（6）「組合せ的デザインとその推測への応用」に関する研究報告

On Difference Sets in Dihedral Groups

Dominic Tion Elvira
Kumamoto University

1. Preliminaries

A (v, k, λ) difference set (DS) is a $k-$element subset D of a group G of order v such that every element $g \neq 1$ of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. The order of the difference set D is the integer $n = k - \lambda$ and D is called non-trivial if and only if $n > 1$. Moreover, a difference set D is called cyclic, non-abelian, etc., if the underlying group G has the respective property. We study difference sets because they are equivalent to symmetric (v, k, λ) designs with a regular automorphism group[4].

Almost always, difference sets are studied in the context of the group ring $\mathbf{Z}(G)$. For $X \subseteq G$ and $t \in \mathbf{Z}$, we write $X^t = \sum_{x \in X} x^t$. With this notation, D satisfies the basic equation $DD^{-1} = n + \lambda G$.

When $n = v/4$, we call D a Hadamard Difference Set(HDS) and its parameters are given by $(4u^2, 2u^2 - u, u^2 - u)$ for some $u \in \mathbf{Z}$ (see [5]). The HDS's provide the most abundant source of known examples of difference sets. See [1] and [4] for more on DS and HDS.

2. Previous Results

Let $D_{2m} = \langle \theta, h \mid \theta^2 = h^m = \theta h \theta h = 1 \rangle$ be the dihedral group of order $2m$. We denote the cyclic subgroup of D_{2m} by $H = \langle h \mid h^m = 1 \rangle \cong Z_m$. Suppose Q is a $(2m, k, \lambda)$ DS in D_{2m}. Then we can write $Q = A + \theta B$ where $A, B \subseteq H$ and the basic equation is equivalent to the following system of equations:

(1) $AA^{-1} + BB^{-1} = \lambda H + n$
(2) $AB^{-1} = BA^{-1} = \frac{\lambda}{2} H$.

Letting $|A| = a$ and $|B| = b$, we have $a^2 + b^2 = \lambda m + n$ and $ab = \lambda m/2$.

In 1985, Fan, Siu, and Ma made the following conjecture.

Conjecture([2]) *No non-trivial difference set exists in* D_{2m}.

In another paper considering difference sets in dihedral groups, Leung, Ma, and Wong obtained the following two results:

Result 2.1 ([3]) *There exist* $\alpha, u \in \mathbf{Z}^+$ *such that* $m = \alpha u$, $n = u^2$, $a = \frac{u}{2}(\alpha - 1 - \sqrt{\alpha^2 - 2\alpha u + 1})$, $b = \frac{u}{2}(\alpha + 1 - \sqrt{\alpha^2 - 2\alpha u + 1})$, and $\lambda = u(\alpha - u - \sqrt{\alpha^2 - 2\alpha u + 1})$.

Result 2.2 ([3]) *n is an odd integer.*

We remark that since $n = u^2$ is odd, u is also an odd integer. Moreover, λ is even, k is odd and we must also have $\alpha^2 - 2\alpha u + 1 > 0$.

3. Main Results

Suppose D_{2m} contains a $(2m, k, \lambda)$ difference set Q where m is even, say, $m = 2l$. As $m = \alpha u$, $u|l$, say, $l = l_0 u$. Then $\alpha = 2l_0$ and $m = 2l_0 u$. By the previous remark, $l_0 \geq u$. Now $2|m$ and since $H \cong \mathbf{Z}_m$ is cyclic, $H \geq {}^{\exists}H' = \langle h^2 \rangle \cong \mathbf{Z}_l$. Then we can write $A = A_0 + A_1 h$ and $B = B_0 + B_1 h$ where $A_0, A_1, B_0, B_1 \subseteq H'$. Let $|A_0| = a_0$, $|A_1| = a_1$, $|B_0| = b_0$, $|B_1| = b_1$. Then $a = a_0 + a_1$ and $b = b_0 + b_1$.

Using equations (1) and (2), and comparing exponents we get

(3) $A_0 A_0^{-1} + A_1 A_1^{-1} + B_0 B_0^{-1} + B_1 B_1^{-1} = \lambda H' + n$
(4) $(A_1 A_0^{-1} + B_1 B_0^{-1})h + (A_0 A_1^{-1} + B_0 B_1^{-1})h^{-1} = \lambda H' h$
(5) $A_0 B_0^{-1} + A_1 B_1^{-1} = \frac{\lambda}{2} H'$
(6) $A_0 B_1^{-1} h^{-1} + A_1 B_0^{-1} h = \frac{\lambda}{2} H' h$.

Using characters of H, we can get the following lemma.

Lemma 3.1 *Let $s = \sqrt{\alpha^2 - 2\alpha u + 1}$. Then we have the following cases:*

(1.) $a_0 = a_1 = b_1 = \frac{u}{4}(\alpha - 1 - s)$, $b_0 = \frac{u}{4}(\alpha + 3 - s)$
(2.) $a_0 = a_1 = b_0 = \frac{u}{4}(\alpha - 1 - s)$, $b_1 = \frac{u}{4}(\alpha + 3 - s)$
(3.) $a_0 = b_0 = b_1 = \frac{u}{4}(\alpha + 1 - s)$, $a_1 = \frac{u}{4}(\alpha - 3 - s)$
(4.) $a_1 = b_0 = b_1 = \frac{u}{4}(\alpha + 1 - s)$, $a_0 = \frac{u}{4}(\alpha - 3 - s)$.

Moreover, $0 < a_0, a_1, b_0, b_1 < l$.

By Lemma 3.1 and applying a nonprincipal character of H', we prove the following:

Theorem 3.2 *If m is even then no non-trivial difference set exists in D_{2m}.*

As a corollary, we have:

Corollary 3.3 *No non-trivial Hadamard difference set exists in any dihedral group.*

References

1. Beth,T., Jungnickel,D., and Lenz,H. 1986. Design Theory. Cambridge: Cambridge University Press.
2. Fan,C.T., Siu,M.K., and Ma,S.L. 1985. Difference Sets in Dihedral Groups and Interlocking Difference Sets. Ars Combinatoria, 20A:99-107.
3. Leung,K.H., Ma,S.L., and Wong,Y.L. 1992. Difference Sets in Dihedral Groups. Designs, Codes and Cryptography, 1, 333-338.
4. Lander, E.S. 1983. Symmetric Designs: An Algebraic Approach, Cambridge: Cambridge University Press.
5. Pott,A. 1995. Finite Geometry and Character Theory, LN 1601, Springer-Verlag, Berlin.

群アソシエーションスキームについて

九州大学大学院数理学研究科 山崎 則男

有限集合 X と X 上の関係 R_λ $(\lambda \in \Lambda)$ の組 $\mathcal{X} = (X, \{R_\lambda\}_{\lambda\in\Lambda})$ で次の 4 条件 (i)-(iv) を満たすものをアソシエーションスキームと呼ぶ：(i) $R_{1_\Lambda} = \{(x,x) \mid x \in X\}$ なる $1_\Lambda \in \Lambda$ が存在。(ii) $\cup_{\lambda\in\Lambda} R_\lambda = X \times X$ かつ $R_\lambda \cap R_\mu = \emptyset$ $(\lambda \neq \mu)$。(iii) $\lambda \in \Lambda$ に対し ${}^tR_\lambda = R_{\lambda'}$ なる $\lambda' \in \Lambda$ が存在する。ここで、${}^tR_\lambda = \{(x,y) \in X \times X \mid (y,x) \in R_{lambda}\}$。(iv) 任意の $\lambda, \mu, \eta \in \Lambda$ に対して、$|\{z \in X \mid (x,y) \in \lambda, (y,z) \in \mu\}|$ が $(x,y) \in R_\eta$ のもとで x, y の取り方によらず一定（この値を $p^\eta_{\lambda,\mu}$ と書き、アソシエーションスキームのパラメータと呼ぶ)。

G を有限群、D を G の部分集合とする。この時、点集合が G、辺集合が $G \times G$ の部分集合 $\{(g,h) \in G \times G \mid g^{-1}h \in D\}$ であるグラフのことを G の D におけるケイリーグラフと呼び、以降 $Cay_D(G)$ と書く事にする。$\{C_\lambda\}_{\lambda\in\Lambda}$ を G の共役類全体とし、R^*_λ $(\lambda \in \Lambda)$ を $Cay_{C\lambda}(G)$ の辺集合とする。この時、一般に $\mathcal{X}(G) = (G, \{R^*_\lambda\}_{\lambda\in\Lambda})$ はアソシエーションスキームとなり、これを我々は群（アソシエーション）スキームと呼ぶ。

アソシエーションスキームの研究において重要視されている問題のひとつとして、既知のアソシエーションスキームと同じパラメータの集合を持つアソシエーションスキームを分類せよ、といういわゆる「アソシエーションスキームのパラメータによる特徴付け問題」と呼ばれる問題がある。ここで、群スキームにおいては全てのパラメータがその群の既約指標による計算公式により求まるという事実があり、群スキームについてのこの問題は「群の指標表による特徴付け問題」の組合せ版と見なす事ができる。

今回の講演において、この「群スキームのパラメータによる特徴付け問題」に関する講演者自身の最近の研究状況の紹介を通じて、有限群のどのような構造が群スキームに良く反映されるか、というような事を紹介できればと思っている。

Quasi-Symmetric SDP Designs on 120 and 136 Points and Their Codes

山形大学理学部 原田 昌晃

A 2-design is called *symmetric* if the number of points in the intersection of any two distinct blocks takes only one value. A 2-design is called *quasi-symmetric* if the number of points in the intersection of any two distinct blocks takes only two values. A non-symmetric 2-(v, k, λ) design with parameters

$$v = 2^{2m-1} - 2^{m-1}, k = 2^{2m-2} - 2^{m-1}, \lambda = 2^{2m-2} - 2^{m-1} - 1, \tag{1}$$

or

$$v = 2^{2m-1} + 2^{m-1}, k = 2^{2m-2}, \lambda = 2^{2m-2} - 2^{m-1}, \tag{2}$$

is said to have the *symmetric difference property*, or to be an *SDP* design, if the symmetric difference of any two blocks is either a block or the complement of a block. Such designs are quasi-symmetric. Quasi-symmetric SDP designs are closely related to certain binary linear codes.

A binary linear $[n, k]$ code C is a k-dimensional vector subspace of $\mathrm{GF}(2)^n$, where $\mathrm{GF}(2)$ is the field of two elements. The elements of C are called codewords and the weight of a codeword is the number of non-zero coordinates. An $[n, k, d]$ code is an $[n, k]$ code with minimum (non-zero) weight d. Two codes are equivalent if one can be obtained from the other by a permutation of coordinates. A code C is said to be *self-complementary* if it is has the property that if $(x_1, x_2, \ldots, x_n)$ is a codeword of C then the complementary vector $(x_1 + 1, x_2 + 1, \ldots, x_n + 1)$ is also a codeword of C. If C is a self-complementary $[n, k, d]$ code then

$$|C| \leq \frac{8d(n-d)}{n - (n-2d)^2}, \tag{3}$$

provided the right-hand side is positive. The bound (??) is known as the *Grey-Rankin bound*. Note that the bound also holds for nonlinear codes but here we consider only linear codes.

Recently McGuire [?] has proved the following:

Theorem 1 (McGuire [?]) *The parameters of a linear self-complementary code meeting the Grey-Rankin bound are*

$$[2^{2m-1} - 2^{m-1}, 2m + 1, 2^{2m-2} - 2^{m-1}], \tag{4}$$

or

$$[2^{2m-1} + 2^{m-1}, 2m + 1, 2^{2m-2}], \tag{5}$$

for even lengths.

There is a linear code with parameters (??) and (??) if and only if there is a quasi-symmetric SDP 2-(v, k, λ) design with parameters (??) and (??), respectively.

A self-complementary codes with parameters (??) or (??) has a unique weight enumerator for each m.

The case $m = 1$ and 2 is trivial. It was shown in [?] that there are exactly four inequivalent self-complementary codes with parameters $[28, 7, 12]$ and $[36, 7, 16]$, thus there are exactly four nonisomorphic quasi-symmetric SDP designs with parameters 2-$(36, 16, 12)$ and 2-$(28, 12, 11)$.

In my talk, I present several new examples for the case $m = 4$ and 5 constructing certain quasi-cyclic self-complementary codes.

Quasi-cyclic codes are a generalization of cyclic codes whereby a cyclic shift of a codeword by p positions results in another codeword. We consider quasi-cyclic codes which can be characterized in terms of $s \times s$ circulant matrices. In this case, C can be constructed from an $s \times sp$ matrix of the form

$$G = [R_0, R_1, R_2, R_3, \ldots, R_{p-1}], \tag{6}$$

where R_i is an $s \times s$ circulant matrix. We say that a code with generator matrix in the form (??) is a *quasi-cyclic code composed of circulant matrices of order s.*

The Case m = 4

For the case $m = 4$, we have the following classification of certain quasi-cyclic codes meeting the Gray-Rankin bound.

Proposition 2 *There is a unique self-complementary quasi-cyclic* $[136, 9, 64]$ *code composed of circulant matrices of order* 17, *up to equivalence.*

Proposition 3 *There are exactly* 24 *inequivalent self-complementary quasi-cyclic* $[120, 9, 56]$ *codes composed of circulant matrices of order* 10. *There are exactly* 4 *inequivalent self-complementary quasi-cyclic* $[120, 9, 56]$ *codes composed of circulant matrices of order* 15, *one of which is inequivalent to the above* 24 *codes.*

By the above proposition, we have the following:

Corollary 4 *There are at least* 25 *non-isomorphic quasi-symmetric SDP designs with parameters* $(120, 56, 55)$ *and* $(136, 64, 56)$. *There are at least* 25 *inequivalent self-complementary* $[136, 9, 64]$ *codes.*

The Case m = 5

For the case $m = 5$, we have the following:

Proposition 5 *There are at least ten inequivalent self-complementary codes with parameters* $[496, 11, 240]$ *and* $[528, 11, 256]$. *There are at least ten non-isomorphic quasi-symmetric SDP designs with parameters* $(496, 240, 239)$ *and* $(528, 256, 240)$.

参考文献

[1] G. McGuire, Quasi-symmetric designs and codes meeting the Grey-Rankin bound, *J. Combin. Theory Ser. A* **78** (1997) pp. 280–291.

[2] V.D. Tonchev, Quasi-symmetric designs, codes, quadrics, and hyperplane sections, *Geom. Dedicata* **48** (1993) pp. 295–308.

Formally self-dual code の分類

名古屋大学多元数理科学研究科 別宮 耕一

1 Introduction

A binary linear $[n,k]$ code C is a k-dimensional vector subspace of $\mathbb{F}_2^n$, where $\mathbb{F}_2$ is the finite field of two elements. The elements of C are called codewords. The weight $wt(x)$ of a codeword x is the number of non-zero coordinates. The minimum weight of C is the smallest weight among all non-zero codewords of C. An $[n,k,d]$ code is an $[n,k]$ code with minimum weight d. Two codes C and C' are equivalent if one can be obtained from the other by permuting the coordinates. The automorphism group of C is the set of permutations of the coordinates which preserve C. The weight enumerator of C is $W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i$, where A_i is the number of codewords of weight i in C. When recording a weight enumerator, we shall set $x = 1$. The dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_2^n |\ x \cdot y = 0 \text{ for all } y \in C\}$ where $x \cdot y$ denotes the standard inner-product of x and y.

A code C is *self-dual* if $C = C^\perp$. A code C is *formally self-dual* if C and $C^\perp$ have identical weight enumerators. Self-dual codes are by definition formally self-dual automatically. There exist formally self-dual codes which are not self-dual.

A code is called *even* if the weights of all codewords are even. A formally self-dual code which is not even is called *odd*.

The minimum weight of an even formally self-dual code of length n is bounded by $2\lfloor \frac{n}{8} \rfloor + 2$. An even formally self-dual $[n, n/2, 2\lfloor \frac{n}{8} \rfloor + 2]$ code is called extremal. The restrictions on odd formally self-dual codes are significantly fewer than on even formally self-dual codes. Thus there can be odd formally self-dual codes with minimum weight exceeding the above bound. This is one reason of interest in odd formally self-dual codes. An odd formally self-dual code with the highest minimum weight for that length is called *optimal*. An *optimal* formally self-dual code has the highest minimum weight among even formally self-dual codes as well as odd formally self-dual codes.

2 Classification of Formally Self-Dual Codes

First we determine the highest minimum weight $d_O(n)$ of odd formally self-dual codes of length n in order to define optimal codes. The highest possible minimum weights are determined from known upper bounds for minimum weights of binary linear $[n, n/2]$ codes given in [?] except lengths 8, 18 and 24. The extended Hamming code is a unique $[8,4,4]$ code. Thus $d_O(8) \leq 3$. Any linear $[18,9,6]$ code is equivalent to the extended quadratic residue code of length 18, which is even formally self-dual [?]. Thus $d_O(18) \leq 5$. Since it is well known that a linear $[24,12,8]$ code is equivalent to the extended Golay code, there is no odd formally self-dual $[24,12,d]$ code with $d \geq 8$.

For length $n \leq 24$, we list in Table ?? the highest minimum weights $d_O(n)$ of odd formally self-dual codes of length n.

