第26回代数的組合せ論シンポジウム報告集

2009年6月24－26日

於　遊学館（山形県生涯学習センター）

平成21年度文部科学省科学研究費基盤研究（B）

（課題番号　18340022　伊藤達郎）

まえがき

この報告集は、２００９年6月２４日（水）から２６日（金）にわたって、遊学館（山形県生涯学習センター）で行われた研究集会「第２６回代数的組合せ論」の講演記録です。研究集会は 65 名の方に参加していただきました。

この報告集の作成にあたっては、科学研究費基盤研究（Ｂ）（研究代表者　金沢大学理工研究域数物科学系 伊藤達郎）から援助をいただきました。この場を借りて御礼申し上げます。

最後になりましたが、講演者の方々、開催にあたり有益な情報・助言をいただいた（財）山形コンベンションビューローに感謝します。

２００９年１２月

脇　克志

小田文仁

原田昌晃

第２６回代数的組合せ論シンポジウム

下記のように研究集会を開催しますので、ご案内申し上げます。

世話人　脇　克志（山形大）
小田 文仁（山形大）
原田 昌晃（山形大・ＪＳＴさきがけ）

記

日程：　２００９年６月２４日（水）～２６日（金）
場所：　遊学館（山形県生涯学習センター）
山形市緑町１丁目２番３６

プログラム

６月２４日（水）

１４：００～１４：５０ Vladimir D. Tonchev (Michigan Technological University)
Polarities, quasi-symmetric designs, and Hamada's conjecture

１５：００～１５：３０ 秋山 献之（福岡大・理学部）、小川 雅之（コンピュータエンジニアリング）、末竹 千博（大分大・工学部）
On $STD_6[18;3]$'s and $STD_7[21;3]$'s admitting a semiregular automorphism group of order 9

１５：５０～１６：４０ 竹村 彰通（東京大・情報理工学系研究科）
最近の統計学における代数的諸問題について

１６：５０～１７：２０ 吉田 知行（北海道大・理学研究院）
分割表生成のための群論的方法

６月２５日（木）

１０：００～１０：５０ 平峰 豊（熊本大・教育学部）
変形一般アダマール行列について

１１：１０～１１：４０ 中川 暢夫（近畿大・理工学部）
座標関数が２次となる平面関数の同値概念とその特性について

１１：５０～１２：２０ 野崎 寛（東北大・情報科学研究科）
パラメーター $(276, 140, 58, 84)$ の強正則グラフの新しい例の構成

１４：００～１４：５０ 小田 文仁（山形大・理学部）、澤辺 正人（千葉大・教育学部）
A collection of subgroups for the generalized Burnside ring

１５：００～１５：３０ 田辺 顕一朗（北海道大・理学研究院）
一変数多項式環の二次拡大から構成される頂点代数の有限次元加群

１５：５０～１６：４０ 島倉 裕樹（愛知教育大）
Frame stabilizers for framed vertex operator algebras associated to lattices

１６：５０～１７：２０ 冨江 雅也（筑波大・数理物質科学研究科）
Generalized noncrossing partition に於ける Möbius 関数および Fuss-Catalan number について

懇親会

6月26日（金）

１０：００～１０：５０ 尾畑 伸明（東北大・情報科学研究科）
量子確率論とグラフのスペクトル解析

１１：１０～１１：４０ 佐久間 雅（山形大・地域教育文化学部）
Colored pebble motion on graphs

１１：５０～１２：２０ 潮 和彦（近畿大・理工学部）
Hamilton C_k-sixfoil designs

１４：００～１４：５０ 坂内 英一（九州大・数理学研究院（学術研究者））、坂内悦子
Euclidean designs and coherent configurations

１５：１０～１５：４０ 花木 章秀（信州大・理学部）
Categories of association schemes and coherent configurations

１５：５０～１６：２０ 須田 庄（東北大・情報科学研究科）
ある Q-多項式スキームの正則性の特徴付け

１６：３０～１７：００ 三枝崎 剛（北海道大・理学研究院）
虚二次体の整数環から作られる球面デザインの非存在について（坂内英一氏との共同研究）

26th Symposium on Algebraic Combinatorics

Organizers Katsushi Waki (Yamagata University)
Fumihito Oda (Yamagata University)
Masaaki Harada (Yamagata University)

June 24–June 26, 2009
Yuugakukan, Yamagata City

Program

June 24 (Wednesday)

14:00–14:50 Vladimir D. Tonchev (Michigan Technological University)
Polarities, quasi-symmetric designs, and Hamada's conjecture

15:00–15:30 Kenzi Akiyama (Fukuoka University) Masayuki Ogawa (Computer Engineering Corp.) and Chihiro Suetake (Oita University)
On $\mathrm{STD}_6[18;3]$'s and $\mathrm{STD}_7[21;3]$'s admitting a semiregular automorphism group of order 9

15:50–16:40 Akimichi Takemura (University of Tokyo)
Current algebraic problems in statistics

16:50–17:20 Tomoyuki Yoshida (Hokkaido University)
A group-theoretic method of generating contingency tables

June 25 (Thursday)

10:00–10:50 Yutaka Hiramine (Kumamoto University)
On modified generalized Hadamard matrices

11:10–11:40 Nobuo Nakagawa (Kinki University)
On equivalent properties of quadratic planar functions

11:50–12:20 Hiroshi Nozaki (Tohoku University)
New examples of strongly regular graphs with parameters $(276, 140, 58, 84)$

14:00–14:50 Fumihito Oda (Yamagata University) and Masato Sawabe (Chiba University)
A collection of subgroups for the generalized Burnside ring

15:00–15:30 Kenichiro Tanabe (Hokkaido University)
Finite-dimensional modules for the vertex algebras constructed from quadratic extensions of the polynomial ring in one variable

15:50–16:40 Hiroki Shimakura (Aichi University of Education)
Frame stabilizers for framed vertex operator algebras associated to lattices

16:50–17:20 Masaya Tomie (University of Tsukuba)
The Möbius functions of Generalized noncrossing partitions and Fuss–Catalan numbers

Party

June 26 (Friday)

10:00–10:50 Nobuaki Obata (Tohoku University)
Quantum probability and spectral analysis of graphs

11:10–11:40 Tadashi Sakuma (Yamagata University)
Colored pebble motion on graphs

11:50–12:20 Kazuhiko Ushio (Kinki University)
Hamilton C_k-sixfoil designs

14:00–14:50 Eiichi Bannai (Kyushu University) and Etsuko Bannai
Euclidean designs and coherent configurations

15:10–15:40 Akihide Hanaki (Shinshu University)
Categories of association schemes and coherent configurations

15:50–16:20 Sho Suda (Tohoku University)
Characterizations of regularity for certain Q-polynomial association schemes

16:30–17:00 Tsuyoshi Miezaki (Hokkaido University)
Nonexistence of spherical designs obtained from integer rings of imaginary quadratic fields (joint work with Eiichi Bannai)

目次

Combinatorial designs of minimum q-rank and Hamada's conjecture

Vladimir D. Tonchev
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931, USA

Abstract

The paper surveys combinatorial designs having the same parameters and q-rank as certain geometric designs having as blocks the subspaces of a given dimension of a finite geometry over a field of order q. The construction of such designs is motivated by Hamada's conjecture from 1973 about the minimum q-rank of geometric designs. A revised version of Hamada's conjecture is proposed that concerns the q-rank of generalized incidence matrices with entries in $GF(q)$ instead of $(0,1)$-incidence matrices.

1 Incidence matrices and Hamada's conjecture

A combinatorial t-(v,k,λ) design is a pair $D = \{X, \mathcal{B}\}$ of a finite set X of v points, and a collection $\mathcal{B}$ of b k-subsets of X called blocks, with the property that every t points are contained in exactly λ blocks [2]. The *incidence matrix* of a design D is a b by v $(0,1)$-matrix with rows indexed by the blocks and columns indexed by the points, where an entry is equal to 1 if the corresponding block and point are incident, and 0 otherwise. Two designs are isomorphic if there is a bijection between their point sets that maps the blocks of the first design to blocks of the second design. An automorphism of a design is a permutation of the points that preserves the collection of blocks.

The *q-rank* of a design D, or $rank_q(D)$, is the rank of the incidence matrix of D over $GF(q)$. Equivalently, the q-rank of a design is the dimension of the linear space over $GF(q)$, or the linear q-ary code spanned by the rows of its incidence matrix.

The interest in designs of low q-rank has been motivated by one of the early applications of combinatorial designs to coding theory, namely, for the construction of majority-logic decodable codes (Rudolph [26]). A linear q-ary code of length n is a linear subspace of $GF(q)^n$. A linear code C of length n whose dual code $C^{\perp}$ supports a 2-(n,w,λ) design among its codewords of weight w can correct up to $(r+\lambda-1)/(2\lambda)$ errors (where $r = \lambda(n-1)/(w-1)$) by majority-logic decoding, and even a greater number of errors if $C^{\perp}$ supports t-designs

with $t > 2$ (Rahman and Blake [25]). Consequently, a linear code being the null space of the incidence matrix of a t-(n, w, λ) design with $t \geq 2$ admits majority-logic decoding. Since the total number of blocks in a t-(n, w, λ) design with $t \geq 2$ and $n > w > 0$ is greater than or equal to n by the Fisher inequality [10], the incidence matrix can be of full rank n, in which case the resulting code is trivial, consisting of the zero vector only. Therefore, for this purpose, it is important to choose a t-(n, w, λ) design of minimal rank (over the considered finite field) among all nonisomorphic designs having the given parameters.

Most of the known majority-logic decodable codes are based on designs arising from finite geometries, the most notable class of such codes being the Reed-Muller codes. We refer to any design having as points and blocks the points and subspaces of a given dimension in a finite affine or projective geometry as a *geometric* design. We denote by $PG_d(m, q)$ (resp. $AG_d(m, q)$) the geometric design having as blocks the d-dimensional subspaces of the m-dimensional projective space $PG(m, q)$ (resp. the m-dimensional affine space $AG(m, q)$) over $GF(q)$. The geometric designs having as blocks the hyperplanes in the corresponding affine or projective geometry ($d = m - 1$), are called *classical* geometric designs.

The ranks of the geometric designs were computed in a series of papers in the late 60's and early 70's, starting with a paper by Graham and MacWilliams [9], where the p-rank of the incidence matrix of the Desarguesian projective plane $PG(2, p^s)$ of order p^s (p a prime, $s \geq 1$), was found to be equal to

$$\binom{p+1}{2}^s + 1. \tag{1}$$

In the special case $s = 1$, the formula (1) implies that the p-rank of the Desarguesian plane $PG(2, p)$ of a prime order p is equal to

$$\binom{p+1}{2} + 1 = \frac{p^2 + p + 2}{2}. \tag{2}$$

We note that formula (1) was derived and is valid specifically for the Desarguesian plane of order p^s, $PG(2, p^s)$, while the formula (2) gives the p-rank of any projective plane of a prime order p. This follows from a more general result for the p-rank of a symmetric 2-(v, k, λ) design (a design is *symmetric* if it has equal number of points and blocks: $b = v$). If p is a prime that divides $k - \lambda$, but p^2 does not divide $k - \lambda$ and p does not divide k and λ, the p-rank of a symmetric 2-(v, k, λ) design is equal to $(v + 1)/2$ [10, page 382, Theorem 17.3.1]. Consequently, since any projective plane of a prime order p is a symmetric 2-$(p^2+p+1, p+1, 1)$ design, its p-rank is given by (2). This implies that although for each prime p the only known plane of order p is the Desarguesian plane $PG(2, p)$, if a non-Desarguesian plane of a prime order p would exist, it will have the same p-rank as the Desarguesian plane $PG(2, p)$.

The result of Graham and MacWillims [9] was generalized by MacWilliams and Mann [22], Goethals and Delsarte [8], and Smith [29] to the following formula for the p-rank r_p of the classical geometric design having as blocks the subspaces of dimension $m - 1$ of the m-dimensional projective space $PG(m, p^s)$:

$$r_p = \binom{p+m-1}{m}^s + 1. \tag{3}$$

A survey of other related results is contained in [32]).

In 1973, Hamada [11], computed the p-rank of all geometric designs in general, when blocks are subspaces of any given dimension d, $1 \leq d \leq m-1$, of a projective space $PG(m,p^s)$ or an affine space $AG(m,p^s)$. In his remarkable paper [11], Hamada made the conjecture that a geometric design arising from a finite geometry over $GF(q)$ has minimum q-rank among all designs with the given parameters.

Hamada's conjecture is of fundamental importance for several reasons. First, it indicates that a geometric design, being a design of minimum p-rank among all nonisomorphic designs with the given parameters, is the best choice for the construction of an error-correcting code with majority-logic decoding. It is known that the number of nonisomorphic designs having the same parameters as the classical geometric designs having as blocks the hyperplanes of $PG(m,q)$ or $AG(m,q)$, $m \geq 3$, grows exponentially with linear growth of m (Jungnickel [16], Kantor [19], C. Lam, S. Lam and Tonchev [20], Lam and Tonchev [21]). This result was extended recently by Jungnickel and Tonchev [18] to designs having the same parameters as a geometric design $PG_d(m,q)$, for any $2 \leq d \leq m-1$ and any prime power q.
Secondly, the conjecture provides a computationally simple characterization of geometric designs in terms of the p-rank of their incidence matrices: the complexity of computing the rank of a matrix is a cubic polynomial in the number of rows (or columns), while the complexity of finding isomorphisms between combinatorial designs is as hard as the notoriously difficult graph isomorphism problem; see [4, Remark VII.6.6].

Last, but not least, Hamada's conjecture implies the famous conjecture in finite geometry that for any prime p, the only (up to isomorphism) projective plane of order p is the Desarguesian plane $PG(2,p)$.

A narrower form of the conjecture, due to Assmus, concerns only designs defined by hyperplanes, i.e. designs with classical parameters, and there is an even more specialized conjecture due to Sachar [28] that applies to projective planes only.

2 The proven cases

Hamada's conjecture has been proved to be true for the classical designs of the hyperplanes in a binary affine or projective space (Hamada and Ohmori [12]), as well as for the designs of the lines in a binary projective or ternary affine geometry (Doyen, Hubaut and Vandensavel [7]), and the designs of the planes in a binary affine geometry (Teirlinck [30]). Namely, the following results are known.

Theorem 2.1 (Hamada and Ohmori [12]). *(i) The 2-rank of the incidence matrix A of any symmetric 2-$(2^{m+1}-1, 2^m, 2^{m-1})$ design D satisfies the inequality*

$$rank_2(A) \geq m+1,$$

with equality if and only if D is isomorphic to the complementary design of the design formed by the hyperplanes in $PG(m,2)$. Consequently, the 2-rank of the incidence matrix A of any

symmetric 2-$(2^{m+1}-1, 2^m-1, 2^{m-1}-1)$ *design D satisfies the inequality*

$$rank_2(A) \geq m+2,$$

with equality if and only if D is isomorphic to the design formed by the hyperplanes in $PG(m,2)$.
(ii) The 2-rank of the incidence matrix A of any 2-$(2^m, 2^{m-1}, 2^{m-1}-1)$ *design D satisfies the inequality*

$$rank_2(A) \geq m+1,$$

with equality if and only if D is isomorphic to the design formed by the hyperplanes in $AG(m,2)$.

Theorem 2.2 (Doyen, Hubaut and Vandensavel [7]). *(i) The 2-rank of the incidence matrix A of any 2-*$(2^m-1, 3, 1)$ *(or a Seiner triple system $STS(2^m-1)$) D satisfies the inequality*

$$rank_2(A) \geq 2^m - 1 - m,$$

with equality if and only if D is isomorphic to the design formed by the lines in $PG(m-1,2)$.
(ii) The 3-rank of the incidence matrix A of any 2-$(3^m, 3, 1)$ *design (or a Steiner triple system $STS(3^m)$) D satisfies the inequality*

$$rank_3(A) \geq 3^m - 1 - m,$$

with equality if and only if D is isomorphic to the design formed by the lines in $AG(m,3)$.

Theorem 2.3 (Teirlinck [30]). *The 2-rank of the incidence matrix A of a 3-*$(2^m, 4, 1)$ *design (or a Steiner quadruple system $STS(2^m)$) D satisfies the inequality*

$$rank_2(A) \geq 2^m - 1 - m,$$

with equality if and only if D is isomorphic to the design formed by the planes in $AG(m,2)$.

We note that the binary code spanned by the $(m-r)$-dimensional subspaces of the m-dimensional binary affine geometry $AG(m,2)$ is the Reed-Muller code $R(r,m)$ of length $n = 2^m$ and order r $(1 \leq r \leq m)$, while a binary code spanned by the subspaces of a given dimension of $PG(m-1,2)$ is a punctured Reed-Muller code.

3 Non-geometric designs having the same p-rank as geometric designs

So far, there are no known examples of designs that have the same parameters, but smaller p-rank than a given geometric design. However, there are some examples of designs that

violate the "only-if" part of the following stronger form of Hamada's conjecture, which holds true in all proven cases of the conjecture:

If D is a design with the same parameters as a design G having as blocks the d-dimensional subspaces of $AG(m,q)$ or $PG(m,q)$, then

$$rank_q(D) \geq rank_q(G), \tag{4}$$

with equality $rank_q(D) = rank_q(G)$ if and only if D is isomorphic to G.

Until recently, there were only three known parameter sets of geometric designs for which there exist non-geometric designs with the same parameters and the same p-rank as their geometric counterparts. These parameter sets are: 2-$(31,7,7)$, 3-$(32,8,7)$, [33] and 2-$(64,16,5)$ [13].

A design having only two distinct block intersection numbers is called a *quasi-symmetric* design [27]. In [33], the author used the classification of binary doubly-even self-dual codes of length 32 to enumerate all quasi-symmetric 2-$(31,7,7)$ designs, proving that up to isomorphism, there are exactly five such designs, all having 2-rank equal to 16. One of the five quasi-symmetric designs is the geometric design $PG_2(4,2)$, while the remaining four are non-geometric designs that violate the "only if" part of Hamada's conjecture. One of these non-geometric designs was mentioned also by Goethals and Delsarte [8]. In [33], the proposer proved also that there exist exactly five non-isomorphic 3-$(32,8,7)$ designs with even block intersection numbers, all having 2-rank 16. One of these five designs is the geometric design $AG_3(5,2)$, having as blocks the 3-subspaces in the binary affine geometry $AG(5,2)$.

In 2005, Harada, Lam and Tonchev [13] found two non-geometric 2-$(64,16,5)$ designs having the same 2-rank as the classical geometric design $AG_2(3,4)$ defined by the planes in the 3-dimensional affine space $AG(3,4)$ over the field of order 4. Up to this date, the non-geometric 2-$(64,16,5)$ designs found in [13] are the only known counter-examples to the Assmus conjecture. An alternative construction of one of the exceptional 2-$(64,16,5)$ designs from [13] based on line spreads in projective space was given by Mavron, Mcdonough and Tonchev in [23].

In June 2008, the first infinite class of non-geometric designs that have the same parameters and q-rank as certain geometric designs was found in a joint work by Dieter Jungnickel and the present author [17].

Theorem 3.1 *[17].*
For every integer $d \geq 2$ and every prime p there exists a 2-design having the same parameters and the same p-rank as the geometric design $PG_d(2d,p)$.

A crucial tool in the construction of the new designs found in [17] were polarities in projective geometry. A *correlation* of a finite geometry $\mathcal{G}$ is a permutation α of the subspaces of $\mathcal{G}$ which inverts inclusion, i.e., $S \subseteq T$ implies $S^\alpha \supseteq T^\alpha$ for all subspaces S, T of $\mathcal{G}$ [6, p. 41]. A *polarity* is a correlation of order 2. A correlation α is a polarity if and only if $S \subseteq T^\alpha$ implies $S^\alpha \supseteq T$ for all subspaces S, T of $\mathcal{G}$ [6], [14].

Jungnickel and the present author proved in [17] that every polarity of $PG(2k-1,q)$, where $k \geq 2$, and q is an arbitrary prime power, gives rise to a design with the same

parameters and the same block intersection numbers as, but not isomorphic to the design $PG_k(2k,q)$ of points and k-subspaces of the projective $2k$-space $PG(2k,q)$ over $GF(q)$.

In particular, the case $k=2$ yields a new infinite family of quasi-symmetric designs with parameters

$$v=\frac{q^5-1}{q-1},\ k=\frac{q^3-1}{q-1},\ \lambda=\frac{q^3-1}{q-1},$$

and block intersection numbers 1 and $q+1$.

By construction, the new designs with geometric parameters share many properties with the geometric designs $PG_k(2k,q)$. In particular, there is always a set H of $q^{2k-1}+\ldots+q+1$ points on which the blocks of the design induce an isomorphic copy of $PG(2k-1,q)$, while a copy of an affine $2k$-space $AG(2k,q)$ is induced on the set A consisting of the remaining q^{2k} points. To prove that the new designs are not isomorphic to the geometric design $PG_k(2k,q)$, the sizes of the lines in these designs were computed. A *line* in a 2-(v,k,λ) design through a pair of points P_1, P_2 is defined as the intersection of the λ blocks containing P_1 and P_2. In any of the new designs, the lines through two points of H or two points of A still have the natural geometric size, that is, $q+1$ or q, respectively, whereas a point of H and a point of A determine a line of size 2.

The construction of these new designs was suggested by a careful examination of the five quasi-symmetric 2-$(31,7,7)$ designs from [33] and observing that one of the designs, having its points partitioned into two orbits of length 15 and 16 under its full automorphism group, shares the following property with the geometric design $PG_2(4,2)$: the restriction on the orbit of 15 points resembled a hyperplane in $PG(4,2)$. It turned out that this particular design can be obtained from $PG_2(4,2)$ via a permutation of the lines in a subspace $PG(3,2)$ defined by a polarity, and that observation led to the general construction.

It was proved in [17] that the q-rank of a design obtained via a polarity is bounded by the q-rank of $PG_k(2k,q)$ from below, and by $((q^{2k+1}-1)/(q-1)+1)/2$ from above for arbitrary prime power q and any $k\geq 2$. In the special case when $q=p$ is a prime, it was proved that the new non-geometric designs have the same p-rank as the geometric design $PG_k(2k,p)$, hence these designs provide the first and only known infinite class of counter-examples to the only-if part of Hamada's conjecture. An essential part of the the proof in [17] that the new non-geometric designs obtained via a polarity from $PG_k(2k,p)$ when p is a prime have the same p-rank as the geometric design $PG_k(2k,p)$, was the derivation of the following apparently new closed formula for the p-rank $r_p(k)$ of $PG_k(2k,p)$:

$$r_p(k)=\frac{1}{2}(\frac{p^{2k+1}-1}{p-1}+1).$$

The simplest previously known version of Hamada's formula for $r_p(k)$, found by Hirschfeld and Shaw [15], (see also [1, Theorem 5.8.1]) looks as follows:

$$r_p(k)=\frac{p^{2k+1}-1}{p-1}-\sum_{i=0}^{k-1}(-1)^i\binom{(k-i)(p-1)-1}{i}\binom{k+(k-i)p}{2k-i}.$$

Recently, Munemasa [24] proved that the block graph of the new designs from [17] is isomorphic to the twisted Grassmann graph discovered by van Dam and Koolen [5].

In a recent paper by Clark, Jungnickel, and the author [3], the following result was proved that extends the construction from [17] to the case of binary affine geometry.

Theorem 3.2 *[3].*
For every $d \geq 3$, there exists a resolvable 3-design with the same parameters, block intersection numbers, and 2-rank as the geometric design $AG_{d+1}(2d+1,2)$ having as blocks the $(d+1)$-subspaces of the binary $(2d+1)$-dimensional affine space $AG(2d+1,2)$.

4 Ranks of generalized incidence matrices

In this section, we discuss a revised version of Hamada's conjecture aiming to characterize finite geometric designs in terms of minimum rank of matrices with entries in $GF(q)$ instead of $(0,1)$-incidence matrices [31].

In order to apply majority decoding to a linear code C, it suffices that the dual code $C^{\perp}$ contains the blocks of a t-(v,k,λ) design among the supports[1] of code words of weight k, and it is not necessary that $C^{\perp}$ contains the incidence matrix of a design Motivated by this, we propose the following

Definition 4.1 *[31]. The dimension of a t-(v,k,λ) design $\mathcal{D}$ over $GF(q)$ (or q-dimension) is defined as the minimum dimension of all linear codes of length v over $GF(q)$ that contain the blocks of $\mathcal{D}$ among the supports of code words of weight k.*

Definition 4.2 *[31]. A* generalized incidence matrix *of a design over $GF(q)$ is a matrix obtained from the $(0,1)$-incidence matrix by replacing 1's with arbitrary nonzero elements from $GF(q)$.*

A design D with b blocks of size k has $(q-1)^{kb}$ generalized incidence matrices over $GF(q)$, and the q-dimension of D is equal to the minimum value among the q-ranks of all of its generalized incidence matrices.

The dimension and the rank of a design coincide if $q = 2$. However, if $q > 2$, a codeword of weight k that supports a block does not have to have constant nonzero coordinates, and consequently, the code does not have to contain the incidence vector of the block. In general, the q-rank of a design is an upper bound for the dimension of the design over $GF(q)$ if $q > 2$. For example, the 3-rank of the $(0,1)$-incidence matrix of the 4-$(11,5,1)$ design supported by the ternary Golay $[11,6,5]$ code is 11, while the code is of dimension 6, hence, the dimension of the 4-$(11,5,1)$ design over $GF(3)$ is at most 6.

In [31], the author determined the dimension of the complementary designs of the classical designs having as blocks the hyperplanes in a finite projective or affine space over $GF(q)$. In addition, it was proved in [31] that the classical designs are the unique designs of minimum dimension.

[1]The *support* of a vector is the set of indices of its nonzero components.

Theorem 4.3 *[31].*
The dimension d of any 2-$(\frac{q^{n+1}-1}{q-1}, q^n, q^n - q^{n-1})$ design ($n \geq 2$) over $GF(q)$ is greater or equal to $n+1$. Moreover, the equality $d = n+1$ holds if and only if the design is isomorphic to the complementary design of the geometric design formed by the hyperplanes in the n-dimensional projective space $PG(n,q)$ over $GF(q)$.

Theorem 4.4 *[31].*
The dimension d of any 2-$(q^n, q^n - q^{n-1}, q^n - q^{n-1} - 1)$ design ($n \geq 2$) over $GF(q)$ is greater or equal to $n+1$. Moreover, $d = n+1$ if and only if the design is isomorphic to the complementary design of the geometric design formed by the hyperplanes in the n-dimensional affine space $AG(n,q)$ over $GF(q)$.

These results generalize Theorem 2.1 by Hamada and Ohmori about the classical designs over the binary field.

The author believes that a revised form of Hamada's conjecture for $q > 2$ modified by replacing the q-rank of the incidence matrix with the minimum q-rank of a generalized incidence matrix of the design over $GF(q)$ may be true in general.

5 Acknowledgments

The author wishes to thank Tohoku University and Yamagata University for the hospitality during his visit in June 2009, and for the support to attend the 26th Symposium on Algebraic Combinatorics, Yamagata, June 24-June 26, 2009.

References

[1] E.F. Assmus and J.D. Key, *Designs and Their Codes*, Cambridge University Press, Cambridge 1992.

[2] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Second Edition, Cambridge University Press, Cambridge 1999.

[3] D. Clark, D. Jungnickel, and V.D. Tonchev, Affine geometry designs, polarities, and Hamada's conjecture, *J. Combin. Theory*, Ser. A, submitted.

[4] C. J. Colbourn and J.F. Dinitz, eds., *Handbook of Combinatorial Designs*, Second Edition, CRC Press, Boca Raton, 2007.

[5] E.R. van Dam and J.H. Koolen, A new family of distance-regular graphs with unbounded diameter, *Invent. Math.* **162** (2005), 189-193.

[6] P. Dembowski, *Finite Geometries*, Springer, Berlin, 1968.

[7] J. Doyen, X. Hubaut, M. Vandensavel, Ranks of incidence matrices of Steiner triple systems, *Math. Z.* **163** (1978), 251–259.

[8] J.M. Goethals and P. Delsarte, On a class of majority logic decodable cyclic codes, *IEEE Trans. Info. Theory* **14** (1968), 182-188.

[9] R.L. Graham and J. MacWilliams, On the number of information symbols in different difference-set cyclic codes, *Bell Sys. Tech. J.* **45** (1966), 1057-1070.

[10] M. Hall, Jr., *Combinatorial Theory*, Second Edition, Wiley, New York, 1986.

[11] N. Hamada, On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its application to error-correcting codes, *Hiroshima Math. J.* **3** (1973), 153-226.

[12] N. Hamada and H. Ohmori, On the BIB design having the minimum p-rank, *J. Combin. Theory* A **18** (1975), 131-140.

[13] M. Harada, C. Lam, and V.D. Tonchev, Symmetric $(4,4)$-nets and generalized Hadamard matrices over groups of order 4, *Designs, Codes, and Cryptography* **34** (2005), 71-87.

[14] J.W.P. Hirschfeld, *Projective Geometries over Finite Fields, Second Edition*, Oxford University Press, Oxford, 1998.

[15] J. W. P. Hirschfeld and R. Shaw: Projective geometry codes over prime fields. In: *Finite Fields: Theory, Application and Algorithms.* Contemporary Math **168** (1994), pp. 151–163. Amer Math. Soc., Providence, R.I.

[16] D. Jungnickel, The number of designs with classical parameters grows exponentially, *Geom. Dedicata* **16** (1984), 167–178.

[17] D. Jungnickel and V.D. Tonchev, Polarities, quasi-symmetric designs, and Hamada's conjecture, *Designs, Codes and Cryptography*, **51** (2009), 131-140.

[18] D. Jungnickel and V.D. Tonchev, The number of designs with geometric parameters grows exponentially, *Designs, Codes and Cryptography*, to appear.

[19] W. M. Kantor: Automorphisms and isomorphisms of symmetric and affine designs. *J. Algebraic Combin.* **3** (1994), 307–338.

[20] C. Lam, S. Lam, V. Tonchev, Bounds on the number of affine, symmetric and Hadamard designs and matrices, *J. Combin. Theory, Ser. A* **92** (2000), 186–196.

[21] C. Lam and V. D. Tonchev: A new bound on the number of designs with classical affine parameters. *Designs, Codes and Cryptography* **27** (2002), 111–117.

[22] F.J. MacWilliams and H.B. Mann, On the p-rank of the design matrix of a difference set, *Information and Control* **12** (1968), 474-488.

[23] V. C. Mavron, T.P. McDonough, and V.D. Tonchev, On affine designs and Hadamard designs with line spreads, *Discrete Math.* **308** (2008), 2742-2750.

[24] A. Munemasa and V.D. Tonchev, The twisted Grassmann graph is the block graph of a design, *Innovations in Incidence Geometry*, to appear.

[25] M. Rahman and Ian F. Blake, Majority logic decoding using combinatorial designs, *IEEE Trans. Info. Theory* **21** (1975), 585-587.

[26] L.D. Rudolph, A class of majority-logic decodable codes, *IEEE Trans. Info. Theory* **13** (1967), 305-307.

[27] M. S. Shrikhande and S. S. Sane, "Quasi-Symmetric Designs", *LMS Lecture Note Ser.* **164**, Cambridge 1991.

[28] H. Sachar, The F_p span of the incidence matrix of a finite projective plane, *Geom. Dedicata* **8** (1979), 407-415.

[29] K.J.C. Smith, On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry, *J. Combin. Theory* **7** (1969), 122-129.

[30] L. Teirlinck, On projective and affine hyperplanes, *J. Combin. Theory Ser. A* **28** (1980), 290-306.

[31] V.D. Tonchev, Linear Perfect Codes and a Characterization of the Classical Designs, *Designs, Codes and Cryptography* **17** (1999), 121-128.

[32] V.D. Tonchev, "Codes and Designs", Chapter 15, Volume II, pp. 1229-1268 in: *Handbook of Coding Theory*, V.S. Pless and W.C. Huffman eds., North Holland, Amsterdam 1998.

[33] V.D. Tonchev, Quasi-symmetric 2-(31,7,7) designs and a revision of Hamada's conjecture, *J. Combin. Theory, Ser. A* **42** (1986), 104-110.

On $\mathrm{STD}_6[18;3]$'s and $\mathrm{STD}_7[21;3]$'s admitting a semiregular automorphism group of order 9

秋山献之 (福岡大学理学部)
(akiyama@sm.fukuoka-u.ac.jp)
末竹千博 (大分大学工学部)
(suetake@csis.oita-u.ac.jp)

§1 導入

この研究は, 秋山献之, 小川雅之, 末竹千博の共同研究である。この研究では, 次の条件を満たす対称横断デザイン $\mathrm{STD}_\lambda[k;u]$ $\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ を考える。$\mathcal{D}$ は $\mathcal{P}$ と $\mathcal{B}$ 両方の上で半正則に作用する位数 su の自己同型群 G を持つ。ここで $s|k$。また G は位数 u の elation group U を含むとする。この報告の前半では, このような $\mathrm{STD}_\lambda[k;u]$ を群環 $\mathbb{Z}[G]$ を使って特徴づける。ここで, $\mathcal{D}$ は位数 u の elation group を持つので, $\mathcal{D}$ には U 上の次数 k のある一般アダマール行列 $\mathrm{GH}(k,U)$ が対応する。この報告の後半では, 位数 3 の elation を含む, 点集合とブロック集合上半正則に作用する位数 9 の非巡回自己同型群を持つ $\mathrm{STD}_6[18;3]$ と $\mathrm{STD}_7[21;3]$ を分類する。

$\mathrm{STD}_\lambda[2\lambda;2]$ の存在は位数 2λ のアダマール行列の存在と同値である。アダマール行列の研究は組合せ論における主要な研究のうちの一つである。従って, 我々は次の大きさのクラスサイズを持つ $\mathrm{STD}_\lambda[3\lambda;3]$ の研究は価値があると考える。n_λ を非同型な $\mathrm{STD}_\lambda[3\lambda;3]$ の個数とすると, 上記の分類は $n_6\geq 20$, $n_7\geq 5$ を与える。なお, $\lambda\leq 5$ に対して n_λ の値は完全に決定されている。すなわち, $n_1=1$, $n_2=1$, $n_3=4$ ([12]), $n_4=1$ ([13]), $n_5=0$ ([5]) である。

もし $\mathrm{STD}_\lambda[k;u]$ が相対差集合を持てば, この STD は我々の仮定を満足するので, 我々の仮定は相対差集合を捜すのに有効であると考えられる。また, もし我々が適当な整数 s の値を仮定するなら, 我々の仮定は新しい $\mathrm{STD}_\lambda[k;u]$ や 新しい $\mathrm{GH}(k;U)$ を捜すために役立つであろう。実際, 最近, 平峰 [7] は我々の結果を横断デザイン TD の上で一般化し, 全ての素数べき q に対して, $V(2q,GF(q))$ の spread を使って $\mathrm{STD}_q[q^2;q]$ を構成した。彼の構成はクラス正則 STD と 非クラス正則 STD を含み, 多くの新しい STD が構成された可能性が強い。Mavron と Tonchev [12] によって見つけられた 4 つの $\mathrm{STD}_3[9;3]$ のうちの少なくとも 2 つは平峰が構成した無限系列に含まれる。

デザイン理論における一般的な記号と概念については [2], [4], [10], [15] 等を参照されることをお勧めします。

§2 TD, RTD, STD の定義

定義 2.1 **横断デザイン** (transversal design) $\mathrm{TD}_\lambda[k;u]$ (TD) とは, 次の 2 つの条件を満たす結合構造 $\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ のことである。
ここで, $k\geq 2$, $u\geq 2$, $\lambda\geq 1$ とする。
(i) 各ブロック $B(\in\mathcal{B})$ は丁度 k 個の点を含む。
(ii) $\mathcal{P}$ は, 次の条件を満たす, サイズがすべて u である k 個の部分集合 $\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}$ に分割される。($\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}$ は $\mathcal{D}$ の**点クラス** (point classes) と呼ばれる。) 相異なる 2 点 p,q に対して, p,q が異なる点クラスに属するならば, p,q を含むブロックは丁度 λ 個あり, そうでなければ p,q を含むブロックは存在しない。

注意 2.2 定義 2.1 において次が成り立つ。
(i) $|\mathcal{P}|=uk$
(ii) $|\mathcal{B}|=u^2\lambda$

定義 2.3 **分割可能な横断デザイン** (resolvable transversal design) $\mathrm{RTD}_\lambda[k;u]$ (RTD) とは, 次の 3 つの条件を満たす結合構造 $\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ のことである。
ここで, $k\geq 2$, $u\geq 2$, $\lambda\geq 1$ とする。

(i) $\mathcal{D}$ は $\mathrm{TD}_\lambda[k;u]$ である。
(ii) 次の条件を満たす $\mathcal{B}$ の分割 $\mathcal{B}=\mathcal{B}_0\cup\mathcal{B}_1\cup\cdots\cup\mathcal{B}_{r-1}$ が存在する。$0\leq i\leq r-1$ とするとき, 任意の B, $B'(\neq)\in\mathcal{B}_i$ に対して, $(B)\cap(B')=\emptyset$ で $\bigcup_{B\in\mathcal{B}_i}(B)=\mathcal{P}$

注意 2.4 定義 2.3 において, $u^2\lambda=\sum_{i=0}^{r-1}|\mathcal{B}_i|$ が成り立つ。

定義 2.5 $\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ を $\mathrm{TD}_\lambda[k;u]$ とする。このとき, $\mathcal{D}$ の双対構造 $\mathcal{D}^d$ もまた $\mathrm{TD}_\lambda[k;u]$ になるとき, $\mathcal{D}$ を**対称横断デザイン** (symmetric transversal design) $\mathrm{STD}_\lambda[k;u]$ (STD) という。ここで, $\mathcal{D}^d$ の点クラスを $\mathcal{D}$ の**ブロッククラス** (block classes) という。

定理 2.6([11]) $\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ を $\mathrm{TD}_\lambda[k;u]$ とし, $k=\lambda u$ とする。このとき $\mathcal{D}$ が $\mathrm{RTD}_\lambda[k;u]$ である。$\Longleftrightarrow$ $\mathcal{D}$ が $\mathrm{STD}_\lambda[k;u]$ である。

注意 2.7 もし $\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ が $\mathrm{RTD}_\lambda[k;u]$ で $k=\lambda u$ ならば, 定義 2.3 (ii) の $\mathcal{B}_0,\mathcal{B}_1,\cdots,\mathcal{B}_{r-1}$ $(r=k)$ が $\mathcal{D}$ のブロッククラスになる。

§3 STD の同型写像と自己同型写像

$\mathcal{D}=(\mathcal{P},\mathcal{B},I)$ を $\mathrm{STD}_\lambda[k;u]$ とする。ここで, $k=\lambda u$
$\Omega=\{\mathcal{P}_0,\mathcal{P}_1,\cdots,\mathcal{P}_{k-1}\}$ を $\mathcal{D}$ の点クラスからなる集合とする。
$\Delta=\{\mathcal{B}_0,\mathcal{B}_1,\cdots,\mathcal{B}_{k-1}\}$ を $\mathcal{D}$ のブロッククラスからなる集合とする。
$\mathcal{P}_0=\{p_0,p_1,\cdots,p_{u-1}\}$, $\mathcal{P}_1=\{p_u,p_{u+1},\cdots,p_{2u-1}\},\cdots,$
$\mathcal{P}_{k-1}=\{p_{(\lambda-1)u},p_{(\lambda-1)u+1},\cdots,p_{\lambda u-1}\}$,
$\mathcal{B}_0=\{B_0,B_1,\cdots,B_{u-1}\}$, $\mathcal{B}_1=\{B_u,B_{u+1},\cdots,B_{2u-1}\},\cdots,$
$\mathcal{B}_{k-1}=\{B_{(\lambda-1)u},B_{(\lambda-1)u+1},\cdots,B_{\lambda u-1}\}$ とする。
$\mathcal{D}'=(\mathcal{P}',\mathcal{B}',I')$ を $\mathrm{STD}_\lambda[k;u]$ とする。
$\Omega'=\{\mathcal{P}_0',\mathcal{P}_1',\cdots,\mathcal{P}_{k-1}'\}$ を $\mathcal{D}'$ の点クラスからなる集合とする。
$\Delta'=\{\mathcal{B}_0',\mathcal{B}_1',\cdots,\mathcal{B}_{k-1}'\}$ を $\mathcal{D}'$ のブロッククラスからなる集合とする。
$\mathcal{P}_0'=\{p_0',p_1',\cdots,p_{u-1}'\}$, $\mathcal{P}_1'=\{p_u',p_{u+1}',\cdots,p_{2u-1}'\},\cdots,$
$\mathcal{P}_{k-1}'=\{p_{(\lambda-1)u}',p_{(\lambda-1)u+1}',\cdots,p_{\lambda u-1}'\}$,
$\mathcal{B}_0'=\{B_0',B_1',\cdots,B_{u-1}'\}$, $\mathcal{B}_1'=\{B_u',B_{u+1}',\cdots,B_{2u-1}'\},\cdots,$
$\mathcal{B}_{k-1}'=\{B_{(\lambda-1)u}',B_{(\lambda-1)u+1}',\cdots,B_{\lambda u-1}'\}$ とする。
Λ を u 次の置換行列全体からなる集合とする。
このような点とブロックの番号付けに対応する $\mathcal{D}$ と $\mathcal{D}'$ の結合行列をそれぞれ

$$L=\begin{pmatrix} L_{0\,0} & \cdots & L_{0\,k-1} \\ \vdots & & \vdots \\ L_{k-1\,0} & \cdots & L_{k-1\,k-1} \end{pmatrix},\quad L'=\begin{pmatrix} L_{0\,0}' & \cdots & L_{0\,k-1}' \\ \vdots & & \vdots \\ L_{k-1\,0}' & \cdots & L_{k-1\,k-1}' \end{pmatrix}$$

とする。ここで, $L_{ij},\ L_{ij}'\in\Lambda\quad(0\le i,j\le k-1)$
以下, $\mathcal{D}$, $\mathcal{D}'$ の各点クラス, 各ブロッククラスでそれぞれ点とブロックの番号を適当に打ち変えて
$L_{i\,0}=L_{i\,0}'=E\quad(0\le i\le k-1)$, $L_{0\,j}=L_{0\,j}'=E\quad(0\le j\le k-1)$ **と仮定する。**

定義 3.1 $S=\{0,1,\cdots,k-1\}$ とおく。S 上の対称群を $\mathrm{Sym}\ S$ と書く。
$f=\begin{pmatrix} 0 & 1 & \cdots & k-1 \\ f(0) & f(1) & \cdots & f(k-1) \end{pmatrix}\in\mathrm{Sym}\ S$ とし, $X_0,X_1,\cdots,X_{k-1}\in\Lambda$ とする。
このとき

(i) $(f,(X_0,X_1,\cdots,X_{k-1}))=\begin{pmatrix} X_{0\,0} & \cdots & X_{0\,k-1} \\ \vdots & \cdots & \vdots \\ X_{k-1\,0} & \cdots & X_{k-1\,k-1} \end{pmatrix}$ を

$X_{ij}=\begin{cases} X_i & \text{if } j=f(i), \\ O & \text{otherwise} \end{cases}$ と定義する。ここで, O は $u\times u$ 型の零行列。

(ii) $(f, \begin{pmatrix} X_0 \\ X_1 \\ \vdots \\ X_{k-1} \end{pmatrix}) = \begin{pmatrix} X_{0\,0} & \cdots & X_{0\,k-1} \\ \vdots & \cdots & \vdots \\ X_{k-1\,0} & \cdots & X_{k-1\,k-1} \end{pmatrix}$ を $X_{ij} = \begin{cases} X_j & \text{if } i = f(j), \\ O & \text{otherwise} \end{cases}$
と定義する。ここで, O は $u \times u$ 型の零行列。

[1] の補題 3.2 より, $\mathcal{D}$ から $\mathcal{D}'$ の上への同型写像は

$$(f, (X_0, X_1, \cdots, X_{k-1}))L(g, \begin{pmatrix} Y_0 \\ Y_1 \\ \vdots \\ Y_{k-1} \end{pmatrix}) = L'$$

を満たす $f, g \in \mathrm{Sym}\ S$ と $X_0, X_1, \cdots X_{k-1}, Y_0, Y_1, \cdots, Y_{k-1} \in \Lambda$ で与えられる。

この等式が成り立つとする。 $X_i L_{f(i)\ g(j)} Y_j = L_{ij}{}'$ $(0 \le i, j \le k-1)$
$X_i L_{f(i)\ g(0)} Y_0 = E$ 故 $X_i = Y_0{}^{-1} L_{f(i)\ g(0)}{}^{-1}$ $(0 \le i \le k-1)$
$X_0 L_{f(0)\ g(j)} Y_j = E$ $(1 \le j \le k-1)$ 故
$Y_j = L_{f(0)\ g(j)}{}^{-1} X_0{}^{-1} = L_{f(0)\ g(j)}{}^{-1} L_{f(0)\ g(0)} Y_0$ $(1 \le j \le k-1)$
$X_i L_{f(i)\ g(j)} Y_j = L_{ij}{}'$ 故
$Y_0{}^{-1} L_{f(i)\ g(0)}{}^{-1} L_{f(i)\ g(j)} L_{f(0)\ g(j)}{}^{-1} L_{f(0)\ g(0)} Y_0 = L_{ij}{}'$
$(0 \le i \le k-1,\ 1 \le j \le k-1)$ 従って次の補題を得る。

補題 3.2 2つの $\mathrm{STD}_\lambda[k; u]$ $\mathcal{D}$ と $\mathcal{D}'$ が同型であるための必要十分条件は,
$Y_0{}^{-1} L_{f(i)\ g(0)}{}^{-1} L_{f(i)\ g(j)} L_{f(0)\ g(j)}{}^{-1} L_{f(0)\ g(0)} Y_0 = L_{ij}{}'$
$(0 \le i \le k-1,\ 1 \le j \le k-1)$
を満たす $(f, g, Y_0) \in \mathrm{Sym}\ S \times \mathrm{Sym}\ S \times \Lambda$ が存在することである。

系 3.3 $\mathcal{D}$ の任意の自己同型写像は
$Y_0{}^{-1} L_{f(i)\ g(0)}{}^{-1} L_{f(i)\ g(j)} L_{f(0)\ g(j)}{}^{-1} L_{f(0)\ g(0)} Y_0 = L_{ij}$
$(0 \le i \le k-1,\ 1 \le j \le k-1)$
を満たす $(f, g, Y_0) \in \mathrm{Sym}\ S \times \mathrm{Sym}\ S \times \Lambda$ で与えられる。
実際,
$(f, g, Y_0)(f', g', Y_0') = (ff', gg', Y_{g'(0)} Y_0')$
ここで, $g'(0) \neq 0$ のとき $Y_{g'(0)} = L_{f(0)\ g(g'(0))}{}^{-1} L_{f(0)\ g(0)} Y_0$

$\Gamma = \{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \}$ とおく。

系 3.4 $u=3$ とする。
$L_{ij},\ L_{ij}{}' \in \Gamma \quad (0 \le i,j \le k-1)$ とする。
このとき
2つの $\mathrm{STD}_\lambda[3\lambda;3]$ $\mathcal{D}$ と $\mathcal{D}'$ が同型であるための必要十分条件は,
$L_{f(i)\ g(0)}{}^{-1} L_{f(i)\ g(j)} L_{f(0)\ g(j)}{}^{-1} L_{f(0)\ g(0)} = L_{ij}{}'$
$(0 \le i \le k-1,\ 1 \le j \le k-1)$
を満たす $(f,g) \in \mathrm{Sym}\ S \times \mathrm{Sym}\ S$, または
$L_{f(i)\ g(0)}{}^{-1} L_{f(i)\ g(j)} L_{f(0)\ g(j)}{}^{-1} L_{f(0)\ g(0)} = L_{ij}{}'^{-1}$
$(0 \le i \le k-1,\ 1 \le j \le k-1)$
を満たす $(f,g) \in \mathrm{Sym}\ S \times \mathrm{Sym}\ S$ が存在することである。

系 3.5 $u=3$ とする。
$L_{ij} \in \Gamma \quad (0 \le i,j \le k-1)$ とする。
このとき
$\mathcal{D}$ の任意の自己同型は
$L_{f(i)\ g(0)}{}^{-1} L_{f(i)\ g(j)} L_{f(0)\ g(j)}{}^{-1} L_{f(0)\ g(0)} = L_{ij}$
$(0 \le i \le k-1,\ 1 \le j \le k-1)$
を満たす $(f,g,Y) \in \mathrm{Sym}\ S \times \mathrm{Sym}\ S \times \Gamma$, または
$L_{f(i)\ g(0)}{}^{-1} L_{f(i)\ g(j)} L_{f(0)\ g(j)}{}^{-1} L_{f(0)\ g(0)} = L_{ij}{}^{-1}$
$(0 \le i \le k-1,\ 1 \le j \le k-1)$
を満たす $(f,g,Y) \in \mathrm{Sym}\ S \times \mathrm{Sym}\ S \times (\Lambda - \Gamma)$ で与えられる。

§4 $\mathrm{STD}_\lambda[k;u]$ の位数 su の半正則自己同型群

$\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ を $\mathrm{STD}_\lambda[k;u]$ とする。$s \in \mathbb{N},\ s|k$ とする。$t = \dfrac{k}{s}$ とおく。
このとき, $k = u\lambda = ts$
$\Omega = \{\mathcal{P}_0, \mathcal{P}_1, \cdots, \mathcal{P}_{k-1}\}$ を $\mathcal{D}$ の点クラスからなる集合とし,
$\Delta = \{\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_{k-1}\}$ を $\mathcal{D}$ のブロッククラスからなる集合とする。
$\mathcal{P}_i = \{p_{iu}, p_{iu+1}, \cdots, p_{(i+1)u-1}\},\ \mathcal{B}_i = \{B_{iu}, B_{iu+1}, \cdots, B_{(i+1)u-1}\} \quad (0 \le i \le k-1)$ とする。
この節では次を仮定する。

仮定 4.1 G を $\mathcal{D}$ の位数 su の自己同型群で, G が $\mathcal{P}$ と $\mathcal{B}$ 上に半正則に作用するとする。更に,

$$G \ni \varphi \longmapsto \begin{pmatrix} \mathcal{P}_i \\ \mathcal{P}_i{}^{\varphi} \end{pmatrix} \in \mathrm{Sym}\Omega$$

の核の位数が u で,

$$G \ni \varphi \longmapsto \begin{pmatrix} \mathcal{B}_j \\ \mathcal{B}_j{}^{\varphi} \end{pmatrix} \in \mathrm{Sym}\Delta$$

の核の位数も u とする。これらの準同型写像の核が一致すると仮定し, それを U とする。U は G の正規部分群になる。

注意 4.2(Hine and Mavron [8]) 仮定 4.1 の2つの準同型写像の核 U は各 $\mathcal{P}_i$ と各 $\mathcal{B}_j$ 上正則に作用する。従って, $\mathcal{D}$ は U 上の次数 k の一般アダマール行列 $\mathrm{GH}(k, U)$ に対応している。U の任意の部分群を U の **elation group** といい, U の元を $\mathcal{P}$ の **elation** という。

以下, 仮定 4.1 を満たす $\mathcal{D}$ を群環 $\mathbb{Z}[G]$ の言葉で表わそう。
$(G/U, \Omega)$ の orbits を $\{\mathcal{P}_{is}, \mathcal{P}_{is+1}, \cdots, \mathcal{P}_{(i+1)s-1}\}$ $(0 \le i \le t-1)$ とする。
$(G/U, \Delta)$ の orbits を $\{\mathcal{B}_{is}, \mathcal{B}_{is+1}, \cdots, \mathcal{B}_{(i+1)s-1}\}$ $(0 \le i \le t-1)$ とする。
$\mathcal{P}$ 上と $\mathcal{B}$ 上の G-orbits を次のようにおく。
$\mathcal{Q}_i = \mathcal{P}_{is} \cup \mathcal{P}_{is+1} \cup \cdots \cup \mathcal{P}_{(i-1)s-1}$, $\mathcal{C}_i = \mathcal{B}_{is} \cup \mathcal{B}_{is+1} \cup \cdots \cup \mathcal{B}_{(i-1)s-1}$ $(0 \le i \le t-1)$
$q_i = p_{isu}$, $C_i = B_{isu}$ $(0 \le i \le t-1)$ とおく。
$0 \le i, j \le t-1$ に対して, $D_{ij} = \{\alpha \in G | q_i{}^{\alpha} \in (C_j)\}$ とおくと, $|D_{ij}| = |\mathcal{Q}_i \cap (C_j)| = s$。

G の任意の部分集合 H に対して, 群環 $\mathbb{Z}[G]$ の元 $\sum_{h \in H} h$ を簡単のため, 単に H と書くことにする。また, $\sum_{h \in H} h^{-1}$ を $H^{(-1)}$ と書くことにする。

補題 4.3 $0 \le i, i' \le t-1$ に対して

$$\sum_{0 \le j \le t-1} D_{ij} D_{i'j}{}^{(-1)} = \begin{cases} \lambda G & \text{if } i \ne i', \\ k + \lambda(G - U) & \text{if } i = i' \end{cases}$$

補題 4.4 $0 \le j, j' \le t-1$ に対して

$$\sum_{0 \le i \le t-1} D_{ij'}{}^{(-1)} D_{ij} = \begin{cases} \lambda G & \text{if } j \ne j', \\ k + \lambda(G - U) & \text{if } j = j' \end{cases}$$

§5 位数 su の群から構成される $\mathrm{STD}_{\lambda}[k; u]$

この節では, 補題 4.3 の逆が成り立つことを示す。

定理 5.1 $\lambda,\ u \in \mathbb{N},\ \ k = \lambda u,\ \ u \geq 2$
$s \in \mathbb{N},\ \ s|k$ とする。$t = \dfrac{k}{s}$ とおく。
G を位数 su の群とする。
U を G の位数 u の正規部分群とする。
$D_{ij} \subseteq G,\ \ |D_{ij}| = s \quad (0 \leq i, j \leq t-1)$ とする。
$0 \leq i, i' \leq t-1$ に対して

$$\sum_{0 \leq j \leq t-1} D_{ij} D_{i'j}^{(-1)} = \begin{cases} \lambda G & \text{if } i \neq i', \\ k + \lambda(G-U) & \text{if } i = i' \end{cases}$$

とする。
$G/U = \{U\tau_0,\ U\tau_1, \cdots, U\tau_{s-1}\}$ とする。
$0 \leq i \leq t-1,\ 0 \leq r \leq s-1$ に対して $\mathcal{P}_{is+r} = \{(i, \varphi\tau_r) |\ \varphi \in U\},\ \mathcal{B}_{is+r} = \{[i, \varphi\tau_r] |\ \varphi \in U\}$ とおく。
このとき, 結合構造 $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ を

$$(i, \alpha) I [j, \beta] \Longleftrightarrow \alpha\beta^{-1} \in D_{ij} \quad (0 \leq i, j \leq t-1;\ \alpha, \beta \in G)$$

と定義すると, $\mathcal{D}$ は点クラス $\mathcal{P}_0, \mathcal{P}_1, \cdots, \mathcal{P}_{k-1}$ とブロッククラス $\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_{k-1}$ を持つ $\mathrm{STD}_\lambda[k; u]$ になる。この場合, 群 G は $\mathcal{D}$ の自己同型群として, 点とブロックの上に半正則に作用する。また, $\Omega = \{\mathcal{P}_0, \mathcal{P}_1, \cdots, \mathcal{P}_{k-1}\}, \Delta = \{\mathcal{B}_0, \mathcal{B}_1, \cdots, \mathcal{B}_{k-1}\}$ とおくと, G は Ω と Δ 上の置換群を導入し, それらの核は共に U で, G/U は Ω と Δ 上半正則に作用する。

次の補題は定理 5.1 で定義された $\mathrm{STD}_\lambda[k; u]$ たちの間の同型・非同型を調べるときに有用である。

補題 5.2 $\lambda,\ u \in \mathbb{N},\ \ k = \lambda u,\ \ u \geq 2$
$s \in \mathbb{N},\ \ s|k$ とする。$t = \dfrac{k}{s}$ とおく。
G を位数 su の群とする。
U を G の位数 u の正規部分群とする。
$D_{ij} \subseteq G,\ \ |D_{ij}| = s \quad (0 \leq i, j \leq t-1)$ とする。
$0 \leq i, l \leq t-1$ に対して

$$\sum_{0 \leq j \leq t-1} D_{ij} D_{lj}^{(-1)} = \begin{cases} \lambda G & \text{if } i \neq l, \\ k + \lambda(G-U) & \text{if } i = l \end{cases}$$

とする。
$G/U = \{U\tau_0,\ U\tau_1, \cdots, U\tau_{s-1}\}$ とする。
$\{D_{ij} |\ 0 \leq i, j \leq t-1\}$ に対して, 結合構造 $\mathcal{D} = (\mathcal{P}, \mathcal{B}, I)$ を定理 5.1 のように定義する。

このとき次が成り立つ。
(i) $\alpha_0, \alpha_1, \cdots, \alpha_{t-1}, \beta_0, \beta_1, \cdots, \beta_{t-1} \in G$ とする。
$D_{ij}{}' = \alpha_i D_{ij} \beta_j \quad (0 \leq i, j \leq t-1)$ とおく。
このとき
$0 \leq i, l \leq t-1$ に対して

$$\sum_{0 \leq j \leq t-1} D_{ij}{}' D_{lj}{}'^{(-1)} = \begin{cases} \lambda G & \text{if } i \neq l, \\ k + \lambda(G - U) & \text{if } i = l \end{cases}$$

が成り立つ。この $\{D_{ij}{}' \mid 0 \leq i, j \leq t-1\}$ に対して, 定理 5.1 のように結合構造 $\mathcal{D}' = (\mathcal{P}', \mathcal{B}', I')$ を定義すると, $\mathcal{D} \cong \mathcal{D}'$ である。
(ii) $p, q \in \mathrm{Sym}\{0, 1, \cdots, t-1\}$ とする。
$D_{ij}{}'' = D_{ip, jq} \quad (0 \leq i, j \leq t-1)$ とおく。
このとき
$0 \leq i, l \leq t-1$ に対して

$$\sum_{0 \leq j \leq t-1} D_{ij}{}'' D_{lj}{}''^{(-1)} = \begin{cases} \lambda G & \text{if } i \neq l, \\ k + \lambda(G - U) & \text{if } i = l \end{cases}$$

が成り立つ。この $\{D_{ij}{}'' \mid 0 \leq i, j \leq t-1\}$ に対して, 定理 5.1 のように結合構造 $\mathcal{D}'' = (\mathcal{P}'', \mathcal{B}'', I'')$ を定義すると, $\mathcal{D} \cong \mathcal{D}''$ である。

§6 $\mathrm{STD}_\lambda[3\lambda; 3]$

この節では, 位数 3 の elation を含む, 位数 9 の基本可換群である半正則 (点とブロック両方に関して) 自己同型群を持つ $\mathrm{STD}_\lambda[3\lambda; 3]$ を考える。そのために, 定理 5.1 で述べられた記号と構成を使う。このとき, $k = 3\lambda$, $u = 3$, $s = 3$, $t = \lambda$。

G を位数 9 の基本可換群とし, U を G の位数 3 の部分群とする。$G = \{(x, y) \mid x, y \in GF(3)\}$, $U = \{(x, 0) \mid x \in GF(3)\}$ とおく。

定義 6.1 $D = \{(a_0, 0), (a_1, 1), (a_2, 2)\}$ なる形の G の部分集合全体からなる集合を Φ とする。D $D' \in \Phi$ とする。Φ における 2 項関係 $\sim$ を次のように定義する。

$$D \sim D' \Longleftrightarrow D' = (a, b) + D \quad \text{for some } (a, b) \in GF(3)$$

補題 6.2 $\sim$ は Φ における同値関係で以下の 5 個の Φ の元は $\Phi/\sim$ の代表元である。$D_1 = \{(0,0), (0,1), (0,2)\}$, $D_2 = \{(0,0), (0,1), (1,2)\}$,
$D_3 = \{(0,0), (2,1), (0,2)\}$, $D_4 = \{(0,0), (1,1), (2,2)\}$, $D_5 = \{(0,0), (2,1), (1,2)\}$。

補題 6.3 $D_{ij} \subseteq G$, $|D_{ij}| = 3$ $(0 \leq i, j \leq \lambda - 1)$ とする。
$0 \leq i, i' \leq \lambda - 1$ に対して

$$\sum_{0 \leq j \leq \lambda - 1} D_{ij} D_{i'j}{}^{(-1)} = \begin{cases} \lambda G & \text{if } i \neq i', \\ 3\lambda + \lambda(G - U) & \text{if } i = i' \end{cases}$$

とする。
(ここで, $D_{i'j}{}^{(-1)} = \sum_{\alpha \in D_{i'j}} (-\alpha)$ であることを注意しておく。)
このとき
(i) $0 \leq i, j \leq \lambda - 1$ に対して,

$$D_{ij} = \{(a_0, 0),\ (a_1, 1),\ (a_2, 2)\} \text{ for some } a_0, a_1, a_2 \in GF(3)$$

(ii) $D_{0\,0} = D_{j_0},\ D_{0\,1} = D_{j_1}, \cdots, D_{0\,\lambda-1} = D_{j_{\lambda-1}}$;
$D_{1\,0} = D_{i_1},\ D_{2\,0} = D_{i_2}, \cdots, D_{\lambda-1\,0} = D_{i_{\lambda-1}}$
for some $1 \leq j_0 \leq j_1 \leq \cdots \leq j_{\lambda-1} \leq 5$ and for some $1 \leq j_0 \leq i_1 \leq i_2 \leq \cdots \leq i_{\lambda-1} \leq 5$, としてよい。

7 $STD_6[18; 3]$

この節では, $\lambda = 6$ のとき, 6節の続きを考える。すなわち, 位数3の elation を含み, 点集合とブロック集合両方の上で半正則に作用する位数9の非巡回自己同型群を持つ $STD_6[18; 3]$ を分類する。

7.1 補題 $(D_{0,0},\ D_{0,1}, \cdots, D_{0,5})$ と $(D_{0,0},\ D_{1,0}, \cdots, D_{5,0})$ の可能性はそれぞれ次の12通りである。
(1) $(D_1, D_1, D_4, D_4, D_5, D_5)$,
(2) $(D_1, D_2, D_2, D_2, D_4, D_5)$,
(3) $(D_1, D_2, D_2, D_3, D_4, D_5)$,
(4) $(D_1, D_2, D_3, D_3, D_4, D_5)$,
(5) $(D_1, D_3, D_3, D_3, D_4, D_5)$,
(6) $(D_2, D_2, D_2, D_2, D_2, D_2)$,
(7) $(D_2, D_2, D_2, D_2, D_2, D_3)$,
(8) $(D_2, D_2, D_2, D_2, D_3, D_3)$,
(9) $(D_2, D_2, D_2, D_3, D_3, D_3)$,
(10) $(D_2, D_2, D_3, D_3, D_3, D_3)$,
(11) $(D_2, D_3, D_3, D_3, D_3, D_3)$,
(12) $(D_3, D_3, D_3, D_3, D_3, D_3)$

次の手順で求める $\mathrm{STD}_6[18;3]$ を決定する。

(i) すべての求める $D=(D_{ij})_{0\le i,j\le 5}$ を決定する。
(ii) これらの D に対応する一般アダマール行列 $\mathrm{GH}(18,GF(3))$ を決定する。
(iii) これらの一般アダマール行列を正規化する。
(iv) 非同型な $\mathrm{STD}_6[18;3]$ に対応するすべての一般アダマール行列を系 3.4 を使って選び出す。

例 7.2 $D=(D_{ij})_{0\le i,j\le 5}$

$$
=\left(\begin{array}{ccc|ccc}
\{(0,0),(0,1),(0,2)\} & \{(0,0),(0,1),(0,2)\} & \{(0,0),(1,1),(2,2)\} \\
\{(0,0),(0,1),(1,2)\} & \{(1,0),(2,1),(2,2)\} & \{(0,0),(0,1),(1,2)\} \\
\{(0,0),(0,1),(1,2)\} & \{(2,0),(1,1),(2,2)\} & \{(1,0),(1,1),(2,2)\} \\
\{(0,0),(0,1),(1,2)\} & \{(2,0),(2,1),(1,2)\} & \{(2,0),(2,1),(0,2)\} \\
\{(0,0),(1,1),(2,2)\} & \{(0,0),(2,1),(1,2)\} & \{(1,0),(0,1),(2,2)\} \\
\{(0,0),(2,1),(1,2)\} & \{(0,0),(1,1),(2,2)\} & \{(0,0),(0,1),(0,2)\}
\end{array}\right|
$$

