon > 0$.

Theorem. The Dirichlet series $\psi(s)$ converges on the half plane $\{s \in \mathbb{C} | \Re(s) > c + 2.3571\}$. Note $\zeta(c) = 2$ and $1 < c < 2$.

Corollary. The Dirichlet series $\psi(s)$ converges on the half plane $\{s \in \mathbb{C} | \Re(s) > 4.3571\}$.

Possible Improvements.

1. For the last corollary, $c = 2$ is in effect used. Use the precise value c with $\zeta(c) = 2$.
2. The relation $|\alpha_l(m)| \leq m^c$ is shown and used. But we need only $\alpha_l(m) = O(m^{c'})$ for some c'. Perhaps a smaller c' would work. Note that to show $|\alpha_l(m)| \leq m^c$, the assertion $\sum_{1 \neq d | m} \frac{1}{d^c} \leq \zeta(c) - 1$ is used, but a better estimate can be used.
3. In the calculation above, the local maximum of $C_k = \frac{2^{2k}(l-k-2)^{l-k-2}}{(k-2)^{k-2}(l-2k)^{l-2k}}$ is obtained and the range of k $(= \left[\frac{l}{2}\right] - 2)$ is multiplied. Instead one can get a better upper bound by integration. One can incorporate the contribution from D_k here also.
4. Even if the considerations mentioned above are carefully taken, the actual gain will be slim.

§3 Convergence of ψ

In the last section, we considered the absolute convergence of the Dirichlet series $\psi(s)$ by a very crude method. In this section the (conditional) convergence of $\psi(s)$ will be discussed. At the outset, however,

we will have to say that no good result for this purpose has yet to be obtained either by us, or by others as far as we know. As such we do not make in this section a precise distinction between absolute or conditional convergence. Numerical calculations appear to say that if $\sigma = \sigma_\psi$ is the abscissa of convergence, then $\sigma = 1$ or very close to it. But to show it, we will have to understand the coefficient a_n of $\psi(s)$ much better. As written before,

$$a_n = \alpha_1(n) + \sum_{l\geq 4}(-1)^l \alpha_{l-1}(n) \sum_{k=2}^{[\frac{l}{2}]} \frac{(-1)^{k-1}}{k} \binom{2k-2}{k-1} \binom{l-k-2}{k-2}.$$

As seen from this expression, each summand changes its sigh alternatively. As a result, an individual term may be a large number but the sum may not be so. In fact, a computer calculation (up to $n = 100,000$ by Chigira) shows that an equality $|a_n| = O(n^{1+\epsilon})$ for any small ϵ may be expected. In fact, we have $|a_n| < 6.2n$ if $n < 100,000$. If it is shown to be true for all n, then $\psi(s)$ would converge absolutely if $\Re(s) > 1$.

The following three theorems are copied almost verbatim from Apostol [5, Chapter 8, with $\lambda(n) = \log n$.]

Theorem. Assume that the series $\sum_{n=1}^{\infty} a_n n^{-s}$ converges for some s with positive real part, say for $s = s_0$ with $\sigma_0 = \Re(s_0) > 0$. Let

$$L = \limsup_{n\to\infty} \frac{\log|\sum_{k=1}^{n} a(k)|}{\log n}.$$

Then $L \leq \sigma_0$. Moreover, the series converges in the half plane $\sigma > L$, and the convergence is uniform on every compact subset of the half plane $\sigma > L$.

Theorem. Assume that the series $\sum_{n=1}^{\infty} a_n n^{-s}$ converges for some s with $\sigma > 0$ but diverges for all s with $\sigma < 0$. Then the number

$$L = \lim_{n\to\infty} \sup \frac{\log |\sum_{k=1}^{n} a(k)|}{\log n}.$$

is the abscissa of convergence of the series. In other words, the series converges for all s with $\sigma > L$ and diverges for all s with $\sigma < L$.

Theorem. Assume that the series $\sum_{n=1}^{\infty} a_n n^{-s}$ converges absolutely for some s with $\sigma > 0$ but diverges for all s with $\sigma < 0$. Then the number

$$\sigma_a = \lim_{n\to\infty} \sup \frac{\log \sum_{k=1}^{n} |a(k)|}{\log n}.$$

is the abscissa of absolute convergence of the series.

A supportive evidence for the assertion σ is 'close' to 1 is given below. In [1], it is shown that if $\mathbb{Z}(SL(2,\mathbb{Z}))$ denotes the group algebra of the group $SL(2,\mathbb{Z})$ over the ring of integers $\mathbb{Z}$, then the orbit of the identity 1 of the ring $D[[s]]$ under the action of $\mathbb{Z}(SL(2,\mathbb{Z}))$ is spanned by

$$\zeta(s)^m, \psi(s)\zeta(s)^n$$

where $m, n \in \mathbb{Z}$. That is to say, $1 \cdot \mathbb{Z}(SL(2,\mathbb{Z})) = \{\zeta(s)^m, \psi(s)\zeta(s)^n\}_{\mathbb{Z}}$, $m, n \in \mathbb{Z}$.