In the third column of the table, we list the number $N(n)$ of the inequivalent optimal odd formally self-dual codes of length n. To compare with $d_O(n)$ we also list the highest minimum weights $d_E(n), d_L(n)$, $d_I(n)$ and $d_{II}(n)$ of even formally self-dual codes of length n, all linear $[n, n/2]$ codes, Type I and Type II self-dual codes of length n, respectively. The highest minimum weights of even formally self-dual codes are determined in [?] and [?]. Note that the even formally self-dual codes which we consider are not self-dual. All even formally self-dual codes of lengths 2 and 4 are self-dual [?]. All extremal Type I and Type II codes of length up to 32 have been classified (see [?]).

we denote the highest minimum weight among all linear $[n, n/2]$ codes, by $d_{max}(n)$ Let $N_S(n)$ $N_E(n)$ and $N_O(n)$ denote the numbers of inequivalent optimal linear $[n, n/2, d_{max}(n)]$ codes which are self-dual, even formally self-dual and odd formally self-dual, respectively, and let $N_T(n)$ denote the total number of inequivalent optimal linear $[n, n/2, d_{max}(n)]$ codes.

表 1: The highest minimum weights of length up to 24

Length n	$d_O(n)$	$N(n)$	$d_E(n)$	$d_L(n)$	$d_I(n)$	$d_{II}(n)$
2	1	1	-	2	2	
4	2	1	-	2	2	
6	3	1	2	3	2	
8	3	2	2	4	2	4
10	4	1	4	4	2	
12	4	5	4	4	4	
14	4	112	4	4	4	
16	5	1	4	5	4	4
18	5	≥ 2	6	6	4	
20	6	1	6	6	4	
22	7	1	6	7	6	
24	7	1	6	8	6	8

表 2: $N_T(n)$, $N_S(n)$, $N_E(n)$ and $N_O(n)$ for $2 \leq n \leq 24$

Length n	$N_T(n)$	$d_{max}(n)$	$N_S(n)$	$N_E(n)$	$N_O(n)$
2	1	2	1	0	0
4	3	2	1	1	1
6	1	3	0	0	1
8	1	4	1	0	0
10	4	4	0	1	1
12	43	4	1	2	5
14	≥ 1360	4	1	9	112
16	1	5	0	0	1
18	1	6	0	1	0
20	≥ 8	6	0	7	1
22	1	7	0	0	1
24	1	8	1	0	0

参考文献

[1] K. Betsumiya, T.A. Gulliver and M. Harada, On binary extremal formally self-dual even codes, *Kyushu J. Math.*, (to appear), (1999).

[2] A.E. Brouwer and T. Verhoeff, An updated table of minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Theory* Vol. 39 (1993) pp. 662–677.

[3] J. Simonis, The $[18, 9, 6]$ code is unique, *Discrete Math.* **106/107** (1992) 439–448.

[4] G. Kennedy and V. Pless, On designs and formally self-dual codes, *Designs, Codes and Cryptogr.* Vol. 4 (1994) pp. 43–55.

[5] M. Harada, The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes, *Finite Fields and Their Appl.* Vol. 3 (1997) pp. 131–139.

[6] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* Vol. 36 (1990) pp. 1319–1333.

表 3: Classification of optimal formally self-dual codes

Length n	$d(n)$	$N(n)$
2	1	1
4	2	1
6	3	1
8	3	2
10	4	2
12	4	7
14	4	121
16	5	1
18	6	1

スペクトラム拡散通信と組合せ的デザイン

藤原　良　　（筑波大学社会工学系）
ミャオ　イン　（筑波大学社会工学系）

スペクトラム拡散通信（ＳＳ通信）の概念が最初に紹介されたのは１９５９年のCostasの論文であろうといわれている．しかし軍事的利用は盛んに行われてきたが，民間利用は周波数効率が余りよくないといわれて，最近まであまり利用されてこなかった．　ところが，最近になってアメリカのQualcomm社が１９９０年デジタル携帯電話の方式（cdmaOne）として提案して以来急に脚光を浴びてきた．　日本でもこの方式は一部導入されており，また次世代携帯電話の方式にもＳＳ通信方式の採用（W-CDMA, CDMA-2000）が決定している．

ＳＳ通信方式とは，従来の無線通信方式に対して全く正反対の概念を持った方式である．従来は与えられた周波数帯域を有効に使うために，できるだけたくさんの狭い周波数帯に区切り，多くのチャンネルを確保することに主眼が置かれていた．これに対してＳＳ通信方式は，広い周波数帯域を一つのチャンネルとして使う，そして複数の利用者がその周波数帯域を同時に使うのである．すなわち複数の携帯電話から同じ周波数に対して同時に電波を発信するのである．　この方法を従来の方法と比較しながら説明しよう．

１．周波数分割（FDMA）／時分割（TDMA）方式

デジタル通信では音声アナログ信号はすぐさま，(0,1)のデジタル信号に変換される．その速度は現在の携帯電話では9600 bit／秒程度である．FDMA方式では，　各区域には数十のチャンネル（狭い周波数帯域）が用意されている．発信するとき，まずチャンネルがいま使われていないかをチェックする．そして使われていないチャネルが見つかればそのチャンネルにパリティをつけてそのままデジタル信号を送る．時分割方式では時間軸に対して数ミリ秒毎に分割し，複数チャンネルを作る．

２．スペクトラム拡散（ＳＳ）方式

音声アナログ信号を(0,1)のデジタル信号に変換するところは同じであるが，その後のプロセスはかなり異なる．いま音声デジタル信号を

1,0,1,1,0,0,....

とすると，1ビット毎に，フレームと呼ばれるv次元(0,1)ベクトルのコードに変換する．0は必ず全ゼロのフレーム（0,0,0,...）に変換．1の場合はたとえば最初の1を(1,0,1,...)と変換するが，3番目の1に関しては(1,1,0,...)というように毎回異なる．

例：　ビット　　フレーム

１０１　->　(1,0,1,1,0)　(0,0,0,0,0)　(1,1,0,1,0)

ＳＳ通信の一方式，直接拡散（ＤＳ）方式では広帯域の一つのチャンネルに送信する，他の利用者も同時に異なるフレームを送信する．当然複数の異なるフレームが同じ周波数に送信されるので空中で電波は重なる．論理的に論理和（OR）をとったフレームが受信される．発信者と受信者は同期して同じフレームを生成できる．受信者は受信したフレームに生成したフレームが含まれるか（ANDをとる）をチェックし，(0,1)ビットに変換し音声デジタル信号を復元する．

第一利用者　１０１...　->　(1,0,1,1,0)　(0,0,0,0,0)　(1,1,0,1,0) . . .

第二利用者　０１１...　->　(0,0,0,0,0)　(1,1,1,0,0)　(0,1,1,1,0) . . .

受信フレーム　　(1,0,1,1,0)　(1,1,1,0,0)　(1,1,1,1,0) . . .

実際のフレームの長さはcdmaOneでは64，次世代携帯電話では1024である．

ＳＳ通信のもう一つの方式である周波数ホッピング（ＦＨ）方式では，広帯域の周波数をいくつか（m個）の周波数帯に分ける．そしてフレームは多値型（m-値）を用いる．

例：　1,0,1　->　(1,4,2,1)　(0,0,0,0)　(6,2,3,1)

そして,フレームが（1,4,2,1）であったら1番目，4番目，2番目，1番目の周波数に逐次信号1を送る．一つのフレームで,異なる周波数に同時に信号を送ることはない．しかし複数利用者のいる区域で受信した場合は複数周波数に同時に1を受信することはある．

例：受信フレーム（｛1,3｝,｛4,2｝,｛2,1｝,｛1｝）

ＳＳ通信のメリットは，複数利用者が同一周波数帯を使うので，ある利用者が会話が少ない時などの時音声デジタル信号の速度を遅くした場合,他の利用者の利用者の通信容量が増加する．フレーム信号が空中でミックスするため，盗聴が難しくなる．フレーム・コードに要求される条件は次のようなものである．

（1）フレームの各位置での1になる確立が等しい．（一様性）

（2）フレームの逐次生成が簡単

（3）フレーム内の1の数（重み）が等しい．

（4）フレーム分離度が高い．

どのようなフレーム・コードがよいか，またどう構成するか，どのような性質を持つかは符号理論あるいは組合せ理論の重要問題である．

3．t-union independent

Vをv要素からなる有限集合とする．いまt個のVの部分集合があるとする．もしt個の部分集合の内，任意のものが，他のものの和集合に含まれることがないとき，このt個の部分集合をunion independentという．今n（n>t）個の部分集合があるとする．もしこの中のどのt個の部分集合もunion independentである時，このn個の部分集合をt-union independentと呼ぶ．この問題はどのt個のフレームが重なっても分離可能であることを意味する．そのような性質を持ち，最大のフレーム個数を持ったコードを構成する問題が重要となる．また最大個数に関する問題も重要である．$ft(v)$をt-union independentである部分集合の最大数，$ftk(v)$を部分集合のサイズをkに制限した時の最大数とする．このとき次のような結果が知られている．

$$f_3^{2m-1}(v) \le \binom{v}{m} / \binom{2m-1}{m}$$

Steiner System S(t, k, v)とはv-集合Vとk-部分集合（ブロック）の集まりBのペア（V，B）で，任意の

$$f_3^{2m}(v) \le \binom{v-1}{m} / \binom{2m-1}{m}$$

$$\binom{n}{t} / \binom{k}{t}^2 \le f_{r+1}^{k}(v) \le \binom{v}{t} / \binom{k-1}{r-1}, \quad t = \lceil k/r \rceil$$

$$f_{r+1}^{r(t-1)+1+d}(v) \le \binom{v-d}{t} / \binom{k-d}{t}, \quad for\ v\ is\ sufficiently\ large,$$

$$whenever\ \ d = 0,1\ \ or\ \ d \le r/2t^2$$

Vのt-部分集合に対し,それを含むブロックが必ず1つBの中に存在するという条件を満たすものである．このような組合せ的デザインの構成や解析は組合せ理論の重要分野の一つである．Steiner System S(t, k-d, n-d)が存在する時，そのデザインからできるコードは上の上界を満たす．また非同期型のCDMAの場合には，巡回型のSteiner Systemあるいは巡回型Group Divisible Designの存在が，上界を満たすコードの構成に役立つ．

組合せデザインの応用II

慶応大学理工学部 神保　雅一

この報告では，(1) (t,m,s)-net と数値解析 および (2) たたみ込み符号と有効ブロックデザイン について概説する。

1　(t,m,s)-net と数値解析

超高次元の数値積分に (t,m,s)-net と呼ばれる組合せ構造が有効である ([4], [5]).

$$I_s = [0,1) \times [0,1) \times \cdots \times [0,1)$$

を s 次元単位 cube とし、$b, m > t$ を正整数とする．また、$d_1, \cdots, d_s$ を $\sum_i d_i = m - t$ を満たす非負整数とする．任意の $0 \leq a_i < b^{d_i}$ に対して，

$$I = I(d_1, \cdots, d_s; a_1, \cdots, a_s) = \prod_{i=1}^{s} \left[\frac{a_i}{b^{d_i}}, \frac{a_i + 1}{b^{d_i}} \right)$$

を elementary interval in base b と呼ぶ．$I(d_1, \cdots, d_s; a_1, \cdots, a_s)$ の体積は b^{t-m} である．ここで，

$$\mathcal{I} = \{ I(d_1, \cdots, d_s; a_1, \cdots, a_s) | \sum_i d_i = m - t, 0 \leq a_i < b^{d_i} \}$$

とおく．

V を I_s の有限部分集合とする．(1) $|V| = b^m$ であり、(2) 任意の $I \in \mathcal{I}$ が V の b^t 個の点を含むとき，V は (t,m,s)-net であるという．V の各点の各座標値を b 進数で表したときの小数以下 $m-t$ 桁までを切り捨てて近似した (格子) 点に置き換えてもまた (t,m,s)-net である。$v_p \in V$ の第 j 座標値を

$$x_j^{(p)} = \frac{x_{1j}^{(p)}}{b^1} + \frac{x_{2j}^{(p)}}{b^2} + \cdots + \frac{x_{m-t,j}^{(p)}}{b^{m-t}}$$

と表し，$\{x_{ij}^{(p)}\}$ を $(m-t) \times s \times b^m$ 配列 $C(V)$ の第 (i,j,p)-成分とする．すなわち、各点の座標値 $\{x_{ij}^{(p)}\}$ を $(m-t) \times s$ 配列に並べ，それを b^m 個重ねた 3 次元配列が $C(V)$ である．

いま，$Q(d_1, \cdots, d_s) = \{(i,j) | 1 \leq i \leq d_j, 1 \leq j \leq s\}$ を qualifying collection と呼ぶ．そして、$\mathcal{Q} = \{Q(d_1, \cdots, d_s) | \sum_i d_i = m - t, 0 \leq d_i\}$ とおく．このとき、$t' \times s \times \lambda n^{t'}$ 配列 $C = (c_{ij}^{(p)})$ が cubic $\mathrm{OA}_\lambda(t', s, n)$ であるとは、次の (1), (2) が成り立つことである．

(1) C の各要素は $Z_n = \{0, 1, \cdots, n-1\}$ の元.
(2) 任意の qualifying collection $Q \in \mathcal{Q}$ に対して，$g_{ij} \in Z_n$ $((i,j) \in Q)$ を任意に fix したとき、すべての $(i,j) \in Q$ に対して $c_{ij}^{(p)} = g_{ij}$ となる p の数が一定 $(= \lambda)$.

命題 (Mullen and Schmid [3]). V が (t,m,s)-net であることと $C(V)$ が cubic $\mathrm{OA}_t(m-t, s, b)$ であることは同値である.

(t,m,s)-net について，その bound, large set of (t,m,s)-net, (t,m,s)-net をなす pseudo random sequence などの研究がなされている．

2　たたみ込み符号と有向ブロックデザイン

単位時間ごとに逐次発生する 0,1 列の情報を

$$a_0, a_1, a_2, a_3, \cdots, a_t, \cdots$$

とする．このデータをそのまま送信すると 1 ビットでも誤りが起こるとその場所を特定することが出来ず，正確な情報を受信することができない．ここでは，ブロック符号の場合と同様に，ある個数以下の誤りに対しては正確に復号ができる符号化の方法について考えてみよう．

まず、上のデータの列を形式的に $a(x) = \sum_i a_i x^i$ と表し，$b(x) == g(x)a(x)$ とおく．ただし，$g(x) = 1 + x^{m_1} + \cdots + x^{m_{2e-1}}$ は F_2 上の多項式であり、生成多項式と呼ばれる．そして、

$$a_0, b_0, a_1, b_1, \cdots, a_n, b_n, \cdots$$

の順にデータを送信する．通信路で、$a_0, a_1, \cdots$; $b_0, b_1, \cdots$ に加わるノイズ系列をそれぞれ、$e_0, e_1, \cdots$; $f_0, f_1, \cdots$ とし、$e(x) = \sum_i e_i x^i$, $f(x) = \sum_i f_i x^i$ とすると、受信列の多項式は、$r(x) = a(x) + e(x)$, $q(x) = b(x) + f(x)$ となる．ただし、演算は F_2 上で考える．

今，$g(x) = 1 + x^{m_1} + x^{m_2} + \cdots + x^{m_{2e-1}}$ において $m_i - m_j (i > j)$ がすべて異なるとき，この符号列を、束縛長 $2(m_{2e-1} + 1)$ ビットの e-誤り訂正たたみ込み符号と呼ぶ．

例．$g(x) = 1 + x$，$g(x) = 1 + x + x^4 + x^6$

上記のたたみ込み符号は，情報ビット (a_i) の information rate が 1/2 であるが、複数の生成多項式 $g_l(x) = 1 + x^{m_{l1}} + \cdots + x^{m_{lk}}$, $(l = 1, \cdots, s)$ に対して，$m_{li} - m_{lj} (i > j, 1 \leq l \leq s))$ がすべて異なるという条件を考えることにより、より rate の高いたたみ込み符号を作ることが出来る．

参考文献

[1] Colbourn, Dinitz and Stinson (1999), *Surveys in Combinatorics*, London Mathematical Society Lecture Note Series 267, Cambridge University Press.

[2] C.F. Laywine and G.L. Mullen (1998), *Discrete mathematics using Latin squares*, Wiley-Interscience.

[3] G.L. Mullen and W.C. Schmid (1996), *J. Combin. Theory*, Ser. A, 76, 164-174.

[4] H. Nederreiter (1987), *Monatshefte Mathematik*, 104, 273-337.

[5] H. Nederreiter (1992), *Discete Math.*, 106/107, 361-367.

[6] 岩垂好裕 (1992), 符号理論入門, 昭晃堂.