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

は補題 6.3 の仮定を満たす。従って, 我々の方法で D からある $\mathrm{STD}_6[18;3]$ を構成することが出来る。この D を定義する正規化された結合行列の作り方について述べる。D に対応する $GF(3)$ 上の 18 次の一般アダマール行列は

$$
\left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc}
0&0&0&0&0&0&0&1&2&0&1&2&0&2&1&0&2&1\\
0&0&0&0&0&0&2&0&1&2&0&1&1&0&2&1&0&2\\
0&0&0&0&0&0&1&2&0&1&2&0&2&1&0&2&1&0\\
\hline
0&0&1&1&2&2&0&0&1&1&1&0&1&2&2&2&1&1\\
1&0&0&2&1&2&1&0&0&0&1&1&2&1&2&1&2&1\\
0&1&0&2&2&1&0&1&0&1&0&1&2&2&1&1&1&2\\
\hline
0&0&1&2&1&2&1&1&2&2&0&0&0&2&0&1&0&0\\
1&0&0&2&2&1&2&1&1&0&2&0&0&0&2&0&1&0\\
0&1&0&1&2&2&1&2&1&0&0&2&2&0&0&0&0&1\\
\hline
0&0&1&2&2&1&2&2&0&2&1&2&1&1&0&0&2&2\\
1&0&0&1&2&2&0&2&2&2&2&1&0&1&1&2&0&2\\
0&1&0&2&1&2&2&0&2&1&2&2&1&0&1&2&2&0\\
\hline
0&1&2&0&2&1&1&0&2&0&0&0&0&1&2&2&2&2\\
2&0&1&1&0&2&2&1&0&0&0&0&2&0&1&2&2&2\\
1&2&0&2&1&0&0&2&1&0&0&0&1&2&0&2&2&2\\
\hline
0&2&1&0&1&2&0&0&0&0&2&1&0&0&0&0&1&2\\
1&0&2&2&0&1&0&0&0&1&0&2&0&0&0&2&0&1\\
2&1&0&1&2&0&0&0&0&2&1&0&0&0&0&1&2&0
\end{array}\right)
$$

この行列を正規化して得られる一般アダマール行列を H とすると

$$H = \left(\begin{array}{ccc|ccc|ccc|ccc|ccc|ccc}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&2&2&2&2&2&2&1&1&1&1&1&1\\
0&0&0&0&0&0&1&1&1&1&1&1&2&2&2&2&2&2\\
\hline
0&0&1&1&2&2&0&2&2&1&0&1&1&0&1&2&2&0\\
0&2&2&1&0&1&0&1&0&2&2&1&1&1&0&0&2&2\\
0&1&0&2&2&1&0&0&1&1&2&2&2&0&0&1&2&1\\
\hline
0&0&1&2&1&2&1&0&0&2&2&1&0&0&2&1&1&2\\
0&2&2&1&1&0&1&2&1&2&0&0&2&0&0&2&1&1\\
0&1&0&1&2&2&1&1&2&0&2&0&2&1&2&0&1&0\\
\hline
0&0&1&2&2&1&2&1&1&2&0&0&1&2&2&0&0&1\\
0&2&2&0&1&1&2&0&2&1&0&1&2&1&2&1&0&0\\
0&1&0&2&1&2&2&2&0&1&1&0&1&1&0&2&0&2\\
\hline
0&1&2&0&2&1&1&2&0&0&2&1&0&2&1&2&0&1\\
0&1&2&2&1&0&0&1&2&1&0&2&0&2&1&0&1&2\\
0&1&2&1&0&2&2&0&1&2&1&0&0&2&1&1&2&0\\
\hline
0&2&1&0&1&2&0&2&1&0&1&2&0&1&2&0&2&1\\
0&2&1&1&2&0&2&1&0&0&1&2&2&0&1&1&0&2\\
0&2&1&2&0&1&1&0&2&0&1&2&1&2&0&2&1&0
\end{array}\right)$$

もし, 行列 H において, 成分0,1,2をそれぞれ $\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}, \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$ で置き換えて得られる行列を $L = (L_{ij})_{0\le i,j\le 17}$ とすると, L はある $\mathrm{STD}_6[18;3]$ の正規化された結合行列になる。

一般アダマール行列 H によって定義される対称横断デザインを $\mathcal{D}(H)$ とする。

定理 7.3 位数9の, 基本可換群である, 位数3の elation を含む半正則 (点とブロックに関して) 群を持つ $\mathrm{STD}_6[18;3]$ は同型を度外視して丁度20個ある。それらは, $\mathcal{D}(H_i)\quad (i=1,2,\cdots,11)$ と $\mathcal{D}(H_j)^d\quad (j=1,2,3,4,5,7,8,9,10)$ である。
ここで, $H_i\quad (i=1,2,\cdots,11)$ は Appendix A で与えられる $GF(3)$ 上の18次の一般アダマール行列である。。
$\Omega_i = \Omega(\mathcal{D}(H_i))$ と $\Delta_i = \Delta(\mathcal{D}(H_i))$ をそれぞれ $\mathcal{D}(H_i)$ の点クラスからなる集合, $\mathcal{D}(H_i)$ のブロッククラスからなる集合とする。このとき, 次の表も得る。

i	$\lvert \mathrm{Aut}\mathcal{D}(H_i) \rvert$	Ω_i の軌道分解	Δ_i の軌道分解	正則自己同型群
1	54×3	(3,6,9)	(18)	非存在
2	54×3	(3,6,9)	(9,9)	非存在
3	54×3	(3,6,9)	(9,9)	非存在
4	54×3	(3,6,9)	(9,9)	非存在
5	108×3	(3,6,9)	(9,9)	非存在
6	324×3	(9,9)	(9,9)	非存在
7	432×3	(6,12)	(18)	非存在
8	432×3	(6,12)	(18)	非存在
9	648×3	(9,9)	(18)	非存在
10	1080×3	(3,15)	(18)	非存在
11	12960×3	(18)	(18)	非存在

注意 7.4 (i) 任意の素数べき q に対して, $\mathrm{STD}_2[2q; q]$ が構成されている。([6] の定理 6.33 を見よ。) 特に, $q = 9$ のとき, $\mathrm{STD}_2[18; 9]$ が構成され, これらの $\mathrm{STD}_2[18; 9]$ を縮小する ([6] または [9] を見よ。) ことによって $\mathrm{STD}_2[18; 3]$ が得られる。我々はこれらの STD がすべてお互いに同型で, この STD は $\mathcal{D}(H_6)$ に同型であることをチェックした。
(ii) 我々は $\mathrm{STD}_2[6; 3]$ と $\mathrm{STD}_1[3; 3]$ のテンソル積によって得られる $\mathrm{STD}_2[18; 3]$ が $\mathcal{D}(H_{11})$ に同型であることも調べた。従って定理 7.3 の $\mathcal{D}(H_6)$ と $\mathcal{D}(H_{11})$ を除くすべての STD は新しい STD と考えられる。n_6 を非同型な $\mathrm{STD}_2[18; 3]$ の個数とすると $n_6 \geq 20$ である。
(iii) $\mathcal{D}(H_{11})$ は点集合とブロック集合両方の上で正則に作用する自己同型群を持たない。

8 $\mathrm{STD}_7[21; 3]$

この節では, $\lambda = 7$ のとき, 6 節の続きを考える。すなわち, 位数 3 の elation を含み, 点集合とブロック集合両方の上で半正則に作用する位数 9 の非巡回自己同型群を持つ $\mathrm{STD}_7[21; 3]$ を分類する。

8.1 補題 $(D_{0,0},\ D_{0,1}, \cdots, D_{0,6})$ と $(D_{0,0},\ D_{1,0}, \cdots, D_{6,0})$ の可能性はそれぞれ次の 15 通りである。
(1) $(D_1, D_1, D_2, D_4, D_4, D_5, D_5)$,
(2) $(D_1, D_1, D_3, D_4, D_4, D_5, D_5)$,
(3) $(D_1, D_2, D_2, D_2, D_2, D_4, D_5)$,
(4) $(D_1, D_2, D_2, D_2, D_3, D_4, D_5)$,
(5) $(D_1, D_2, D_2, D_3, D_3, D_4, D_5)$,
(6) $(D_1, D_2, D_3, D_3, D_3, D_4, D_5)$,

(7) $(D_1, D_3, D_3, D_3, D_3, D_4, D_5)$,
(8) $(D_2, D_2, D_2, D_2, D_2, D_2, D_2)$,
(9) $(D_2, D_2, D_2, D_2, D_2, D_2, D_3)$,
(10) $(D_2, D_2, D_2, D_2, D_2, D_3, D_3)$,
(11) $(D_2, D_2, D_2, D_2, D_3, D_3, D_3)$,
(12) $(D_2, D_2, D_2, D_3, D_3, D_3, D_3)$,
(13) $(D_2, D_2, D_3, D_3, D_3, D_3, D_3)$,
(14) $(D_2, D_3, D_3, D_3, D_3, D_3, D_3)$,
(15) $(D_3, D_3, D_3, D_3, D_3, D_3, D_3)$

§7 におけるのと同様な計算をして次の定理を得る。

定理 8.2 位数9の, 基本可換群である, 位数3の elation を含む半正則 (点とブロックに関して) 群を持つ $\mathrm{STD}_7[21;3]$ は同型を度外視して丁度3個ある。それらは, $\mathcal{D}(K_1)$, $\mathcal{D}(K_2)$ と $\mathcal{D}(K_1)^d$ である。
ここで, K_1, K_2 は Appendix B で与えられる $GF(3)$ 上の21次の一般アダマール行列である。
$\Omega_i = \Omega(\mathcal{D}(K_i))$ と $\Delta_i = \Delta(\mathcal{D}(K_i))$ をそれぞれ $\mathcal{D}(K_i)$ の点クラスからなる集合, $\mathcal{D}(K_i)$ のブロッククラスからなる集合とする。このとき, 次の表も得る。

i	$\lvert\mathrm{Aut}\mathcal{D}(H_i)\rvert$	Ω_i の軌道分解	Δ_i の軌道分解	正則自己同型群
1	18×3	(3,9,9)	(3,9,9)	非存在
2	336×3	(21)	(21)	存在

注意 8.3 (i) $\mathcal{D}(K_1)$ と $\mathcal{D}(K_1)^d$ は新しい2つの STD である。
(ii) $\mathcal{D}(K_2)$ は点集合とブロック集合両方の上で正則に作用する自己同型群を持つ。$\mathcal{D}(K_2)$ は [14] で構成された。
(iii) B. Brock と A. Murray [8] は Appendix C で与えられた他の2つの一般アダマール行列 K_3 と K_4 を構成した。$\mathcal{D}(K_i)$ $(i = 3, 4)$ を K_i に対応する $\mathrm{STD}_7[21;3]$ とする。このとき $\mathcal{D}(K_3)$ と $\mathcal{D}(K_4)$ は共に self dual で, 次の表を得る。

i	$\lvert\mathrm{Aut}\mathcal{D}(H_i)\rvert$	Ω_i の軌道分解	Δ_i の軌道分解	正則自己同型群
3	12×3	(1,2,3,3,12)	(1,2,3,3,12)	非存在
4	16×3	(1,4,8,8)	(1,4,8,8)	存在

(iv) 従って n_7 を非同型な $\mathrm{STD}_7[21;3]$ の個数とすると, $n_7 \geq 5$ である。

参考文献

[1] K. Akiyama and C. Suetake, On $STD_{\frac{k}{3}}[k;3]$'s, *Discrete Math.* **308**(2008), 6449–6465.

[2] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Volumes I and II, Cambridge University Press, Cambridge (1999).

[3] B. Brock and A. Murray, A personal communication.

[4] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, Second Edition, Chapman & Hall/CRC Press, Boca Raton (2007).

[5] H. Haemers, Conditions for singular incidence matrices, *J. Algebraic Combin.* **21**(2005), 179–183.

[6] A. S. Hedayat, N. J. A. Sloane, and John Stufken, *Orthogonal Arrays*, Springer-Verlag New York (1999).

[7] Y. Hiramine, Modified generalized Hadamard matrices and construction for transversal designs, preprint.

[8] T. C. Hine and V. C. Mavron, Translations of symmetric and complete nets, *Math. Z.* **182**(1983), 237–244.

[9] Y. Hiramine and C. Suetake, A contraction of square transversal designs, *Discrete Math.* **308**(2008), 3257–3264.

[10] Y. J. Ionin and M. S. Shrikhande, *Combinatorics of Symmetric Designs*, Cambridge University Press, Cambridge (2006).

[11] D. Jungnickel, On difference matrices, resolvable transversal designs and generalized Hadamard matrices, *Math. Z.* **167**(1979), 49–60.

[12] V. C. Mavron and V. D. Tonchev, On symmetric nets and generalized Hadamard matrices from affine design, *J. Geom.* **67**(2000), 180–187.

[13] C. Suetake, The classification of symmetric transversal designs $STD_4[12;3]$'s, *Des. Codes Crypt.* **37**(2005), 293–304.

[14] C. Suetake, The existence of a symmetric transversal design $STD_7[21;3]$, *Des. Codes Crypt.* **37**(2005), 525–528.

[15] V. D. Tonchev, *Combinatorial Configurations*, PitmanMonographs and Survey's in Pure and Applied Mathematics, Longman Scientific and Technical, Essex (1988).

追記 Appendix A は紙数の関係上省かせていただきます。Tonchev は我々が構成した $\mathrm{STD}_6[18;3]$ を新しい興味ある 2-デザインに拡大することを試みたそうですが, 多くのものは知られたものだったそうです。彼が用いた方法は, $\mathrm{STD}_1[q;q]$ を位数 q のアファイン平面に拡大する方法の一般化であることを最近知り, とても驚きました。(多くのデザインの専門家はご存知でしょうが。) 我々は, 現時点では我々の方法を用いて新しい STD の無限系列の構成に成功していませんが, 熊本大の平峰先生は我々の方法を一般化し興味ある $\mathrm{STD}_q[q;q]$ (q は任意素数べき) の無限系列を構成されました。また, 国際基督教大の鈴木寛先生は一般アダマール行列とアソシエーションスキームとの関係を指摘されました。我々の研究に興味を持って頂いた方々に感謝いたします。

Appendix B

$K_1 =$

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	2	1	0	2	1	0	2	1	0	2	2	2	2	1	1	1
0	0	0	0	1	2	0	1	2	0	1	2	0	1	2	1	1	1	2	2	2
0	0	1	0	0	1	2	2	2	2	2	0	1	2	0	1	0	1	2	1	1
0	2	2	1	2	1	2	1	0	0	1	0	0	0	0	2	2	1	1	2	1
0	1	0	0	2	2	2	0	1	2	1	1	2	1	0	1	2	2	0	0	1
0	0	1	0	2	1	1	1	1	1	2	1	2	0	2	2	0	0	0	2	2
0	2	2	1	2	0	1	0	2	1	0	0	2	1	1	1	0	1	2	0	2
0	1	0	2	2	2	1	2	0	2	2	0	0	0	1	1	1	0	1	1	2
0	0	1	1	2	0	2	2	1	0	1	2	2	0	1	0	1	2	2	1	0
0	2	2	0	0	0	1	1	0	2	2	2	1	1	1	0	1	2	0	2	1
0	1	0	2	1	0	2	2	1	1	0	2	0	2	1	2	0	1	0	2	1
0	0	1	2	1	1	0	0	0	2	2	2	2	1	1	2	2	1	1	0	0
0	2	2	1	1	2	0	2	1	2	1	0	1	1	2	2	0	0	0	1	0
0	1	0	1	2	1	0	1	2	2	0	1	1	2	1	0	2	0	2	2	0
0	1	2	0	0	0	0	2	0	1	1	1	2	2	2	0	2	1	1	1	2
0	1	2	2	1	0	2	1	2	0	2	1	1	0	2	1	0	2	1	0	0
0	1	2	2	0	1	1	0	1	0	1	2	1	2	0	2	1	0	2	0	2
0	2	1	1	1	2	2	0	0	1	2	1	0	2	2	0	1	0	2	0	1
0	2	1	2	0	2	0	1	1	1	0	0	2	2	0	1	1	2	1	2	0
0	2	1	2	1	1	1	2	2	0	0	1	0	1	0	0	2	2	1	1	2

$K_2 =$

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	2	1	0	2	1	0	2	0	1	2	2	2	2	1	1	1
0	0	0	0	1	2	0	1	2	0	1	2	2	1	0	1	1	1	2	2	2
0	0	1	0	2	1	1	1	0	2	2	2	1	0	2	2	0	1	1	0	2
0	2	2	1	2	0	0	0	2	2	1	0	1	1	1	2	0	1	2	1	0
0	1	0	2	2	2	1	1	0	2	0	1	2	0	1	1	2	0	2	1	0
0	0	1	1	2	1	2	2	2	1	1	1	0	0	2	0	1	0	2	2	0
0	2	2	1	0	0	2	1	0	1	0	2	1	0	1	1	1	2	0	2	2
0	1	0	2	2	0	2	0	1	1	2	0	2	0	0	2	1	1	1	2	1
0	0	1	2	1	0	0	2	1	0	2	2	1	0	1	0	2	2	2	1	1
0	2	2	0	1	2	1	2	0	2	2	0	0	1	1	0	1	0	1	2	1
0	1	0	1	1	1	2	2	2	2	0	2	2	2	1	0	0	1	0	0	1
0	2	0	2	2	2	1	2	1	1	1	1	1	1	0	0	0	2	0	0	2
0	0	2	0	2	1	2	1	1	2	1	0	0	2	0	1	2	2	0	1	1
0	1	1	0	1	2	0	0	1	2	0	1	1	2	2	2	1	2	0	2	0
0	1	2	0	0	0	0	2	0	1	1	1	2	2	2	0	2	1	1	1	2
0	1	2	2	1	0	2	1	2	0	2	1	0	1	2	1	0	2	1	0	0
0	1	2	2	0	1	1	0	1	0	1	2	0	2	1	2	1	0	2	0	2
0	2	1	1	0	2	0	1	1	1	2	0	2	2	2	1	0	0	2	0	1
0	2	1	2	0	1	1	2	2	0	0	0	1	2	0	1	2	1	1	2	0
0	2	1	1	1	1	2	0	0	0	2	1	2	1	0	2	2	0	0	1	2

Appendix C

$K_3 =$

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	1	1	1	1	1	1	2	2	2	2	2	2	2
0	0	0	0	0	0	1	0	2	2	2	2	2	2	1	1	1	1	1	1	2
0	1	0	2	2	1	1	0	0	0	1	1	2	2	0	2	0	1	2	2	1
0	0	2	2	1	1	2	1	2	1	0	1	0	2	2	1	0	1	0	0	2
0	2	1	1	2	0	1	2	0	1	0	0	1	2	0	1	1	2	2	0	2
0	0	2	1	2	2	1	1	0	1	2	1	2	0	2	0	1	0	1	2	0
0	1	2	2	1	0	2	0	0	1	2	2	1	1	1	0	0	2	2	1	0
0	0	1	1	2	2	1	0	1	2	0	2	0	1	2	2	0	2	0	1	1
0	1	2	0	1	2	1	2	1	2	1	0	0	0	1	1	0	0	2	2	2
0	0	2	0	1	1	2	2	1	0	2	0	2	1	0	2	1	2	1	0	1
0	2	1	2	1	0	0	1	2	2	2	1	0	0	0	2	1	0	2	1	1
0	2	2	1	0	1	0	2	1	0	1	2	0	2	2	0	1	1	2	1	0
0	2	0	1	1	2	2	1	0	2	1	0	2	1	0	0	2	1	0	1	2
0	2	0	2	1	2	1	1	1	0	0	2	1	2	1	2	2	0	1	0	0
0	2	1	0	2	1	2	0	2	1	1	2	0	1	0	1	2	0	1	2	0
0	1	1	2	2	1	0	0	1	2	2	0	1	0	2	0	2	1	1	0	2
0	1	1	0	0	2	2	2	0	0	2	1	1	2	2	1	2	0	0	1	1
0	1	1	2	0	2	0	2	2	1	0	0	2	1	1	2	1	1	0	2	0
0	1	2	1	2	0	0	1	2	0	1	2	2	0	1	1	2	2	0	0	1
0	2	0	1	0	1	2	2	2	2	0	1	1	0	1	0	0	2	1	2	1

$$K_4 = \begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&1&1&1&1&1&1&1&2&2&2&2&2&2&2\\
0&0&0&0&0&0&1&2&2&2&2&2&2&0&1&1&1&1&1&1&2\\
0&0&1&1&0&2&2&2&2&1&1&0&0&2&1&1&0&0&2&2&1\\
0&0&2&2&1&2&1&2&2&0&0&1&1&1&1&1&2&2&0&0&0\\
0&0&2&2&1&1&1&0&0&1&1&2&2&0&0&0&1&2&2&2&1\\
0&0&1&1&2&2&2&0&0&2&2&1&1&1&0&0&0&2&1&1&2\\
0&1&2&1&2&0&1&1&2&0&2&0&1&0&0&2&2&0&2&1&1\\
0&1&2&0&0&1&2&1&2&2&0&1&0&2&2&0&1&2&0&1&1\\
0&1&0&2&2&1&0&0&2&2&1&0&1&2&1&0&2&1&1&2&0\\
0&1&2&1&2&1&0&2&1&1&0&0&2&0&2&1&0&2&1&0&2\\
0&1&1&2&0&2&1&1&0&1&0&2&0&2&0&2&2&1&1&0&2\\
0&1&0&2&1&2&0&2&1&0&2&2&0&1&2&0&0&1&2&1&1\\
0&1&1&0&2&2&2&2&1&0&1&1&2&0&0&2&1&1&0&2&0\\
0&2&0&1&1&0&2&0&1&2&0&1&2&2&0&1&2&1&2&0&1\\
0&2&1&2&1&0&2&1&2&0&1&0&2&1&2&0&1&0&1&0&2\\
0&2&2&1&2&0&1&1&0&2&1&2&0&1&2&1&0&1&0&2&0\\
0&2&1&2&0&1&2&0&1&1&2&2&1&0&2&1&2&0&0&1&0\\
0&2&2&0&1&1&1&0&1&0&2&1&0&2&1&2&0&0&1&2&2\\
0&2&1&0&2&1&0&2&0&2&0&2&1&1&1&2&1&0&2&0&1\\
0&2&0&1&1&2&0&1&0&1&2&0&2&2&1&2&1&2&0&1&0
\end{pmatrix}$$

最近の統計学における代数的諸問題について

竹村 彰通*†

概 要

本稿では計算代数統計で扱われる問題について，簡単な例題などを用いて紹介する．

1 はじめに

計算代数統計にかかわるようになってからすでに10年近い時間がたった．そのきっかけは2001年の春頃にDiaconis-Sturmfelsの論文([10])のグレブナー基底，特に3×3×3分割表の無3因子交互作用モデルの正確検定のためのグレブナー基底の形について，青木敏君から説明を受けて不思議な印象があり，考え始めたという偶然的なものであった．計算代数統計に関してはすでに何回か紹介の機会を与えられている([2], [22], [23], [26], [24])．本稿では，いくつかの研究集会でお話させていただいたことなどをもとに，簡単な例題などを用いて計算代数統計の話題についてあらためて紹介する．また，本稿は，日本統計学会誌和文誌への投稿論文([25])ともかなり重複があることをお断りしておく．

以下，2節では，計算代数統計の一つの発端であるPistone-Wynn流の実験計画について説明する．また3節では，壷のモデルという離散確率分布を考える際の最も基本的な考え方に戻って，分割表のマルコフ基底に関する考え方を説明する．

2 Pistone-Wynn 流の実験計画

この節では，伝統的な一部実施要因計画の割付けや別名関係などの数学的な構造を，Pistone-Wynn流の計算代数統計([17, 18])の観点から眺めることにより，計算代数統計への動機づけを与える．以下では説明の簡単のために，おもに各要因の水準が2水

*東京大学大学院情報理工学系研究科
†JST CREST

準である場合について説明する．ただし，多項式環の手法を用いれば水準数が2以外の場合も同様に扱うことができる．

各要因の水準が2水準であるような多因子要因実験の一部実施法は，Wu and Hamada (2000) などの実験計画法の教科書で標準的に解説されている．一方，奥野・芳賀 (1969) の8章には以下のような記述があり，田口玄一などのわが国の貢献が強調されている．

> 多因子実験の計画と解析は，「直交表」を用いることによって，きわめてエレガントにおこなうことができる．これは，わが国独特の手法であって，田口玄一氏等に負うものである．諸外国では，いまだに直交表を用いず，面倒な割付け方をしているために，この有用な手法の普及がたいへん遅れている．

一部実施要因計画の別名関係の扱いには，いかにも代数的な感じがする．しかしながら，この「代数的な感じ」が，実は多項式環のイデアルの操作に対応することについては，私自身は [3] の改訂作業おいてようやく気がついた．それ以前にマルコフ基底の研究の中で，多項式環のイデアルの操作にはかなり慣れていたはずであったが，Pistone-Wynn 流の実験計画の考え方も同様であることにはなかなか気がつかなかった．ただし，Pistone, Riccomagno and Wynn (2000) の本での説明も，やや形式的に過ぎる部分があり，標準的な一部実施要因計画との関連がわかりにくいことは事実であると思う．文献としても，このあたりの明確な記述は Pistone 等の本より後になってであり，1) 2水準系の議論は Fontana et al. [13]，2) より一般の場合は Pistone and Rogantin (2008)，で明らかにされて来ている状況と考えられる．

2.1 2水準系の一部実施計画の基本 (乗法型の記法)

まず，2水準系の一部実施計画の基本について教科書的な説明を与えよう．ある製品の製造工程において，製品の品質に影響を与える要因として，温度や圧力などいくつかの要因が考えられるとする．具体例のために，要因数を6とし，それらの要因を A, B, C, D, E, F とする．それぞれの要因を「低水準」と「高水準」のいずれかに設定して実験をおこなうこととする．「積型」の記法では，高水準を $+1$ (あるいは簡単に $+$)，低水準を -1 (あるいは $-$) と表すこととする．

水準のすべての組合せを行うとすると，$64 = 2^6$ 回の実験が必要となる．そこで，実験回数を 1/4 の16回で済ませることを考える．このような実験を 2^{6-2} design という．そして，1/4 に減らすための「定義対比」として次の二つを考える:

$$I = ABE, \quad I = ACDF \tag{1}$$

表 1: 2^{6-2} 計画の例

A	B	C	D	E	F
+	+	+	+	+	+
+	+	+	−	+	−
+	+	−	+	+	−
+	+	−	−	+	+
⋮	⋮	⋮	⋮	⋮	⋮
−	−	−	+	+	+
−	−	−	−	+	−

例えば，$I = ABE$ の意味は，A, B, C のそれぞれの水準 (± 1) をかけ合わせた時に，それらの積が $+1$ となるように水準の組合せが定まっていることを意味する．このルールに従えば，$A = B = +1$ の時には $E = +1$ と「割り付け」る．

いま，それぞれの水準は ± 1 であるから，2乗すると常に $+1$ である．そこで

$$A^2 = B^2 = C^2 = D^2 = E^2 = F^2 = I \tag{2}$$

という操作のルールを定める．そして，(1) の第1式の両辺には E をかけ，(1) の第2式の両辺に F をかけると

$$E = AB, \quad F = ACD \tag{3}$$

と書き直すことができる．この第一式のルールは，要因 E の水準を A, B の積として定めることを示している．A, B, C, D の水準をまず自由に $2^4 = 16$ 通りの組合せでおこない，E,F の水準をそれぞれ (3) 式のように定めてやると，16回の実験の水準の組合せの設定は表1のようになる．ただし，紙面の節約のために16行のうち6行のみを示している．

さて (2) 式のルールのもとで (1) の二つの式を辺々かけあわせると

$$I = ABE = ACDF = BCDEF \tag{4}$$

という関係を得る．I を含むようなこのような関係を contrast subgroup と言う．I を含まない等号関係としては，(4) 式に例えば A をかけることによって

$$A = BE = CDF = ABCDEF$$

などを得る．このような関係を「別名関係」という．統計的には，これらの4個の主効果および交互作用が一部実施のために完全に「交絡」しており，別々には推定できないことを意味している．

2.2 加法型への書き換えと線形符号との同値性

ここでは前節の例を加法型に書き換えることにより2水準系の一部実施計画と線形符号の同値性を説明しよう．前節では水準を ± 1 とし，水準の組合せの演算を AB などの積の形で表した．しかしながら数学的には 2 を法とする加法の演算を考えたほうが，議論はある意味では明確となる．それは，2 を法とする加法と乗法により $\mathbb{F}_2 = \{0,1\}$ が「体」をなしており，$\mathbb{F}_2$ の要素からなるベクトルを通常の線形代数の手法で扱うことができるからである．いま「高水準」と「低水準」を 0 および 1 で符号化する．つまり

$$+ \ \to \ 0, \qquad - \ \to \ 1$$

と符号化を変えてやる．そうすると，前節の積の演算が mod 2 での "exclusive or" の加法の演算と同じであることがわかる．

前節の 2^{6-2} design の例で，6個の factor の水準を6個の「ビット」と考え $x_1, \ldots, x_6$ と表す．まず最初の4ビットについては full factorial (完全実施計画) の形に書く．このことは，最初の4ビットはそのまま「送信する」ことを意味している．5ビット目と6ビット目は，誤り訂正のために一定のルールで値を定めて付加する．(3) 式を加法的に表せば

$$\begin{aligned} x_5 &\equiv x_1 + x_2 \qquad (\mathrm{mod}\ 2) \\ x_6 &\equiv x_1 + x_3 + x_4 \qquad (\mathrm{mod}\ 2) \end{aligned}$$

となる．つまり最初の4ビットの1の数の偶奇を求め，それに応じて5ビット目と6ビット目を定めることとなる．最初の4ビットのすべての組み合わせについて実行すれば以下となる．ただし紙面の節約のために16行のうち6行のみを示す．

$$\begin{array}{cccc|cc} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 \end{array} \tag{5}$$

これが表1と全く同じ形であることは明らかである．

すでに述べたように，加法型に書くことのメリットは，一部実施計画を有限体上の通常の線形代数によって理解できる点にある．2元体 $\mathbb{F}_2 = \{0,1\}$ の元を要素とする p 次元のベクトルについて，要素ごとに mod 2 で演算をおこなうことによって，$\{0,1\}^p$ は $\mathbb{F}_2$ 上

の線形空間となる．この観点からは contrast subgroup $I = ABE = ACDF = BCDEF$ は

$$\{(0,0,0,0,0,0),\ (1,1,0,0,1,0),\ (1,0,1,1,0,1),\ (0,1,1,1,1,1)\}$$

の 4 点からからなる 2 次元の線形部分空間 L であり，その基底として $I = ABE = ACDF$ の 2 本のベクトル

$$(1,1,0,0,1,0),\ (1,0,1,1,0,1)$$

をとる事ができる．そして (5) 式の行からなる 16 点は L の直交補空間である．

2.3 積型記法のメリット

前節のように説明すると，いかにも加法型の記法のほうが数学的に見通しがよい感じを受ける．それに対して，2.1 節の積型の記法は「単なる説明」のように見える．私自身は長い間そのような印象を持っていた．しかし実は積型の記法のほうがより代数的なのである．

そもそも Diaconis-Sturmfels 流のマルコフ基底に関する計算代数統計を勉強しはじめた時に，分割表を単項式 (monomial) に対応させること自体が不思議な感じがした．move を考える時に，負の要素をなぜ負のべきに対応せずに，monomial の差として表すのか，がわからなかった．monimial の記法は「積型」である．積型に書いて，はじめて代数の手法が使えるわけである．Pistone-Wynn 流の実験計画の代数統計でも同じことが起きていることに長い間気がつかなかった．

2.1 節の積型記法の代数的な説明は次のように簡単なものである．いま A, B, C, D, E, F の 6 個の文字を「不定元」と考えて，これらの不定元からなる多項式環 $k[A, B, C, D, E, F]$ を考える．k は適当な体でよい．$k[A, B, C, D, E, F]$ の中に，次の 8 個の多項式で生成されるイデアルを考える．

$$I = \langle A^2 - 1, B^2 - 1, C^2 - 1, D^2 - 1, E^2 - 1, F^2 - 1, ABE - 1, ACDF - 1 \rangle$$

Pistone and Wynn の用語では "design ideal" である．16 回の実験は I の零点集合として与えられる．2.1 節の形式的な操作は，商環 $k[A, B, C, D, E, F]/I$ の操作と全く同じである．2 個の monomial が別名関係にあるための必要十分条件は，それらの差が design ideal I に属することである．例えば

$$BE - ABCDEF \in I$$

である．この観点に立てば，Pistone-Wynn の言うように，例えば別名関係の判定はイデアル帰属問題であるから，I のグレブナー基底を求めておけば別名関係が判定でき

ることになる．いずれにしても，ここで強調すべき点は2.1節のような積型の記法での一部実施計画の説明が便宜的なものではなく，代数的に由緒正しいものであるということである．このことは，積型の記法がなぜ加法型の記法によって駆逐されなかったのか，ということの理由にもなっていると思われる．

以上述べてきた2水準系の場合では，$(+,-) \leftrightarrow (0,1)$ の対応がいかにも単純で，どちらで考えても同じではないかと思われるかも知れない．しかしながら，例えば3水準の実験を考える場合にはより本質的な差が見えてくるのである ([3])．

また，積型の記法のメリットとして，non-regular な一部実施計画を統一的に扱うことができるという点があげられる．(4) 式のような contrast subgroup を用いて水準の組み合わせを指定する計画を regular fractional factorial design とよぶ．このような形に表されない計画を non-regular fractional factorial design とよぶ．現状では，一部実施計画の理論は regular な場合にかたよっており，non-regular な実験計画の研究は重要な課題である．

例えば Pistone, Riccomagno and Wynn の本の 4.6 節には2水準の要因が5個の場合に，"indicator function" f を

$$\begin{aligned} f(x_1,\ldots,x_5) &= \frac{1}{2} + \frac{1}{4}x_1x_2x_4 - \frac{1}{4}x_1x_2x_3 + \frac{1}{4}x_1x_2x_4x_5 + \frac{1}{4}x_1x_2x_3x_5 \\ &= \frac{1}{2} + \frac{x_1x_2\big(x_4(x_5+1) + x_3(x_5-1)\big)}{4} \end{aligned}$$

と定義し，16回の実験の水準の組み合わせを，

$$I = \langle x_1^2 - 1, \ldots, x_5^2 - 1, f(x_1,\ldots,x_5) - 1 \rangle \tag{6}$$

の零点集合として選ぶ例が示されている．Fontana et al. (2000) によって，任意の一部実施計画が indicator function f を用いて (6) 式の形のイデアルの零点集合として与えられることが示されている．Indicator function の考え方は non-regular design の研究に大変有用であり，[5] では indicator function の性質を用いて，どんな regular fractional factorial design の部分集合ともならないような実験計画の性質を調べている．

3　壷のモデルから見たマルコフ基底

この節では，壷のモデルという離散確率分布を考える際の最も基本的な考え方がマルコフ基底の理解にも有用であることを説明する．2元分割表についての例題をまじえながら，グレブナー基底，sorting, 対称群の作用などについて述べる．さらに多元分割表の分解可能モデルへの拡張も指摘する．

3.1　2元分割表と北西隅ルール

まず次の簡単な 3×3 分割表の例題を考えよう.

例題1　周辺頻度が以下のように与えられている分割表の中身をうまくうめよ.

表 2: 3×3 周辺表の例

*	*	*	6
*	*	*	5
*	*	*	5
7	5	4	16

解答例: 行優先で右下からうめることを考える. まず右下を $\min(4,5) = 4$ とする.

*	*	*	6
*	*	*	5
*	*	4	1
7	5	0	12

この段階で, 実は3列目が $(0\ 0\ 4)^T$ となることは見えているが, 行優先の時にはそこはまだ確定しないことにする. そこで次に (3,2) 要素を $\min(1,5) = 1$ でうめると (3,1) 要素も 0 となり

*	*	*	6
*	*	*	5
0	1	4	0
7	4	0	11

となる. さらに (2,3) 要素を $\min(0,5) = 0$ とし, 続いて他の2行目をうめると

*	*	*	6
1	4	0	0
0	1	4	0
6	0	0	6

となり, 結果は

6	0	0	0
1	4	0	0
0	1	4	0
0	0	0	0

となる.

一方最後の列から，列優先でうめる方法を考える．第3列が下から上へ

*	*	0	6
*	*	0	5
*	*	4	1
7	5	0	12

とうまり，次に第2列が下から上へ

*	0	0	6
*	4	0	1
*	1	4	0
7	0	0	7

と定まり，結局同じ表に到達する． (解答例終)

以上の例が示唆していることは次のことである．右下の要素からできるだけ大きい値を入れて行く操作は，グレブナー基底の観点からは revlex 式の項順序 (term order) を考えていることにあたる．そして，2元表においては，列優先の revlex でも行優先の revlex でも，結果が同じになる．結果表はグレブナー基底による割り算の「余り」(standard monomial) にあたる．つまり2元表においては，二つの異なる term order に基づいて実際に割算を行うと，常に同じ standard monomial に到達する．また，最適化の観点からは，異なる term order が同じ最適解を与える例となっている．

最適化された解は，対角付近に頻度が集まっており，順位相関を最大化していると見ることもできる．このような解は，離散最適化の分野で「北西隅ルール」(Northwest corner rule) とよばれている．北西隅ルールは列の周辺分布を行の周辺分布に変換する「輸送問題」の許容解であり，もし輸送コストが "Monge 性" と呼ばれる性質を持つ時は，コストを最小化した解となっている事が知られている．これらの点については松井知己氏よりご教示いただいた．

3.2 添字の sorting による方法

次に添字の sorting の方法を上の例を用いて説明する．Sorting の方法は Sturmfels の本 ([21]) の 14 章にあり，さらに大杉・日比により発展されている方法である ([6, 7]

を参照). Sorting の操作は，グレブナー基底の理論で現れるものであるが，他の分野ではあまり見かけない操作のように思われる．

同時頻度をうめた次の表をもとに考える．

3	2	1	6
2	1	2	5
2	2	1	5
7	5	4	16

これを単項式に対応させる:

$$x_{11}^3 x_{12}^2 x_{13} x_{21}^2 x_{22} x_{23}^2 x_{31}^2 x_{32}^2 x_{33}$$

行の添字のみ集めてくると，周辺頻度より

1が6個，2が5個，3が5個

である．列の添字は同様に

1が7個，2が5個，3が4個

である．ここで，列の添字のほうが，グループとして，行の添字より後と考える．例えば，列の添字に 3 を加えて x_{ij} を $x_{i,j+3}$ と表す．この場合，例えば x_{11} を x_{14} と表すことになる．そうしたうえで，行の添字と列の添字を区別せずに sort すると

1 1 1 1 1 1 2 2 2 2 2 3 3 3 3 3 4 4 4 4 4 4 4 5 5 5 5 5 6 6 6 6

となる．ここで，x_{ij} の1桁目の i の部分に上の数字を左から順にうめていく:

$$x_{1?}x_{1?}x_{1?}x_{1?}x_{1?}x_{1?}x_{2?}x_{2?}x_{2?}x_{2?}x_{2?}.x_{3?}x_{3?}x_{3?}x_{3?}x_{3?}$$

ここで一巡したので，つぎに後半を2桁目にうめていく

$$x_{14}x_{14}x_{14}x_{14}x_{14}x_{14}x_{24}x_{25}x_{25}x_{25}x_{25}x_{35}x_{36}x_{36}x_{36}x_{36}$$

ここで，$4,5,6 \to 1,2,3$ と添字を戻すと

$$x_{11}^6 x_{21} x_{22}^4 x_{32} x_{33}^4$$

となり，sorting を一回施すだけで最適化の解を得る．

3.3 2元表と壷のモデル

前節の sorting は実は壷のモデルで考えるとわかりやすい．例題1を次のように書き換える．

例題2　いま，壷の中に，1から16まで番号のふった16枚のカードがあるとする．各カードには2桁の数字を書く欄がある．ここにこれから数字を書いていく．それぞれの欄とも 1,2,3 のいずれかの数字を書く．そして，第1桁には

1を書くカードは6枚
2を書くカードは5枚
3を書くカードは5枚

とせよ．また第2桁には

1を書くカードは7枚
2を書くカードは5枚
3を書くカードは4枚

とせよ．このような数字のうめ方で，最も規則的で簡単な方法を示せ．

解答例: 第1桁には，カードの番号順に，1を6枚に書き，2を5枚に書き，3を残りの5枚に書く．第2桁も同様に書く．

Sorting は，同時頻度からまず添字を sort することによって周辺頻度を得て，それから例題2の方法で数字をうめ直していることにあたっている．さらに，グレブナー基底の観点から重要な事実，すなわち2元表の場合には平方自由な2次の2項式からなるグレブナー基底が存在すること，に対応して次が成り立つ．

例題3　以上のような16枚への数字のうめ方と異なるうめ方をした場合，必ず2枚のカードを選ぶことができ，第2桁の数字をとりかえることによって，規則的なうめ方に近づけることができることを示せ．

第2桁の数字をとりかえることは，個票データの秘匿措置における swapping に対応する([27]). Swapping は，次数が2の move に密接に対応している．それは swapping を分割表の頻度で考えれば，$\begin{smallmatrix}+1 & -1\\ -1 & +1\end{smallmatrix}$ の形の move となるからである．standard monomial に近づけるように swapping することは，グレブナー基底の要素での割算に対応している．

3.4　壷への対称群の作用

独立モデルのもとで周辺を与えた $I \times J$ の2元分割表の条件つき分布は超幾何分布であり，確率関数は

$$\frac{\prod_{i=1}^{I} x_{i+}! \prod_{j=1}^{J} x_{+j}!}{n! \prod_{ij} x_{ij}!}$$

の形で与えられる．この分布からの直接のサンプリングは，壷のモデルを考えると以下のように簡明である．この簡単な事実が対称群 S_n の作用として理解できることは，北海道大学の吉田知行教授により指摘されている．

いま表2のように周辺が所与として，超幾何分布に従って2元表を発生させたいとする．そのために，1から16までの連番と2桁の欄(当初は空白)がある16枚のカードを壷に入れる．そして，壷の中をよく混ぜてから，順番にカードを取り出して，まず第1桁目には

6枚のカードに 1
5枚のカードに 2
5枚のカードに 3

と順にうめていく．次に，カードを壷にもどして再度よく混ぜてから第2桁目には

7枚のカードに 1
5枚のカードに 2
4枚のカードに 3

と順にうめる．これで分割表がランダムに生成できて，その分布は超幾何分布である．

さて，以上では壷の中を2回まぜているが，これは対称群 S_n, $n = 16$, をそれぞれの桁に独立に作用させていると理解することができる．すなわち $S_n \times S_n$ がカードの集合に作用している．ただし，2元表の場合は，実は1回目の混合操作は不要なことは明らかである．すなわちこの場合には S_n を1回だけ第2桁に作用させればよい．

第2回目の混合操作を省略して，規則的にうめれば，前節で述べた sorting となり，北西隅型の standard monomial が得られている．

以上のように，2元表の超幾何分布の場合には，対称群上の一様分布に対応させることにより，超幾何分布からの直接の sampling が可能である．しかしながら，一般にはMCMC のほうが適用範囲が広いので $\begin{smallmatrix} +1 & -1 \\ -1 & +1 \end{smallmatrix}$ の形の move を用いた MCMC を考察してみる．そうすると，吉田知行教授によって指摘されているように，この move を元の壷に引き戻して考えれば，実は S_n の生成元である互換をランダムに作用させていることがわかる．このように S_n に引き戻して考えると，分割表のファイバー上の MCMC が，S_n の互換によって生成されるランダムウォークに対応していることがわかる．そして，S_n 上のランダムウォークの収束速度の評価は，Diaconis の仕事([9]) にあるように，対称群の表現の指標を用いて解析することができる．

3.5 分解可能モデルへの一般化

ここまでの2元表の議論のほとんどは一般の分解可能モデルに素直に一般化される．ただし，以下では $2 \times 2 \times 2 \times 2$ の一例を示すことにとどめる．いま固定する周辺を $\{1,2\},\{2,3\},\{3,4\}$ とする．

例題4　壷の中に1から16まで番号のふった16枚のカードがあるとする．各カードには4桁の数字を書く欄がある．ここにこれから数字を書いていく．それぞれの欄とも1,2のいずれかの数字を書く．そして
第(1,2)桁には
　　(1,1)の組合せが6枚，(1,2)が3枚，(2,1)が2枚，(2,2)が5枚
第(2,3)桁には
　　いずれの組合せも4枚づつ
第(3,4)桁には
　　(1,1)の組合せが3枚，(1,2)が5枚，(2,1)が3枚，(2,2)が5枚
になるようにせよ．このような数字のうめ方で，最も規則的で簡単な方法を求めよ．

解答例: (1,2)桁は単に順にうめて行く．(2,3)桁は，2桁目の数字があうカードを順にひろいながら，3桁目を順にうめて行く．(3,4)桁は，3桁目の数字があうカードを順にひろいながら，4桁目を順にうめて行く．

次の例題は実はかなり難しい．
例題5　以上のような数字のうめ方と異なるうめ方をした場合，必ず2枚のカードを選ぶことができて，書いてある数字を入れ換えることによって，必ず以上のうめ方に近づくことができることを示せ．

例題6　例題4と同じ周辺頻度を持つ表を，超幾何分布から直接サンプリングするにはどうすればよいかを示せ．

解答例: (1,2)桁は単に順にうめて行く．(2,3)桁は，2桁目の数字によって壷を部分壷に層別して，部分壷ごとに混ぜる．(3,4)桁は，3桁目の数字によって壷を部分壷に層別して，部分壷ごとに混ぜる．

例題5は，分解可能モデルには2次のsquare-free binomialからなるグレブナー基底が存在することに対応している．例題6をMCMC版に焼直せば，MCMCの収束速度の解析も可能になると予想される．

参考文献

[1] Satoshi Aoki and Akimichi Takemura. (2006). Markov chain Monte Carlo tests for designed experiments. arXiv:math/0611463v1. Submitted for publication.

[2] 青木 敏・竹村彰通．統計学とグレブナー基底 – 計算代数統計の発端と展開．数学，第59巻第3号，283–302. 2007.

[3] Satoshi Aoki and Akimichi Takemura. (2007). Markov basis for design of experiments with three-level factors. arXiv:0709.4323v2. To appear in *Algebraic and Geometric Methods in Statistics* dedicated to Professor Giovanni Pistone, Cambridge University Press (P. Gibilisco, E. Riccomagno, M.P. Rogantin and H.P. Wynn, eds.)

[4] Satoshi Aoki and A.Takemura. (2008). The largest group of invariance for Markov bases and toric ideals. *Journal of Symbolic Computation*, **43**, 342–358.

[5] Satoshi Aoki and Akimichi Takemura. Some characterizations of affinely full-dimensional factorial designs. *Journal of Statistical Planning and Inference.* doi:10.1016/j.jspi.2009.04.002. 2009.

[6] Aoki, S., Hibi, T., Ohsugi, H. and Takemura, A. (2007a). Markov basis and Groebner basis of Segre-Veronese configuration for testing independence in group-wise selections. arXiv:0704.1074v2. To appear in *Annals of the Institute of Statistical Mathematics*,

[7] Aoki, S., Hibi, T., Ohsugi, H. and Takemura, A. (2008). Gröbner bases of nested configurations. *Journal of Algebra*, **320**, 2583–2593.

[8] Colbourn, Charles J. and Dinitz, Jeffrey H. (2007). *Handbook of Cmbinatorial Designs*, 2nd ed., Chapman & Hall/CRC, Boca Raton.

[9] Diaconis, P. (1988). *Group Representations in Probability and Statistics*, Lecutre Notes-Monograph Series, Vol.11, Institute of Mathematical Statistics, Hayward, California.

[10] Diaconis, P. and Sturmfels, B. (1998). Algebraic algorithms for sampling from conditional distributions. *Annals of Statistics*, **26**, 363–397.

[11] A. Dobra and S. Sullivant. A divide-and-conquer algorithm for generating Markov bases of multi-way tables. *Comput. Statist.*, 19:347-366, 2004.

[12] Roberto Fontana and Maria-Piera Rogantin. (2009). Indicator function and sudoku designs. To appear in *Algebraic and Geometric Methods in Statistics* dedicated to Professor Giovanni Pistone, Cambridge University Press (P. Gibilisco, E. Riccomagno, M.P. Rogantin and H.P. Wynn, eds.)

[13] Roberto Fontana, Giovanni Pistone and Maria-Piera Rogantin. (2000). Classification of two-level factorial fractions. *J. Statist. Plann. Inference*, **87**, 149–172.

[14] H. Hara and A. Takemura. (2009). Connecting tables with zero-one entries by a subset of a Markov basis. arXiv:0908.4461v1

[15] S. Hoşten and S. Sullivant. Gröbner bases and polyhedral geometry of reducible and cyclic models. *J. Combin. Theory* Ser. A, 100:277-301, 2002.

[16] 奥野忠一・芳賀敏郎 (1969). 実験計画法. 培風館.

[17] Pistone, G. and Wynn, H. P. (1996). Generalised confounding with Gröbner bases, *Biometrika*, **83**, 653–666.

[18] Pistone, G., Riccomagno, E. and Wynn, H. P. (2000). *Algebraic Statistics, Computational Commutative Algebra in Statistics*. Chapman & Hall.

[19] Giovanni Pistone and Maria-Piera Rogantin. (2008). Indicator function and complex coding for mixed fractional factorial designs. *Journal of Statistical Planning and Inference*, **138**, No.3, 787–802.

[20] Tomonari Sei, Satoshi Aoki and Akimichi Takemura. (2009). Perturbation method for determining the group of invariance of hierarchical models. *Advances in Applied Mathematics*, doi:10.1016/j.aam.2009.02.005.

[21] Bernd Sturmfels. (1996). *Gröbner Bases and Convex Polytopes*, American Mathematical Society, Providence, RI.

[22] 竹村彰通 (2006). 統計数学における計算代数的方法. 日本数学会 2006 年度秋期総合分科会総合講演.

[23] 竹村彰通 (2008). 分割表のグラフィカルモデルとその周辺. 応用統計学会特別講演. 筑波大学. 2008 年 6 月.

[24] 竹村彰通 (2008). 計算代数統計の話題. 日本統計学会賞受賞講演. 慶応義塾大学. 2008 年 9 月.

[25] 竹村彰通 (2009). 計算代数統計の最近の話題について. 日本統計学会雑誌和文誌投稿論文.

[26] 竹村彰通, 青木敏 (2006). 統計学におけるグレブナー基底. グレブナー基底の現在, 日比孝之 [編], 数学書房, 第 3 章所収.

[27] Takemura, A. and Hara, H. (2007). Conditions for swappability of records in a microdata set when some marginals are fixed. *Computational Statistics*, **22**, 173–185.

[28] Wu, C. F. J. and Hamada, M. (2000). *Experiments: Planning, analysis, and parameter design optimization*. Wiley, New York.

分割表生成のための群論的方法

A group-theoretic method of generating contingency tabless

吉田 知行 (YOSHIDA, Tomoyuki) (北大・理)
yoshidat@math.sci.hokudai.ac.jp

2009/06/24 Yamagata

概 要

分割用の検定はもっとも基本的かつ頻用されるな統計の手法である．現代の統計学では，そのために，大量の分割表の生成が必要になる．具体的には，マルコフ連鎖モンテカルロ法 (MCMC 法) により，与えられた分割表から，次々に新たな分割表を構成して行く．ここでは，有限群上のランダムウォークの Diaconis による理論を紹介し，分割表構成 (Metropolis-Heisting 法) の群論的背景を述べる．

1 マルコフ空間とマルコフ作用素

代数学を学んだものから見ると，確率統計の分野はまだ数学的記述が未熟に感じる．ただし，著者が確率統計の考えに不慣れなことに主要な原因があると考えるべきだろう．ここでは，最初の作業として，有限群の表現論や組合せ論を応用しやすいように，マルコフ連鎖周辺の基礎を少し書き直しておく．

まず $\Delta := [0,1]$ を単位区間とする．アイデアは，線形代数や群の表現論の基礎体を，Δ にすることである．したがって「Δ 上の線形空間 C」とは，凸多面体であると考える．Δ の作用は，

$$C \times \Delta \times C \to C; (x,t,y) \mapsto (1-t)x + ty$$

でであり,「Δ-線形写像」 $f : C \to D$ はアファイン写像 (凸写像) と考える：

$$f((1-t)x+ty) = (1-t)f(x)+tf(y), \quad \forall x, y \in C, t \in \Delta.$$

凸多面体とアファイン写像のなすカテゴリーは次の性質を持つ. (1) すべての有限極限, 有限余極限を持つ. (2) アファイン写像は一意的全単射分解を持つ. (3) cartesian closed, すなわち $\mathrm{Hom}(C, D)$ も凸多面体の構造を持つ.

ここでは簡単のため, 主に単体的な凸集合で考える. 以下, X などは有限集合とする. X 上の確率分布とか確率測度と言われるのは, 写像 $\mu : X \to \Delta$ であって, $\sum_{x \in X} \mu(x) = 1$ を満たすものである. ここでは単に**分布**ということにする. X 上の分布の集合を ∇X で表す. さらに

$$\Delta X := \{\textstyle\sum_{x \in X} \mu(x)x \mid \mu \in \nabla X\} \subset \mathbb{R}X$$

と置き, これを X 上の**マルコフ集合**という (確率単体などともいう). この集合 (X を頂点集合とする単体) は凸集合であり, ∇X と一対一対応がある：

$$\mu \longleftrightarrow \widehat{\mu} := \sum_{x \in X} \mu(x)x.$$

マルコフ集合の間の**マルコフ写像**は, 凸集合間のアファイン写像として定義する. これらの用語と記法はあまり標準的でないことに注意しておく.

有限集合 X (**状態集合**という) 上の**マルコフ連鎖**とは, 三つ組 $(\Delta X, \mu_0, \boldsymbol{P})$ のことである. ここで, $\mu_0 \in \Delta X$ で, $\boldsymbol{P} : \Delta X \to \Delta X$ はマルコフ写像である. μ_0 は, $\mu_0 \in \nabla X$ によって $\mu_0 = \widehat{\mu_0}$ と表せる. μ_0 を初期分布という. $\boldsymbol{P}$ は, 頂点の行き先で決まる：

$$\boldsymbol{P} : x(\in X) \mapsto \sum_{y \in Y} P(x, y)y$$

と表せる. このときの行列 $P = (P(x, y))_{x,y \in X}$ を**遷移行列** (transition matrix) という. 各 $x \in X$ に対し, $y \mapsto P(x, y)$ は X 上の分布である. すなわち

$$\sum_{y \in X} P(x, y) = 1, \; P(x, y) \in \Delta.$$

なおこの条件を満たす行列 $P=(P(x,y))_{x,y\in X}$ を，確率行列 (stochastic matrix) とかマルコフ核ということがある．普通，マルコフ連鎖 $(\Delta X,\mu_0,P)$ を指定するには，(X,μ_0,P) を指定する．

マルコフ連鎖 $(\Delta X,\mu_0,P)$ があれば，マルコフ空間内の点列

$$\mu_0\to\mu_1\to\mu_2\to\cdots\to\mu_m\to\cdots,\quad \mu_m=P(\mu_{m-1})=P^m(\mu_0).$$

が出来る．対応する確率分布の列は

$$\mu_0\to\mu_1\to\mu_2\to\cdots\to\mu_m\to\cdots,\quad \mu_m:=\mu_{m-1}P=\mu_0P^m$$

となる (μ_0P^m は，μ_0 をベクトルと見て，行列 P^m を乗じたもの)．

点 $x_0\in X$ を確率 $\mu_0(x_0)$ で選び，次いで x_1 を確率 $P(x_0,x_1)$ で選び，この過程をくり返して，X の点列 $x_0\to x_1\to x_2\to\cdots$ (X 上のランダムウォーク) が得られる．$P(x,y)$ は，点 x が y に移る確率を表す．

ある自然数 r によって，$P^r(X)\cap X=\emptyset$，同じことだが遷移確率行列 P が既約なら，Perron-Frobenius の定理や，コーシー列の収束性，あるいは Brouwer の不動点定理により，$P^m(X)$ はただ一点 (停留分布あるいは不変分布) に収束する．

2　有限群上のマルコフ連鎖

G を有限群とする．このとき，ΔG は群環 $\mathbb{C}G$ の中で，積に関して閉じている．

$$\left(\sum_{g\in G}p(g)g\right)\cdot\left(\sum_{g\in G}q(g)g\right)=\sum_{g,h\in G}p(g)q(h)gh=\sum_{g\in G}(p*q)(g)\,g$$

ここで $p*q$ はたたみ込み積 (convolution product) である．

$$p*q(g)=\sum_{h\in G}p(gh^{-1})q(h),\quad \text{すなわち}\quad \widehat{p}\,\widehat{q}=\widehat{(p*q)}$$

この場合，単位元でのディラック分布 $\delta_1=p^{(*0)}$ から始まる分布の列 $p^{(*m)}$ $(m=0,1,2,\cdots)$ が得られる．これは G 上のマルコフ連鎖 $(\Delta G,1,\widehat{p})$ を与える．遷移確率は $p(x^{-1}y)$ である．このマルコフ連鎖の漸近的性質は $\widehat{p}^m=\widehat{p^{(*m)}}$ $(m=0,1,2,\cdots)$ の挙動で決まる．ここで $p^{(*m)}$ は m 回合成積である．

以下では，p が**類関数の場合**の Diaconis の理論を紹介する．行列表現でなく，加群を使った現代的な有限群の表現論にしたがって全面的に改めている．有限群の表現論の常識から始めたい．$\mathrm{Irr}(G)$ は G の既約指標の集合を表すとする．各 $\chi \in \mathrm{Irr}(G)$ に対応する $\mathbb{C}G$ の中心原始ベキ等元は

$$e_\chi := \frac{\chi(1)}{|G|}\widehat{\overline{\chi}} = \frac{\chi}{|G|}\sum_{g\in G}\overline{\chi(g)}g$$

の形をしている．また線形写像 $\omega_\chi : \mathbb{C}G \to \mathbb{C}$ を

$$\omega_\chi : g \mapsto \frac{\chi(g)}{\chi(1)}$$

で定義する．$a \in \mathbb{C}G$ と $c \in Z(\mathbb{C}G)$ に対し，$\omega_\chi(ac) = \omega_\chi(a)\omega_\chi(c)$ であることは容易にわかる．とくに，ω_χ は $Z(\mathbb{C}G)$ に制限すると多元環準同型となっている．さらに直交関係より $\omega_\chi(e_\theta) = \delta_{\chi\theta}$ である．

p が類関数の場合，$\widehat{p} = \sum_{g\in G} p(g)g \in Z(\mathbb{C}G)$ は次のように展開される：

$$\begin{aligned} \widehat{p} &= \sum_{\chi\in\mathrm{Irr}(G)} \omega_\chi(\widehat{p})e_\chi \\ \therefore\ \widehat{p^{(*m)}} &= \widehat{p}^m = \sum_{\chi\in\mathrm{Irr}(G)} \omega_\chi(\widehat{p})^m e_\chi \qquad (m = 0, 1, 2, \cdots). \end{aligned}$$

ここで，

$$\omega_\chi(\widehat{p}) = \frac{|G|}{\chi(1)}\langle\chi, p\rangle = \sum_{g\in G} p(g)\frac{\chi(g)}{\chi(1)}$$

なので，$0 \le p(g) \le 1$ と $|\chi(g)/\chi(1)| \le 1$ より $|\omega_\chi(\widehat{p})| \le 1$ であることに注意しておく．結局，$\widehat{p^{(*m)}}$ の極限分布を調べるには，いつ $|\omega_\chi(\widehat{p})| = 1$ が起こるかを調べればよい．$S := \mathrm{supp}(p) = \{g \in G \mid p(g) \neq 0\}$，$N := \langle S^{-1}S\rangle$ と置く．このとき S は共役類の和集合であり，N は正規部分群である．$g_0 \in S$ なら，$S \subset g_0N$ であり，したがって $S \subset Z(G \mod N)$ である．

簡単な表現論により次が容易に示される．

補題. $|\omega_\chi(\widehat{p})| = 1 \iff N \subset \mathrm{Ker}\,\chi.$

定理 1. 確率分布 $q \in \nabla G$ を

$$q(g) := \begin{cases} 1/|N| & g \in SN \\ 0 & \text{その他} \end{cases}$$

で定義する．このとき次が成り立つ．

(1) $p^{(*m)} - q^{(*m)} \to 0 \quad (m \to \infty)$ である．

(2) $p^{(*m)}$ が収束するための必要十分条件は $S \subset N$ で，そのときの極限分布は q.