Therefore if the abscissa of absolute convergence of $f(s) = \psi(s)$, $\psi(s)\zeta(s)$, or $\psi(s)\zeta^{-1}(s)$ is shown to be (close to) 1, then every series in the orbit $1 \cdot \mathbb{Z}(SL(2,\mathbb{Z}))$ will have the same property. Write $f(s) = \sum_{i=1}^{\infty} b_n n^{-s}$. Put

$$B(n) = \sum_{i=1}^{n} b_i,$$

and

$$C(n) = \sum_{i=1}^{n} |b_i|$$

Define

$$M(n) = \max\left\{\frac{\log|B(d)|}{\log d}, 1 < d \le n\right\}$$

or

$$M(n) = \max\left\{\frac{\log C(d)}{\log d}, 1 < d \le n\right\}.$$

The following tables are computed by Naoki Chigira for $1 < n \le 1000$.

According to $f(s) = \psi(s)$, or $\psi(s)\zeta(s)$, or $\psi(s)\zeta^{-1}(s)$, the results are listed as TBP, TBPZ, TBPZI. On the other hand, if $C(n) = \sum_{i=1}^{n} |b_n|$ and $M(n) = \max\{\log C(n)/\log d, 1 < d \le n\}$, then they are listed as TCP, TCPZ, TCPZI.

Obviously $M(n)$ is an increasing function with respect to n. The printout shows the value of $M(n)$ and n when it actually increases.

TBP

(0.000000000000000000000000000000, [2])
(0.630929753571457437099527114343, [3])
(0.792481250360578090726869471974, [4])
(0.861353116140786101340213137528, [5])
(0.898244401703027173073232958087, [6])
(0.920782221161601790318727245176, [7])
(0.923723511772581956604318014905, [240])
(0.924173540732028622052480931150, [241])
(0.947972554146407325281239723079, [252])
(0.948247739084622471486949120722, [253])
(0.948520203905733807703778061984, [254])
(0.948666869150585810013302912609, [265])
(0.965035758547732550723631988332, [270])
(0.965201119339614978034881078819 3, [271])
(0.967738410969457588990050537300, [272])
(0.973380963577729283495181252159, [280])
(0.973499903439966615451715758137, [281])
(0.998973088688021980071075644138, [336])
(0.998977265685295842028973328555, [337])
(1.027398113715701819423632917 45, [360])
(1.047922845654974873119829391 08, [420])
(1.050294525602835492314695969 39, [540])
(1.053500559478606095992802063795, [544])
(1.062752974044160669450022340 64, [560])
(1.066314395723716800305611884 01, [630])

TBPZ

(0.000000000000000000000000000000, [2])
(0.630929753571457437099527114343, [3])
(1.000000000000000000000000000000, [4])
(1.000000000000000000000000000000, [5])
(1.160558421703624760610738415 40, [6])
(1.167358759736396346689801203 62, [9])
(1.204119982055924780854955578 90, [10])
(1.205041013843696655022879350 61, [840])

TBPZI

(0.000000000000000000000000000000, [2])
(0.630929753571457437099527114343, [3])
(0.682686194485985295134566359271, [5])
(0.683010746090858993946227916302, [21])
(0.710836104806327464960572141564, [22])
(0.727552779548046027016326804911, [27])
(0.791985402323490542401449025338, [28])
(0.849810062032815140390241857041, [30])
(0.861198595275138724740960762991, [42])
(0.870949181949880962040834454129, [44])
(0.893485406390003993241341415145 8, [45])
(0.896020564000534016040755519890, [46])
(0.915391813874107841854092803233, [180])
(0.916067452988075353581042264696, [181])
(0.949870201109991922800425434908, [252])
(0.958059171219887918233073488219, [264])
(0.978961386526596101583212814367, [270])
(0.979057586755965514339183365496, [271])
(0.984954608852080552879129908091, [272])
(1.000000000000000000000000000000, [280])
(1.000000000000000000000000000000, [281])
(1.032467981616757911574794238 14, [420])