Group testing problem and related designs

大阪府立大・工　栗木 進二

$\mathcal{P}$ を b 個の item からなる集合とし，そのうちの d 個は “ defect ive ” な item であり，残りの $b-d$ 個は “ good ” であるとする．いくつかの i tem を集めて，test を行うことにし，その集められた item の集合を $X(\subset \mathcal{P})$ とすると，group test の結果として，X が少なくとも 1 つの defecti ve item を含むとき “ yes (positive) ”，そうでないとき “ no (negative) ” が得られるものとする．Group testing problem の目的は，何回かの group test を行って，どの item が defective であるかを正確に決めることである．何回かの grou p test が同時に行われるとき，この問題は nonadaptive，そうでないとき，adaptiv e といい，ここでは，nonadaptive の場合を考えることにする．Group testing の始まりは Dorfman (1943) においてみられ，大きな母集団（兵隊）からある病気（梅毒）の人を特定するために group testing が用いられた．最近の group testing の応用は Bruno, Knill, etc. (1995) にみられ，DNA の string をいくつかの部分（clo ne という）に分け，特別な DNA の列を含む clone を特定することが問題とされている．ここでは，group testing problem に関連する組合せ構造を紹介することにする．

$\mathcal{X}$ を group test に対応する $\mathcal{P}$ の部分集合の集まりとする．このとき，$(\mathcal{P}, \mathcal{X})$ が nonadaptive group testing problem の解であるための必要十分条件は，defective と考えられる item からなる任意の集合 D_1, D_2 に対して，

$$\{X : D_1 \cap X \neq \emptyset, X \in \mathcal{X}\} = \{X : D_2 \cap X \neq \emptyset, X \in \mathcal{X}\} \quad \Longrightarrow \quad D_1 = D_2 \tag{1}$$

が成り立つことである．

V を v 個の点の集合とし，$\mathcal{B}$ を V の部分集合（block という）の集まりとするとき，$(V, \mathcal{B})$ を design という．$(\mathcal{P}, \mathcal{X})$ の dual を design $(V, \mathcal{B})$ と考えることができ，$\mathcal{X}$ の group test の個数を v とし，その group test を V の点に対応させ，b 個の item を $\mathcal{B}$ の block に対応させる．D_1, D_2 に対応する block の集まりを $\mathcal{B}_1, \mathcal{B}_2$ とすると，(1) は

$$\bigcup_{B_1 \in \mathcal{B}_1} B_1 = \bigcup_{B_2 \in \mathcal{B}_2} B_2 \quad \Longrightarrow \quad \mathcal{B}_1 = \mathcal{B}_2 \tag{2}$$

と書き換えられる．Group testing problem においては，点 (group test) の個数 v が与えられたとき，block (item) の個数 b を最大にすることが目的とされる．ある threshold value p があって，多くの場合，$d \leq p$ が成り立ち，hype rgeometric problem では，$d \leq p$ が仮定される．また，strict problem では，$d \leq p$ のとき，defective item を特定しなければならないが，$d > p$ のときには，そうであることを判断し，defective item を特定する必要はない．

$(V, \mathcal{B})$ が $d \leq p$ である hypergeometric nonadaptive group testin g problem の解であるための必要十分条件は，$|\mathcal{B}_1| \leq p$, $|\mathcal{B}_2| \leq p$ である任意の $\mathcal{B}_1, \mathcal{B}_2$ に対して，(2) が成り立つことである．このとき，$(V, \mathcal{B})$ の接合行列は “ 高々 p 列からなる 2 つの集合のそれぞれの union は異なる ” という性質をもつ．このような行列を rp-separable といい，それに対応する set system を p-union free という．$\bar{p}$-separable な行列の列は superimposed code を生成し，同時に p 個までの codeword を送ることができる．しかし，decode するためには，p 列までのすべての union を調べることが必要となるであろう．もう少し条件を強くして，その接合行列が “ p 列からなる集合の union がその他の列を cover しない（集合として含まない）” という性質をもつとき，p-disjunct といい，それに対応する set system を p-cover free という．この性質については，“ p 列 ” と ‘‘ 高々 p 列 ” とは同じ意味である．この場合の decoding は

簡単で，受け取られた union によって cover されるすべての codeword が“ positive ”である．明らかに，p-disjunct (p-cover free) ならば，$\bar{p}$-separable (p-unio n free) である．

$(V,\mathcal{B})$ において，$\mathcal{B}$ の block size が一定 (k) で，V の任意の t 個の点がちょうど1つの block に含まれるとき，$(V,\mathcal{B})$ を Stei ner t-design といい，$S(t,k,v)$ と表す．

定理 2.1. (Erdös, Frankl and Füredi (1982)) 点の個数が v で，blo ck size が一定 (k) の 2-cover free family において，block の個数が最大となるものが，$k=2t-1$ のとき，Steiner t-design $S(t,2t-1,v)$ によって与えられ，$k=2t$ のとき，ある design $(V^*,\mathcal{B}^*)$ によって与えられる．ここで，$\mathcal{B}^*=\{\{x\}\cup B : B\in\mathcal{B}\}$ で，$x(\in V^*)$ に対して，$(V^*\backslash\{x\},\mathcal{B})$ は $S(t,2t-1,v-1)$ である．なお，$t\geq 2$ である．

定理 2.2. (Frankl and Füredi (1984)) 点の個数が v で，block size が 3 である 2-union free family において，block の個数が最大となるものが Ste iner triple system $S(2,3,v)$ によって与えられる．

また，$(V,\mathcal{B})$ が strict problem の解であるための必要十分条件は，$|alB_1|\leq p$ である任意の $\mathcal{B}_1,\mathcal{B}_2$ に対して，(2) が成り立つことであるが，この条件は p-disjunct (p-cover free) の条件と同値である．

Group test の結果として，“ false positive ”が許される場合を考え，そのような false positive の個数は q 以下であるとする．$(V,\mathcal{B})$ が threshold value p をもち，q 個までの false positive に対して error correcting できる strict group testing problem の解（(p,q)-solution という）であるための必要十分条件は，$|\mathcal{B}_1|\leq p$ である任意の $\mathcal{B}_1,\mathcal{B}_2$ に対して，

$$\left|\left(\bigcup_{B_1\in\mathcal{B}_1}B_1\right)\triangle\left(\bigcup_{B_2\in\mathcal{B}_2}B_2\right)\right|>q$$

が成り立つことである．ここで，$B\triangle C=(B\backslash C)\cup(ClashB)$ である．

定理 2.3. (Balding and Torney (1996)) $(V,\mathcal{B})$ が (p,q)-soluti on であるための必要十分条件は p 個の block の任意の union に対して，残りのすべての block がこの union には含まれない少なくとも $q+1$ 個の点をもつことである．

$(V,\mathcal{B})$ が (t,k,v)-packing であるとは，$\mathcal{B}$ の block size が一定 (k) で，任意の2つの block B_1, B_2 に対して，$|B_1\cap B_2|\leq qt$ が成り立つことである．明らかに，$k\geq pt+q+1$ である任意の (t,k,v)-packing は定理 2.3 の必要十分条件を満たす．また，$S(t,k,v)$ は $(t-1,k,v)$-p acking である．

定理 2.4. (Balding and Torney (1996)) 点の個数が v で，block size が一定の $(2,q)$-solution において，Steiner system $S(t^*,2t^*+q-1,v)$ は bloc k の個数が最大の解を与える．ここで，t^* は

$$v\leq 5t+2+\frac{q(q-1)}{t+q}$$

を満たす最小の整数である．

Flag-Transitive 2-$(v,4,1)$ Designs

九州大学大学院数理学研究科 宗政 昭弘

2-$(v,k,1)$ デザイン $(X,\mathcal{B})$ において、 incident な point-block の組全体に自己同型群が可移に作用しているとき、$(X,\mathcal{B})$ を flag-transitive （旗上可移）であるという。Flag-transitive な Steiner triple system はすでに分類されているが、ブロックサイズが 4 以上の場合の分類は未解決である。しかし、1991 年にアナウンスされた Buekenhout, Delandtsheer, Doyen, Kleidman, Liebeck, Saxl らの結果によれば、 知られていない flag-transitive design の自己同型群は、有限体上の m 次元アフィン空間 $X = AG(m,p)$ に作用している 1 次元アフィン半線形群 $A\Gamma L(1,p^m)$ の部分群である （特に可解群であり、非可換単純群ではない)。この定理の意味する所は、有限単純群の分類を使ってできる flag-transitive design の分類は完成し、残っていてできない部分は組合せ論や有限体の専門家の手にゆだねられた、ということである。

本講演では、$p=2$ で、ブロックが 2 次元アフィン部分空間であるような flag-transitive 2-$(v,4,1)$ デザインの数え上げと構成法について最近の結果を発表する。Flag-transitive という性質から、このようなデザインを考えることは射影空間 $PG(m-1,2)$ の line を考えることに帰着され、それはさらに有限体 $GF(2^m)$ における代数的な問題に帰着される。

Bounds on numbers of constraints for three-symbol balanced arrays of strength two

弓場　弘　国際自然研
小川　友和　鳥城高校
兵頭　義史　岡山理大・理, 国際自然研

シンボル 0,1,2 を要素とする $N \times m$ 配列 T を強さ 2 の 3 シンボル均斉配列 $\mathrm{BA}(N,m,3,2;\{\mu^{(2)}_{p_0p_1p_2}\})$ とし, そのシンボルの重み分布を $W=[(w_0),(w_1),(w_2)]$ とする. ここに $(w_\alpha)=(w_\alpha(1),\cdots,w_\alpha(N))'$ で, $w_\alpha(j)$ は, T の第 j 行におけるシンボル α の個数を表す. このとき, 次の関係式が成り立つ:

$$\sum_{j=1}^{N} w_0(j)^{[q_0]}w_1(j)^{[q_1]}w_2(j)^{[q_2]} = m^{[u]}\mu^{(u)}_{q_0q_1q_2} \quad (^\forall u \in \{1,2\})$$

ここに $\mu^{(u)}_{q_0q_1q_2}=\sum_{p_0+p_1+p_2=2}\frac{(2-u)!}{\prod_{i=0}^{2}(p_i-q_i)!}\mu^{(2)}_{p_0p_1p_2}$ であり, 階乗関数 $x^{[k]}=\prod_{i=1}^{k}(x-i+1)$ を表す.

N 次元列ベクトル $(\varphi_\alpha)=(\varphi_\alpha(1),\cdots,\varphi_\alpha(N))'$ ($\varphi_\alpha(j)$: $w_\gamma(j)(\gamma=0,1,2)$ のある関数) の集合を $\Phi=\{(\varphi_1),\cdots,(\varphi_k)\}$ とする. このとき, 集合 Φ の各要素が制約条件:

$$\varphi_\alpha(j)\varphi_\beta(j) \text{ が } w_\gamma(j) \text{ の } u(\in\{1,2\}) \text{ 次多項式である}$$

を満たすならば Φ から構成される Gram 行列 $[(\varphi_1),\cdots,(\varphi_k)]'[(\varphi_1),\cdots,(\varphi_k)]$ の各要素は, 均斉配列 T の制約数 m と指標 $\mu^{(2)}_{p_0p_1p_2}$ のある関数となり, その行列の半正値性から m に関する不等式系が導かれる. 上記制約条件を満たす N 次元列ベクトルの集合として $A=\{(1),(w_0),(w_1),(w_2)\}$ が考えられる. ここに N 次元列ベクトル $(1)=(1,\cdots,1)'$ である. この集合から導かれる不等式系により制約数 m の上界 $m(W)$ が得られる.

[注意 1] 集合 A から導かれる m に関する不等式系は, 集合 $A_1\equiv\{(w_0),(w_1),(w_2)\}$ から導かれる m に関する等式系と同値である.

[注意 2] 集合 A_1 から導かれる m に関する不等式系は, 集合 $A_2\equiv\{(1),(w_1),(w_2)\}$ から導かれる m に関する不等式系:

$$\begin{aligned}
&\text{(i)} && m\{(\mu^{(2)}_{200}+\mu^{(2)}_{110}+\mu^{(2)}_{101})^2-N\mu^{(2)}_{200}\} \le N(\mu^{(2)}_{110}+\mu^{(2)}_{101})\\
&\text{(ii)} && m\{(\mu^{(2)}_{110}+\mu^{(2)}_{020}+\mu^{(2)}_{011})^2-N\mu^{(2)}_{020}\} \le N(\mu^{(2)}_{110}+\mu^{(2)}_{011})\\
&\text{(iii)} && \{(m-1)N\mu^{(2)}_{110}-m(\mu^{(2)}_{200}+\mu^{(2)}_{110}+\mu^{(2)}_{101})(\mu^{(2)}_{110}+\mu^{(2)}_{020}+\mu^{(2)}_{011})\}^2\\
&&& \le [N(\mu^{(2)}_{110}+\mu^{(2)}_{101})-m\{(\mu^{(2)}_{200}+\mu^{(2)}_{110}+\mu^{(2)}_{101})^2-N\mu^{(2)}_{200}\}]\\
&&& \cdot[N(\mu^{(2)}_{110}+\mu^{(2)}_{011})-m\{(\mu^{(2)}_{110}+\mu^{(2)}_{020}+\mu^{(2)}_{011})^2-N\mu^{(2)}_{020}\}]
\end{aligned}$$

と同値である.

このことから, 実質的には, 集合 A_2 から導かれる不等式系を用いて, 制約数 m の上界 $m(W)$ が得られる.

一方, 3^m 要因計画の処理組合せ $(j_1,j_2,\cdots,j_m)$ $(j_p=0,1,2)$ を 3 進の順に配列したものを Z とし, その観測値ベクトルを $\boldsymbol{y}(Z)$ とする. このとき, すべての要因効果ベクトルを $\boldsymbol{\Theta}(Z)=(1/3^m)D'_{(m)}E[\boldsymbol{y}(Z)]$ で定義する. ここに $D_{(m)}$ は $D=[\boldsymbol{d}_0,\boldsymbol{d}_1,\boldsymbol{d}_2]$ の m 回のクロネッカー積で, $\boldsymbol{d}'_0=(1,1,1)$, $\boldsymbol{d}'_i=(d_{0i},d_{1i},d_{2i})$ $(i=1,2)$ は $\boldsymbol{d}'_i\boldsymbol{d}_k=3\delta_{ik}$ $(i,k=0,1,2)$ を満たす. この定義の下に, 強さ 2 の 3 シンボル均斉配列 $\mathrm{BA}(N,m,3,2;\{\mu^{(2)}_{p_0p_1p_2}\})$ から導かれる一部実施 3^m 要因計画 (3^m-FF 計画) T を考える. ただし 2 因子以上の高次交互作用は無視可能とする. このとき, 線形模型は $\boldsymbol{y}(T)=E(1,T)\boldsymbol{\theta}+\boldsymbol{e}(T)$ で与えられる. ここに $E(1,T)$ は一般平均と主効果に対応する列ベクトルで構成される $N\times(1+2m)$ 計画行列,

$\theta(=(\theta(\phi);(\theta\{p^{i_P}\})'))$ は主効果までの要因効果ベクトル, $\boldsymbol{e}(T)$ は誤差ベクトル $(\boldsymbol{e}(T)\sim(\boldsymbol{0},\sigma^2 I_N))$ である. この場合, 情報行列 $M(1,T)(=E(1,T)'E(1,T))$ は, 次式で与えられる:

$$M(1,T)=P'\mathrm{diag}(K_0;\overbrace{K_1\cdots K_1}^{m-1})P \quad (^{\exists}P\in \mathrm{O}(2m+1))$$

ここに 3 次対称行列 $K_0=[\kappa_0^{ij}]$ および 2 次対称行列 $K_1=[\kappa_1^{ij}]$ の各要素は次式で与えられる:

$$\begin{aligned}
\kappa_0^{00} &= N \\
\kappa_0^{0i} &= \sum_{\alpha=0}^{2}\sqrt{m}d_{\alpha i}\mu^{(2)}_{0\cdots p_\alpha\cdots 0}+\sum_{0\le\alpha<\beta\le 2}\sqrt{m}(d_{\alpha i}+d_{\beta i})\mu_{0\cdots q_\alpha\cdots q_\beta\cdots 0} \qquad (i=1,2)\\
\kappa_0^{ij} &= \sum_{\alpha=0}^{2}md_{\alpha i}d_{\alpha j}\mu^{(2)}_{0\cdots p_\alpha\cdots 0}+\sum_{0\le\alpha<\beta\le 2}[d_{\alpha i}\{d_{\alpha j}+(m-1)d_{\beta j}\}\\
&\quad +d_{\beta i}\{d_{\beta j}+(m-1)d_{\alpha j}\}]\mu^{(2)}_{0\cdots q_\alpha\cdots q_\beta\cdots 0} \qquad (1\le i\le j\le 2)\\
\kappa_1^{i-1j-1} &= \sum_{0\le\alpha<\beta\le 2}(d_{\alpha i}-d_{\beta i})(d_{\alpha j}-d_{\beta j})\mu^{(2)}_{0\cdots q_\alpha\cdots q_\beta\cdots 0} \qquad (i,j=1,2)
\end{aligned}$$

ただし $p_\alpha=2;\ q_\alpha,q_\beta=1$ である.

このとき, 情報行列 $M(1,T)$ すなわちその相似行列の部分行列 K_0 の半正値性から均斉配列 T の制約数 m の上界 $m(I)$ が得られる.

[注意 1], [注意 2] および関係式: $[(w_0),(w_1),(w_2)]'[(w_0),(w_1),(w_2)]=LK_0L'$ を用いて, 次の定理が得られる. ここに $L=\frac{1}{3}D\mathrm{diag}(m,\sqrt{m},\sqrt{m})(\in \mathrm{GL}(3,\boldsymbol{R}))$ である.

定理 強さ 2 の 3 シンボル均斉配列の制約数 m の重み分布から得られる上界 $m(W)$ は, 情報行列から得られる m の上界 $m(I)$ に等しい.