(3) $p^{(*m)}$ が一様分布に収束するための必要十分条件は $N = G$ である．

例. $G = C_n = \langle g_0 \rangle$ を位数 n の巡回群とする．

G 上の確率分布 p を

$$p(g) = \begin{cases} p_0 & (g = g_0) \\ q_0 & (g = g_0^{-1}) \\ 0 & (\text{else}), \end{cases}$$

で定義する．ただし $0 < p_0 < 1, q_0 := 1 - p_0$ である．このとき $\widehat{p} = p_0 g_0 + q_0 g_0^{-1} \in \mathbb{C}G$ である．

χ_k を $\chi_k(g_0) = \zeta^k$，ここで $\zeta := \exp(2\pi\sqrt{-1}/n)$，なる G の既約指標とする．また $\mathbb{C}G$ の原始ベキ等元は

$$e_k := e_{\chi_k} = \frac{1}{n} \sum_{j=0}^{n-1} \zeta^{-jk} g^j$$

となる．さらに

$$c_k := \omega_{\chi_k}(\widehat{p}) = p_0 \zeta^k + q_0 \zeta^{-k}$$

とすれば，

$$\widehat{p} = \sum_{k=0}^{n-1} c_k e_k, \quad c_k := p_0 \zeta^k + q_0 \zeta^{-k}.$$

したがって

$$\widehat{p^{(*m)}} = \widehat{p}^k = \sum_{k=0}^{n-1} c_k^m e_k$$

同じことだが，

$$p^{(*m)} = \frac{1}{n} \sum_{k=0}^{n-1} c_k^m \overline{\chi_k}$$

$$|c_k|^2 = p_0^2 + q_0^2 + 2p_0q_0\cos\frac{4k\pi}{n}$$

$|c_k| = 1$ となるのは，$k = 0$ と $k = n/2$ (この場合 n は偶数) の場合である．$c_0 = 1$, $c_{n/2} = -1$ となる．また $k \neq 0, n/2$ で $|c_k|$ の最大値は，$k = 1, n-1$ のときの

$$\rho = p_0^2 + q_0^2 + 2p_0q_0\cos\frac{4\pi}{n} = 1 - 4p_0q_0\sin^2\frac{2\pi}{n}$$

例． 対称群 $G = S_5$ 上の次の確率分布を考える．

$$p(g) = \begin{cases} 1/10 & (g \text{ が互換の場合}) \\ 0 & \text{その他} \end{cases}$$

この場合，$N = A_5$ である．さらに $\omega_\chi(\widehat{p}) = \chi(\tau)/\chi(1)$．ここで τ は互換である．χ_i に対応する中心原始ベキ等元を e_i とすると，指標表により

$$\begin{aligned}
\widehat{p} &= e_1 + \frac{1}{2}e_2 + \frac{1}{5}e_3 - \frac{1}{5}e_5 - \frac{1}{2}e_6 - e_7, \\
\therefore \widehat{p}^m &= e_1 + \left(\frac{1}{2}\right)^m e_2 + \left(\frac{1}{5}\right)^m e_3 + \left(\frac{-1}{5}\right)^m e_5 + \left(\frac{-1}{2}\right)^m e_6 + (-1)^m e_7, \\
\therefore p^{(*m)} &= \frac{1}{120}\chi_1 + \frac{1}{30}\left(\frac{1}{2}\right)^m \chi_2 + \frac{1}{24}\left(\frac{1}{5}\right)^m \chi_3 + \frac{1}{24}\left(\frac{-1}{5}\right)^m \chi_5 \\
&\qquad + \frac{1}{30}\left(\frac{-1}{2}\right)^m \chi_6 + \frac{1}{120}(-1)^m\chi_7 \\
&\approx \frac{1}{120}\chi_1 + \frac{1}{120}(-1)^m\chi_7 = q^{(*m)}.
\end{aligned}$$

ここで，$q = (1/120)(\chi_1 - \chi_7)$ は，偶置換で 0，奇置換で $1/60$ を取る S_5 上の確率分布．$p^{(*m)} - q^{(*m)} = O(2^{-m})$ $(m \to \infty)$ である．

3 G-集合上のランダムウォーク

G を有限群，X を右 G-集合，$\mu_0 \in \nabla X$ とする．また X に付随する置換指標を π_X とする．このとき G 上の確率分布 $p \in \nabla G$ は X 上のランダムウォーク $\mu^{(*m)}$ $(m = 0, 1, 2, \dots)$ を誘導する．ここで $\mu^{(*m)} = \mu_0 * p^{(*m)}$．

ここでも p は類関数とする．もし $\chi \leq \pi_X$ (既約指標 χ が π_X の成分) でないなら，$(\mathbb{C}X)e_\chi = 0$ なので，各 $x \in X$ に対し，

$$x\widehat{p} = \sum_{\chi \leq \pi_X} \omega_\chi(\widehat{p}) x e_\chi.$$

χ	型	(1)	(2)	(3)	(4)	$(2)^2$	(3)(2)	(5)	$\omega_\chi(\widehat{p})$
χ_1	$[5]$	1	1	1	1	1	1	1	1
χ_2	$[4,1]$	4	2	1	0	0	-1	-1	$1/2$
χ_3	$[3,2]$	5	1	-1	-1	1	1	0	$1/5$
χ_4	$[3,1^2]$	6	0	0	0	-2	0	1	0
χ_5	$[2^2,1]$	5	-1	-1	1	1	-1	0	$-1/5$
χ_6	$[2,1^3]$	4	-2	1	0	0	1	-1	$-1/2$
χ_7	$[1^5]$	1	-1	1	-1	1	-1	1	-1

表 1: S_5 の指標表

となる．したがって，

$$\widehat{\mu p}^m = \sum_{\chi \leq \pi_X} \omega_\chi(\widehat{p})^m \widehat{\mu} e_\chi.$$

結局のところ，G-集合上のランダムウォークも有限群上のと実質的には変わらない．

講演では，ヘッケ環や Gelfand 対の分割表などへの応用についても触れたが，ここでは省略する．2009 年 8 月の札幌での数理研研究集会での講演参照．

4 データセットと分割表

$N := \{1, 2, \cdots, n\}$ で，$I, J, \cdots$ を有限集合とする．S_n は N 上の対称群とする．

(1 次元) **データセット**とは，写像 $[f : N \to I]$ のことである．ここで，単なる写像 f と区別するために，括弧を付けてある．データセット $[f : N \to I]$ の**度数分布表** (あるいはヒストグラム) とは，$\mathsf{tab}[f] := (|f^{-1}(i)|)_{i \in I}$ のことである．

統計学的には，N は番号付きの「観察」(observation または case) の集合，f は $a \in N$ に，a 番目の観察結果 $f(a) \in I$ を与える「確率変数」(random variable)，I の元は「水準」(level) と呼ばれる．I はカテゴリーと呼ぶこともあるし，確率変数と同一視することもあるようだ．確率統計の概念を離散数学の用語で書き表すのはやっかいである．

ふたつのデータセット $[f : N \to I]$ と $[f' : N \to I]$ が**同型** ($[f] \cong [f']$) であるとは，ある $\pi \in S_n$ が存在して $f = f' \circ \pi$ を満たすことである．容易に分かるように，この条件は同じ度数分布表を持つことと同値である．これは，コンマカテゴリー $\mathbf{set}/I$ における同型判定定理そのものである．より一般に，有限 Hom-sets を持ち，一意的全単射分解が出来るカテゴリーにおいて，

$$X \cong Y \Leftrightarrow |\mathrm{Hom}(A, X)| = |\mathrm{Hom}(A, Y)| \quad \forall A \text{ (直既約)}$$

が成り立つ．

$\boldsymbol{a} = (a_i)_{i \in I}$ を，$\sum a_i = n$ を満たす非負整数ベクトルとする．

$$\mathsf{DS}_N(\boldsymbol{a}) := \{[f] \in I^N \mid \mathsf{tab}[f] = \boldsymbol{a}\}$$

は，データセットの同型類の集合である．同じことだが，対称群 S_n を，$[f]\pi := [f \circ \pi]$ で作用させたときの軌道でもある．すなわち $\mathsf{tab}[f] = \boldsymbol{a} = (a_i)$ としたとき，

$$\mathsf{DS}_N(\boldsymbol{a}) \cong S_f \backslash S_n$$

であり，したがって

$$\mathsf{DS}_N(\boldsymbol{a}) = (S_n : S_f) = \frac{n!}{\boldsymbol{a}!} = \frac{n!}{\prod a_i!}.$$

ここで，$S_f \leq S_n$ は Young 部分群である．$\mathsf{tab}[f] = (a_i)$ のとき，

$$S_f = \{\pi \in S_n \mid f\pi = f\} \cong \prod_{i \in I} S_{a_i}.$$

(2次元) データセット $[f, g]$ とは $I^N \times J^N$ の元，同じことだが $(I \times J)^N$ の元のことである．$\mathsf{tab}[f], \mathsf{tab}[g]$ を**周辺度数分布**という．与えられた周辺度数分布 $\boldsymbol{a}, \boldsymbol{b}$ を持つ2次元データセットの集合を $\mathsf{DS}_N(\boldsymbol{a}, \boldsymbol{b}) := \mathsf{DS}_N(\boldsymbol{a}) \times \mathsf{DS}(\boldsymbol{b})$ で表す:

$$\mathsf{DS}_N(\boldsymbol{a}, \boldsymbol{b}) := \{[f, g] \mid \mathsf{tab}[f] = \boldsymbol{a}, \mathsf{tab}[g] = \boldsymbol{b}\}.$$

このとき，$S_n \times S_n$ は $\mathsf{DS}_N(\boldsymbol{a}, \boldsymbol{b})$ に可移に作用する：$[f, g](\sigma, \tau) := [f \circ \sigma, g \circ \tau]$.

2次元データセット $[f, g]$ の**分割表**とは $I \times J$ 型行列

$$\mathsf{tab}[f, g] := (|f^{-1}(i) \cap g^{-1}(j)|)_{i \in I, j \in J}$$

のことである．同型 $[f,g] \cong [f',g']$ を，$f = f' \circ \pi, g = g' \circ \pi$ を満たす $\pi \in S_n$ の存在として定義する．この条件は，$\mathsf{tab}[f,g] = \mathsf{tab}[f',g']$ なることと同値である．

一般に $(\boldsymbol{a},\boldsymbol{b})$ 型の分割表を，非負整数行列 $X = (x_{i,j})_{i\in I, j\in J}$ で，与えられた周辺和 $\sum_j x_{i,j} = a_i$, $\sum_i x_{i,j} = b_j$ を持つものと定義する．そのような分割表の集合を $\mathsf{TAB}[\boldsymbol{a},\boldsymbol{b}]$ とする．このとき写像 tab は，次の全単射を与える：

$$\mathsf{DS}(\boldsymbol{a},\boldsymbol{b})/DS_n \cong \mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$$

ここで $DS_n := \{(\pi,\pi) \mid \pi \in S_n\}$ は，対角部分群である．これより，$[f,g]$ と同じ分割表を持つ2次元データセットの個数は

$$|\mathsf{tab}^{-1}(\mathsf{tab}[f,g])| = \sharp\{[f',g'] \cong [f,g]\} = \frac{n!}{|S_f \cap S_g|} = \frac{n!}{\prod_{i,j} x_{ij}!}$$

ここで，$\mathsf{tab}[f,g] = (x_{i,j})$ とした．集合 $\mathsf{tab}^{-1}(\mathsf{tab}[f,g])$ はファイバーと呼ばれる．とくに $\mathsf{tab}[f] = \boldsymbol{a}, \mathsf{tab}[g] = \boldsymbol{b}$ のとき，

$$\mathsf{TAB}(\boldsymbol{a},\boldsymbol{b}) \cong S_f \backslash S_n / S_g$$

である．

対称群上の RW から $\mathsf{DS}(\boldsymbol{a},\boldsymbol{b})$ 上の RW が誘導され，さらに $\mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$ 上の RW が誘導される．ただし S_n と $\mathsf{DS}(\boldsymbol{a},\boldsymbol{b})$ 上の確率分布は一様分布である．それから誘導される $\mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$ 上の確率分布は多項超幾何分布

$$\begin{aligned} H(\boldsymbol{x}) &= \mathrm{Prob}(X[f,g] = (x_{ij}) \mid \mathsf{tab}[f] = \boldsymbol{a}, \mathsf{tab}[g] = \boldsymbol{b}) \\ &= \prod_i a_i! \prod_j b_j! \Big/ n! \prod_{ij} x_{ij}! \end{aligned}$$

である．

データセットでなく，分割表で考えるなら，$S_n \times S_n$ を作用させる必要はない．S_n の作用 $([f,g],\sigma) \mapsto [f\sigma,g]$ だけで十分である．これは $\mathsf{tab}[f\sigma,g\tau] = \mathsf{tab}[f\sigma\tau^{-1},g]$ が成り立つからである．

例. $[f,g] \in \mathsf{DS}(\boldsymbol{a},\boldsymbol{b})$, $\mathsf{tab}[f] = \boldsymbol{a}, \mathsf{tab}[g] = \boldsymbol{b}$ とする．このとき，S_n 上の RW は，$\mathsf{TAB}(\boldsymbol{a},\boldsymbol{b})$ 上の RW(極限分布が多項超幾何分布) を誘導する．対称群上の RW として，「random transiposition」によるものを考える．これは互換 τ をランダムかつ一様に選んで，$\sigma \to \sigma\tau$ を

5　分割表の一致率検定への応用

ここでは $I=J$ とし，データセット $[f,g:N\to I]$ を考える．対応する分割表は $I\times I$ 型の正方行列である：

$$\mathsf{tab}[f,g]=(|f^{-1}(i)\cap g^{-1}(j)|)_{i,j\in I}$$

周辺分布を $a_i:=|f^{-1}(i)|, b_j;=|g^{-1}(j)|$ とする．$\mathsf{tab}[f,g]$ のトレースを**一致数** (measure of agreement) という:

$$x_0[f,g]:=\mathrm{Tr}(\mathsf{tab}[f,g])=\sharp\{a\in N\mid f(a)=g(a)\}.$$

データセット $[f,g]\in\mathsf{DS}(a,b)$ をランダムに取ったときの一致数 $x_0[f,g]$ の分布を知りたい.

定理. (1) G を集合 $N=\{1,2,\cdots,n\}$ 上の可移置換群 (作用は左から) とする．各 $\pi\in G$ に対し $x(\pi):=x_0(f\pi,g)$ と置く．このとき $x(\pi),\pi\in G$ の平均値 m は

$$m:=E_{\pi\in G}[x(\pi)]=\frac{1}{n}\sum_{i\in I}a_ib_i$$

で与えられる.

(2) G を集合 $N=\{1,2,\cdots,n\}$ 上の t-重可移置換群 (作用は左から) とする．このとき $x(\pi),\pi\in G$ の t 次組合せモーメントは

$$E_\pi\left[\binom{x(\pi)}{t}\right]=\frac{(n-t)!}{n!}\sum_{\sum t_i=t}\prod_i\binom{a_i}{t_i}\binom{b_i}{t_i}t_i!$$

で与えられる.

とくに対称群 $G=S_n$ の場合に適用すれば，周辺分布 $\boldsymbol{a}=(a_i),\boldsymbol{b}=(b_j)$ から，一致数 $x(\pi)$ の分布が一意的に決まることがわかる．具体的には，以下のようにして正確な P-値を求めることが出来る.

まず ${}_2F_0$ 型の超幾何級数を用意する.

$$F_{a,b}(z)={}_2F_0(-a,-b;z)=\sum_{k\geq 0}\binom{a}{k}\binom{b}{k}\,k!\,z^k$$

この級数の収束半径は一般にゼロだが，a,b の一方が非負整数なら多項式 (超幾何多項式) である.

与えられた周辺分布 $\boldsymbol{a}=(a_i), \boldsymbol{b}=(b_j)$ に対し,

$$F(z) := \prod_{i \in I} F_{a_i,b_i}(z) = \sum_{k \geq 0} \binom{n}{k} k! q(k)\, z^k$$

と展開する. さらに

$$\sum_{k \geq 1} q(k)\,(z-1)^{k-1} = \sum_{k \geq 1} P(k)\, z^{k-1}$$

と展開する.

定理. 上で与えられた $P(r)$ $(r=1,2,\cdots)$ は一致数に対する P-値である:

$$P(r) = \mathrm{Prob}(x(\pi) \geq r) = \frac{1}{n!} \sharp\{\pi \in S_n \mid x(\pi) \geq r\}$$

このようにして二次元正方分割表の一致数 (対角和) の値の分布が分かり, したがって正確な p-値は計算できることになる. ここで述べた方法は, Fisher の並べ替え検定という統計学の手法そのものである.

一次元周辺和を固定した三次元分割表の対角和については, ${}_3F_0$-超幾何多項式を使えば同様の結果が得られる. しかし本当に難しいのは3つある2次元周辺和 $x_{i++}, x_{+j+}, x_{++k}$ をすべて固定した分割表について, 統計量 S (対角和やカイ二乗統計量など) の正確な p-値

$$\mathrm{Prob}(S(\boldsymbol{x}) < \epsilon)$$

を求めることである. これについては対角和についても難しい.

6 分割表のランダムサンプリング

分割表検定の現代的な方法は, 与えられた周辺和を持つ分割表をランダムにたくさん作る. そのためには Markov chain Monte Carlo (MCMC) 法が使われる.

$\mathsf{tab}[f_0, g_0]$ を観察されたデータセット $[f_0 : N \to I, g_0 : N \to J]$ から得られた分割表とする. このとき対称群 S_n 上の RW は, 周辺分布が $\mathsf{tab}[f_0] =: \boldsymbol{a}, \mathsf{tab}[g_0] =: \boldsymbol{b}$ であるような分割表の RW を誘導する.

$$S_n \to \mathsf{TAB}\boldsymbol{a}, \boldsymbol{b}); \sigma \mapsto \mathsf{tab}[f_0\sigma, g_0]$$

対称群上のRWが一様分布に収束すれば，分割表の上のRWは多項超幾何分布に収束する．一様分布の仮定はもう少し弱く出来る．例えば，次の結果がある．

まず，データセットの分割表 tab$[f_0.g_0]$ が自明であるとは，各行各列に1が高々ひとつしかないことをいう．周辺度数 $a_i = 0$ (または $b_j = 0$) のなるのは，統計的には考える必要がない．したがって周辺度数に0が出てこないような場合，自明な分割表とは，置換行列であることを意味する．

定理 分割表 tab$[f_0, g_0]$ は自明でないと仮定する．さらに確率分布 $p \in \nabla S_n$ が類関数であり，$p \neq \delta_1$(ディラック分布) と仮定する．このとき p から誘導される TAB(a, b) 上のRWは一様分布に収束する．

例. 対称群 S_n 上の確率分布

$$p_2(\sigma) = \begin{cases} \binom{n}{2}^{-1} & \sigma \text{ が互換} \\ 0 & \text{それ以外} \end{cases}$$

を考える．まず，p_2 は対称群上の一様分布に収束しない．実際，$p^{(*2m)}$ は $m \to \infty$ で交代群 A_n 上の一様分布に収束し，$p^{(2m+1)}$ は $S_n - A_n$ 上の一様分布に収束する．

ところが，この分布から誘導される分割表の上のRWは一様分布に収束する．自明でない分割表では，ある互換 τ が存在して，tab$[f, g]$ = tab$[f\tau, g]$ となっているからである．

参考文献

[] 津野義道「ランダム・ウォーク—乱れに潜む不思議な現象」牧野書店 (2002)
専門外の人にも読める．逆正弦法則の証明がきちんとのっている．

[] L.Saloff-Coste, Lectures on finite Markov chains, in "Lecftures on Porbability Theory and Statistics," Springer LNM 1665 (1997), pp 301–413.
有限マルコフ連鎖の定義と様々な分野との関連を述べている．[] P.Diaconis, "Group representations in probability and statistics," IMS, Harvard, 1986.
有限群上のランダムウォークへの表現論の応用として記念碑的論文．講義録で手に入りにくい．おすすめ．[] P.Good, "Permutation, Parametric, and Bootstrap Tests of Nypotheses", Springer, 2005.
リサンプリング法の入門書．確率と統計の初歩を知っている必要がある．

[] S.Lauritzen, "Graphical Models", Oxford, 1995.
3次元以上の分割表について，マルコフ基底構成の難しさが分かる．かなり専門的.

[] 甘利・竹内　・竹村・伊庭編「統計科学のフロンティア」岩波書店, 2003.
とくに「計算数学 I」と「計算数学 II」が興味深い．読み物としてもおもしろい．[] O.Häggström ,"Finite Markov Chains and Algorithmic Applications", London M.S., 2002.
薄いがコンパクトにまとまっていて読みやすい．入門書としておすすめ.
[] L. Pachter B. Sturmfels, " Algebraic Statistics for Computational Biology", Cambridge, 2005.
代数統計学の生物分野への様々な応用．数学・統計・生物の初歩についてどれかに詳しければ何とか読める．おすすめ.

この分野でもっとも活躍しているのは，海外では Diaconis と Saloff-Coste，日本では竹村彰通東大教授とそのグループである．ネットを検索すればたくさんのサイトが見つかる.

変形一般アダマール行列について

平峰 豊 (熊本大学)

1 はじめに

結合構造 $(\mathbb{P}, \mathbb{B})$ が *transversal design* $\mathrm{TD}_\lambda[k;u]$ $(u>1, k=u\lambda)$ であるとは $|\mathbb{P}| = |\mathbb{B}| = ku\ (=u^2\lambda)$ で次をみたすことをいう.

(i) $\mathbb{P}$ は点集合で k 個の点クラス (point class) $C_1, \cdots, C_k$ に分割され各クラスは u 点からなる: $\mathbb{P} = C_1 \cup C_2 \cup \cdots \cup C_k, \quad |\forall C_i| = u.$

(ii) $\mathbb{B}$ は $\mathbb{P}$ の k-部分集合 (ブロック) のある family である.

(iii) $\mathbb{P}$ の異なる 2 点を含むブロック数

$$= \begin{cases} \lambda & \text{異なる点クラスの 2 点のとき,} \\ 0 & \text{同じ点クラスの 2 点のとき.} \end{cases}$$

transversal design $\mathcal{D} = (\mathbb{P}, \mathbb{B})$ の双対構造 $\mathcal{D}^*$ も同じ parameters の transversal design であるとき $\mathcal{D}$ は *symmetric* であるという.

transversal design $\mathcal{D}$ が U $(\leq \mathrm{Aut}(\mathcal{D}),\ |U| = u)$ に関して *class regular* であるとは U が各 point class に正則 (単位元以外固定点を持たず可移) に作用することをいう. $\mathcal{D}$ が U に関して class regular ならば U に成分をもつ $k(=u\lambda)$ 次正方行列 $M = [d_{i,j}]$ が存在して *generalized Hadamard matrix* と呼ばれて次を満たす.

$$\sum_{1\leq j\leq k} d_{ij}d_{\ell j}^{-1} = \lambda\widehat{U} \in \mathbb{Z}[U]\ (1 \leq i \neq \ell \leq k), \quad \widehat{U} = \sum_{x\in U} x$$

以下では M を $\mathrm{GH}(u,\lambda)$-行列とも呼ぶ.

逆に位数 u の群 U 上の generalized Hadamard matrix $\mathrm{GH}(u,\lambda)$ が存在すれば U を class regular な自己同型群としてもつ transversal design $\mathrm{TD}_\lambda[k;u]$ が構成される ([2]). この場合 $(\mathbb{P}, \mathbb{B})$ は必然的に symmetric であることが示されている ([5]). このことから, transversal design $\mathrm{TD}_\lambda[k;u]$ がもし非対称ならば class regular な自己同型群を持たないことになり, このような非対称 transversal design は generalized Hadamard matrix から構成することはできない.

ここでは，上記のような場合でもtransversal designを構成できる方法について考察する．transversal design$(\mathbb{P},\mathbb{B})$が$\mathbb{P}\cup\mathbb{B}$上に半正則に作用する(固定点または固定ブロックを持つ元は単位元に限る)自己同型群Gを持ち，各point class $\mathcal{C}$に対応してGの部分群$U_{\mathcal{C}}(\leq G)$が定まって，それが$\mathcal{C}$上正則に作用するものを考えてそれを**変形一般アダマール行列**と呼ぶ (Theorem 3, Definition 4)．この意味において，$U_{\mathcal{C}}$は "個別のclass regularな群" (depending on $\mathcal{C}$)とでも呼ぶべきものであることが分かる．逆に，変形一般アダマール行列が与えられればtransversal designが構成されてそれは一般にはclass regularな自己同型群を持たない (Theorem 7)．例として，この方法を用いて任意のtranslation planeからtransversal designが構成されることを示す (Theorem 14)．さらに，**変形Kronecker積**により多くのtransversal designsが得られることを示す (Theorem 17, Corollary 20)．以下での証明等の詳細は [4] 参照.

2 Preliminaries

Example 1. $\mathbb{Z}_3$上の行列$M=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$はGH$(3,1)$行列である.

既知のTD$_\lambda[k;u]$構成法：GH(u,λ)行列の利用

上のExample 1のGH$(3,1)$行列からTD$_1[3,3]$を構成する．点集合として$\mathbb{P}=\{1,2,3\}\times\mathbb{Z}_3$と定める ($\{1,2,3\}$は行番号に対応，$G=\mathbb{Z}_3$は群に対応)．ブロック集合$\mathbb{B}$を定めるためにまず，$M$の列を利用して次の3個の "base blocks" を定義する：

$\{(1,1),(2,0),(3,0)\}$, $\{(1,0),(2,1),(3,0)\}$, $\{(1,0),(2,0),(3,1)\}$

$\mathbb{B}$としてbase blocksを群Gの作用によりtranslateしたもの全体として定める：

$\{(1,1),(2,0),(3,0)\},\{(1,2),(2,1),(3,1)\},\{(1,0),(2,2),(3,2)\},$

$\{(1,0),(2,1),(3,0)\},\{(1,1),(2,2),(3,1)\},\{(1,2),(2,0),(3,2)\},$

$\{(1,0),(2,0),(3,1)\},\{(1,1),(2,1),(3,2)\},\{(1,2),(2,2),(3,0)\}$

このとき$(\mathbb{P},\mathbb{B})$は次のクラス分けをもつTD$_1[3,3]$となる.

$\mathcal{C}_1=\{1\}\times G$, $\mathcal{C}_2=\{2\}\times G$, $\mathcal{C}_3=\{3\}\times G$

一般の場合も同様の方法でGH(u,λ)行列からTD$_\lambda[k;u]$を構成できる．このようにして得られたTD$_\lambda[k;u]$について次が成り立つ.

Generalized Hadamard 行列から得られる $\mathrm{TD}_\lambda[k;u]$ の性質

- 位数 u の群 U 上の generalized Hadamard 行列 $\mathrm{GH}(u,\lambda)$ が与えられると class regular な自己同型群を持つ transversal design $\mathrm{TD}_\lambda[k;u]$ が構成される ([2]).

- class regular な自己同型群をもつ $\mathrm{TD}_\lambda[k;u]$ は常に symmetric である (Jungnickel [3]). 従って, transversal design $\mathrm{TD}_\lambda[k;u]$ が non-symmetric のときは, それが generalized Hadamard 行列から得られることはない.

3 新しい構成法 – クラスごとの正則群達の利用

transversal design に対して, $\mathbb{P}\cup\mathbb{B}$ 上半正則な自己同型群 G で, 点クラス C_i に対して部分群 $U_{C_i}(\leq G)$ があって C_i 上正則に作用する (U_{C_i} はクラス C_i に依存してよい !) ものについて考える. こののような transversal design のクラスとして次の性質をもつものを考察する.

Hypothesis 2. $(\mathbb{P},\mathbb{B})$ を $\mathrm{TD}_\lambda[k;u]$ とするとき, $(\mathbb{P},\mathbb{B})$ の自己同型群 H が次の (i)(ii) をみたすとする.

(i) H は $\mathbb{P}$ および $\mathbb{B}$ 上に半正則に作用する.
(ii) $\mathbb{P}$ 上の各 H-orbit はいくつかの点クラスの和集合になっている.

以下では Hypothesis 2 のもとで得られた結果 (1)–(5) について述べる.

(1) generalized Hadamard 行列を変形した *modified generalized Hadamard* 行列が得られる.
(2) 逆に, modified generalized Hadamard 行列 から transversal design を構成できる. (たとえ class regular な自己同型群をもたなくても)
(3) 任意の translation plane からこの方法により多くの transversal designs が構成される.
(4) 変形された Kronecker 積より transversal designs が構成される.
(5) G 上で与えられた modified generalized Hadamard 行列 から G の適当な部分群で modified generalized Hadamard 行列を構成できる.

このとき次が成り立つことは明らかである.

- Hypothesis 2 よりある整数 s $(s \mid u\lambda = k)$ があって $|H| = us$ と表されて $\mathbb{P}$ 上の各 H-orbit はちょうど s 個の点クラスからなる.

- $t=\frac{k}{s}$ とおけば H は $\mathbb{P}$ 上にも $\mathbb{B}$ 上にもちょうど t 個の H-orbits をもつ.

次が成り立つ.

Theorem 3. Hypothesis 2 のもとで, $\{\mathbb{Q}_1,\cdots,\mathbb{Q}_t\}$ を $\mathbb{P}$ 上の H-orbits 全体とし, $\{\mathbb{B}_1,\cdots,\mathbb{B}_t\}$ を $\mathbb{B}$ 上の H-orbits 全体とする. 各 i $(1\le i\le t)$ ごとに $Q_i\in\mathbb{Q}_i$ および $B_i\in\mathbb{B}_i$ を選んで固定する. このとき次が成り立つ.

(i) $U_i=\{x\in H: Q_ix\sim Q_i\}$, $1\le i\le t$ とおくと U_i は H の位数 u の部分群である.

(ii) $D_{ij}=\{x\in H: Q_ix\in B_j\}$, $1\le i,j\le t$ とおくと次をみたす.

(a) $|D_{ij}|=s \quad (1\le i,j\le t)$.

(b) $\sum_{j=1}^{t} D_{ij}D_{ij}^{(-1)}=k+\lambda(H-U_i) \quad (1\le i\le t)$.

(c) $\sum_{j=1}^{t} D_{ij}D_{\ell j}^{(-1)}=\lambda H \quad (1\le i\ne\ell\le t)$.

(上では G の部分集合 S と群環の元 $\sum_{x\in S}x$ を同一視, 以下でも同様)

変形一般アダマール行列 $\mathbf{GH}(s,u,\lambda)$ の定義

Definition 4. 位数 su の群 H の s-部分集合達 D_{ij} $(1\le i,j\le t, st=u\lambda)$ に対して, t 次正方行列 $[D_{ij}]$ が H の位数 u の部分群 $U_1,\cdots U_t$ に関する $\mathbb{Z}[H]$ 上の**変形一般アダマール行列** (modified generalized Hadamard matrix) であるとは次の条件をみたすことを言う.

$$\sum_{1\le j\le t} D_{ij}D_{\ell j}^{(-1)}=\begin{cases}k+\lambda(H-U_i) & (i=\ell\text{のとき})\\ \lambda H & (i\ne\ell\text{のとき})\end{cases} \tag{1}$$

以下では $[D_{ij}]$ を U_i, $1\le i\le t$ に関する $\mathbf{GH}(s,u,\lambda)$ **行列**と省略形でいう.

Example 5. $H=\langle a,b\rangle\simeq\mathbb{Z}_2\times\mathbb{Z}_2$ and $U_1=\langle b\rangle$, $U_2=\langle ab\rangle$ とするとき, $\begin{bmatrix}1+a & a+b\\ 1+b & 1+a\end{bmatrix}$ は $\mathbb{Z}[H]$ 上の $\mathrm{GH}(2,2,2)$ 行列である.

Remark 6. (1) $U_1=\cdots=U_t(=U)$ のとき $[D_{ij}]$ は U に関する $\mathrm{GH}(s,u,\lambda)$ 行列であるということにする. $H\rhd U$ のとき, Definition 4 は Akiyama-Ogawa-Suetake [1] で定義されているものと同じである.
(2) U に関する $\mathrm{GH}(1,u,\lambda)$ 行列は通常の generalized Hadamard 行列 $\mathrm{GH}(u,\lambda)$ over U と一致する.

(3) 群 G の U に関する $(u\lambda, u, u\lambda, \lambda)$-差集合 D に対して 1×1 行列 $[D]$ は U に関する $\mathrm{GH}(u\lambda, u, \lambda)$ 行列であるとみることができる.

群 H に対して，$\mathbb{Z}[H]$ 上の t 次正方行列全体を $\mathrm{M}_t(\mathbb{Z}[H])$ で表す.

$\mathrm{GH}(s,u,\lambda)$ からの $\mathbb{P}$ と $\mathbb{B}$ の定義

$\mathrm{GH}(s,u,\lambda)$ 行列 $[D_{ij}]\in \mathrm{M}_t(\mathbb{Z}[H])$, $t=u\lambda/s$, に対して点集合 $\mathbb{P}$ とブロック集合 $\mathbb{B}$ を次で定める.

$$\mathbb{P} = \{1,2,\cdots,t\}\times H, \tag{2}$$

$$\mathbb{B} = \{B_{jh} : 1\le j\le t,\ h\in H\}, \tag{3}$$

ここで

$$B_{jh} = \bigcup_{1\le i\le t} (i, D_{ij}h)$$

(2) と (3) を用いて次を示す.

Theorem 7. *su の群 H に対して $[D_{ij}]\in \mathrm{M}_t(\mathbb{Z}[H])$ を位数 u の部分群達 U_i $(1\le i\le t=u\lambda/s)$ に関する $\mathrm{GH}(s,u,\lambda)$ 行列とする. $\mathbb{P}$ と $\mathbb{B}$ を (2)(3) により定めるとき次が成り立つ.*

(i) $(\mathbb{P},\mathbb{B})$ は $\mathrm{TD}_\lambda[k;u]$ $(k=u\lambda)$ である.

(ii) 任意の $x\in H$ に対して $C_{i,U_ix}=\{(i,wx) : w\in U_i\}$ $(x\in H)$ とおけば C_{i,U_ix} は $(\mathbb{P},\mathbb{B})$ の点クラスである $(\forall i)$.

(iii) $(\mathbb{P},\mathbb{B})$ 上への H の作用を次で定義すれば $H\le \mathrm{Aut}(\mathbb{P},\mathbb{B})$ で H は $\mathbb{P}$ および $\mathbb{B}$ 上に半正則に作用する.

$$(i,c)^x=(i,cx),\quad (B_{j,d})^x=B_{j,dx}\quad(\forall i)$$

(iv) $x^{-1}U_i\,x$ は 点クラス C_{i,U_ix} 上正則に作用する $(\forall x\in H,\ \forall i)$.

Example 8. $u=3$, $\lambda=2$ かつ $H=\langle a,b\rangle\simeq \mathbb{Z}_3\times\mathbb{Z}_3$ で $s=3$, $t=2$ とする. $D_{ij}\in\mathbb{Z}[H]$, $1\le i,j\le 2$ と $U_i\simeq\mathbb{Z}_3$, $1\le i\le 2$ を次で定める.

$$U_1=\langle b\rangle,\quad U_2=\langle a\rangle$$

$$[D_{ij}]=\begin{bmatrix} 1+ab+a^2b & a^2+b+ab \\ 1+ab+ab^2 & 1+a^2b^2+a^2b \end{bmatrix}$$

このとき D_{ij} と U_j が次をみたすことを確かめることができる.

$$D_{11}D_{11}{}^{(-1)} + D_{12}D_{12}{}^{(-1)} = 6 + 2(H - U_1)$$
$$D_{21}D_{21}{}^{(-1)} + D_{22}D_{22}{}^{(-1)} = 6 + 2(H - U_2)$$
$$D_{11}D_{21}{}^{(-1)} + D_{12}D_{22}{}^{(-1)} = 2H$$

従って $[D_{ij}]$ は U_1, U_2 に関する GH(3,3,2) 行列である. Theorem 7 を適用して $\mathrm{TD}_2[6;3]$ を得る.

Example 9. $u=3$, $\lambda=4$ で $H=\langle a,b\rangle \simeq \mathbb{Z}_3\times\mathbb{Z}_6$ とおく. さらに $t=2$, $s=6$ とおく. D_{ij} $(1\le i,j\le 2)$ と $U_i \simeq \mathbb{Z}_3$ $(1\le i\le 2)$ を次で定める.

$$U_1=\langle ab^2\rangle, \quad U_2=\langle ab^4\rangle$$

$$[D_{ij}]=\begin{bmatrix} 1+b+b^2+b^3+a+ab & 1+a^2b^5+ab^4+a^2b+b^4+ab \\ 1+ab^5+a^2b^4+ab+b^4+a^2b & 1+b+b^2+b^3+a^2+a^2b \end{bmatrix}$$

このとき $[D_{ij}]$ は部分群 U_1, U_2 に関する GH(6,3,4) 行列であることを確かめることができる. 従って 同様に Theorem 7 より $\mathrm{TD}_4[12;3]$ を得る.

Example 10. Example 9 で H の部分群 $L=\langle a,c\rangle \simeq \mathbb{Z}_3\times\mathbb{Z}_3, c=b^2$ を考える. $s=3$, $u=3$, $\lambda=4$ で $t=4$ とおく. また, $U_1=U_2=\langle ac\rangle$, $U_3=U_4=\langle ac^2\rangle$ とおけば次の $[D_{ij}]$ は部分群 $U_1,\cdots,U_4$ に関する GH(3,3,4) 行列である. これより $\mathrm{TD}_4[12;3]$ が得られる.

$$[D_{ij}]=\begin{bmatrix} 1+c+a & c+c^2+ac & 1+ac^2+c^2 & a^2+a^2c+ac \\ 1+c+a & 1+c+a & a^2c^2+a^2+a & 1+ac^2+c^2 \\ 1+a^2c^2+c^2 & a+ac+a^2c & 1+c+a^2 & c+c^2+a^2c \\ ac^2+a+a^2 & 1+a^2c^2+c^2 & 1+c+a^2 & 1+c+a^2 \end{bmatrix}.$$

上の Example 10 の行列は Example 9 の行列をもとにして得られたものであるがその方法については Section 5 の Example 23 で述べる.

Remark 11. (i) 任意の i, $1\le i\le t$ について $H\rhd U_i$ であることは起こりうる. しかし, $U_1=\cdots=U_t$ であるとは限らない.
(ii) 部分群達 U_i から生成される群 $\langle U_1,\cdots,U_t\rangle$ は, 群を用いて transversal design が定義できるためのある意味で**最小の群**といえる. たとえ class regular な群が存在しない non-symmetric な場合でもこれは存在の可能性がある.

Theorem 7で得られるtransversal designがsymmetricであるための判定条件について述べる.

Theorem 12. 位数suの群Hに対して$[D_{ij}] \in \mathrm{M}_t(\mathbb{Z}[H])$を位数$u$の部分群達$U_i$ $(1 \le i \le t = u\lambda/s)$に関するGH$(s,u,\lambda)$行列とする. このとき$[D_{ij}]$に対応するTD$_\lambda[k;u], k = u\lambda$がsymmetricであるための必要十分条件は

$$[D_{ij}{}^{(-1)}]^T = \begin{bmatrix} D_{11}{}^{(-1)} & D_{21}{}^{(-1)} & \cdots & D_{t1}{}^{(-1)} \\ D_{12}{}^{(-1)} & D_{22}{}^{(-1)} & \cdots & D_{t2}{}^{(-1)} \\ \vdots & \cdots & \cdots & \vdots \\ D_{1t}{}^{(-1)} & D_{2t}{}^{(-1)} & \cdots & D_{tt}{}^{(-1)} \end{bmatrix}$$

がHの適当な部分群達V_i of H, $1 \le i \le t$に関するGH(s,u,λ)行列となることである. すなわち,

$$\sum_{1\le i\le t} D_{ij}^{(-1)} D_{i\ell} = \begin{cases} k + \lambda(H - V_j) & (j = \ell \text{のとき}, \exists V_j \le H) \\ \lambda H & (j \ne \ell \text{のとき}) \end{cases} \tag{4}$$

上の定理を用いてnon-symmetricなtransversal designの例をあげる.

Example 13. $H = \langle a,b \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$とする.
$[D_{ij}] = \begin{bmatrix} 1+ab+a^2b & a^2+b+ab \\ 1+ab+ab^2 & 1+a^2b^2+a^2b \end{bmatrix}$をExample 8で定めた$\mathbb{Z}[H]$上のGH$(3,3,2)$行列とする. このとき,

$D_{11}{}^{(-1)} D_{11} + D_{21}{}^{(-1)} D_{21} = 6 + (H - \langle a \rangle) + (H - \langle b \rangle)$.

であるから, Theorem 12より$[D_{ij}]$から得られるTD$_2[6;3]$はnon-symmetricである. 同様にExample 9のGH$(6,3,4)$行列から得られるTD$_4[12;3]$はnon-symmetricである. なぜなら次が確かめられるから.

$$D_{11}{}^{(-1)} D_{11} + D_{21}{}^{(-1)} D_{21} = 12 + 2(ab^2 + ab^4 + a^2b^2 + a^2b^4) + 3(ab + a^2b^5) + 4(a + a^2 + b + b^2 + b^3 + b^4 + b^5 + ab^3 + a^2b^3) + 5(ab^5 + a^2b).$$

4 Spreadを用いたtransversal designsの構成

素数pの冪$q = p^d$に対して位数q^2の群Hの位数qの部分群$\{H_1, \cdots, H_{q+1}\}$がspreadであるとは次がみたされることを言う([6]参照).

$$|H_1| = |H_2| = \cdots = |H_{q+1}| = q, \quad H_i H_j = H \quad (\forall i \ne \forall j)$$

この条件から$H^* = H_1^* \cup \cdots \cup H_{q+1}{}^*$は単位元以外の$H$の元全体$H^*$の分割を与える. この性質を利用して, 次が成り立つことが分かる.

Theorem 14. pを素数で$q=p^d$とし，$\{H_1,\cdots,H_{q+1}\}$を位数q^2の群Hのspreadとする．$A=[n_{ij}]$を成分を$I=\{1,2,\cdots,q+1\}$に持つq次正方行列で次をみたすものとする．

$$I=\{n_{i1},n_{i2},\cdots,n_{iq},m_i\},\quad 1\le i\le q, \tag{5}$$

$$I=\{n_{1j},n_{2j},\cdots,n_{qj},\ell_j\},\quad 1\le j\le q, \tag{6}$$

$$(\exists m_i\in I,\ \exists \ell_j\in I\ )$$

$D_{ij}=H_{n_{ij}}$，$1\le i,j\le q$とおく．このとき，$[D_{ij}]$は$H_{m_1},\ldots,H_{m_q}$に関するGH(q,q,q)行列で$[D_{ij}]$から得られるTD$_q[q^2;q]$はsymmetricである．

5 GH(s,u,λ)達からのproduct construction

群U上のGH(u,λ)行列とGH(u,λ')行列からKronecker積によりGH$(u,u\lambda\lambda')$行列が得られることが知られている．ここではこの方法をGH(s,u,λ)行列とGH(s',u,λ')行列の場合に一般化する．

Definition 15. GおよびNを群とする．また，$f_i:N\longrightarrow G$を中への同型写像とする$(i,1\le i\le n)$.

$z=\sum_{x\in N}c_xx$ $(\in\mathbb{Z}[N])$に対して$z^{f_i}=\sum_{x\in N}c_xx^{f_i}$ $(\in\mathbb{Z}[G])$と定める．

$A=[a_{ij}]\in \mathrm{M}_n(\mathbb{Z}[G])$と$B=[b_{ij}]\in \mathrm{M}_r[\mathbb{Z}[N]]$に対して$nr$次正方行列$A\otimes B^{(f_1,\cdots,f_n)}$を次で定める．

$$A\otimes B^{(f_1,\cdots,f_n)}=\begin{bmatrix} B^{f_1}a_{11} & B^{f_1}a_{12} & \cdots & B^{f_1}a_{1n}\\ B^{f_2}a_{21} & B^{f_2}a_{22} & \cdots & B^{f_2}a_{2n}\\ \vdots & \vdots & \vdots & \vdots\\ B^{f_n}a_{n1} & B^{f_n}a_{n2} & \cdots & B^{f_n}a_{nn}\end{bmatrix},$$

ここで $B^{f_\ell}=[b_{ij}^{f_\ell}]$.

$A\otimes B^{(f_1,\cdots,f_n)}$を**変形Kronecker積**と呼ぶことにする．

変形Kronecker積を用いるためにGに関する次の条件を考える．

Hypothesis 16. H と H' を群 G の部分群で $H \triangleleft G = HH'$ をみたすとする. また $U = H \cap H'$, $|U| = u$, $|H| = su$, $|H'| = us'$ とおく.

(i) $D = [D_{ij}] \in \mathrm{M}_t(\mathbb{Z}[H])$ $(t = u\lambda/s)$ は部分群 U_i $(1 \leq i \leq t)$ に関する $\mathbb{Z}[H]$ 上の $\mathrm{GH}(s, u, \lambda)$ 行列とする.

(ii) $W = [W_{\ell m}] \in \mathrm{M}_{t'}(\mathbb{Z}[H'])$ $(t' = u\lambda'/s')$ は部分群 U に関する $\mathbb{Z}[H']$ 上の $\mathrm{GH}(s', u, \lambda')$ 行列とする.

Hypothesis 16 のもとで次が成り立つ.

Theorem 17. Hypothesis 16 の仮定と記号のもとで各 i $(1 \leq i \leq t)$ について中への同型写像 $f_i : H' \longrightarrow G$ が次をみたすとする.

$$U^{f_i} = U_i, \quad G = H(H')^{f_i} \tag{7}$$

このとき $\Delta = \{1, \cdots, t\} \times \{1, \cdots, t'\}$ とおけば次が成り立つ.

(i) tt' 次正方行列 $D \otimes W^{(f_1, \cdots, f_t)}$ は 部分群達 $U_{(i,\ell)} = U_i$ $((i, \ell) \in \Delta)$ に関する $\mathbb{Z}[G]$ 上の $\mathrm{GH}(ss', u, u\lambda\lambda')$ 行列である.

(ii) $D \otimes W^{(f_1, \cdots, f_t)}$ から得られる transversal design が symmetric であるための必要十分条件は D から得られる transversal design が symmetric となることである.

Example 18. $W = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$. とおくと W は $\mathbb{Z}_3$ 上の $\mathrm{GH}(3, 1)$ 行列である. $D = [D_{ij}]$ を Example 8 で得られた $\mathbb{Z}[H]$ 上の $\mathrm{GH}(3, 3, 2)$ 行列とする $(H = \langle a, b \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3)$. 中への同型写像 f_1, $f_2 : \mathbb{Z}_3 \longrightarrow H$ を $f_1(x) = b^x$, $f_2(x) = a^x$ $(x \in \mathbb{Z}_3)$ で定める. このとき, Theorem 17 を繰り返し適用して得られる $D \otimes (\otimes_{i=1}^{n} W)^{(f_1, f_2)}$ は $\mathbb{Z}[H]$ 上の $\mathrm{GH}(3, 3, 2 \cdot 3^n)$ 行列である. Theorem 17 より対応する transversal design は non-symmetric である.

Example 19. $D = [D_{ij}]$ を Example 10 で得られた $\mathbb{Z}[H]$ 上の $\mathrm{GH}(3, 3, 4)$ 行列とする $(H = \langle a, b \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3)$. この行列から得られる transversal design が non-symmetric であることは Theorem 12 を用いて容易に確かめられる. 一方, 中への同型写像 f_i $(1 \leq i \leq 4)$: $\mathbb{Z}_3 \longrightarrow H$ を $f_i(x) = a^x$ $(i = 1, 3)$ および $f_i(x) = b^x$ $(i = 2, 4)$ $(x \in \mathbb{Z}_3)$ で定義するとき $\mathbb{Z}[H]$ 上の $\mathrm{GH}(3, 3, 3^n 4)$ 行列 $D \otimes (\otimes_{i=1}^{n} W)^{(f_1, \cdots, f_4)}$ を得る. Theorem 17 より対応する $\mathrm{TD}_{3^n 4}[3^{n+1}4; 3]$ は non-symmetric である.

Theorem 17 から次を得る.

Corollary 20. H_1, H_2 を G の正規部分群で $G = H_1H_2$, $U = H_1 \cap H_2$, $|U| = u$ をみたすとする. $i = 1, 2$ に対して $D_i \in M_{t_i}(\mathbb{Z}[G])$ を 部分群 U に関する $\mathbb{Z}[H]$ 上の $\mathrm{GH}(s_i, u, \lambda_i)$ 行列する $(t_i = \frac{u\lambda}{s_i})$. このとき, $D_1 \otimes {D_2}^{\mathrm{id}_U}$ は $\mathbb{Z}[G]$ 上の $\mathrm{GH}(s_1s_2, u, \lambda_1\lambda_2 u)$ 行列である. ここで, id_U は恒等写像とする.

Remark 21. Corollary 20 は Davis の半正則相対差集合に対する product construction ([3]) の一般化である.

部分群における $\mathrm{GH}(s, u, \lambda)$ の構成

群 G における空でない部分集合 X に対して G における X の normal closure X^G を $X^G = \langle g^{-1}Xg : g \in G \rangle$ で定める. この記号のもとで, ある群における $\mathrm{GH}(s, u, \lambda)$ から, その部分群おける $\mathrm{GH}(s_1, u, \lambda)$ を得る方法について述べる.

Proposition 22. H を位数 su の群とする. $[D_{ij}] \in \mathrm{M}_t(\mathbb{Z}[H])$ を位数 u の部分群達 U_i $(1 \le i \le t)$ に関する $\mathbb{Z}[H]$ 上の $\mathrm{GH}(s, u, \lambda)$ 行列とする. H の部分群 N が $N \ge \langle U_1^H, \cdots, U_t^H \rangle$ をみたすとして $|N| = s_1u$, $r = [H : N]$ とおく. さらに N に関する右剰余類分解を $H = g_1N \cup g_2N \cup \cdots \cup g_rN$ とする. このとき, $D_{(i,\ell),(j,m)} = N \cap {g_\ell}^{-1} D_{ij} g_m$ とおけば rt 次正方行列 $[D_{(i,\ell),(j,m)}] \in M_{rt}(\mathbb{Z}[N])$ は $U_{(i,j)} = {g_j}^{-1} U_i g_j$ $(1 \le i \le t, 1 \le j \le r)$ に関する $\mathbb{Z}[N]$ 上の $\mathrm{GH}(s_1, u, \lambda)$ 行列である.

Example 23. $[D_{ij}]$ を Example 9 で得られた群 $H = \langle a, b \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_6$ 上の $\mathrm{GH}(6, 3, 4)$ 行列として, $N = \langle U_1^H, U_2^H \rangle (= \langle U_1, U_2 \rangle)$ とおく. このとき, $N = \langle a, b^2 \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ である. N に関する H の右剰余類分解を $H = 1N + bN$ とおくと Proposition 22 より GH(3,3,4) 行列が得られるが, これが Example 10 で既に与えた例となっている.

参考文献

[1] Akiyama, M. Ogawa and C. Suetake, On $STD_6[18;3]$'s and $STD_7[21;3]$'s admitting a semiregular automorphism group of order 9, preprint.

[2] T. Beth, D. Jungnickel and H. Lenz, "Design Theory" Volume I, Second Edition, Cambridge University Press, 1999.

[3] J. A. Davis, A Note on Products of Relative Difference Sets, Designs, Codes and Cryptography, Vol. 1 (1991), 117-119.

[4] Y. Hiramine, Modified generalized Hadamard matrices and constructions for transversal designs, submitted

[5] D. Jungnickel, On automorphism groups of divisible designs, Canad. J. Math. Vol. 34, 1982, 257–297.

[6] H. Lüneburg, "Translation Planes", Springer-Verlag, Berlin-Heidelberg-New York, 1980.

Quadratic Planar Functions について

近畿大学・理工学部・理学科
中川 暢夫

Section 1 序

pを奇素数とし、VとWを$GF(p)$上のn次元ベクトル空間とする。
$f: V \mapsto W,\ x \mapsto f(x)$と$a \in V\ (a \neq 0)$に対し、

$$\Delta_a(f)\ : V \mapsto W,\ \ x \mapsto f(x+a) - f(x)$$

をaについてのfの差分関数という。

(定義) 零でない任意の$a \in V$に対して、$\Delta_a(f)$がbijectionであるときfはplanar function(またはPN-function)という。

上記のfについて、

$$b_f(x,y) = f(x+y) - f(x) - f(y) + f(0)$$

と定める。
(定義) 上の$b_f(x,y)$がsymmetric bilinear formになるとき、fをquadratic functionであるという。

注意 1
fがquadraticであるための必要十分条件は

$$f(x+y+z) = f(x+y) + f(y+z) + f(z+x) - f(x) - f(y) - f(z) + f(0)$$

が成り立つことである。

注意 2
$V =< e_1, e_2, \cdots, e_n >,\ W =< u_1, u_2, \cdots, u_n >$とする。

$$f(\sum_{i=1}^{n} x_i e_i) = \sum_{i=1}^{n} f_i(x_1, x_2, \cdots, x_n) u_i$$

となっているとき、$f_i(x_1, x_2, \cdots, x_n)$が$f$の第$i$座標関数である。さて、$f$の各座標関数が$GF(p)$上$x_1, x_2, \cdots, x_n$に関する対称2次形式ならば、$f$はquadraticである。
特に

$$f: GF(p^n) \mapsto GF(p^n),\ \ f(x) = \sum_{i<j} a_{i,j} x^{p^i} x^{p^j}$$

なる形の関数はquadraticである。

Section 2 Quadratic planar functions と commutative semifields の構成。

f を V から W への quadratic planar function とする。
$GF(P)$ 上のベクトル W に積を導入しよう。まず、V の零でない元 e を一つ取り出す。つぎに

$$\Delta_e(f)(a) = 0$$

なる $a \in V$ を考える。このような a は唯一つ存在する。

$$g(x) := f(x+a) - f(a) \quad (\forall x \in V)$$

と定める。このとき、g はまた quadratic planar である。この g は元 e による f の正規化と呼ばれる。

$$g(0) = f(a) - f(a) = 0, \ \ g(e) = f(e+a) - f(a) = \Delta_e(f)(a) = 0.$$

以下 f の e による正規化関数を改めて f とかく。

$$\Delta_e(f) : \ V \mapsto W$$

の逆写像を φ とする。($\varphi : \ W \mapsto V$) さて、

$$x \circ y = b_f(\varphi(x), \varphi(y))$$

と定義する。
(2.1). ($\varphi(x) = 0$ ならば、 $x = 0$)
なぜなら, $x = \Delta_e(f)(\varphi(x)) = f(\varphi(x) + e) - f(\varphi(x))$

(2.2). $(W, +, \circ)$ は零因子をもたない。
なぜなら、$x \circ y = 0$ かつ $x \neq 0$ とせよ。(2.1) より、$\varphi(x) \neq 0$. また、$f(\varphi(x) + \varphi(y)) - f(\varphi(x)) - f(\varphi(y)) = 0$ だから、$\Delta_{\varphi(x)}(f)(\varphi(y)) = f(\varphi(x)) = \Delta_{\varphi(x)}(f)(0)$. $\Delta_{\varphi(x)}(f)$ が bijection より、$\varphi(y) = 0$. ゆえに、(2.1) より、$y = 0$.

(2.3). $\Delta_e(f)$ は V から W への isomorphism である。
なぜなら $\Delta_e(f)(u+v) = f(u+v+e) - f(u+v)$ $\Delta_e(f)(u) = f(u+e) - f(u)$, $\Delta_e(f)(v) = f(v+e) - f(v)$ $f(e) = 0$ に注意すれば、f が quadratic より $\Delta_e(f)(u+v) = \Delta_e(f)(u) + \Delta_e(f)(v)$.

(2.4). $(W, +, \circ)$ で、分配律が成立する。
まず、$\Delta_e(f)$ の逆関数 φ も和を保つ。$\varphi(x + x') = \varphi(x) + \varphi(x')$ に注意して、

$$(x + x') \circ y = f(\varphi(x) + \varphi(x') + \varphi(y)) - f(\varphi(x) + \varphi(x')) - f(\varphi(y)) =$$

$$f(\varphi(x)+\varphi(y))+f(\varphi(x')+\varphi(y))-f(\varphi(x))-f(\varphi(x'))-2f(\varphi(y))=$$
$$x\circ y+x'\circ y.$$

(2.5). $f(2e)$ は $(W,\circ)$ の単位元である。
なぜなら、$\Delta_e(f)(e)=f(e+e)-f(e)=f(2e)$ より、$\varphi(f(2e))=e$ すると、$x\circ f(2e)=f(\varphi(x)+\varphi(f(2e)))-f(\varphi(x))-f(\varphi(f(2e)))=f(\varphi(x)+e)-f(\varphi(x))-f(e)=\Delta_e(f)(\varphi(x))=x$.

Section 3 Commutative semifields と quadratic planar functions の再構成および平方写像。

Commutaive semifield $(E,+,\circ)$ に対し平方写像 $f(x)=x\circ x : E\mapsto E$ が planar であることはすぐ確認できる。今、qoadratic planar function $f:V\mapsto W$ に対して

$$x\circ y=b_f(\varphi(x),\varphi(y))$$

により W は commutative semifild であることは前のセクションでみたとおりである。$f(0)=f(e)=0,\varphi=\Delta_e(f)^{-1}$ であったことに留意せよ。また、$\Delta_e(f)$ は V から W への isomorphism であった。では、W の平方写像ともとの quadratic planar function f との関係はどうなっているのかを見てみよう。

$$V\mapsto W\mapsto W,\ \ u\mapsto\Delta_e(f)(u)\mapsto\Delta_e(f)(u)\circ\Delta_e(f)(u)$$

を g とおくと、$g(u)=f(2u)-2f(u)$ となる。
$u=(x_1,x_2,\cdots,x_n)$ に対し、f の各座標関数 $f_i(x_1,x_2,\cdots,x_n)$ が $x_1,x_2,\cdots,x_n$ の2次形式なら、$g(u)=2f(u)$ となる。

planar function $f:V\mapsto W$ に対し、$\mathbf{P}:V\times W$ を points set,
$\mathbf{L}:D+(a,\alpha),L_c\ \ (a,c\in V,\ \alpha\in W)$, ここで、$D:=\{(x,f(x))\mid x\in V\},\ L_c:=\{(c,y)\mid y\in W\}$ を lines set として affine plane $\mathbf{A}(f)$ が構成される。

commutative semifield W からも $W\times W$ を points set とする affine plane $\mathbf{A}(W)$ が自然に構成される。lines sets は傾き ∞ の直線達と

$$y=m\circ x+k\ \ (m,k\in W)$$

で表される直線達である。

planar function $f : V \mapsto W$ から出発するとき、$\mathbf{A}(f) \cong \mathbf{A}(W)$ が成り立つ。また $g(x) = f(2x) - 2f(x)$ のとき、$\mathbf{A}(f) \cong \mathbf{A}(g)$ も成り立つ。

Section 4 E-A equivalence と CCZ equivalence

二つの写像 $f, g : V \mapsto W$ に対し

$$g = A_1 f A_2 + A_3$$

が成り立つとき f と g は**Extended affine 同値**という。ここで、$A_2 : V \mapsto V$ affine bijective, $A_1 : W \mapsto W$ affine bijective, $A_3 : V \mapsto W$ affine maps である。このとき、$f \sim g$ (EA) とかく。

また、$V \times W$ 上の affine bijective L があって、$L(G_f) = G_g$ が成り立つとき f と g は**CCZ 同値**という。

ここで、G_f と G_g はそれぞれ f と g の graph である。また、$L(x, y) := (L_1(x, y), L_2(x, y))$ で、L_1 は $V \times W$ から V への affine injective, 、L_2 は $V \times W$ から W への affine injective で $V \mapsto V \times W \mapsto V$, $x \mapsto (x, f(x)) \mapsto L_1(x, f(x))$ は bijective である。このとき、$f \sim g$ (CCZ) とかく。

(4.1) $f, g : V \mapsto W$ に対し, $f \sim g$ (EA) ならば $f \sim g$ (CCZ) である。

(4.2) $f, g : V \mapsto W$ and f を planar とする。$f \sim g$ (CCZ) ならば、g も planar である。

(4.3) $f, g : V \mapsto W$ and f を quadratic とする。$f \sim g$ (EA) ならば、g も quadratic である。

(4.4) $f, g : V \mapsto W$ and f を quadratic planar とする。$f \sim g$ (EA) ならば、$\mathbf{A}(f) \cong \mathbf{A}(g)$ である。

(4.5)(Budaghyan-Helleseth) $f, g : V \mapsto W$
f を planar とする。$f \sim g$ (EA) と $f \sim g$ (CCZ) は同値である。

Section 5 Commutative semifields の平方写像

これまでにあまり多くの Commutative semifields は構成されていない。既知のほとんどの Comm. semifields の平方写像は quadratic planar function になっている。

(1): Dickson semifields の平方写像。
(2): Cohen-Ganley semifields の平方写像。
(3): Ganley semifields の平方写像。
(4): Penttilia-Williams semifields の平方写像。
(5): Couter-Mattews semifields の平方写像。

(6): Ding-Yuan semifields の平方写像。
(7): Couter-Henderson-Kosick semifields の平方写像。
(8): Budaghyan-Heleseth semifields の平方写像。
(8) の Case の quadratic planar functions は次のように記述される。

s,k は正の整数で、$2^\ell|(p^s+1)$, $2^{\ell+1}\not|(p^k+1)$、 $\sum_{i=0}^{k-1}c_ix^{p^i}$ を $GF(p^n)$ 上 bijective とする。 また、$b\neq 0$, し、$gcd(k+s,2k)=gcd(k+s,2k)$ または $(p^{gcd(k,s)}-1)\not|((p^k-p^s)/2)$ とする。
このとき、

$$f(x)=(bx)^{p^s+1}-(bx)^{p^{s+k}+p^k}+\sum_{i=0}^{k-1}c_ix^{p^{i+k}+p^i}$$

は $GF(p^n)$ 上 quadratic planar function である。

(Problem)
Commutative semifields の平方写像は quadratic planar fuction であるか。"否" ならこの反例を与えよ。

Section 6 正則な symmetric 3-cubes と commutative semifields

$F=GF(p^e)$ 上の n 次 3-cube とは、n^3 個の F の要素の配列

$$(a_{i,j,k})=\{(a_{i,j,k})|\, a_{i,j,k}\in F, 1\leq i,j,k\leq n\}$$

をいう。これを n 個の n 次行列とみることができる。
k をパラメータとする配置を「正面から裏面への配置」ということにすると、

$$A_1=(a_{i,j,1}),A_2=(a_{i,j,2}),\cdots,A_n=(a_{i,j,n})$$

がその配置で、j をパラメータとする配置を「左の面から右の面への配置」ということにすると、

$$B_1=(a_{i,1,k}),B_2=(a_{i,2,k}),\cdots,B_n=(a_{i,n,k})$$

がその配置で、
i をパラメータとする配置を「上面から下面への配置」ということにすると、

$$C_1=(a_{1,j,k}),C_2=(a_{2,j,k}),\cdots,C_n=(a_{n,j,k})$$

がその配置となる。

3次の置換 S_3 の元 σ と n 次の 3-cube $(a_{i,j,k})$ に対し、$(a_{\sigma(i),\sigma(j),\sigma(k)})$ を $(a_{i,j,k})^\sigma$ で表す。

これらの6つの置換は「正面から裏面への配置」、「左の面から右の面への配置」、および「上面から下面への配置」の間の入れ替えと各配置における転置行列をとることに相当する。

（定義） n 次の 3-cube $(a_{i,j,k})$ が正則であるとは、

$$\alpha_1 A_1 + \alpha_2 A_2 + \cdots + \alpha_n A_n$$

が非正則ならば常に $\alpha_1 = 0, \alpha_2 = 0, \cdots, \alpha_n = 0$ となるときにいう。

(6.1)(D.Knuth) 任意の $\sigma \in S_3$ を与える。3-cube $(a_{i,j,k})$ が正則ならば、$(a_{i,j,k})^\sigma$ も正則である。

（例） 下記の cube は $GF(3)$ 上の3次3-cube である.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

p を奇素数とし、$\Omega = \{A_1, A_2, \cdots, A_n\}$ を各 A_i が対称行列であるような $GF(p)$ 上の 3-cube とする。また、V を $GF(p)$ 上の n 次元ベクトル空間とし、$e_1, e_2, \cdots, e_n$ をその基底とする。V に次のように積を入れる。任意の $x = \sum_{i=1}^n x_i e_i$, $y = \sum_{j=1}^n y_j e_j \in V$ に対し、

$$x \circ y := \sum_{i=1}^{n} (x_1, x_2, \cdots, x_n) A_i (y_1, y_2, \cdots, y_n)^T e_i.$$

このとき、$V(+, \circ)$ が零因子をもたなければ、可換 semifield である。また、3-cube Ω が正則ならば、$V(+, \circ)$ は commutaive semifield であり、その逆も成り立つ。

参考文献

[1] L.Budaghyan and T.Helleseth, New perfect nonlinear multinomials over F_p^{2k} for any odd prime p, submitted.

[2] P.Dembowski and G.T.Ostrom, Planes of Order n with Collineation Groups of Order n^2, Math.Z. 103(1968), 239-258.

[3] E.D.Knuth, Finite SEmifields and Projective Planes, J.Algebra 2(1965), 182-217.

[4] K.Minami and N.Nakagawa, On planar functions of elementary abelian p-group type,Hokkaido Mathematical Jounal 37,No3(2008) 531-544.

[5] N.Nakagawa, On Polynomial Families in n Indeterminates over Finite Prime Fields Coming from PLanar Functions, Proceedings of the sixth Conference of Finite Fields with Applications to Coding Theory, Crytography and related Areas, Springer.

パラメーター $(276, 140, 58, 84)$ の強正則グラフの新しい例の構成

野崎寛

東北大学大学院情報科学研究科数学教室
日本学術振興会特別研究員 PD
nozaki@ims.is.tohoku.ac.jp

1 概要

パラメーター $(276, 140, 58, 84)$ の強正則グラフについては，具体例が一つだけ Goethals-Seidel により構成されていた [7]．また，1984 年の Brouwer-Lint による Survey paper で，このパラメーターを持つ強正則グラフが一意的かどうかという問題が提示されている．現在知られているパラメーター $(276, 140, 58, 84)$ の強正則グラフ $G = (V, E)$ に，Seidel switching と呼ばれる操作を施し，パラメーター $(276, 140, 58, 84)$ の強正則グラフの新しい例の構成を行う．強正則グラフの Seidel switching から，新たな強正則グラフを構成できるとき，その強正則グラフは Regular two-graph と呼ばれる対象から構成できることが知られている [2]．また Regular two-graph は幾何学的には，ある種の上界を満たすユークリッド空間上の equiangular lines と同一視されることが知られている．ここでは，その equiangular lines に注目し，幾何学的な視点から Bose-Shrikahande が与えていた強正則グラフの switching に関する定理を簡略化する．

2 準備

$G := (V, E)$ を単純グラフ（ループ辺，重複辺がない）とする．$G = (V, E)$ がパラメーター (n, k, λ, μ) の強正則グラフと呼ばれるのは，次の 4 条件を満たす時である．

(1) $|V| = n$.

(2) 任意の $v \in V$ に対して，$|\{\{v, u\} \mid u \in V, \{v, u\} \in E\}| = k$ (k-正則).

(3) 任意の $\{v, u\} \in E$ に対して，$|\{t \in V \mid \{t, u\} \in E, \{t, v\} \in E\}| = \lambda$.

(4) 任意の $\{v, u\} \notin E$ $(u \neq v)$ に対して，$|\{t \in V \mid \{t, u\} \in E, \{t, v\} \in E\}| = \mu$.