TCP

(0.0000000000000000000000000000000, [2])
(0.6309297535714574370095271143 43, [3])
(0.7924812503605780907268604719 74, [4])
(0.8613531161467861013402131375 28, [5])
(0.8982444017039271730732329580 87, [6])
(0.9207822211616017903187272451 76, [7])
(0.9649840459813437508581130002 48, [12])
(0.9687936498860341635789003848 22, [13])
(0.9719187714029214025201015798 21, [14])
(0.9745230455997933509937922363 42, [15])
(0.9767226489021296323310145933 50, [16])
(0.9786021684729041215590459049 27, [17])
(1.0000000000000000000000000000000, [18])
(1.0000000000000000000000000000000, [19])
(1.0102865509130280545672402502 2, [20])
(1.0485047415985339971165808380 1, [24])
(1.0605016347207985023509632723 3, [30])
(1.0744041451525913801183165703 5, [36])
(1.0813538625251402249280418726, [40])
(1.0954270923770265040603426088 2, [42])
(1.0966003109320840025714278471 9, [45])
(1.1011259464518514275750301889, [48])
(1.1047222039054719031117827145 0, [54])
(1.1094454501785347720582151603 7, [56])
(1.1198294156714055858970510120 0, [60])
(1.1240855133171327948026158072 5, [66])
(1.1268076248941000808603716776 0, [70])
(1.1434950557587577320711532329, [72])
(1.1468324229318143880400644955 3, [84])
(1.1503041487961253848968341704, [90])
(1.1618975340164836209031065044 5, [96])
(1.1621412276488463325407790649 6, [100])
(1.1632278871105631085230672881 3, [102])
(1.1632693068258087989096638915 7, [104])
(1.1656631381927661219184466123 5, [105])
(1.1714316970661920333382337810, [108])
(1.1720094903086843701268701190 3, [110])
(1.1724507841946514044978877542 2, [114])
(1.1864610760472111905436070316 8, [120])
(1.2015002809236408843414900001 7, [144])
(1.2033130505624341818187118725, [160])
(1.2097038038144421270338326092, [168])
(1.2105902661094964337680110035 2, [180])
(1.2226869025825901364578320351, [216])
(1.2235474360882130288741130025 6, [224])
(1.2237663418281237617650924525 0, [225])
(1.2358194857189091169065285151 01, [240])
(1.2386570429309819655659122426, [252])
(1.2392066630855497145464280473 8, [264])
(1.2408810988191958612152591067, [270])
(1.2416934758737579126378449289 3, [280])
(1.2429512030109676816524186886 7, [288])
(1.2452201903588918735288204835 5, [300])
(1.2459748779454393534674684040 5, [324])
(1.2506503863162870936444012313 8, [336])
(1.2587505087120833306247468371, [360])
(1.2601781518057968178512313025 3, [384])
(1.2612957139564854057803851832, [396])
(1.2631935327881896216318289758 7, [400])
(1.2685070027944487052063790420 7, [420])
(1.2702488570001200314958198015 0, [432])
(1.2703517234669522283027777040, [450])
(1.2704901633032358914843119508 3, [468])
(1.2710000874349431197096739447 7, [480])
(1.2747713828822728284898676168, [504])
(1.2752985695047081729908153658 1, [528])
(1.2786359175784381366260720127 6, [540])
(1.2795832524336463938487041948 7, [560])
(1.2865603070906401378737261231 4, [576])
(1.2890827325470930459068598126 2, [600])
(1.2900583277666097826036791906 1, [624])
(1.2923148209559360415958168400 2, [630])
(1.2923425057012940095835077645 7, [640])
(1.2933631783081201412038100629 1, [648])
(1.2944377776571539942740230223 5, [660])
(1.2944599189600201080360453057 9, [672])
(1.2949558140535802777734328763, [684])
(1.2994000540171856172911089468 8, [720])
(1.2997457079622080584414435004 0, [780])
(1.3000233845358282842759507469 7, [784])
(1.3015244325697918210452416189 4, [792])
(1.3010748835832080396442975270 5, [816])
(1.3038813956028443552811468039 1, [840])
(1.3094091760552672275266545431 0, [864])
(1.3109075558619803555004080684 5, [900])
(1.3112890450197105704298032471 5, [924])
(1.3119167856115195834742058883 3, [936])
(1.3172153386693926490978051248, [960])