すべての指標 $\mu^{(2)}_{p_0p_1p_2}$ に (i) 0,1,2 および (ii) 0,1,2,3 を与えたとき, 強さ 2 の 3 シンボル均斉配列の制約数 m の上界 $m(W)=m(I)$ のすべての組数は, 次表で与えられる:

表　3 シンボル均斉配列の制約数の組数

(i)

上界	組数
2	198
3	218
4	90
5	36
6	16
7	27
8	21
11	12
16	3
19	6
$+\infty$	101

総数 : 728

(ii)

上界	組数	上界	組数
2	975	16	42
3	1218	17	6
4	523	19	12
5	285	20	6
6	130	21	3
7	105	24	6
8	78	25	9
9	61	27	12
10	12	28	6
11	66	38	6
12	27	39	6
13	27	40	6
14	6	$+\infty$	450
15	12		

総数 : 4095

The intersection of conics on a projective plane

東京理科大学理工学部 宮本 暢子

1. はじめに

f を斉次多項式とする。$PG(n,q)$ 上で $f(\boldsymbol{x})=0$ を満たす。すべての点集合を *variety* と呼び、$V(f)$ で表わす。次に以下のような3つの条件を満たすような variety の集合 $V(f_1),V(f_2),\ldots,V(f_s)$ を考える。

(i) M は非負整数の集合とする。

(ii) $1\leq i\leq s$ に対して、$|V(f_i)|=\rho$ を満たす。

(iii) $1\leq i,j\leq s$,$i\neq j$ に対して $|V(f_i)\cap V(f_j)|\in M$ を満たす。

このような集合を *mutually M-intersecting varieties* と呼び、$\mathcal{V}(\rho,M)$ と書く。q^2 個の elliptic quadric からなる $\mathcal{V}(q^2+1,q+1)$ や、q^2 個の hyperbolic quadric からなる $\mathcal{V}((q+1)^2,3q+1)$ が、直交配列や均斉配列の構成に用いられることがわかっている [2,3]。特に $PG(2,q)$ 上の q^2+q+1 個の conic からなる $\mathcal{V}(q+1,1)$ は、*projective bundle* とも呼ばれる。

ここでは次のように定義されるある code の構成に役立つことを示す。

$(v,k,\lambda_a,\lambda_b)$ *optical orthogonal code* (OOC) C とは、次の2つの条件を満たす長さ v、重み k の $(0,1)$-sequence の集まりである。任意の $\boldsymbol{y}=(y_0,y_1,\ldots,y_{v-1}),\boldsymbol{z}=(z_0,z_1,\ldots,z_{v-1})\in C$ に対して、

(i) $\sum_{0\leq t\leq v-1}y_ty_{t+i}\leq\lambda_a$, $i\not\equiv 0 \bmod v$ を満たす。

(ii) $\sum_{0\leq t\leq v-1}y_tz_{t+i}\leq\lambda_b$ を満たす。

また、$\lambda_a=\lambda_b=\lambda$ のとき、(v,k,λ) OOC と書く。

2. 構成法

(v,k,λ) OOC が $\lfloor((v-1)(v-2)\cdots(v-\lambda))/(k(k-1)(k-2)\cdots(k-\lambda))\rfloor$ 個の符合語を持つとき、*optimal* OOC と呼ばれる。optimal $(v,k,1)$ OOC と optimal $(v,k,1)$ cyclic packing design が同値であることや、$k=3$ のときの存在、非存在についてはすでに知られている [4]。そこでより一般のパラメータを持つ OOC を構成するために、次のような mutually M-intersecting varieties を考える。

定理

Γ を $PG(n,q)$ 上の Singer group とする。$V(f_i),V(f_j)\in\mathcal{V}(\rho,M)$ に対して、$|V(f_i)\cap V(\gamma(f_i))|\leq\lambda_a$, $\gamma\in\Gamma$, かつ $|V(f_i)\cap V(f_j)|\leq\lambda_b$ を満たすならば、$\mathcal{V}(\rho,M)$ は $((q^{n+1}-1)/(q-1),\rho,\lambda_a,\lambda_b)$ OOC を構成する。

3. Projective bundle

$\pi_0=PG(2,q)$ とする。π_0 を $\pi=PG(2,q^3)$ に埋め込む。π 上の conic が π_0 と conic として交わるとき、*real conic* という。$GF(q)^3$ 上の原始既約多項式を $x^3=a_0+a_1x+a_2x^2$ とするとき、π_0 上の Singer cycle は、$\{T^i:i=0,\ldots,q^2+q\}$,

$$T=\begin{pmatrix}0&1&0\\0&0&1\\a_0&a_1&a_2\end{pmatrix}$$

として与えることができる。

既知の結果

σ を Frobenius collineation, P を π_0 の直線上にない点とする。このとき $P,P^{\sigma},P^{\sigma^2}$ を通る q^2+q+1 個の real conic が存在し、projective bundle をなす。

定理

$P=(a_0,(\alpha-a_2)\alpha,\alpha)$ とする。ただし、α は $x^3=a_0+a_1x+a_2x^2$ の原始元とする。そのとき $P,P^{\sigma},P^{\sigma^2}$ を通る q^2+q+1 個の real conic $C_0,\ldots,C_{q^2+q}$ は、

$$C_i=T^iC_0T^{i'},i=1,\ldots,q^2+q$$

と表せる。つまりこの $\mathcal{V}(q+1,1)$ は、optimal $(q^2+q+1,q+1,1)$-OOC をなす。

4. 計算結果 $(q=3)$

$$F_1=\begin{pmatrix}1&0&0\\0&0&1\\0&0&0\end{pmatrix},G_1=\begin{pmatrix}1&0&0\\0&0&1\\0&0&0\end{pmatrix},H_1=\begin{pmatrix}0&1&0\\0&0&1\\0&0&1\end{pmatrix}$$

$$F_2=\begin{pmatrix}0&1&0\\0&0&0\\0&0&1\end{pmatrix},G_2=\begin{pmatrix}1&0&1\\0&0&1\\0&0&0\end{pmatrix},H_2=\begin{pmatrix}0&1&2\\0&1&0\\0&0&0\end{pmatrix}$$

$\lambda_1F_1+\mu_1G_1+\nu_1H_1$ および $\lambda_2F_2+\mu_2G_2+\nu_2H_2$, $(\lambda_i,\mu_i,\nu_i\in GF(q),i=1,2)$ は、各々projective bundle であり、$(q^2+q+1,q+1,1)$-OOC を構成する。また、

$$|V(\lambda_1F_1+\mu_1G_1+\nu_1H_1)\cap V(\lambda_2F_2+\mu_2G_2+\nu_2H_2)|\leq 2$$

であることから、$(q^2+q+1,q+1,1,2)$-OOC を構成する。

参考文献

[**1**] R.D. Baker, J.M.N. Brown, G.L. Ebert, J.C. Fisher, Projective bundles, *Bull. Belg, Math. Soc.* 3 (1994) 329-336.

[**2**] R. Fuji-Hara and N. Miyamoto, *Balanced Arrays from Quadratic Functions* (to appear).

[**3**] R. Fuji-Hara and N. Miyamoto, *A Construction of Combinatorial arrays from Non-linear Functions*, Utilitas Math. 52 (1997), 183-192.

[**4**] J.X. Yin, Some combinatorial constructions for optical orthogonal codes, *Discrete Math.* 185 (1998) 201-219.

Optimal balanced incomplete split-block designとそのefficiency

小澤　和弘　（岐阜大学・工学部）
神保　雅一　（慶應義塾大学・理工学部）
景山　三平　（広島大学・学校教育学部）
Stanisław MEJZA　（Agricultural Univ. Poznań）

2つの要因 A と C があり，各要因はそれぞれ v_1, v_2 個の処理（水準）を持つとし，処理の集合を $A = \{A_1, \ldots, A_{v_1}\}$, $C = \{C_1, \ldots, C_{v_2}\}$ とする．各ブロックは，いずれも k_1 行 k_2 列の配列であり，行毎に要因 A の1つの処理が施され，列毎に要因 C の1つの処理が施されるものとする．また，$k_1 \leq v_1$，$k_2 \leq v_2$ とし，同一ブロック内では，どの処理も高々1度施される (binary 実験) とする．split-block design では，通常，交互作用効果に関する推定が主目的となることが多い．Ozawa et al.[?] では，split-block design における線形モデルとして，行，列に施される処理の割り当てに randomization を施し，処理の主効果，交互作用効果，およびブロック効果を母数とする下記のモデルIの混合モデルを考えた．本報告では，処理の主効果，交互作用効果を母数とし，ブロック効果を誤差の共分散に変量として組込んだ Hering and Mejza[?] で扱われているモデルと同等な混合モデル（モデルII）についても考える．

モデルI：Ozawa et al.[?] の混合モデル

$$\boldsymbol{y} = X_1\boldsymbol{\alpha} + X_2\boldsymbol{\gamma} + X_{12}(\boldsymbol{\alpha\gamma}) + X_3\boldsymbol{\beta} + \boldsymbol{\varepsilon}, \quad \mathrm{E}(\boldsymbol{\varepsilon}) = 0, \quad \mathrm{Cov}(\boldsymbol{\varepsilon}) = \sigma^2\Sigma,$$

$$\mathrm{Cov}(\varepsilon_{trc}, \varepsilon_{t'r'c'}) = \sigma^2 \times \begin{cases} 1 & t = t',\ r = r',\ c = c', \\ \rho_1 & t = t',\ r = r',\ c \neq c', \\ \rho_2 & t = t',\ r \neq r',\ c = c', \\ \rho_3 & t = t',\ r \neq r',\ c \neq c', \\ 0 & t \neq t'. \end{cases}$$

モデルII：Hering and Mejza[?] と同等の混合モデル

$$\boldsymbol{y} = X_1\boldsymbol{\alpha} + X_2\boldsymbol{\gamma} + X_{12}(\boldsymbol{\alpha\gamma}) + \boldsymbol{\varepsilon}, \quad \mathrm{E}(\boldsymbol{\varepsilon}) = 0, \quad \mathrm{Cov}(\boldsymbol{\varepsilon}) = \sigma^2\Sigma,$$

$$\mathrm{Cov}(\varepsilon_{trc}, \varepsilon_{t'r'c'}) = \sigma^2 \times \begin{cases} 1 & t = t',\ r = r',\ c = c', \\ \rho_1 & t = t',\ r = r',\ c \neq c', \\ \rho_2 & t = t',\ r \neq r',\ c = c', \\ \rho_3 & t = t',\ r \neq r',\ c \neq c', \\ \rho_4 & t \neq t'. \end{cases}$$

ただし，$\boldsymbol{y}, \boldsymbol{\varepsilon}$ は，bk_1k_2 次の観測値ベクトルと誤差ベクトルであり，$\boldsymbol{\alpha}, \boldsymbol{\gamma}$ は要因 A, C の主効果，$(\boldsymbol{\alpha\gamma})$ は要因 A，C の交互作用効果，$\boldsymbol{\beta}$ はブロック効果，X_1, X_2, X_{12}, X_3 はそれぞれ，プロットと要因 A，プロットと要因 C，プロットと交互作用効果，プロットとブロックそれぞれの間の計画行列である．また，Σ を正定値行列と仮定する．

交互作用効果 $(\boldsymbol{\alpha\gamma})$ の最小2乗推定量 $\widehat{(\boldsymbol{\alpha\gamma})}$ に対する正規方程式は，

$$C_{(\quad)}(X)\widehat{(\boldsymbol{\alpha\gamma})} = F(X)\boldsymbol{y}$$

となる．ただし，$C_{(\quad)}(X), F(X)$ ともにかなり複雑なため，詳細は省略する．

モデルI(Ozawa et al.[?]) のもとでは，要因 A および C に対していずれも釣合い型不完備ブロック計画を与える計画行列の集合を $\Xi_{(\quad)}$ としたとき，処理 A_i, $A_{i'}$, C_j, $C_{j'}$ を共に含むブロックの数が一定であ

れば，計画行列 X は $\Xi_{(\quad)}$ の中で交互作用効果 $(\boldsymbol{\alpha\gamma})$ の基本対比の推定に関して universally optimum であった．本報告では，モデル II の下においても Ozawa et al.[?] 同様な結果が得られることを示す．

定理 モデル II の計画行列 $X \in \Xi_{(\quad)}$ に対して，

$$\rho_2 + (k_2 - 1)\rho_3 - k_2\rho_4 \geq 0, \quad \rho_1 + (k_1 - 1)\rho_3 - k_1\rho_4 \geq 0$$

の 2 つの条件を満たし，$\mu(i, i'; j, j')$ が i, i', j, j' の選び方によらず一定 $(= \lambda_{22})$ であれば，計画行列 X は $\Xi_{(\quad)}$ の中で交互作用効果 $(\widetilde{\alpha\gamma})$ の基本対比の推定に関して universally optimum である．

そして，定理を満たす incomplete split-block design を balanced incomplete split-block design と呼び，BISBD(v_1, k_1; v_2, k_2; λ_{22}) と書く．

また，efficiency factor は，計画行列の良さを測るときよく利用され，以下の式で定義される．

$$E = \frac{\overline{V}_R}{\overline{V}}$$

ただし，$\overline{V}_R$ は，完全計画行列 $(v_i = k_i)$ の交互作用効果の基本対比の推定量の基本対比平均分散であり，$\overline{V}$ は，efficiency factor が測られる計画行列の交互作用効果の基本対比の推定量の基本対比平均分散である．

本報告では，この efficiency factor E を用いて，unviersally optimum な計画行列の良さを測り，さらに，universally optimum ではないが，その最適値に近い efficiency をもつ計画行列の組合せ論的特徴についても考える．

また，モデル I，II のもとで Hering and Mejza[?] の実験のデータを利用し，主効果の対比，交互作用効果の基本対比，誤差の共分散行列の各パラメータに対する MLE を求め，モデル間で比較を行う．これらの MLE を求めるために，各モデルにおいて母数に無駄があるために以下を仮定する．

仮定 I モデル I において，$\mathrm{V}(\varepsilon) = \Sigma$ の 1 個の固有値に対して

$$\sigma^2\{1 + (k_2 - 1)\rho_1 + (k_1 - 1)\rho_2 + (k_1 - 1)(k_2 - 1)\rho_3\} = 0.$$

仮定 II モデル II において，$\mathrm{V}(\varepsilon) = \Sigma$ の 1 個の固有値に対して

$$\sigma^2\{1 + (k_2 - 1)\rho_1 + (k_1 - 1)\rho_2 + (k_1 - 1)(k_2 - 1)\rho_3 + k_1k_2(b - 1)\rho_4\} = 0.$$

さらに，GLSE を用いて交互作用効果の基本対比を推定する場合と stratum を用いて交互作用効果の基本対比を推定する場合における efficiency factor を測り，efficiency fator で比較する場合の交互作用効果の基本対比の推定方法の良さについても言及する．

参考文献

[1] F. Hering and S. Mejza, Incomplete split-block designs, *Biom. J.* **39** (1995), 227-238.

[2] K. Ozawa, M. Jimbo, S. Kageyama and S. Mejza, Optimality and Construction of Incomplete Split-block Designs, submitted.

Some series of balanced bipartite block designs

岐阜大学工学部応用情報学科　三嶋 美和子
國立交通大學應用數學系 (台湾)　傅 恆霖

In a recent paper of Mishima, Jimbo and Kageyama [?], a special type of balanced bipartite block designs $(V_1, V_2, \mathcal{B})$ was discussed, which satisfies the following conditions. Let V_1 be a set of v_1 points, V_2 be another set of v_2 points and $\mathcal{B}$ be a collection of k-subsets, called *blocks* (*superblocks*), of $V_1 \cup V_2$.

(i) The pair $(V_i, \mathcal{B}_i)$ forms a balanced incomplete block (BIB) design with parameters v_i, b, r_i, k_i, λ_i for $i = 1, 2$, where $\mathcal{B}_i = \{B \cap V_i \mid B \in \mathcal{B}\}$;

(ii) each pair of points in $V_1 \times V_2$ occurs exactly λ_3 subsets of $\mathcal{B}$;

(iii) each superblock of $\mathcal{B}$ is divided into a k_1-subset of V_1 and a k_2-subset of V_2, i.e., $k = k_1 + k_2$.

Conforming to [?], such a design $(V_1, V_2, \mathcal{B})$ is simply called a balanced bipartite block design with parameters v_1, v_2, b, r_1, r_2, k_1, k_2, λ_1, λ_2, λ_3. By conditions (i), (ii) and (iii), it is easy to see that the parameters satisfy the following:

$$r_1 = \frac{v_2\lambda_3}{k_2} = \frac{(v_1-1)\lambda_1}{k_1-1}, \qquad r_2 = \frac{v_1\lambda_3}{k_1} = \frac{(v_2-1)\lambda_2}{k_2-1},$$

$$b = \frac{r_1 v_1}{k_1} = \frac{r_2 v_2}{k_2} = \frac{v_1 v_2 \lambda_3}{k_1 k_2}.$$

For such a design, some constructions have been given by Sinha and Kageyama [?], and Mishima, Jimbo and Kageyama [?]. The most basic construction would be one in [?], which is regarded as a direct product of blocks in two initial BIB designs. But it is possible that a balanced bipartite block design with lesser number of superblocks exists.

Then what is a lower bound of the number of superblocks of a balanced bipartite block design? An answer to the question was given in [?] as follows:

Theorem 1 *If there exists a balanced bipartite block design with parameters v_1, v_2, b, r_1, r_2, k_1, k_2, λ_1, λ_2, λ_3, then b is divisible by*

$$\frac{4}{d_1 d_2 d_3}\binom{v_1}{2}\binom{v_2}{2}, \tag{1}$$

that is, (??) is a lower bound of b, where

$$d_1 = \gcd(k_2(v_1-1), (k_1-1)v_2), \qquad d_2 = \gcd(k_1(v_2-1), (k_2-1)v_1),$$
$$d_3 = \gcd\left(\frac{k_2(v_1-1)}{d_1}, \frac{k_1(v_2-1)}{d_2}\right).$$

It is natural that the reader wonders with what parameters a balanced bipartite block design attains the lower bound of Theorem ??. In this talk, we will consider the most primary case, i.e., $k_1 = k_2 = 2$, and show the following theorem by using the method of graph decomposition.