強正則グラフとその補グラフがどちらも連結なとき，原始的であると呼ぶ．強正則グラフの補グラフは，また強正則グラフとなる．グラフ G に対する $(0, 1)$ 隣接行列 A は，V により添え字づけられた行列で，その成分は，$\{u, v\} \in E$ のとき $M(u, v) = 1$，その他の成分は 0 と定義される．グラフ G に対する $(0, 1, -1)$ 隣接行列 B は，V により添え字づけられた行列で，その成分は，$\{u, v\} \in E$ のとき $M(u, v) = -1$，$\{u, v\} \notin E$ のとき $M(u, v) = 1$，対角成分は 0 と定義される．

$H_1 \subset V$, $H_2 \subset V$ $(H_1 \cup H_2 = V(\text{disjoint union}))$ に対して，$E' := \{\{u, v\} \in E \mid u \in H_1, v \in H_1\} \cup \{\{u, v\} \in E \mid u \in H_2, v \in H_2\} \cup \{\{u, v\} \notin E \mid u \in H_1, v \in H_2\}$ と定義する． $H_1 \subset V$, $H_2 \subset V$ に関する switching とは，辺集合を $(V, E) \to (V, E')$ と変化させる操作である．また，単に H_1 に関する switching とも呼ぶ．これは H_1 と H_2 の間の隣接関係を逆転させることを意味している．単純グラフの switching に関する同値類を switching class と呼ぶ．

任意の G から，ユークリッド空間 $\mathbb{R}^d$ へ，equiangular lines としての埋め込みが知られている．$(0, 1, -1)$ 隣接行列 B の最小固有値を $-\rho < 0$，その重複度を m とする．そのとき，$B + \rho I$ は半正定値な対称行列であり，ユークリッド空間 $\mathbb{R}^{|V|-m}$ 上の有限集合と同一視される．つまり，単位球面 $S^{|V|-m-1}$ 上の有限集合 X でグラム行列 $M(x, y) = (\langle x, y \rangle)_{x,y \in X} = 1/\rho B + I$ を持つものが存在している（$\langle x, y \rangle$ は標準内積）．ここで，$A(X) := \{\langle x, y \rangle \mid x, y \in X, x \neq y\} = \{\pm 1/\rho\}$ であり，equiangular lines と同一視できる．

特に B の固有値が2つしかない場合，そのグラフから得られる equiangular lines は直線の個数に対する上界 $|V| \leq d(\rho^2-1)/(\rho^2-d)$ を達成することが知られている．また，B の固有値が2つしかない，単純グラフの switching class は Regular two-graph と呼ばれる対象と同一視出来ることが知られている．Regular two-graph と同一視できる switching class を，Regular two-graph に関する switching class と呼ぶことにする．ここでは，Regular two-graph の定義は行わない．

強正則グラフは，クラス2の対称なアソシエーションスキームとして知られている [1]．$A_0 = I$（単位行列），強正則グラフの $(0,1)$ 隣接行列を A_1，補グラフの $(0,1)$ 隣接行列を A_2 とする（$A_0 + A_1 + A_2 = J$(all one matrix)）．A_0，A_1，A_2 で生成される代数を Bose-Mesner 代数と呼ぶ．強正則グラフの Bose-Mesnar 代数の原子冪等元 $E_0 = I/v$，E_1，E_2 （$E_iE_j = \delta_{i,j}E_i$，$\delta_{i,j} = 1(i=j), \delta_{i,j} = 0(i \neq j)$ ）は一意的に定まり，実成分の対称行列であることが知られている．m_i を E_i のランクとする．各 E_i を用いて，次のように，強正則グラフ（アソシエーションスキーム）の頂点集合をユークリッド空間の単位球面 S^{m_i-1} に埋め込むことが出来る：

$$x \in V \to \sqrt{\frac{n}{m_i}} E_i e_v.$$

ここで，$n = |V|$，$e_x \in \mathbb{R}^v$ は x 番目の成分が1で他の成分は0の列ベクトルある．ここで，冪等元の性質から，$E_i^T E_i = E_i E_i = E_i$ であるから，E_i は半正定値行列である．また E_i の対角成分は一定 m_i/n であり，$\sqrt{n/m_i}E_i$ の列ベクトルたちは S^{m_i-1} 上の集合と同一視できる．

ここで，球面上の有限集合とアソシエーションスキームの関係を考察するうえで，特に重要な球面有限集合の性質である，s 距離集合と球面 t デザインの性質を紹介する．X を球面 S^{d-1} 上の有限集合とする．上で定義した $A(X)$ の個数が s 個のとき X を s 距離集合と呼ぶ．$\mathrm{Harm}_l(\mathbb{R}^d)$ を d 変数 l 次斉次調和多項式の線形空間とする．ここで，調和多項式とはラプラシアン $\Delta := \sum_{i=1}^{d} \partial^2/\partial x_i^2$ の作用で0になる関数である．X が球面 t デザインと呼ばれるのは，任意の $f \in \mathrm{Harm}_l(\mathbb{R}^d)(1 \leq l \leq t)$ に対して $\sum_{x \in X} f(x) = 0$ となるときである．s 距離集合と球面 t デザインの s と t に対して，$t \geq 2s-2$ を満たす X は内積を関係にもつクラス s のアソシエーションスキームの構造を持つことが知られている [6]．つまり，$A(X) := \{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ に対して，$(x,y) \in R_i \Leftrightarrow \langle x,y \rangle = \alpha_i$ と関係づけたとき，$\{X, \{R_i\}_{i=0,1,\ldots,s}\}$ がアソシエーションスキームとなる．強正則グラフについては，2距離集合で $t \geq 2$ のときに X は強正則グラフの構造を持つ．また原始的な強正則グラフの E_i に関する球面の埋め込みは，2距離集合，2デザインであることが知られている [5]．E_i は A_i たちの線形結合で書かれることから，E_i に関する埋め込みは，内積として関係を保存していることが分かる．つまり，球面上の2距離集合，2デザインを分類することは，原始的な強正則グラフを分類することに他ならない．

3 主結果

$S(G,H)$ をグラフ $G=(V,E)$ から $H \subset V$ に関する switching から得られるグラフとする．H の誘導部分グラフとは，G の隣接関係を保存するグラフ $(H, \{\{u,v\} \mid u,v \in H, \{u,v\} \in E\})$ のことである．強正則グラフの switching に関して，次の定理が知られている [2]．

Theorem 3.1. $G=(V,E)$ をパラメーター (v,k,λ,μ) の強正則グラフとする．H_1 を V の部分集合とし，$H_2 := V \setminus H_1$ とする．また h_i を H_i の元の個数とする．$2k - v/2 = \lambda + \mu$ を仮定したとき，次が同値である．

(i) $S(G,H_1)$ が強正則グラフである．

(ii) H_1 の誘導部分グラフが w_1-正則かつ H_2 の誘導部分グラフが w_2-正則で，次の等式を満たす．

$$w_1 - w_2 = \frac{h_1 - h_2}{2}.$$

強正則グラフの switching から強正則グラフ（同じパラメーターとは限らない）が得られるとき，その強正則グラフは $2k - v/2 = \lambda + \mu$ を満たさなければならない [2]．$2k - v/2 = \lambda + \mu$ を満たす距離正則グラフは，Regular two-graph の switching class に含まれることが知られている [3]．強正則グラフの switching から同じパラメーターの強正則グラフが得られるのは次の場合である [2]．

Theorem 3.2. 仮定は *Theorem 3.1* と同じである．

(i) $S(G,H_1)$ が強正則グラフである．

(ii) H_1 の全ての元が $h_2/2$ 個の H_2 の元と隣接し，H_2 の全ての元が $h_1/2$ 個の H_1 の元と隣接している．

switching から得られる強正則グラフが同じパラメーターを持たないとき，そのパラメーターは $(v, k+c, \lambda+c, \mu+c)$ となることが分かる．ここで $c = v/2 - 2\mu$．θ_1 を G の $(0,1)$ 隣接行列の k とは異なる正の固有値であるとする．$2k - v/2 = \lambda + \mu$ を満たす強正則グラフ，またその補グラフは $v = 2(k - \theta_1)$ を満たす．switching に関する 2 つの定理を次の様に簡略化した．

Theorem 3.3. $G = (V, E)$ をパラメーター (v, k, λ, μ) の原始的な強正則グラフであるとする．H を V の部分集合で，元の個数を h とする．このとき，$v = 2(k - \theta_1)$ を仮定すると次が同値である．
(i) $S(G, H)$ がパラメーター (v, k, λ, μ) の強正則グラフである．
(ii) H の誘導部分グラフが $(k - \frac{v-h}{2})$-正則である．

Theorem 3.4. 仮定は *Theorem 3.3* と同じである．$c = v/2 - 2\mu$ とする．
(i) $S(G, H)$ がパラメーター $(v, k+c, \lambda+c, \mu+c)$ の強正則グラフである．
(ii) H の誘導部分グラフの頂点数が $v/2$ であり，$(k - \mu)$-正則である．

4 主結果の証明

この節では主結果の証明の概略を述べる．詳細は [8] を参照されたい．
Theorem 3.3 の証明では，次の補題が重要である．

Lemma 4.1. $G = (V, E)$ を $v = 2(k - \theta_1)$ を満たす，原始的な強正則グラフであるとする．そのとき，E_2 に関する球面への埋め込みが *equiangular lines* としての球面への埋め込みと一致する．

この補題から，equiangular lines の埋め込みが球面 2 デザインであることが分かる．equiangular lines としての埋め込みの写像を $\varphi : V \to X$ とする．グラフの $H \subset V$ に関する switching を equiangular lines として解釈すると，対応する $\varphi(H)$ を極対的な集合である $-\varphi(H)$ に移動させることを意味している．$S(G, H)$ の equiangular lines としての球面への埋め込みを X_H とすれば，$X_H = (X \setminus \varphi(H)) \cup (-\varphi(H))$ となる．このとき，X_H は 2 距離集合の性質を保つことに注意されたい．ここで X_H が 2 デザインとなれば，X_H すなわち $S(G, H)$ は強正則グラフの構造を持つことになる．また逆に，$S(G, H)$ が強正則グラフの構造を持つならば，X_H が 2 デザインでなければならないことが示される．X_H が 2 デザインであることと，$\varphi(H)$ が 1 デザインであることは同値である．また，$\varphi(H)$ が 1 デザインであることと，H の誘導部分グラフが $(k - \frac{v-h}{2})$-正則であることが同値である．これは，Theorem 3.3 を意味している．
Theorem 3.4 の証明では，次の補題が重要である．

Lemma 4.2. $G = (V, E)$ を $v = 2(k - \theta_1)$ を満たす，原始的な強正則グラフであるとする．また，$c = v/2 - 2\mu$ とする．もし，$S(G, H)$ がパラメーター $(v, k+c, \lambda+c, \mu+c)$ の強正則グラフとなる様な H が存在したとすれば，E_2 に関する球面への埋め込みは高々 $m_2 - 1$ 次元の平行な 2 つの超平面の上に存在する．

$\varphi(H)$ は一つの超平面に乗っている．さらに，1 デザインの性質から，H の元の個数は $v/2$ であることが分かる．H に関する switching は，$\varphi(H)$ を $-\varphi(H)$ に移動させることを意味していたから，X_H は一つの超平面に乗ることになる．H の個数が決まれば，Theorem 3.1 から H の性質を絞ることが出来る．

5 応用

Theorem 3.3 を適用して，パラメーター $(276, 140, 58, 84)$ の強正則グラフの新しい例を構成する．以下は Magma による計算である．まず，[2] から，一つだけ知られていた具体例 G を取り出す．G の誘導部分グラフで 6 点完全グラフ（すべての異なる頂点間に辺がある）であるものを全て抜き出す．このとき 6 点完全誘導部分グラフは Theorem 3.3 を満たしている．G の自己同型群 $\mathrm{Aut}(G)$ を構成する．自己同型で移りあう誘導部分グラフ H，H' から与えられる $S(G, H)$，$S(G, H')$ は明らかに同型であるから，自己同型で移りあわない 6 点完全誘導部分グラフの代表を抜き出す．現在知られているパラメーター $(276, 140, 58, 84)$ の強正則グラフは，そのような 6 点完全誘導部分グラフを 6 つだけ持っている．このそれぞれの switching から互いに同型でない同じパラメーターをもつ強正則グラフを新たに 5 つ構成することが出来る．自己同型群で移りあわない誘導部分グラフたちでも，同型な $S(G, H)$ を与える可能性があることに注意されたい．グラフの同型判定は Magma の組み込み関数を用いた．得られた 5 つの新しい強正則グラフに対しても，同じ操作を行うことが出来る．この操作を繰り返すことで，10 万以上の互いに非同型な強正則グラフを構成することに成功した（実際には計算機が止まりそうになかったので停止させた）．

この異常に多くの非同型な球面デザインが構成できたことを球面デザインの理論で解釈すると自然である．Theorem 3.3 の (ii) の条件は，H の埋め込み先である $\varphi(H)$ が球面 1 デザインであることと同値である．2 つの球面 t デザイン X，X' が共通部分を持たない（disjoint）とき，その二つの和集合はまた球面 t デザインである．つまり，6 点完全誘導部分グラフたちの disjoint な和集合はまた，Theorem 3.3 の (ii) の条件を満たしている．初めに与えられていた強正則グラフは，6 点完全誘導部分グラフを 27000 以上含んでいた．これらを適当に組み合わせれば，膨大な数の条件を満たす H を構成することができる．ゆえに，10 万個の新しい例はほんの一部に過ぎないことが，容易に推測されるだろう．

パラメーター $(276, 140, 58, 84)$ の強正則グラフに Theorem 3.4 を適用したときに得られるパラメーターは $(276, 110, 28, 54)$ である。このパラメーターの強正則グラフは非存在であることが知られている．これを球面の理論で解釈する．Theorem 3.4 の証明から，このグラフは 2 距離集合として，S^{21} に埋め込められなければならない．しかし，距離集合の元の個数にはある種の自然な上界が知られており，S^{21} 上の 2 距離集合の元の個数は 275 以下である．ここから，矛盾を導ける．

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin/Cummings, 1984.

[2] R.C. Bose and S.S. Shrikhande, Graphs in which each pair of vertices is adjacent to the same number d of other vertices, *Studia Sci. Math. Hungar.* 5 (1970), 181–195.

[3] A.E. Brouwer, A.M. Cohen and A. Neumaier, *Distance-Regular Graphs*, Springer-Verlag, 1989.

[4] A.E. Brouwer and J.H. Lint, Strongly regular graphs and partial geometries, *Enumeration and design (Waterloo, Ont., 1982)*, 85–122, *Academic Press, Toronto, ON*, 1984.

[5] P.J. Cameron, J.M. Goethals and J.J. Seidel, Strongly regular graphs having strongly regular subconstituents, *J. Algebra* 55 (1978), 257–280.

[6] P. Delsarte, J.M. Goethals, and J.J. Seidel, Spherical codes and designs, *Geom. Dedicata* 6 (1977), no. 3, 363–388.

[7] J.M. Goethals and J.J. Seidel, The regular two-graph on 276 vertices, *Discrete Math.* 12 (1975) 143–158.

[8] H. Nozaki, New strongly regular graphs from switching of edges, arXiv:0909.2603.

A collection of subgroups for the generalized Burnside ring

小田 文仁* 澤辺正人†

[OS09] の概略を報告する.

G を有限群とする. $\mathcal{D}$ を G-共役の作用で閉じている G の部分群の族とする. 有限 G-集合 X はその任意の元 $x \in X$ の G における安定化群が $\mathcal{D}$ に含まれるとき $(G,\mathcal{D})$-集合と呼ぶ. $(G,\mathcal{D})$-集合と G-写像の圏の疎な直和に関する Grothendieck 群を $\Omega(G,\mathcal{D})$ で表す. $\Omega(G,\mathcal{D})$ は $\{[G/H] \mid (H) \in C(\mathcal{D})\}$, (ただし, $[G/H]$ は可移 G-集合 G/H の同型類, $C(\mathcal{D})$ は $\mathcal{D}$ の G-共役類の集合) を自由アーベル群の基底として持つ. 特に $\mathcal{D}$ がすべての部分群の族のとき, $\Omega(G,\mathcal{D})$ は通常のバーンサイド環 $\Omega(G)$ となる.

Yoshida は [Yd90] で単位元を持つ可換環 R に対して「$R \otimes_{\mathbb{Z}} \Omega(G)$ の R-部分加群 $R \otimes_{\mathbb{Z}} \Omega(G,\mathcal{D})$ がいかなる条件下で環構造を持つか」という問題を考えた. 詳細な定義は [Yd90] または [OS09] に譲るが, $R \otimes_{\mathbb{Z}} \Omega(G)$ はある条件を満たす環構造を持つとき $\mathcal{D}$ に関する**一般バーンサイド環 (generalized Burnside ring w.r.t. $\mathcal{D}$)** と呼ばれている. Yoshida は, 特に $\mathbb{Z}$ の素数 p による局所環 $\mathbb{Z}_{(p)}(\subseteq \mathbb{Q})$ が R である場合の条件を考察した.

部分群 $H \leq G$ に対し次のように部分群 $\overline{H}$ を定める:

$$\overline{H} := \begin{cases} \bigcap_{S \in \mathcal{D}(\geq H)} S & \text{if} \quad \mathcal{D}(\geq H) \neq \emptyset, \\ G & \text{if} \quad \mathcal{D}(\geq H) = \emptyset. \end{cases}$$

ただし, $\mathcal{D}(\geq H)$ は $D \geq H$ を満たす $\mathcal{D}$ の元全体の集合とする. $S \in \mathcal{D}$ に対して, 剰余群 $WS := N_G(S)/S$ の一つの Sylow p-部分群を $(WS)_p$ と書く. Yoshida は次のような条件を与えた:

$(\mathrm{C})_p$ $S \in \mathcal{D}$, $gS \in (WS)_p \Longrightarrow \overline{\langle g \rangle S} \in \mathcal{D}$.

$(\mathrm{C}')_p$ $S \in \mathcal{D}$, $gS \in (WS)_p \Longrightarrow \langle g \rangle S \in \mathcal{D}$.

ただし, $\langle g \rangle S$ は S と g で生成される部分群とする. $(\mathrm{C}')_p \Longrightarrow (\mathrm{C})_p$ が成り立つことを注意する. さらに「すべての素数 p に対して $(\mathrm{C})_p$ が成立すること」と必要十分な以下の条件を与えた:

$(\mathrm{C})_\infty$ $S \in \mathcal{D}$, $gS \in WS \Longrightarrow \langle g \rangle S \in \mathcal{D}$.

p を素数とする. 加法群 M に対し, $M_{(p)} := \mathbb{Z}_{(p)} \otimes_{\mathbb{Z}} M$ とする. Yoshida の定理は以下の通りである:

Lemma 1. [Yd90, Theorem 3.11]

*山形大学理学部数理科学科 odaf@sci.kj.yamagata-u.ac.jp
†千葉大学教育学部数学科 sawabe@faculty.chiba-u.jp

(1) Under the condition $(\mathrm{C})_p$, $\Omega(G,\mathcal{D})_{(p)}$ *is realized as a generalized Burnside ring.*
(2) In particular, under the condition $(\mathrm{C})_\infty$, $\Omega(G,\mathcal{D})$ *is realized as a generalized Burnside ring. Furthermore, for a prime* p*, the two ring structures on* $\Omega(G,\mathcal{D})_{(p)}$ *defined by (1) and (2) coincide.*

G の非自明な p-部分群 U は 条件 $O_p(N_G(U)) = U$ を満たすとき p-根基 と呼ばれている．G の p-根基部分群の全体を $\mathcal{B}_p(G)$ と書く．$\mathcal{B}_p(G)$ の部分集合 $\mathfrak{X}$ は G-共役で閉じているものとする．例えば，$\mathcal{B}_p(G)$ の元 U で $C_G(U)$ の任意の p-元が U に含まれるもの全体は G-共役で閉じていることが知られている．それら全体を $\mathcal{B}_p^{\mathrm{cen}}(G)$ で表す．$\mathcal{B}_p^{\mathrm{cen}}(G)$ の元は中心的 p-根基部分群と呼ばれている．$\mathfrak{X}$ の極小な部分群の全体を $\mathfrak{X}_{\min}$ で表す．G の Sylow p-部分群 P を 1 つ固定し

$$\mathfrak{X}_{\min}(\leq P) := \{U_1, U_2, \ldots, U_l\}$$

とする．そのインデックス集合を $I = \{1, \ldots, l\}$ とする．$\emptyset \neq F \subseteq I$ に対し，$U_F := \langle U_i \mid i \in F \rangle$ とする．このとき G と $\mathfrak{X} \subseteq \mathcal{B}_p(G)$ に対し [OS09] の主役である族 $\mathcal{N}_G(\mathfrak{X})$ は以下のように定義される:

$$\mathcal{N}_G(\mathfrak{X}) := \{{}^gN_G(U_F) \mid g \in G, \emptyset \neq F \subseteq I\}.$$

ただし，部分群 $H \leq G$ と $g \in G$ に対し，${}^gH = gHg^{-1}$ とする．
[Sa03] で初めて取り扱われた次の二つの条件を仮定する:

Hypothesis (W). *Each* U_i $(1 \leq i \leq l)$ *is weakly closed in* P *with respect to* G*. In other words, if* ${}^gU_i \leq P$ *for some* $g \in G$ *then* ${}^gU_i = U_i$*.*

Hypothesis (P). *For any* $\emptyset \neq F \subseteq I$, $U_F \in \mathfrak{X}$*.*

仮定 (W) の下で $\mathfrak{X}_{\min}(\leq P)$ は $\mathfrak{X}_{\min}$ の G-共役類の完全代表系であること，仮定 (P) の下で $\mathcal{N}_G(\mathfrak{X})$ に含まれる部分群 H は self-normalizing, すなわち $N_G(H) = H$ を満たすことに注意する．すべての元が self-normalizing であるような族 (self-normalizing collection) $\mathcal{D}$ は $(\mathrm{C}')_p$ を満たすので, Lemma 1 の (1) により $\Omega(G,\mathcal{D})_{(p)}$ は一般バーンサイド環になる．

さらに以下の仮定を準備する:

Hypothesis (Z). *For* $(S), (T) \in C(\mathcal{D})$,

$$\sharp(T\text{-fixed points in } G/S) = \begin{cases} 1 & \text{if } T \leq {}^gS \text{ for some } g \in G, \\ 0 & \text{otherwise.} \end{cases}$$

仮定 (Z) からは次の基本的な結果が得られる:

Lemma 2. ([OS09, Lemma 7]) *Assume* (Z) *for a collection* $\mathcal{D}$ *of subgroups of* G*.*

(1) Any element S *in* $\mathcal{D}$ *is a self-normalizing subgroup of* G*.*

(2) $\mathcal{D}$ *satisfies* $(\mathrm{C}')_r$ *for any prime* r*, and hence* $(\mathrm{C})_\infty$ *holds for* $\mathcal{D}$*. Consequently,* $\Omega(G,\mathcal{D})_{(r)}$ *for any prime* r *(or* $\Omega(G,\mathcal{D})$*) is a generalized Burnside ring.*

以下のような関係が成立していることを注意する:

(Z) for $\mathcal{D}$ $\overset{\text{Lem2(1)}}{\Rightarrow}$ $\mathcal{D}$ は self-normalizing な族 $\Rightarrow$ $(\mathrm{C}')_r$ for $\mathcal{D}$ for all prime r $\Rightarrow$ (C_∞) for $\mathcal{D}$ $\overset{\text{Lem1(2)}}{\Rightarrow}$ $\Omega(G,\mathcal{D})$ は一般バーンサイド環.

[OS09] の主定理は次の通りである：

Theorem. ([OS09, Theorem 1]) *Assume* (W) *and* (P) *for* $\mathfrak{X} \subseteq \mathcal{B}_p(G)$. *Then the collection* $\mathcal{N}_G(\mathfrak{X})$ *satisfies* (Z). *Consequently,* $\Omega(G,\mathcal{N}_G(\mathfrak{X}))$ *is realized as a generalized Burnside ring.*

Proof: $\mathcal{N}_G(\mathfrak{X})$ の二つの元を以下のようにとる：

$$H := {}^{h_1}N_G(U_F) \text{ and } K := {}^{h_2}N_G(U_J) \in \mathcal{N}_G(\mathfrak{X}),$$

ただし，$h_1, h_2 \in G$, $\emptyset \neq F, J \subseteq I$ とする．$\varphi_H([G/K]) = |\{gK \in G/K \mid H \leq {}^gK\}|$ が成立するので，$x, y \in G$ に対し $H \leq {}^xK$ かつ $H \leq {}^yK$ が成り立つならば $x^{-1}y \in K$ が成り立つことを示せばよい．

$H \leq {}^xK$ を仮定する．このとき

$$N_G(U_F) \leq {}^{h_1^{-1}xh_2}N_G(U_J) = N_G({}^{h_1^{-1}xh_2}U_J)$$

が成り立つ．$N_G({}^{h_1^{-1}xh_2}U_J) = M$ とする．仮定 (P) より U_F は p-根基部分群となる．従って，Smith-Yoshiara の定理 [SY97, Lemma1.9] より $O_p(M) \leq U_F$ が成立する．同様に仮定 (P) より ${}^{h_1^{-1}xh_2}U_J$ は p-根基部分群なので

$${}^{h_1^{-1}xh_2}U_J = O_p(M) \leq U_F \leq P \geq U_J$$

が成り立つ．ゆえに仮定 (W) から ${}^{h_1^{-1}xh_2}U_J = U_J$ となるので，$h_1^{-1}xh_2 \in N_G(U_J)$ が示される．同様に $h_1^{-1}yh_2 \in N_G(U_J)$ も成り立つので

$$h_2^{-1}x^{-1}yh_2 = (h_1^{-1}xh_2)^{-1}(h_1^{-1}yh_2) \in N_G(U_J)$$

となり $x^{-1}y \in {}^{h_2}N_G(U_J) = K$ が示される．□

例

(1) **Lie type groups in characteristic p:** $L(p)$ を標数 p の Lie 型の有限群，$\mathfrak{X} = \mathcal{B}_p(L(p))$ とする．$L(p)$ の Sylow p-部分群 P をとると

$$\mathfrak{X}_{\min}(\leq P) = \{U_1, U_2, \ldots, U_l\}$$

について l は $L(p)$ の Lie rank となる．このとき，$\mathfrak{X}$ は仮定 (W) と (P) を満たすことが知られている．ゆえに階数 $2^l - 1$ の一般バーンサイド環 $\Omega(G,\mathcal{N}_{L(p)}(\mathfrak{X}))$ を得る．$\mathcal{N}_{L(p)}(\mathfrak{X}) = \{{}^gN_{L(p)}(U_F) \mid g \in L(p),\ \emptyset \neq F \subseteq I\}$ は $L(p)$ のすべての真のパラボリック部分群である．ホモトピー同値 $\Delta(\mathcal{B}_p(L(p))) \sim \Delta(\mathcal{N}_{L(p)}(\mathfrak{X}))$ が成立する一方 $\mathcal{N}_{L(p)}(\mathfrak{X})$ は $(\mathrm{C})_p$ を満たすが $\mathcal{B}_p(L(p))$ はそれを満たさないことを注意する．

(2) **Mathieu group M_{24} and $p = 2$:** G を Mathieu simple group M_{24}，$\mathfrak{X} := \mathcal{B}_2^{\mathrm{cen}}(G) = \mathcal{B}_2(G)$ とする．G のひとつの Sylow 2-部分群 P について

$$\mathfrak{X}_{min}(\leq P) = \{U_O \cong 2^4,\ U_T \cong 2^6,\ U_S \cong 2^6\}$$

が成り立つことがわかる．$\mathfrak{X}$ が 仮定 (W)，(P) を満たすことは 2002 年に Sawabe により示された．従って，階数 $2^3-1=7$ の一般バーンサイド環 $\Omega(M_{24},\mathcal{N}_{M_{24}}(\mathfrak{X}))$ を得る．

(3) **Conway group Co_1, Monster M, and $p=2$:** G を Conway simple group Co_1 または Monster simple group M，$\mathfrak{X}:=\mathcal{B}_2^{\mathrm{cen}}(G)\subset\mathcal{B}_2(G)$ とする．Co_1 の 2-根基部分群は 1999 年に Sawabe により，また M のそれは 2005 年に Yoshiara によりそれぞれ決定された．Co_1 と M の $\mathfrak{X}$ が仮定 (W) と仮定 (P) を満たすことは 2002 年，2006 年にそれぞれ Sawabe により示された．階数 $2^4-1=15$ の一般バーンサイド環 $\Omega(Co_1,\mathcal{N}_{Co_1}(\mathfrak{X}))$ 階数 $2^5-1=31$ の一般バーンサイド環 $\Omega(M,\mathcal{N}_M(\mathfrak{X}))$ が得られる．

参考文献

[OS09] F. Oda and M. Sawabe, A collection of subgroups for the generalized Burnside ring, *Adv. in Math.* **222** (2009), 307–317.

[Sa03] M. Sawabe, On a p-local geometry associated with a complex of non-trivial p-subgroups, *Bull. London. Math. Soc.* **35** (2003), 196–202.

[SY97] S.D. Smith and S. Yoshiara, Some homotopy equivalences for sporadic geometries, *J. Algebra* **192** (1997), 326–379.

[Yd90] T. Yoshida, The generalized Burnside ring of a finite group, *Hokkaido Math. J.* **19** (1990), 509–574.

一変数多項式環の二次拡大から構成される頂点代数の有限次元加群

田辺顕一朗 (北海道大学大学院理学研究院数学部門)

1 準備と動機

頂点代数とは1986年にBorcherds[1]によって導入された無限個の積を持つ代数系である．頂点代数の定義を述べるために，x を形式的変数，U を $\mathbb{C}$ 上のベクトル空間として以下の記号を準備する：

$$U[[x,x^{-1}]] = \{\sum_{i\in\mathbb{Z}} u_{(i)}x^i \mid u_{(i)} \in U\},$$
$$U((x)) = \{\sum_{i\in\mathbb{Z}} u_{(i)}x^i \mid u_{(i)} \in U, u_{(i)} = 0\ (^\forall i \ll 0)\},$$
$$U[[x]] = \{\sum_{i=0}^{\infty} u_{(i)}x^i \mid u_{(i)} \in U\}.$$

次が頂点代数の定義である．

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

(1) V は $\mathbb{C}$ 上のベクトル空間．

(2) $Y(-,x)$ は V から $(\mathrm{End}\, V)[[x,x^{-1}]]$ への $\mathbb{C}$ 線型写像．$a \in V$ に対して，$Y(a,x) = \sum_{n\in\mathbb{Z}} a_n x^{-n-1}, a_n \in \mathrm{End}\, V$, と展開を書く．

(3) $a, u \in V$ に対して $Y(a,x)u \in V((x))$.

(4) $1 \in V$ で $Y(1,x) = \mathrm{id}_V (= 1_{-1}x^{-(-1)-1})$.

(5) $a \in V$ に対して，$a_n 1 = 0$ $(^\forall n \geq 0)$ と $a_{-1}1 = a$.

(6) (Borcherds 恒等式) $a, b, u \in V$, $l, m, n \in \mathbb{Z}$ に対して，

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

続けて頂点代数 V に対して V 加群の定義を与える．

定義 2. 次の条件を満たす対 (M, Y_M) を V 加群という．

(1) M は $\mathbb{C}$ 上のベクトル空間．

(2) $Y_M(-,x)$ は V から $(\mathrm{End}\, M)[[x,x^{-1}]]$ への $\mathbb{C}$ 線型写像．$a \in V$ に対して，$Y_M(a,x) = \sum_{n\in\mathbb{Z}} a_n x^{-n-1}, a_n \in \mathrm{End}\, M$, と展開を書く．

(3) $a \in V, u \in M$ に対して $Y_M(a,x)u \in M((x))$.

(4) $Y_M(1,x) = \mathrm{id}_M$.

(5) (Borcherds 恒等式) $a,b \in V, u \in M$, $l,m,n \in \mathbb{Z}$ に対して

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

頂点代数にさらにいくつかの条件を課したものを頂点作用素代数という．モンスター単純群が全自己同型群となっているムーンシャイン頂点作用素代数はその有名な例である．頂点作用素代数とその自己同型群に関しては興味深い予想があるので，筆者の研究の動機とともにその説明を少しする．頂点作用素代数 V とその位数有限の自己同型群 $G \leq \mathrm{Aut}\, V$ が与えられたとき，不変部分空間 $V^G = \{u \in V \mid gu = u, {}^\forall g \in G\}$ は V の部分頂点作用素代数となる．V 加群と V^G 加群との関係を問うのは自然であり，V に関する適切な条件下で V^G 加群と twisted V 加群とには対応があることが予想されている [4]．twisted V 加群 [3] とは V 加群の定義を拡張したものであるが，ここではこれ以上述べない．この予想はムーンシャイン頂点作用素代数の別構成にも関わっている重要なものである．この予想は位数が小さな巡回群の場合にはいくつかの例で検証されている ([5] の文献参照) が，一つ一つの例において V^G 加群を決めるために大変な労力を必要としている．G が非可換群の場合には，自明な場合を除いて検証は非常に困難だと思うし，実際予想の検証例はない．

筆者は頂点作用素代数という条件を緩めて頂点代数の具体例上で予想を調べてみることを考えてみた．もともと予想自体は頂点代数の言葉だけで述べることが出来る．以下に見るように，可換 $\mathbb{C}$ 多元環とその上の導分から頂点代数の扱いやすい例を構成することが出来る．これらの例における自己同型群に対して予想を検証し，一般の場合の手掛かりとしたいというのが研究の動機である．実際，命題 3 にあるように一変数多項式環の場合には予想が成り立っていることを検証出来る．ただし，この場合には有限位数の自己同型群は自動的に巡回群となってしまう．頂点作用素代数の例ではこれまで既約加群達の対応が検証されてきた．一変数多項式環の場合には既約加群ばかりでなく，直既約加群達の対応も示されていることが興味深い．

可換 $\mathbb{C}$ 多元環 A とその上の導分 D から頂点代数を構成した Borcherds の結果を次に紹介する．そのようにして得られる頂点代数の特徴付けも出来る．証明は導分の性質を用いて直接計算で出来る．ここで $D(ab) = (Da)b + a(Db)$ を満たす $\mathbb{C}$ 線型写像 $D : A \to A$ を A 上の導分といっている．

命題 1. [1]

(1) Dを可換$\mathbb{C}$多元環A上の導分とする．$a \in A$に対して，$Y(a,x) = \sum_{i=0}^{\infty} \frac{D^i a}{i!} x^i \in (\mathrm{End}\, A)[[x]]$ と定めると，$(A, Y, 1_A)$は頂点代数となる．ここで$a, b \in A$に対して$Y(a,x)b = \sum_{i=0}^{\infty} \frac{(D^i a)b}{i!} x^i$であり，$A$の単位元を$1_A$と書いている．

(2) 任意の$u \in V$に対して$Y(u,x) \in (\mathrm{End}\, V)[[x]]$となる頂点代数$(V, Y, 1)$が与えられたとする．$u, v \in V$に対して$u \cdot v = u_{-1}v$と定めると，定めると$(V, \cdot)$は単位元1を持つ可換$\mathbb{C}$多元環となる．さらに，写像$\mathcal{D} : V \to V$を$\mathcal{D}u = u_{-2}1$と定めると，$\mathcal{D}$は$V$上の導分となる．

以下Aを可換$\mathbb{C}$多元環，DをA上の導分として(A, D)から構成された頂点代数上の加群を考察していく．加群を区別するために，多元環としてのA加群を多元環A加群，頂点代数としてのA加群を頂点代数(A, D)加群ということにする．命題1と同様の結果が加群に対しても成り立つ．

命題 2. [1]

(1) Mを多元環A加群とする．$a \in A$に対して$Y_M(a,x) = \sum_{i=0}^{\infty} \frac{D^i a}{i!} x^i \in (\mathrm{End}\, M)[[x]]$と定めると，$(M, Y_M)$は頂点代数$(A, D)$加群となる．ここで$a \in A, v \in M$に対して$Y_M(a,x)v = \sum_{i=0}^{\infty} \frac{(D^i a)v}{i!} x^i$である．

(2) 任意の$a \in A$に対して$Y_M(a,x) \in (\mathrm{End}\, M)[[x]]$となる頂点代数$(A, D)$加群$(M, Y_M)$が与えられたとする．$a \in A, v \in M$に対して$a \cdot v = a_{-1}v$と定めると$M$は多元環$A$加群となる．

命題2は，多元環A加群は頂点代数(A, D)加群とみなせることを主張している．しかし多元環A加群から頂点代数(A, D)加群が全て得られることは保証していない．これは既にBorcherdsによって指摘されていたことである．$D = 0$の場合や$\dim_{\mathbb{C}} A < \infty$の場合には，多元環$A$加群から頂点代数$(A, D)$加群が全て得られることが直ぐに分かる．しかし，次はそうなっていない例を与えている．以下，加群は$\mathbb{C}$上有限次元のものを考える．

命題 3. [6] 一変数多項式環$\mathbb{C}[s]$とその上の導分$D = p(s)\frac{d}{ds}, p(s) \in \mathbb{C}[s]$,を考える．

(1) 多元環A加群から構成されない$\mathbb{C}$上有限次元な頂点代数$(\mathbb{C}[s], D)$加群が存在するための必要十分条件は$\deg p = 2$である．$\deg p = 2$の場合には各$n = 1, 2, \ldots$に対して，そのようなn次元直既約な頂点代数$(\mathbb{C}[s], D)$加群M_nが同型を除いてただ一つ存在する．M_nは次の性質を満たす．

- M_nは既約 $\Leftrightarrow n = 1$.

• $0 \subset M_1 \subset M_2 \subset \cdots \subset M_{n-1} \subset M_n$ で $M_n/M_{n-1} \cong M_1$ となる.

(2) $g \in \mathrm{Aut}\,\mathbb{C}[s]$ を位数有限の自己同型とし, $gD = D$ が成り立っているとする. 有限次元な g-twisted 頂点代数 $(\mathbb{C}[s], D)$ 加群は分類出来る. 特に任意の有限次元な頂点代数 $(\mathbb{C}[s]^g, D)$ 加群は g-twisted 頂点代数 $(\mathbb{C}[s], D)$ 加群から得られることが分かる.

加群 M_n は具体的な表示を与えることが出来るが, 長くなるので省略する. (2) は頂点代数 V とその位数有限の自己同型群 $G \leq \mathrm{Aut}\,V$ に対して V^G 加群と twisted V 加群とが対応していることの検証例となっている.

一変数多項式環の場合ですら, 多元環としてみた場合と頂点代数としてみた場合とでは加群が異なる場合が出てくる. 一変数多項式環を例として含む広いクラスの可換多元環に対して, 多元環 A 加群から得られない頂点代数 (A, D) 加群が存在するための条件が見つかれば面白いと思うが, まだうまく条件を捉えることが出来ない.

次の節では, 一変数多項式環の拡大環で一番簡単そうな $\mathbb{C}[s,t]/(t^2 - f(s))$ に関して, その頂点代数加群に関する結果を報告する.

2 $\mathbb{C}[s,t]/(t^2 - f(s))$ 上の頂点代数加群

$f(s) = \sum_{i=0}^{N} f_i s^i \in \mathbb{C}[s]$ を平方因子を持たず, 次数が3以上で最高次の係数が1の多項式とする. $A = \mathbb{C}[s,t]/(t^2 - f(s))$ とおき, D を A 上の導分として, 頂点代数 (A, D) 加群について調べたことを書く. A の分数体は $\mathbb{C}(s)$ の二次拡大 $\mathbb{C}(s)[t]/(t^2 - f(s))$ となることに注意する. A は Dedekind 整域になっており, 有限生成な多元環 A 加群の分類はよく知られている (cf. [2, Theorem 6.3.23]). このことから有限次元な頂点代数 (A, D) 加群の分類も可能ではないかと考え, 一変数多項式環の場合の続きとして頂点代数 (A, D) 加群を考察した. 主張を述べるために次の記号を準備する: $D(s) = a_1(s) + a_2(s)t, a_1(s), a_2(s) \in \mathbb{C}[s]$, としたとき,

$$g_{\pm}(s) = a_1(s) \pm a_2(s) s^{N/2} (1 + \sum_{i=0}^{N-1} f_i s^{i-N})^{1/2}$$

$$= a_1(s) \pm s^{N/2} a_2(s) \sum_{j=0}^{\infty} \binom{1/2}{j} (\sum_{i=1}^{N} f_{N-i} s^{-i})^j) \in \mathbb{C}((s^{-1/2}))$$

とおく. $g_{\pm}(s)$ は $D(s)$ を $\mathbb{C}((s^{-1/2}))$ において展開したものである. このとき, 次の結果を得た:

定理 1. 多元環 A 加群から構成されない $\mathbb{C}$ 上有限次元な頂点代数 (A, D) 加群が存在するための必要十分条件は,

- $\deg f$ が偶数 (このとき, $g_{\pm}(s) \in \mathbb{C}((s^{-1}))$ となる) かつ
- $g_+(s)$ or $g_-(s) = \sum_{i \leq 2} g_i s^i, g_2 \neq 0,$

である. さらに, この場合に各 $n = 1, 2, \ldots$ に対してそのような n 次元直既約な頂点代数 (A, D) 加群が同型を除いてただ一つ存在する.

例 1. 定理の条件を満たす多項式 $f(s)$ と導分 D の例を与える. $f(s) = \sum_{i=0}^{4} f_i s^i, f_4 = 1,$ を平方因子を持たない任意の 4 次モニック多項式とする.

$$a_1(s) = f(s), \qquad a_2(s) = a_{20} - \frac{f_3}{2}s - s^2, \ \mathbb{C} \ni a_{20} \neq \frac{1}{8}f_3^2 - \frac{1}{2}f_2$$

とおく.

$$D(s) = a_1(s) + a_2(s)t, \qquad D(t) = \frac{f'(s)a_2(s)}{2} + \frac{f'(s)}{2}t$$

と定められた D は $\mathbb{C}[s,t]/(t^2 - f(s))$ 上の導分となる. このとき, $D(s)$ を $\mathbb{C}((s^{-1}))$ において展開した $g_+(s)$ は,

$$\begin{aligned} g_+(s) = &(-\frac{f_3^2}{8} + \frac{f_2}{2} + a_{20})s^2 + (\frac{f_1}{2} + \frac{f_3 a_{20}}{2})s \\ &+ ((\frac{f_2}{2} - \frac{f_3^2}{8})a_{20} + \frac{f_0}{2} + \frac{f_2^2}{8} - \frac{f_3^2 f_2}{16} + \frac{f_3^4}{128})s^0 \\ &+ (s^{-1} \text{ を変数とする形式的べき級数}) \end{aligned}$$

となり, $(f(s), D)$ は定理の条件を満たしていることが確認出来る. また定理の条件を満たす多項式 $f(s)$ と導分 D はこの例以外に大量に構成することが出来る.

参考文献

[1] R. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster, *Proc. Nat. Acad. Sci. U.S.A.* **83** (1986), 3068–3071.

[2] A. J. Berrick and M.E. Keating, *An introduction to rings and modules with K-theory in view*, Cambridge Studies in Advanced Mathematics, **65**, Cambridge University Press, 2000.

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

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

[5] J. Lepowsky and H.S. Li, *Introduction to Vertex Operator Algebras and their Representations*, Progress in Mathematics, **227**, Birkhauser Boston, Inc., Boston, MA, 2004.

[6] K. Tanabe, Finite-dimensional modules for the polynomial ring in one variable as a vertex algebra, *J. Algebra* **320**, 1261–1274 (2008).

Frame stabilizers for framed vertex operator algebras associated to lattices

島倉 裕樹 (Hiroki SHIMAKURA)

愛知教育大学 数学教育講座
Department of Mathematics,
Aichi University of Education
e-mail: shima@auecc.aichi-edu.ac.jp

序

枠付き頂点作用素代数 (VOA) はムーンシャイン VOA を含む良いクラスの一つである. 本稿では 格子に付随する枠付き VOA の frame stabilizer についての Lam 氏との共同研究を紹介する. 詳細は [LS] を参照にされたい.

1 枠付き頂点作用素代数と構造符号

本節では枠付き VOA の定義と性質について述べる. 詳細は [DGH98] を参照せよ.

$L(1/2,0)$ を中心電荷 1/2 の単純ヴィラソロ VOA とする. $L(1/2,0)$ は有理的であり, 既約加群は同型を除いて $L(1/2,0), L(1/2,1/2), L(1/2,1/16)$ の三つである. $e \in V_2$ が **イジング元** であるとは e が生成する頂点代数が e をヴィラソロ元とする $L(1/2,0)$ と同型な VOA となることである. イジング元 $e, f \in V_2$ が **直交する** とは $[Y(e,z_1), Y(f,z_2)] = 0$ を満たすことである.

定義 1.1. [DGH98] V を単純 *VOA* とする.

- V が **枠付き (framed)** であるとは次を満たす互いに直交する V のイジング元 $\{e^1, \cdots, e^r\}$ が存在することである.[1]
$$\omega = e^1 + \cdots + e^r.$$
- $T_r = VA(\{e_1, e_2, \cdots, e_r\}) \cong L(1/2,0)^{\otimes r}$ を V の**ヴィラソロ枠 (Virasoro frame)** という.[2]

定理 1.2. [DGH98] 枠付き *VOA* は有理的かつ C_2-有限である.

[1] 条件から V の中心電荷が $r/2$ となる.
[2] しばしば $\{e^1, \ldots, e^r\}$ をヴィラソロ枠という.

V を枠付き VOA として, T_r をヴィラソロ枠とする. T_r は有理的なので, V は T_r 加群として完全可約である. また, 任意の既約 T_r-加群は既約 $L(1/2,0)$-加群の r 個のテンソル積と同型になる. よって T_r-加群として

$$V \cong \bigoplus_{h_i \in \{0, \frac{1}{2}, \frac{1}{16}\}} m_{h_1,\dots,h_r} \bigotimes_{i=1}^{r} L(1/2, h_i)$$

と分解される. ただし $m_{h_1,\dots,h_r}$ は重複度であり, 有限である ([DMZ94]).

$\alpha = (\alpha_1, \dots, \alpha_r) \in \mathbb{Z}_2^r$ に対して, V^α で $h_i = 1/16$ となるのが $\alpha_i = 1$ に限られる V の T_r-部分加群 $m_{h_1,\dots,h_r} \bigotimes_{i=1}^{r} L(1/2, h_i)$ の和を表すとする. 特に V^0 は部分 VOA となり, V^α は V^0-加群となる.

命題 1.3. [DGH98] $D := \{\alpha \in \mathbb{Z}_2^r \mid V^\alpha \neq 0\}$ は長さ r の $\mathbb{Z}_2$ 上の線形符号となる.

さらに, V^0 の T_r-加群としての分解を考えて,

$$V^0 \cong \bigoplus_{h_i \in \{0, \frac{1}{2}\}} m_{h_1,\dots,h_r} \bigotimes_{i=1}^{r} L(1/2, h_i).$$

を得る. そして, 重複度 $m_{h_1,\dots,h_r}$ は 1 または 0 であることが知られている ([DMZ94]). このとき $\beta = (\beta_1, \dots, \beta_r) \in \mathbb{Z}_2^r$ に対して M^β を V^0 の T_r-部分加群 $m_{h_1,\dots,h_r} \bigotimes_{i=1}^{r} L(1/2, h_i)$ で $h_i = 1/2$ となるのが $\beta_i = 1$ に限られる加群を表すことにする.

命題 1.4. [DGH98] $C := \{\beta \in \mathbb{Z}_2^r \mid M^\beta \neq 0\}$ は長さ r の $\mathbb{Z}_2$ 上の線形符号となる.

定義 1.5. 符号の組 (C, D) を T_r に関する V の**構造符号** (structure codes) という.

注意 1.6. 構造符号はヴィラソロ枠の取り方に依存する.

枠付き VOA に関する基本的な問題として次がある.

問題 1.7. *枠付き VOA のヴィラソロ枠を分類し, また, 構造符号を分類せよ.*

2 偶格子に付随する頂点作用素代数

本節では, 偶格子 L に付随する VOA V_L とそこから $\mathbb{Z}_2$-軌道体構成法によって得られる $\tilde{V}_L$ について述べる.

L を偶格子として, V_L を格子 VOA とする ([Bo86, FLM88]). V_L の自己同型群 $\mathrm{Aut}(V_L)$ は格子の自己同型群 $\mathrm{Aut}(L)$ の持ち上げを含むので, $-1 \in \mathrm{Aut}(L)$ の持ち上げとして位数 2 の元 θ を取る. このとき, θ による固定点 $V_L^+ := \{v \in V_L \mid \theta(v) = v\}$ は V_L の部分 VOA となる. [3]

ここで L をユニモジュラとし, 整数の重さを持つ twist 型の既約 V_L^+-加群 $V_L^{T,+}$ を取る.[4]

[3] θ の取り方は一意ではないが, V_L^+ は同型を除いて一意的である [DGH98].
[4] L がユニモジュラなので, このような既約加群は同型をのぞいて一意である ([AD04]).

定理 2.1. [FLM88, Mi04, LY08] L をユニモジュラ偶格子として, L が 4-フレームを持つとする.[5] このとき, $\tilde{V}_L := V_L^+ \oplus V_L^{T,+}$ は *VOA* 構造を持ち, その構造は V_L^+-加群を拡張したものとして同型を除いて一意的である.

このような VOA の構成法を $\mathbb{Z}_2$-**軌道体構成法** と言う. L が 4-フレームを持つ仮定から V_L が枠付き VOA となり, 枠付き VOA の理論として上の定理が [Mi04, LY08] で得られている.[6] しかし, 元々は [FLM88] において, triality 自己同型を用いてリーチ格子 Λ に付随する $V^\natural = \tilde{V}_\Lambda$ 上に頂点作用素が定義され, (非常に煩雑な計算を経て) $V^\natural$ が VOA 構造をもつことが示されている.

さて, $V_L, \tilde{V}_L$ の L の 4-フレームに付随するヴィラソロ枠について見てみよう.

命題 2.2. [DMZ94] L を階数 n の偶格子とし, 4-フレーム $F = \{\pm f_1, \dots, \pm f_n\}$ を持つとする. このとき,

$$\omega^{\pm}(f_i) = \frac{1}{16} f_i(-1)^2 \cdot \mathbf{1} \pm \frac{1}{4}(e^{f_i} + e^{-f_i}).$$

はイジング元であり, $V_L, V_L^+, \tilde{V}_L$ は F に付随するヴィラソロ枠 $T_F = \{\omega^{\pm}(f_i)\}$ を持つ枠付き *VOA* である.

ここで F と F から生成される L の部分格子 $\oplus_{i=1}^n \mathbb{Z} f_i$ を同一視し, $\mathbb{Z}_4$-符号 $\mathfrak{C} = L/F \subset F^*/F \cong \mathbb{Z}_4^n$ を考える. このとき

$$\begin{aligned} \mathfrak{C}_0 &= \{(\alpha_1, \dots, \alpha_n) \in \{0,1\}^n \mid (2\alpha_1, \dots, 2\alpha_n) \in \mathfrak{C}\}, \\ \mathfrak{C}_1 &= \{(\alpha_1, \dots, \alpha_n) \mod 2 \mid (\alpha_1, \dots, \alpha_n) \in \mathfrak{C}\}. \end{aligned}$$

は長さ n の $\mathbb{Z}_2$ 上の線形符号である.

さて $V_L, \tilde{V}_L$ の T_F に関する構造符号を記述しよう. そのために $\mathbb{Z}_2^n$ から $\mathbb{Z}_2^{2n}$ への二つの線形写像

$$\begin{aligned} d &: (x_1, x_2, \dots, x_n) \mapsto (x_1, x_1, x_2, x_2, \dots, x_n, x_n) \\ e &: (x_1, x_2, \dots, x_n) \mapsto (x_1, 0, x_2, 0, \dots, x_n, 0) \end{aligned}$$

を用いる.

命題 2.3. [DGH98]

(1) T_F に関する V_L の構造符号は次で与えられる.

$$D = d(\mathfrak{C}_1), \quad C = \mathrm{Span}_{\mathbb{Z}_2}\{d(\mathbb{Z}_2^n), e(\mathfrak{C}_0)\}.$$

(2) T_F に関する $\tilde{V}_L$ の構造符号は次で与えられる.

$$D = \mathrm{Span}_{\mathbb{Z}_2}\{d(\mathfrak{C}_1), e((1^n))\}, \quad C = \mathrm{Span}_{\mathbb{Z}_2}\{d(\mathcal{E}_n), e(\mathfrak{C}_0)\}.$$

ただし $\mathcal{E}_n = \{c \in \mathbb{Z}_2^n \mid \mathrm{wt}(c) \in 2\mathbb{Z}\}$.

---

[5] $F = \{\pm f_i \mid i = 1, 2, \dots, n\} \subset L$ が階数 n の格子 L の 4-フレームであるとは $(f_i, f_j) = 4\delta_{i,j}$ が成立することである. しばしば F が生成する格子 $\oplus_{i=1}^n \mathbb{Z} f_i$ も 4-フレームと呼ぶ.

[6] 筆者には, 任意のユニモジュラ偶格子 L に対して, $\tilde{V}_L$ が VOA 構造を持つことの証明は与えられてないと思われる.

3 Frame stabilizer

本章では frame stabilizer と pointwise frame stabilizer について述べる.

定義 3.1. V を枠付き VOA とし, T_τ をヴィラソロ枠とする. このとき, T_τ の **pointwise frame stabilizer** とは

$$\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V)}(T_\tau) = \{g \in \mathrm{Aut}(V) \mid g = 1 \text{ on } T_\tau\}$$

であり, **frame stabilizer** とは

$$\mathrm{Stab}_{\mathrm{Aut}(V)}(T_\tau) = \{g \in \mathrm{Aut}(V) \mid g(T_\tau) = T_\tau\}$$

である.

pointwise frame stabilizer は既に構造符号を用いて完全に決定されている.

定理 3.2. [LY08] V をヴィラソロ枠 T_τ を持つ枠付き VOA とし, (C, D) を T_τ に関する構造符号とする. このとき, 次のような完全系列がある[7]

$$1 \to \mathbb{Z}_2^\tau/D \to \mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V)}(T_\tau) \to P/C^\perp \to 1.$$

ただし $P = \{\xi \in \mathbb{Z}_2^\tau \mid \alpha \cap \xi \in C \ \forall \alpha \in D\}$.

そこで, 次に考えるべきは frame stabilizer である. pointwise frame stabilizer は frame stabilizer の中で正規であり, その剰余群はヴィラソロ枠に忠実に作用する. 特に, イジング元の置換とみて, τ 次対称群の部分群と思える. さらに, 次の命題が知られている.

命題 3.3. [DGH98, LY08] V をヴィラソロ枠 T_τ を持つ枠付き VOA とし, (C, D) を T_τ に関する構造符号とする. このとき $\mathrm{Stab}_{\mathrm{Aut}(V)}(T_\tau)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V)}(T_\tau)$ は $\mathrm{Aut}(C) \cap \mathrm{Aut}(D)$ の部分群と同型である.

次の問題の解決が今回の研究の動機の一つである.

問題 3.4. $\mathrm{Stab}_{\mathrm{Aut}(V)}(T_\tau)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V)}(T_\tau)$ を決定せよ.

これは pointwise frame stabilizer の次に考えるべき対象という自然な動機があるが, それだけでなく次のような応用が期待される.

- frame stabilizer が非同型であれば, ヴィラソロ枠は共役でない. よって, ヴィラソロ枠の分類の役に立つことが期待される.
- frame stabilizer は符号の自己同型を用いて記述される. よって, 枠付き VOA の自己同型群の理解に役立つと思われる.

まずは簡単な場合として [Mi96] で導入された符号 VOA の場合を考えてみる.

[7] 交換関係も C, D を用いて [LY08] で完全に記述されている.

定義 3.5. [Mi96] 枠付き *VOA* で $(C,0)$ という構造符号を持つものを C に付随する **符号 VOA** といい, V_C と書く.[8]

定理 3.6. [Mi96, Mi98] $\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V_C)}(T_r) \cong \mathbb{Z}_2^r/C^\perp$, であり, 次の分裂完全系列がある:

$$1 \longrightarrow \mathbb{Z}_2^r/C^\perp \longrightarrow \mathrm{Stab}_{\mathrm{Aut}(V_C)}(T_r) \longrightarrow \mathrm{Aut}(C) \longrightarrow 1.$$

したがって, 符号 VOA の frame stabilizer は構造符号を用いて完全に記述される. また, $\mathrm{Aut}(V_C)$ のヴィラソロ枠への作用は [LSY07] で研究されている.

命題 3.7. [LSY07] C が重さ 2 の元を持たなければ $\mathrm{Aut}(V_C)$ がヴィラソロ枠へ可移に作用する. 特に, 構造符号は一意である.

次に, 一般の場合の frame stabilizer を考えてみよう. V を枠付き VOA とし, ヴィラソロ枠 T_r をとり, T_r に関する構造符号を (C,D) とする. このとき, V^0 は符号 VOA なので, C から完全に VOA 構造が決まるが, V の VOA 構造は V^0 と D だけでは一意に決まらない. よって, $\mathrm{Stab}_{\mathrm{Aut}(V)}(T_r)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V)}(T_r)$ を C と D だけでは決まらないと思われる. 実際に, 次の例がある.

例 3.8. (1) リーチ格子 Λ に付随する格子 *VOA* V_Λ とムーンシャイン *VOA* $V^\natural$ は同じ構造符号を与えるヴィラソロ枠を持つ.

(2) $V^\natural$ は *frame stabilizer* が非同型だが同じ構造符号を与えるヴィラソロ枠を持つ.

したがって, 構造符号以外の情報を仮定しないと, frame stabilizer を記述するのは難しい.
そこで, 今回は Lam 氏と共同で $V = V_L$ または $\tilde{V}_L$ の場合に L の 4-フレームに付随するヴィラソロ枠 T_F の frame stabilizer について研究したのである.[9]

4 主結果

L を階数 n の偶格子とし, 4-フレーム F を持つとする. $\mathfrak{C} = L/F$ を $\mathbb{Z}_4$-符号とする. このとき $\mathrm{Aut}(\mathfrak{C})$ は $\mathfrak{C}$ を保つ $\mathrm{Aut}(\mathbb{Z}_4^n)$ の部分群とする. ただし, $\mathrm{Aut}(\mathbb{Z}_4^n)$ は完全系列 $1 \to \mathbb{Z}_2^n \to \mathrm{Aut}(\mathbb{Z}_4^n) \overset{\rightarrow}{\to} \mathrm{Sym}_n \to 1$ で与えられる.

定理 4.1. [LS] $K = \mathrm{Stab}_{\mathrm{Aut}(V_L)}(T_F)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V_L)}(T_F)$ とおく.

- K は $\mathrm{Aut}(L)$ のいくつかの元の持ち上げと *triality* 自己同型で生成される.
- $|\mathrm{Aut}(C) : K| = |\mathrm{Aut}(\mathfrak{C}_0) : \overline{\mathrm{Aut}(\mathfrak{C})}|$.

定理 4.2. [LS] L をユニモジュラ偶格子とし, $\tilde{K} = \mathrm{Stab}_{\mathrm{Aut}(\tilde{V}_L)}(T_F)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(\tilde{V}_L)}(T_F)$ とおく. また $\mathfrak{C}_0$ の最小重みが 4 であると仮定する.[10]

[8] もちろん [Mi96] の定義とは異なるが, 枠付き VOA を用いた定義はこのようになる.

[9] しかし, 最近, 別宮-原田-宗政-島倉の研究によって, V_L または $\tilde{V}_L$ の構造が現れない枠付き VOA が存在が符号の研究から明らかになった. ゆえに, 一般の (正則) 枠付き VOA に関する frame stabilizer の研究が必要となった. しかし, 今回の結果はムーンシャイン VOA を含む多くの場合に適用出来ることを強調しておく.

[10] もし, L がノルム 2 の元を持たなければ, この仮定は満たされる. 例えば $V^\natural$ へは適用可能である.

- $\tilde{K}$ は $\mathrm{Aut}(L)$ のいくつかの元の持ち上げと *triality* 自己同型で生成される.
- $|\mathrm{Aut}(C) : \tilde{K}| = |\mathrm{Aut}(\mathfrak{C}_0) : \overline{\mathrm{Aut}(\mathfrak{C})}|$.

この定理から原理的に, 符号の自己同型群や格子の自己同型群を用いて frame stabilizer が記述できるようになる. 特に, $\mathrm{Aut}(\mathfrak{C}_0) = \overline{\mathrm{Aut}(\mathfrak{C})}$ であるならば $K = \mathrm{Aut}(C)$, $\tilde{K} = \mathrm{Aut}(C)$ となる.

簡単に $V = V_L$ (resp. $V = \tilde{V}_L$) の場合の証明のスケッチを与える. 命題 2.3 より C が $d(\mathbb{Z}_2^n)$ (resp. $d(\mathcal{E}_n)$) を部分符号として含むことがわかる. そこで, $\mathcal{H}$ で $d(\mathbb{Z}_2^n)$ (resp. $d(\mathcal{E}_n)$) と同値な C の部分符号全体の集合を表すことにする. $k = \dim \mathfrak{C}_0^1$ と置く.

まず, K (resp. $\tilde{K}$) の元が $d(\mathbb{Z}_2^n)$ (resp. $d(\mathcal{E}_n)$) を固定するならば, 部分 VOA V_F (resp. V_F^+) を固定することになるので, F を保つ格子の自己同型の持ち上げと見ることが出来る. そして $\mathfrak{C}$ の自己同型として記述することで次を得る.

補題 4.3. *$d(\mathbb{Z}_2^n)$ (resp. $d(\mathcal{E}_n)$) の K (resp. $\tilde{K}$) における固定部分群は $2 \wr \overline{\mathrm{Aut}(\mathfrak{C})}$ (resp. $2^k : \overline{\mathrm{Aut}(\mathfrak{C})}$) と同型である.*[11].

$V = V_L$ の場合は次数 1 の元を含むので, 内部自己同型[12]を用いて次を得ることが出来る.[13]

補題 4.4. *K は $\mathcal{H}$ に可移に作用する.*

$V = \tilde{V}_L$ の場合は一般には内部自己同型を用いることが出来ない.[14] そこで, 格子の自己同型の持ち上げ以外の自己同型である triality 自己同型 ([FLM88]) を用いて可移を示す. そのために, まず, C の構成法と組合せ論的手法 (数え上げ, 場合分け, 帰納法等) を用いて $\mathcal{H}$ を決定する. 得られた $\mathcal{H}$ に属する符号 E の形を見ると, E がノルム 2 の直交基底 $\{g_1, \ldots, g_n\} \subset \mathbb{R}^n \setminus L$ で $g_i + g_j \in L$ かつ $\{g_{2k-1} \pm g_{2k}\} = F$ を満たすものを定めることがわかる. 特に, [KKM91] から L がリーチ格子のような構成法で Type II $\mathbb{Z}_2$-符号から得られていることがわかる. よって [FLM88] に適用して triality 自己同型 σ を構成することが出来る.[15] この σ は $\{g_{2k-1} \pm g_{2k}\} = F$ より T_F を保ち, また (もうちょっと詳細な g_i の性質と triality の作用を見ることで) $\sigma(d(\mathbb{Z}_2^n)) = E$ となることがわかる.

補題 4.5. *$\tilde{K}$ は $\mathcal{H}$ に可移に作用する.*

また, 簡単な符号の自己同型の計算から次が得られる.

補題 4.6. *$\mathrm{Aut}(C)$ における $d(\mathbb{Z}_2^n)$ (resp. $d(\mathcal{E}_n)$) の固定部分群は $2 \wr \mathrm{Aut}(\mathfrak{C}_0)$ (resp. $2^k : \mathrm{Aut}(\mathfrak{C}_0)$) と同型である.*

これら補題を組合わせることで主結果を得ることが出来る.

---

[11] V_L の場合に関しては [GH03] に格子を用いて記述されている本質的に同じ定理がある

[12] V_1 の元の exponential で生成される自己同型.

[13] 実質は [FLM88] において triality と呼ばれている自己同型を用いる.

[14] 例えば $V^\natural$ の場合は内部自己同型はない.

[15] [FLM88] では triality 自己同型の構成は $V^\natural$ よりも一般的な符号から得られた格子に付随する VOA で考えられている.

5 例

5.1 V_{E_8}

もっとも中心電荷が小さい正則 VOA である V_{E_8} を考えてみる. まずは長さ 8 の Type II $\mathbb{Z}_4$-符号について思い出す.

命題 5.1. [CS93] 長さ 8 の *Type II* $\mathbb{Z}_4$-符号は同値を除いて丁度 4 つある.

各々の符号に対して, 次が成り立つ事が簡単に確かめられる.

補題 5.2. 長さ 8 の *Type II* $\mathbb{Z}_4$-符号 $\mathfrak{C}$ に対して, $\mathrm{Aut}(\mathfrak{C}_0) = \overline{\mathrm{Aut}(\mathfrak{C})}$.

したがって, E_8 の 4-フレーム F に対して, $\mathrm{Stab}_{\mathrm{Aut}(V_{E_8})}(T_F)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V_{E_8})}(T_F) = \mathrm{Aut}(C)$ が成立する. ところで, [GH03] で V_{E_8} のヴィラソロ枠は分類されている.

定理 5.3. [GH03] V_{E_8} のヴィラソロ枠は共役を除いて丁度 5 個ある. 特に, 任意の V_{E_8} のヴィラソロ枠は 4-フレイムに付随する V_{E_8} または $\tilde{V}_{E_8}(\cong V_{E_8})$ のヴィラソロ枠と共役である.

よって, まとめて次の結果を得る.

定理 5.4. [GH03, LS] T を V_{E_8} の任意のヴィラソロ枠とし, (C, D) を T に関する構造符号とする. このとき $\mathrm{Stab}_{\mathrm{Aut}(V_{E_8})}(T)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V_{E_8})}(T) = \mathrm{Aut}(C)$ となる.

[GH03] での frame stabilizer の決定は個別の計算により行われている. 特に対称群の細かい性質等を用いて証明している部分もある. 一方で [LS] の結果を使うことで, 本質的に $\mathrm{Aut}(\mathfrak{C}_0) = \overline{\mathrm{Aut}(\mathfrak{C})}$ が重要な事がわかる.

