(13)「実験計画とその周辺における数理構造の解明とその応用Ⅱ」に関する研究報告

Resolvable C_k-Foil Designs
—Tightly Balanced C_k-Foil Decomposition of Symmetric Complete Multi-Digraphs—

Kazuhiko Ushio (Kinki University)

Abstract

We show that the necessary condition for the existence of a tightly balanced C_k-t-foil decomposition of the symmetric complete multi-digraph λK_n^* is $\lambda \equiv 0 \pmod{k}$ and $n = (k-1)t+1$.
Some sufficient conditions are also given.

Keywords: Tightly balanced C_k-t-foil decomposition; Symmetric complete multi-digraph

1. Introduction

Let K_n^* denote *the symmetric complete digraph* of n vertices. *The symmetric complete multi-digraph* λK_n^* is the symmetric complete digraph K_n^* in which every edge is taken λ times. Let C_k be *the directed cycle* on k vertices. *The C_k-t-foil* is a digraph of t edge-disjoint C_k's with a common vertex and the common vertex is called *the center of the C_k-t-foil.* In particular, the C_k-2-foil and the C_k-3-foil are called *the C_k-bowtie* and *the C_k-trefoil*, respectively. When λK_n^* is decomposed into edge-disjoint sum of C_k-t-foils, we say that λK_n^* *has a C_k-t-foil decomposition.* Moreover, when $n = (k-1)t+1$ and every vertex of λK_n^* appears in the same number of C_k-t-foils, we say that λK_n^* *has a tightly balanced C_k-t-foil decomposition* and this number is called *the replication number.*
This decomposition is a type of *resolvable C_k-foil designs.*

2. Tightly balanced C_k-t-foil decomposition of symmetric complete multi-digraphs

Theorem 1. If λK_n^* has a tightly balanced C_k-t-foil decomposition, then $\lambda \equiv 0 \pmod{k}$ and $n = (k-1)t+1$.
Proof. When $n = (k-1)t+1$, we suppose that λK_n^* has a tightly balanced C_k-t-foil decomposition. Let b be the number of C_k-t-foils and r be the replication number. Then $b = \lambda n(n-1)/kt = \lambda(k-1)\{(k-1)t+1\}/k$ and $r = \{(k-1)t+1\}b/n = \lambda(k-1)\{(k-1)t+1\}/k$. Among r C_k-t-foils having a vertex v of λK_n^*, let r_1 and r_2 be the numbers of C_k-t-foils in which v is the center and v is not the center, respectively. Then $r_1 + r_2 = r$. Counting the number of vertices adjacent to v, $tr_1 + r_2 = \lambda(n-1)$. From these relations, $r_1 = \lambda(k-1)/k$ and $r_2 = \lambda(k-1)^2 t/k$. Thus, $\lambda \equiv 0 \pmod{k}$.

Theorem 2. If λK_n^* has a tightly balanced C_k-t-foil decomposition, then $s\lambda K_n^*$ has a tightly balanced C_k-t-foil decomposition.
Proof. Obvious. Repeat a tightly balanced C_k-t-foil decomposition of λK_n^* s times.

Theorem F. Let p be prime and a be integer. Then $a^p \equiv a \pmod{p}$.

Corollaly F1. Let p be prime and $(a,p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Corollaly F2. Let p be prime and $(a,p) = 1$. Then $sa^{p-1} \equiv s \pmod{p}$ for $1 \le s \le p-1$.

Kazuhiko Ushio, Department of Informatics, Faculty of Science and Technology, Kinki University, Osaka 577-8502, JAPAN. E-mail:ushio@info.kindai.ac.jp Tel:+81-6-6721-2332 (ext. 4615) Fax:+81-6-6730-1320

Definition. When $sa^{n-1} \equiv s \pmod{n}$, let $a_i = \underline{sa^{i-1} \bmod n}$ $(i = 1, 2, ..., n)$ for $1 \leq s \leq n-1$. Find the first i $(i = 2, 3, ..., n)$ such that $a_i = s$. Put the i be L.
Then the sequence $a_1(= s), a_2(= sa), a_3(= sa^2), ..., a_L(= s)$ is called *an L-orbit starting s.*
When there exist $(n-1)$ L-orbits starting $1, 2, ..., n-1$, we say that n *admits L-orbits.*

Note. Let p be prime. It is a widely known result that p admits p-orbits and that a is called *a primitive root w.r.t. mod p.*

Theorem 3. When $n = p = (k-1)t + 1$, kK_n^* has a tightly balanced C_k-t-foil decomposition.