Theorem 2 (Main Theorem) *Let $v_1 \le v_2$. In the case when $k_1 = k_2 = 2$, if $v_1 = 3, 4, 5, 6, 7$, then there exists a balanced bipartite block design such that the number of superblocks attains the lower bound of Theorem ??, irrespective of v_2.*

A balanced bipartite block design with parameters v_1, v_2, b, r_1, r_2, $k_1 = k_2 = 2$, λ_1, λ_2, λ_3, is expressed as a graph

$$\lambda_1 K_{v_1} \cup \lambda_2 K_{v_2} \cup \lambda_3 K_{v_1, v_2} \tag{2}$$

which can be decomposed into b K_4's, where K_v is a complete graph on v vertices. In this case,

$$\lambda_1\binom{v_1}{2} = \lambda_2\binom{v_2}{2} = \frac{\lambda_3 v_1 v_2}{4}$$

holds. Since λ_3 is determined by λ_1 and λ_2, a graph of type (??) is simply denoted by $\lambda_1 K_{v_1} \vee \lambda_2 K_{v_2}$ hereafter. Minimizing the number of superblocks is equivalent to minimizing λ_1 and λ_2 under given v_1 and v_2, which allows us to restate Theorem ?? as follows:

Theorem 3 *If there exists a balanced bipartite block design with parameters v_1, v_2, b, r_1, r_2, k_1, k_2, λ_1, λ_2, λ_3, then a lower bound of b is*

$$\frac{t}{g}\binom{v_1}{2}\binom{v_2}{2},$$

where $g = \gcd\left(\binom{v_1}{2}, \binom{v_2}{2}\right)$ and t is the smallest integer for $\lambda_3 = t(v_1-1)(v_2-1)/g$ to be an integer. In this case, $\lambda_1 = t\binom{v_2}{2}/g$ and $\lambda_2 = t\binom{v_1}{2}/g$.

¿From Theorem ??, we have only to consider v_2 modulo $v_1(v_1-1)$ and Theorem ?? can be established by the following lemmas and propositions.

Lemma 4 *Let $\delta = 2$ if u is even, otherwise $\delta = 1$. Then a graph $\lambda_1 K_u \vee \lambda_2 K_v$ can be decomposed into b K_4's when $\lambda_1 = 2s\binom{v}{2}/(\delta(u-1))$ and $\lambda_2 = su/\delta$ for some integer s such that $s\binom{v}{2}$ is divisible by $\delta(u-1)/2$. In this case, $b = su\binom{v}{2}/\delta$.*

Lemma 5 *Let u be an odd integer. Further let $\delta = 2$ if $(u-1)/2$ is even, otherwise $\delta = 1$. Then a graph $\lambda_1 K_u \vee \lambda_2 K_v$ can be decomposed into b K_4's when $\lambda_1 = s\binom{v}{2}/(\delta u)$ and $\lambda_2 = s(u-1)/(2\delta)$ for some integer s such that $s\binom{v}{2}$ is divisible by $\delta u/2$. In this case, $b = s(u-1)\binom{v}{2}/(2\delta)$.*

A set of pairwise independent edges of a graph G is called a *matching* in G. A matching M in G is said to be *perfect* if every vertex of G is incident with an edge of M.

Proposition 6 *A complete graph K_{10} can be decomposed into five subgraphs on six vertices, each of which consists of three perfect matchings.*

Lemma 7 *Let F be a 1-factor in a graph on six vertices and let G be another graph on six vertices consisting of three perfect matchings. Then $3F \vee G$ can be decomposed into 9 K_4's.*

Lemma 8 *Let F be a 1-factor in a graph on six vertices. Then $2F \vee K_4$ can be decomposed into 6 K_4's.*

Proposition 9 *Let u and v be integers divisible by 3. Then a bipartite graph $K_{u,v}$ can be decomposed into $uv/9$ $K_{3,3}$'s.*

Lemma 10 *Let F be a 1-factor in a graph on six vertices. Then $3F \vee K_{3,3}$ can be decomposed into 9 K_4's.*

Lemma 11 *For some positive integer $n < 10$, let $v \equiv 3n+1 \pmod{30}$ and assume that $(n(3n+1)/10)K_6 \vee K_{3n+1}$ can be decomposed into $3n(3n+1)/2$ K_4's. Then $(v(v-1)/30)K_6 \vee K_v$ can be decomposed into $v(v-1)/2$ K_4's.*

Acknowledgements

The first author was supported by the Inamori Foundation and Grant-in-Aid for Encouragement of Young Scientists, the Ministry of Education, Science, Sports and Culture under Contract Number 11780169.

References

[1] M. Mishima, M. Jimbo and S. Kageyama, Constructions for a certain type of balanced bipartite block designs, J. Statist. Plann. Inference, to appear.

[2] K. Sinha and S. Kageyama, Further constructions of balanced bipartite block designs, Utilitas Math. **38** (1990), 155–160.

Nested row and column design の構成法

岐阜大学工学部 菱田 隆彰
慶應義塾大学理工学部 神保 雅一

For a set V of v *points*, let $\mathcal{A}$ be a set of $k_1 \times k_2$ arrays called *blocks*, whose entries are elements of V. We denote the number of blocks of $\mathcal{A}$ in which two distinct points i and j occur in the same row, in the same column, and in the same block by $\lambda_R(i,j)$, $\lambda_C(i,j)$ and $\lambda_B(i,j)$, respectively. The pair $(V,\mathcal{A})$ is called a *balanced incomplete block design with nested rows and columns*, denoted by $BIBRC(v,b,r,k_1,k_2,\lambda)$, or *BIBRC* for short, if the following conditions are satisfied :

(i) Every point occurs at most once in each block of $\mathcal{A}$.
(ii) Every point occurs in exactly r blocks of $\mathcal{A}$.
(iii) For any pair of points (i,j),

$$\lambda = k_1\lambda_R(i,j) + k_2\lambda_C(i,j) - \lambda_B(i,j)$$

is a constant independent of the pair of points (i,j).

Moreover, if $v = k_1k_2$ then $(V,\mathcal{A})$ is called a balanced *complete* block design with nested rows and columns, which is denoted by $BCBRC(v,b,r,k_1,k_2,\lambda)$ or *BCBRC* for short. The notion of BIBRC was introduced by Singh and Dey (1979, *Biometrika*, **54**, 479-486).

In this talk, we shall show some constructions of a completely balanced BIBRC or a BCBRC by utilizing the method of differences. The construction given in this paper includes those of Uddin and Morgan (1990, *Biometrika*, **77**, 193-202) as special cases. Furthermore, we shall compare the designs constructed by our Theorem with that of Jimbo and Kuriki (1983, *Ars Combinatoria*, **16**, 275-285) and shall show that, under some conditions, our methods generate BIBRC's with fewer replication number than theirs.

Theorem 1 *If there exist*

(i) *a completely balanced* $BIBRC(v,b,r,k_1,k_2,\lambda)$,

(ii) *a completely balanced* $BIBRC(v',b',r',k_1,k_2,\lambda\lambda')$,

(iii) *an* $OA(\lambda'v'^2,k_1k_2,\lambda')$,

then there exists a completely balanced $BIBRC(vv',\ \lambda'v'^2b+vb',\ \lambda'v'r+r',\ k_1,k_2,\ \lambda\lambda')$.

Theorem 2 *Let* $v = mpqf+1$ *be a prime power, where* $\gcd(p,q)=1$. *Let* α *be a primitive element of* $V = GF(v)$ *and* $\theta = \alpha^m$. *We write* $\alpha^{u_i} = 1-\theta^i$ *for* $i = 1,\cdots,pqf-1$.

(i) *If there exists an integer* u *such that* $u \not\equiv u_i - u_j \pmod m$ *for any* $i,j = 1,\cdots,pqf-1$, *then there exists a completely balanced BIBRC with parameters*

$$v = mpqf+1, \quad b = mav, \quad r = mak_1k_2,$$
$$k_1 = pf, \quad k_2 = qf, \quad \lambda = af(pf-1)(qf-1),$$

where $a = p$ *and* q.

(ii) *If there exists an integer* u *such that* $u \not\equiv -u_i$, $u \not\equiv u_i - u_j \pmod{m}$ *for any* $i, j = 1, \cdots, pqf - 1$, *then there exists a completely balanced BIBRC with parameters*

$$v = mpqf + 1, \quad b = mqv, \quad r = mqk_1k_2,$$
$$k_1 = pf, \quad k_2 = qf + 1, \quad \lambda = qf(pf - 1)(qf + 1).$$

Moreover, in Theorem **??**, If pqf is odd and m is even, then we can obtain a BIBRC's with half repication number.

Theorem 3 *Let* $v = 2pqfm + 1$ *be a prime power,* α *be a primitive element of* $GF(v)$ *and* $\theta = \alpha^{2m}$. *We write* $\alpha^{w_i} = 1 - \theta^{qi}$ *and* $\alpha^{u_j} = 1 - \theta^{pj}$ *for* $i = 1, 2, \cdots, pf - 1$ *and* $j = 1, 2, \cdots, qf - 1$.

(i) *If there exists an integer* u *such that* $u \not\equiv 0, u_j - w_i \pmod{m}$ *for any* i *and* j, *then there exists a completely balanced BIBRC with parameters*

$$v = 2pqfm + 1, \quad b = 2pqmv, \quad r = 2pqmk_1k_2,$$
$$k_1 = pf, \quad k_2 = qf, \quad \lambda = pqf(pf - 1)(qf - 1).$$

(ii) *If there exists an integer* u *such that* $u \not\equiv 0, -w_i, u_j - w_i \pmod{m}$ *for any* i *and* j, *then there exists a completely balanced BIBRC with parameters*

$$v = 2pqfm + 1, \quad b = 2pqmv, \quad r = 2pqmk_1k_2,$$
$$k_1 = pf, \quad k_2 = qf + 1, \quad \lambda = pqf(pf - 1)(qf + 1).$$

(iii) *If there exists an integer* u *such that* $u \not\equiv 0, u_j, -w_i, u_j - w_i \pmod{m}$ *for any* i *and* j, *then there exists a completely balanced BIBRC with parameters*

$$v = 2pqfm + 1, \quad b = 2pqmv, \quad r = 2pqmk_1k_2,$$
$$k_1 = pf + 1, \quad k_2 = qf + 1, \quad \lambda = pqf(pf + 1)(qf + 1).$$

Moreover if pqf *is odd then there exists a completely balanced BIBRC with the following parameters corresponding to* (i), (ii), (iii)*:*

(i)' $v = 2pqfm + 1$, $b = pqmv$, $r = pqmk_1k_2$, $k_1 = pf$, $k_2 = qf$, $\lambda = \frac{1}{2}pqf(pf - 1)(qf - 1)$.
(ii)' $v = 2pqfm + 1$, $b = pqmv$, $r = pqmk_1k_2$, $k_1 = pf$, $k_2 = qf + 1$, $\lambda = \frac{1}{2}pqf(pf - 1)(qf + 1)$.
(iii)' $v = 2pqfm + 1$, $b = pqmv$, $r = pqmk_1k_2$, $k_1 = pf + 1$, $k_2 = qf + 1$, $\lambda = \frac{1}{2}pqf(pf + 1)(qf + 1)$.

参考文献

[1] M. Jimbo and S. Kuriki (1983). Constructions of nested designs, *Ars Combinatoria*, **16**, 275-285.

[2] D. A. Preece (1967). Nested balanced incomplete block designs, *Biometrika*, **54**, 479-486.

[3] M. Singh and A. Dey (1979). Block designs with nested rows and columns, *Biometrika*, **66**, 321-326.

[4] N. Uddin and J. P. Morgan (1990). Some constructions for balanced incomplete block designs with nested rows and columns, *Biometrika*, **77**, 193-202.

グラフのカットについて

工学院大学工学部 金子篤司
日本大学理工学部 善本　潔

Gを連結グラフとし、Sを$V(G)$の部分集合とする。$G-S$が非連結のとき、SはグラフGのカットと呼ばれる。さらに、SがGの独立点集合である（Sの内部にGの辺がない！）とき、SをGの独立カットという。最近、G.Chenらは次の定理を証明した。以下、nをグラフGの位数とする。

定理 A [1]　Gを連結グラフとする。このとき$|E(G)| \leq 2n-4$ならば、Gには独立カットが存在する。

$K_{n-2,2}$の2点から成る部集合に一辺を加えたグラフは、$2n-3$辺を持ち、独立カットを持たない。従って、上記の$2n-4$を$2n-3$で置き換える事はできない。

証明の概略

Gがカット点xを持てば、xが所望の独立カットとなるので、以下の命題(*)を証明すればよい。

命題(*)　Gを2－連結グラフとし、xをGの頂点とする。このとき$|E(G)| \leq 2n-4$ならば、Gには独立カットSでxを含まないものが存在する。

xの隣接点集合$N_G(G)$内に辺yzがあるとしてよい。ここで、辺xyを縮約するとGの辺が少なくとも2辺以上減少する事に注意し、辺xyの縮約がGの2－連結性を保存するかどうかで場合を分け、帰納法を用いればよい。

G.Chenらは独立カットの大きさを制限する方向で研究を続けているようであるが、ここでは別の視点からこの定理の周辺を見てみたい。

予想 1　Gを連結グラフとする。このとき$|E(G)| \leq 3n-7$ならば、GのカットSで、Sで誘導されるGの部分グラフがサイクルを持たないもの（林カット）が存在する。

以下の場合に、この予想は正しい。

（1）Gが平面グラフであるとき、
（2）Gにすべての頂点と隣接する頂点（次数$n-1$の頂点）があるとき。

$K_{n-3,3}$の3点から成る部集合に3辺を加えたグラフは、$3n-6$辺を持ち、林カットを持たない。従って、上記の$3n-7$を$3n-6$で置き換える事はできない。

問題 2　Gを連結グラフとする。このときGのすべての極小カットが独立カットになっているグラフを特徴づけよ。

問題 3　Gを連結グラフとする。このときGのどのカットも独立カットではないグラフを特徴づけよ。

以下は、G の最小次数の点 x と $N_G(x)$ 内の G の辺を考えれば明らかである。

Fact 4　G を完全グラフではない連結グラフとする。このとき (G の辺数にかかわらず)G のカット S で、$\frac{|E(G(S))|}{|S|} < \frac{|E(G)|}{n}$ を充たすものが常に存在する。

定理 A や予想 1 から考えるともう少し強い事が言えるかもしれない。

問題 5　G を位数 n が十分に大きな連結グラフとする。このとき、$|E(G)| \leq kn - c$ (c: 定数、$k \geq 2$) ならば、G のカット S で $|E(G(S))| \leq (k-2)n$ となるものが存在するか。

1 点を切り出すカット（各点の近傍）に関しては、以下の定理が証明される。

定理 6　G を連結グラフとする。このとき、$|E(G)| \leq \frac{3}{2}n - 2$ ならば、G の点 x で $N_G(x)$ が G の独立点集合となるものが存在する。

定理 7　G を連結グラフとする。このとき、$|E(G)| \leq 2n - 3$ ならば、G の点 x で $N_G(x)$ 内に G のサイクルが存在しないものがある。

参考文献

[1] Guantao Chen and Xingxing Yu, A note on fragile-graphs, preprint.

Radial Perfect Partitions of Convex Sets in the Plane

J. Akiyama (Tokai University), A. Kaneko (Kogakuin University),
M. Kano (baraki University), G. Nakamura (Tokai University),
E. Rivera-Campo (Universidad Autónoma Metropolitana),
S. Tokunaga (Tokyo Medical and Dental University) and
J. Urrutia (University of Ottawa)

The problem studied in this paper arises from a simple practical problem: how to divide a cake among the children attending a birthday party in such a way that every child gets the same amount of cake and the same amout of icing (exposed area), where only the top and sides of the cake are iced [1]. If the height of the cake is constant, then the above problem can be said as follows. Let S be a convex set in the plane, which corresponds to the base of the cake. Then is it possible to partition S into n convex subsets so that each subset has the same area and the same boundary length of S. If such a partition exists, we say that S can be *perfectly partitioned* into n convex subsets, and call this partition a *perfect n-partition* (see Figure 1). In this paper we deal with a perfect n-partition that is obtained by n rays emanating from the same point in S. We call such a special perfect n-partition a *radial perfect n-partition*, and if S has a radial perfect n-partition, then we say that S is *radially perfectly partitioned* into n convex subsets (see Figure 1).

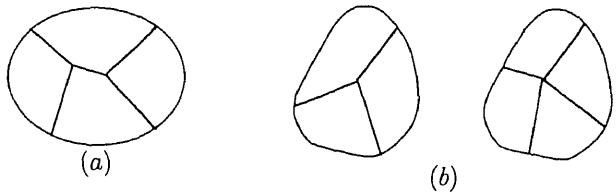

Figure 1: (a) A perfect 4-partition; (b) Radial perfect 3 and 4-partitions.

Theorem 1 *A convex polygon P in the plane has a radial perfect n-partition for every $n \geq 2$ if and only if P is a circumscriptible polygon (i.e., a polygon that contains a circle tangent to all its edges.) In particular, every triangle has a radial perfect n-partition for every n (see Figure 2).*

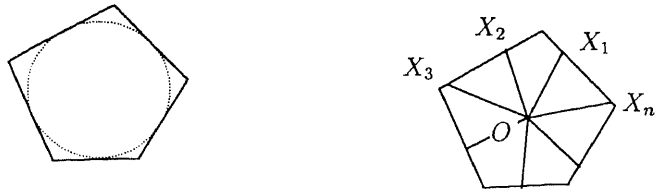

Figure 2: a circumscriptible polygon.

Theorem 2 *Every convex set S in the plane can be radially perfectly partitioned into three convex subsets (see Figure 1).*

Theorem 3 *Let S be a convex set in the plane possessing the property that for every* $\mathrm{lune}(XY)$ *with* $\ell(\mathrm{arc}(XY)) = \ell(\partial(S))/4$, *it follows that* $\mathrm{area}(\mathrm{lune}(XY)) < \mathrm{area}(S)/4$. *Then S can be radially perfectly partitioned into four convex subsets (see Figures 1).*

Theorem 4 *Every convex set S in the plane can be perfectly partitioned into n convex subsets for every $n \geq 3$ (see Figure 1).*

In order to prove the above theorems, we need some lemmas. We show some of these lemmas.