TCPZ

(0.0000000000000000000000000000000, [2])
(0.6309297535714574370095271143 43, [3])
(1.0000000000000000000000000000000, [4])
(1.0000000000000000000000000000000, [5])
(1.1605584217036247606107384154 0, [6])
(1.1673587597363963468980120302, [9])
(1.2041199826559247808549555789 0, [10])
(1.2105398728382053391980112739 5, [144])
(1.2106465017023081106977271501 1, [150])
(1.2148190542213700722458862491, [160])
(1.2268040759196423312120618618 7, [216])
(1.2273879035283820102800009586, [220])
(1.2291217514696212039789603355 2, [224])
(1.2293491422279894892846046806, [228])
(1.2429837450454477243034050006 0, [240])
(1.2484940378928878059143360651 0, [336])
(1.2627170311983050938804370666 8, [360])
(1.2644074016042389010243225416 6, [504])
(1.2667368965996600905189076713 0, [528])
(1.2733477025293721788789272274 1, [540])
(1.2737249106349375791545316579 3, [546])
(1.2757856905984293073388132191 0, [560])
(1.2815310983722036073425775788 7, [576])
(1.2846332302786025050106727627 8, [600])
(1.2848836827686041979360309082 0, [630])
(1.2848455225063898921497034660 7, [810])
(1.2863811043689599273501359787 1, [816])
(1.2923648058135203270524832250 4, [840])
(1.2986990798577227004104605078 1, [864])
(1.2987649670425873330250921726 1, [880])
(1.2987936627812142408548590139 3, [882])
(1.3019706743234792350922179679 3, [900])
(1.3021121682910461306680524561 4, [912])
(1.3036274854342714933632612023 1, [936])
(1.3077596223762563390830161451 12, [960])

TCPZI

(0.0000000000000000000000000000000, [2])
(0.6309297535714574370095271143 43, [3])
(0.6826061944859582951340360350271, [5])
(0.7737056144690831737404022700 36, [6])
(0.8270874753469161503037514830 45, [7])
(0.8616541669070520604845790479 83, [8])
(0.8671944789536635777986330231 00, [11])
(0.9640840459813437508581130002 48, [12])
(0.9687936498860341635789003848 22, [13])
(0.9719187714029214025201015798 21, [14])
(0.9745230455997933509037922363 42, [15])
(0.9767226489021296323310145933 59, [16])
(0.9786021684729041215590459049 27, [17])
(1.0187059748015355844936182320 8, [18])
(1.0466536825000300873397027930 6, [20])
(1.0695016347297085623650632723 3, [30])
(1.0755733068599781807537038350 7, [45])
(1.1011259464518514275725030188 9, [48])
(1.1026170838820670403937804843 1, [52])
(1.1039030894100103488756152506 3, [66])
(1.1052092850527055405049999610, [68])
(1.1106282583522486270083922149 9, [70])
(1.1417309153209075082230007260 4, [72])
(1.1438925161071844390497052003 5, [78])
(1.1524019428114125348906835203 2, [80])
(1.1623804303034334839110095133 3, [108])
(1.1632981558490931914002197962 18, [110])
(1.1676146348458023874681810653 2, [112])
(1.1683187579699024503692096878 3, [114])
(1.1920877510344138527999117950 4, [120])
(1.1961540390703937816841082746, [168])
(1.1972409955580621713124041752 82, [176])
(1.2143908082610822983805152030, [180])
(1.2188123802108083966077715301 1, [252])
(1.2227210011245733709974780076 6, [264])
(1.2273264403671113702302910708 3, [270])
(1.2275516014052543107619371649 1, [272])
(1.2276613367486309769149559173 5, [273])
(1.2311576005452000159513527036 4, [280])
(1.2415515702040245514711418830 1, [288])
(1.2439226701717350778200049740 7, [300])
(1.2447051673371200782833870521 3, [312])
(1.2458294033841508202560060055 4, [396])
(1.2462394488544122328757272356, [400])
(1.2481125847043802881582325848 0, [408])
(1.2549463260293813067915030851 7, [420])
(1.2632194826137388109897455275 8, [432])
(1.2639068767130090060105679484 74, [440])
(1.2657544854194651891629492642 6, [450])
(1.2665562522800630344617755632 31, [456])
(1.2674985007832890707284781955 9, [468])
(1.2750186889035501728315955010 2, [480])
(1.2753274002401981341043986181 9, [630])
(1.2756378160851612156003262820 6, [640])
(1.2798352177537116278743394286 9, [648])
(1.2818613116110583738889763233 6, [660])
(1.2856050235137885402966201255 7, [672])
(1.2856352320173081600533719032 3, [680])
(1.2867017915775831982008864075 5, [684])
(1.2873948974403051400516505352 5, [702])
(1.2874026440020438006452835292, [704])
(1.2991938020000954211380457817 3, [720])

We are aware that in calculating $\lim_{n\to\infty}\sup$, we should ignore the first finite terms but the tables above use only the first finite terms. Therefore, one can not really obtain any solid conclusions from those tables. We still believe that the abscissa of convergence of $\psi(s)$ is in the neighborhood of 1. In any event, however, it must be a very interesting problem to find the abscissa of convergence of ψ, absolute or conditional, by any mean.

References

[1] P. Sin and J. G. Thompson, The Divisor Matrix, Dirichlet Series and $SL(2,\mathbb{Z})$, arXiv:0712.0837v6 [math.NT] 18 Jul 2008. 30 pages.