5.2 Pseudo Golay 符号に付随する $V^\natural$ のヴィラソロ枠

定義 5.5. [Ra99, HM] 長さ 24 の極値的な *Type II* $\mathbb{Z}_4$-符号 $\mathfrak{C}$ で $\mathfrak{C}_0 = \mathfrak{C}_1 \cong G_{24}$ を満たすものを pseudo[16] Golay 符号 という.[17]

命題 5.6. [Ra99] 丁度 13 個の非同値な *pseudo Golay* 符号が存在する.[18]

定理 5.7. [LS] F をリーチ格子 Λ の 4-フレームで $\mathfrak{C} = \Lambda/F$ が *pseudo Golay* 符号となるものとする. このとき $\mathrm{Stab}_{\mathrm{Aut}(V^\natural)}(T_F)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V^\natural)}(T_F) \cong 2^{12}.\overline{\mathrm{Aut}(\mathfrak{C})}$.

証明. $\mathfrak{C}_0$ の最小重みは 8 なので, 任意の C の重さ 4 の符号は $d(\mathcal{E}_{24})$ に属する. よって $\mathrm{Stab}_{\mathrm{Aut}(V^\natural)}(T_F)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V^\natural)}(T_F)$ は $d(\mathcal{E}_{24})$ を保ち, 補題 4.3 から定理が従う. □

[Ra99] に書かれている $\mathfrak{C}$ の自己同型群の構造を見ることで, 実際に構造符号が一致するが frame stabilizer が非同型なヴィラソロ枠が pseudo Golay 符号から得られることがわかる. これは例 3.8 (2) の具体例となっている.

[16] 発音が間違っていることを指摘してもらった多くの方に感謝します. p は発音しません.

[17] Rains の本来の定義は別の表現であって, この定義で同値な事が原田さんと宗政さんによって証明されています. 指摘してもらった宗政さんに感謝します.

[18] 講演中は原田さんと宗政さんによって分類されたと言いましたが, Rains の論文の中で丁度 13 個であると書かれています. 指摘してもらった宗政さんに感謝します.

5.3 リーチ格子のある 4-フレームに付随する $V^\natural$ のヴィラソロ枠

よく知られているように, Golay 符号 G_{24} から

$$\Lambda = \frac{1}{\sqrt{2}}\{(v_i) \in \mathbb{Z}^{24} \mid (\bar{v}_i) \in G_{24},\ \sum_{i=1}^{n} v_i \in 4\mathbb{Z}\}) + \mathbb{Z}\frac{1}{2\sqrt{2}}(-3,1,1,\ldots,1)$$

によって, リーチ格子 Λ が得られる. このとき

$$\varepsilon_1 = \frac{1}{\sqrt{2}}(2,0,\ldots,0),\ \varepsilon_2 = \frac{1}{\sqrt{2}}(0,2,0,\ldots,0),\ \ldots,\ \varepsilon_{24} = \frac{1}{\sqrt{2}}(0,\ldots,0,2)$$
$$f_{2i-1} = \varepsilon_{2i} + \varepsilon_{2i-1}, \quad f_{2i} = \varepsilon_{2i} - \varepsilon_{2i-1} \quad (i = 1,2,\ldots,12)$$

と置くと, $F = \{\pm f_i \mid i = 1,2,\ldots,24\}$ は 4-フレームとなる. 特に, Golay 符号が極値的であることから $\mathfrak{C} = \Lambda/F$ は長さ 24 の極値的 type II $\mathbb{Z}_4$-符号となる. しかし, この 4-フレームの作り方は Golay 符号の座標の取り方に依存する.[19] そこで, ここでは Golay 符号の MOG 座標 ([CS99]) を考える. この座標から得られる 4-フレーム F に付随する $V^\natural$ のヴィラソロ枠 T_F について, 次が知られている.

命題 5.8. [DGH98] (C,D) を $V^\natural$ の T_F に関する構造符号とする. このとき $C = D^\perp$, $\dim D = 7$ であって $D \cong \{(c,c,c),(1^{16}0^{32}),(0^{16}1^{16}0^{16}) \mid c \in \mathrm{RM}(1,4)\}$. さらに, $\mathrm{Aut}(D) = \mathrm{Aut}(C) \cong 2^{12}.(\mathfrak{S}_3 \times \mathrm{GL}(4,2))$.

F から得られる $\mathbb{Z}_4$-符号 $\mathfrak{C}$ について次が成り立つ事が計算機で確かめられる.

命題 5.9. [HM] $\mathrm{Aut}(\mathfrak{C}_0) = \overline{\mathrm{Aut}(\mathfrak{C})}$.

[LY08] より $\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V^\natural)}(T_F) \cong 2^{7+20}$ である. よって, frame stabilizer は次のようになる

定理 5.10. [Mi04, LS] $\mathrm{Stab}_{\mathrm{Aut}(V^\natural)}(T_F)/\mathrm{Stab}^{\mathrm{pt}}_{\mathrm{Aut}(V^\natural)}(T_F) \cong \mathrm{Aut}(C) \cong 2^{12}.(\mathfrak{S}_3 \times \mathrm{GL}(4,2))$. さらに, $\mathrm{Stab}_{\mathrm{Aut}(V^\natural)}(T_F) \cong 2^{7+20}.(2^{12}.(\mathfrak{S}_3 \times \mathrm{GL}(4,2)))$

この結果は [Mi04] では符号の自己同型が VOA の自己同型に持ち上がる事を対応する部分 VOA の性質を使いながら直接示している.

このようにモンスターの (割と大きい) 部分群[20]を符号を用いて記述することが出来, 理解をする手がかりとなることが期待される. また, ヴィラソロ枠の分類に対しても有益であることが期待される.

参考文献

[AD04] T. Abe and C. Dong, Classification of irreducible modules for the vertex operator algebra V_L^+: General case, *J. Algebra*, **273** (2004), 657–685.

[19][DGH98] では $\{1,2,\ldots,24\}$ の $\{2$ 点 $\} \times 12$ の分割をマーキングと呼んでいる.

[20]この群はモンスターの極大 2-局所部分群 $2^5.2^{10}.2^{20}(\mathfrak{S}_3 \times \mathrm{GL}(5,2))$ の部分群であると思われる. [Mi04] の中に $\mathrm{GL}(4,2)$ を $\mathrm{GL}(5,2)$ の部分群として取り扱う記述があることを講演中にコメントし忘れました.

[Bo86] R.E. Borcherds, Vertex algebras, Kac-Moody algebras, and the Monster, *Proc. Nat'l. Acad. Sci. U.S.A*, **83** (1986), 3068–3071.

[CS93] J.H. Conway, N.J.A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory Ser. A* **62** (1993), 30–45.

[CS99] J.H. Conway and N.J.A. Sloane, Sphere packings, lattices and groups, 3rd Edition, Springer, New York, 1999.

[DGH98] C. Dong, R.L. Griess and G. Höhn, Framed vertex operator algebras, codes and the Moonshine module, *Comm. Math. Phys.* **193** (1998), 407–448.

[DMZ94] C. Dong, G. Mason and Y. Zhu, Discrete series of the Virasoro algebra and the moonshine module, *Proc. Symp. Pure. Math.* **56** II (1994), 295–316.

[FLM88] I. Frenkel, J. Lepowsky and A. Meurman, Vertex operator algebras and the Monster, Pure and Appl. Math., Vol.134, Academic Press, Boston, 1988.

[GH03] R.L. Griess and G. Höhn, Virasoro frames and their stabilizers for the E_8 lattice type vertex operator algebra, *J. Reine Angew. Math.* **561** (2003), 1–37.

[KKM91] M. Kitazume, T. Kondo and I. Miyamoto, Even lattices and doubly even codes, *J. Math. Soc. Japan* **43** (1991), 67–87.

[LSY07] C.H Lam, S. Sakuma and H. Yamauchi, Ising vectors and automorphism groups of commutant subalgebras related to root systems, *Math. Z.* **255** (2007), 597–626.

[LS] C.H. Lam and H. Shimakura, Frame Stabilizers for framed vertex operator algebras associated to lattices having 4-frames, to appear in *Int. Math. Res. Not. IMRN.*, arXiv:0905.4769.

[LY08] C.H. Lam and H. Yamauchi, On the structure of framed vertex operator algebras and their pointwise frame stabilizers, *Comm. Math. Phys.* **277** (2008), 237–285.

[HM] M. Harada and A. Munemasa, private communication.

[Mi96] M. Miyamoto, Binary codes and vertex operator (super)algebras, *J. Algebra* **181** (1996), 207–222.

[Mi98] M. Miyamoto, Representation theory of code vertex operator algebras, *J. Algebra* **201** (1998), 115–150.

[Mi04] M. Miyamoto, A new construction of the moonshine vertex operator algebra over the real number field, *Ann. of Math* **159** (2004), 535–596.

[Ra99] E. Rains, Optimal self-dual codes over $\mathbb{Z}_4$, *Discrete Math.* **203** (1999), 215–228.

Möbius numbers of some modified generalized noncrossing partitions

冨江　雅也 (筑波大学数理物質科学研究科)

tomie@math.tsukuba.ac.jp

本稿は第２６回代数的組合せ論シンポジウムでの講演内容にいくつかの補足を加えまとめたものである。

1 Introduction

noncrossing partition およびCatalan number との関係は noncrossing partition の数え上げおよび refinement order によって定まる poset のMöbius function を考察したKrewerasの論文[6]に始まり多くの人たちによって研究がなされてきた。noncrossing partition とは自然数 n の分割で円周上に1から n までを時計回りに等間隔に並べたものに実現したとき各ブロックの凸閉包が交わらないようなものを意味する。とくに古典的には A 型,B 型,D 型の noncrossing partition およびその一般化となる k-divisable noncrossing partition などがEdelman, Reiner らにより研究されてきた。一方 Biane らは noncrossing partition と Coxeter group との関係に言及し Coxeter group の absolute order を用いて noncrossing partition 自然に定義した。[3] 2006年 Armstrong は論文[1]により Biane の方法をより一般的に捉え k-divisable noncrossing partition に対応するものを Coxeter group を用いて自然に構成した。彼は同論文において k-divisable noncrossing partition の性質をさまざまな側面から詳しく調べている。k-divisable noncrossing partition には EL-labeling, parking function,

narayana polynomial, associahedron 等多くの興味深い対象とのつながりが指摘されているが本稿では Möbius function (同じ意味であるが Möbius number) の話を中心に進めていきたい。

2 Möbius function

局所有限な半順序集合（以下 poset と呼ぶ）上の Möbius function は以下のように定義される。

Definition 1

P を局所有限 *poset*, $\mathrm{Int}(P)$ を P の *interval* の集合とする。

$\mu: \quad P \longrightarrow \mathbb{Z}$ が *Möbius function*

$\Longleftrightarrow_{\mathrm{def}}$ μ が $\sum_{x \le y \le z} \mu(x,y) = \delta_{x,z}$ を満たす。

この定義より Möbius function は存在して一意に定まる。以下 poset P が最小元 $\hat{0}$, 最大元 $\hat{1}$ を持つとき $\mu(P) = \mu(\hat{0}, \hat{1})$ とする。

Example 2.1

(1) Boolean algebra B_n *の Möbius function は* $\mu(B_n) = (-1)^n$ となる。

(2) set partition Π_n *の Möbius function は* $(-1)^n n!$ となる。

(3) noncrossing partition $NC(n)$ *の Möbius function は* $(-1)^n C_n$ となる。ただし C_n は *Catalan number*。

Möbius function の最も重要な応用は Möbius inversion formula と呼ばれるものである。

Theorem 1

$F, G: \quad P \longrightarrow \mathbb{Z}$ に対して

$F(x) = \sum_{x \le y} G(y) \iff G(x) = \sum_{x \le y} \mu(x,y) F(y).$

この公式はふるいの方法と呼ばれているもので単純なものであるが非常に強力なもので超平面配置における部屋の個数が特性多項式より導かれる事実 *[9]* も本質的には *Möbius inversion formula* に基づ

いている。また *Combinatorial Hopf algebra* において非自明な同型を見つける際にも応用されている。

3 Fuss–Catalan number

有限型 Coxeter 群 (W, S) および degrees $d_1 \leq \cdots \leq d_n$ に対して (positive) Fuss–Catalan number を以下で定める。[1]

Definition 2

(1) $\mathrm{Cat}^{(k)}(W) := \frac{1}{|W|} \cdot \Pi_{i=1}^{n}(kh + d_i)$. *Fuss–Catalan number.*

(2) $\mathrm{Cat}_{+}^{(k)}(W) := \frac{1}{|W|} \cdot \Pi_{i=1}^{n}(kh + d_i - 2)$. *positive Fuss–Catalan number.*

A 型,$k = 1$ とすると Fuss–Catalan number から Catalan number が復元でき Catalan number の大幅な一般化と見ることができる。Stanley の教科書 [7] には大量の Catalan object が演習問題として列挙されているが A 型の Fuss–Catalan object に関しては割りと多くの例が見つかっているものの一般的には多くは知られていない。以下いくつか例を挙げる。

Example 3.1

(1) root 系から定まる *Extended Shi arrangement* における *positive chamber* の個数（*Fuss–Catalan number*）およびその中で有界であるものの個数。*(positive Fuss–Catalan number)*

(2) root poset から定まる *anti chain* の個数。

(3) associahedron における頂点の個数。

次の章で Fuss–Catalan object のひとつである generalized noncrossing partition について述べる。

4 Generalized noncrossing partition

(W,S)を有限型Coxeter groupとする。$T := \{wsw^{-1} \mid w \in W,\ s \in S\}$とおく。そして$l_T : W \longrightarrow \mathbb{Z}$を$l_T(w) := \min\{i \mid w = t_1 \cdots t_i\, t_1, \ldots t_i \in T\}$と定める。

Definition 3 (absolute order)
$w_1 \leq w_2 \iff l_T(w_2) = l_T(w_1^{-1}w_2) + l_T(w_1)$.

これはTの代わりに生成系Sを用いればl_Sは通常の長さ関数となりweak Bruhat orderを得る。absolute orderはweak Bruhat orderの類似と見ることもできる。absolute orderは最小元として単位元eを持つが最大元は存在せずCoxeter elementsが極大元となる。今c: Coxeter elementをとり$NC(W) := [e,c]$とする。このときCoxeter elementsは互いに共役であること,l_Tは共役で不変であることより同型を除いて一意に定まる。$NC(W)$をnoncrossing partitionと呼ぶ。特にA型に関しては以下のことが知られている。[3]

Theorem 2 (Biane 1997 [3])
$NC(A_{n-1}) \simeq NC(n)$.

古典的B_n型のnoncrossing partitionとはA_{2n-1}型のnoncrossing partitionを1から$2n$までを等間隔に配置した円周上に実現したときπ rotationで不変なものの集合して特徴付けられる。これを$NC_B(2n)$とおく。このとき以下のことが知られている。

Theorem 3 (Biane,Goodman,Nica 2003 [4])
$NC(B_n) \simeq NC_B(2n)$.

noncrossing partitionの数え上げに関しては以下の定理が知られている。

Theorem 4 (Reiner, Bessis)
(1) $|\mathrm{NC}(W)| = \mathrm{Cat}^{(1)}(W)$.
(2) $\mu(\mathrm{NC}(W)) = (-1)^{n-1}\mathrm{Cat}^{(1)}_{+}(W)$.

Reinerが1997年に古典型に関してcase by case proofを与え2003年Bessisが例外型について計算機で証明した。分類によらない証明はいまだ知られていない。

次にCoxeter groupからk-divisable noncrossing partitionを定義する。

Definition 4 (Armstrong 2006 [1])

$\mathrm{NC}_{(k)}(W) :=$
$\{(\delta_1, \ldots, \delta_k) | \delta_i \in \mathrm{NC}(W), \text{ for } 1 \leq i \leq k \ l_T(\delta_1) + \cdots + l_T(\delta_i) = l_T(\delta_1 \cdots \delta_i)\}$.

$NC_{(k)}(W)$をgeneralized noncrossing partitionという。(流儀によってはk-divissable noncrossing partitionと呼ぶこともある。) 実際$k = 1$とすると$NC(W)$が復元される。そして$NC_{(k)}(W)$に関して以下の定理が知られている。

Theorem 5 (Armstrong 2006 [1])

$\mathrm{NC}_{(k)}(A_{n-1})^{\mathrm{dual}} \simeq \mathrm{NC}^{(k)}(n)$.

$NC(W)$はself dualなのでTheorem 2との整合性は取れていることに注意。ここで$\mathrm{NC}^{(k)}(n)$で古典的A_n型k-divisble noncrossing partition ,すなわちknのnoncrossing partitionであり各ブロックの元の個数がkの倍数であるようなもの全体にrefinement orderを入れてposetと見なしたものを表す。古典的B_n型k-divisble noncrossing partitionも$k = 1$のときの類似で$\mathrm{NC}^{(k)}(n)$の元で1から$2kn$を時計回りに等間隔に配置した円周上に実現したときπ rotationで不変なもの全体とする。これを$NC_B^k(2kn)$とおく。このとき次のことが成り立つ。

Theorem 6 (Armstrong 2006 [1])

$\mathrm{NC}_{(k)}(B_n)^{\mathrm{dual}} \simeq \mathrm{NC}_B^{(k)}(2kn)$.

つまり$NC_{(k)}(W)$は(古典的)noncrossing partitionの一般化となっている。generalized noncrossing partitionの数え上げに関して以下のことが知られている。

Theorem 7 (Armstrong 2006 [1])
(1) $|\mathrm{NC}_{(k)}(W)| = \mathrm{Cat}^{(k)}(W)$.
(2) $\mu(\mathrm{NC}_{(k)}(W) \cup \{\widehat{1}\}) = (-1)^{n-1}\mathrm{Cat}_{+}^{(k)}(W)$.

この結果は本質的にはChapotonによる$NC(W)$に対する多重鎖の計算[5]に依存している。この結果の類似を以下の形で得た。

Theorem 8 (Armstrong, Krattenthaler 2009 [2] ,Tomie 2009 [8])
(W,S) を有限型 *Coxeter group* とする。$\mathbf{maxs}_{(k)}(W)$ を $NC_{(k)}(W)$ における極大元の集合とする。このとき
(1) $|\{\mathrm{NC}_{(k)}(W)\backslash\mathbf{maxs}_{(k)}(W)\}\cup\{\widehat{1}\}| = \left(\mathrm{Cat}^{(k)}(W) - \mathrm{Cat}^{(k-1)}(W)\right)$.
(2) $\mu(\{\mathrm{NC}_{(k)}(W)\backslash\mathbf{maxs}_{(k)}(W)\}\cup\{\widehat{1}\}) = (-1)^{n}\left(\mathrm{Cat}_{+}^{(k)}(W) - \mathrm{Cat}_{+}^{(k-1)}(W\right.$

REFERENCE

[1] D. Armstrong, Generalized Noncrossing Partitions and Combinatorics of Coxeter Groups, to appear in Mem. Amer. Math. Soc.

[2] D. Armstrong, C. Krattenthaler, Euler characteristic of the truncated order complex of generalized noncrossing partitions. arXiv:0905.0205

[3] P. Biane, Some properties of crossings and partitions, Discrete Math. 175 (1997), 41-53.

[4] P. Biane, F. Goodman, A. Nica, Non-crossing cumulants of type B, Trans. Amer. Math. Soc. 355 (2003), 2263-2303.

[5] F. Chapoton, Enumerative properties of generalized associahedra, Seminarie Lotharingien de Combinatorie 51 (2004), Article B51b.

[6] G. Kreweras, sur les partitions non croisess d'un cycle, Discrete Math. 1 (1972), 333-350.

[7] R. Stanley, Enumerative Combinatorics, vol.2, Cambridge University Press, Cambridge, 1999.

[8] M.Tomie, Möbius numbers of some modified generalized non-crossing partitions. arXiv:0905.1660

[9] T. Zaslavky, Facing up to arrangements: face-count formulas for partitions of space by hyperplanes, Mem. Amer. Math. Soc. 1 (1975).

グラフのスペクトル解析における量子確率論の手法

尾畑伸明
東北大学大学院情報科学研究科
www.math.is.tohoku.ac.jp/~obata

要旨

グラフの様々な構造を調べる上で, その隣接行列の固有値分布（スペクトル分布）は基本的であり, 多くの結果の蓄積がある. 近年, 量子確率論の手法が導入され, 特に, 大きなグラフ（成長するグラフ）の漸近的スペクトル解析において興味深い結果が得られている. 本報告では, 拙著 [4, 23] にしたがって, 量子確率論の基本的概念を紹介し, グラフのスペクトル解析への応用を概観する.

1 量子確率論の基礎概念

量子確率論 (quantum probability) は, 非可換確率論 (noncommutative probability), あるいは代数的確率論 (algebraic probability) とも呼ばれる. その端緒はフォンノイマンの有名な著書「量子力学の数学的基礎」(1932) に見ることができ, 言葉こそ違っているが, 代数的確率空間を基礎とした新しい確率の計算方法が定式化された. 量子確率論という名称の起源はここにあるのだが, 後年, 確率変数・確率過程・条件付確率・独立性・従属性・マルコフ性など確率論における基本概念が付け加わり, 量子力学に限らず幅広い応用と結びつきながら今日に至っている. 単に「確率論」というと, 伝統的なコルモゴロフ流の確率論を指すのが普通であるが, 本報告では, これを「古典確率論」と呼んで区別し, 「量子確率論」はこれを含む広い理論体系として扱う.

1.1 代数的確率空間

複素数体 $\mathbb{C}$ 上の代数 $\mathcal{A}$ に対合と呼ばれる演算 $a \mapsto a^*$ を与えたものを $*$-代数という. 本報告では, つねに乗法の単位元 $1 = 1_{\mathcal{A}}$ の存在を仮定する.

定義 1.1 $*$-代数 $\mathcal{A}$ 上で定義された $\mathbb{C}$-値関数は, 次の 3 つの性質を満たすとき, $\mathcal{A}$ 上の状態 (state) と呼ばれる.

(i) $\varphi : \mathcal{A} \to \mathbb{C}$ は線形関数.
(ii) すべての $a \in \mathcal{A}$ に対して $\varphi(a^*a) \geq 0$.
(iii) $\varphi(1_{\mathcal{A}}) = 1$.

$*$-代数 $\mathcal{A}$ とその上で定義された状態 φ を組にした $(\mathcal{A}, \varphi)$ を**代数的確率空間** (algebraic probability space) という.

この概念は非常に広いものであって, $*$-代数に位相的な性質 (C^* 代数等) を仮定しない. これによって, 確率論で自然に現れる非有界作用素 (ガウス型確率変数, ポアソン型確率変数, 生成作用素や消滅作用素など) を量子確率論の枠組みに取り込みやすくなる.

例 1.2 n 次複素行列の全体 $M(n,\mathbb{C})$ は $*$-代数である. $\rho \in M(n,\mathbb{C})$ は, 次の 2 性質を満たすとき**密度行列**と呼ばれる.

(i) 正 (定) 値である (つまり, $\rho = \rho^*$ ですべての固有値が ≥ 0).

(ii) $\mathrm{Tr}\,\rho = 1$.

密度行列 ρ に対して

$$\varphi(a) = \mathrm{Tr}(\rho a), \qquad a \in M(n,\mathbb{C}),$$

で定義される φ は $M(n,\mathbb{C})$ 上の状態になる. 逆に, $M(n,\mathbb{C})$ 上のすべて状態はこの形であり, 状態と密度行列は 1 対 1 対応する.

例 1.3 $M(n,\mathbb{C})$ は n 次元ヒルベルト空間 $\mathbb{C}^n$ に行列の積で作用する. $\mathbb{C}^n$ の内積は

$$\langle \xi, \eta \rangle = \sum_{k=1}^{n} \overline{\xi_k} \eta_k, \qquad \xi = \begin{bmatrix} \xi_1 \\ \vdots \\ \xi_n \end{bmatrix}, \quad \eta = \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_n \end{bmatrix},$$

によって定義する. 単位ベクトル $\xi \in \mathbb{C}^n$ に対して,

$$\varphi(a) = \langle \xi, a\xi \rangle, \qquad a \in M(n,\mathbb{C}),$$

は $M(n,\mathbb{C})$ 上の状態になる. これを ξ に付随するベクトル状態という. $M(n,\mathbb{C})$ 上のベクトル状態は階数 1 の密度行列によって表現される.

例 1.4 $(\Omega, \mathcal{F}, P)$ を古典確率空間とする.

$$L^{\infty-}(\Omega) = \bigcap_{1 \leq p < \infty} L^p(\Omega)$$

はすべての次数のモーメントが有限になる $\mathbb{C}$-値確率変数の全体である. 明らかに, $L^{\infty-}(\Omega)$ は積で閉じており, 可換な $*$-代数になる. 確率変数 X の平均値

$$\mathbf{E}(X) = \int_\Omega X(\omega) P(d\omega) = \int_{-\infty}^{+\infty} x \mu_X(dx)$$

は $L^{\infty-}(\Omega)$ 上の状態になる. したがって, $(L^{\infty-}(\Omega), \mathbf{E})$ は代数的確率空間になる. これを古典確率空間 $(\Omega, \mathcal{F}, P)$ に対応する代数的確率空間と呼ぶ. 多くの問題では, 確率空間そのものより確率変数およびその分布が重要である. その意味で, 代数的確率空間 $(L^{\infty-}(\Omega), \mathbf{E})$ には古典確率空間 $(\Omega, \mathcal{F}, P)$ のもつ (確率論的に本質的な) 情報がすべて移っている.

1.2 代数的確率変数

定義 1.5 代数的確率空間 $(\mathcal{A}, \varphi)$ が与えられたとき, 各 $a \in \mathcal{A}$ を**代数的確率変数**, または単に**確率変数**と呼ぶ. 特に $a = a^*$ をみたすときには**実確率変数**という.

確率変数 $a \in \mathcal{A}$ に対して, $\varphi(a^{\epsilon_1}a^{\epsilon_2}\cdots a^{\epsilon_m})$ の形の量を a の混合モーメントと総称する. ただし, $\epsilon_1,\ldots,\epsilon_m \in \{1,*\}$, $m \geq 1$. 代数的確率変数の統計的性質は混合モーメントで与えられる. この意味で, 2つの代数的確率空間 $(\mathcal{A},\varphi)$, $(\mathcal{B},\psi)$ の確率変数 a,b は, その混合モーメントがすべて一致するときに確率同値であるという.

実確率変数に対しては, モーメント列 $\{\varphi(a^m)\,;\,m=0,1,2,\ldots\}$ が確率変数を特徴づける ($m=0$ のときは $a^0=1_{\mathcal{A}}$ とする). このとき,

$$\varphi(a^m)=\int_{-\infty}^{+\infty}x^m\mu(dx),\qquad m=0,1,2,\ldots, \tag{1.1}$$

をみたす $\mathbb{R}$ 上のボレル確率測度 μ が存在する. 証明は $\{\varphi(a^m)\,;\,m=0,1,2,\ldots\}$ からつくられるハンケル行列式の正値性とハンブルガーの定理 [10, 38] による. (1.1) の μ を a の φ における分布という.

注意 1.6 (1.1) を満たす分布 μ の一意性は難しい問題 (モーメント問題) である. 簡単な十分条件としてカルレマン条件がよく知られている. すなわち, モーメント列 $\{M_m\}$ が

$$\sum_{m=0}^{\infty}M_{2m}^{-\frac{1}{2m}}=+\infty$$

を満たせば,

$$M_m=\int_{-\infty}^{+\infty}x^m\mu(dx),\qquad m=0,1,2,\ldots,$$

を満たす確率分布 (ボレル確率測度) μ は一意的に定まる [38]. たとえば, コンパクト台をもつ確率分布, ガウス分布やポアソン分布に対しては一意性が成り立つ.

例 1.7 $\mathcal{A}=M(2,\mathbb{C})$ とする.

$$\varphi(b)=\frac{1}{2}\operatorname{Tr}b=\frac{1}{2}(b_{11}+b_{22}),\qquad b=\begin{bmatrix}b_{11}&b_{12}\\b_{21}&b_{22}\end{bmatrix}$$

とおくと, $(\mathcal{A},\varphi)$ は代数的確率空間になる. 特に,

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

は実確率変数 ($a=a^*$) であり, そのモーメント列は,

$$\varphi(a^m)=\begin{cases}1, & m\text{ が偶数のとき},\\ 0, & m\text{ が奇数のとき}\end{cases}$$

で与えられる. 明らかに,

$$\varphi(a^m)=\int_{-\infty}^{+\infty}x^m\frac{1}{2}(\delta_{-1}+\delta_{+1})(dx),\quad m=1,2,\ldots.$$

したがって, a の分布は, ベルヌイ分布 $(\delta_{-1}+\delta_{+1})/2$ である. この意味で, a は (ふつうの) コイン投げの「確率モデル」を与えている.

定義 1.8 古典確率空間 $(\Omega, \mathcal{F}, P)$ で定義された確率変数 X に対して,

$$\varphi(a^m) = \mathrm{E}(X^m) = \int_{-\infty}^{+\infty} x^m \mu_X(dx), \quad m = 0, 1, 2, \ldots$$

を満たす代数的確率変数 a (と代数的確率空間 $(\mathcal{A}, \varphi)$) を X の代数的実現と呼ぶ.

1.3 相互作用フォック確率空間

定義 1.9 実数の無限列 $\{\omega_n\,;\, n = 1, 2, \ldots\}$ で, 次の条件 (i) または (ii) を満たすものをヤコビ数列と呼ぶ.

(i) [無限型] すべての $n \geq 1$ に対して $\omega_n > 0$.
(ii) [有限型] ある番号 $m_0 \geq 1$ があって, $\omega_1 > 0, \ldots, \omega_{m_0-1} > 0, \omega_{m_0} = \omega_{m_0+1} = \cdots = 0$.

有限型の場合は, m_0 番以降をカットして正数の有限列 (項数が 0 のものも含む) として扱うこともある.

ヤコビ数列 $\{\omega_n\}$ が与えられたとき, それが無限型か有限型かに応じて, 正規直交基底 $\{\Phi_n\}_{n=0}^{\infty}$, $\{\Phi_n\}_{n=0}^{m_0-1}$ をもつヒルベルト空間 $\Gamma(\mathbb{C})$ を考える. しばしば, Φ_0 は真空ベクトルと呼ばれる. 次に, $\Gamma(\mathbb{C})$ 上の線型作用素 $B^{\pm}$ を

$$\begin{cases} B^+\Phi_n = \sqrt{\omega_{n+1}}\,\Phi_{n+1}, \quad n = 0, 1, \ldots, \\ B^-\Phi_0 = 0, \quad B^-\Phi_n = \sqrt{\omega_n}\,\Phi_{n-1}, \quad n = 1, 2, \ldots, \end{cases} \tag{1.2}$$

によって定義する. ただし, 有限型の場合は, $B^+\Phi_{m_0-1} = 0$ とおく. $B^{\pm}$ の定義域として $\{\Phi_n\}$ の張る線型部分空間をとる. このとき,

$$\langle \Phi_m, B^{\pm}\Phi_n \rangle = \langle B^{\mp}\Phi_m, \Phi_n \rangle, \qquad m, n = 0, 1, 2, \ldots,$$

が成り立ち, この意味で $B^{\pm}$ は互いに共役になる.

定義 1.10 $\{\omega_n\}$ をヤコビ数列とする. 上の述べたように, ヒルベルト空間 $\Gamma(\mathbb{C})$ と作用素 $B^{\pm}$ を定義し, それらを組にした $(\Gamma(\mathbb{C}), \{\Phi_n\}, B^+, B^-)$ を $\{\omega_n\}$ に付随する**相互作用フォック空間**と呼ぶ. また, B^- を**消滅作用素**, B^+ を**生成作用素**と呼ぶ.

定義 1.11 相互作用フォック空間 $(\Gamma(\mathbb{C}), \{\Phi_n\}, B^+, B^-)$ に対して, $B^{\pm}$ で生成される $*$-代数を相互作用フォック代数という. 相互作用フォック代数に真空状態 (真空ベクトル Φ_0 の定めるベクトル状態) を合わせたものを**相互作用フォック確率空間**と呼ぶ.

数列 $\{\alpha_n\}_{n=1}^{\infty}$ に対して, 対角型作用素 α_{N+1} を

$$\alpha_{N+1}\Phi_n = \alpha_{n+1}\Phi_n, \qquad n = 0, 1, 2, \ldots,$$

によって定義する. 問題(たとえば, 隣接作用素の量子分解)によっては, $B^{\pm}$ に加えて α_{N+1} によって生成される $*$-代数を考える. これを $(\{\omega_n\},\{\alpha_n\})$ に付随する相互作用フォック代数という. 特に興味のある確率変数は,

$$B^+ + B^-, \qquad (B^+ + \sqrt{\lambda})(B^- + \sqrt{\lambda}) \qquad B^+ + B^- + \alpha_{N+1}$$

などである.

例 1.12 基本的な例は以下のとおりである.

フォック空間	ヤコビ数列	交換関係	$B^+ + B^-$ の分布
ボゾン	$\omega_n = n$	$B^-B^+ - B^+B^- = 1$	ガウス分布
フェルミオン	$\omega_1 = 1, \omega_2 = \cdots = 0$	$B^-B^+ + B^+B^- = 1$	ベルヌイ分布
自由	$\omega_n \equiv 1$	$B^-B^+ = 1$	半円則
q-	$\omega_n = [n]_q$	$B^-B^+ - qB^+B^- = 1$	q-変形ガウス分布

ただし, q-フォック空間では $-1 \le q \le 1$ とし, $[n]_q = 1 + q + \cdots + q^{n-1}$ は q-整数.

2 独立性と量子中心極限定理

2.1 独立性の諸定義

2つの古典確率変数 X, Y が独立であれば, 平均値の乗法性によって,

$$\mathbf{E}(XYXXYXY) = \mathbf{E}(X^4Y^3) = \mathbf{E}(X^4)\mathbf{E}(Y^3)$$

が成り立つ. 言い換えれば, 独立性は混合モーメントの計算ルールを与えているといえる. 代数的確率空間では, 確率変数の非可換性を反映した計算ルールがいろいろと考えられる. 以下に述べる4つの独立性は特に基本的であると思われるが, それ以外にもさまざまな「独立性」が議論されている [2, 3, 8, 27, 28, 29, 42, 43, 44].

さて, $(\mathcal{A}, \varphi)$ を代数的確率空間とする. 独立性は, 確率変数の族というよりはむしろそれらが生成する $*$-部分代数の族に対して定義しておいた方が便利である. (2つの古典確率変数 X, Y が独立であれば, それらの多項式 $p(X), q(Y)$ も独立になることを思い出そう.) そこで, $\mathcal{A}$ の $*$-部分代数の族 $\{\mathcal{A}_\lambda ; \lambda \in \Lambda\}$ の独立性を n 個の元

$$a_i \in \mathcal{A}_{\lambda_i}, \quad a_i \notin \mathbb{C}1, \quad \lambda_1 \ne \lambda_2 \ne \cdots \ne \lambda_n, \quad n \ge 2, \tag{2.1}$$

に対する混合モーメント $\varphi(a_1 \cdots a_n)$ の計算ルールとして定義する.

定義 2.1 (可換独立) $\{\mathcal{A}_\lambda\}$ が可換独立 (またはテンソル独立) であるとは, $\lambda_1 = \lambda_r$ となる $r \in \{2, \ldots, n\}$ が存在しなければ,

$$\varphi(a_1 \cdots a_n) = \varphi(a_1)\varphi(a_2 \cdots a_n).$$

そのような r が存在するときは, そのうちで番号が最小のものをあらためて r として,

$$\varphi(a_1 \cdots a_n) = \varphi(a_2 \cdots a_{r-1}(a_1 a_r) a_{r+1} \cdots a_n).$$

定義 2.2 (自由独立 [41]) $\{\mathcal{A}_\lambda\}$ が自由独立であるとは, (2.1) に加えて, $\varphi(a_2)=\cdots=\varphi(a_n)=0$ であれば,

$$\varphi(a_1\cdots a_n)=\varphi(a_1)\varphi(a_2\cdots a_n).$$

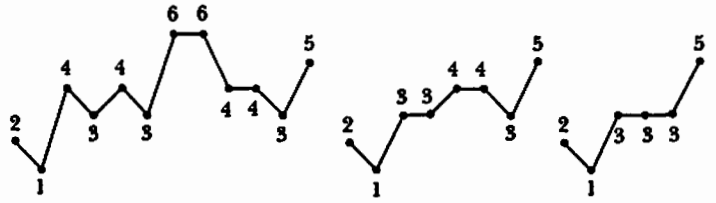
定義 2.3 (ブール独立 [39]) $\{\mathcal{A}_\lambda\}$ がブール (Boole) 独立であるとは,

$$\varphi(a_1\cdots a_n)=\varphi(a_1)\varphi(a_2\cdots a_n).$$

定義 2.4 (単調独立 [31, 32]) 添字の集合 Λ に全順序 $<$ が与えられているものとする. $\{\mathcal{A}_\lambda\}$ が単調独立であるとは, $\lambda_{i-1}<\lambda_i$ かつ $\lambda_i>\lambda_{i+1}$ が成り立つような $i\in\{1,2,\ldots,n\}$ があれば ($i=1$ または $i=n$ に対しては条件の一方を落とす),

$$\varphi(a_1\cdots a_n)=\varphi(a_i)\varphi(a_1\cdots\check{a}_i\cdots a_n).$$

ただし, $\check{a}_i$ はその項が取り除かれていることを示す. たとえば,



$$\begin{aligned}\varphi(214343664435)&=\varphi(4)\varphi(4)\varphi(66)\varphi(21334435)\\&=\varphi(4)\varphi(4)\varphi(66)\varphi(44)\varphi(213335)\\&=\cdots\\&=\varphi(4)\varphi(4)\varphi(66)\varphi(44)\varphi(2)\varphi(5)\varphi(333)\varphi(1)\end{aligned}$$

注意 2.5 ブール独立と単調独立の定義においては, $*$-部分代数 $\mathcal{A}_\lambda$ が $\mathcal{A}$ の単位元 $1_\mathcal{A}$ を含むことを仮定しない. $1_\mathcal{A}$ を含む $*$-部分代数 $\mathcal{A}_\lambda$ に対してその定義を適用すると, 自明な状況になる. たとえば, 代数的確率空間 $(\mathcal{A},\varphi)$ の 2 つの $*$-部分代数 $\mathcal{A}_1$, $\mathcal{A}_2$ を考え, $1_\mathcal{A}\in\mathcal{A}_1$ を仮定する ($\mathcal{A}_2$ についてはどちらでもよい). $\mathcal{A}_1$, $\mathcal{A}_2$ がブール独立または単調独立であれば,

$$\varphi(a_2^*a_2)=\varphi(a_2a_2^*)=|\varphi(a_2)|^2,\qquad a_2\in\mathcal{A}_2,$$

が成り立つ. したがって, a と $\varphi(a)1_\mathcal{A}$ が確率同値になる.

独立性の定義と明らかな等式

$$a_1\cdots a_n=a_1\cdots(a_i-\varphi(a_i))\cdots a_n+\varphi(a_i)a_1\cdots\check{a}_i\cdots a_n$$

を組み合わせれば, 一般の $\lambda_1,\ldots,\lambda_n\in\Lambda$ と $a_i\in\mathcal{A}_{\lambda_i}$ に対しても $\varphi(a_1\cdots a_n)$ を低次のモーメントで表示する公式が導かれる. 例を示そう. $\{\mathcal{A}_1,\mathcal{A}_2\}$ が上の 4 つの意味で独立であるとき, $a\in\mathcal{A}_1$, $b\in\mathcal{A}_2$ に対して, $\varphi(aba)$ などの計算公式は以下のようになる. (単調独立に必要な添字の順序は $1<2$ とする.)

	可換独立	自由独立	Boole 独立	単調独立
$\varphi(aba)$	$\varphi(a^2)\varphi(b)$	$\varphi(a^2)\varphi(b)$	$\varphi(a)^2\varphi(b)$	$\varphi(a^2)\varphi(b)$
$\varphi(bab)$	$\varphi(a)\varphi(b^2)$	$\varphi(a)\varphi(b^2)$	$\varphi(a)\varphi(b)^2$	$\varphi(a)\varphi(b)^2$
$\varphi(abab)$	$\varphi(a^2)\varphi(b^2)$	$\varphi(a)^2\varphi(b^2)$ $+\varphi(a^2)\varphi(b)^2$ $-\varphi(a)^2\varphi(b)^2$	$\varphi(a)^2\varphi(b)^2$	$\varphi(a^2)\varphi(b)^2$

例 2.6 $\mathcal{H}_1, \mathcal{H}_2, \ldots$ をヒルベルト空間とする. $\mathcal{B}(\mathcal{H}_n)$ の単位元を 1_n とおく. $\mathcal{A}_n$ を

$$1_1 \otimes \cdots \otimes 1_{n-1} \otimes S_n \otimes 1_{n+1} \otimes \cdots \otimes 1_N, \qquad S_n \in \mathcal{B}(\mathcal{H}_n),$$

の形の作用素が生成する $*$-代数とする. また, φ_n を $\mathcal{B}(\mathcal{H}_n)$ 上の状態とする. このとき, $\{\mathcal{A}_n\}$ は代数的確率空間 $(\mathcal{B}(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N), \varphi_1 \otimes \cdots \otimes \varphi_N)$ において可換独立である.

例 2.7 例2.6と同じ記号を用いる. 各ヒルベルト空間 $\mathcal{H}_n$ から単位ベクトル Ω_n が1つずつ選ばれているものとし, それが張る1次元部分空間への射影を P_n とする. $\mathcal{A}_n$ を

$$P_1 \otimes \cdots \otimes P_{n-1} \otimes S_n \otimes P_{n+1} \otimes \cdots \otimes P_N, \qquad S_n \in \mathcal{B}(\mathcal{H}_n),$$

の形の作用素が生成する $*$-代数とする. このとき, $\{\mathcal{A}_n\}$ は代数的確率空間 $(\mathcal{B}(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N), \Omega_1 \otimes \cdots \otimes \Omega_N)$ においてブール独立である.

例 2.8 例2.6と同じ記号を用いる. $\mathcal{M}_n$ を

$$1_1 \otimes \cdots \otimes 1_{n-1} \otimes S_n \otimes P_{n+1} \otimes \cdots \otimes P_N, \qquad S_n \in \mathcal{B}(\mathcal{H}_n),$$

の形の作用素が生成する $*$-代数とする. このとき, $\{\mathcal{M}_n\}$ は代数的確率空間 $(\mathcal{B}(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N), \psi \otimes \Omega_2 \otimes \cdots \otimes \Omega_N)$ において単調独立である. ここで ψ は $\mathcal{B}(\mathcal{H}_1)$ の任意の状態である.

例 2.9 ヒルベルト空間 $\mathcal{H}$ 上の自由フォック空間を $\mathcal{F}(\mathcal{H})$ とする. $\{e_n\}$ を $\mathcal{H}$ の正規直交系として, $l(e_n), l^*(e_n)$ を e_n に付随する消滅作用素, 生成作用素とする. これらの生成する $*$-部分代数を $\mathcal{A}_n$ とおくと, $\{\mathcal{A}_n\}$ は真空状態 Ω において自由独立になる. これは自由独立性の基本的な例であるが, 詳細は省略する. [15, 41] などを見よ.

2.2 量子中心極限定理

古典確率論において, 確率変数列の極限挙動は基本的な問題であり, とりわけ中心極限定理の重要性はよく認識されている. 量子確率論においても同様である. $a_1, a_2, \ldots$ を代数的確率空間 $(\mathcal{A}, \varphi)$ の実確率変数列であり, 平均 $\varphi(a_n) = 0$, 分散 $\varphi(a_n^2) = 1$ のように正規化されているものとする. $a_1, a_2, \ldots$ が独立であるとき,

$$\lim_{N\to\infty} \frac{1}{\sqrt{N}} \sum_{n=1}^{N} a_n$$

の分布を述べるのが中心極限定理である. 量子確率論では, A の非可換性を反映して多様な独立性が考えられるが, ここでは前節で導入した4つの独立性に付随した量子中心極限定理を示すことにする.

一般に, 確率変数列の収束は次のように定義される.

定義 2.10 確率変数 a_n の属する代数的確率空間を $(\mathcal{A}_n, \varphi_n)$ とし, 別の代数的確率空間 $(\mathcal{B}, \psi)$ と $b \in \mathcal{B}$ があって,

$$\lim_{n\to\infty} \varphi_n(a_n^{\epsilon_1} a_n^{\epsilon_2} \cdots a_n^{\epsilon_m}) = \psi(b^{\epsilon_1} b^{\epsilon_2} \cdots b^{\epsilon_m})$$

がすべての組合せ $\epsilon_1, \ldots, \epsilon_m \in \{1, *\}$, $m = 1, 2, \ldots$, に対して成り立つとき, b を $\{a_n\}$ のモーメント極限または単に確率極限という. このとき, $\{a_n\}$ は b にモーメント収束または確率収束するという.

代数的確率変数 $a_1, a_2, \ldots, b$ が実確率変数であれば, それらの分布 $\mu_1, \mu_2, \ldots, \mu$ が定義される. このとき, $\{a_n\}$ が b に確率収束するための必要十分条件は,

$$\lim_{n\to\infty} \int_{-\infty}^{+\infty} x^m \, \mu_n(dx) = \int_{-\infty}^{+\infty} x^m \, \mu(dx), \qquad m = 0, 1, 2, \ldots, \tag{2.2}$$

が成り立つことである.

注意 2.11 もし, μ がモーメント問題の一意解であれば, モーメント収束から確率測度の弱収束が従う. つまり, 任意の有界連続関数 $f(x)$ に対して,

$$\lim_{n\to\infty} \int_{-\infty}^{+\infty} f(x) \, \mu_n(dx) = \int_{-\infty}^{+\infty} f(x) \, \mu(dx)$$

が成り立つ. (2.2) では $f(x)$ として多項式をとったことになる. 多項式の全体と有界連続関数の全体には包含関係はないことに注意しておこう.

定理 2.12 (量子中心極限定理) 代数的確率空間 $(\mathcal{A}, \varphi)$ の確率変数列 $\{a_n\}$ が次の3条件を満たしているものとする.

(i) a_n は実確率変数である. つまり $a_n = a_n^*$.
(ii) a_n は正規化されている. つまり $\varphi(a_n) = 0$ かつ $\varphi(a_n^2) = 1$.
(iii) $\{a_n\}$ は一様有界な混合モーメントをもつ. つまり, 各 $m \geq 1$ に対して,

$$\sup\{|\varphi(a_{n_1} \cdots a_{n_m})| \, ; \, n_1, \ldots, n_m \geq 1\} < \infty. \tag{2.3}$$

さらに, a_n の生成する $*$-部分代数を $\mathcal{A}_n$ とするとき, それらが (1) 可換独立であれば,

$$\lim_{N\to\infty} \varphi\left[\left(\frac{1}{\sqrt{N}} \sum_{n=1}^{N} a_n\right)^m\right] = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} x^m e^{-x^2/2} dx,$$

(2) 自由独立であれば,

$$\lim_{N\to\infty}\varphi\left[\left(\frac{1}{\sqrt{N}}\sum_{n=1}^{N}a_n\right)^m\right]=\frac{1}{2\pi}\int_{-2}^{+2}x^m\sqrt{4-x^2}\,dx,$$

(3) ブール独立であれば,

$$\lim_{N\to\infty}\varphi\left[\left(\frac{1}{\sqrt{N}}\sum_{n=1}^{N}a_n\right)^m\right]=\frac{1}{2}\int_{-\infty}^{+\infty}x^m(\delta_{-1}+\delta_{+1})(dx),$$

(4) 単調独立であれば,

$$\lim_{N\to\infty}\varphi\left[\left(\frac{1}{\sqrt{N}}\sum_{n=1}^{N}a_n\right)^m\right]=\frac{1}{\pi}\int_{-\sqrt{2}}^{+\sqrt{2}}\frac{x^m}{\sqrt{2-x^2}}\,dx,$$

がすべての $m=0,1,2,\ldots$ で成り立つ. ここで現れた極限分布は, (1) ガウス分布, (2) 半円則, (3) ベルヌイ分布, (4) 逆正弦則.

証明は,

$$\lim_{n\to\infty}\varphi\left[\left(\frac{1}{\sqrt{N}}\sum_{n=1}^{N}a_n\right)^m\right]=\lim_{n\to\infty}\frac{1}{N^{m/2}}\sum_{n\in\mathfrak{M}(m,N)}\varphi(a_{n_1}\cdots a_{n_m})$$

を計算することによる. ただし, $\mathfrak{M}(m,N)$ は $\{1,\ldots,m\}$ から $\{1,\ldots,N\}$ への写像の全体のことである. 右辺の和において, それぞれの独立性の下で $N\to\infty$ で消えるものを取り除くことで, 極限値を具体的に求めることができ, それぞれの確率分布のモーメントに一致することが示される [4, 23]. ちなみに, 定理 2.12 に述べた 4 つの確率分布について, 奇数次のモーメントはいずれも消え, $2m$ 次のモーメントは次のようになる:

(1) $\dfrac{(2m)!}{2^m m!}$　(2) $\dfrac{(2m)!}{m!(m+1)!}$ (カタラン数)　(3) 1　(4) $\dfrac{(2m)!}{2^m m!m!}$

3 グラフのスペクトル解析

3.1 グラフの隣接行列と隣接代数

(単純無向) グラフ $G=(V,E)$ の**隣接行列**とは, 頂点集合 V を添字集合とする行列 $A=(A_{xy})$ で

$$A_{xy}=\begin{cases}1, & x\sim y,\\ 0, & \text{その他},\end{cases}$$

によって定義されるものをいう. ここで, 2 頂点 $x,y\in V$ が $\{x,y\}\in E$ を満たすとき, それらは隣接しているといい $x\sim y$ で表すこととした. 隣接行列はグラフの代数的表現として基本的である. 実際, 隣接行列はグラフを (同型を除いて) 再現する.

グラフ $G=(V,E)$ は, V が有限 ($|V|<\infty$) のとき有限グラフ, そうでないとき無限グラフと呼ばれる. 本報告では両方を扱うが, 無限グラフのときは局所有限性 (すべての $x\in V$ の次数について $\deg(x)<\infty$ となること) を仮定する. これによって, 隣接行列のべき乗 A^m が定義される. 実際, 行列の積の定義から

$$\begin{aligned}(A^m)_{xy} &= \sum_{x_1,\dots,x_{m-1}\in V} A_{xx_1}A_{x_1x_2}\cdots A_{x_{m-1}y}\\ &= |\{x \text{ と } y \text{ を結ぶ長さ } m \text{ の歩道}\}|\end{aligned}$$

となる. ここで, x と y を結ぶ長さ m の歩道 (walk) とは頂点の有限列 $x_0,x_1,\dots,x_m\in V$ で $x=x_0\sim x_1\sim\cdots\sim x_{m-1}\sim x_m=y$ をみたすものをいう ($x_0,x_1,\dots,x_m$ の中に一致する頂点があってもかまわない). こうして, A の複素係数多項式が定義され, その全体 $\mathcal{A}(G)$ は通常の行列演算で可換な $*$-代数となる. これをグラフ G の隣接代数という.

一方, A はヒルベルト空間 $\ell^2(V)$ に自然な仕方で作用する. 各 $x\in V$ に対して, 1点集合 $\{x\}$ の定義関数を δ_x で表す. このとき, $\{\delta_x\,;\,x\in V\}$ は $\ell^2(V)$ の正規直交基底となる. それらの張る線形空間を $C_0(V)$ とすれば, A は $C_0(V)$ 上の線形作用素になる. このとき,

$$A\delta_x=\sum_{y\sim x}\delta_y,\qquad x\in V,$$

が成り立ち, 特に,

$$A_{xy}=\langle\delta_x,A\delta_y\rangle$$

となる. グラフ $G=(V,E)$ の隣接行列 A が $\ell^2(V)$ 上の有界線形作用素になるための必要十分条件は $\sup\{\deg x\,;\,x\in V\}<\infty$ である.

3.2 グラフに付随する代数的確率空間

隣接代数 $\mathcal{A}(G)$ に状態 φ を考え合わせることで, 隣接行列 A を確率変数として取り扱うことができる. A の状態 φ における分布をグラフの φ におけるスペクトル分布という. 次の3つの状態に興味がある.

(a) **トレース** $G=(V,E)$ を有限グラフとする. 正規化されたトレース

$$\varphi_{\mathrm{tr}}(a)=\frac{1}{|V|}\operatorname{Tr}a,\quad a\in\mathcal{A}(G),$$

は, 隣接代数 $\mathcal{A}(G)$ 上の状態になる. 隣接行列 A の φ_{tr} における分布は, グラフのスペクトル分布 (隣接行列 A の固有値分布) に一致する.

(b) **真空状態** 頂点 $o\in V$ に付随するベクトル状態が

$$\varphi_o(a)=\langle\delta_o,a\delta_o\rangle,\quad a\in\mathcal{A}(G),$$

で定義される. これを頂点 $o\in V$ に付随する真空状態という. A の φ_o における分布を μ とすれば,

$$\langle\delta_o,A^m\delta_o\rangle=\varphi_o(A^m)=\int_{-\infty}^{+\infty}x^m\mu(dx),\qquad m=1,2,\dots,$$

が成り立つ. したがって, 分布 μ は o を出発して m ステップで o に戻る歩道の個数の積分表示に現れる. なお, 真空状態を考えるときは, 実際上, $o \in V$ を含む連結成分だけを問題にすることになるから, はじめからグラフは連結であるものとする.

(c) **真空状態の1径数変形** (連結) グラフ $G=(V,E)$ の2頂点 $x,y \in V$ の距離を $\partial(x,y)$ で表わす. $-1 \le q \le 1$ に対して,

$$Q = Q_q = \left(q^{\partial(x,y)}\right)$$

によって定義される行列をグラフの Q-行列という. $\mathcal{A}(G)$ 上の線形関数

$$\varphi_q(a) = \langle Q_q \delta_o, a\delta_o \rangle, \quad a \in \mathcal{A}(G),$$

は, フォック空間でいうコヒーレント状態に近い性質をもつ. φ_q がどのような $q \in [-1,1]$ に対して隣接代数 $\mathcal{A}(G)$ 上の状態になるか (正値性 $\varphi_q(a^*a) \ge 0$ が問題) に興味がある. 簡単な十分条件として (i) Q は V 上の正 (定) 値核であり, (ii) $AQ = QA$, を満たすことがすぐわかる. しかしながら, (i) が成り立つための条件はあまり知られていない [7, 36].

4 グラフの積構造と漸近的スペクトル

4.1 グラフの直積

2つのグラフ $G_i = (V^{(i)}, E^{(i)})$ $(i=1,2)$ を考える. このとき, $V = V^{(1)} \times V^{(2)}$ を頂点の集合とし, 辺集合を

$$E = \left\{ \{(x,y),(x',y')\}\,;\ \begin{array}{l} \text{(i) } x = x',\ y \sim y'; \text{ または,} \\ \text{(ii) } x \sim x',\ y = y' \end{array} \right\}$$

で定義する. こうしてできるグラフ (V,E) を G_1 と G_2 の直積といい, $G = G_1 \times G_2$ と書く. 明らかに, $G_1 \times G_2 \cong G_2 \times G_1$ と $G_1 \times (G_2 \times G_3) \cong (G_1 \times G_2) \times G_3$ が成り立つ. これによって, 2個以上のグラフの直積 $G_1 \times \cdots \times G_n$ が帰納的に定義される.

例 4.1 (整数格子) $\mathbb{Z}^n = \mathbb{Z} \times \cdots \times \mathbb{Z}$ (n 個の直積).

例 4.2 (ハミング・グラフ) $H(d,n) = K_n \times \cdots \times K_n$ (完全グラフ K_n の d 個の直積).

グラフ G_i の隣接行列を A_i とする. A_i は $C_0(V^{(i)}) \subset \ell^2(V^{(i)})$ 上の線形作用素である. 自然な対応で $C_0(V^{(1)} \times V^{(2)}) \cong C_0(V^{(1)}) \otimes C_0(V^{(2)})$ であるから, $G = G_1 \times G_2$ の隣接行列 A を $C_0(V^{(1)}) \otimes C_0(V^{(2)})$ 上の作用素と考えることができる.

補題 4.3 $G_1, G_2, \ldots, G_n$ をグラフとし, それらの隣接行列を $A_1, A_2, \ldots, A_n$ とする. 直積グラフ $G = G_1 \times G_2 \times \cdots \times G_n$ の隣接行列 A は, $C_0(V^{(1)}) \otimes C_0(V^{(2)}) \otimes \cdots \otimes C_0(V^{(n)})$ 上の作用素として, 次のように分解される:

$$A = \sum_{k=1}^{n} 1_1 \otimes \cdots \otimes 1_{k-1} \otimes A_k \otimes 1_{k+1} \otimes \cdots \otimes 1_n\,. \tag{4.1}$$

例2.6で述べたように, (4.1) は直積型の状態に関して可換独立な確率変数の和になっている. したがって, 可換独立に関する中心極限定理を組み合わせれば, 直積グラフ $G^N = G \times \cdots \times G$ (N 個の直積) の漸近的スペクトル分布を求めることができる.

定理 4.4 $G = (V, E)$ をグラフとし, $o \in V$ を原点として固定する. その N 重直積 G^N の頂点 $o = o_N = (o, \ldots, o)$ における真空状態を $\langle \cdot \rangle$ とおく. G^N の隣接行列を $A^{(N)}$ とすると,

$$\lim_{N\to\infty} \left\langle \left(\frac{A^{(N)}}{\sqrt{N \deg(o)}} \right)^m \right\rangle = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} x^m e^{-x^2/2}\, dx, \quad m = 0, 1, 2, \ldots.$$

証明 補題4.3によって,

$$A^{(N)} = \sum_{k=1}^{N} \overbrace{1 \otimes \cdots \otimes 1}^{k-1} \otimes A \otimes \overbrace{1 \otimes \cdots \otimes 1}^{N-k} \tag{4.2}$$

となる. 真空状態は直積型の状態であるから, 例2.6で述べたように (4.2) は真空状態に関して可換独立な確率変数の和であり, 各項は同じ分布をもつ. その平均と分散は,

$$\langle 1 \otimes \cdots \otimes 1 \otimes A \otimes 1 \otimes \cdots \otimes 1 \rangle = \langle A \rangle = \langle \delta_o, A\delta_o \rangle = 0,$$
$$\langle (1 \otimes \cdots \otimes 1 \otimes A \otimes 1 \otimes \cdots \otimes 1)^2 \rangle = \langle A^2 \rangle = \langle \delta_o, A^2 \delta_o \rangle = \deg(o).$$

で与えられる. したがって,

$$\frac{1}{\sqrt{\deg(o)}} 1^{\otimes(k-1)} \otimes A \otimes 1^{\otimes(N-k)}, \qquad k = 1, 2, \ldots, N,$$

が正規化された実確率変数列となる. そうすれば, 可換独立に関する中心極限定理によって,

$$\frac{A^{(N)}}{\sqrt{N \deg(o)}} = \frac{1}{\sqrt{N}} \sum_{k=1}^{N} \frac{1}{\sqrt{\deg(o)}} 1^{\otimes(k-1)} \otimes A \otimes 1^{\otimes(N-k)}$$

の分布は標準ガウス分布に近づく. ∎

4.2 グラフの櫛形積

2つのグラフ 2つのグラフ $G_i = (V^{(i)}, E^{(i)})$ $(i = 1, 2)$ を考え, それらの隣接行列を $A^{(i)}$ とする. また, G_2 には原点 $o \in V^{(2)}$ が定められているものとする. このとき, $V_1 \times V_2$ を頂点の集合として,

$$A_{(x,y),(x',y')} = A^{(1)}_{xx'} \delta_{yo} \delta_{y'o} + \delta_{xx'} A^{(2)}_{yy'}, \quad x, x' \in V^{(1)}, \quad y, y' \in V^{(2)}, \tag{4.3}$$

を隣接行列とする (連結な局所有限) グラフが得られる (図 1). これを G_1 と G_2 の櫛形積 (comb product) と呼び, $G_1 \triangleright_o G_2$ で表す. その隣接行列を $A^{(1)} \triangleright_o A^{(2)}$ と書く (混乱がなければ, 添字 o を省略する). 櫛形積は結合法則

$$(G_1 \triangleright_{o_2} G_2) \triangleright_{o_3} G_3 = G_1 \triangleright_{(o_2, o_3)} (G_2 \triangleright_{o_3} G_3)$$

を満たす. これを $G_1 \triangleright_{o_2} G_2 \triangleright_{o_3} G_3$ と略記する.

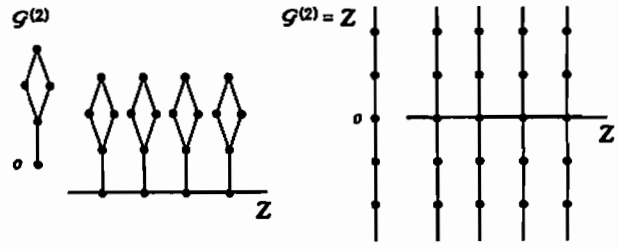


図 1: 櫛形グラフの例: $\mathbf{Z} \triangleright_o G_2$ と 2 次元櫛形格子 $\mathbf{Z} \triangleright_o \mathbf{Z}$

補題 4.5 $G_n = (V^{(n)}, E^{(n)})$ が与えられ, 各グラフには原点 $o_n \in V^{(n)}$ が定まっているものとする. このとき, 櫛形積 $G_1 \triangleright_{o_2} G_2 \triangleright_{o_3} \cdots \triangleright_{o_N} G_N$ の隣接行列は $C_0(V^{(1)} \times \cdots \times V^{(N)}) \cong C_0(V^{(1)}) \otimes \cdots \otimes C_0(V^{(N)})$ 上の作用素であり, 次のように分解する:

$$A^{(1)} \triangleright A^{(2)} \triangleright \cdots \triangleright A^{(N)} = \sum_{n=1}^{N} 1_1 \otimes \cdots \otimes 1_{n-1} \otimes A^{(n)} \otimes P_{n+1} \otimes \cdots \otimes P_N . \qquad (4.4)$$

ここで, P_n は $\ell^2(V^{(n)})$ から δ_{o_n} で張られる 1 次元空間への射影である.

証明は (4.3) を用いた簡単な計算である. 例 2.8 で見たように, (4.4) の右辺はベクトル状態 $\delta_{o_1} \otimes \cdots \otimes \delta_{o_N}$ に関して単調独立な確率変数の和になっている. そうすれば, 単調独立に関する中心極限定理 (定理 2.12) を適用して次の結果が得られる.

定理 4.6 ([1]) グラフ $G = (V, E)$ には原点 $o \in V$ が定まっているとし, その N 重櫛形積 $G^{\triangleright N}$ の隣接行列を $A^{\triangleright N}$ とする. このとき, 頂点 $o_N = (o, \ldots, o)$ における真空状態において,

$$\lim_{N\to\infty} \left\langle \left(\frac{A^{\triangleright N}}{\sqrt{N \deg(o)}} \right)^m \right\rangle = \frac{1}{\pi} \int_{-\sqrt{2}}^{+\sqrt{2}} \frac{x^m}{\sqrt{2-x^2}}\, dx, \quad m = 0, 1, 2, \ldots .$$

4.3 グラフの星形積

前節と同様に, 2 つのグラフ G_i $(i = 1, 2)$ を考える. 今度は双方の G_i に原点 $o_i \in V^{(i)}$ が定められているものとする. このとき, $V_1 \times V_2$ を添字とする行列

$$A_{(x,y),(x',y')} = A^{(1)}_{xx'} \delta_{yo_2} \delta_{y'o_2} + \delta_{xo_1} \delta_{x'o_1} A^{(2)}_{yy'}, \quad x, x' \in V^{(1)}, \quad y, y' \in V^{(2)}, \qquad (4.5)$$

を考える. A は対角成分が 0, その他の成分が 0 と 1 のみからなる対称行列になる. したがって, A は (連結とは限らない) グラフの隣接行列である. このグラフの (o_1, o_2) を含む連結成分を G_1 と G_2 の星形積と呼び, $G_1 \star_{(o_1,o_2)} G_2$ で表す (図 2).

補題 4.7 N 個のグラフ $G_n = (V^{(n)}, E^{(n)})$ が与えられ, 各グラフには原点 $o_n \in V^{(n)}$ が定まっているものとする. このとき, 星形積 $G = (V, E) = G_1 \star G_2 \star \cdots \star G_N$ の隣接行列 A

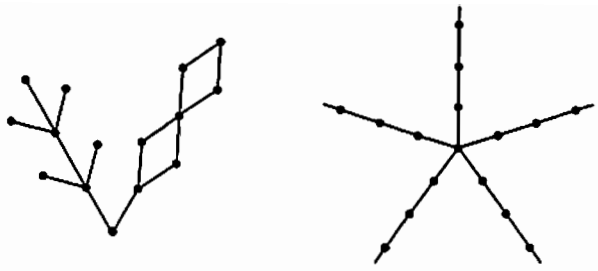


図 2: 星形グラフ (右は星形格子 $\mathbf{Z}_+^{*5}$)

は $C_0(V) \subset C_0(V^{(1)}) \otimes \cdots \otimes C_0(V^{(N)})$ 上の作用素であり, 次のように分解する:

$$A = \sum_{n=1}^{N} P_1 \otimes \cdots \otimes P_{n-1} \otimes A^{(n)} \otimes P_{n+1} \otimes \cdots \otimes P_N . \tag{4.6}$$

証明は (4.5) を用いた簡単な計算である. そうすれば, 例 2.7 で見たように, (4.6) の右辺はベクトル状態 $\delta_{o_1} \otimes \cdots \otimes \delta_{o_N}$ に関してブール独立な確率変数の和になっている. ブール独立に関する中心極限定理 (定理 2.12) を適用して次の結果が得られる.