Conjecture 4. When $p = (k-1)t_0 + 1$ and $n = p^\alpha = (k-1)t + 1$, kK_n^* has a tightly balanced C_k-t-foil decomposition.

Conjecture 5. Let the orbits starting $1, 2, ..., n-1$ be L_1-orbit, L_2-orbit,...,L_{n-1}-orbit, respectively. When $n = (k-1)t + 1$ and $L_s - 1 \equiv 0 \pmod{k-1}$ $(1 \leq s \leq n-1)$, kK_n^* has a tightly balanced C_k-t-foil decomposition.

Theorem 6. $3K_{2t+1}^*$ has a tightly balanced C_3-t-foil decomposition.

Table 6. Tightly balanced C_3-t-foil decomposition of $3K_{2t+1}^*$.

$k=3$	$t=2$	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	$n=5$	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55	57	59	61

Main Conjecture. λK_n^* has a tightly balanced C_k-t-foil decomposition if and only if $\lambda \equiv 0 \pmod{k}$ and $n = (k-1)t + 1$.

References

[1] C. J. Colbourn, CRC Handbook of Combinatorial Designs, CRC Press, 1996.
[2] C. J. Colbourn and A. Rosa, Triple Systems, Clarendom Press, Oxford, 1999.
[3] P. Horák and A. Rosa, Decomposing Steiner triple systems into small configurations, *Ars Combinatoria*, Vol. 26, pp. 91–105, 1988.
[4] C. C. Lindner, Design Theory, CRC Press, 1997.
[5] K. Ushio, G-designs and related designs, *Discrete Math.*, Vol. 116, pp. 299–311, 1993.
[6] K. Ushio, Bowtie-decomposition and trefoil-decomposition of the complete tripartite graph and the symmetric complete tripartite digraph, *J. School Sci. Eng. Kinki Univ.*, Vol. 36, pp. 161–164, 2000.
[7] K. Ushio, Balanced bowtie and trefoil decomposition of symmetric complete tripartite digraphs, *Information and Communication Studies of The Faculty of Information and Communication Bunkyo University*, Vol. 25, pp. 19–24, 2000.
[8] K. Ushio and H. Fujimoto, Balanced bowtie and trefoil decomposition of complete tripartite multigraphs, *IEICE Trans. Fundamentals*, Vol. E84-A, No. 3, pp. 839–844, March 2001.
[9] K. Ushio and H. Fujimoto, Balanced foil decomposition of complete graphs, *IEICE Trans. Fundamentals*, Vol. E84-A, No. 12, pp. 3132–3137, December 2001.
[10] K. Ushio and H. Fujimoto, Balanced bowtie decomposition of complete multigraphs, *IEICE Trans. Fundamentals*, Vol. E86-A, No. 9, pp. 2360–2365, September 2003.
[11] K. Ushio and H. Fujimoto, Balanced bowtie decomposition of symmetric complete multi-digraphs, *IEICE Trans. Fundamentals*, Vol. E87-A, No. 10, pp. 2769–2773, October 2004.
[12] W. D. Wallis, Combinatorial Designs, Marcel Dekker, New York and Basel, 1988.

Split-block designs and PBIB designs

大阪府立大・工　逸見　亮太
大阪府立大・工　栗木　進二

1. 序

ISBD のモデルとして，処理効果が母数で，ブロック効果，行効果，列効果が確率変数である混合モデルを考える．また，3 段階の無作為化，(1) ブロックの無作為化，(2) ブロックの中の行の無作為化，(3) ブロックの中の列の無作為化を考える．Multistratum 分析において，stratum 情報行列 $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4$ は

$$\mathbf{A}_1 = \frac{1}{pq}\mathbf{N}_1\mathbf{N}_1' - \frac{r}{v}\mathbf{J}_v, \quad \mathbf{A}_2 = \frac{1}{q}\mathbf{N}_2\mathbf{N}_2' - \frac{1}{pq}\mathbf{N}_1\mathbf{N}_1'$$

$$\mathbf{A}_3 = \frac{1}{p}\mathbf{N}_3\mathbf{N}_3' - \frac{1}{pq}\mathbf{N}_1\mathbf{N}_1', \quad \mathbf{A}_4 = r\mathbf{I}_v - \frac{1}{q}\mathbf{N}_2\mathbf{N}_2' - \frac{1}{p}\mathbf{N}_3\mathbf{N}_3' + \frac{1}{pq}\mathbf{N}_1\mathbf{N}_1'$$