[2] P. Sin and J. G. Thompson, The Divisor Matrix, Dirichlet Series and $SL(2,\mathbb{Z})$, II, arXiv:0803.1121v8 [math.NT] 12 Mar 2010. 11 pages.

[3] E. Goursat, A Course in Mathematical Analysis, Volume 1, Dover Publications, Inc., 1959.

[4] H. Rademacher, Topics in Analytic Number Theory, Springer, 1973.

[5] T. M. Apostol, Modular Functions and Dirichlet Series in Number Theory, Springer, 1976.

An orbifold VOA of free bosonic type and C_1-cofiniteness

Masahiko Miyamoto (Univ. of Tsukuba)

1 Introduction

A vertex operator algebra (shortly VOA) is an $\mathbb{N}$-graded vector space

$$V = V_0 \oplus V_1 \oplus V_2 \oplus \cdots$$

with infinitely many products $v*_n u \in V \quad \forall v, u \in V, n \in \mathbb{Z}$ satisfying several natural conditions. There are two streams in the past research of VOAs.

Research of specific VOA	**Research of general VOAs**
(Research of 2-dim. CFT)	$SL_2(\mathbb{Z})$-invariance of trace functions [Z]
Research of the Moonshine VOA	$SL_2(\mathbb{Z})$-invariance of orbifold type [DLM]
Research of W-algebras	Verlinde formula [H],[MS]
Research of Frame VOAs	
etc.	They assumed C_2-cofiniteness and that
The main purpose is a construction of	all modules are completely reducible.
new VOAs and to study their modules.	Namely, we need to assume the final purpose
(Classification of simple modules and	in the left column and so we can't use these
studies of their extensions.)	general theories for the left purposes.
In many cases, the aim is to prove that	
all modules are completely reducible.	Except for Zhu-algebra, we have no general
Research of interesting properties of	method for the purpose of the left column.
specific VOA.	

In the recent research of VOAs, we realize the significance of C_2-cofiniteness. Namely, if

$$C_2(V) := \langle v*_{-j} u \mid v, u \in V, -j \leq -2 \rangle$$

is large enough, in other words, if $\dim V/C_2(V) < \infty$, V has many good properties.
An important problem is:
For a lattice M with finite $G < \mathrm{Aut}(M)$, is $(V_M)^G$ C_2-cofinite?

Here V_M is a lattice VOA and $(V_M)^G$ denotes the fixed point subVOA.
This is an open question except very rare cases. Recently, I have proved it for $G \cong \mathbb{Z}/3\mathbb{Z}$.
The followings follow from this result.

(1) A $\mathbb{Z}/p\mathbb{Z}$-orbifold construction of the moonshine VOA $V^\natural$.
(2) A new series of nice VOAs.

The proof of C_2-cofiniteness is not easy. So we enlarge $C_2(V)$ to

$$C_1(V) = C_2(V) + \langle v_{-1}u \mid v, u \in \oplus_{m=1}^{\infty} V_m \rangle$$

and we want to show $\dim V/C_1(V) < \infty$. (C_1-cofinite).

We note that $V/C_2(V)$ has a good algebraic structure.
From the fundamental commutativity property (Commutativity) of VOA

$$(v *_n u *_m - u *_m v *_n)w = \sum_{i=0}^{\infty} \binom{n}{i} (v *_i u) *_{n+m-i} w,$$

$V/C_2(V)$ becomes a Poisson algebra with

commutative algebra	by $*_{-1}$
Lie algebra	by $*_0$

[Remark] $V/C_1(V)$ is a generator of $(V/C_2(V), \times_{-1})$.
Hence, C_1-cofinite and all elements in $V/C_1(V)$ are nilpotent $\Longrightarrow$ C_2-cofinite.

2 2-dim. Heisenberg algebra

To treat an action of cyclic group $< \sigma >$ of order $p \in \mathbb{N}$ preserving inner product, let

$$L = \mathbb{C}a + \mathbb{C}b \quad \text{with} \quad \langle a, a \rangle = \langle b, b \rangle = 0, \qquad \langle a, b \rangle = \langle b, a \rangle = 1$$

be a 2-dim. inner product space and we define an action of σ by

$$\sigma(a) = \xi a, \qquad \sigma(b) = \xi^{-1} b$$

where $\xi \in \mathbb{C}$ is a primitive root of the unity.