定理 4.8 ([34]) グラフ $G = (V, E)$ には原点 $o \in V$ が定まっているとし, その N 重星形積 $G^{\triangleright N}$ の隣接行列を A^{*N} とする. このとき, 頂点 $o_N = (o, \ldots, o)$ における真空状態において,

$$\lim_{N\to\infty} \left\langle \left(\frac{A^{*N}}{\sqrt{N \deg(o)}} \right)^m \right\rangle = \frac{1}{2} \int_{-\infty}^{+\infty} x^m (\delta_{-1} + \delta_{+1})(dx), \qquad m = 0, 1, 2, \ldots .$$

これまでに, 隣接行列を通してグラフの積構造と独立性を結びつけて議論してきた. 概ね次のようにまとめられる (自由独立性については省略).

	可換独立	自由独立	ブール独立	単調独立
中心極限分布	ガウス分布	半円則	ベルヌイ分布	逆正弦則
グラフの例	正方格子	等質樹木	星形グラフ	櫛形グラフ

5 成長する正則グラフに対する漸近的スペクトル理論

5.1 直交多項式

実数 $\mathbb{R}$ 上のボレル確率測度で, すべての次数のモーメントが有限になるものの全体を $\mathfrak{P}_{\mathrm{fm}}(\mathbb{R})$ とおく. $\mu \in \mathfrak{P}_{\mathrm{fm}}(\mathbb{R})$ に対して

$$M_m = M_m(\mu) = \int_{-\infty}^{+\infty} x^m \, \mu(dx) \tag{5.1}$$

によって定義される実数列 $\{M_0=1, M_1, \dots\}$ を μ のモーメント列という. 以下, $\mu \in \mathfrak{P}_{\mathrm{fm}}(\mathbb{R})$ とする. 単項式列 $1, x, x^2, x^3, \cdots \in L^2(\mathbb{R}, \mu)$ にシュミットの直交化を施して得られる多項式列

$$P_0(x)=1, \quad \dots, \quad P_n(x)=x^n+\cdots, \quad \dots$$

を μ に付随する直交多項式という.

定理 5.1 (3項間漸化式) $\{P_n\}_{n=0}^{\infty}$ を $\mu \in \mathfrak{P}_{\mathrm{fm}}(\mathbb{R})$ に付随する直交多項式とする. μ の台が無限集合であれば, 数列 $\{\alpha_n\}_{n=1}^{\infty}$ と $\{\omega_n\}_{n=1}^{\infty}$ で $\alpha_n \in \mathbb{R}$, $\omega_n > 0$ を満たすものがあって,

$$\begin{cases} P_0(x)=1, \\ P_1(x)=x-\alpha_1, \\ xP_n(x)=P_{n+1}(x)+\alpha_{n+1}P_n(x)+\omega_n P_{n-1}(x), \quad n=1,2,\dots. \end{cases} \tag{5.2}$$

さらに,

$$\|P_0\|=1, \qquad \|P_n\|=\sqrt{\omega_1\omega_2\cdots\omega_n}, \quad n \geq 1.$$

証明は容易 [10, 38]. したがって, μ に付随する直交多項式 $\{P_n\}_{n=0}^{\infty}$ は, 2つの数列 $\{\omega_n\}_{n=1}^{\infty}$, $\{\alpha_n\}_{n=1}^{\infty}$ によって完全に決定される. これら2つの数列を μ に (または $\{P_n\}$ に) 付随するヤコビ係数と呼ぶことにする. 明らかに,

$$\alpha_1=M_1(\mu)=\int_{-\infty}^{+\infty} x\mu(dx), \qquad \omega_1=\int_{-\infty}^{+\infty}(x-\alpha_1)^2\mu(dx).$$

つまり, α_1 と ω_1 はそれぞれ μ の平均と分散である.

注意 5.2 確率分布 μ の台が丁度 $N+1$ 個の点からなるときに限り, 直交化の手続きが $\{P_0, P_1, \dots, P_N\}$ の $N+1$ 個の多項式を得た段階で終了する. そのとき, (5.2) は $P_{N+1}=0$ として成り立ち, ヤコビ係数は2組の有限数列 $\{\alpha_1, \alpha_2, \dots, \alpha_{N+1}\}$, $\{\omega_1, \omega_2, \dots, \omega_N\}$ になる. 最後の番号の定数は, (5.2) において $P_{N+1}=0$ として決定される. 以下では, 直交多項式 $\{P_n\}$ が無限列の場合に即した記述をするが, 有限列 $\{P_0, P_1, \dots, P_N\}$ に帰着している場合の変更は容易である.

定理 5.3 $\mu \in \mathfrak{P}_{\mathrm{fm}}(\mathbb{R})$ のヤコビ係数を $(\{\omega_n\}, \{\alpha_n\})$ とする. もし, μ がモーメント問題の一意解であれば,

$$\int_{-\infty}^{+\infty}\frac{\mu(dx)}{z-x}=\cfrac{1}{z-\alpha_1-\cfrac{\omega_1}{z-\alpha_2-\cfrac{\omega_2}{z-\alpha_3-\cfrac{\omega_3}{z-\alpha_4-\cdots}}}} \tag{5.3}$$

が成り立つ. ただし, 右辺の連分数は $\{\mathrm{Im}\, z \neq 0\}$ で収束する.

(5.3) の左辺は, (有限なモーメントをもつとは限らない) すべての確率分布 μ に対して定義される. これを μ のスチルチェス変換といい, $G_\mu(z)$ と書く. $G_\mu(z)$ は $\{\mathrm{Im}\, z \neq 0\}$ で正則である. このとき,

$$-\frac{2}{\pi}\lim_{y \to +0}\int_s^t \mathrm{Im}\, G_\mu(x+iy)dx=\mu(\{s\})+\mu(\{t\})+2\mu((s,t)), \quad s<t$$

が成り立つ. これをスチルチェス逆変換という. μ の絶対連続部分 $\rho(x)dx$ は,

$$\rho(x) = -\frac{1}{\pi} \lim_{y \to +0} \operatorname{Im} G_\mu(x+iy)$$

で与えられる. さらに, (5.3) の第 n 近似分数

$$\frac{1}{z-\alpha_1} \underset{-}{} \frac{\omega_1}{z-\alpha_2} \underset{-}{} \frac{\omega_2}{z-\alpha_3} \underset{-}{} \frac{\omega_3}{z-\alpha_4} \underset{-}{} \cdots \underset{-}{} \frac{\omega_n}{z-\alpha_{n+1}} = \frac{Q_n(z)}{P_{n+1}(z)}$$

で, 分母・分子ともに最高次の係数を 1 と基準化すれば, 分母の多項式が μ に付随する直交多項式に一致する. なお, $\{Q_n\}$ は μ の (または $\{P_n\}$ の) 随伴直交多項式と呼ばれる.

5.2 実確率変数の量子分解

古典確率変数 X で分布 μ が $\mathfrak{P}_{\mathrm{fm}}(\mathbb{R})$ に属するものを考えよう. この μ に付随する直交多項式を $\{P_n\}$, ヤコビ係数を $(\{\omega_n\}, \{\alpha_n\})$ とする. $\{\omega_n\}$ はヤコビ数列なので, それに付随する相互作用フォック空間 $(\Gamma(\mathbb{C}), \{\Phi_n\}, B^+, B^-)$ を考える. 等距離作用素 $U : \Gamma(\mathbb{C}) \to L^2(\mathbb{R}, \mu)$ が

$$U : \sqrt{\omega_n \cdots \omega_2 \omega_1}\, \Phi_n \mapsto P_n$$

によって定義される (U は必ずしもユニタリではないことに注意). $L^2(\mathbb{R}, \mu)$ において x による掛け算作用素を Q で表す. 相互作用フォック空間の定義と直交多項式の満たす 3 項間漸化式を比較すれば,

$$Q = U(B^+ + B^- + B^\circ)U^*, \qquad B^\circ = \alpha_{N+1},$$

が容易にわかる. したがって,

$$\int_{-\infty}^{+\infty} x^m \mu(dx) = \langle P_0, Q^m P_0 \rangle = \langle \Phi_0, (B^+ + B^- + B^\circ)^m \Phi_0 \rangle, \quad m = 0, 1, 2, \ldots. \tag{5.4}$$

一方, μ は X の分布なので, (5.4) は $\mathrm{E}(X^m)$ に等しい. よって, 代数的確率変数として

$$X = B^+ + B^- + B^\circ \tag{5.5}$$

が成り立つ. これを X の**量子分解**, $\{B^+, B^-, B^\circ\}$ をその量子成分という.

例 5.4 例 1.12 で述べた $B^+ + B^-$ はそれぞれの分布をもつ古典確率変数の量子分解を与えている.

ここでは, 古典確率空間で定義された確率変数 X の量子分解として話を進めてきたが, 代数的確率空間における実確率変数 a も同様にして量子分解される. X や a の分布を議論するとき, それらが生成する可換 $*$-代数を使っているといえる. 確率変数を量子分解して量子成分を取り出すと, それらは互いに非可換である. したがって, 量子成分を扱うためには, その可換 $*$-代数の非可換拡張を考えることになる. 問題によっては, この非可換拡張が有効に使えるのである. この実例を次節で扱う.

5.3 グラフの階層化と隣接行列の量子分解

グラフ $G=(V,E)$ には原点 $o\in V$ が定まっているものとする. このとき, グラフには自然な階層構造が導入される:

$$V=\bigcup_{n=0}^{\infty}V_n,\qquad V_n=\{x\in V\,;\,\partial(o,x)=n\}. \tag{5.6}$$

ある番号 $m\geq 1$ で $V_m=\emptyset$ となれば, その先 $n\geq m$ すべてで $V_n=\emptyset$ となる. (5.6) にしたがって, 隣接行列 A の量子成分を定義しよう. $x\in V_n$ として

$$(A^\epsilon)_{yx}=\begin{cases}A_{yx}=1, & y\sim x\text{ かつ }y\in V_{n+\epsilon},\\ 0, & \text{その他,}\end{cases}\qquad \epsilon\in\{+,-,\circ\}.$$

ただし, $n+\epsilon$ は $\epsilon=+,-,\circ$ に応じて, $n+1,n-1,n$ を意味する (図 3). 明らかに, $(A^+)^*=A^-$, $(A^\circ)^*=A^\circ$ および

$$A=A^+ + A^- + A^\circ \tag{5.7}$$

が成り立つ. (5.7) を A の量子分解という. 量子分解はグラフの階層化 (つまり, 原点 $o\in V$ のとり方) に依存して定まる.

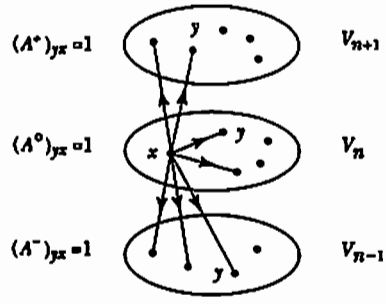


図 3: 量子分解: $A=A^+ + A^- + A^\circ$

次に, $V_n\neq\emptyset$ なる $n\geq 0$ に対して

$$\Phi_n=|V_n|^{-1/2}\sum_{x\in V_n}\delta_x$$

とおくと, $\{\Phi_n\}$ は $\ell^2(V)$ の正規直交系となる. $\{\Phi_n\}$ によって張られる $\ell^2(V)$ の閉部分空間 $\Gamma(G)$ をグラフ G の階層化 (5.6) に付随するフォック空間と呼ぶことにする. 一般には, $\Gamma(G)$ は, A の量子成分に関して不変であるとは限らない. 興味があるのは,

(i) $\Gamma(G)$ が A の量子成分に関して不変である場合;
(ii) $\Gamma(G)$ が A の量子成分に関して漸近的に不変である場合;

である. (i) のときは, $(\Gamma(G), A^{\pm})$ が相互作用フォック空間になり, $A = A^{+} + A^{-} + A^{\circ}$ の分布は前節で述べた方法で求めることができる. (ii) については, 節をあらためて述べる. すべての距離正則グラフは条件 (i) を満たす. 次はその典型例である.

例 5.5 (ケステン分布) 次数 $\kappa \geq 2$ の等質樹木 $\mathcal{T}_{\kappa}$ の隣接行列を $A = A_{\kappa}$ とする. 原点 o を定め, 付随するフォック空間 $\Gamma(\mathcal{T}_{\kappa})$ とその正規直交基底 $\{\Phi_n\}_{n=0}^{\infty}$ を上のように定める. 簡単な計算によって,

$$\begin{cases} A\Phi_0 = \sqrt{\kappa}\,\Phi_1, \\ A\Phi_1 = \sqrt{\kappa}\,\Phi_0 + \sqrt{\kappa-1}\,\Phi_2, \\ A\Phi_n = \sqrt{\kappa-1}\,\Phi_{n-1} + \sqrt{\kappa-1}\,\Phi_{n+1}, \quad n \geq 2, \end{cases} \tag{5.8}$$

がわかる. $\Gamma(\mathcal{T}_{\kappa})$ は A の盤子成分 $A^{\pm}$ で不変であり, $(\Gamma(\mathcal{T}_{\kappa}), A^{\pm})$ は相互作用フォック空間になる. (5.8) から Jacobi 係数 $\{\alpha_n \equiv 0\}$, $\{\omega_1 = \kappa, \omega_2 = \omega_3 = \cdots = \kappa - 1\}$ が求まる. これらを係数とする連分数 (5.3) を計算すれば, A の Φ_0 における分布が求められる:

$$\langle \Phi_0, A^m \Phi_0 \rangle = \int_{-2\sqrt{\kappa-1}}^{+2\sqrt{\kappa-1}} x^m \rho_{\kappa}(x)\,dx, \qquad m = 1, 2, \ldots, \tag{5.9}$$

$$\rho_{\kappa}(x) = \frac{1}{2\pi} \frac{\kappa\sqrt{4(\kappa-1) - x^2}}{\kappa^2 - x^2}, \qquad |x| \leq 2\sqrt{\kappa-1}.$$

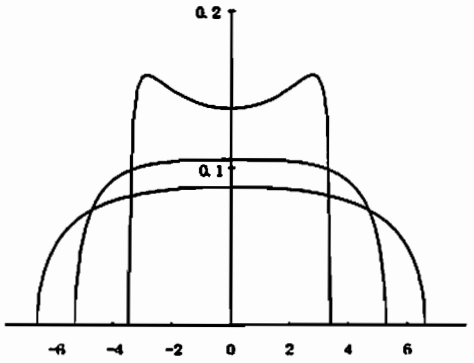


図 4: ケステン分布: $\rho_4, \rho_8, \rho_{12}$

Kesten [26] は, N 個の生成元をもつ自由群の Cayley グラフ (次数 $2N$ の等質樹木) において, 推移行列 $P_N = (2N)^{-1} A_{2N}$ の δ_e における分布を導いた. それは, (5.9) に簡単なスケール変換を施すことで得られる. また, ケステン分布を分散が 1 になるように正規化して, $\kappa \to \infty$ とすると半円則に収束する. これは, グラフの自由積と自由独立性に関する中心極限定理の特別な場合にあたる.

5.4 $\Gamma(G)$ が A の量子成分に関して漸近的に不変である場合

整数格子 $\mathbb{Z}^N$ で説明しよう．隣接行列を A_N とする．原点を $o=(0,\dots,0)$ として，δ_o における A_N のスペクトル分布の高次元極限 $N\to\infty$ に興味がある．$\mathbb{Z}^N$ を

$$\mathbb{Z}^N=\bigcup_{n=0}^{\infty}V_n,\quad V_n=\{x\in\mathbb{Z}^N;\partial(x,o)=n\},$$

のように階層化して，各階層に対応する単位ベクトル $\Phi_n\in\ell^2(\mathbb{Z}^N)$ を

$$\Phi_n=|V_n|^{-1/2}\sum_{x\in V_n}\delta_x,\quad n=0,1,2,\dots,$$

で定義する．任意の頂点 $x\in V$ に隣接する点は，すぐ上または下の階層にだけ存在することから，隣接行列 A_N の量子分解は，

$$A_N=A_N^+ + A_N^-$$

で与えられる．簡単な考察によって，

$$\frac{A_N^+}{\sqrt{2N}}\Phi_n=\sqrt{n+1}\,\Phi_{n+1}+O(N^{-1/2}),$$
$$\frac{A_N^-}{\sqrt{2N}}\Phi_n=\sqrt{n}\,\Phi_{n-1}+O(N^{-1}),$$

が得られる．つまり，$\Gamma(\mathbb{Z}^N)$ は A_N の量子成分 $A_N^{\pm}$ で不変ではないが，$N\to\infty$ において「ほぼ」不変である．そのおかげで，

$$\lim_{N\to\infty}\frac{A_N^{\pm}}{\sqrt{2N}}=B^{\pm}$$

はボゾン・フォック空間の生成・消滅作用素の作用に一致する．さらに，ボゾン・フォック空間において $B^+ + B^-$ の真空状態における分布は標準ガウス分布であることが知られているので，

$$\lim_{N\to\infty}\left\langle\delta_o,\left(\frac{A_N}{\sqrt{2N}}\right)^m\delta_o\right\rangle=\langle\Omega,(B^+ + B^-)^m\Omega\rangle_{\text{Boson}}$$
$$=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty}x^m e^{-x^2/2}dx,\quad m=1,2,\dots,$$

が成り立つ．ただし，Ω はボゾン・フォック空間の真空ベクトルである．つまり，整数格子 $\mathbb{Z}^N$ の隣接行列 A_N の真空状態におけるスペクトル分布は標準ガウス分布に漸近する．この結果は可換独立性を用いた議論でも導かれている (4.1 節)．

上に述べてきた $\mathbb{Z}^N$ に対する考察を一般化して，成長する正則グラフ $G^{(\nu)}=(V^{(\nu)},E^{(\nu)})$ の漸近的スペクトルを求めることができる．ここで ν は成長を表すパラメータであり，あ

る有向集合を走るものとする. 以降では, 考える極限を $\nu \to \infty$ のように簡単に書くことにする. まず,

$$\omega_\epsilon(x) = \{y \in V\,;\, \partial(o,y) = \partial(o,x) + \epsilon\}, \quad \epsilon \in \{+,-,\circ\}$$

として, ω_ϵ の各階層 V_n における3つの統計量を

$$M(\omega_\epsilon|V_n) = \frac{1}{|V_n|}\sum_{x\in V_n}|\omega_\epsilon(x)|$$

$$\Sigma^2(\omega_\epsilon|V_n) = \frac{1}{|V_n|}\sum_{x\in V_n}\left\{|\omega_\epsilon(x)| - M(\omega_\epsilon|V_n)\right\}^2$$

$$L(\omega_\epsilon|V_n) = \max\{|\omega_\epsilon(x)|\,;\, x \in V_n\}$$

で定義する. 次に, これらの統計量が $\nu \to \infty$ でどのように挙動するかの仮定をおく. 簡単のため $\kappa(\nu) = \deg(G^{(\nu)})$ とおく.

(A1) $\lim_{\nu\to\infty} \kappa(\nu) = \infty$.

(A2) 各 $n = 1,2,\ldots$ に対して,

$$\lim_{\nu\to\infty} M(\omega_-|V_n^{(\nu)}) \equiv \omega_n < \infty, \quad \lim_{\nu\to\infty}\Sigma^2(\omega_-|V_n^{(\nu)}) = 0, \quad \sup_\nu L(\omega_-|V_n^{(\nu)}) < \infty.$$

(A3) 各 $n = 0,1,2,\ldots$ に対して,

$$\lim_{\nu\to\infty}\frac{M(\omega_\circ|V_n^{(\nu)})}{\sqrt{\kappa(\nu)}} \equiv \alpha_{n+1} < \infty, \quad \lim_{\nu\to\infty}\frac{\Sigma^2(\omega_\circ|V_n^{(\nu)})}{\kappa(\nu)} = 0, \quad \sup_\nu\frac{L(\omega_\circ|V_n^{(\nu)})}{\sqrt{\kappa(\nu)}} < \infty.$$

定理 5.6 (量子中心極限定理) $\{G^{(\nu)} = (V^{(\nu)}, E^{(\nu)})\}$ を成長する正則グラフで (A1)–(A3) を満たすものとする. $(\Gamma(\mathbb{C}), \{\Psi_n\}, B^+, B^-)$ を $\{\omega_n\}$ に付随する相互作用フォック空間とし, B° を $\{\alpha_n\}$ に付随する対角作用素とする. このとき, すべての $\epsilon_1,\ldots,\epsilon_m \in \{+,-,\circ\}$ と $m = 1,2,\ldots, j,n = 0,1,2,\ldots$ に対して次が成り立つ:

$$\lim_\nu\left\langle \Phi_j^{(\nu)}, \frac{A_\nu^{\epsilon_m}}{\sqrt{\kappa(\nu)}}\cdots\frac{A_\nu^{\epsilon_1}}{\sqrt{\kappa(\nu)}}\Phi_n^{(\nu)}\right\rangle = \langle\Psi_j, B^{\epsilon_m}\cdots B^{\epsilon_1}\Psi_n\rangle.$$

証明は, 量子成分の作用の主要項が相互作用フォック空間で記述され, 剰余項の作用が極限で消えることを示すことにある. 詳しくは [24] を見よ. 定理 5.6 を隣接行列 $A_\nu = A_\nu^+ + A_\nu^- + A_\nu^\circ$ に適用すれば, 次の結果が得られる.

定理 5.7 定理 5.6 の仮定の下で,

$$\lim_\nu\left\langle\delta_o, \left(\frac{A_\nu}{\sqrt{\deg(G^{(\nu)})}}\right)^m\delta_0\right\rangle = \langle\Phi_0, (B^+ + B^- + B^\circ)^m\Psi_0\rangle$$
$$= \int_{-\infty}^{+\infty} x^m\mu(dx), \quad m = 1,2,\ldots.$$

よって, $A_\nu/\sqrt{\deg(G^{(\nu)})}$ の真空状態におけるスペクトル分布は, ヤコビ係数 $(\{\omega_n\},\{\alpha_n\})$ で定まる確率分布に (モーメントの意味で) 収束する.

注意 5.8 定理 5.6–5.7 は Q 行列による真空状態の 1 径数変形に拡張される [24].

ここに述べた成長グラフに対する量子中心極限定理は, 個別の議論で得られた多くの具体例を統一するものとなった.

グラフ	IFS	真空状態	その 1 径数変形
Hamming graphs $H(d,N)$	$\omega_n = n$ (Boson)	Gaussian $(N/d \to 0)$ Poisson $(N/d \to \lambda^{-1} > 0)$	Gaussian or Poisson
Johnson graphs $J(v,d)$	$\omega_n = n^2$	exponential $(2d/v \to 1)$ geometric $(2d/v \to p \in (0,1))$	'Poissonization' of exponential distribution
odd graphs O_k	$\omega_{2n-1} = n$ $\omega_{2n} = n$	two-sided Rayleigh	?
homogeneous trees $\mathcal{T}_\kappa$	$\omega_n = 1$ (free)	Wigner semicircle	free Poisson
integer lattices $\mathbb{Z}^N$	$\omega_n = n$ (Boson)	Gaussian	Gaussian
symmetric groups $\mathfrak{S}_n$ (Coxeter)	$\omega_n = n$ (Boson)	Gaussian	Gaussian
Coxeter groups (Fendler)	$\omega_n = 1$ (free)	Wigner semicircle	free Poisson
Spidernets $S(a,b,c)$	$\omega_1 = 1$ $\omega_2 = \cdots = q$	free Meixner law	(free Meixner law)

5.5 コメント

隣接行列 A_ν の量子成分 A_ν° に対して, その漸近挙動を記述する相互作用フォック空間 $(\Gamma(\mathbb{C}), \{\Phi_n\}, B^+, B^-)$ を構成し, $B^+ + B^- + B^\circ$ の分布から A_ν の漸近的スペクトルを導出した. この方法によれば, 組合せ論的な問題が極限移行した後に現れるので, 有限の ν で直面する組合せ論的な問題 (こちらのほうが込み入っていることが多い) を回避することができる.

本稿で扱ってきた「グラフの漸近的スペクトル解析」の端緒は Hora [16] にある. そこでは, 量子分解によらず, 古典的な結果 [5] を援用して距離正則グラフの隣接行列の漸近的スペクトルが導出された. それに示唆されて, Hashimoto–Obata–Tabei [14] は量子分解の方法をハミング・グラフに適用し, 古典的手法に現れる組合せ論的議論なしに極限分布 (Gauss 分布と Poisson 分布) が導出できることを示した. Hashimoto [12] は同様な方法を Cayley グラフに適用して一般論を展開した. 量子分解のアイデアそのものは素朴なもので, これまでにもさまざまな文脈に現れているが, 隣接行列や古典確率変数を量子確率論の枠組みで解析するための方法として, 「量子分解」という言葉を初めて使ったのは Hashimoto [12] である.

量子分解の手法が有効であるのは, $\Gamma(G_\nu)$ が A_ν° に関して「漸近的に」不変であるときに限る. そうでないときに量子分解の手法を拡張することは興味深い問題である. 多変数

の直交多項式も関連してくるであろう.

成長するグラフは複雑ネットワークのモデルとしても興味がある [9]. グラフの成長を, 各時刻で「独立増分」が付け加わってゆくような形で定式化できると面白いと思う. 本稿で論じてきたグラフの「積構造」と量子確率論の「独立性」の関連を発展させることでヒントが得られるかも知れない. それに関連して, ランダム・グラフ [6] への適用も興味深い研究テーマであろう.

謝辞

本シンポジウムで講演する機会をくださった関係者の方々に感謝します. 距離正則グラフやアソシエーション・スキームなどに関連して, 量子確率論の広がりが期待できる有益なコメントをくださった坂内英一氏, 伊藤達郎氏, 鈴木寛氏, 宗政昭弘氏, 田中太初氏に感謝いたします.

参考文献

[1] L. Accardi, A. Ben Ghorbal and N. Obata: *Monotone independence, comb graphs and Bose-Einstein condensation*, Infin. Dimen. Anal. Quantum Probab. Relat. Top. **7** (2004), 419–435.

[2] L. Accardi, Y. Hashimoto and N. Obata: *Notions of independence related to the free group*, Infin. Dimen. Anal. Quantum Probab. Relat. Top. **1** (1998), 201–220.

[3] L. Accardi, Y. Hashimoto and N. Obata: *Singleton independence*, Banach Center Publ. **43** (1998), 9–24.

[4] 明出伊類似・尾畑伸明: 量子確率論の基礎, 数理情報科学シリーズ 21, 牧野書店, 2003.

[5] E. Bannai and T. Ito: "Algebraic Combinatorics I: Association Schemes," Perseus Books, 1984.

[6] M. Bauer and O. Golinelli: *Random incidence matrices: moments of the spectral density*, J. Statist. Phys. **103** (2001), 301–337.

[7] M. Bożejko: *Positive-definite kernels, length functions on groups and noncommutative von Neumann inequality*, Studia Math. **XCV** (1989), 107–118.

[8] M. Bożejko and R. Speicher: *ψ-independence and symmetrized white noise*, in "Quantum Probability and Related Topics VI (L. Accardi, Ed.)," pp. 170–186, World Scientific, Singapore, 1991.

[9] S. N. Dorogovtsev, A. V. Goltsev, J. F. F. Mendes and A. N. Samukhin: *Random networks: eigenvalue spectra*, Physica A **338** (2004), 76–83.

[10] T. S. Chihara: "An Introduction to Orthogonal Polynomials," Gordon and Breach, 1978.

[11] Y. Hashimoto: *Deformations of the semicircle law derived from random walks on free groups*, Prob. Math. Stat. **18** (1998), 399–410.

[12] Y. Hashimoto: *Quantum decomposition in discrete groups and interacting Fock spaces*, Infin. Dimen. Anal. Quantum Probab. Relat. Top. **4** (2001), 277–287.

[13] Y. Hashimoto, A. Hora and N. Obata: *Central limit theorems for large graphs: Method of quantum decomposition*, J. Math. Phys. **44** (2003), 71–88.

[14] Y. Hashimoto, N. Obata and N. Tabei: *A quantum aspect of asymptotic spectral analysis of large Hamming graphs*, in "Quantum Information III (T. Hida and K. Saitô, Eds.)," pp. 45–57, World Scientific, 2001.

[15] F. Hiai and D. Petz: "The Semicircle Law, Free Random Variables and Entropy," Amer. Math. Soc., 2000.

[16] A. Hora: *Central limit theorems and asymptotic spectral analysis on large graphs*, Infin. Dimen. Anal. Quantum Probab. Relat. Top. **1** (1998), 221–246.

[17] A. Hora: *Central limit theorem for the adjacency operators on the infinite symmetric group*, Commun. Math. Phys. **195** (1998), 405–416.

[18] A. Hora: *Gibbs state on a distance-regular graph and its application to a scaling limit of the spectral distributions of discrete Laplacians*, Probab. Theory Relat. Fields **118** (2000), 115–130.

[19] A. Hora: *A noncommutative version of Kerov's Gaussian limit for the Plancherel measure of the symmetric group*, in "Asymptotic Combinatorics with Applications to Mathematical Physics (A. M. Vershik, Ed.)," pp. 77–88, Lect. Notes in Math. Vol. 1815, Springer–Verlag, 2003.

[20] A. Hora: *Scaling limit for Gibbs states for Johnson graphs and resulting Meixner classes*, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **6** (2003), 139–143.

[21] A. Hora and N. Obata: *Quantum decomposition and quantum central limit theorem*, in "Fundamental Problems in Quantum Physics (L. Accardi and S. Tasaki, Eds.)," pp. 284–305, World Scientific, 2003.

[22] A. Hora and N. Obata: *An interacting Fock space with periodic Jacobi parameter obtained from regular graphs in large scale limit*, in "Quantum Information V (T. Hida and K. Saitô, Eds.)," pp. 121–144, World Scientific, 2006.

[23] A. Hora and N. Obata: "Quantum Probability and Spectral Analysis of Graphs," Springer, 2007.

[24] A. Hora, N. Obata: *Asymptotic spectral analysis of growing regular graphs*, Trans. Amer. Math. Soc. **360** (2008), 899–923.

[25] D. Igarashi and N. Obata: *Asymptotic spectral analysis of growing graphs: Odd graphs and spidernets*, Banach Center Publications **73** (2006), 245–265.

[26] H. Kesten: *Symmetric random walks on groups*, Trans. Amer. Math. Soc. **92** (1959), 336–354.

[27] R. Lenczewski: *On sums of q-independent $SU_q(2)$ quantum variables*, Commun. Math. Phys. **154** (1993), 127–134.

[28] R. Lenczewski: *Unification of independence in quantum probability*, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **1** (1998), 383–405.

[29] R. Lenczewski: *On noncommutative independence*, in "QP–PQ: Quantum Probab. White Noise Anal., Vol. 18," pp. 320–336, World Scientific, 2005.

[30] S. Liang, N. Obata and S. Takahashi: *Asymptotic spectral analysis of generalized Erdős–Rényi random graphs*, Banach Center Publications **78** (2007), 211–229.

[31] Y.-G. Lu: *An interacting free Fock space and the arcsine law*, Probab. Math. Stat. **17** (1997), 149–166.

[32] N. Muraki: *Noncommutative Brownian motion in monotone Fock space*, Commun. Math. Phys. **183** (1997), 557–570.

[33] N. Muraki: *Monotonic independence, monotonic central limit theorem and monotonic law of small numbers*, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **4** (2001), 39–58.

[34] N. Obata: *Quantum probabilistic approach to spectral analysis of star graphs*, Interdiscip. Inform. Sci. **10** (2004), 41–52.

[35] 尾畑伸明: 畳子確率論における独立性とグラフのスペクトル解析, 数学 **57** (2005), 1–20.

[36] N. Obata: *Positive Q-matrices of graphs*, Studia Math. **179** (2007), 81–97.

[37] N. Obata: *Notions of independence in quantum probability and spectral analysis of graphs*, Amer. Math. Soc. Transl. **223** (2008), 115–136.

[38] J. A. Shohat and J. D. Tamarkin: "The Problem of Moments," Amer. Math. Soc., 1943.

[39] R. Speicher and R. Woroudi: *Boolean convolution*, in "Free Probability Theory (D. Voiculescu, Ed.)," pp. 267–279, Fields Inst. Commun. Vol. 12, Amer. Math. Soc., 1997.

[40] H. van Leeuwen and H. Maassen: *A q deformation of the Gauss distribution*, J. Math. Phys. **36** (1995), 4743–4756.

[41] D. Voiculescu, K. Dykema and A. Nica: "Free Random Variables," CRM Monograph Series 1, Amer. Math. Soc., Providence, 1992.

[42] J. Wysoczański: *Monotonic independence associated with partially ordered sets*, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **10** (2007), 17–41.

[43] J. Wysoczański: *bm-independence and central limit theorems associated with symmetric cones*, Banach Center Publ. **78** (2007), 315–320,

[44] J. Wysoczański: *bm-central limit theorems for positive definite real symmetric matrices*, Infin. Dimens. Anal. Quantum Probab. Relat. Top. **11** (2008), 33–51.

Pebble Exchange on Graphs (Extended Abstract)

Shinya Fujita[1]

Department of Mathematics
Gunma National College of Technology
580 Toriba, Maebashi 371-8530, Japan

Tomoki Nakamigawa[2]

Department of Information Science
Shonan Institute of Technology
1-1-25 Tsujido-Nishikaigan, Fujisawa 251-8511, Japan

Tadashi Sakuma[3]

Systems Science and Information Studies
Faculty of Education, Art and Science
Yamagata University
1-4-12 Kojirakawa, Yamagata 990-8560, Japan

Abstract

Let X and Y be connected graphs with n vertices. We introduce a graph puzzle (X, Y) in which X is a board graph and the set of vertices of Y is the set of pebbles. A configuration of Y on X is defined as a bijection from the set of vertices of X to that of Y. A move of pebbles is defined as exchanging two pebbles which are adjacent on both X and Y. For a pair of configurations f and g, we say that g is equivalent to f if f can be transformed into g by a sequence of finite moves. If X is a 4×4 grid graph and Y is a star, then the puzzle (X, Y) corresponds to the well-known 15-puzzle. A puzzle (X, Y) is called feasible if all the configurations of Y on X are mutually equivalent. In this paper, we study the feasibility of the puzzle under various conditions. Among other results, for the case where one of the two graphs X and Y is a complete multipartite graph or a cycle, necessary and sufficient conditions for the feasibility of the puzzle (X, Y) are shown.

[1]This work was supported by Japan Society for the Promotion of Science, Grant-in-Aid for young scientists. Email: fujita@nat.gunma-ct.ac.jp

[2]Email: nakami@info.shonan-it.ac.jp

[3]This work was supported by Grant-in-Aid for Scientific Research (C).
Email: sakuma@e.yamagata-u.ac.jp

1 Introduction

A graph is finite and undirected with no multiple edge or loop. For a graph X, we denote the vertex set and the edge set of X by $V(X)$ and $E(X)$, respectively. Let X and Y be a pair of connected graphs with n vertices. Let us define a graph puzzle (X,Y). A *configuration* of Y on X is defined as a bijection f from $V(X)$ to $V(Y)$. Given a configuration f, it is considered that a vertex $x \in V(X)$ on the board X is occupied by a pebble $f(x) \in V(Y)$. A *move* is defined as exchanging two pebbles $f(x_1)$ and $f(x_2)$, if $x_1x_2 \in E(X)$ and $f(x_1)f(x_2) \in E(Y)$. Let us define the puzzle graph $\mathrm{puz}(X,Y)$ such that $V(\mathrm{puz}(X,Y))$ is the set of all the configurations $\mathcal{F}(X,Y)$, and $E(\mathrm{puz}(X,Y)) = \{(f,g) : f,g \in \mathcal{F}(X,Y), f$ can be transformed into g by some move$\}$. Note that $\mathrm{puz}(X,Y)$ is isomorphic to $\mathrm{puz}(Y,X)$ by the symmetry of the definition of a move.

We say that (X,Y) is *transitive* if for any configuration $f \in \mathcal{F}(X,Y)$ and for any vertex $x \in V(X)$, a pebble $f(x)$ can be shifted to any other vertex of X by a sequence of finite moves. For a graph Z, let $c(Z)$ be the number of connected components of Z. We say that (X,Y) is *feasible* if $c(\mathrm{puz}(X,Y)) = 1$.

Wilson studied the problem for the case $Y = K_{1,n-1}$ by considering permutation groups associated with the puzzle. It is not difficult to see that $(X,K_{1,n-1})$ is transitive if and only if X is 2-connected. Hence, we assume X is 2-connected in the following. Let S_m and A_m denote the symmetric group and the alternating group of order m, respectively. For a finite set M, let $S(M)$ be the symmetric group on M. For a vertex $x \in V(X)$, let $\mathcal{F}_x$ be the set of configurations $f \in \mathcal{F}(X,Y)$ with $f(x) = c$, where c is the center of $K_{1,n-1}$, and define G_x as the set of permutations $\sigma \in S(V(X))$ such that $\sigma(x) = x$ and for any $f \in \mathcal{F}_x$, f can be transformed into $f \circ \sigma$ by a sequence of finite moves. Then (1) G_x is isomorphic to a subgroup of S_{n-1}, (2) G_x is independent on x up to isomorphism, and (3) $c(\mathrm{puz}(X,K_{1,n-1})) = [S_{n-1} : G_x] = (n-1)!/|G_x|$. For positive integers a_1, a_2, a_3, we define $\theta(a_1,a_2,a_3)$-graph such that (1) there exists a pair of vertices u and v of degree 3, and (2) u and v are linked by three disjoint paths containing a_1, a_2 and a_3 inner vertices, respectively.

Theorem A(Wilson[7]). Let $n \geq 2$. Let X be a graph with n vertices. Suppose that X is 2-connected and X is not a cycle. Let G_x be as defined as above, and let $c = c(\mathrm{puz}(X,K_{1,n-1}))$.
(1) If X is a bipartite graph, then $G_x \cong A_{n-1}$ and $c = 2$.
(2) If X is not a bipartite graph except $\theta(1,2,2)$, then $G_x \cong S_{n-1}$ and $c = 1$.
(3) If X is $\theta(1,2,2)$, then $G_x \cong PGL_2(5)$ and $c = 6$, where $PGL_2(5)$ is the

projective general linear group on 2-dimensional verctor space over a finite field of order 5. □

Let p and q be positive integers with $p+q=n$. Theorem A is generalized for the case $Y=\overline{K_p}+K_q$ with $2\leq q$, where $\overline{K_p}$ is the complement of K_p ([4]). Let Z be a connected graph. Let $d\geq 1$. A path $P=v_1\cdots v_d$ of Z is called an *isthmus* if (1) every edge of P is a bridge of Z, (2) every vertex of P is a cutvertex of Z, and (3) $\deg_Z(v_i)=2$ for $1<i<d$. An isthmus with d vertices is called a d-isthmus.

Theorem B(Kornhauser, Miller, Spirakis[4]). Let $2\leq q\leq n-1$ and $p+q=n$. Let X be a connected graph with n vertices. Suppose that X is not a cycle. Let $Y=\overline{K_p}+K_q$. Then the following conditions are equivalent.
(1) X has no q-isthmus.
(2) (X,Y) is transitive.
(3) (X,Y) is feasible. □

For applications, it is important to estimate the number of moves that is necessary in order to transform an initial configuration into a target configuration. Several works have dealt with the reconfiguration problem on graphs from the algorithmic viewpoint([1, 2, 4, 5, 6]).

2 Complete Multipartite Graph

In this section, we consider the case where Y is a complete multipartite graph ([3]).

Let $r\geq 2$ and let $n, n_1, \ldots, n_r$ be positive integers with $n_1\leq\cdots\leq n_r$ such that $n=n_1+\cdots+n_r$. Let X be a graph with n vertices. Let $Y=K_{n_1,n_2,\ldots,n_r}$. For $1\leq i\leq r$, let P_i be the i-th partite set of Y of order n_i.

Firstly, we focus on the case where $r=2$. Let us consider a vertex partition $V(X)=V_1\cup V_2$ with $|V_i|=n_i$ for $i=1,2$. Let us define a family of configurations $\mathcal{F}(V_1,V_2)=\{f\in\mathcal{F}(X,Y) : f(V_i)=P_i \text{ for } i=1,2\}$, and let us define a family of permutations $S(V_1,V_2)=\{\sigma\in S(V(X)) : \sigma(V_i)=V_i \text{ for } i=1,2\}$.

Moreover, we define a group of permutations $G(V_1,V_2)$ arisen from pebble motion such that $G(V_1,V_2)=\{\sigma\in S(V_1,V_2) : f\sim f\circ\sigma \text{ for all } f\in\mathcal{F}(V_1,V_2)\}$. We denote the identity element of a given group by e. For $i=1,2$, let us define $G_i(V_1,V_2)$ as $\{\sigma\in S(V_i) : \sigma=\tau|_{V_i} \text{ for some } \tau\in G(V_1,V_2)\}$, where $\tau|_{V_i}$ is the restriction of τ on V_i. Furthermore, for $i=1,2$, let us define $H_i(V_1,V_2)$ as $\{\sigma\in S(V_i) : \sigma=\tau|_{V_i} \text{ for some } \tau\in G(V_1,V_2) \text{ such that } \tau|_{\overline{V_i}}=e|_{\overline{V_i}}\}$, where $\overline{V_i}$ is the complement of V_i in $V(X)$.

Lemma 1. *All $G(V_1, V_2)$ and $G_i(V_1, V_2)$, $H_i(V_1, V_2)$ for $i = 1, 2$ are independent of the partition $V = V_1 \cup V_2$ with $|V_i| = n_i$ for $i = 1, 2$, up to isomorphism.*

In the following, $G(V_1, V_2)$, $G_i(V_1, V_2)$, and $H_i(V_1, V_2)$ are simply denoted by G, G_i, and H_i, respectively.

Lemma 2. *H_i is a normal subgroup of G_i for $i = 1, 2$.*

Lemma 3. *Let X be a connected graph. Let G, G_1, G_2, H_1, and H_2 be as defined above. Then $G/(H_1 \times H_2) \cong G_1/H_1 \cong G_2/H_2$.*

By Theorem A, the problem for $n_1 = 1$ is already settled. Hence, we may assume $2 \leq n_1$. By Theorem B, if X has no n_1-isthmus, then (X, K_{n_1,n_2}) is transitive and $G_i \cong S_{n_i}$ for $i = 1, 2$.

Let us introduce some more graphs. Let X_0 be a cycle graph with six vertices such that $V(X_0) = \{x_i : 0 \leq i \leq 5\}$ and $E(X_0) = \{x_0x_1, x_1x_2, \ldots, x_5x_0\}$. We define graphs $Q(1)$, $Q(2)$, $Q(1,i)$ for $1 \leq i \leq 3$ with additional vertices y, z, as follows.

$V(Q(1)) = V(X_0) \cup \{y\}$, $E(Q(1)) = E(X_0) \cup \{x_0y\}$,

$V(Q(2)) = V(X_0) \cup \{y, z\}$, $E(Q(2)) = E(X_0) \cup \{x_0y, yz\}$,

$V(Q(1,i)) = V(X_0) \cup \{y, z\}$, $E(Q(1,i)) = E(X_0) \cup \{x_0y, x_iz\}$ for $1 \leq i \leq 3$.

For positive integers a_1, a_2, a_3, we define a tree $T(a_1, a_2, a_3)$ such that (1) there exists a vertex u of degree 3, and (2) u is attached with three disjoint paths of length a_1, a_2 and a_3. Let us denote the dihedral group of order 4 by D_2, which is so-called Klein's group.

Theorem 4. *Let n_1, n_2 be positive integers with $2 \leq n_1 \leq n_2$. Let X be a connected graph with n vertices, where $n = n_1 + n_2$. Suppose that X is not a cycle and X has no n_1-isthmus. Let $Y = K_{n_1,n_2}$. Let H_1, H_2 be as defined above, and let $c = c(\mathrm{puz}(X, Y))$.*

(1) *If X is not a bipartite graph, then $H_1 \cong S_{n_1}$, $H_2 \cong S_{n_2}$ and $c = 1$.*

(2) *If X is a bipartite graph except graphs in* (3)*, then $H_1 \cong A_{n_1}$, $H_2 \cong A_{n_2}$ and $c = 2$.*

(3) (3-1) *Let $n_1 = 3$, $n_2 = 3$. If X is $T(1, 2, 2)$, then $H_1 \cong \{e\}$, $H_2 \cong \{e\}$ and $c = 6$.*

(3-2) *Let $n_1 = 3$, $n_2 = 4$. If X is one of $Q(1)$ and $T(2, 2, 2)$, then $H_1 \cong \{e\}$, $H_2 \cong D_2$ and $c = 6$.*

(3-3) *Let $n_1 = 4$, $n_2 = 4$. If X is one of $\theta(2, 2, 2)$, $Q(1, 3)$, $Q(2)$ and $T(2, 2, 3)$, then $H_1 \cong D_2$, $H_2 \cong D_2$ and $c = 6$.*

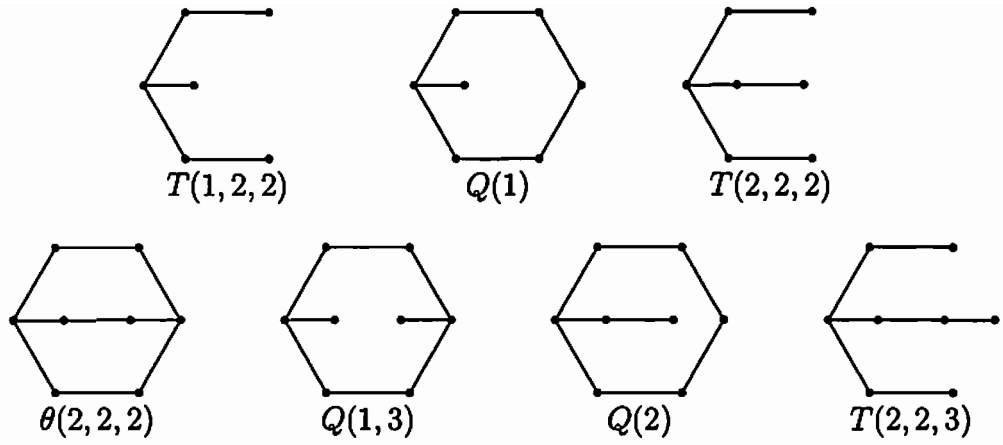


Figure 1. Exceptional graphs in Theorem 4.

For the case where the number of partite sets is at least 3, we have a rather simple result with no exceptional graph.

Theorem 5. *Let $r \geq 3$. Let $n_1, \ldots, n_r$ be positive integers with $n_1 \leq \ldots \leq n_r$. Let X be a connected graph with n vertices, where $n = n_1 + \cdots + n_r$. Suppose that X is not a cycle and X has no $(n - n_r)$-isthmus. Then $(X, K_{n_1,\ldots,n_r})$ is feasible.*

3 Connectivity

In this section, we consider the case where X has a large connectivity. For a graph X, let us denote the maximum degree of X by $\Delta(X)$, and let us denote the connectivity of X by $\kappa(X)$.

Theorem 6. *Let $n \geq 3$. Let X and Y be connected graphs with n vertices. Let $d = \Delta(Y)$. If X is $(n - d + 1)$-connected, then (X, Y) is transitive.*

Let X and Y be bipartite graphs. In this case, for $f, g \in \mathcal{F}(X, Y)$, if $g^{-1} \circ f$ is an odd permutation of $V(X)$ then $f \not\sim g$. We say that (X, Y) is *semi-feasible* if $f \sim g$ holds for any two configurations f and g such that $g^{-1} \circ f$ is an even permutation.

Theorem 7. *Let $n \geq 3$. Let X and Y be graphs with n vertices. Let Y be a tree with $\Delta(Y) = d$. Suppose that X is $(n - d + 1)$-connected.*
(1) *If X is not a bipartite graph, then (X, Y) is feasible except for* (3).
(2) *If X is a bipartite graph, then (X, Y) is semi-feasible except for* (3).
(3) *If $Y = K_{1,n-1}$ and X is one of cycle graphs of order at least 5 and $\theta(1,2,2)$, then (X, Y) is neither feasible nor semi-feasible.*

On the other hand, the existence of a long isthmus is an obstacle for the feasibility.

Proposition 8. *Let $1 \leq k \leq n-2$. Let X and Y be connected graphs with n vertices. If Y has a k-isthmus and $\kappa(X) = k$, then (X, Y) is not transitive.*

We will show that the connectivity in the assumptions of Theorem 6 and Theorem 7 is best possible for some family of graphs. For $3 \leq k \leq n-2$, let $Y(n,k)$ be a tree such that $V(Y(n,k)) = \{y_i : 1 \leq i \leq n\}$ and $E(Y(n,k)) = \{y_i y_{i+1} : 1 \leq i < k\} \cup \{y_k y_i : k < i \leq n\}$. Then $Y(n,k)$ has a $(k-1)$-isthmus and $\Delta(Y(n,k))$ is $n-k+1$. By Theorem 6, Theorem 7 and Proposition 8, we have the following result.

Corollary 9. *Let $3 \leq k \leq n-2$. Let X be a graph with n vertices. Let $Y = Y(n,k)$.*
(1) *(X, Y) is transitive if and only if X is k-connected.*
(2) *If X is k-connected and non-bipartite, then (X, Y) is feasible.*
(3) *If X is k-connected and bipartite, then (X, Y) is semi-feasible.*

4 Cycle

In this section, we consider the case where X is a cycle graph.

For a set of positive integers $c_1, c_2, \ldots, c_r$, let $\gcd(c_1, c_2, \ldots, c_r)$ denote their greatest common divisor.

Theorem 10. *Let $n \geq 3$. Let X be a cycle with n vertices, and let Y be a graph with n vertices. Then (X, Y) is feasible if and only if* (1) *$\overline{Y}$ is a forest, and* (2) *$\gcd(c_1, c_2, \ldots, c_r) = 1$, where r is the number of components of $\overline{Y}$ and c_i is the cardinality of the i-th component of $\overline{Y}$.*

References

[1] V. Auletta, A. Monti, M. Parente, and P. Persiano, A linear-time algorithm for the feasibility of pebble motion in trees, *Algorithmica* **23** (1999), 223–245.

[2] G. Calinescu, A. Dumitrescu, and J. Pach, Reconfigurations in Graphs and Grids, *Proceedings of the 7-th Latin American Symposium on Theoretical Informatics*, LATIN 2006, LNCS 3887, 262–273.

[3] S. Fujita, T. Nakamigawa, and T. Sakuma, Colored Pebble Motion on Graphs(Extended Abstract), *Electronic Notes in Discrete Mathematics*, **34** (2009), 185-189.

[4] D. Kohnhauser, G. Miller, and P. Spirakis, Coodinating pebble motion on graphs, the diameter of permutation groups, and applications, *Proceedings of the 25-th Symposium on Foundations of Computer Science*, (FOCS '84), 241–250.

[5] C. Papadimitriou, P. Raghavan, M. Sudan, and H. Tamaki, Motion planning on a graph, *Proceedings of the 35-th Symposium on Foundations of Computer Science*, (FOCS '94), 511–520.

[6] D. Ratner and M. Warmuth, Finding a shortest solution for the $(N \times N)$-extension of the 15-puzzle is intractable, *J. Symbolic Computation* **10** (1990), 111–137.

[7] R. M. Wilson, Graph puzzles, homotopy, and the alternating group, *J. Combin. Theory Ser. B* **16** (1974), 86–96.

Hamilton C_k-Sixfoil Designs

Kazuhiko Ushio Kinki University

The complete multi-graph λK_n is the complete graph K_n in which every edge is taken λ times. Let C_k be *the k-cycle* (or *the cycle* on k vertices). *The C_k-sixfoil* is a graph of 6 edge-disjoint C_k's with a common vertex and the common vertex is called *the center of the C_k-sixfoil*. In particular, a C_k-sixfoil satisfying $n = 6(k-1)+1$ is called *the Hamilton C_k-sixfoil* because the C_k-sixfoil spans λK_n.
When λK_n is decomposed into edge-disjoint sum of Hamilton C_k-sixfoils, we say that λK_n *has a Hamilton C_k-sixfoil decomposition*. This decomposition is called *a Hamilton C_k-sixfoil design*.

Theorem 1. If λK_n has a Hamilton C_k-sixfoil decomposition, then (i) $n = 6(k-1)+1$ and (ii) $\lambda \equiv 0 \pmod{2k}$ for $k \equiv 2,4,6,8 \pmod{10}$, $\lambda \equiv 0 \pmod{k}$ for $k \equiv 1,3,7,9 \pmod{10}$, $\lambda \equiv 0 \pmod{2k/5}$ for $k \equiv 0 \pmod{10}$, $\lambda \equiv 0 \pmod{k/5}$ for $k \equiv 5 \pmod{10}$.
Proof. When $n = 6(k-1)+1$, suppose that λK_n is decomposed into b Hamilton C_k-sixfoils. Then $b = \lambda n(n-1)/12k = \lambda(6k-5)(k-1)/2k$. Thus, (i), (ii) hold.

Theorem 2. If λK_n has a Hamilton C_k-sixfoil decomposition, then $(s\lambda)K_n$ has a Hamilton C_k-sixfoil decomposition for every s.

Theorem 3. Let n be prime. When $n = 6(k-1)+1$, $\lambda \equiv 0 \pmod{2k}$, and $k \equiv 2,4,6,8 \pmod{10}$, λK_n has a Hamilton C_k-sixfoil decomposition.

Example 3.1. Hamilton C_4-sixfoil of $8K_{19}$.
$(n,g) = (19,2)$ n-orbit : $1,2,4,8,16,13,7,14,9,18,17,15,11,3,6,12,5,10,1$.
Hamilton C_4-sixfoil = $(19,1,2,4) \cup (19,8,16,13) \cup (19,7,14,9) \cup (19,18,17,15) \cup (19,11,3,6) \cup (19,12,5,10)$
Hamilton C_4-sixfoil = $(19,2,4,8) \cup (19,16,13,7) \cup (19,14,9,18) \cup (19,17,15,11) \cup (19,3,6,12) \cup (19,5,10,1)$
Hamilton C_4-sixfoil = $(19,4,8,16) \cup (19,13,7,14) \cup (19,9,18,17) \cup (19,15,11,3) \cup (19,6,12,5) \cup (19,10,1,2)$.
(72 edges = (9 all lengths) * 8 times)
These 3 starters comprise a Hamilton C_4-sixfoil decomposition of $8K_{19}$.

Example 3.2. Hamilton C_6-sixfoil of $12K_{31}$.
$(n,g) = (31,3)$ n-orbit : $1,3,9,27,19,26,16,17,20,29,25,13,8,24,10,30,28,22,4,12,5,15,14,11,2,6,18,23,7,21,1$.
Hamilton C_6-sixfoil = $(31,1,3,9,27,19) \cup (31,26,16,17,20,29) \cup (31,25,13,8,24,10) \cup (31,30,28,22,4,12) \cup (31,5,15,14,11,2) \cup (31,6,18,23,7,21)$
Hamilton C_6-sixfoil = $(31,3,9,27,19,26) \cup (31,16,17,20,29,25) \cup (31,13,8,24,10,30) \cup (31,28,22,4,12,5) \cup (31,15,14,11,2,6) \cup (31,18,23,7,21,1)$
Hamilton C_6-sixfoil = $(31,9,27,19,26,16) \cup (31,17,20,29,25,13) \cup (31,8,24,10,30,28) \cup (31,22,4,12,5,15) \cup (31,14,11,2,6,18) \cup (31,23,7,21,1,3)$
Hamilton C_6-sixfoil = $(31,27,19,26,16,17) \cup (31,20,29,25,13,8) \cup (31,24,10,30,28,22) \cup (31,4,12,5,15,14) \cup (31,11,2,6,18,23) \cup (31,7,21,1,3,9)$

Department of Informatics, Faculty of Science and Technology, Kinki University, Osaka 577-8502, JAPAN.
E-mail:ushio@info.kindai.ac.jp Tel:+81-6-6721-2332 (ext. 5409) Fax:+81-6-6727-2024

Hamilton C_6-sixfoil = $(31,19,26,16,17,20) \cup (31,29,25,13,8,24) \cup (31,10,30,28,22,4)$
$\cup (31,12,5,15,14,11) \cup (31,2,6,18,23,7) \cup (31,21,1,3,9,27)$.
(180 edges = (15 all lengths) * 12 times)
These 5 starters comprise a Hamilton C_6-sixfoil decomposition of $12K_{31}$.

Example 3.3. Hamilton C_8-sixfoil of $16K_{43}$.
$(n,g) = (43,3)$ n-orbit : $1,3,9,27,38,28,41,37,25,32,10,30,4,12,36,22,23,26,35,19,14,$
$42,40,34,16,5,15,2,6,18,11,33,13,39,31,7,21,20,17,8,24,29,1$.
Hamilton C_8-sixfoil = $(43,1,3,9,27,38,28,41) \cup (43,37,25,32,10,30,4,12)$
$\cup (43,36,22,23,26,35,19,14) \cup (43,42,40,34,16,5,15,2) \cup (43,6,18,11,33,13,39,31)$
$\cup (43,7,21,20,17,8,24,29)$
Hamilton C_8-sixfoil = $(43,3,9,27,38,28,41,37) \cup (43,25,32,10,30,4,12,36)$
$\cup (43,22,23,26,35,19,14,42) \cup (43,40,34,16,5,15,2,6) \cup (43,18,11,33,13,39,31,7)$
$\cup (43,21,20,17,8,24,29,1)$
Hamilton C_8-sixfoil = $(43,9,27,38,28,41,37,25) \cup (43,32,10,30,4,12,36,22)$
$\cup (43,23,26,35,19,14,42,40) \cup (43,34,16,5,15,2,6,18) \cup (43,11,33,13,39,31,7,21)$
$\cup (43,20,17,8,24,29,1,3)$
...
Hamilton C_8-sixfoil = $(43,41,37,25,32,10,30,4) \cup (43,12,36,22,23,26,35,19)$
$\cup (43,14,42,40,34,16,5,15) \cup (43,2,6,18,11,33,13,39) \cup (43,31,7,21,20,17,8,24)$
$\cup (43,29,1,3,9,27,38,28)$.
(336 edges = (21 all lengths) * 16 times)
These 7 starters comprise a Hamilton C_8-sixfoil decomposition of $16K_{43}$.

Example 3.4. Hamilton C_{12}-sixfoil of $24K_{67}$.
$(n,g) = (67,2)$ n-orbit : $1,2,4,8,16,32,64,61,55,43,19,38,9,18,36,5,10,20,40,13,26,52,$
$37,7,14,28,56,45,23,46,25,50,33,66,65,63,59,51,35,3,6,12,24,48,29,58,49,31,62,57,$
$47,27,54,41,15,30,60,53,39,11,22,44,21,42,17,34,1$.
Hamilton C_{12}-sixfoil = $(67,1,...) \cup (67,...) \cup (67,...) \cup (67,...) \cup (67,...) \cup (67,...)$
Hamilton C_{12}-sixfoil = $(67,2,...) \cup (67,...) \cup (67,...) \cup (67,...) \cup (67,...) \cup (67,...)$
Hamilton C_{12}-sixfoil = $(67,4,...) \cup (67,...) \cup (67,...) \cup (67,...) \cup (67,...) \cup (67,...)$
...
Hamilton C_{12}-sixfoil = $(67,19,...) \cup (67,...) \cup (67,...) \cup (67,...) \cup (67,...) \cup (67,...)$.
(792 edges = (33 all lengths) * 24 times)
These 11 starters comprise a Hamilton C_{12}-sixfoil decomposition of $24K_{67}$.

Example 3.5. Hamilton C_{14}-sixfoil of $28K_{79}$.
$(n,g) = (79,3)$ n-orbit : $1,3,9,27,2,6,18,54,4,12,36,29,8,24,72,58,16,48,65,37,32,17,$
$51,74,64,34,23,69,49,68,46,59,19,57,13,39,38,35,26,78,76,70,52,77,73,61,25,75,67,$
$43,50,71,55,7,21,63,31,14,42,47,62,28,5,15,45,56,10,30,11,33,20,60,22,66,40,41,44,$
$53,1$.
Hamilton C_{14}-sixfoil = $(79,1,...) \cup (79,...) \cup (79,...) \cup (79,...) \cup (79,...) \cup (79,...)$
Hamilton C_{14}-sixfoil = $(79,3,...) \cup (79,...) \cup (79,...) \cup (79,...) \cup (79,...) \cup (79,...)$
Hamilton C_{14}-sixfoil = $(79,9,...) \cup (79,...) \cup (79,...) \cup (79,...) \cup (79,...) \cup (79,...)$
...
Hamilton C_{14}-sixfoil = $(79,8,...) \cup (79,...) \cup (79,...) \cup (79,...) \cup (79,...) \cup (79,...)$.
(1092 edges = (39 all lengths) * 28 times)
These 13 starters comprise a Hamilton C_{14}-sixfoil decomposition of $28K_{79}$.

Example 3.6. Hamilton C_{18}-sixfoil of $36K_{103}$.

$(n,g) = (103,5)$ n-orbit: 1,5,25,22,7,35,72,51,49,39,92,48,34,67,26,27,32,57,79,86,18,90,38,
87,23,12,60,94,58,84,8,40,97,73,56,74,61,99,83,3,15,75,66,21,2,10,50,44,14,70,41,102,98,
78,81,96,68,31,52,54,64,11,55,69,36,77,76,71,46,24,17,85,13,65,16,80,91,43,9,45,19,95,
63,6,30,47,29,42,4,20,100,88,28,37,82,101,93,53,59,89,33,62,1.
17 starters comprise a Hamilton C_{18}-sixfoil decomposition of $36K_{103}$.

Example 3.7. Hamilton C_{22}-sixfoil of $44K_{127}$.
$(n,g) = (127,3)$ n-orbit: 1,3,9,27,81,116,94,28,84,125,121,109,73,92,22,66,71,86,4,12,36,
108,70,83,122,112,82,119,103,55,38,114,88,10,30,90,16,48,17,51,26,78,107,67,74,95,31,
93,25,75,98,40,120,106,64,65,68,77,104,58,47,14,42,126,124,118,100,46,11,33,99,43,2,6,
18,54,35,105,61,56,41,123,115,91,19,57,44,5,15,45,8,24,72,89,13,39,117,97,37,111,79,110,
76,101,49,20,60,53,32,96,34,102,52,29,87,7,21,63,62,59,50,23,69,80,113,85,1.
21 starters comprise a Hamilton C_{22}-sixfoil decomposition of $44K_{127}$.

Example 3.8. Hamilton C_{24}-sixfoil of $48K_{139}$.
$(n,g) = (139,2)$ n-orbit: 1,2,4,8,16,32,64,128,117,95,51,102,65,130,121,103,67,134,129,119,
99,59,118,97,55,110,81,23,46,92,45,90,41,82,25,50,100,61,122,105,71,3,6,12,24,48,96,53,
106,73,7,14,28,56,112,85,31,62,124,109,79,19,38,76,13,26,52,104,69,138,137,135,131,123,
107,75,11,22,44,88,37,74,9,18,36,72,5,10,20,40,80,21,42,84,29,58,116,93,47,94,49,98,57,
114,89,39,78,17,34,68,136,133,127,115,91,43,86,33,66,132,125,111,83,27,54,108,77,15,30,
60,120,101,63,126,113,87,35,70,1.
23 starters comprise a Hamilton C_{24}-sixfoil decomposition of $48K_{139}$.

Example 3.9. Hamilton C_{26}-sixfoil of $52K_{151}$.
$(n,g) = (151,6)$ n-orbit: 1,6,36,65,88,75,148,133,43,107,38,77,9,54,22,132,37,71,124,140,85,
57,40,89,81,33,47,131,31,35,59,52,10,60,58,46,125,146,121,122,128,13,78,15,90,87,69,112,
68,106,32,41,95,117,98,135,55,28,17,102,8,48,137,67,100,147,127,7,42,101,2,12,72,130,25,
150,145,115,86,63,76,3,18,108,44,113,74,142,97,129,19,114,80,27,11,66,94,111,62,70,118,
104,20,120,116,92,99,141,91,93,105,26,5,30,29,23,138,73,136,61,64,82,39,83,45,119,110,
56,34,53,16,96,123,134,49,143,103,14,84,51,4,24,144,109,50,149,139,79,21,126,1.
25 starters comprise a Hamilton C_{26}-sixfoil decomposition of $52K_{151}$.