Lemma 5 *Let $\triangle ABC$ be a triangle in the plane such that $\angle B \geq \angle C$, and let X, Y and Z be points on AC, AB and AB, respectively, such that $|CX| + |XY| + |YB| = |CZ| + |ZB|$ (see* Figure 2*). Then*

$$\mathrm{area}(\triangle ZBC) < \mathrm{area}(\mathrm{quad}(XYBC)).$$

Lemma 6 *Let S be a convex set in the plane, and P_1, P_2, P_3 be three points on $\partial(S)$ such that $\ell(\mathrm{arc}(P_1P_2)) = \ell(\mathrm{arc}(P_2P_3)) = \ell(\mathrm{arc}(P_3P_1))$. Then for at least two $i \in \{1,2,3\}$, we have* $\mathrm{area}(\mathrm{lune}(P_iP_{i+1})) < \mathrm{area}(S)/3$, *where $P_4 = P_1$.*

References

[1] J. Akiyama, G. Nakamura, E. Rivera-Campo, and J. Urrutia, Perfect division of a cake, *Proceedings of the Tenth Canadian Conference on Computational Geometry*, 114-115.

[2] J. Goodman and J. O'Rourke, *Handbook of Discrete and Computational Geometry*, CRC Press, (1997)

[3] A. Kaneko and M. Kano, *Perfect n-partitions of convex sets in the plane*, submitted.

Steiner Pentagon Covering Designs

F. E. Bennett
Department of Mathematics
Mount Saint Vincent University
Halifax, Nova Scotia B3M 2J6, Canada

(joint work with R.J.R. Abel, H. Zhang and L. Zhu)

1 Introduction and Summary

Let K_n be the complete undirected graph on n vertices. A *pentagon system* (PS) of order n is a pair $(K_n, \mathcal{B})$, where $\mathcal{B}$ is a collection of edge disjoint pentagons which partition the edges of K_n. A *Steiner pentagon system* (SPS) of order n is a pentagon system $(K_n, \mathcal{B})$ with the additional property that every pair of vertices are joined by a path of length 2 in exactly one pentagon of $\mathcal{B}$. It is known (Lindner and Stinson, 1984) that the spectrum of SPSs is precisely the set of all $n \equiv 1$ or $5 \ (mod\ 10)$, except $n = 15$ for which no such system exists. For other values of n, we have Steiner pentagon covering and packing designs.

A *Steiner pentagon covering* (SPC) of order n is a pair $(K_n, \mathcal{B})$, where $\mathcal{B}$ is a collection of pentagons from K_n such that any two vertices are joined by a path of length 1 in at least one pentagon of $\mathcal{B}$, and also by a path of length 2 in at least one pentagon of $\mathcal{B}$. It is well known that any SPS of order n gives a BIBD on n points with block size $k = 5$ and index $\lambda = 2$. Similarly, an SPC of order n may lead to a usual covering on n points with $k = 5$ and index $\lambda = 2$. It is known that such a covering contains at least

$$c(n) = \lceil \tfrac{n}{5} \lceil \tfrac{n-1}{2} \rceil \rceil$$

blocks. If an SPC(n) contains the minimum number of $c(n)$ pentagons, we call it a *Steiner pentagon covering design* (SPCD), denoted by SPCD(n).

It is clear that an SPS(n) is also an SPCD(n), which is known to exist for $n \equiv 1, 5 \ (mod\ 10)$ and $n \neq 15$.

Theorem 1.1 *For any positive integer $n \equiv 1$ or $5 \ (mod\ 10)$, there exists an SPCD(n), except for $n = 15$.*

The following results are also known from earlier investigations:

Theorem 1.2 *For any positive integer* $n \equiv 7 \pmod{10}$, *there exists an SPCD*(n) *except possibly when* $n = 17, 27, 37, 47, 67$ *or* 77.

Theorem 1.3 *For any positive integer* $n \equiv 9 \pmod{10}$, *there exists an SPCD*(n) *except possibly when* $n = 9, 19, 29, 49, 69, 79, 89, 99, 109, 119, 129, 139, 149, 159, 169,$ *or* 189.

The main purpose of this paper is to investigate the existence of SPCDs. Since there are above known results for odd orders, we shall focus on the existence of SPCDs when n is even. The following result is established in this paper:

Theorem 1.4 *For any even integer* $n \geq 6$, *there exists an SPCD*(n) *except possibly for* $n \in D$, *where* D *contains the integers in the following table:*

$n \pmod{10}$	n
0	*none*
2	$22, 42, 82$
4	$14, 74$
6	*none*
8	$18, 28, 38$

We also give some improvements to the known results of Theorems $1.2 - 1.3$ as follows.

Theorem 1.5 *For any positive odd integer* $n \not\equiv 3 \pmod{10}$, *there exists an SPCD*(n) *except for* $n = 9, 15$ *and possibly for* $n \in F$, *where* F *contains the integers in the following table:*

$n \pmod{10}$	n
1	*none*
5	*none*
7	$27, 37$
9	$19, 29, 119, 139, 159$

Wide-diameter of graphs

Kiyoshi Ando
University of Electro-Communications, Chofu, Tokyo, JAPAN

1. Introduction

In this note we consider a generalized distance arising from a system of k internally disjoint (edge disjoint) paths in a graph. In some situation, systems consisting of long paths may not be of any use, so it is natural to consider systems consisting only of paths of bounded length. We deal only finite graphs with no self-loops. Let $V(G)$ and $E(G)$ denote the vertex set and the edge set of a graph G, respectively. Let P be a path in G. We define the length of P by the number of edges of P and denote it by $len(P)$. Each vertex of degree 2 in $V(P)$ is called an internal vertex of P and we denote the set of internal vertices of P by $Int(P)$. Let P and P' be paths in G. If $V(P) \cap V(P') = \emptyset$, then we say P and P' are disjoint. Similarly, if $E(P) \cap E(P') = \emptyset$, then we say P and P' are edge disjoint. If $Int(P) \cap Int(P') = \emptyset$, then we say P and P' are internally disjoint.

Let G be a connected graph and let k be a positive integer. Let U and W be subsets of $V(G)$. A *Menger path system* $\mathcal{P}_k(U,W)$ of width k between U and W is a set of k internally disjoint paths between U and W. The maximum value of the lengths of paths in $\mathcal{P}_k(U,W)$ is said to be the length of $\mathcal{P}_k(U,W)$ and is denoted by $len(\mathcal{P}_k(U,W))$. A Menger path system $\mathcal{P}_k(U,W)$ is said to be disjoint if any pair of paths in it are mutually disjoint. Let $u \in V(G)$ and $W \subset V(G)$ such that $|W| = k$. A $(u,W)-fan$ is a Menger path system $\mathcal{P}_k(\{u\},W)$ such that all end vertices of paths in it other than u are distinct. In the case that both U and W are singleton, say $U = \{u\}$ and $W = \{w\}$, we write $\mathcal{P}_k(u,w)$ for $\mathcal{P}_k(\{u\},\{w\})$. Sometimes a Menger path system $\mathcal{P}_k(u,w)$ is called a container of width k and denoted by $C(u,w)$ ([?]).

We define the k-wide-distance $d_k(u,w)$ between u and v as follows.

$$d_k(u,w) = \begin{cases} 0 & \text{if } u = w \\ \infty & \text{if there is no Menger path system of width } k \\ & \text{between } u \text{ and } w \\ \min\{len(\mathcal{P}_k(u,w))\} & \text{otherwise} \end{cases}$$

The maximum value of $d_k(u,w)$ in G is called the k-wide-diameter of G and is denoted by $d_k(G)$. Using edge disjoint paths instead of internally disjoint paths, we can define an *edge version Menger path system*. The edge version k-wide-distance $d_k^e(u,v)$ and the edge version k-wide-diameter $d_k^e(G)$ are defined similarly.

By definition we observe that $d_1(u,v) = d_1^e(u,v)$ is the distance between u and w. So, each of the k-wide-distance and the edge version k-wide-distance is a generalization of the distance in a graph. The concepts of Menger path system, wide-distance, and wide-diameter are arising quite naturally from the study of transmission delay, reliability, and fault tolerance in interconnection networks for parallel and distributed computer systems.

Many sufficient conditions for a graph to have the given wide-diameter were investigated by Faudree et al. [?], [?].

Some lower bounds on the number of edges in a graph with edge version wide-diameter 2 or 3 were given [?].

For a fixed positive integer k, edge version k-wide diameter of a k-edge connected graph with diameter d is bounded by a polynomial of d of which degree is k [?].

In this note we give some results on fan, cycle and path.

2. Fan, cycle and path

Let k be a positive integer and let G be a k-connected graph. Let u be a vertex in G and let X and Y be subsets of $V(G)$ such that $|X| = |Y| = k$. Then Menger's theorem assures us that there exist the followings in G.

(i) A (u,X)-fan.

(ii) A cycle containing all vertices in X.
(iii) A disjoint Menger path system between X and Y.

Now we give some results on the relation between the wide-diameter of G and the lengths of fans, cycles and path systems in a k-connected graph. Note that Menger's theorem itself gives us no information about the lengths of them.

Theorem 1 ([?]) Let $k \geq 2$ and $d \geq 1$ be integers and let G be a k-connected graph. Let u be a vertex in G and let X be a subset of $V(G)$ such that $|X| = k$. If the wide-diameter of G is d, then there is a (u, X)-fan $\mathcal{P}_k(u, X)$ such that

$$len(\mathcal{P}_k(u, X)) \leq \max\{d, (k-1)d - 4k + 7\}.$$

Theorem 2 ([?]) Let $k \geq 3$ and $d \geq 2$ be integers. Let G be a graph with the wide-diameter d. Then for any k distinct vertices in G, there is a cycle C containing these k vertices such that

$$|E(C)| \leq 2(k-3)(d-1) + \max\{3d, \lfloor \frac{18d-16}{5} \rfloor\}.$$

Theorem 3 ([?]) Let $k \geq 3$ and $d \geq 1$ be integers. Let G a graph with the wide-diameter d. Then for any given two subsets X and Y such that $|X| = |Y| = k$, there is a disjoint Menger path system $\mathcal{P}_k(X, Y)$ such that

$$len(\mathcal{P}_k(X, Y) \leq \begin{cases} d & \text{if } d \leq 3 \\ k+1 & \text{if } d = 4 \\ (k-2)(k+1)d/2 - 2(k^2 - k - 4) & \text{if } d \geq 4 \end{cases}$$

References

[1] Ando, K. , Egawa, Y., The number of edges in a graph with edge version wide-diameter 2 or 3, *Combinatorics, Graph Thery, and Algorithm: Proceedings of the Eighth Quadrennial International Conference on Graph Theory, Combinatorics, Algorithm, and Applications*, Edited by Alavi, Lick and Schwenk, , **Vol. 1**, (1999), 43 - 58.

[2] Ando, K. , Kaneko, A., 2-wide diameter of 2-edge connected graph with diameter d, preprint.

[3] Faudree, R. J. , Some Strong Variations of Connectivity, *Combinatorcs,* Paul Erdös *is Eighty* , Vol. **1**, Edited by Miklós, Sós and Szöyi, (1993), 125 - 144.

[4] Faudree, R. J. , Jacobson, M. S., Ordman, E. T., Shelp, R. H., and Tusa, Zs., Menger's Theorem and Short Paths, *J. Combin. Math. Combin. Comp.* , **2**, (1987), 235 - 253.

[5] Faudree, R. J., Gould, R. J., and Shelp, R. H., Menger Path Systems, *J. Combin. Math. Combin. Comp.* , **6**, (1989), 235 - 253. Hsu, D. F., On Container Width and Length in Graphs, Groups and Networks, *IEICE TRANS. FUNDAMENTALS*, Vol. **E77-A**, No. 4 (1995), 668-680.

[6] Kojima, T., Ando, K., Minimum length of cycles through specified vertices in graphs with wide-diameter at most d, *Ars Combinatoria*, to appear.

[7] Kojima, T., Ando, K., Wide-diameter and minimum length of fan, *Theoretical Computer Science*, to appear.

[8] Kojima, T., Ando, K., Wide-diameter and minimum length of disjoint Menger path system, preprint.

[9] Kojima, T., Ando, K., Kaneko, A., Edge version wide-diameter of graphs with diameter d, preprint.

2因子とハミルトンサイクル

金子　篤司（工学院大）
善本　　潔（日大理工）

2-正則全域部分グラフを **2-factor (2-因子)** という．特に、連結成分が一つの時はハミルトンサイクルになる．与えられたグラフの最小次数がその位数の半分より大きいとき、Dirac [?] はそのグラフがハミルトンサイクルをもつこと示している．この結果を Brandt [?] らが以下のように一般化した．

Theorem 1 (Brandt et al.) グラフ G の最小次数が $|V(G)|/2$ より大きいとき、任意の $k \leq n/4$ なる整数 k に対して、G は成分を k 個持つ *2-factor* を含む．

江川ら [?] の定理から、グラフの任意の辺を一本指定したとき、ある例外を除いてその辺を通るようにハミルトンサイクルを取れることがわかる．

Theorem 2 (Egawa et al.) グラフ G の最小次数が $|V(G)|/2$ より大きいとし、xy を G の任意の辺とする．このとき、次の例外を除いてその辺を含むハミルトンサイクルがある．

1. G の位数は偶数で、頂点 x, y を含む $|V(G)|/2$ 個の頂点からなる点集合 S が存在し、$G - S$ は辺を持たない．*i.e.*, G は適当な $L \subset K_{\frac{n}{2}}$ に対して、$\overline{K_{\frac{n}{2}}} + L$ と同型．
2. $G - \{x, y\}$ は非連結である．*i.e.*, G は $K_{\frac{|V(G)|}{2}-1} + xy + K_{rac|V(G)|2-1}$ と同型．

我々は、さらに指定された辺を通るような 2 成分からなる 2-factor が存在することを示した [?].

Theorem 3 グラフ G の最小次数が $|V(G)|/2$ より大きいとし、xy を G の任意の辺とする．このとき、次の例外を除いてその辺を含む *2* 成分からなる *2-factor* がある．

1. G の位数は偶数で、頂点 x, y を含む $|V(G)|/2$ 個の頂点からなる点集合 S が存在し、$G - S$ は辺を持たない．
2. 位数が高々 *8* の例外グラフのいずれかと同型である．

例外 2 の位数は高々8 であり、それ以上大きいグラフが指定された辺を通る 2-factor を持つための必要十分条件は例外 1 が成り立たないことである．したがってこれらの結果から、自然 Brandt らの結果はより拡張できることが予想される．

Conjecture 1 グラフ G が十分な位数を持ち、最小次数がその半分より大きいとする．このとき 例外1 を除いて、任意の $k \leq n/4$ なる整数 k に対して、G は任意に指定された一辺を含むような k 成分からなる *2-factor* を持つ．

我々は最初、Faudree [?] らの「最小次数 5 以上のハミルトングラフは、2 成分からなる 2-factor を持つか」という問題の反例を作ろうと試み、その失敗の副産物として上の結果を得た．定理 **??**から直ちに次の系が得られる．

Corollary 4 グラフ G の最小次数が $|V(G)|/2$ より大きいとし、x, y を G の任意の *2* 頂点とするとする．このとき、次の例外を除いて x, y を端点とするパス P が存在し、$G - V(P)$ はハミルトンになる．

1. G の位数は偶数で、頂点 x, y を含む $|V(G)|/2$ 個の頂点からなる点集合 S が存在し、$G - S$ は辺を持たない．
2. 位数が高々 *8* の例外グラフのいずれかと同型である．

もし上の例外1がxとyを端点とするハミルトンパスを持てば、それを三つ数珠繋ぎすることによって位数が大きいFaudreeらの問題の反例ができるが、上で欲しているパスを持たない理由と同じ理由から、そのようなハミルトンパスもない.

一方、任意の2頂点を隣接させないようにハミルトンサイクルをとることは容易であり、さらに次の主張を示すことも比較的やさしい.

Fact 1 グラフGの最小次数が$|V(G)|/2$より大きいとする. このとき、高々$n/4$個からなる頂点集合のどの2頂点も隣接させないようにハミルトンサイクルをとることが出来る.

我々[?]は、より一般に以下の主張を示すことが出来た.

Theorem 5 グラフGの最小次数が$|V(G)|/2$より大きいとし、dを高々$n/4$の整数とする. このとき、高々$n/2d$個の任意の頂点部分集合に対して、そのどの2頂点も距離dだけ離れているようにハミルトンサイクルをとることが出来る.

但し、2頂点間の距離は辺の数で定義する. $d=1$の場合が上のFact 1に対応している.