We introduce $a(n), b(n)$ for $n \in \mathbb{Z}$ and consider an ∞-dim. Lie algebra

$$\mathcal{H} := (\oplus_{n \in \mathbb{Z}} \mathbb{C}a(n)) \bigoplus (\oplus_{n \in \mathbb{Z}} \mathbb{C}b(n)) \bigoplus \mathbb{C}$$

$$[a(n), b(-n)] := a(n)b(-n) - b(-n)a(n) = n \quad \forall n \in \mathbb{Z}$$
$$\text{else} = 0 \qquad \text{i.e. the others are commutative together}$$

We introduce "weight" by $\mathrm{wt}(v(n)) = -n$.

3 Fock space and Operators

Set

$$a(z) := \sum a(n)z^{-n-1} \qquad b(z) := \sum b(n)z^{-n-1}$$

and

$$v^-(z) = \sum_{n<0} v(n)z^{-n-1} \quad \text{(nonnegative power of } z\text{)}$$
$$v^+(z) = \sum_{n\geq 0} v(n)z^{-n-1} \quad \text{(negative power of } z\text{)}$$

where $+$ denotes a dagger $\dagger$ to kill.

Let $U :=< a(n), b(n) \mid n \in \mathbb{Z} >$ be a universal enveloping algebra of $\mathcal{H}$. As a basis of U, we can take

$$u^1(n_1)\cdots u^k(n_k) \mid u^i \in \{a, b\}, n_1 \leq \ldots \leq n_k.$$

It is generated by two commutative subalgebras

$$U^+ := \langle u(n) \mid n \geq 0\rangle \qquad U^- := \langle u(n) \mid n < 0\rangle$$

The starting element of our desired space $M_2(1)$ on which $\mathcal{H}$ acts is a vacuum 1 (weight 0) is defined by

$$u(n)1 = 0 \qquad \forall n \geq 0$$

and $u(n)$ $n < 0$ acts on freely. Namely,

$$M_2(1) := U \otimes_{U^+} 1 \cong U^-1 \qquad \text{(as graded spaces)}$$

weight k	$\dim(M_2(1))_n$	basis of $(M_2(1))_k$
0	1	1
1	2	$a := a(-1)1, \quad b := b(-1)1$ (identify)
2	5	$a(-2)1, a(-1)a(-1)1, b(-2)1, b(-1)^2 1, a(-1)b(-1)1$
3	10	$a(-3)1, a(-2)a(-1)1, a(-1)^3 1, b(-3)1, b(-2)b(-1)1, b(-1)^3 1$
		$a(-2)b(-1)1, a(-1)^2 b(-1)1, a(-1)b(-2)1, a(-1)b(-1)b(-1)1$

The action of elements $v(n)$ in $\mathcal{H}$ on this space is given by

$$v(n)\cdot a(-n_1)\cdots a(-n_k)b(-m_1)\cdots b(-m_r)1 = v(n)a(-n_1)\cdots a(-n_k)b(-m_1)\cdots b(-m_r)1$$

then rewrite it by using the commutative relations. For example,

$$\begin{aligned} a(-3)a(-2)b(-3)a(2)b(-2)1 &= a(-3)a(-2)b(-3)b(-2)a(2)1 + a(-3)a(-2)b(-3)2 \times 1 \\ &= 0 + 2a(-3)a(-2)b(-3)1 \end{aligned}$$

We next introduce infinitely many products in $M_2(1)$:

$$Y(1, z) = 1 \qquad \text{(i.e. } 1_{-1} = 1, 1_m = 0 \forall m \neq -1\text{)}$$
$$Y(a(-1)1, z) = \sum a(n)z^{-n-1} = a(z)$$
$$Y(b(-1)1, z) = \sum b(n)z^{-n-1} = b(z)$$

Generally, for a base $v^1(-n_1-1)\cdots v^k(-n_k-1)\mathbf{1}$,

$$Y(v^1(-n_1-1)\cdots v^k(-n_k-1)\mathbf{1},z) =: (\frac{1}{n_1!}\frac{d^{n_1}v^1(z)}{dz^{n_1}})\cdots(\frac{1}{n_k!}\frac{d^{n_k}v^k(z)}{dz^{n_k}}) :$$

Here differential(higher-order differential) is given by

$$\frac{d}{dz}(\sum v(n)z^{-n-1}) = \sum(-n-1)v(n)z^{-n-2}$$

and $: * :$ denotes normal product which implies to shift annihilator operator $v^+(z)$ to the right side formally. In other words,

$$:(v^-(z)+v^+(z))u^1(z)\cdots u^k(z) := v^-(z) : u^1(z)\cdots u^k(z) : + : u^1(z)\cdots u^k(z) : v^+(z)$$

Fact 1 $(M_2(1),Y)$ *is a vertex operator algebra.*

4 Automorphism

Expanding

$$\sigma : a \to \xi a, \qquad \sigma : b \to \xi^{-1}b$$

to $M_2(1)$ by

$$\sigma(\mathbf{1}) = \mathbf{1}, \qquad \sigma a(n) = \xi a(n), \qquad \sigma b(n) = \xi^{-1}b(n),$$

σ becomes an automorphism of a VOA $M_2(1)$. Namely, it satisfies

$$Y(\sigma(v),z) = \sigma Y(v,z)\sigma^{-1}.$$

Then the fixed point subspace $M_2(1)^\sigma$ becomes also a VOA.