Example 3.10. Hamilton C_{28}-sixfoil of $56K_{163}$.
$(n,g) = (163,2)$ n-orbit: 1,2,4,8,16,32,64,128,93,23,46,92,21,42,84,5,10,20,40,80,160,157,
151,139,115,67,134,105,47,94,25,50,100,37,74,148,133,103,43,86,9,18,36,72,144,125,87,
11,22,44,88,13,26,52,104,45,90,17,34,68,136,109,55,110,57,114,65,130,97,31,62,124,85,
7,14,28,56,112,61,122,81,162,161,159,155,147,131,99,35,70,140,117,71,142,121,79,158,153,
143,123,83,3,6,12,24,48,96,29,58,116,69,138,113,63,126,89,15,30,60,120,77,154,145,127,
91,19,38,76,152,141,119,75,150,137,111,59,118,73,146,129,95,27,54,108,53,106,49,98,33,
66,132,101,39,78,156,149,135,107,51,102,41,82,1.
27 starters comprise a Hamilton C_{28}-sixfoil decomposition of $56K_{163}$.

Example 3.11. Hamilton C_{34}-sixfoil of $68K_{199}$.
$(n,g) = (199,3)$ n-orbit: 1,3,9,27,81,44,132,197,193,181,145,37,111,134,4,12,36,108,125,176,
130,191,175,127,182,148,46,138,16,48,144,34,102,107,122,167,103,110,131,194,184,154,64,
192,178,136,10,30,90,71,14,42,126,179,139,19,57,171,115,146,40,120,161,85,56,168,106,119,
158,76,29,87,62,186,160,82,47,141,25,75,26,78,35,105,116,149,49,147,43,129,188,166,100,
101,104,113,140,22,66,198,196,190,172,118,155,67,2,6,18,54,162,88,65,195,187,163,91,74,
23,69,8,24,72,17,51,153,61,183,151,55,165,97,92,77,32,96,89,68,5,15,45,135,7,21,63,189,
169,109,128,185,157,73,20,60,180,142,28,84,53,159,79,38,114,143,31,93,80,41,123,170,112,

137, 13, 39, 117, 152, 58, 174, 124, 173, 121, 164, 94, 83, 50, 150, 52, 156, 70, 11, 33, 99, 98, 95, 86, 59, 177, 133, 1.
33 starters comprise a Hamilton C_{34}-sixfoil decomposition of $68K_{199}$.

Theorem 4. Let n be prime. When $n = 6(k-1)+1$, $\lambda \equiv 0 \pmod{k}$, and $k \equiv 1,3,7,9 \pmod{10}$, λK_n has a Hamilton C_k-sixfoil decomposition.

Example 4.1. Hamilton C_3-sixfoil of $3K_{13}$.
$(n, g) = (13, 2)$ n-orbit : 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1.
L_1 : 1, 12, 1
L_2 : 2, 11, 2
L_3 : 4, 9, 4
L_4 : 8, 5, 8
L_5 : 3, 10, 3
L_6 : 6, 7, 6.
Hamilton C_3-sixfoil = (13, 1, 12) ∪ (13, 2, 11) ∪ (13, 4, 9) ∪ (13, 8, 5) ∪ (13, 3, 10) ∪ (13, 6, 7).
(18 edges = (6 all lengths) * 3 times)
This starter comprises a Hamilton C_3-sixfoil decomposition of $3K_{13}$.

Example 4.2. Hamilton C_7-sixfoil of $7K_{37}$.
$(n, g) = (37, 2)$ n-orbit : 1, 2, 4, 8, 16, 32, 27, 17, 34, 31, 25, 13, 26, 15, 30, 23, 9, 18, 36, 35, 33, 29, 21, 5, 10, 20, 3, 6, 12, 24, 11, 22, 7, 14, 28, 19, 1.
L_1 : 1, 27, 26, 36, 10, 11, 1
L_2 : 2, 17, 15, 35, 20, 22, 2
L_3 : 4, 34, 30, 33, 3, 7, 4
L_4 : 8, 31, 23, 29, 6, 14, 8
L_5 : 16, 25, 9, 21, 12, 28, 16
L_6 : 32, 13, 18, 5, 24, 19, 32.
Hamilton C_7-sixfoil = (37, 1, 27, 26, 36, 10, 11) ∪ (37, 2, 17, 15, 35, 20, 22) ∪ (37, 4, 34, 30, 33, 3, 7) ∪ (37, 8, 31, 23, 29, 6, 14) ∪ (37, 16, 25, 9, 21, 12, 28) ∪ (37, 32, 13, 18, 5, 24, 19)
Hamilton C_7-sixfoil = (37, 27, 26, 36, 10, 11, 1) ∪ (37, 17, 15, 35, 20, 22, 2) ∪ (37, 34, 30, 33, 3, 7, 4) ∪ (37, 31, 23, 29, 6, 14, 8) ∪ (37, 25, 9, 21, 12, 28, 16) ∪ (37, 13, 18, 5, 24, 19, 32)
Hamilton C_7-sixfoil = (37, 26, 36, 10, 11, 1, 27) ∪ (37, 15, 35, 20, 22, 2, 17) ∪ (37, 30, 33, 3, 7, 4, 34) ∪ (37, 23, 29, 6, 14, 8, 31) ∪ (37, 9, 21, 12, 28, 16, 25) ∪ (37, 18, 5, 24, 19, 32, 13).
(126 edges = (18 all lengths) * 7 times)
These 3 starters comprise a Hamilton C_7-sixfoil decomposition of $7K_{37}$.

Example 4.3. Hamilton C_{11}-sixfoil of $11K_{61}$.
$(n, g) = (61, 2)$ n-orbit : 1, 2, 4, 8, 16, 32, 3, 6, 12, 24, 48, 35, 9, 18, 36, 11, 22, 44, 27, 54, 47, 33, 5, 10, 20, 40, 19, 38, 15, 30, 60, 59, 57, 53, 45, 29, 58, 55, 49, 37, 13, 26, 52, 43, 25, 50, 39, 17, 34, 7, 14, 28, 56, 51, 41, 21, 42, 23, 46, 31, 1.
L_1 : 1, 3, 9, 27, 20, 60, 58, 52, 34, 41, 1
L_2 : 2, 6, 18, 54, 40, 59, 55, 43, 7, 21, 2
L_3 : 4, 12, 36, 47, 19, 57, 49, 25, 14, 42, 4
L_4 : 8, 24, 11, 33, 38, 53, 37, 50, 28, 23, 8
L_5 : 16, 48, 22, 5, 15, 45, 13, 39, 56, 46, 16
L_6 : 32, 35, 44, 10, 30, 29, 26, 17, 51, 31, 32.
Hamilton C_{11}-sixfoil = (61, 1, ...) ∪ (61, 2, ...) ∪ (61, 4, ...) ∪ (61, 8, ...) ∪ (61, 16, ...) ∪ (61, 32, ...)
Hamilton C_{11}-sixfoil = (61, 3, ...) ∪ (61, 6, ...) ∪ (61, 12, ...) ∪ (61, 24, ...) ∪ (61, 48, ...) ∪ (61, 35, ...)
Hamilton C_{11}-sixfoil = (61, 9, ...) ∪ (61, 18, ...) ∪ (61, 36, ...) ∪ (61, 11, ...) ∪ (61, 22, ...) ∪ (61, 44, ...)

Hamilton C_{11}-sixfoil = $(61,27,...) \cup (61,54,...) \cup (61,47,...) \cup (61,33,...) \cup (61,5,...) \cup (61,10,...)$
Hamilton C_{11}-sixfoil = $(61,20,...) \cup (61,40,...) \cup (61,19,...) \cup (61,38,...) \cup (61,15,...) \cup (61,30,...)$.
(330 edges = (30 all lengths) * 11 times)
These 5 starters comprise a Hamilton C_{11}-sixfoil decomposition of $11K_{61}$.

Example 4.4. Hamilton C_{13}-sixfoil of $13K_{73}$.
$(n,g) = (73,5)$ n-orbit : 1,5,25,52,41,59,3,15,2,10,50,31,9,45,6,30,4,20,27,62,18,17,
12,60,8,40,54,51,36,34,24,47,16,7,35,29,72,68,48,21,32,14,70,58,71,63,23,42,64,28,
67,43,69,53,46,11,55,56,61,13,65,33,19,22,37,39,49,26,57,66,38,44,1.
L_1 : 1,3,9,27,8,24,72,70,64,46,65,49,1
L_2 : 5,15,45,62,40,47,68,58,28,11,33,26,5
L_3 : 25,2,6,18,54,16,48,71,67,55,19,57,25
L_4 : 52,10,30,17,51,7,21,63,43,56,22,66,52
L_5 : 41,50,4,12,36,35,32,23,69,61,37,38,41
L_6 : 59,31,20,60,34,29,14,42,53,13,39,44,59.
Hamilton C_{13}-sixfoil = $(73,1,...) \cup (73,5,...) \cup (73,25,...) \cup (73,52,...) \cup (73,41,...) \cup (73,59,...)$
Hamilton C_{13}-sixfoil = $(73,3,...) \cup (73,15,...) \cup (73,2,...) \cup (73,10,...) \cup (73,50,...) \cup (73,31,...)$
Hamilton C_{13}-sixfoil = $(73,9,...) \cup (73,45,...) \cup (73,6,...) \cup (73,30,...) \cup (73,4,...) \cup (73,20,...)$
...
Hamilton C_{13}-sixfoil = $(73,24,...) \cup (73,47,...) \cup (73,16,...) \cup (73,7,...) \cup (73,35,...) \cup (73,29,...)$.
(468 edges = (36 all lengths) * 13 times)
These 6 starters comprise a Hamilton C_{13}-sixfoil decomposition of $13K_{73}$.

Example 4.5. Hamilton C_{17}-sixfoil of $17K_{97}$.
$(n,g) = (97,5)$ n-orbit : 1,5,25,28,43,21,8,40,6,30,53,71,64,29,48,46,36,83,27,38,93,
77,94,82,22,13,65,34,73,74,79,7,35,78,2,10,50,56,86,42,16,80,12,60,9,45,31,58,96,
92,72,69,54,76,89,57,91,67,44,26,33,68,49,51,61,14,70,59,4,20,3,15,75,84,32,63,24,
23,18,90,62,19,95,87,47,41,11,55,81,17,85,37,88,52,66,39,1.
L_1 : 1,8,64,27,22,79,50,12,96,89,33,70,75,18,47,85,1
L_2 : 5,40,29,38,13,7,56,60,92,57,68,59,84,90,41,37,5
L_3 : 25,6,48,93,65,35,86,9,72,91,49,4,32,62,11,88,25
L_4 : 28,30,46,77,34,78,42,45,69,67,51,20,63,19,55,52,28
L_5 : 43,53,36,94,73,2,16,31,54,44,61,3,24,95,81,66,43
L_6 : 21,71,83,82,74,10,80,58,76,26,14,15,23,87,17,39,21.
Hamilton C_{17}-sixfoil = $(97,1,...) \cup (97,5,...) \cup (97,25,...) \cup (97,28,...) \cup (97,43,...) \cup (97,21,...)$
Hamilton C_{17}-sixfoil = $(97,8,...) \cup (97,40,...) \cup (97,6,...) \cup (97,30,...) \cup (97,53,...) \cup (97,71,...)$
Hamilton C_{17}-sixfoil = $(97,64,...) \cup (97,29,...) \cup (97,48,...) \cup (97,46,...) \cup (97,36,...) \cup (97,83,...)$
...
Hamilton C_{17}-sixfoil = $(97,12,...) \cup (97,60,...) \cup (97,9,...) \cup (97,45,...) \cup (97,31,...) \cup (97,58,...)$.
(816 edges = (48 all lengths) * 17 times)
These 8 starters comprise a Hamilton C_{17}-sixfoil decomposition of $17K_{97}$.

Example 4.6. Hamilton C_{19}-sixfoil of $19K_{109}$.
$(n,g) = (109,6)$ n-orbit : 1,6,36,107,97,37,4,24,35,101,61,39,16,96,31,77,26,47,64,57,15,90,
104,79,38,10,60,33,89,98,43,40,22,23,29,65,63,51,88,92,7,42,34,95,25,41,28,59,27,53,100,
55,3,18,108,103,73,2,12,72,105,85,74,8,48,70,93,13,78,32,83,62,45,52,94,19,5,30,71,99,
49,76,20,11,66,69,87,86,80,44,46,58,21,17,102,67,75,14,84,68,81,50,82,56,9,54,106,91,1.
9 starters comprise a Hamilton C_{19}-sixfoil decomposition of $19K_{109}$.

Example 4.7. Hamilton C_{27}-sixfoil of $27K_{157}$.

$(n,g) = (157,5)$ n-orbit : 1,5,25,125,154,142,82,96,9,45,68,26,130,22,110,79,81,91,141,77,71, 41,48,83,101,34,13,65,11,55,118,119,124,149,117,114,99,24,120,129,17,85,111,84,106,59, 138,62,153,137,57,128,12,60,143,87,121,134,42,53,108,69,31,155,147,107,64,6,30,150,122, 139,67,21,105,54,113,94,156,152,132,32,3,15,75,61,148,112,89,131,27,135,47,78,76,66,16, 80,86,116,109,74,56,123,144,92,146,102,39,38,33,8,40,43,58,133,37,28,140,72,46,73,51, 98,19,95,4,20,100,29,145,97,14,70,36,23,115,104,49,88,126,2,10,50,93,151,127,7,35,18, 90,136,52,103,44,63,1.
13 starters comprise a Hamilton C_{27}-sixfoil decomposition of $27K_{157}$.

Example 4.8. Hamilton C_{31}-sixfoil of $31K_{181}$.
$(n,g) = (181,2)$ n-orbit : 1,2,4,8,16,32,64,128,75,150,119,57,114,47,94,7,14,28,56,112,43, 86,172,163,145,109,37,74,148,115,49,98,15,30,60,120,59,118,55,110,39,78,156,131,81,162, 143,105,29,58,116,51,102,23,46,92,3,6,12,24,48,96,11,22,44,88,176,171,161,141,101,21,42, 84,168,155,129,77,154,127,73,146,111,41,82,164,147,113,45,90,180,179,177,173,165,149,117, 53,106,31,62,124,67,134,87,174,167,153,125,69,138,95,9,18,36,72,144,107,33,66,132,83,166, 151,121,61,122,63,126,71,142,103,25,50,100,19,38,76,152,123,65,130,79,158,135,89,178,175, 169,157,133,85,170,159,137,93,5,10,20,40,80,160,139,97,13,26,52,104,27,54,108,35,70,140, 99,17,34,68,136,91,1.
15 starters comprise a Hamilton C_{31}-sixfoil decomposition of $31K_{181}$.

Example 4.9. Hamilton C_{33}-sixfoil of $33K_{193}$.
$(n,g) = (193,5)$ n-orbit : 1,5,25,125,46,37,185,153,186,158,18,90,64,127,56,87,49,52,67, 142,131,76,187,163,43,22,110,164,48,47,42,17,85,39,2,10,50,57,92,74,177,113,179,123,36, 180,128,61,112,174,98,104,134,91,69,152,181,133,86,44,27,135,96,94,84,34,170,78,4,20, 100,114,184,148,161,33,165,53,72,167,63,122,31,155,3,15,75,182,138,111,169,73,172,88, 54,77,192,188,168,68,147,156,8,40,7,35,175,103,129,66,137,106,144,141,126,51,62,117,6, 30,150,171,83,29,145,146,151,176,108,154,191,183,143,136,101,119,16,80,14,70,157,13,65, 132,81,19,95,89,59,102,124,41,12,60,107,149,166,58,97,99,109,159,23,115,189,173,93,79, 9,45,32,160,28,140,121,26,130,71,162,38,190,178,118,11,55,82,24,120,21,105,139,116,1.
16 starters comprise a Hamilton C_{33}-sixfoil decomposition of $33K_{193}$.

References

[1] K. Ushio and H. Fujimoto, Balanced bowtie and trefoil decomposition of complete tripartite multigraphs, *IEICE Trans. Fundamentals*, Vol. E84-A, pp. 839–844, 2001.
[2] —, Balanced foil decomposition of complete graphs, *IEICE Trans. Fundamentals*, Vol. E84-A, pp. 3132–3137, 2001.
[3] —, Balanced bowtie decomposition of complete multigraphs, *IEICE Trans. Fundamentals*, Vol. E86-A, pp. 2360–2365, 2003.
[4] —, Balanced bowtie decomposition of symmetric complete multi-digraphs, *IEICE Trans. Fundamentals*, Vol. E87-A, pp. 2769–2773, 2004.
[5] —, Balanced quatrefoil decomposition of complete multigraphs, *IEICE Trans. Information and Systems*, Vol. E88-D, pp. 19–22, 2005.
[6] —, Balanced C_4-bowtie decomposition of complete multigraphs, *IEICE Trans. Fundamentals*, Vol. E88-A, pp. 1148–1154, 2005.
[7] —, Balanced C_4-trefoil decomposition of complete multigraphs, *IEICE Trans. Fundamentals*, Vol. E89-A, pp. 1173–1180, 2006.

Euclidean Designs and Coherent Configurations

Eiichi Bannai (Kyushu University)
and
Etsuko Bannai (Maebaru, Fukuoka)

この原稿は山形での講演の OHP シートをほぼそのままに並べたものです。スタイルは少しだけ変更してあります。

この原稿の内容は、同著者による同じ題名の論文として
rXiv: 0905.2143 に掲載されていますので、興味ある方はそれをご覧いただけたらと思います。

Euclidean Designs

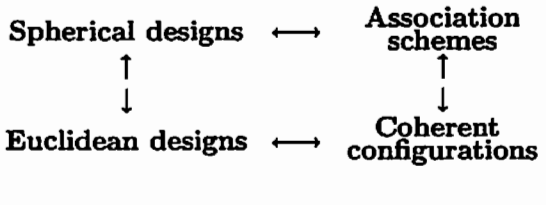
and

Coherent Configurations

Eiichi Bannai and Etsuko Bannai

at Yamagata

June 26, 2009



2

Spherical t-design

[Delsarte-Goethals-Seidel 1977] = approximating the sphere by a finite set (w.r.t. the integrals of polynomials)

For $r > 0$,
$S^{n-1}(r) = \{(x_1, \ldots, x_n) \in R^n \mid x_1^2 + \cdots + x_n^2 = r^2\} \subset \mathbb{R}^n$.

$X \subset S^{n-1}(r)$, $|X| < \infty$, is a spherical t-design
$\Longleftrightarrow$
$\frac{1}{|S^{n-1}(r)|} \int_{S^{n-1}(r)} f(x) d\sigma(x) = \frac{1}{|X|} \sum_{x \in X} f(x)$
for $^\forall f(x) = f(x_1, \ldots, x_n)$, polynomials of degree $\leq t$.

Here $|S^{n-1}(r)|$ = the area of $S^{n-1}(r)$, and the integral in the LHS is the usual surface integral on $S^{n-1}(r)$

3

Equivalent definitions of spherical t-design

$X \subset S^{n-1}$ is a spherical t-design
$\Longleftrightarrow$
$\sum_{x \in X} f(x) = 0$, $\forall f(x)$, homogeneous harmonic polynomials of degree $1, 2, \ldots, t$.
$\Longleftrightarrow$
All kinds of moments of degree $\leq t$ of X are invariant under any orthogonal transformation.
Namely

$$\sum_{x \in X} x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} = \sum_{x \in \sigma(X)} x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}$$

$\lambda_1, \ldots, \lambda_n \geq 0$, $\lambda_1 + \cdots + \lambda_n \leq t$, $^\forall \sigma \in O(n)$

4

Facts on spherical t-designs

1. X is a t-design $\Longrightarrow$ X is a i-design $^\forall i \leq t$.
2. X is a t-design $\Longrightarrow$ $\sigma(X)$ is a t-design $^\forall \sigma \in O(n)$.
3. X_1, X_2 ($X_1 \cap X_2 = \emptyset$) are t-designs $\Longrightarrow$ $X_1 \cup X_2$ is a t-design.

5

Lower bounds (Fisher type inequality)

(Delsarte-Goethals-Seidel 1977)
X is a t-design in $S^{n-1} \subset \mathbb{R}^n$
$t = 2e \Longrightarrow |X| \geq \binom{n-1+e}{e} + \binom{n-1+e-1}{e-1}$
$t = 2e+1 \Longrightarrow |X| \geq 2\binom{n-1+e}{e}$
If " $=$ " holds, then X is a spherical tight t-design.

6

Examples

• Vertices of a regular $(t+1)$-gon on the circle S^1 form a t-design, and it is a tight t-design.

• Vertices of a regular polyhedron in $S^2 \subset \mathbb{R}^3$ form a spherical t-design.

regular polyhedron	no. of vertices	t	tight
simplex	4	2	yes
cube	6	3	yes
octahedron	8	3	no
icosahedron	12	5	yes
dodecahedron	20	5	no

7

• Many good examples of spherical t-designs are obtained as orbits of finite subgroups $G \subset O(n)$

$X = \{g(x_0) \mid g \in G\} \subset S^{n-1}$ for a fixed $x_0 \in S^{n-1}$

• Many good examples of spherical t-designs are obtained as shells of lattices $L \subset \mathbb{R}^n$

$X = L_r = \{x \in L \mid \|x\|^2 = r^2\}$

• $L = E_8$-lattice $\subset \mathbb{R}^8$

$G = Aut(L) = W(E_8) \subset O(8)$.

All the orbits of $G = W(E_8)$ are spherical 7-designs.

(Some of them are 11-designs.)

All the shells of E_8 lattice L are 7-designs.

(It is an open question whether any of them is an 8-design. This is equivalent to Lehmer's conjecture.)

8

• $L =$ Leech lattice $\subset \mathbb{R}^{24}$

$G = Aut(L) =$ Conway $\cdot 0 \subset O(24)$.

All the orbits of G are spherical 11-designs.

(Some of them are 15-designs.)

All the shells of Leech lattice L are 11-designs.

(It is an open question whether any of them is a 12-design.)

• As far as the known examples with $n \geq 3$ are concerned, those obtained as orbits of $G \subset O(n)$ are at most 19-designs, and those obtained as shells of lattices in $\mathbb{R}^n$ are at most 11-designs.

9

So, it is an interesting question whether any 12-design is obtained as a shell of a lattice.
Also, it is an interesting question whether any t-design with arbitrary large t are obtained as orbits of finite groups in $O(n)$.
• Theorem (Seymour-Zaslavsky 1984) for any t and for any n, spherical t-design X on S^{n-1} exists.
• Explicit constructions of spherical t-design X for large t on S^{n-1} for $n \geq 3$ are difficult in general. (cf. G. Kuperberg 2006 for $n = 3$)

10

• Tight spherical t-designs on S^{n-1} are classified (up to orthogonal transformations) except for $t = 4, 5, 7$ (Bannai-Damerell 1979, 1980).
If $n \geq 3$, then $t = 1, 2, 3, 4, 5, 7, 11$.
$t = 1 \Longrightarrow \quad |X| = 2$, a pair of antipodal points.
$t = 2 \Longrightarrow \quad |X| = n + 1$, regular simplex.
$t = 3 \Longrightarrow \quad |X| = 2n$, cross polytope (gen. octahedron).
$t = 11 \Longrightarrow \quad n = 24$, $|X| = 196560$, $X =$ the set of min. vectors of Leech lattice in $\mathbb{R}^{24}$
$t = 4 \Longrightarrow \quad n = (2k+1)^2 - 3$
$t = 5 \Longrightarrow \quad n = 3$ or $(2k+1)^2 - 2$
$t = 7 \Longrightarrow \quad n = 3d^2 - 4$
Bannai-Munemasa-Venkov (2004) obtained more non-existence results for $t = 4, 5, 7$.

11

Association schemes and coherent configurations Association scheme $(X, \{R_i\}_{i \in I})$ is a pair of a finite set X and a set of relations $\{R_i\}_{i \in I}$ on X satisfying certain axioms.

Coherent configuration is a more general concept (than association scheme) defined as follows.

12

coherent configurations
X : a finite set $R_1, R_2, \ldots, R_l \subset X \times X$.

If the following conditions (1)~(4) are satisfied,
then $\mathfrak{X} = (X, \{R_i\}_{1 \leq i \leq l})$ is a coherent configuration

1. $X \times X = R_1 \cup R_2 \cup \cdots \cup R_l$ is a partition.
2. $^{\exists}p$ s.t. $1 \leq p < l$, $R_1 \cup \cdots \cup R_p = \{(x, x) \mid x \in X\}$.
3. For each i, $^{\exists}i'$ such that ${}^tR_i = R_{i'}$, $1 \leq i' \leq l$, (where ${}^tR_i := \{(x, y) \mid (y, x) \in R_i\}$)
4. For each i, j, k, $|\{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\}|$ is a constant on $(x, y) \in R_k$ (depends only on i, j, k). (We denote it by $p^k_{i,j}$.)

13

Association schemes are special cases of coherent configurations with $p = 1$, i.e.,

$$\{(x, x) \mid x \in X\} = R_1.$$

• Coherent configuration was defined by D. G. Higman in 1970, and is a combinatorial axiomatization of general (not necessarily transitive) finite permutation groups.
• Association scheme is a combinatorial axiomatization of transitive finite permutation groups.
• Important classes of association schemes:
P-polynomial association schemes,
Q-polynomial association schemes,

P- and Q-polynomial association schemes.

14

s-distance set on S^{n-1}

Let $X \subset S^{n-1}$ be a finite set. Define

$$A(X) = \{x \cdot y \mid x \neq y \in X\}$$

X is called an s-distance set if $|A(X)| = s$.
• Theorem (Delsarte-Goethals-Seidel 1977)
Let $X \subset S^{n-1}$ be a finite set which is a t-design and an s-distance set. Then the followings hold:

1. $t \leq 2s$.
2. $t = 2s \iff X$ is a tight $2s$-design.
3. $t = 2s - 1$ and X is antipodal $\iff X$ is a tight $(2s-1)$-design.

15

Moreover, we have
4. $\boxed{t \geq 2s-2} \implies \boxed{(X, \{R_i\}_{0 \leq i \leq s}) \text{ is a Q-polynomial scheme.}}$
Here we define
$A(X) = \{\alpha_1, \ldots, \alpha_s \mid -1 \leq \alpha_i < 1\}$.
$R_i = \{(x, y) \in X \times X \mid x \cdot y = \alpha_i\}, \quad (1 \leq i \leq s)$
$R_0 = \{(x, x) \mid x \in X\}$
Here we use the notations $R_0, \ldots, R_s$ instead of $R_1, \ldots, R_{s+1}$
• Remark (B-B):

$\boxed{t \geq 2s-3 \text{ and } X \text{ is antipodal}} \Rightarrow \boxed{(X, \{R_i\}_{0 \leq i \leq s}) \text{ is a Q-polynomial scheme.}}$

16

Euclidean t-designs

A two step generalization of spherical t-designs, that is X has a weight w and X is in $\mathbb{R}^n$ (not necessarily on S^{n-1}.)

Notation: $X \subset \mathbb{R}^n$, a finite set

$\{\|x\| \mid x \in X\} = \{r_1, \ldots, r_p\}$,

$S_i = \{x \in \mathbb{R}^n \mid \|x\| = r_i\}$, $X_i = S_i \cap X$ $(1 \leq i \leq p)$.

We say X is supported by $S = \cup_{i=1}^{p} S_i$.

$$\varepsilon_S = \begin{cases} 0 & \text{if } 0 \notin S \\ 1 & \text{otherwise.} \end{cases}$$

$w : X \longrightarrow \mathbb{R}_{>0}$, a weight function

$w(X_i) = \sum_{x \in X_i} w(x)$,

$|S^{n-1}| = \int_{S^{n-1}} d\sigma(x)$, $|S_i| = \int_{S_i} d\sigma_i(x)$,

17

If $r_i = 0$, then $\frac{1}{|S_i|} \int_{S_i} f(x) d\sigma_i(x) = f(0)$ for $^\forall f(x) \in \mathcal{P}(n)$,

$|S_i| = {r_i}^{n-1} |S^{n-1}|$ for $r_i > 0$.

Definition(Neumaier-Seidel, 1988)

(X, w) is a Euclidean t-design if

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

for any polynomial $f(x)$ of degree at most t, wehre $w(X_i) = \sum_{x \in X_i} w(x)$.

Remark:

$p = 1$, $X \neq \{0\}$, $w(x) \equiv 1$, $\Longrightarrow$ Spherical t-designs.

18

Equivalent definitions of Euclidean t-design

(X, w) is a Euclidean t-design.

$\Longleftrightarrow$

$\sum_{x \in X} w(x) \|x\|^{2j} \varphi_l(x) = 0$ for any homogeneous harmonic polynomial φ_l of degree l, where l and j are integers satisfying $1 \leq l \leq t$ and $0 \leq j \leq \frac{t-l}{2}$.

19

$\Longleftrightarrow$

All kinds of moments of degree $\leq t$ of X are invariant under any orthogonal transformation.

(Namely, $\sum_{x \in X} w(x) f(x) = \sum_{x \in X} w(x) f(\sigma(x))$ holds for any polynomial f of degree $\leq t$ and $\sigma \in O(n)$.)

20

Natural lower bounds (Fisher type inequality)
Theorem (Möller 1976)
Let $X \subset \mathbb{R}^n$ be a finite set and w be a positive weight function on X.

1. (X, w): Euclidean $2e$-design $\Longrightarrow |X| \geq \dim(\mathcal{P}_e(n)|_S)$.
2. (X, w): Euclidean $(2e+1)$-design.
   (a) e odd, or e even and $0 \notin X \Longrightarrow |X| \geq 2\dim(\mathcal{P}_e^*(n)|_S)$.
   (b) e even and $0 \in X \Longrightarrow |X| \geq 2\dim(\mathcal{P}_e^*(n)|S) - 1$,

where $\mathcal{P}_e(n) = \oplus_{i=0}^{e} \mathrm{Hom}_i(n)$, $\mathcal{P}_e^*(n) = \oplus_{i=0}^{[\frac{e}{2}]} \mathrm{Hom}_{e-2i}(n)$,
where $\mathrm{Hom}_i(n)$ is the space of homogeneous polynomials of degree i, and $S = S_1 \cup \cdots \cup S_p$ (= the set of concentric spheres supporting X).

21

Tight designs
If " $=$ " holds in the previous page, then (X, w) is a tight t-designon p concentric spheres
Moreover if
(1) $\dim(\mathcal{P}_e(n)|_S) = \dim(\mathcal{P}_e(n))$ (for $t = 2e$),
or
(2) $\dim(\mathcal{P}_e^*(n)|_S) = \dim(\mathcal{P}_e^*(n))$ (for $t = 2e+1$)
holds, then (X, w) is a tight t-design in $\mathbb{R}^n$

Note that these conditions (1) and (2) are satisfied if p is large enough ($p \geq \frac{e}{2}$ approximately).

22

Some more notation

(X, w): Euclidean t-design in $\mathbb{R}^n$.
For any $X_\lambda, X_\mu \neq \{0\}$, we define

$$A(X_\lambda, X_\mu) := \left\{ \frac{x \cdot y}{\|x\|\|y\|} \;\middle|\; x \in X_\lambda, y \in X_\mu, x \neq y \right\}.$$

Let $s_{\lambda,\mu} := |A(X_\lambda, X_\mu)|$,
$A(X_\lambda, X_\mu) = \{\alpha_{\lambda,\mu}^{(u)} \mid u = 1, \ldots, s_{\lambda,\mu}\}$, $\quad \alpha_{\lambda,\lambda}^{(0)} := 1$.

(Then clearly $A(X_\lambda, X_\mu) = A(X_\mu, X_\lambda)$, $s_{\lambda,\mu} = s_{\mu,\lambda}$ and $\alpha_{\lambda,\mu}^{(u)} = \alpha_{\mu,\lambda}^{(u)}$.)

23

The following results (Theorem A ~ Theorem E) are the main theorems of this talk.

Theorem A

(X, w): a Euclidean t-design, $w(x) \equiv w_\nu$ for any $x \in X_\nu$.
and one of the following (1) or (2) holds.

1. If $s_{\lambda,\nu} + s_{\nu,\mu} \leq t - 2(p - \varepsilon_S - 2)$ holds for any λ, ν and μ with $1 \leq \lambda, \nu, \mu \leq p$.
2. If X is antipodal and
$$s_{\lambda,\nu} + s_{\nu,\mu} - \delta_{\lambda,\nu} - \delta_{\nu,\mu} \leq t - 2(p - \varepsilon_S - 2)$$
holds for any λ, ν and μ satisfying
$1 \leq \lambda, \nu, \mu \leq p$.

Then X has the structure of a coherent configuration.

24

In other words, for $(x, y) \in X_\lambda \times X_\mu$, with $x \cdot y = \alpha_{\lambda,\mu}^{(k)}$,

$$|\{z \in X_\nu \mid x \cdot z = \alpha_{\lambda,\nu}^{(i)},\ z \cdot y = \alpha_{\nu,\mu}^{(j)}\}|$$

depends only on λ, ν, μ, i, j, k. (Here $1 \leq \lambda, \nu, \mu \leq p$, and $1 - \delta_{\lambda,\nu} \leq i \leq s_{\lambda,\nu}$, $1 - \delta_{\nu,\mu} \leq j \leq s_{\nu,\mu}$, and $1 - \delta_{\lambda,\mu} \leq k \leq s_{\lambda,\mu}$.)

25

Theorem B

Let (X, w) be a tight Euclidean t-design on 2 concentric spheres. Then X has the structure of a coherent configuration.

26

Towards the classification of Euclidean 4-designs on 2 concentric spheres having the structures of coherent configurations.

Theorem C

(X, w): a Euclidean 4-design in $\mathbb{R}^n$ on 2 concentric spheres. $0 \notin X$ and w is constant on each X_λ, $s_{\lambda,\mu} \leq 2$ $(\lambda, \mu = 1, 2)$. Then X has the structure of a coherent configuration and the following holds.
(1) $s_{1,2} = 2$.
(2) (X, w) is a tight Euclidean 4-design or similar to one of the Euclidean 4-design having the parameters given in (i) and (ii).

27

(i) $n = 2$,
$X_1 = \{\pm(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}), \pm(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})\}$,
$X_2 = \{(\pm r_2, 0), (0, \pm r_2)\}$,
$w(x) = 1$ on X_1, $w(x) = r_2^{-4}$ on X_2,
r_2: any positive real number satisfying $r_2 \neq 1$.

28

(ii) $n = (2k-1)^2 - 4$,
$|X_1| = 2(2k+1)(k-1)^3$, $\quad |X_2| = 2k^3(2k-3)$,
$A(X_1) = \{\frac{k-2}{k(2k-3)}, -\frac{1}{2k-3}\}$,
$A(X_2) = \{\frac{1}{2k+1}, -\frac{k+1}{(k-1)(2k+1)}\}$,
$A(X_1, X_2) = \{\frac{1}{\sqrt{n}}, -\frac{1}{\sqrt{n}}\}$,
$r_1 = 1$, $w_1 = 1$,
$w_2 = \frac{(2k+1)^2(k-1)^4}{(2k-3)^2k^4} r_2^{-4}$,
where k is any integer satisfying $k \geq 2$ and r_2 is any positive real number satisfying $r_2 \neq 1$.

The intersection numbers of the corresponding coherent configurations for Theorem C (ii) are given in the Appendix I.

29

Theorem D
A Euclidean 4-design in $\mathbb{R}^n$ having the parameters given in Theorem C (2) (ii) exists if and only if a tight spherical 4-design on $S^n \subset \mathbb{R}^{n+1}$ exists.
(Note that the classification of tight Euclidean 4-designs on 2 concentric spheres is still open.)

30

Theorem E (1) The following is a series of feasible parameters for tight Euclidean 4-design in $\mathbb{R}^n$.
$n = (6k-3)^2 - 3$,
$|X_1| = (6k^2 - 6k + 1)(36k^2 - 36k + 7)$, $\quad |X_2| = 3(36k^2 - 36k + 7)(2k-1)^2$,
$$A(X_1) = \left\{ \frac{18k^2-27k+8}{6(9k^2-9k+1)(2k-1)}, \; -\frac{18k^2-9k-1}{6(9k^2-9k+1)(2k-1)} \right\},$$
$$A(X_2) = \left\{ \frac{36k^3-54k^2+25k-4}{2(6k^2-6k+1)(18k^2-18k+5)}, \; -\frac{36k^3-54k^2+25k-3}{2(6k^2-6k+1)(18k^2-18k+5)} \right\},$$
$$A(X_1, X_2) = \left\{ \sqrt{\frac{36k^2-36k+4}{(36k^2-36k+6)(36k^2-36k+10)}}, -\sqrt{\frac{36k^2-36k+10}{(36k^2-36k+6)(36k^2-36k+4)}} \right\},$$
$r_1 = 1$, $\quad r_2 = \sqrt{\frac{3(18k^2-18k+5)(6k^2-6k+1)}{9k^2-9k+1}}$, $\quad w_1 = 1$, $\quad w_2 = \frac{1}{81(2k-1)^4}$.

31

(2) If $2 \leq n \leq 15^2 - 3$, then tight Euclidean 4-design supported by 2 concentric spheres is similar to one of the examples given in Theorem I, II and III in the paper by Etsuko Bannai (2009) or to the one of those having the parameters given in Theorem E .

The intersection numbers of the corresponding coherent configurations (given in Theorem E(1)) are given in the Appendix II.

32

Examples of tight Euclidean 4-designs on 2 concentric spheres(Etsuko Bannai 2009)
Theorem I. $|X_1| = n+1$.

n	$\lvert X_1\rvert$	$\lvert X_2\rvert$	r_1	r_2	$A(X_1)$	$A(X_2)$	$A(X_1, X_2)$	w_1	w_2
2	3	3	1	$r \neq 1$	$-\frac{1}{2}$	$-\frac{1}{2}r^2$	$\frac{1}{2}r,\ -r$	1	$\frac{1}{r^3}$
4	5	10	1	$\frac{1}{\sqrt{6}}$	$-\frac{1}{4}$	$\frac{1}{36},\ -\frac{1}{9}$	$\frac{1}{6},\ -\frac{1}{4}$	1	27
5	6	15	1	$\sqrt{\frac{8}{5}}$	$-\frac{1}{5}$	$\frac{2}{5},\ -\frac{4}{5}$	$\frac{2}{5},\ -\frac{4}{5}$	1	$\frac{1}{2}$
6	7	21	1	$\sqrt{15}$	$-\frac{1}{6}$	$\frac{9}{2},\ -6$	$1,\ -\frac{5}{2}$	1	$\frac{1}{81}$
22	23	253	1	$\sqrt{\frac{126}{11}}$	$-\frac{1}{22}$	$\frac{45}{22},\ -\frac{117}{44}$	$\frac{21}{44},\ -\frac{12}{11}$	1	$\frac{1}{81}$

For $n = 4,\ 5,\ 6$, X_2 has the structure of the Johnson scheme $J(n+1, 2)$, that is, the trivial tight 4-design in $J(n+1, 2)$. For $n = 22$, X_2 has the structure of tight 4-$(23, 7, 1)$ design in the Johnson schem $J(23, 7)$.

33

Theorem II

$|X_1| = n+2$,

n	$\lvert X_1\rvert$	$\lvert X_2\rvert$	r_1	r_2	$A(X_1)$	$A(X_2)$	$A(X_1, X_2)$	w_1	w_2
4	6	9	1	$\sqrt{2}$	$0,\ -\frac{1}{2}$	$\frac{1}{2},\ -1$	$\frac{1}{2},\ -1$	1	$\frac{1}{3}$

X_2 has the structure of the Hamming scheme $H(2, 3)$, that is, trivial tight 4-design of the Hamming scheme.

Theorem III

n	$\lvert X_1\rvert$	$\lvert X_2\rvert$	r_1	r_2	$A(X_1)$	$A(X_2)$	$A(X_1, X_2)$	w_1	w_2
22	33	243	1	$\sqrt{11}$	$0,\ -\frac{1}{2}$	$2,\ -\frac{5}{2}$	$\frac{1}{2},\ -1$	1	$\frac{1}{81}$

X_2 has the structure of tight 4-design in the Hamming scheme $H(11, 3)$.
Note that the inner products $A(Y_i)$ or $A(Y_i, Y_j)$ are differently normalized from the previous normalization in this talk.

34

For more details of this talk, see our paper:
Euclidean designs and coherent configurations
by Eiichi Bannai and Etsuko Bannai,which will be available in arXiv:0905.2143.

THANK YOU

Appendix I

Feasible parameters of the Euclidean 4-design (X, w) given in Theorem C(2)(ii) and the intersection numbers of the coresponding coherent configuration.

$$n = (2k-1)^2 - 4,$$
$$|X_1| = 2(2k+1)(k-1)^3, \quad |X_2| = 2k^3(2k-3),$$
$$A(X_1, X_1) = \{\tfrac{k-2}{k(2k-3)}, -\tfrac{1}{2k-3}\}, \quad A(X_2, X_2) = \{\tfrac{1}{2k+1}, -\tfrac{k+1}{(k-1)(2k+1)}\},$$
$$A(X_1, X_2) = \{\tfrac{1}{\sqrt{n}}, -\tfrac{1}{\sqrt{n}}\},$$
$$r_1 = 1, \quad w_1 = 1, \quad w_2 = \tfrac{(2k+1)^2(k-1)^4}{(2k-3)^2k^4} r_2^{-4},$$

Intersection matrices and Character tables of the association scheme for X_1

$$B_1^{(1)} = \begin{bmatrix} 0 & 1 & 0 \\ k^3(2k-3) & (k+1)(k^2-k-1)k & (k-1)k^3 \\ 0 & (k^2-k-1)(k-1)^2 & k^3(k-2) \end{bmatrix},$$

$$B_2^{(1)} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & (k^2-k-1)(k-1)^2 & k^3(k-2) \\ (k-1)(2k-3)(k^2-k-1) & (k-2)(k-1)(k^2-k-1) & (k-1)(k-2)(k^2-2k-2) \end{bmatrix},$$

$$P_1 = \begin{bmatrix} 1 & k^3(2k-3) & (k-1)(2k-3)(k^2-k-1) \\ 1 & k^2(k-2) & -1-k^2(k-2) \\ 1 & -k & -1+k \end{bmatrix},$$

$$Q_1 = \begin{bmatrix} 1 & (2k+1)(2k-3) & 2(2k-3)(k^2-k-1)k \\ 1 & \frac{(k-2)(2k+1)}{k} & -\frac{2(k^2-k-1)}{k} \\ 1 & -2k-1 & 2k \end{bmatrix},$$

Intersection matrices and Character tables of the association scheme for X_2

$$B_1^{(2)} = \begin{bmatrix} 0 & 1 & 0 \\ (2k+1)(k^2-k-1)k & (k+1)(k^2-3)k & (k+1)(k^2-k-1)k \\ 0 & (k+1)(k-1)^3 & (k^2-k-1)k^2 \end{bmatrix},$$

$$B_2^{(2)} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & (k+1)(k-1)^3 & (k^2-k-1)k^2 \\ (2k+1)(k-1)^3 & (k-1)^3k & (k-2)(k-1)(k^2-k-1) \end{bmatrix}$$

$$P_2 = \begin{bmatrix} 1 & (2k+1)(k^2-k-1)k & (k-1)(2k^3-3k^2+1) \\ 1 & k(k^2-k-1) & -(k-1)(k^2-1) \\ 1 & -k & k-1]]) \end{bmatrix}$$

$$Q_2 = \begin{bmatrix} 1 & (2k+1)(2k-3) & 2(k-1)(2k+1)(k^2-k-1) \\ 1 & 2k-3 & -2k+2 \\ 1 & -\frac{(2k-3)(k+1)}{k-1} & \frac{2(k^2-k-1)}{k-1} \end{bmatrix}$$

$$p_{\gamma_1,\gamma_1}^{\alpha_0} = k^3(2k-3), \quad p_{\gamma_1,\gamma_1}^{\beta_0} = (2k+1)(k-1)^3$$
$$p_{\gamma_2,\gamma_2}^{\alpha_1} = (k^2-k-1)k^2, \quad p_{\gamma_1,\gamma_2}^{\alpha_1} = (k-1)^2k^2, \quad p_{\gamma_1,\gamma_1}^{\alpha_1} = (k^2-k-1)k^2$$

$$p^{\alpha_2}_{\gamma_2,\gamma_2} = k^3(k-2), \quad p^{\alpha_2}_{\gamma_1,\gamma_2} = (k-1)k^3, \quad p^{\alpha_2}_{\gamma_1,\gamma_1} = k^3(k-2)$$
$$p^{\beta_1}_{\gamma_1,\gamma_2} = (k-1)^3k, \quad p^{\beta_1}_{\gamma_2,\gamma_2} = (k+1)(k-1)^3, \quad p^{\beta_1}_{\gamma_1,\gamma_1} = (k+1)(k-1)^3$$
$$p^{\beta_2}_{\gamma_1,\gamma_2} = (k-1)^2k^2, \quad p^{\beta_2}_{\gamma_2,\gamma_2} = (k^2-k-1)(k-1)^2, \quad p^{\beta_2}_{\gamma_1,\gamma_1} = (k^2-k-1)(k-1)^2,$$

$$p^{\gamma_1}_{\gamma_2,\beta_2} = (k-1)^2k^2, \quad p^{\gamma_1}_{\alpha_2,\gamma_2} = (k^2-k-1)(k-1)^2, \quad p^{\gamma_1}_{\gamma_1,\beta_1} = (k+1)(k^2-k-1)k,$$

$$p^{\gamma_1}_{\gamma_2,\beta_1} = (k^2-k-1)k^2\ , \quad p^{\gamma_1}_{\alpha_1,\gamma_1} = (k^2-k-1)k^2, \quad p^{\gamma_1}_{\alpha_1,\gamma_2} = (k-1)^2k^2,$$

$$p^{\gamma_1}_{\gamma_1,\beta_2} = (k^2-k-1)(k-1)^2, \quad p^{\gamma_1}_{\alpha_2,\gamma_1} = (k-2)(k-1)(k^2-k-1),$$

$$p^{\gamma_2}_{\gamma_2,\beta_2} = (k^2-k-1)(k-1)^2\ , \quad p^{\gamma_2}_{\alpha_2,\gamma_2} = (k-2)(k-1)(k^2-k-1),$$

$$p^{\gamma_2}_{\gamma_1,\beta_2} = (k-1)^2k^2, \quad p^{\gamma_2}_{\gamma_1,\beta_1} = (k^2-k-1)k^2, \quad p^{\gamma_2}_{\alpha_1,\gamma_2} = (k^2-k-1)k^2,$$

$$p^{\gamma_2}_{\alpha_2,\gamma_1} = (k^2-k-1)(k-1)^2, \quad p^{\gamma_2}_{\gamma_2,\beta_1} = (k+1)(k^2-k-1)k, \quad p^{\gamma_2}_{\alpha_1,\gamma_1} = (k-1)^2k^2.$$

In above $p^c_{a,b} = p^c_{b,a}$ holds for any $a, b, c \in \{\alpha_i, \beta_j, \gamma_k \mid i,\ j = 0, 1, 2, k = 1, 2\}$.

Appendix II

The feasible parameters of the Euclidean tight 4-design given in Theorem E and intersection numbers of the corresponding coherent configuration.

$$n = (6k-3)^2 - 3,$$
$$|X_1| = (6k^2-6k+1)(36k^2-36k+7), \quad |X_2| = 3(36k^2-36k+7)(2k-1)^2,$$
$$A(X_1, X_1) = \left\{ \frac{18k^2-27k+8}{6(9k^2-9k+1)(2k-1)}, \ -\frac{18k^2-9k-1}{6(9k^2-9k+1)(2k-1)} \right\},$$
$$A(X_2, X_2) = \left\{ \frac{36k^3-54k^2+25k-4}{2(6k^2-6k+1)(18k^2-18k+5)}, \ -\frac{36k^3-54k^2+25k-3}{2(6k^2-6k+1)(18k^2-18k+5)} \right\},$$
$$A(X_1, X_2) = \left\{ \sqrt{\frac{36k^2-36k+4}{(36k^2-36k+6)(36k^2-36k+10)}}, \ -\sqrt{\frac{36k^2-36k+10}{(36k^2-36k+6)(36k^2-36k+4)}} \right\},$$
$$r_1 = 1, \quad r_2 = \sqrt{\tfrac{3(18k^2-18k+5)(6k^2-6k+1)}{9k^2-9k+1}}, \quad w_1 = 1, \quad w_2 = \tfrac{1}{81(2k-1)^4}.$$

Intersection matrices and the Character tables of the association scheme for X_1

$$B_1^{(1)} = \begin{bmatrix} 0 & 1 & 0 \\ 6(-1+2k)(9k^2-9k+1)k & 54k^4-45k^3-12k^2+7k+1 & (18k^2-9k-1)k(3k-2) \\ 0 & (3k-2)(k-1)(18k^2-9k-1) & k(3k-1)(18k^2-27k+8) \end{bmatrix},$$

$$B_1^{(2)} = \begin{bmatrix} 0 & 0 & \\ 0 & (3k-2)(k-1)(18k^2-9k-1) & \\ 6(k-1)(-1+2k)(9k^2-9k+1) & (18k^2-27k+8)(k-1)(3k-1) & \\ & & 1 \\ & & k(3k-1)(18k^2-27k+8) \\ & & 54k^4-171k^3+177k^2-64k+5 \end{bmatrix},$$

$$P_1 = \begin{bmatrix} 1 & 6(-1+2k)(9k^2-9k+1)k & 6(k-1)(-1+2k)(9k^2-9k+1) \\ 1 & -3k+1 & 3k-2 \\ 1 & k(18k^2-27k+8) & -(k-1)(18k^2-9k-1) \end{bmatrix},$$

$$Q_1 = \begin{bmatrix} 1 & 6(36k^2-36k+7)(k-1)k & 36k^2-36k+6 \\ 1 & -\frac{(3k-1)(k-1)(36k^2-36k+7)}{(-1+2k)(9k^2-9k+1)} & \frac{(18k^2-27k+8)(6k^2-6k+1)}{(-1+2k)(9k^2-9k+1)} \\ 1 & \frac{k(3k-2)(36k^2-36k+7)}{(-1+2k)(9k^2-9k+1)} & -\frac{(18k^2-9k-1)(6k^2-6k+1)}{(-1+2k)(9k^2-9k+1)} \end{bmatrix},$$

Intersection matrices and the Character tables of the association scheme for X_2

$$B_2^{(1)} = \begin{bmatrix} 0 & 1 & \\ 2(6k^2-6k+1)(18k^2-18k+5) & (9k^2-9k+1)(12k^2-10k+3) & \\ 0 & (3k-2)(36k^3-54k^2+25k-3) & \\ & & 0 \\ & & (3k-2)(36k^3-54k^2+25k-3) \\ & & (36k^3-54k^2+25k-4)(3k-1) \end{bmatrix},$$

$$B_2^{(2)} = \begin{bmatrix} 0 & 1 & \\ 0 & (3k-2)(36k^3-54k^2+25k-3) & \\ 2(6k^2-6k+1)(18k^2-18k+5) & (36k^3-54k^2+25k-4)(3k-1) & \\ & & 0 \\ & & (36k^3-54k^2+25k-4)(3k-1) \\ & & (9k^2-9k+1)(12k^2-14k+5) \end{bmatrix},$$

$$P_2 = \begin{bmatrix} 1 & 2(6k^2-6k+1)(18k^2-18k+5) & 2(6k^2-6k+1)(18k^2-18k+5) \\ 1 & -3k+1 & 3k-2 \\ 1 & 36k^3-54k^2+25k-4 & 3-36k^3+54k^2-25k \end{bmatrix},$$

$$Q_2 = \begin{bmatrix} 1 & 2(6k^2-6k+1)(36k^2-36k+7) & 36k^2-36k+6 \\ 1 & -\frac{(3k-1)(36k^2-36k+7)}{18k^2-18k+5} & \frac{3(36k^3-54k^2+25k-4)}{18k^2-18k+5} \\ 1 & \frac{(3k-2)(36k^2-36k+7)}{18k^2-18k+5} & -\frac{3(36k^3-54k^2+25k-3)}{18k^2-18k+5} \end{bmatrix},$$

$$p_{\gamma_1,\gamma_1}^{\alpha_0} = 3(18k^2-18k+5)(2k-1)^2, \quad p_{\gamma_1,\gamma_1}^{\beta_0} = (6k^2-6k+1)(18k^2-18k+5),$$

$$p_{\gamma_2,\gamma_2}^{\alpha_1} = (2k-1)(54k^3-72k^2+15k+4), \quad p_{\gamma_1,\gamma_2}^{\alpha_1} = (3k-2)(2k-1)(18k^2-18k+5),$$
$$p_{\gamma_1,\gamma_1}^{\alpha_1} = (2k-1)(3k-1)(18k^2-18k+5),$$

$$p_{\gamma_2,\gamma_2}^{\alpha_2} = (54k^3-90k^2+33k-1)(2k-1), \quad p_{\gamma_1,\gamma_2}^{\alpha_2} = (2k-1)(3k-1)(18k^2-18k+5),$$
$$p_{\gamma_1,\gamma_1}^{\alpha_2} = (3k-2)(2k-1)(18k^2-18k+5),$$

$$p_{\gamma_1,\gamma_2}^{\beta_1} = (2k-1)(3k-2)(9k^2-9k+1), \quad p_{\gamma_2,\gamma_2}^{\beta_1} = (9k^2-9k+1)k(6k-5),$$
$$p_{\gamma_1,\gamma_1}^{\beta_1} = (3k-1)(18k^3-27k^2+14k-3),$$

$$p^{\beta_2}_{\gamma_1,\gamma_2} = (3k-1)(9k^2-9k+1)(2k-1), \quad p^{\beta_2}_{\gamma_2,\gamma_2} = (9k^2-9k+1)(6k-1)(k-1),$$
$$p^{\beta_2}_{\gamma_1,\gamma_1} = (3k-2)(18k^3-27k^2+14k-2),$$

$$p^{\gamma_1}_{\gamma_2,\beta_2} = 2(3k-1)(9k^2-9k+1)(2k-1), \quad p^{\gamma_1}_{\alpha_2,\gamma_2} = 2(3k-1)(k-1)(9k^2-9k+1),$$
$$p^{\gamma_1}_{\gamma_1,\beta_1} = 2(3k-1)(18k^3-27k^2+14k-3), \quad p^{\gamma_1}_{\gamma_2,\beta_1} = 2(2k-1)(3k-2)(9k^2-9k+1),$$
$$p^{\gamma_1}_{\alpha_1,\gamma_1} = 2k(3k-1)(9k^2-9k+1), \quad p^{\gamma_1}_{\alpha_1,\gamma_2} = 2k(3k-2)(9k^2-9k+1),$$
$$p^{\gamma_1}_{\gamma_1,\beta_2} = 2(3k-2)(18k^3-27k^2+14k-2), \quad p^{\gamma_1}_{\alpha_2,\gamma_1} = 2(k-1)(9k^2-9k+1)(3k-2),$$

$$p^{\gamma_2}_{\gamma_2,\beta_2} = (6k-1)(k-1)(18k^2-18k+5), \quad p^{\gamma_2}_{\alpha_2,\gamma_2} = (k-1)(54k^3-90k^2+33k-1),$$
$$p^{\gamma_2}_{\gamma_1,\beta_2} = (2k-1)(3k-1)(18k^2-18k+5), \quad p^{\gamma_2}_{\gamma_1,\beta_1} = (3k-2)(2k-1)(18k^2-18k+5),$$
$$p^{\gamma_2}_{\alpha_1,\gamma_2} = k(54k^3-72k^2+15k+4), \quad p^{\gamma_2}_{\alpha_2,\gamma_1} = (18k^2-18k+5)(3k-1)(k-1),$$
$$p^{\gamma_2}_{\gamma_2,\beta_1} = (6k-5)k(18k^2-18k+5), \quad p^{\gamma_2}_{\alpha_1,\gamma_1} = (3k-2)k(18k^2-18k+5).$$

In above $p^c_{a,b} = p^c_{b,a}$ holds for any $a, b, c \in \{\alpha_i, \beta_j, \gamma_k \mid i,\ j = 0, 1, 2, k = 1, 2\}$.

Categories of association schemes and coherent configurations

Akihide Hanaki (Shinshu University)

現代の数学においては、数学的対象のなす圏を考え、その性質を調べることによって問題の解決を目指すという手法が多く用いられている。しかしながら、組合せ論的な対象のなす圏は、一般にそれほど良い性質をもたないためあまり多くは考えられていないように思われる。ここではアソシエーション・スキームの圏と、より一般的な coherent configuration の圏を定義し、その基本的な性質を考察する。ここで定義する圏は、有限群の圏を充満部分圏に含み、したがってそれほど良い性質をもつ圏ではない。また、現時点ではこれらの圏を考えることによって得られる本質的に新しいことは何もない。しかし、これまでに定義されている概念をこの圏の中で特徴付けることによって、その普遍性や定義の意味をより深く理解できるものと信じている。

アソシエーション・スキームに関する文献は [5]、coherent confuguration については [3]、また圏論については [4] を参照して頂きたい。なお、アソシエーション・スキームの圏に関する結果は、2 年ほど前にいくつかの小さな集会で発表したものとほとんど同じである。

1 アソシエーション・スキームと coherent configuration の圏

X を空でない有限集合とし S を $X \times X$ の分割とする。すなわち $X \times X = \bigcup_{s \in S} s$ であり、各 $s \in S$ は空でなく、$s \neq s'$ ならば $s \cap s' = \emptyset$ である。(X, S) が以下の条件をみたすとき、これを**アソシエーション・スキーム**であるという。

(1) $1_S = \{(x, x) \mid x \in X\}$ とおくと、$1_S \in S$ である。

(2) $s \in S$ に対して $s^* = \{(y, x) \mid (x, y) \in S\}$ とおくと、$s^* \in S$ である。

(3) $s,t,u \in S$ に対して $p_{st}^{u} \in \mathbb{Z}_{\geq 0}$ が存在して、$(x,y) \in u$ の取り方によらず $\sharp\{z \in X \mid (x,z) \in s,\ (z,y) \in t\} = p_{st}^{u}$ である。

(1) の条件を次の (1') で置き換えたものが **coherent configuration** である。

(1') $s \in S$ に対して $s \cap 1_S \neq \emptyset$ ならば、$s \subset 1_S$ である。

アソシエーション・スキーム[1]が coherent configuration であることは定義よりすぐに分かる。定義から $(x,y) \in X \times X$ に対して $(x,y) \in s$ となる $s \in S$ が一意的に存在する。したがって、写像 $r : X \times X \to S$ が定義され、これは全射となる。

例 1.1. G を有限集合 X 上の置換群とする。G は $X \times X$ 上にも自然に作用する。この軌道の定める $X \times X$ の分割は coherent configuration となる。G の X への作用を可移と仮定するとアソシエーション・スキームが得られる。

アソシエーション・スキームと coherent configuration の圏を定義する。

アソシエーション・スキームの圏 $\mathcal{AS}$ は対象としてアソシエーション・スキームをもち、射 $f : (X,S) \to (Y,T)$ は写像 $f : X \cup S \to Y \cup T$ で $f(X) \subset Y$, $f(S) \subset T$, $f(r(x,x')) = r(f(x),f(x'))$ をみたすものとする。これが圏を定めることは容易に確認できる。この射の定義は [5, §1.7] の定義と同じものである。まったく同様に coherent configuration の圏 $\mathcal{CC}$ も定義される。

ここで定義した圏 $\mathcal{AS}$ と $\mathcal{CC}$ について、このままで議論を進めることもできるが、これらの圏は零対象 (zero object) をもたず、その議論はやや繁雑になる。そこで次のように更に特別な圏を定義する。

集合を対象とする圏 $\mathcal{S}$ は零対象をもたないが、空でない集合に一つの特別な要素 (base point) を定め、射としては base point を bese point に移すものだけを考えれば、これはまた圏をなす。これを**基点つき集合の圏**といい $\mathcal{S}_0$ で表す。$\mathcal{S}_0$ においては、一つの要素のみからなる集合が零対象となる。

これと同様に**基点つきアソシエーション・スキームの圏** $\mathcal{AS}_0$ と**基点つき coherent configuration の圏** $\mathcal{CC}_0$ を定める。すなわち、アソシエーション・スキーム (X,S) に対して $x \in X$ を一つ定めたもの (X,S,x) を対象とし、(X,S,x) から (Y,T,y) への射としては、$\mathcal{AS}$ における射 f であって $f(x) = y$ なるものとする。これが圏をなすことは明らかである。これを $\mathcal{AS}_0$ と表す。$\mathcal{CC}_0$ も同様に定義される。$\mathcal{S}_0$ と同じように、X が一つの要素からなるとき、

[1] Higman [3] では、ここで定義したアソシエーション・スキームを homogeneous coherent configuration と呼んでいる。また、例えば [1] のように、常に $s^* = s$ を仮定する流儀もあるが、ここでは一般に $s^* = s$ とは限らないものを扱う。

すなわち $X=\{x\}$ であるときに (X,S,x) は零対象となる。以後、単にアソシエーション・スキームといって基点付きのアソシエーション・スキームを意味することも許すものとする。

以後、$\mathcal{AS}_0$ と $\mathcal{CC}_0$ について考察をしていくが、議論が繁雑になるだけで類似のことは $\mathcal{AS}$ と $\mathcal{CC}$ でも考えることができる。

次のことはすぐに分かる。

定理 1.2. $\mathcal{AS}_0$ は $\mathcal{CC}_0$ の充満部分圏である。有限群はアソシエーション・スキームと見ることができて、その意味で、有限群のなす圏は $\mathcal{AS}_0$ の充満部分圏である。

2 単型と全型

ここでは基本的な関手を定義して、それを通して $\mathcal{AS}_0$ と $\mathcal{CC}_0$ の射が単型、あるいは全型であることを特徴付ける。どちらの圏でもほとんど同じ議論が成り立つので　$\mathcal{AS}_0$ についてのみ解説する。

$\mathcal{AS}_0$ の射 $f:(X,S,x)\to(Y,T,y)$ は写像 $f:X\cup S\to Y\cup T$ で与えられる。これを X に制限して、共変関手 $P:\mathcal{AS}_0\to\mathcal{S}_0$ が得られる。同様に S に制限すれば、やはり共変関手 $R:\mathcal{AS}_0\to\mathcal{S}_0$ が得られる。ここで R を考えるときには 1_S を基点と考えて $f(1_S)=1_T$ が成り立っている。

基本的な性質として以下が成り立つ。

定理 2.1. P は忠実な関手である。

射の単型、全型について次の定理が成り立つ。

定理 2.2. f を $\mathcal{AS}_0$ の射とするとき次の関係が成り立つ。

$$\begin{array}{ccccc} P(f)\text{ は全射} & \Longleftrightarrow & f\text{ は全型} & \Longrightarrow & R(f)\text{ は全射} \\ P(f)\text{ は単射} & \Longleftrightarrow & f\text{ は単型} & \Longleftarrow & R(f)\text{ は単射} \end{array}$$

f と $R(f)$ の関係は必要十分ではなく、実際に、単型 f で $R(f)$ が単射でないもの、全型でない f で $R(f)$ が全射であるもの、は存在する。

$\mathcal{AS}_0$ においては、双型、すなわち単型かつ全型、であることと $P(f)$ が全単射であることは同値である。双型は同型とは限らず、よって $\mathcal{AS}_0$ は balanced ではない。$\mathcal{AS}_0$ の双型を fusion scheme という。これは [5, §1.7] の定義と本質的に同じである。

$\mathcal{CC}_0$ では次が成り立つ。

定理 2.3. f を $\mathcal{CC}_0$ の射とするとき次の関係が成り立つ。

$$P(f) \text{ は全射} \iff f \text{ は全型} \implies R(f) \text{ は全射}$$
$$P(f) \text{ は単射} \implies f \text{ は単型} \impliedby R(f) \text{ は単射}$$

これは $\mathcal{AS}_0$ の場合とほぼ同じ結果であるが f が単型であるときに $P(f)$ が単射になるかどうかは分かっておらず、また反例も知らない。

3 部分スキームと剰余スキーム

(X, S, x_0) をアソシエーションスキームとする。$x \in X$, $s \in S$ に対して $xs = \{y \in X \mid (x, y) \in s\}$ とおく。$T \subset S$ に対しても $xT = \bigcup_{t \in T} xt$ とする。また $s, t \in S$ に対して $st = \{u \in S \mid p^u_{st} > 0\}$ とおく。$T, U \subset S$ に対しても $TU = \bigcup_{t \in T} \bigcup_{u \in U} tu$ とする。

$TT \subset T$ が成り立つとき T を S の**閉部分集合** (closed subset) という。T を閉部分集合とする。このとき $X/T = \{xT \mid x \in X\}$ は X の分割を定める。また $S_{x_0T} = \{s \cap (x_0T \times x_0T) \mid s \in S, s \cap (x_0T \times x_0T) \neq \emptyset\}$ は $x_0T \times x_0T$ の分割となる。このとき (x_0T, S_{x_0T}, x_0) はアソシエーション・スキームとなる。これを (X, S, x_0) の T によって定まる**部分スキーム** (subscheme) [2] という。また $s \in S$ に対して $s^T = \{(xT, yT) \mid s \cap (xT \times yT) \neq \emptyset\}$ とおき、更に $S/\!/T = \{s^T \mid s \in S\}$ とおく。このとき $(X/T, S/\!/T, x_0T)$ はまたアソシエーション・スキームとなる。これを (X, S, x_0) の T によって定まる**商スキーム** (quotient scheme) という。

Coherent configuration に対しても同様に部分構造と商構造が考えられるが、商構造の定義には色々とあるようである。

次の節で部分スキームと剰余スキームを圏 $\mathcal{AS}_0$, $\mathcal{CC}_0$ の中で特徴付ける。$\mathcal{AS}_0$, $\mathcal{CC}_0$ においては部分スキームとは上のように定義されたものからの自然な埋め込みとして定義する。また商スキームは自然な全射によって定義する。よってこれらの圏においては、部分スキーム、商スキームは対象ではなく射であることに注意して欲しい。

4 核と余核

次の定理が成り立つ。

---

[2] これは [5] による定義と同じであるが [2] では異なる意味で subscheme という言葉を使っている。また一般に基点を定めないと、閉部分集合に対する部分スキームは (同型を除いたとしても) 一意的ではない。これは基点を定めたアソシエーション・スキームを考えることの一つの利点といえる。

定理 4.1. $\mathcal{AS}_0$ と $\mathcal{CC}_0$ は核と余核をもつ。すなわち $\mathcal{AS}_0$ と $\mathcal{CC}_0$ の任意の射は核と余核をもつ。

$f:(X,S,x_0)\to(Y,T,y_0)$ を $\mathcal{AS}_0$ の射とする。このとき $f^{-1}(1_T)$ は S の閉部分集合となる。この閉部分集合の定める部分スキームを考えるとこれが f の核となる。また $f(S)$ を含む T の最小の閉部分集合を考えれば、これによる商スキームが f の余核となる。

一般に核と余核をもつ圏において、ある射の核となる射を**正規部分対象**、ある射の余核となる射を**余正規商対象**という。上のことは正規部分対象は部分スキームと同値であり、余正規商対象は商スキームと同値であるということを意味するが、逆も正しい。

定理 4.2. $\mathcal{AS}_0$ の射が正規部分対象であるための必要十分条件は、それが部分スキームと同値であることである。$\mathcal{AS}_0$ の射が余正規商対象であるための必要十分条件は、それが商スキームと同値であることである。

射 f の (余) 核は零射と f との (co)equalizer であるが、一般に $\mathcal{AS}_0$ の二つの射に対して (co)equalizer が存在するかどうかは分かっていない。

5 像

次の定理が成り立つ。

定理 5.1. $\mathcal{AS}_0$ は像をもつ。すなわち $\mathcal{AS}_0$ の任意の射は像をもつ。

$\mathcal{AS}_0$ の射 f に対して、f の核の余核が f の像となる。

6 完全列

$\mathcal{AS}_0$ は完全圏 (exact category) ではないが、核と像をもつため完全列を考えることができる。$\mathcal{AS}_0$ の射の列

$$\cdots\to M_{i-1}\xrightarrow{f_{i-1}}M_i\xrightarrow{f_i}M_{i+1}\to\cdots$$

が**完全列** (exact sequence) であるとは、各 i について f_i の核が f_{i-1} の像となることである。ただし、有限の列を考えるときには端の部分は考えない。このとき次の定理が成り立つ。

定理 6.1. $\mathcal{AS}_0$ において次が成り立つ。

(1) $0 \to M \xrightarrow{f} N$ が完全列であることと f が単型であることは同値である。

(2) $M \xrightarrow{f} N \to 0$ が完全列であることと f が商スキーム (余正規商対象) であることは同値である。

(3) $0 \to M \xrightarrow{f} N \to 0$ が完全列であることと f が同型であることは同値である。

(4) $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ が完全列であることと $f = \mathrm{Ker}(g)$ かつ $g = \mathrm{Coker}(f)$ であることは同値である。

7 群の圏

定理 1.2 で見たように $\mathcal{AS}_0$ は有限群の圏を充満部分圏として含んでいる。この部分圏との関係を考えることによって [5], [6] などで定義されている thin radical, thin residue, schurian scheme などを圏論的な普遍性によって特徴付けることができる。これについては、まだ定義が出来ただけで深い議論はしていない。今後の発展が望まれる。

References

[1] R. A. Bailey, *Association schemes*, Cambridge Studies in Advanced Mathematics, vol. 84, Cambridge University Press, Cambridge, 2004.