参考文献

[1] S. Brandt, G. Chen, R. J. Gould and L. Lesniak, *Degree conditions for 2-factors*, J. Graph Theory 24 (1997) 165-173

[2] G. A. Dirac, *Some theorems on abstract graphs*, Proc. London Math. Soc. 2 (1952) 69-81

[3] Y. Egawa, R.J. Faudree, E. Győri, Y. Ishigami, R.H. Schelp and H. Wang, *Vertex-disjoint cycles containing spcified edges*, Graphs Combin., *to appear*

[4] A. Kaneko and K. Yoshimoto, *On a 2-factor with specified edge*, submitted

[5] A. Kaneko and K. Yoshimoto, *On a Hamiltonian cycle in which specified vertices are uniformly distributed*, submitted

[6] 斉藤　明, 99年度春期日本数学会 応用数学分科会講演アブストラクト, 14-17

Another Construction of Dudeney sets of K_{p+2}

静岡県立大学　小林みどり
静岡県立大学　武藤伸明
半導体研究所　喜安善市
東海大学　中村義作

1. はじめに

$K_n = (V_n, E_n)$ を n 個の頂点をもつ完全グラフとする．K_n の任意の 2-path (長さ 2 の path) をちょうど 1 回ずつ含む Hamilton cycle の集合を K_n の Dudeney 集合という．すべての K_n に対して Dudeney 集合を構成する問題は Dudeney の円卓問題と呼ばれている．

n が偶数のときの Dudeney 集合は既に構成されている [3]．n が奇数のときの Dudeney 集合については，現在までに構成されているのは，

(1) $n = 2^e + 1$ (e は自然数) [4]

(2) $n = p + 2$ (p は奇素数，2 は mod p の原始根) [1]

(3) $n = p + 2$ (p は奇素数で $p \equiv 3 \pmod 4$，2 は mod p の原始根の 2 乗) [2]

のときのみである．

一般の奇数について Dudeney 集合を構成するには，$n = p + 2$ (p は奇素数) の場合が核となるが，この場合は，(2), (3) のとき，すなわち，2 か -2 が mod p の原始根のときしか構成されていない．しかも，その構成法は，複雑であり拡張することが容易ではない．ここでは，(2), (3) の場合について，より単純で包括的な構成法を示す．今後は，この構成法を用いて，他の場合への拡張を試みたい．

2. 記号と準備

$n = p+1$ とおく．ここで p は奇素数 ≥ 19 とする．K_n の 頂点集合を $V_n = \{\infty\} \cup \{0, 1, 2, \cdots, p-1\}$ とおき，1 因子 F_i, I_i $(0 \leq i \leq p-1)$ を $F_i = \{\{\infty, i\}\} \cup \{\{a, b\} \in E_n \mid a, b \neq \infty, a + b \equiv 2i \pmod p\}$, $I_i = \{\{\infty, i/2\}\} \cup \{\{a, b\} \in E_n \mid a, b \neq \infty, a + b \equiv i \pmod p\}$ と定義する．頂点の置換を $\sigma = (\infty)(0\ 1\ 2\ 3\ \cdots\ p-1)$ と定義し，$\Sigma = <\sigma>$ とおく．

K_n の l-path $P = (a_1, a_2, \cdots, a_l)$ $(a_i \neq \infty, 1 \leq i \leq l)$ について P の difference sequence を次のように定義する：

$$d(P) = (a_2 - a_1, a_3 - a_2, \cdots, a_l - a_{l-1})$$

2 つの difference sequence $d = (d_1, d_2, \cdots, d_t)$, $d' = (d'_1, d'_2, \cdots, d'_t)$ について，$d = d'$ を $d_1 = d'_1, d_2 = d'_2, \cdots, d_t = d'_t$, または，$d_1 = -d'_t, d_2 = -d'_{t-1}, \cdots, d_t = -d'_1$ と定める．こと Hamilton cycle の difference sequence は次のように決める．K_{p+1} の Hamilton cycle C は ∞ を先頭に書くことにし，$C = (\infty, a_1, a_2, \cdots, a_p)$ について，$d(C) = (a_2 - a_1, a_3 - a_2, \cdots, a_p - a_{p-1})$ と決める．

3. $h(0)$ の構成

p は奇素数で，2 または -2 が mod p の原始根であるとする．$r = (p-1)/2$ とおく．$h(0)$ を次のように作る．

(i) $p \equiv 1 \pmod 4$ のとき，$h(0) = (\infty, 1, -1, -2, 2, 2^2, -2^2, -2^3, 2^3, \cdots, -2^{r-1}, 2^{r-1}, 0)$

(ii) $p \equiv 3 \pmod 4$ のとき，$h(0) = (\infty, 1, -1, -2, 2, 2^2, -2^2, -2^3, 2^3, \cdots, 2^{r-1}, -2^{r-1}, 0)$

4. $h(1)$ の構成

次の性質を持つ K_{p+1} の Hamilton cycle $h(1)$ を構成したい．

1. $h(1)$ は 5-path $(\infty, 0, 1, -1, -2, 2)$ を含む．

2. 任意の half-set H mod p に対して，$\Sigma\{ah(1) \mid a \in H\}$ は K_{p+1} の Dudeney 集合である．

$h(1)$ は，K_{p+1} の Hamilton cycle $F_0 \cup I_1 = (\infty, 0, 1, -1, 2, -2, 3, -3, \cdots, r, -r)$ を基にして，これを変形して作る．ここでは，$p \equiv 3 \pmod 4$ の場合について作り方を示す．($p \equiv 1 \pmod 4$ の場合も同様である．) $F_0 \cup I_1$ の difference sequence d は，

$$d = (1, -2, 3, -4, 5, -6, 7, \cdots, -(r-1), r; r, -(r-1), \cdots, 7, -6, 5, -4, 3, -2, 1)$$

である．これを変形して

$$d_1 = (1, -2, -1, 4, -5, 6, -7, \cdots, (r-1), -r; -r, (r-1), \cdots, -7, 6, -5, 4, -3, 2, -1)$$

を作る．difference sequence d_1 に含まれる $(-2, -1, 4)$ を -3^{-1} 倍すると，$(2\cdot 3^{-1}, 3^{-1}, -4\cdot 3^{-1})$ となる．これは，d_1 の前半部分に存在する．3^{-1} の絶対最小剰余を b とおくと，b は偶数で，$(2\cdot 3^{-1}, 3^{-1}, -4\cdot 3^{-1}) = (-(b-1), b, -(b+1))$ であることが示される．ここで，等号は，dif.seq. としての等号である．

そこで，d_1 を変形して次のように d_2 を作る．符号を変える．

$$\begin{aligned} d_2 = \quad & (1, -2, -1, 4, -5, 6, -7, \cdots, -(b-1), -1, (b+1), -(b+2), \cdots, -(r-1), r; \\ & r, -(r-1), \cdots, -(b+2), (b+1), -1, -(b-1), \cdots, -7, 6, -5, 4, -1, -2, 1). \end{aligned}$$

d_2 に対応する Hamilton cycle を $h(1)$ とおくと，これが求めるものである．

sequence が含まれて

5. Dudeney 集合の構成

$h(0) = F_0 \cup G$ とおく．G の各枝に新しい頂点 λ を挿入して G^λ を作る．すなわち，$G^\lambda = \{(a, \lambda, b) \mid \{a, b\} \in G\}$ とする．ここで，(a, λ, b) は K_{p+2} における 2-path である．$h(a) = ah(1)$ (a は整数 $\neq 0$) とおく．G の枝は長さがすべて異なるので，次がいえる．

命題 1 $\Sigma(\{h(a) \mid a \in H\} \cup \{F_0 \cup G^\lambda\})$ は K_{p+2} の任意の 2-path をちょうど 1 回ずつ含む．

$F_0 \cup G^\lambda$ に入っている $r+1$ 個の λ のうち，1 個を残して他の r 個を $h(a)$ へ 1 個ずつ分けることができればよい．$H_1 = \{(-2)^i \mid i = 0, 1, 2, \cdots, r-2\}$ とおく．$h(1)$ は 3-path $(1, -1, -2, 2)$ を含むから，$h((-2)^i)$ は 3-path $((-2)^i, -(-2)^i, -2(-2)^i, 2(-2)^i)$ を含む．この 3-path の中間に λ を挿入した cycle を $h((-2)^i)^\lambda$ と書く．また，$h(1)$ は $(\infty, 0, 1, -1)$ を含む．G が $\{r, 0\}$ を含むときは，$H = H_1 \cup \{r\}$ とし，$h(r)$ の $(\infty, 0, r, -r)$ の中間に λ を入れた cycle を $h(r)^\lambda$ と書く．G が $\{-r, 0\}$ を含むときは，$H = H_1 \cup \{-r\}$ とし，$h(-r)$ の $(\infty, 0, -r, r)$ の中間に λ を入れた cycle を $h(-r)^\lambda$ と書く．$h(0)$ の枝 $\{\infty, 1\}$ の間に λ を入れた cycle を $h(0)^\lambda$ と書く．

定理 2 $\Sigma(\{h(0)^\lambda\} \cup \{h(a)^\lambda \mid a \in H\})$ は K_{p+2} の Dudeney 集合である．

参考文献

[1] K.Heinrich, M.Kobayashi and G.Nakamura, Dudeney's Round Table Problem, *Annals of Discrete Math.* **92** (1991) 107-125.

[2] M.Kobayashi, J.Akiyama and G.Nakamura, On Dudeney's round table problem for $p+2$, submitted.

[3] M.Kobayashi, Kiyasu-Z. and G.Nakamura, A solution of Dudeney's round table problem for an even number of people, *J. Combinatorial Theory* (A) **62** (1993), 26-42.

[4] G.Nakamura, Kiyasu-Z. and N.Ikeno, Solution of the round table problem for the case of $p^k + 1$ persons, *Commentarii Mathematici Universitatis Santi Pauli* **29** (1980) 7-20.

NORM OF ALIAS MATRICES FOR BALANCED FRACTIONAL 2^m FACTORIAL DESIGNS WHEN INTERESTING FACTORIAL EFFECTS ARE NOT ALIASED WITH EFFECTS NOT OF INTEREST IN ESTIMATION

Masahide KUWADA
Hiroshima University

Consider the following linear model:

$$\varepsilon\,[\boldsymbol{y}_T] = E_1\boldsymbol{\theta}_1 + E_2\boldsymbol{\theta}_2 + E_3\boldsymbol{\theta}_3, \tag{1}$$

where $\boldsymbol{y}_T$ is an N-vector of observations for a fraction T with two levels (0 and 1, say) and N assemblies, E_p (p=1,2,3) are $N\times n_p$ design matrices corresponding to $\boldsymbol{\theta}_p$ of T. Here $\boldsymbol{\theta}_1'=(\{\Theta(\phi)\};\{\Theta(u)\};\cdots;\{\Theta(u_1\cdots u_\ell)\})$, $\boldsymbol{\theta}_2'=(\{\Theta(u_1\cdots u_{\ell+1})\};\cdots;\{\Theta(u_1\cdots u_{\ell+f})\})$ and $\boldsymbol{\theta}_3'=(\{\Theta(u_1\cdots u_{\ell+f+1})\};\cdots;\{\Theta(1\cdots m)\})$ are an n_1-vector of factorial effects to be of interest in estimation, an n_2-one not of interest in estimation and not assumed to be negligible, and an n_3-one assumed to be negligible, respectively, and n_p are the number of elements in $\boldsymbol{\theta}_p$. Under $\boldsymbol{\theta}_3=\boldsymbol{0}_{n_3}$, the normal equations for estimating ($\boldsymbol{\theta}_1'$; $\boldsymbol{\theta}_2'$) are given by

$$M_{11}\hat{\boldsymbol{\theta}}_1 + M_{12}\hat{\boldsymbol{\theta}}_2 = E_1'\boldsymbol{y}_T \quad\text{and}\quad M_{21}\hat{\boldsymbol{\theta}}_1 + M_{22}\hat{\boldsymbol{\theta}}_2 = E_2'\boldsymbol{y}_T, \tag{2}$$

where $M_{pq}=E_p'E_q$. Then under $\det(M_{11})\neq 0$, solving (2) with respect to $\boldsymbol{\theta}_1$ and $\boldsymbol{\theta}_2$, we have the following solutions:

$$\hat{\boldsymbol{\theta}}_1 = \{M_{11}^{-1}E_1' - M_{11}^{-1}M_{12}B^g(E_2' - M_{21}M_{11}^{-1}E_1')\}\boldsymbol{y}_T - M_{11}^{-1}M_{12}(I_{n_2}-B^gB)\boldsymbol{z}$$

and

$$\hat{\boldsymbol{\theta}}_2 = B^g(E_2' - M_{21}M_{11}^{-1}E_1')\boldsymbol{y}_T + (I_{n_2}-B^gB)\boldsymbol{z},$$

where $B=M_{22}-M_{21}M_{11}^{-1}M_{12}$ and A^g is the generalized inverse of A. Therefore a necessary and sufficient condition for $\boldsymbol{\theta}_1$ not to be aliased with $\boldsymbol{\theta}_2$ is the following equation holds:

$$M_{12}(I_{n_2}-B^gB) = 0_{n_1\times n_2}. \tag{3}$$

Under (3), if $\boldsymbol{\theta}_3\neq\boldsymbol{0}_{n_3}$ in (1), then

$$\varepsilon\,[\,\hat{\boldsymbol{\theta}}_1] = \boldsymbol{\theta}_1 + A_T\boldsymbol{\theta}_3,$$

where $A_T=M_{11}^{-1}\{M_{13}-M_{12}B^g(M_{23}-M_{21}M_{11}^{-1}M_{13})\}$ is called the alias matrix of T. As a measure of comparing designs, the norm $\|A_T\|=\{\mathrm{tr}(A_T'A_T)\}^{1/2}$ was introduced by Hedayat, Raktoe and Federer (1974).

By utilizing the triangular multidimensional partially balanced association scheme and its algebra, the matrix $\|M_{pq}\|$ (p,q=1,2) associated with a simple array (S-array) T, which is written as SA(m; $\{\lambda_i\}$) for brevity, is isomorphic to $K_\beta=\|\kappa_\beta^{u,v}\|$ for $0\le\beta\le\ell+f$, where $\kappa_\beta^{u,v}$ are given by some linear combinations of λ_i. Consider the partitioning of the matrix K_β for $0\le\beta\le\ell+f$ such that $K_\beta=\|K_\beta(p,q)\|$ (p,q=1,2), where $K_\beta(1,1)$ are the first $(\ell+1-\beta)\times(\ell+1-\beta)$ submatrices of K_β for $0\le\beta\le\ell$, $K_\beta(1,2)(=K_\beta(2,1)')$ are the $(\ell+1-\beta)\times f$ ones of K_β for $0\le\beta\le\ell$, and $K_\beta(2,2)$ are the $f\times f$ ones of K_β

for $0\le\beta\le\ell$ and the $(\ell+f+1-\beta)\times(\ell+f+1-\beta)$ ones for $\ell+1\le\beta\le\ell+f$. The matrix $\|E_p(i)'E_q(i)\|$ $(p,q=1,2)$ associated with T_i, which is an SA$(m;\{\lambda_i=1,\ \lambda_j=0\ (j\neq i)\})$, is isomorphic to $H_\beta(i)=\|\eta_\beta^{u,v}(i)\|$ for $0\le\beta\le\ell+f$. Further let $H_\beta(i)=\|H_\beta(p,q;i)\|$ $(p,q=1,2)$. Then we can get the following:

Theorem. *Consider an* SA$(m;\{\lambda_i\})$, T. *Then under* $\det(M_{11})\neq0$ *and* $M_{12}(I_{n_2}-B^gB)=0_{n_1\times n_2}$,

$$\|A_T\|^2 = 2^m\Big[\Sigma_{\beta=0}^{\ell}\,\phi_\beta\{\mathrm{tr}[K_\beta(1,1)^{-1}+Q_\beta'L_\beta^gQ_\beta + \Sigma_i\lambda_i(\lambda_i-1)\{K_\beta(1,1)^{-1}[(I_{(\ell+1-\beta)}+P_\beta Q_\beta)H_\beta(1,1;i)(I_{(\ell+1-\beta)}+P_\beta Q_\beta)' - 2(I_{(\ell+1-\beta)}+P_\beta Q_\beta)H_\beta(1,2;i)P_\beta' + P_\beta H_\beta(2,2;i)P_\beta']K_\beta(1,1)^{-1}\}]\}\Big] - n_1,$$

where $P_\beta=K_\beta(1,2)L_\beta^g$, $Q_\beta=K_\beta(2,1)K_\beta(1,1)^{-1}$, $L_\beta=K_\beta(2,2)-K_\beta(2,1)K_\beta(1,1)^{-1}K_\beta(1,2)$ *and* $\phi_\beta=\binom{m}{\beta}-\binom{m}{\beta-1}$ *for* $0\le\beta\le\ell$.

Let T be an SA$(m;\{\lambda_i\})$ with N assemblies satisfying $\det(M_{11})\neq0$ and $M_{12}(I_{n_2}-B^gB)=0_{n_1\times n_2}$. Then if $\|A_T\|\le\|A_{T^*}\|$ for any S-array T^* with N assemblies, which also satisfies the same conditions mentioned above, T is called a best alias design.

Consider 2^6-BFF designs derived from SA$(m=6;\{\lambda_i\})$ satisfying $\det(M_{11})\neq0$ and $M_{12}(I_{n_2}-B^gB)=0_{n_1\times n_2}$. When $42\le N$, there exist resolution VII designs. Thus we consider S-arrays with $N\le41$. For (I) $\ell=1$ and $f=2$ and (II) $\ell=2$ and $f=1$, best alias 2^6-BFF designs satisfying $\det(M_{11})\neq0$ and $M_{12}(I_{35}-B^gB)=0_{7\times35}$ are given in Tables 1 and 2, respectively.

Table 1

N	$\|A_T\|$	λ_0	λ_1	λ_2	λ_3	λ_4	λ_5	λ_6
28	5.5076	0	1	1	0	0	1	1
29	5.4863	1	1	1	0	0	1	1
30	5.4870	2	1	1	0	0	1	1
31	5.4877	3	1	1	0	0	1	1
32	2.6458	0	1	0	1	0	1	0
		1	0	1	0	1	0	1
33	2.6458	1	1	0	1	0	1	0
		2	0	1	0	1	0	1
34	2.6339	1	1	0	1	0	1	1
35	2.6342	2	1	0	1	0	1	1
36	2.6344	3	1	0	1	0	1	1
37	2.5482	1	0	1	0	1	1	0
38	2.5125	1	0	1	0	1	1	1
39	2.5128	2	0	1	0	1	1	1
40	2.5127	2	0	1	0	1	1	2
41	2.5126	3	0	1	0	1	1	2

Table 2

N	$\|A_T\|$	λ_0	λ_1	λ_2	λ_3	λ_4	λ_5	λ_6
32	4.6904	0	1	0	1	0	1	0
		1	0	1	0	1	0	1
33	4.6904	1	1	0	1	0	1	0
		2	0	1	0	1	0	1
34	4.5826	1	1	0	1	0	1	1
35	4.5848	2	1	0	1	0	1	1
36	4.5869	3	1	0	1	0	1	1
37	4.5884	4	1	0	1	0	1	1
38	4.5826	1	0	1	0	1	1	1
39	4.5830	2	0	1	0	1	1	1
40	4.5833	3	0	1	0	1	1	1
41	4.5836	4	0	1	0	1	1	1

References

Hedayat, A., B.L. Raktoe and W.T. Federer (1974). *Ann. Statist.* 2, 650-660.