Conjecture $M_2(1)^\sigma$ is C_1-cofinite.

Known results: For $p=2$ [G. Yamskulna 04]. For $p=3$, [M 10]
If p is even (or a multiple of 3), then we can apply it to the research of the monster simple group and the moonshine VOA.

5 Case $p=3$

$u = a(-i_1)\cdots a(-i_h)b(-j_1)\cdots b(-j_k)\mathbf{1} \in M_2(1)^\sigma \Leftrightarrow h-k \equiv 0 \pmod 3$.
For example,

$$a(-n)b(-m)\mathbf{1}, a(-n_1)a(-n_2)a(-n_3)\mathbf{1}, b(-n_1)b(-n_2)b(-n_3)\mathbf{1} \in M_2(1)^\sigma$$

We note that $\omega = a(-1)b = b(-1)a$ is the Virasoro element ω.

Weight function : $(\omega_1 u) = \mathrm{wt}(u)u$

Differential : $(\omega_0 u)_m = -mu_{m-1}$

We also have:

$$(\omega_0 v) = \omega_0 v_{-1}\mathbf{1} = v_{-2}\mathbf{1} \in C_2(V)$$

Our aim is to show the following theorem:

Theorem 1 *Set*

$\mathcal{S}_1 = \{\mathbf{1}, a(-i_1)a(-i_2)a(-1)\mathbf{1}, b(-i_1)b(-i_2)b(-1)\mathbf{1}, a(-i_3)b(-1)\mathbf{1}, \mathbf{1} \mid i_1, i_2 \leq 5, i_3 \leq 4\}$

Then $M_2(1)^\sigma = C_1(M_2(1)^\sigma) + <\mathcal{S}_1>_{\mathbb{C}}$. *In particular,* $M_2(1)^\sigma$ *is* C_1*-cofinite.*

5.1 Outline of the proof

As an important property of VOA, it satisfies Associativity

$$(v_m u)_k = \sum_{i=0}^{\infty} \binom{m}{i} (-1)^i \{v_{m-i}u_{k+i} - (-1)^m u_{k+m-i}v_i\}$$

We will use it frequently. For example,

$$(a(m)b(-1)\mathbf{1})_k = \sum_{i=0}^{\infty} \binom{m}{i} (-1)^i \{a(m-i)b(k+i) - (-1)^m b(k+m-i)a(i)\}$$

We note that for a VOA V, $C_1(V)$ is invariant under 0-th product:

$$v_0(u_{-1}w) = u_{-1}v_0 w + (v_0 u)_{-1}w$$
$$(u_{-1}w)_0 v = \sum u_{-1-i}w_i v + \sum w_{-1-i}u_i v$$

We first show

Lemma 2 *Set*

$$\mathcal{S} = < a(-n_1)b(-m_1)\mathbf{1}, a(-n_1)a(-n_2)a(-n_3)\mathbf{1}, b(-m_1)b(-m_2)b(-m_3)\mathbf{1} \mid n, m \in \mathbb{N} > .$$

Then $M_2(1)^\sigma = \mathcal{S} + C_1(M_2(1)^\sigma)$.

[Proof] Introduce an order

$$a(-n_1)\cdots a(-n_h)b(-m_1)\cdots b(-m_k)\mathbf{1} > a(-s_1)\cdots a(-s_p)b(-t_1)\cdots b(-t_q)\mathbf{1}$$

if $h > p$, or $h = p$ and $k > q$, or $h = p$, $k = q$ and dictionary order

Suppose the Lemma is false and let's choose a minimal base (w.r.t. the above order)

$$u = a(-n_1)\cdots a(-n_k)b(-m_1)\cdots b(-m_r)\mathbf{1} \notin \mathcal{S} + C_1(M_2(1)^\sigma)$$

Case 1: Assume $n_k, m_r \geq 1$ and set $u = a(-n_1)b(-m_1)u^*$. Since

$$(a(-n_1)b)_{-m_r} = a(-n_1)b(-m_r) + \sum_{i=1}^{\infty} \lambda_i a(-n_1 - i)b(-m_r + i) + \sum_{j=0}^{\infty} \mu_j b(-n_1 - m_r - j)a(j),$$

we have $C_1(M_2(1)^\sigma) \ni (a(-n_1)b)_{-m_r}u^* = u +$ elements less than u.