[2] E. Bannai and T. Ito, *Algebraic combinatorics. I*, The Benjamin/Cummings Publishing Co. Inc., Menlo Park, CA, 1984.

[3] D. G. Higman, *Coherent configurations. I. Ordinary representation theory*, Geometriae Dedicata 4 (1975), no. 1, 1–32.

[4] B. Mitchell, *Theory of categories*, Pure and Applied Mathematics, Vol. XVII, Academic Press, New York, 1965.

[5] P.-H. Zieschang, *An algebraic approach to association schemes*, Lecture Notes in Mathematics, vol. 1628, Springer-Verlag, Berlin, 1996.

[6] ———, *Theory of association schemes*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.

Characterizations of regularity for certain Q-polynomial association schemes

Sho Suda
Division of Mathematics, Graduated School of Information Sciences, Tohoku University,
6-3-09 Aramaki-Aza-Aoba, Aoba-ku, Sendai 980-8579, Japan
suda@ims.is.tohoku.ac.jp

Abstract

The author showed that linked systems of symmetric designs with $a_1^* = 0$ and mutually unbiased bases (MUB) are triply regular association schemes. In this paper, we characterize triple regularity of linked systems of symmetric designs by its Krein number. And we prove that maximal MUB carries a quadruply regular association scheme and characterize the quadruple regularity of MUB by its parameter.

1 Introduction

We study the regularity of 3-class (respectively 4-class) Q-polynomial association schemes with Q-antipodal (respectively both Q-antipodal and Q-bipartite).

In Section 2, we consider linked systems of symmetric designs. Systems of projective designs, that were defined by P. J. Cameron [3], are the combinatorial object of finite doubly transitive groups which have more than two pairwise inequivalent permutation representations with the same permutation character. We call it linked systems of symmetric designs, if symmetric designs appearing in systems of projective designs are all same parameters. Noda [9] showed several inequalities concerning the parameters of linked systems of symmetric designs. Mathon [8] showed every linked system of symmetric designs carries a 3-class association scheme and calculated its eigenmatrices. It implies that these association schemes are Q-polynomial with Q-antipodal. Conversely van Dam [4] showed every 3-class Q-polynomial association scheme with Q-antipodal arises from a linked system of symmetric designs. The author [10] proved that every linked system of symmetric designs with $a_1^* = 0$ is a triply regular association scheme. Main theorem in this section is the converse proposition, that is, if a linked system of symmetric designs is triply regular, then $a_1^* = 0$. This proof is essentially due to [9, Theorem 2].

In Section 3, we consider the quadruple regularity of symmetric association schemes. We define the quadruple regularity and give the sufficient condition that spherical designs become the quadruply regular symmetric association schemes.

In Section 4, we consider the real mutually unbiased bases (MUB). One important problem of real MUB is to determine the maximal number of real MUB in $\mathbb{R}^d$. It is well known that its number is at most $d/2 + 1$. Real MUB is said to be maximal if equality holds. Recently W. J. Martin et al. [6] showed that there is a one-to-one correspondence between real MUB and 4-class Q-polynomial association schemes which is both Q-bipartite and Q-antipodal. Moreover W.J. Martin et al. [7] had shown that a 4-class Q-polynomial association schemes which is both Q-bipartite and Q-antipodal is obtained by the extended Q-bipartite double of a linked system of symmetric design with certain parameters. The author proved in [10] that every MUB carries

a triply regular association scheme. The main theorem in this section is that MUB carries a quadruply regular association scheme if and only if MUB is maximal.

2 Linked systems of symmetric designs

Definition 2.1. Let $(X_i, X_j, I_{i,j})$ be an incidence structure satisfying $X_i \cap X_j = \emptyset$, $I_{j,i}^t = I_{i,j}$ for any distinct integers $i, j \in \{1, \ldots, f\}$. We put $X = \bigcup_{i=1}^f X_i$, $I = \bigcup_{i \neq j} I_{i,j}$. (X, I) is called a linked system of symmetric (v, k, λ) designs if the following conditions hold:

(1) for any distinct integers $i, j \in \{1, \ldots, f\}$, $(X_i, X_j, I_{i,j})$ is a symmetric (v, k, λ) design,

(2) for any distinct integers $i, j, l \in \{1, \ldots, f\}$, and for any $x \in X_i, y \in X_j$, the number of $z \in X_l$ incident with both x and y depends only on whether x and y are incident or not, and does not depend on i, j, l.

We define the integers σ, τ by

$$|\{z \in X_l \mid (x,z) \in I_{i,l}, (y,z) \in I_{j,l}\}| = \begin{cases} \sigma & \text{if } (x,y) \in I_{i,j}, \\ \tau & \text{if } (x,y) \notin I_{i,j}, \end{cases}$$

where $i, j, l \in \{1, \ldots, f\}$ are distinct and $x \in X_i$, $y \in X_j$. Theorem 1 in [3] shows

$$(\sigma, \tau) = \left(\frac{1}{v}(k^2 \mp \sqrt{n}(v-k)), \frac{k}{v}(k \pm \sqrt{n}) \right),$$

where $n = k - \lambda$. Considering complement designs $(X_i, X_j, \overline{I_{i,j}})$ for any distinct integers $i, j \in \{1, \ldots, f\}$, we can assume either $(\sigma, \tau) = (\frac{1}{v}(k^2 - \sqrt{n}(v-k)), \frac{k}{v}(k + \sqrt{n}))$ or $(\frac{1}{v}(k^2 + \sqrt{n}(v-k)), \frac{k}{v}(k - \sqrt{n}))$.

We obtain a Q-antipodal 3-class Q-polynomial association scheme $(X, \{R_i\}_{i=0}^3)$ where

$$\begin{aligned} R_0 &= \{(x,x) \mid x \in X\}, \\ R_1 &= \{(x,y) \mid x \in X_i, y \in X_j, (x,y) \in I_{i,j} \text{ for some } i \neq j\}, \\ R_2 &= \{(x,y) \mid x, y \in X_i, x \neq y \text{ for some } i\}, \\ R_3 &= \{(x,y) \mid x \in X_i, y \in X_j, (x,y) \notin I_{i,j} \text{ for some } i \neq j\}. \end{aligned}$$

Conversely every Q-antipodal 3-class Q-polynomial association scheme with equivalence relation $R_0 \cup R_2$ arises from a linked system of symmetric designs in [4, Theorem 5.8].

Theorem 2.2. *$(X, \{R_i\}_{i=0}^3)$ is a Q-polynomial association scheme which is Q-antipodal with equivalence relation $R_0 \cup R_2$. Then the following are equivalent.*

(1) *$(X, \{R_i\}_{i=0}^3)$ is triply regular.*

(2) $a_1^* = 0$.

Proof. (2)⇒(1): Follows from [10, Corollary 6.2].

(1)⇒(2):Let $\{X_i, \ldots, X_f\}$ be a system of imprimitivity with respect to the equivalence relation $R_0 \cup R_2$ and (X, R_1) a linked system of symmetric (v, k, λ) designs. Assume that

$$\sigma = \frac{1}{v}(k^2 - \sqrt{n}(v-k)), \quad \tau = \frac{k}{v}(k + \sqrt{n}).$$

By the assumption of triple regularity, the following number

$$|\{w \in X \mid (x,w),(y,w),(z,w) \in R_1\}|$$

for distinct points $x,y,z \in X_1$ does not depend on $x,y,z \in X_1$. This implies that a pair $(X_1, \bigcup_{i=2}^{f} X_i)$ is a 3-design, therefore equality holds in [9, Theorem 2]. It follows that

$$f-1 = \frac{(v-2)\sqrt{k(v-k)}}{(v-2k)\sqrt{v-1}}.$$

This implies $a_1^* = 0$ (See [10, p.14]). □

Remark 2.3. Mathon [8] pointed out that the inequality in [9, Theorem 2] is equivalent to $a_1^* \geq 0$.

3 Quadruple regularity of symmetric association schemes

Definition 3.1. Let $(X, \{R_i\}_{i=0}^d)$ be a symmetric association scheme. Then the association scheme X is said to be quadruply regular if, for all $I = (i_1,i_2,i_3,i_4) \subset \{0,1,\ldots,d\}^4$, $J = (j_{\alpha,\beta})_{1\leq\alpha<\beta\leq 4} \subset \{0,1,\ldots,d\}^6$ and $x_1,\ldots,x_4 \in X$ such that $(x_k,x_l) \in R_{j_{k,l}}$ for any $1 \leq k < l \leq 4$, the number

$$|R_{i_1}(x_1) \cap R_{i_2}(x_2) \cap R_{i_3}(x_3) \cap R_{i_4}(x_4)|$$

depends only on I, J and not on $x_1,\ldots,x_4$.

Let $(X, \{R_i\}_{i=0}^d)$ be a symmetric association scheme. We define the i-th subconstituent with respect to $z \in X$ by $R_i(z) := \{y \in X \mid (z,y) \in R_i\}$ and the (i,j)-th subconstituent with respect to $(z_1,z_2) \in X \times X$ by $R_{i,j}(z_1,z_2) := R_i(z_1) \cap R_j(z_2)$. We denote by $R_{i,j,k,l}^{m,n}(z_1,z_2)$ the restriction R_n to $R_{i,j}(z_1,z_2) \times R_{k,l}(z_1,z_2)$ for $(z_1,z_2) \in R_m$. Moreover let $(X, \{R_i\}_{i=0}^d)$ be triply regular. We denote $p_{l,m,n}^{i,j,k} = |R_m(x) \cap R_n(y) \cap R_l(z)|$ for $x,y,z \in X$ such that $(x,y) \in R_i, (y,z) \in R_j, (z,x) \in R_k$. Quadruple regularity is characterized by the concept of coherent configuration. We omit easy proof of the following lemma.

Lemma 3.2. *A symmetric association scheme $(X, \{R_i\}_{i=0}^d)$ is quadruply regular if and only if $(X, \{R_i\}_{i=0}^d)$ is triply regular and for all $m \in \{1,\ldots,d\}$ and $z_1,z_2 \in X$ with $(z_1,z_2) \in R_m$, $(\bigcup_{i,j=1}^d R_{i,j}(z_1,z_2), \{R_{i,j,k,l}^{m,n}(z_1,z_2) \mid 1 \leq i,j,k,l \leq d, p_{i,j,m}^{l,k,n} \neq 0\})$ is a coherent configuration whose parameters depend only on m, not on the choice of z_1,z_2 with $(z_1,z_2) \in R_m$.*

Let X be a finite subset in S^{d-1} with degree s, and $A(X) = \{\alpha_1,\ldots,\alpha_s\}$. For $z_1,z_2 \in X$ with $\langle z_1,z_2\rangle = \alpha_m \neq \pm 1$, $X_{i,j}^m = X_{i,j}^m(z_1,z_2)$ will denote the orthogonal projection of $\{y \in X \mid \langle y,z_1\rangle = \alpha_i, \langle y,z_2\rangle = \alpha_j\}$ to $\langle z_1,z_2\rangle^\perp = \{y \in \mathbb{R}^d \mid \langle y,z_1\rangle = \langle y,z_1\rangle = 0\}$, rescaled to lie in S^{d-3}. If $\langle x,z_1\rangle = \alpha_i$, $\langle x,z_2\rangle = \alpha_j$, $\langle y,z_1\rangle = \alpha_k$, $\langle y,z_2\rangle = \alpha_l$ and $\langle x,y\rangle = \alpha_n$, then the inner product of the orthogonal projections of x,y to $\langle z_1,z_2\rangle^\perp$ rescaled to lie in S^{d-3} is

$$\alpha_{i,j,k,l}^{m,n} := \frac{(\alpha_n - \alpha_i\alpha_k)(1-\alpha_m^2) - (\alpha_j - \alpha_i\alpha_m)(\alpha_l - \alpha_k\alpha_m)}{\sqrt{(1-\alpha_i^2-\alpha_j^2-\alpha_m^2+2\alpha_i\alpha_j\alpha_m)(1-\alpha_k^2-\alpha_l^2-\alpha_m^2+2\alpha_k\alpha_l\alpha_m)}}.$$

We denote $p_{\alpha,\beta}^{(i,j,m)}(x,y) = |\{z \in X_{i,j}^m \mid \langle x,z\rangle = \alpha, \langle y,z\rangle = \beta\}|$.

Lemma 3.3. *Let $X \subset S^{d-1}$ be a finite set and $A'(X) = \{\alpha_1,\ldots,\alpha_s\}$. Assume that $(X, \{R_k\}_{k=0}^s)$ is a symmetric association scheme, where $R_k = \{(x,y) \in X \times X \mid \langle x,y\rangle = \alpha_k\}$ $(0 \leq k \leq s)$ and $\alpha_0 = 1$. Then $|\{(i,j) \in \{1,\ldots,s\}^2 \mid X_{i,j}^m(z_1,z_2) \neq \emptyset\}| = |\{\langle i,j\rangle \in \{1,\ldots,s\}^2 \mid p_{i,j}^m \neq 0\}|$ for $\langle z_1,z_2\rangle = \alpha_m$.*

Proof. Immediate from definition. □

The following theorem is used to prove Corollary 3.6.

Theorem 3.4 ([10, Theorem 2.6]). *Let $X_i \subset S^{d-1}$ be a spherical t_i-design for $i \in \{1,\dots,n\}$. Assume that $X_i \cap X_j = \emptyset$ or $X_i = X_j$, and $X_i \cap (-X_j) = \emptyset$ or $X_i = -X_j$ for $i,j \in \{1,\dots,n\}$. Let $s_{i,j} = |A(X_i,X_j)|$, $s^*_{i,j} = |A'(X_i,X_j)|$ and $A(X_i,X_j) = \{\alpha^1_{i,j},\dots,\alpha^{s_{i,j}}_{i,j}\}$, $\alpha^0_{i,j} = 1$, when $-1 \in A'(X_i,X_j)$, we define $\alpha^{s^*_{i,j}}_{i,j} = -1$. We define $R^k_{i,j} = \{(x,y) \in X_i \times X_j \mid \langle x,y\rangle = \alpha^k_{i,j}\}$. If one of the following holds depending on the choice of $i,j,k \in \{1,\dots,n\}$:*

(1) $s_{i,j} + s_{j,k} - 2 \le t_j$,

(2) $s_{i,j}+s_{j,k}-3 = t_j$ *and for any* $\gamma \in A(X_i,X_k)$ *there exist* $\alpha \in A(X_i,X_j), \beta \in A(X_j,X_k)$ *such that the number* $p^j_{\alpha,\beta}(x,y)$ *is independent of the choice of* $x \in X_i, y \in X_k$ *with* $\gamma = \langle x,y\rangle$,

(3) $s_{i,j} + s_{j,k} - 4 = t_j$ *and for any* $\gamma \in A(X_i,X_k)$ *there exist* $\alpha,\alpha' \in A(X_i,X_j), \beta,\beta' \in A(X_j,X_k)$ *such that* $\alpha \ne \alpha'$, $\beta \ne \beta'$ *and the numbers* $p^j_{\alpha,\beta}(x,y)$, $p^j_{\alpha,\beta'}(x,y)$ *and* $p^j_{\alpha',\beta}(x,y)$ *are independent of the choice of* $x \in X_i, y \in X_k$ *with* $\gamma = \langle x,y\rangle$,

then $(\coprod_{i=1}^n X_i, \{R^k_{i,j} \mid 1 \le i,j \le n, 1 - \delta_{X_i,X_j} \le k \le s^*_{i,j}\})$ *is a coherent configuration. The parameters of this coherent configuration are determined by* $A(X_i,X_j)$, $|X_i|$, t_i, δ_{X_i,X_j}, $\delta_{X_i,-X_j}$, *and when* $s_{i,j} + s_{j,k} - 3 = t_j$ *(resp.* $s_{i,j} + s_{j,k} - 4 = t_j$*), the numbers* $p^j_{\alpha,\beta}(x,y)$ *(resp.* $p^j_{\alpha,\beta}(x,y)$, $p^j_{\alpha',\beta}(x,y)$, $p^j_{\alpha,\beta'}(x,y)$*) which are assumed be independent of* (x,y) *with* $\langle x,y\rangle = \gamma$.

The following lemma shows the antipodal double cover of coeherent configurations are also coherent configurations.

Lemma 3.5. *Let $X^+_i, X^-_i \subset S^{d-1}$ be a finite subset such that $X^+_i = -X^-_i$ for $i \in \{1,\dots,n\}$. If $\{X^+_i\}_{i=1}^n$ carries a coherent configuration, then $\{X^+_i, X^-_i\}_{i=1}^n$ carries also a coherent configuration.*

Proof. We define $X^\varepsilon_i(x,\alpha) = \{w \in X^\varepsilon_i \mid \langle x,w\rangle = \alpha\}$, and $X^\varepsilon_i(x,\alpha;y,\beta) = X^\varepsilon_i(x,\alpha) \cap X^\varepsilon_i(y,\beta)$ for $x \in S^{d-1}$, $\varepsilon = +$ or $-$. Then the following equalities hold:

(1) $X^+_i(x,-\alpha) = X^+_i(-x,\alpha)$,

(2) $X^+_i(x,\alpha) = -X^-_i(x,-\alpha)$.

By (1), $X^+_i(x,\alpha;y,\beta) = X^+_i(-x,-\alpha;y,\beta) = X^+_i(x,\alpha;-y,-\beta)$ holds. By (2), $X^+_i(x,\alpha;y,\beta) = -X^-_i(x,-\alpha;y,-\beta)$ holds. Therefore $|X^+_i(x,\alpha;y,\beta)| = |X^+_i(-x,-\alpha;y,\beta)| = |X^+_i(x,\alpha;-y,-\beta)| = |X^-_i(x,-\alpha;y,-\beta)|$ holds. This implies that intersection numbers on $\{X^+_i, X^-_i\}_{i=1}^n$ is determined by the coherent configuration $\{X^+_i\}_{i=1}^n$. □

The following corollary gives the sufficient condition of the quadruple regularity of triply regular association schemes obtained from an antipodal finite subset of sphere. Its proof follows from the same argument of [10, Corollary 2.9].

Corollary 3.6. *Let $X \subset S^{d-1}$ be an antipodal finite subset and $A'(X) = \{\alpha_1,\dots,\alpha_s\}$ with $\alpha_1 > \cdots > \alpha_s = -1$. Assume that $(X,\{R_k\}_{k=0}^s)$ is a triply regular symmetric association scheme, where $R_k = \{(x,y) \in X \times X \mid \langle x,y\rangle = \alpha_k\}$ $(0 \le k \le s)$ and $\alpha_0 = 1$. Then for $1 \le i,j,k,l,m \le s-1$ such that $p^m_{i,j} \ne 0$ and $p^m_{k,l} \ne 0$*

(1) $A(X^m_{i,j}(z_1,z_2), X^m_{k,l}(z_1,z_2)) = \{\alpha^{m,n}_{i,j,k,l} \mid 0 \le n \le s, p^{l,k,n}_{i,j,m} \ne 0, \alpha^{m,n}_{i,j,k,l} \ne \pm 1\}$.

(2) $X^m_{i,j}(z_1,z_2) = X^m_{k,l}(z_1,z_2)$ *or* $X^m_{i,j}(z_1,z_2) \cap X^m_{k,l}(z_1,z_2) = \emptyset$, *and* $X^m_{i,j}(z_1,z_2) = -X^m_{k,l}(z_1,z_2)$ *or* $X^m_{i,j}(z_1,z_2) \cap -X^m_{k,l}(z_1,z_2) = \emptyset$ *for any* $z_1, z_2 \in X$ *with* $\langle z_1,z_2\rangle = \alpha_m$ *And* $\delta_{X^m_{i,j}(z_1,z_2),X^m_{k,l}(z_1,z_2)}$, $\delta_{X^m_{i,j}(z_1,z_2),-X^m_{k,l}(z_1,z_2)}$ *are independent of* $z_1, z_2 \in X$ *with* $\alpha_m = \langle z_1,z_2\rangle$.

(3) $X^m_{i,j}(z_1,z_2)$ *has the same strength for all* $z_1, z_2 \in X$ *with* $\alpha_m = \langle z_1,z_2\rangle$.

Moreover if the assumption (1),(2) *or* (3) *of Theorem 3.4 is satisfied for* $\{X^m_{i,j}(z_1,z_2) \mid 1 \le i \le \frac{s-1}{2}, 1 \le j \le s-1, p^m_{i,j} \neq 0\} \cup \{X^m_{i,j}(z_1,z_2) \mid \frac{s-1}{2} \le i \le \frac{s+1}{2}, 1 \le j \le \frac{s+1}{2}, p^m_{i,j} \neq 0\}$ *with* $m \neq 0$ *or* s, *and when* $((i,j),(k,l),(m,n))$ *satisfies* (2) *(resp.* (3)*) the numbers* $p^{(k,l,m)}_{\alpha,\beta}(x,y)$ *(resp.* $p^{(k,l,m)}_{\alpha,\beta}(x,y)$, $p^{(k,l,m)}_{\alpha,\beta'}(x,y)$, $p^{(k,l,m)}_{\alpha',\beta}(x,y)$*) which are assumed to be independent of* (x,y) *with* $\gamma = \langle x,y\rangle$ *are independent of the choice of* z_1, z_2 *with* $\alpha_m = \langle z_1,z_2\rangle$, *then* $(X,\{R_k\}^s_{k=0})$ *is a quadruply regular association scheme.*

Proof. (1), (2), (3) follow from arguments similar to that in [10, Corollary 2.9].

Fix $z_1, z_2 \in X$ with $\alpha_m = \langle z_1,z_2\rangle$.

If $m = 0$ or s, then $\bigcup^s_{i,j=1} R_i(z_1) \cap R_j(z_2) = \bigcup^s_{i=1} R_i(z_1)$. The triple regularity of $(X,\{R_k\}^s_{k=0})$ is equivalent that $\bigcup^s_{i,j=1} R_i(z_1) \cap R_j(z_2)$ to be a coherent configuration whose parameters are independent of z_1, z_2 with $\langle z_1,z_2\rangle = \pm 1$.

If $1 \le m \le s-1$, then $X^m_{i,s}(z_1,z_2) \neq \emptyset$ if and only if $X^m_{s,i}(z_1,z_2) \neq \emptyset$ if and only if $i = s-m$ hold, and then $X^m_{s,m-s}(z_1,z_2) = \{-z_1\}$, $X^m_{s-m,s}(z_1,z_2) = \{-z_2\}$ hold. Moreover $X^m_{i,j} = -X^m_{s-i,s-j}$ hold for any $1 \le i,j \le s-1$. By Lemma 3.5, it is sufficient to show that $\{X^m_{i,j}(z_1,z_2) \mid 1 \le i \le \frac{s-1}{2}, 1 \le j \le s-1, p^m_{i,j} \neq 0\} \cup \{X^m_{i,j}(z_1,z_2) \mid \frac{s-1}{2} \le i \le \frac{s+1}{2}, 1 \le j \le \frac{s+1}{2}, p^m_{i,j} \neq 0\}$ carries a coherent configuration whose parameters are independent of z_1, z_2 with $\alpha_m = \langle z_1,z_2\rangle$, and the rest of the proof follows from the similar argument of that in [10, Corollary 2.9]. □

4 Real mutually unbiased bases

Definition 4.1. Let $M = \{M_i\}^f_{i=1}$ be a collection of orthonormal bases of $\mathbb{R}^d$. M is called real mutually unbiased bases (MUB) if any two vectors x and y from different bases satisfy $\langle x,y\rangle = \pm 1/\sqrt{d}$.

Let $M = \{M_i\}^f_{i=1}$ be a MUB, and put $X = M \cup (-M)$. The angle set of X is

$$A'(X) = \{\frac{1}{\sqrt{d}}, 0, -\frac{1}{\sqrt{d}}, -1\}.$$

We set

$$\alpha_0 = 1, \quad \alpha_1 = \frac{1}{\sqrt{d}}, \quad \alpha_2 = 0, \quad \alpha_3 = -\frac{1}{\sqrt{d}}, \quad \alpha_4 = -1,$$

and we define $R_k = \{(x,y) \in X \times X \mid \langle x,y\rangle = \alpha_k\}$. Then $(X,\{R_k\}^4_{k=0})$ is a Q-polynomial association scheme which is both Q-antipodal and Q-bipartite in [6, Theorem 4.1].

Conversely let $(X,\{R_k\}^4_{k=0})$ be a Q-polynomial association scheme which is both Q-antipodal and Q-bipartite, then the image of the embedding into first eigenspace by primitive idempotent E_1 is $M \cup (-M)$, where M is mutually unbiased bases in [6, Theorem 4.2].

Applying [2, Theorem 4.8] to the above scheme for $i = j = 1$ using the paramerters in [6, Appendix], we obtain the inequality $f \le \frac{d}{2} + 1$. We call M a maximal MUB if this upper bound is attained.

Lemma 4.2. *$(X, \{R_i\}_{i=0}^4)$ is a Q-polynomial association scheme which is both Q-antipodal and Q-bipartite with f Q-antipodal classes of size $2d$. Assume $f \geq 3$. Then for $z \in X$ and $j = 1, 3$ $(R_j(z), \{R_i \cap (R_j(z) \times R_j(z))\}_{i=0}^3)$ is a Q-polynomial association scheme which is Q-antipodal with $(f-1)$ Q-antipodal classes of size d and $a_1^* = \frac{d}{f-1} - 2$.*

Proof. It was shown in [10, Secton 5] that $(X, \{R_i\}_{i=0}^4)$ is triply regular, in particular $R_j(z)$ carries an association scheme for any $z \in X$, $j \in \{1, 3\}$. Let $X_j(z)$ be a derived design in S^{d-2} of X with respect to z, α_j. We verify the intersection numbers of $X_j(z)$. For $x, y \in X_j(z)$, we set

$$p_{\alpha,\beta}(x, y) = |\{w \in X_j(z) \mid \langle x, w\rangle = \alpha, \langle w, y\rangle = \beta\}|.$$

The angle set of $X_j(z)$ is

$$A(X_j(z)) = \left\{\alpha_1 := \frac{\sqrt{d}-1}{d-1}, \alpha_2 := \frac{-1}{d-1}, \alpha_3 := \frac{-\sqrt{d}-1}{d-1}\right\},$$

$X_j(z)$ is a $s := 3$-distance set. $X_j(z)$ is a $t := 2$-design in S^{d-2}, therefore $X_j(z)$ satisfies $t = 2s-4$. And for any $\gamma = \langle x, y\rangle$, the intersection numbers $p_{\alpha_2,\alpha_2}(x, y)$, $p_{\alpha_2,\alpha_1}(x, y)$, $p_{\alpha_1,\alpha_2}(x, y)$ are independent of the choice of $x, y \in X_j(z)$ with $\gamma = \langle x, y\rangle$ as follows:

$$p_{\alpha_2,\alpha_2}(x, y) = \begin{cases} 0 & \text{if } \langle x, y\rangle = \alpha_1, \\ d-2 & \text{if } \langle x, y\rangle = \alpha_2, \\ 0 & \text{if } \langle x, y\rangle = \alpha_3, \end{cases} \quad p_{\alpha_2,\alpha_1}(x, y) = p_{\alpha_1,\alpha_2}(x, y) = \begin{cases} \frac{d+\sqrt{d}}{2} - 1 & \text{if } \langle x, y\rangle = \alpha_1, \\ 0 & \text{if } \langle x, y\rangle = \alpha_2, \\ \frac{d+\sqrt{d}}{2} & \text{if } \langle x, y\rangle = \alpha_3. \end{cases}$$

For $0 \leq \lambda \leq 2$, $0 \leq \mu \leq 2$ and $(\lambda, \mu) \neq (1, 2), (2, 1), (2, 2)$, we obtain a system of 6 linear equations

$$\sum_{\substack{1 \leq l \leq 3 \\ 1 \leq m \leq 3 \\ (l,m) \neq (2,2),(2,1),(1,2)}} \alpha_l^\lambda \beta_m^\mu p_{\alpha_l,\alpha_m}(x, y) = |X_j(z)| F_{\lambda,\mu}(\langle x, y\rangle) - \langle x, y\rangle^\lambda - \langle x, y\rangle^\mu - \alpha_2^\lambda \alpha_2^\mu p^j_{\alpha_2,\alpha_2}(x, y) - \alpha_2^\lambda \alpha_1^\mu p^j_{\alpha_2,\alpha_1}(x, y) - \alpha_1^\lambda \alpha_2^\mu p^j_{\alpha_1,\alpha_2}(x, y),$$

where $F_{\lambda,\mu}(t)$ is defined in [5, Section 7]. $\{p_{\alpha_i,\alpha_j}(x, y) \mid 1 \leq i, j \leq 3, (i, j) \neq (2, 2), (2, 1), (1, 2)\}$ is uniquely determined by Theorem 3.4. The intersection matrices B_i and the second eigenmatrix Q are as follows:

$$B_1 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ \frac{(f-2)(d+\sqrt{d})}{2} & \frac{(f-3)(d+3\sqrt{d})}{4} & \frac{d+2\sqrt{d}}{4} & \frac{d+\sqrt{d}}{4} \\ 0 & \frac{d+\sqrt{d}-2}{2} & 0 & \frac{d+\sqrt{d}}{2} \\ 0 & \frac{(f-3)(d-\sqrt{d})}{4} & \frac{(f-2)d}{4} & \frac{(f-3)(d+\sqrt{d})}{4} \end{pmatrix},$$

$$B_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & \frac{d+\sqrt{d}-2}{2} & 0 & \frac{d+\sqrt{d}}{2} \\ d-1 & 0 & d-2 & 0 \\ 0 & \frac{d-\sqrt{d}}{2} & 0 & \frac{d-\sqrt{d}-2}{2} \end{pmatrix},$$

$$B_3 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & \frac{(f-3)(d-\sqrt{d})}{4} & \frac{(f-2)d}{4} & \frac{(f-3)(d+\sqrt{d})}{4} \\ 0 & \frac{d-\sqrt{d}}{2} & 0 & \frac{d-\sqrt{d}-2}{2} \\ \frac{(f-2)(d-\sqrt{d})}{2} & \frac{(f-3)(d-\sqrt{d})}{4} & \frac{(f-2)(d-2\sqrt{d})}{4} & \frac{(f-3)(d-3\sqrt{d})}{4} \end{pmatrix},$$

$$Q = \begin{pmatrix} 1 & d-1 & (f-1)(d-1) & f-1 \\ 1 & \sqrt{d}-1 & -\sqrt{d}+1 & -1 \\ 1 & -1 & -f+1 & f-1 \\ 1 & -\sqrt{d}-1 & \sqrt{d}+1 & -1 \end{pmatrix},$$

and hence the Krein matrix B_1^* is given as follows:

$$B_1^* = \begin{pmatrix} 0 & 1 & 0 & 0 \\ d-1 & \frac{d}{f-1}-2 & \frac{d}{f-1} & 0 \\ 0 & \frac{(f-2)d}{f-1} & \frac{(f-2)d}{f-1}-2 & d-1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Therefore $X_1(z)$ is a Q-polynomial association scheme which is Q-antipodal. □

The following Theorem shows that maximal MUB carries a quadruply regular association scheme and the quadruple regularity of an association scheme obtained from MUB is characterized by its parameter.

Theorem 4.3. *$(X, \{R_i\}_{i=0}^4)$ is a Q-polynomial association scheme which is both Q-antipodal and Q-bipartite. Then the following conditions are equivalent:*

(1) *$(X, \{R_i\}_{i=0}^4)$ is quadruply regular,*

(2) $f = \frac{d}{2} + 1$.

Proof. (1)⇒(2):Assume $(X, \{R_i\}_{i=0}^4)$ is quadruply regular. Then $X_1(z)$ is triply regular for any $z \in X$. By Lemma 4.2 and Theorem 2.2, $\frac{d}{f-1} - 2 = 0$. Therefore $f = \frac{d}{2} + 1$ holds.

(2)⇒(1): By [10, Corollary 5.3] it is sufficient to show that the assumption of Corollary 3.6 is satisfied.

(i) When $\langle z_1, z_2 \rangle = \alpha_2$, $\{(i,j) \mid 1 \le i \le \frac{s-1}{2}, 1 \le j \le s-1, p_{i,j}^m \neq 0\} \cup \{(i,j) \mid \frac{s-1}{2} \le i \le \frac{s+1}{2}, 1 \le j \le \frac{s+1}{2}, p_{i,j}^m \neq 0\}$ is $\{(1,1),(1,3),(2,2)\}$. $X_{i,j}^2 = X_{i,j}^2(z_1, z_2)$ is a 3-design in S^{d-3} for $(i,j) \in \{(1,1),(1,3),(2,2)\}$. Indeed $X_{2,2}^2$ is a cross polytope in S^{d-3}. $|X_{1,1}^2| = p_{1,1}^2 = \frac{d^2}{4}$, $|X_{1,3}^2| = p_{1,3}^2 = \frac{d^2}{4}$ where $p_{1,1}^2$ and $p_{1,3}^2$ are the intersectioin numbers of X in [1, 6 Appendix]. And the angle sets $A(X_{1,1}^2) = A(X_{1,3}^2) = \{\frac{\sqrt{d}-2}{d-2}, \frac{-2}{d-2}, \frac{-\sqrt{d}-2}{d-2}\}$ hold, so Gegenbauer polynomial expansion of their annihilator polynomial $F(t) := \prod_{\alpha \in A'(X_{i,j}^2)} \frac{t-\alpha}{1-\alpha}$ is

$$F(t) = \frac{4}{d^2}Q_0(t) + \frac{2(d^2+6)(d-2)}{d^3(d-1)}Q_1(t) + \frac{(d-2)^3(d+3)}{d^3(d-1)}Q_2(t) + \frac{6(d-2)(d-3)}{d^2(d-1)},$$

therefore $X_{1,1}^2$ and $X_{1,3}^2$ are 3-designs in S^{d-3} by [5, Theorem 6.5]. We renumber as follows:

$$X_1 = X_{2,2}^2, \quad X_2 = X_{1,1}^2, \quad X_3 = X_{1,3}^2.$$

We define $s_{i,j} = |A(X_i, X_j)|$. Then the matrix $(s_{i,j})$ is

$$\begin{pmatrix} 1 & 2 & 2 \\ 2 & 3 & 3 \\ 2 & 3 & 3 \end{pmatrix}.$$

If $s_{i,j} + s_{j,k} - 2 \le 3$, that is, when one of the i, j, k at least is equal to 1, then the assumption (1) of Theorem 3.4 holds.

If $s_{i,j} + s_{j,k} - 3 = 3$, that is, when

$$(i,j,k) \in \{(l,m,n) \mid 2 \le l, m, n \le 3\}, \tag{4.1}$$

And $X_2 \cup X_3$ carries a subconstituent association scheme $R_1(z_1)$ of X whose parameters are independent of z_1 by Lemma 4.2, therefore those for $(2,3,3)$ (respectively $(2,3,2)$, $(3,2,3)$)

are determined by those for $(2,2,3)$ (respectively $(2,2,2)$, $(3,3,3)$). The intersection numbers $\{p^j_{\alpha,\beta} \mid \alpha = \alpha^2_{i,j} \text{ or } \beta = \alpha^2_{j,k}\}$ for $x \in X_i$, $y \in X_k$ and $(i,j,k) \in \{(2,2,2),(3,3,3),(2,2,3)\}$ are given in Table 1. These numbers are independent of $z_1, z_2 \in X$ with $\langle z_1, z_2\rangle = \alpha_2$. Hence the assumption of (2) of Theorem 3.4 holds for i,j,k (i,j,k) in (4.1).

(ii) When $\langle z_1, z_2\rangle = \alpha_1$, $\{X^m_{i,j}(z_1,z_2) \mid 1 \le i \le \frac{s-1}{2}, 1 \le j \le s-1, p^m_{i,j} \ne 0\} \cup \{X^m_{i,j}(z_1,z_2) \mid \frac{s-1}{2} \le i \le \frac{s+1}{2}, 1 \le j \le \frac{s+1}{2}, p^m_{i,j} \ne 0\}$ is $\{X^1_{1,1}, X^1_{1,2}, X^1_{1,3}, X^1_{2,1}\}$. $X^1_{i,j} = X^1_{i,j}(z_1,z_2)$ is a 2-design in S^{d-3} for $(i,j) \in \{(1,1),(1,2),(1,3),(2,1)\}$. Indeed $X^1_{1,2}$, $X^1_{2,1}$ are regular simplexes in S^{d-3}. And $X^1_{1,1}$ and $X^1_{1,3}$ are subconstituents of $X_1(z_1)$ with respect to $z_2 \in X_1(z_1)$. $X_1(z_1)$ is a Q-polynomial association scheme by Theorem 4.2 with $a^*_1 = 0$, so Lemma 4.2 in [10] implies that $X^1_{1,1}$ and $X^1_{1,3}$ are 2-designs in S^{d-3}. We renumber as follows:

$$X_1 = X^1_{2,1}, \quad X_2 = X^1_{1,2}, \quad X_3 = X^1_{1,1}, \quad X_4 = X^1_{1,3}.$$

We define $s_{i,j} = |A(X_i, X_j)|$. Then the matrix $(s_{i,j})$ is

$$\begin{pmatrix} 1 & 2 & 2 & 2 \\ 2 & 1 & 2 & 2 \\ 2 & 2 & 3 & 3 \\ 2 & 2 & 3 & 3 \end{pmatrix}.$$

If $s_{i,j} + s_{j,k} - 2 \le 2$, that is, when

$$(i,j,k) \in \{(l,m,n) \mid 1 \le l,m \le 2, 3 \le n \le 4 \text{ or } 3 \le l \le 4, 1 \le m,n \le 2 \text{ or } 1 \le l,m,n \le 2\},$$

then the assumption (1) of Theorem 3.4 holds.

If $s_{i,j} + s_{j,k} - 3 = 2$, that is, when

$$(i,j,k) \in \{(l,m,n) \mid 1 \le l \le 2, 3 \le m,n \le 4 \text{ or } 3 \le l,m \le 4, 1 \le n \le 2\}, \tag{4.2}$$

or if $s_{i,j} + s_{j,k} - 4 = 2$, that is, when

$$(i,j,k) \in \{(l,m,n) \mid 3 \le l,m,n \le 4\}, \tag{4.3}$$

we do not show that the (i,j,k) in (4.2) (respectively (4.3)) satisfy the assumption (2) (respectively (3)) of Theorem 3.4, directly verify that the intersection numbers on X_j for $x \in X_i$, $y \in X_k$ are independent of x, y and of z_1, z_2 by using the triple regularity of subconsitituents of X. $X_2 \cup X_3 \cup X_4$ carries a subconstituent association scheme $R_1(z_1)$ which is obtained from a system of linked symmetric designs with $a^*_1 = 0$, and X_2, X_3, X_4 are the subconstituents of $R_1(z_1)$ with respect to $z_2 \in R_1(z_1)$. $R_1(z_1)$ is triply regular, so $X_2 \cup X_3 \cup X_4$ carries a coherent configuration whose parameters are independent of z_2. The parameters of $X_2 \cup X_3 \cup X_4$ depends on those of $R_1(z_1)$ which is independent of z_1. Therefore the parameters of $X_2 \cup X_3 \cup X_4$ are independent of z_1, z_2 with $\langle z_1, z_2\rangle = \alpha_1$. Interchanging z_1 with z_2 and using $X_4 = -X^1_{3,1}$, we can show $X_1 \cup X_3 \cup X_4$ carries a coherent configuration whose parameters are independent of z_1, z_2 with $\langle z_1, z_2\rangle = \alpha_1$.

(iii) The case $\langle z_1, z_2\rangle = \alpha_3$ is similar to the case $\langle z_1, z_2\rangle = \alpha_1$.

By Corollary 3.6, we obtain the desired result. □

Remark 4.4. Let M be a maximal MUB and $X = M \cup (-M)$. It was already shown in [1, Theorem 5] that $\{x \in X \mid \langle x, z_1\rangle = \langle x, z_2\rangle = \frac{1}{\sqrt{d}}\}$ for $z_1, z_2 \in X$ such that $\langle z_1, z_2\rangle = 0$ carries an association scheme.

Table 1: the values of $p^j_{\alpha,\beta}(x,y)$, where $x \in X_i(z)$, $y \in X_k(z)$

(i,j,k)	(α,β)	$p^j_{\alpha,\beta}(x,y)$	(i,j,k)	(α,β)	$p^j_{\alpha,\beta}(x,y)$
$(2,2,2)$ $(3,3,3)$	$(\alpha^2_{i,j},\alpha^2_{j,k})$	$\begin{cases} 0 & \langle x,y\rangle = \alpha^1_{i,k} \\ \frac{d}{2}-1 & \langle x,y\rangle = \alpha^2_{i,k} \\ 0 & \langle x,y\rangle = \alpha^3_{i,k} \end{cases}$	$(2,2,3)$	$(\alpha^2_{2,2},\alpha^2_{2,3})$	$\begin{cases} 0 & \langle x,y\rangle = \alpha^1_{2,3} \\ \frac{d}{2}-1 & \langle x,y\rangle = \alpha^2_{2,3} \\ 0 & \langle x,y\rangle = \alpha^3_{2,3} \end{cases}$
	$(\alpha^2_{i,j},\alpha^1_{j,k})$ $(\alpha^1_{i,j},\alpha^2_{j,k})$	$\begin{cases} \frac{d+2\sqrt{d}}{4}-1 & \langle x,y\rangle = \alpha^1_{i,k} \\ 0 & \langle x,y\rangle = \alpha^2_{i,k} \\ \frac{d+2\sqrt{d}}{4} & \langle x,y\rangle = \alpha^3_{i,k} \end{cases}$		$(\alpha^2_{2,2},\alpha^1_{2,3})$	$\begin{cases} \frac{d}{4}-1 & \langle x,y\rangle = \alpha^1_{2,3} \\ 0 & \langle x,y\rangle = \alpha^2_{2,3} \\ \frac{d}{4} & \langle x,y\rangle = \alpha^3_{2,3} \end{cases}$
	$(\alpha^2_{i,j},\alpha^3_{j,k})$ $(\alpha^3_{i,j},\alpha^2_{j,k})$	$\begin{cases} \frac{d-2\sqrt{d}}{4} & \langle x,y\rangle = \alpha^1_{i,k} \\ 0 & \langle x,y\rangle = \alpha^2_{i,k} \\ \frac{d-2\sqrt{d}}{4}-1 & \langle x,y\rangle = \alpha^3_{i,k} \end{cases}$		$(\alpha^2_{2,2},\alpha^3_{2,3})$	$\begin{cases} \frac{d}{4}-1 & \langle x,y\rangle = \alpha^1_{2,3} \\ 0 & \langle x,y\rangle = \alpha^2_{2,3} \\ \frac{d}{4} & \langle x,y\rangle = \alpha^3_{2,3} \end{cases}$
				$(\alpha^1_{2,2},\alpha^2_{2,3})$	$\begin{cases} \frac{d+2\sqrt{d}}{4} & \langle x,y\rangle = \alpha^1_{2,3} \\ 0 & \langle x,y\rangle = \alpha^2_{2,3} \\ \frac{d+2\sqrt{d}}{4} & \langle x,y\rangle = \alpha^3_{2,3} \end{cases}$
				$(\alpha^3_{2,2},\alpha^2_{2,3})$	$\begin{cases} \frac{d-2\sqrt{d}}{4} & \langle x,y\rangle = \alpha^1_{2,3} \\ 0 & \langle x,y\rangle = \alpha^2_{2,3} \\ \frac{d-2\sqrt{d}}{4} & \langle x,y\rangle = \alpha^3_{2,3} \end{cases}$

References

[1] K. Abdukhalikov, E. Bannai, S. Suda, Association schemes related to universally optimal configurations, Kerdock codes and extremal Euclidean line-sets, J. Combin. Theory Ser. A 116 (2009), no.2, 434–448.

[2] E. Bannai, T. Ito, Algebraic Combinatorics I: Association Schemes, Benjamin/Cummings, Menro Park, CA, 1984.

[3] P. J. Cameron, On groups with several doubly transitive permutation representation, Math. Z. 128, (1972), 1–14.

[4] E. van. Dam, Three-class association schemes, J. Algebraic. Combin. 10(1) (1999), 69–107.

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

[6] N. LeCompte, W. J. Martin, W. Owens, On the equivalence between real mutually unbiased bases and a certain class of association schemes, preprint.

[7] W. J. Martin, M. Muzychuk, J. Williford, Imprimitive cometric association schemes: constructions and analysis, J. Algebraic Combin. 25 (2007), 399–415.

[8] R. Mathon, The systems of linked 2-(16,6,2) designs, Ars Comb, 11 (1981), 131–148.

[9] R. Noda, On homogeneous systems of linked symmetric designs, Math. Z. 138 (1974) 15–20.

[10] S. Suda, Coherent configurations and triply regular association schemes obtained from spherical designs, arXiv:math/0903.5169v1[math.CO].

虚二次体の整数環から作られる球面デザインの非存在について

三枝崎 剛 Tsuyoshi Miezaki *

この原稿は，2009年6月の第26回代数的組合せ論シンポジウム（遊学館（山形））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 “Nonexistence of spherical designs obtained from integer rings of imaginary quadratic fields (joint work with Eiichi Bannai) ” であり，坂内，三枝崎の著者によるこのタイトルのプレプリント（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 [5] 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:

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

が，全ての次数 t 以下の多項式 $f(x) = f(x_1, x_2, \cdots, x_n)$ 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，$|S^{n-1}|$ で球 S^{n-1} 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．

(1) と同値な条件は，幾つも知られていますが，特に以下の議論で有効な次の条件を紹介します:

*Research Fellow of the Japan Society for the Promotion of Science and Department of Mathematics, Hokkaido University, Hokkaido 060–0810, Japan, e-mail: miezaki@math.sci.hokudai.ac.jp

X が球面 t-デザイン

$\Leftrightarrow$

$$\sum_{x\in X} P(x) = 0$$

が全ての $P \in \mathrm{Harm}_j(\mathbb{R}^n)$, $1 \le j \le t$ に対して成立する. ($\mathrm{Harm}_j(\mathbb{R}^n)$ で n 変数 j 次斉次多項式を表します.) 更に X が対極的, 即ち $-X = X$ の時は, j が奇数だと上の条件は自動的に満たされますから, 偶数次の斉次調和多項式のみ調べれば良い事になります. 一般に球面デザインの具体的構成は難しい問題ですが, 格子を用いた体系的な構成法が知られています. 以下ではその構成法を紹介します.

$\mathbb{R}^n$ の部分集合 Λ が格子とは, $\mathbb{R}^n$ の基底 $\{e_1, \cdots, e_n\}$ が存在し, $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$ と書ける集合です. 双対格子 $\Lambda^\sharp$ とは以下で定義されます:

$$\Lambda^\sharp := \{y \in \mathbb{R}^n \mid \langle y|x\rangle \in \mathbb{Z},\ \forall x \in \Lambda\}.$$

格子が整数格子とは $\langle x|y\rangle \in \mathbb{Z}$ for all $x, y \in \Lambda$, 整数格子が偶格子とは $\langle x|x\rangle \in 2\mathbb{Z}$ for all $x \in \Lambda$, 奇格子とは偶格子でない整数格子と定義されます. 整数格子が自己双対とは $\Lambda^\sharp = \Lambda$ が成立する事です. 更に正の実数 $m > 0$ に対して, 格子 Λ のノルム m の殻 $(\Lambda)_m$ を以下で定義します:

$$\Lambda_m := \{x \in \Lambda \mid \langle x|x\rangle = m\} = \Lambda \cap S^{n-1}(m).$$

ここで, $\mathbb{H} := \{z \in \mathbb{C} \mid \Im z > 0\}$ を上半平面, P を多項式として, 格子の重さ付きテータ級数を定義します:

$$\Theta_{\Lambda,P}(z) := \sum_{x\in\Lambda} P(x) e^{i\pi z\langle x|x\rangle}$$

テータ級数は, 次の補題の様に, 格子から作られる t-デザインの研究に有用である事が知られています. ([9], [10], [3], [8], [4], [1] を見よ.)

補題 1.1 (cf. [9], [10], [8], Lemma 5). Λ を $\mathbb{R}^n$ の整数格子とする. $m > 0$ に対して, 空でない殻 Λ_m が t-デザイン

$\Leftrightarrow$

$$a_m^{(P)} = 0$$

が全ての $P \in \mathrm{Harm}_{2j}(\mathbb{R}^n)$, $1 \le 2j \le t$ に対して成立する, ここで $a_m^{(P)}$ は次の様に定義されます :

$$\Theta_{\Lambda,P}(z) = \sum_{m\ge 0} a_m^{(P)} q^m.$$

重さ $P \in \mathrm{Harm}_j(\mathbb{R}^n)$ の $\Lambda \subset \mathbb{R}^n$ のテータ級数は，ある群 $\Gamma \subset SL_2(\mathbb{R})$ のウェイト $n/2+j$ のモジュラ形式になる事が知られています．特に $\deg(P) \geq 1$ の時はカスプ形式になります．(詳しくは，[2] を見て下さい.) 以上を用いて，E_8 格子を例に取り，t-デザインを具体的に構成してみます．

Λ を E_8 格子とします．Λ の重さ付きテータ級数は，$SL_2(\mathbb{Z})$ に関するモジュラ形式で，空間 $\mathbb{C}[E_4, \Delta]$ に入っている事が知られています．ここで，$E_4(q) = 1 + 240\sum_{m=1}^{\infty} \sigma_3(m)q^{2m}$, $\Delta_{24}(q) = (q^{1/12}\prod_{m\geq 1}(1-q^{2m}))^{24} = \sum_{m\geq 1}\tau(m)q^m$．さて，次数 $j = 2, 4, 6$ の多項式で重さ付けたテータ級数は，ウェイト $6, 8, 10$ のモジュラ形式になります．しかしよく知られている様に $SL_2(\mathbb{Z})$ のウェイト $6, 8, 10$ のモジュラ形式は，0 になります．($\dim S_k(SL_2(\mathbb{Z})) = 0$ による.) つまり $\Theta_{\Lambda,P}(z) = 0$ がわかり，Lemma 1.1 から，E_8 格子の全ての殻は 7-デザインになる事がわかるという仕組みです．

ここで次の疑問が生まれます:

E_8 格子の殻には，8-デザインとなるものはないか？

これに関して以下が知られています:

命題 1.1 (cf. [8]).

1. $\tau(m) = 0$.
2. $(E_8)_{2m}$ が 8-*design*.

そして非常に面白い事に，$\tau(m)$ が 0 になるか否かは，古くから Lehmer 予想として知られているのです．Lehmer 予想自身は，難しくて手が出ないのが現状ですが，E_8 格子の代りに，もっと簡単な格子を考え，Lehmer 型の問題を考えようというのが，研究の始まりです．以下では，セクション 2 で，格子 $\mathbb{Z}^2$, A_2，セクション 3 で類数 1, 2 の整数環のイデアル類の格子に対する，Lehmer 型の問題を考えます．

2 格子 $\mathbb{Z}$, A_2

このセクションでは，格子 $\mathbb{Z}$, A_2 を取り上げ，そのデザインを調べます．まず，$\mathbb{Z}$ の任意の殻が 3-デザイン，A_2 の任意の殻が 5-デザインである事はすぐにわかります [8, 2]．では，それぞれ 4，6-デザインとなる殻はないのでしょうか？この場合も E_8 の時と同じく，格子の重さ付きテータ級

数の係数が0か否かに対応します．更にそのテータ級数は，Hecke eigen form という係数 $a(m)$ に関して次の性質を満たす関数になっています．

$$a(mn) = a(m)a(n) \qquad (m, n \text{ coprime})$$
$$a(p^{\alpha+1}) = a(p)a(p^{\alpha}) - \chi(p)p^{k-1}a(p^{\alpha-1}) \qquad (p \text{ a prime}).$$

一番目の性質から，係数が0か否かは，素数べきだけ考えればよいのですが，更に次がわかります．

命題 2.1 (cf. [2]). もし $a(p^e) = 0$ ならば $e = 1$.

つまり，素数の所のみを考えればよいことになります．そして，例えば格子 $\mathbb{Z}^2$ ならば，ノルムが素数の格子の個数は，次の様にわかっています．

補題 2.1 (cf. [2]). $p =$ 素数とする．もし $p \equiv 1 \pmod 4$ ならば $r_2(p) = 8$. もし $p \equiv 3 \pmod 4$ ならば

$$r_2(p^n) = \begin{cases} 0 & \text{if} \quad n \textit{ is odd}, \\ 4 & \text{if} \quad n \textit{ is even}. \end{cases}$$

以上を用いて，後は初等幾何的な方法で，もしくはテータ級数の係数の合同関係などにより，もし $(\mathbb{Z}^2) \neq \emptyset$ ならば係数 $a(m)$ は0にならない事が証明できます．(詳しくは [2] を見てください.) つまり

定理 2.1 (cf. [2]). 格子 $\mathbb{Z}^2$，A_2 の殻にそれぞれ5，7-デザインは存在しない．

3 類数1，2の虚二次体の整数環のイデアル類の格子

セクション2の内容を九州大学の小池正夫先生にお話したところ，次の様な事を教えていただきました．「格子 $\mathbb{Z}^2$, A_2 の場合の，証明の鍵となった重さ付きテータ級数は，虚二次体の整数環のイデアル類の Hecke character から作られるカスプ形式と見る事が出来る.」よく知られているように，虚二次体の整環のイデアル類には類数個の格子が対応する事が知られています．(表1，2にそれぞれ類数が1，2のときの対応を載せます．) つまり格子 $\mathbb{Z}^2$, A_2 以外にも広いクラスの格子に対して Lehmer 型の問題を証明できるのではないかと考えました．実際セクション2で述べた方法と，ほとんど同じく次が証明できます．

定理 3.1 (cf. [2]). 格子 $\mathbb{Z}^2$, A_2 以外の類数 1, 2 の虚二次体の整数環のイデアル類の格子の殻に，2-デザインは存在しない．

類数 1 では 1 つの格子の重さ付きテータ級数が，類数 2 では 2 つの格子の重さ付きテータ級数の和が，Hecke eigen form になっている事が証明の鍵となっています．(詳しい計算結果は，[6] にあります．)

では，類数 3 以上でうまく行かない最大の理由は，重さ付きテータ級数の和を考えると，Hecke eigen form が作れるのですが，一般に整数係数にならない事です．その結果，素数のみを考えればよいという事が証明できません．しかし計算結果から 2 次元格子のデザインは，次の様になると予想されます:

予想 3.1. $L = 2$ 次元整数格子，対応する 2 次形式を $ax^2 + bxy + cy^2$ とする．

1. $b^2 - 4ac = (Integer)^2 \times -3$ と仮定する．そのとき L の殻は 6-デザインでない．しかし 5-デザインになる殻はある．更に全ての殻が 5-デザインならば $b^2 - 4ac = -3$, つまり格子 A_2 になる．

2. $b^2 - 4ac = (Integer)^2 \times -4$ と仮定する．そのとき L の殻は 4-デザインでない．しかし 3-デザインになる殻はある．更に全ての殻が 3-デザインならば $b^2 - 4ac = -4$, つまり格子 $\mathbb{Z}^2$ になる．

3. 他の場合，L の殻は 2-デザインにならない．

注意 3.1. 上の予想と関係しますが，2 次元整数格子で，6-デザインの殻を持つ格子は知られておらず，ないと予想されますが未解決です．更に 3 次元整数格子では，4-デザイン，一般の次元の整数格子で，12-デザインの殻を持つ格子は知られておらず，同じく未解決です．

最後になりましたが，世話人の皆様，特に講演を薦めてくださりました原田昌晃氏，旅費を援助してくださりました小田文仁氏に感謝いたします．またシンポジウム中，沢山の有意義なコメントを頂きました，青木宏樹氏に感謝いたします．

参考文献

[1] E. Bannai, M. Koike, M. Shinohara, M. Tagami, Spherical designs attached to extremal lattices and the modulo p property of Fourier

表 1: $|\mathrm{Cl}_K| = 1$

$-D$	$-D \pmod 4$	d_K	L_o
-1	3	-2^2	$[1, \sqrt{-1}]$
-2	2	-2^3	$[1, \sqrt{-2}]$
-3	1	-3	$[1, (1+\sqrt{-3})/2]$
-7	1	-7	$[1, (1+\sqrt{-7})/2]$
-11	1	-11	$[1, (1+\sqrt{-11})/2]$
-19	1	-19	$[1, (1+\sqrt{-19})/2]$
-43	1	-43	$[1, (1+\sqrt{-43})/2]$
-67	1	-67	$[1, (1+\sqrt{-67})/2]$
-163	1	-163	$[1, (1+\sqrt{-163})/2]$

coefficients of extremal modular forms, *Mosc. Math. J.* , **6-2** (2006), 225–264.

[2] E. Bannai, T. Miezaki, Toy models for D. H. Lehmer's conjecture, (submitted).

[3] P. de la Harpe and C. Pache, Cubature formulas, geometrical designs, reproducing kernels, and Markov operators, *Infinite groups: geometric, combinatorial and dynamical aspects*, *Progr. Math.*, Birkhäuser, Basel, **248** (2005), 219–267.

[4] P. de la Harpe, C. Pache, B. Venkov, Construction of spherical cubature formulas using lattices, *Algebra i Analiz*, **18-1** (2006), 162–186, ; translation in *St. Petersburg Math. J.* **18-1** (2007), 119–139.

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

[6] T. Miezaki, http://www.math.sci.hokudai.ac.jp/ miezaki/

[7] K. Ono, *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[8] C. Pache, Shells of selfdual lattices viewed as spherical designs, *International Journal of Algebra and Computation* 5 (2005), 1085–1127.

表 2: $|\mathrm{Cl}_K| = 2$

$-D$	$D \pmod 4$	d_K	L_o	L_a
-5	3	$-2^2 \times 5$	$[1, \sqrt{-5}]$	$[2, 1+\sqrt{-5}]$
-6	2	$-2^3 \times 3$	$[1, \sqrt{-6}]$	$[2, \sqrt{-6}]$
-10	2	$-2^3 \times 5$	$[1, \sqrt{-10}]$	$[2, \sqrt{-10}]$
-13	3	$-2^2 \times 13$	$[1, \sqrt{-13}]$	$[2, 1+\sqrt{-13}]$
-15	1	-3×5	$[1, (1+\sqrt{-15})/2]$	$[2, (1+\sqrt{-15})/2]$
-22	2	$-2^3 \times 11$	$[1, \sqrt{-22}]$	$[2, \sqrt{-22}]$
-35	1	-5×7	$[1, (1+\sqrt{-35})/2]$	$[3, (1+\sqrt{-35})/2]$
-37	3	$-2^2 \times 37$	$[1, \sqrt{-37}]$	$[2, 1+\sqrt{-37}]$
-51	1	-3×17	$[1, (1+\sqrt{-51})/2]$	$[3, (3+\sqrt{-51})/2]$
-58	2	$-2^3 \times 29$	$[1, \sqrt{-58}]$	$[2, \sqrt{-58}]$
-91	1	-7×13	$[1, (1+\sqrt{-91})/2]$	$[5, 2+\sqrt{-91}]$
-115	1	-5×23	$[1, (1+\sqrt{-115})/2]$	$[5, \sqrt{-115}]$
-123	1	-3×41	$[1, (1+\sqrt{-123})/2]$	$[3, (3+\sqrt{-123})/2]$
-187	1	-11×17	$[1, (1+\sqrt{-187})/2]$	$[7, 3+\sqrt{-187}]$
-235	1	-5×47	$[1, (1+\sqrt{-235})/2]$	$[5, \sqrt{-235}]$
-267	1	-3×89	$[1, (1+\sqrt{-267})/2]$	$[3, (3-\sqrt{-267})/2]$
-403	1	-13×31	$[1, (1+\sqrt{-403})/2]$	$[11, 2+\sqrt{-403}]$
-427	1	-7×61	$[1, (1+\sqrt{-427})/2]$	$[7, \sqrt{-427}]$

[9] B. B. Venkov, Even unimodular extremal lattices, (Russian) *Algebraic geometry and its applications. Trudy Mat. Inst. Steklov.*, **165** (1984), 43–48; translation in *Proc. Steklov Inst. Math.* **165** (1985) 47–52.

[10] B. B. Venkov, Boris Réseaux et designs sphériques, (French) [Lattices and spherical designs], *Réseaux euclidiens, designs sphériques et formes modulaires*, Monogr. Enseign. Math. **37** (2001), 10–86, Enseignement Math., Geneva.