検索可能計画における未知母数2個の場合の検索手順の比較について

神戸市立高専　末次武明
神戸大学発達科学部　白倉暉弘

誤差のある場合の検索可能計画 (SD) では、未知母数の個数 k が2以上の場合は、特に理論的な解明が難しい。そこで、$k=2$ の場合に絞り、シミュレーションで、検索手順の比較、さらに、いろいろな計画の比較を通じて、SD の構造を探っていくことを目標にする。

1．準備

次のような線形モデルを考える。

$$\mathbf{y} = A_1\boldsymbol{\xi_1} + A_2\boldsymbol{\xi_2} + \mathbf{e}\ , \quad V(\mathbf{e}) = \sigma^2 I_N$$

ここで、$\mathbf{y}(N\times 1)$ は観測値ベクトル、$A_i(N\times\nu_i)$ は計画行列 $(i=1,2)$、$\boldsymbol{\xi_i}(\nu_i\times 1)$ は母数ベクトル $(i=1,2)$、$\mathbf{e}(N\times 1)$ は誤差ベクトル、σ^2 は誤差分散、I_N は大きさ N の単位行列である。

特に、上のモデルにおいて、(a) $\boldsymbol{\xi_1}$ のすべての要素は未知、(b) $\boldsymbol{\xi_2}$ の中に、どれか分からないが高々2個の未知母数が含まれ、残りは0である、場合を考える。

このとき、Srivastava(1975) は、次のことを示した。

$\boldsymbol{\xi_2}$ の高々2個の未知母数が検索可能かつ $\boldsymbol{\xi_1}$ と共に推定可能である必要条件は、A_2 のすべての $N\times 4$ 部分行列 A_{22} に対して、次の等式が成り立つことである。($\sigma^2=0$ の場合は十分条件でもある)

$$rank(A_1 : A_{22}) = \nu_1 + 4\ . \tag{1}$$

条件 (??) を満たす計画を検索可能計画という。

$\boldsymbol{\zeta}(2\times 1)$ を $\boldsymbol{\xi_2}$ の未知母数ベクトル，A_{20} は $\boldsymbol{\zeta}$ に対応する A_2 の $N\times 2$ 部分行列，$Q_1 = A_1(A_1'A_1)^{-1}A_1'$, $B=(I-Q_1)A_{20}$ とすると、$\boldsymbol{\zeta}$ の推定量 $\hat{\boldsymbol{\zeta}} = (B'B)^{-1}B'\mathbf{y}$ となり、残差平方和 S_e^2 は次のようになる。

$$S_e^2 = |\mathbf{y}-\hat{\mathbf{y}}|^2 = \mathbf{y}'[I-Q_1-B(B'B)^{-1}B']\mathbf{y}\ .$$

また、$\gamma=\boldsymbol{\zeta}'\boldsymbol{\zeta}$ とすると、$\psi=\hat{\boldsymbol{\zeta}}'\hat{\boldsymbol{\zeta}} = \mathbf{y}'B(B'B)^{-2}B'\mathbf{y}$ と置いて、γ の不偏推定量 $\hat{\gamma}$ は次のようになる。

$$\hat{\gamma} = \psi - (tr(B'B)^{-1})(N-\nu_1-k)^{-1}S_e^2$$

よって、Srivastava は、真の未知母数ベクトル $\boldsymbol{\zeta}_0$ を検索するための、次の4つの手順を示した。

(M_1) 残差平方和 S_e^2 をそれぞれ計算し、S_e^2 が最小になる ζ_1 をとる。

(M_2) $\boldsymbol{\zeta}'\boldsymbol{\zeta}(=\gamma)$ の推定量 $\hat{\gamma}$ をそれぞれ計算し、$\hat{\gamma}$ が最大になる ζ_2 をとる。

(M_3) S_e^2 が小さい方から h 個になるような $\boldsymbol{\zeta}$ を求める。これらの h 個のベクトルに現れる $2h$ 個の成分（重複する）のうち、最も良く出現する2個の成分を持つ ζ_3 をとる。

(M_4) $\hat{\gamma}$ が大きい方から h 個になるような $\boldsymbol{\zeta}$ を求める。これらの h 個のベクトルに現れる $2h$ 個の成分（重複する）のうち、最も良く出現する2個の成分を持つ ζ_4 をとる。

次に、$\tau = (B\boldsymbol{\zeta})'B\boldsymbol{\zeta} = \boldsymbol{\zeta}'A_{20}'(I-Q_1)A_{20}\boldsymbol{\zeta}$ を考える。

$\Lambda = (\widehat{B\boldsymbol{\zeta}})'\widehat{B\boldsymbol{\zeta}}$ とすれば、$\Lambda = \hat{\boldsymbol{\zeta}}'B'B\hat{\boldsymbol{\zeta}} = \mathbf{y}'B(B'B)^{-1}B'\mathbf{y}$ より、τ の不偏推定量 $\hat{\tau}$ は次のようになる。

$$\hat{\tau} = \Lambda - (N-\nu_1-k)^{-1}S_e^2 = \mathbf{y}'B(B'B)^{-1}B'\mathbf{y}\left(1+\frac{1}{N-\nu_1-k}\right) - \frac{\mathbf{y}'(I-Q_1)\mathbf{y}}{N-\nu_1-k}$$

これから、$\boldsymbol{\zeta}$ の検索のために、次の手順が得られる。

(M_5) $\hat{\tau}$ をそれぞれ計算し、$\hat{\tau}$ が最大になる ζ_5 をとる．

2．実行手順の比較

具体的なシミュレーションの方法は、C言語でプログラムを組み、基本的に2000回の繰り返し計算を実施している。また、試行した中で、何回、真のnon-zeroの値の組を検索できたか、ζの取り方について最小値を取ったものを「検索成功率」と呼ぶことにする。

まず、実行手順の比較として、Srivastavaの提唱した上記の4つの方法とその改良について述べる。M3),M4)の検索成功率が良くないため、改良案をいろいろ考えたが、次のM6),M7)だけをあげる。

(M_6)　S_e^2が小さい方から1/10の範囲にあるζだけ取り、最も良く出てくる2個の成分を持つζ_5をとる。
(M_7)　$\hat{\gamma}$が大きい方から1/10の範囲にあるζだけ取り、最も良く出てくる2個の成分を持つζ_6をとる。

下表1に、上記の方法を比較した例をあげる。「BA16-6」は、MEP.2 plan (Ω (6,2), Ω (6,6))である。最初に、ζの2つの要素z_1, z_2を$z_1 = z_2$としてその大きさを仮定している。M3) , M4)では、hとして、因子数6の半分の3を取っている。

表1 BA16-6の検索成功率

z	$M1)$	$M3)$	$M6)$	$M2)$	$M4)$	$M7)$
1.0	0.537	0.336	0.510	0.119	0.194	0.129
1.2	0.717	0.440	0.707	0.225	0.311	0.206
1.4	0.864	0.513	0.842	0.365	0.432	0.281
1.6	0.940	0.544	0.929	0.505	0.561	0.384
1.8	0.978	0.560	0.969	0.641	0.680	0.459
2.0	0.992	0.563	0.987	0.756	0.661	0.547
2.2	0.998	0.568	0.995	0.843	0.627	0.630
2.4	0.999	0.563	0.998	0.899	0.594	0.693

表2 (BA16-6の検索成功率)

δ	z	率
3.0	0.896*or*1.118	0.462
4.0	1.195*or*1.491	0.771
5.0	1.494*or*1.863	0.946
6.0	1.793*or*2.236	0.987
7.0	2.092*or*2.609	0.998
8.0	2.390*or*2.981	0.999

結論としては、S_e^2の最小を使う方法M1)がもっとも良い。$\hat{\gamma}$の最大を使うM2)では、なかなか検索が成功しない。M3)やM4)のようにhを固定的に取る方法では、かえって検索成功率が悪くなる。そこでM6) , M7)など、さまざまな改良案を考えてみたが、結局、M1)より良いものはなかった。

次に、τを与えて、シミュレーションしていく手順M5)を実行してみる。ただし、$\delta = \sqrt{\tau/2}$をはじめに与えている。$\hat{\tau}$を使う代わりに、同値で少し計算の楽な$y'B(B'B)^{-1}B'y$を使い、以下はM1)と同じ手順で、計算している。上記の表2で例を示している。

この手順は、下記のように、いろいろなSDの比較に役に立つ。

3．いろいろなSDの比較

まず、主効果までを推定し、2因子交互作用から2個までをnon-zeroとするMEP.2 planを考える。

典型的な比較例として、BAとBAでない場合を比べてみる。例えば、BAとして上記の「BA16-6」を、BAでない例として(Ω (6,1), Ω (6,5))にBIBD(4,6,3,2,1)を加えた「BI16-6」を比べてみる。

結論としては、同じ型の行列のとき、M1)では、BAの方が検索成功率が高いとは言えない。しかし、M5)では、検索成功率は、BAの方が良い。

その他にも、行を追加したり削除したりした場合や、Hadamard行列を利用して作ったSDと、BIBDを利用して作ったSDの比較や、違うBIBDから作ったSDどうしを比べている。

次に、主効果・2因子交互作用までを推定し、3因子交互作用から2個までをnon-zeroとするV.2 planを考える。

例えば、「36-6V2」:(Ω (6,1), Ω (6,2), Ω (6,4))と「36-6'V2」:(Ω (6,0), Ω (6,3), Ω (6,4))では、36-6'V2の方が検索成功率がM1)でもM5)でも高く、単純な構造になっているらしいことを見出した。

Recent developments in supersaturated design

東京理科大学工学部経営工学科 山田 秀 (Shu YAMADA, Science University of Tokyo)

1 Outline of supersaturated design

Supersaturated designs are a form of fractional factorial design in which the number of columns is greater than the number of experimental runs. In practice, it is used for screening the active factors, where the collected data are analyzed under an assumption of effect sparsity. Supersaturated designs were originated by Satterthwaite (1959) as a random balance design and formulated by Booth and Cox (1962) in a systematic manner. Let $\boldsymbol{c}^2$ and $\mathcal{C}_n^2$ be an n-dimensional column vector consisting of equal numbers of 1's and 2's and the set of $\boldsymbol{c}^2$, respectively. A vector $\boldsymbol{c}^2$ in the set $\mathcal{C}^n$ is called a two-level column and a matrix $\boldsymbol{C} = [\boldsymbol{c}_1^2, \boldsymbol{c}_2^2, \ldots, \boldsymbol{c}_k^2]$ is called a design matrix with n runs and k columns. A matrix is called saturated and supersaturated design matrix if $n = k$ and $n < k$ respectively.

The orthogonality between two two-level columns, $\boldsymbol{c}_i^2$ and $\boldsymbol{c}_j^2$, are measured by the squared inner product s_{ij}^2 between $\tilde{\boldsymbol{c}}_i^2$ and $\tilde{\boldsymbol{c}}_j^2$, where $\tilde{\boldsymbol{c}}^2$ denotes a transformed vector whose elements are -1's and 1's. The reason of application of s_{ij}^2 is that the dependency of the two estimates of factor effects assigned to the two columns can be described by a function of s_{ij}. The whole orthogonality of given design is measured by several ways. The most popular criterion of the design orthogonality would be average of the squared inner products over all paired columns, where it is sometimes denoted by $E(s^2)$. Booth and Cox (1962) introduced a design criterion based on the maximum value of the squared inner products over all paired columns. Wu (1993) points out that $E(s^2)$ criterion can be regarded as the criterion for two active factors. He derives D_f and A_f design criterion by extension of $E(s^2)$ to the case of f active factors based on the submatrix from the original design matrix. Deng, Ling and Wang (1999) proposed a new class of criteria, named Resolution Rank.

2 Developments in supersaturated design

(1) Consider construction of two-level supersaturated design. After three decades from the appearance of supersaturated designs, Lin (1993) obtained a simple but effective constructing method of supersaturated design. The constructing method is called "Half Fraction of Hadamard Matrices," which produces a supersaturated design with n rows and k columns from $2n \times (k+1)$ Plackett and Burman design, where the Plackett and Burman designs are derived by Hadamard Matrices. A theoretical justification in terms of $E(s^2)$ criterion is given by Cheng (1997).

Wu (1993) has proposed supersaturated designs by adding the cross products of two columns in the Plackett and Burman design. Iida (1994) has obtained some mathematical background on the addition of the cross products in the Placket and Burman design. Lin (1995) has examined the maximum number of columns that can be accommodated when the degree of non-orthogonality is specified by computer search. Nguyen (1996) described a method of constructing supersaturated designs from balanced incomplete block designs. Tang and Wu (1997) have shown a method for constructing supersaturated designs while considering the average squared inner products. Furthermore, they had shown a lower bound of $E(s^2)$ criterion for any type of two-level supersaturated design, where Nguyen (1996) also shows the similar bound by the different ways. Li and Wu (1997) have developed

columnwise-pairwise algorithms to construct supersaturated designs. Yamada and Lin (1997) have given a new class of supersaturated design including an orthogonal base.

(2) One of the major criticisms for supersaturated design would be difficulty of analysis of data collected by supersaturated design, e.g. Wang (1995). Lin (1993) recommends stepwise regression for data analysis through some numerical examples. Westfall, Young and Lin (1998) show a method to control the Type I error in stepwise regression for the data analysis. Yamada (1999) evaluates the Type II error via computer simulation and obtained that supersaturated design would work better under the small number of active factors.

(3) The definition of supersaturated design is naturally extended to multi-level and mixed level supersaturated design. Let c^3 and $\mathcal{C}_n^3$ be an n-dimensional column vector consisting of equal numbers of 1's, 2's and 3's and the set of c^3, respectively. A mixed-level design consisting of two and three-level columns is denoted by $\boldsymbol{C} = [c_1^2, \ldots, c_{p_1}^2, c_1^3, \ldots, c_{p_2}^3]$, where $c_i^2 \in \mathcal{C}_n^2 (1 \leq i \leq p_1)$ and $c_i^3 \in \mathcal{C}_n^3 (1 \leq i \leq p_2)$. For the case of multi-level and mixed level design, some orthogonality measures are proposed such as application of χ^2-statisitc (Yamada and Lin (1999)), the degree of equality on the number of appearance of paired levels (Fang, Lin and Ma (1999)). The design measures are defined by average χ^2 statistics, the average of the degree of equality and so on. Some multi-level and mixed-level supersaturated designs had been proposed. A lower bound on the χ^2-statistic had been proposed by Yamada and Matsui (1998), which is simliar to the bound by Tang and Wu (1997).

Bibliography

Booth, K. H. V. and Cox, D. R. (1962). Some systematic supersaturated designs. *Technometrics* **4** 489-495.

Cheng, C. S. (1997). $E(s^2)$- optimal supersaturated designs. *Statistica Sinica* **7** 929-939.

Deng, L. Y., Lin, D. K. J. and Wang, J. N. (1999). A resolution rank criterion for supersaturated designs. *Statistica Sinica* **9** 605-610.

Iida, T. (1994). A construction method of two-level supersaturated design derived from $L12$. *Japanese Journal of Applied Statistics* **23** 147-153 (in Japanese).

Lin, D. K. J. (1993). A new class of supersaturated designs. *Technometrics* **35** 28-31.

Lin, D. K. J. (1995). Generating systematic supersaturated designs. *Technometrics* **37** 213-225.

Li, W. W. and Wu, C. F. J. (1997). Columnwise-pairwise algorithms with applications to the construction of supersaturated designs. *Technometrics* **39** 171-179.

Nguyen, N. K. (1996). An algorithm approach to constructing supersaturated designs. *Technometrics* **38** 69-73.

Plackett, R. L., and Burman, J. P. (1946). The design of optimum multifactorial experiments. *Biometrika* **33** 303-325.

Satterthwaite, F. E. (1959). Random balance experimentation (with discussion). *Technometrics* **1** 111-137.

Tang, B. and Wu, C. F. J. (1997). A method for constructing supersaturated designs and its $E(s^2)$ optimality. *Canadian Journal of Statistics* **25** 191-201.

Wang, P. C. (1995). Comments to Lin (1993). *Technometrics* **37** 358.

Westfall, P. H., Young, S. S. and Lin, D. K. L. (1998). Forward selection error control in the analysis of supersaturated design. *Statistica Sinica* **8** 101-117.

Wu, C. F. J. (1993). Construction of supersaturated designs through partially aliased interactions. *Biometrika* **80** 661-669.

Yamada, S. (1999). Selection errors in the data analysis of supersaturated design. *Proceedings of Joint Statistical Meetings 1999* Section on Physical and Engineering Sciences. (in printing)

Yamada, S., Ikebe, Y., Hashiguchi, H. and Niki, N., (1999). Construction of three-Level supersaturated design. *Journal of Statistical Planning and Inference* (accepted).

Yamada, S. and Lin, D. K. J. (1997). Supersaturated designs including an orthogonal base. *Canadian Journal of Statistics* **25** 203-213.

Yamada, S. and Lin, D. K. J. (1999). Three-level supersaturated design, *Statistics and Probability Letters* (accepted).

Yamada, S. and Matsui, T.(1998). Optimality of mixed-level supersaturated designs. *Tech. Rep. University of Tokyo, Dept. Mathematical Engineering and Information Physics* METR 98-05