Case 2: Only a or b appears in u. Set $u = a(-n_1)a(-n_2)a(-n_3)u^*$. Since

$$C_1(M_2(1)^\sigma) \ni (a(-n_1)a(-n_2)a(-1)\mathbf{1})_{-n_3}u^*$$
$$= a(-n_1)a(-n_2)a(-n_3)u^* + \textstyle\sum_{i,j\in\mathbb{N},(i,j)\neq 0} \lambda_{i,j} a(-n_1 - i)a(-n_2 - j)a(-n_3 + i + j)u^*,$$

we have $u \equiv -\sum_{i,j\in\mathbb{N},(i,j)\neq 0} \lambda_{i,j} a(-n_1-i)a(-n_2-j)a(-n_3+i+j)u^* =$ elements less than u.

5.2 Calculation of $a(-r)a(-s)b(-n)b(-1)\mathbf{1}$

Set $\gamma(n) = a(-n+1)b(-1)\mathbf{1}$.

From $0 \equiv \omega_0(a(-n)b(-m)\mathbf{1}) = na(-n-1)b(-m)\mathbf{1} + ma(-n)b(-m-1)\mathbf{1}$, we have:

Lemma 3 $\quad a(-n)b(-m-1)\mathbf{1} \equiv \binom{-n}{m}\gamma(n+m+1) \pmod{\omega_0 V_L}$

We calculate $a(-r)a(-s)b(-n)b(-1)\mathbf{1}$ modulo $C_2(M_2(1)^\sigma)$ by two ways.

Proposition 4

$$a(-r)a(-m)b(-n)b(-1)\mathbf{1} \equiv \binom{-m}{n-1}\gamma(r+1)\gamma(m+n) - \frac{(-1)^{n-1}(r+m+n-1)!(m+n+r+1)}{(r-1)!(m-1)!(n-1)!(m+1)(r+n)}\gamma(t)$$

modulo $\omega_0 M_2(1)^\sigma$, *where* $t = r+m+n+1$. *In particular, by replacing* r *with* m, *we have*

$$\gamma(n+3) \equiv \frac{6}{(n-1)(n-2)(n+3)}\{\gamma(3)_{-1}\gamma(n) - (n-1)\gamma(2)_{-1}\gamma(n+1)\}$$

for $n \geq 3$ *and so* $\gamma(n) \in C_1(M_2(1)^\sigma)$ *for* $n \geq 6$.

[Proof] The assertion comes from the direct calculation:

$$\begin{aligned}
&\binom{-m}{n-1}\gamma(r+1)_{-1}\gamma(m+n) \equiv (a(-r)b)_{-1}a(-m)b(-n)\mathbf{1}\\
&\equiv \textstyle\sum_i \binom{-r}{i}(-1)^i\{a(-r-i)b(-1+i) - (-1)^{-r}b(-r-1-i)a(i)\}a(-m)b(-n)\mathbf{1}\\
&\equiv a(-r)b(-1)a(-m)b(-n)\mathbf{1} + \binom{r+m}{m+1}ma(-r-m-1)b(-n)\mathbf{1}\\
&\quad - (-1)^r\binom{r+n-1}{n}b(-r-1-n)na(-m)\mathbf{1}\\
&\equiv a(-r)a(-m)b(-n)b + \left\{\binom{r+m}{m+1}m\binom{-r-m-1}{n-1} - (-1)^n\binom{r+n-1}{n}n\binom{m+r+n-1}{r+n}\right\}\gamma(t)\\
&\equiv a(-r)a(-m)b(-n)b + \frac{(-1)^{n-1}(r+m+n-1)!(m+r+n+1)}{(r-1)!(m-1)!(n-1)!(m+1)(r+n)}\gamma(t).
\end{aligned}$$

We finally prove the theorem. Suppose that the proposition is false and let

$$u = a(-i_1)\cdots a(-i_h)b(-j_1)\cdots b(-j_k)\mathbf{1} \notin C_1(M_2(1)^\sigma) + < S_1 > .$$

be a minimal base w.r.t. the order.

As we showed, $u = a(-i_1)a(-i_2)a$ or $u = a(-m)b$. By the above proposition, we obtain

$$a(-k+1)b \in C_1(M_2(1)^\sigma) \quad \text{for all } k \geq 6$$

Since $C_1(M_2(1)^\sigma)$ is closed by the 0-th product, we have:

(1) $C_1(M_2(1)^\sigma) \ni (a(-k+1)b)_0(a(-1)a(-1)a) = 3(k-1)a(-k)a(-1)a$ and so

(2) $C_1(M_2(1)^\sigma) \ni (a(-n)b)_0a(-k)a(-1)a = 2a(-n-1)a(-k)a + ka(-n-k)a(-1)a.$