によって与えられる．$\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3$ は，処理組合せとブロック，行，列の接合行列である．また，$\mathbf{A}_f/r$ $(f = 1,2,3,4)$ の固有値を stratum efficiency factor といい，それに対応する固有ベクトルを basic contrast という．Hering and Mejza (2002) は Group Divisible 型 PBIBD のクロネッカー積を用いて ISBD を構成し，その stratum efficiency factor を与えた．ここでは，Triangular 型 PBIBD を用いて ISBD を構成し，その stratum efficiency factor を与える．

2. Triangular 型 PBIBD

Triangular 型 PBIBD の接合行列を $\mathbf{N}$ とし，そのアソシエーション行列を $\mathbf{P}_0, \mathbf{P}_1, \mathbf{P}_2$ とすると，

$$\mathbf{N}\mathbf{N}' = r\mathbf{P}_0 + \lambda_1\mathbf{P}_1 + \lambda_2\mathbf{P}_2$$

であり，$\mathbf{N}\mathbf{N}'$ のスペクトル分解は

$$\mathbf{N}\mathbf{N}' = \zeta_0\mathbf{P}_0^{\#} + \zeta_1\mathbf{P}_1^{\#} + \zeta_2\mathbf{P}_2^{\#}$$

によって与えられる．また，処理 w が Triangular 型アソシエーションスキームの $n \times n$ の正方形の s 行 t 列にあるとき，その処理効果 α_w に

$$\alpha_w = \theta_s + \theta_t + \delta_{st}$$

なる内部構造を考える．ここで，θ_s $(s = 1,2,\cdots,n)$ は主効果，δ_{st} $(s \neq t, s,t = 1,2,\cdots,n)$ は交互作用効果であり，条件

$$\sum_{s=1}^{n}\theta_s = 0, \quad \delta_{st} = \delta_{ts}, \quad \sum_{t\neq s}\delta_{st} = 0, \quad (s,t = 1,2,\cdots,n)$$

を満たしているとする．

定理 2.1. $\mathbf{N}\mathbf{N}'$ は固有値 $\zeta_0, \zeta_1, \zeta_2$ をもち，その重複度はそれぞれ $1, n-1, n(n-3)/2$ である．

定理 2.2. $\mathbf{P}_0^{\#}\boldsymbol{\alpha} = 0$ であり，$\mathbf{P}_1^{\#}\boldsymbol{\alpha}, \mathbf{P}_2^{\#}\boldsymbol{\alpha}$ はそれぞれ主効果 θ_s $(s = 1,2,\cdots,n)$，交互作用効果 δ_{st} $(s \neq t, s,t = 1,2,\cdots,n)$ の contrast を表す．ここで，

$$\boldsymbol{\alpha} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_v \end{pmatrix}$$

である．

3. ISBD の構成法

2つの Triangular 型 PBIBD $\mathcal{D}_A, \mathcal{D}_B$ の接合行列を $\mathbf{N}_A, \mathbf{N}_B$ とし，

$$\mathbf{N}_1 = \mathbf{N}_A \otimes \mathbf{N}_B$$

として，ISBD $\mathcal{D}$ を構成する．行処理，列処理の処理効果を，前節と同様に，

$$\alpha_w = \theta_s + \theta_t + \delta_{st}, \quad \beta_j = \varphi_{s'} + \varphi_{t'} + \psi_{s't'}$$

とし，ISBD の処理効果 τ_i を

$$\tau_i = \mu + \theta_s + \theta_t + \delta_{st} + \varphi_{s'} + \varphi_{t'} + \psi_{s't'} + (\theta\varphi)_{ss'} + (\theta\varphi)_{st'} + (\theta\varphi)_{ts'} + (\theta\varphi)_{tt'}$$

とする．ここで，$(\theta\varphi)_{ss'}$ $(s = 1, 2, \cdots, n, s' = 1, 2, \cdots, m)$ は行処理の主効果と列処理の主効果の交互作用効果である．$\mathbf{N}_A\mathbf{N}'_A$, $\mathbf{N}_B\mathbf{N}'_B$ のスペクトル分解を

$$\mathbf{N}_A\mathbf{N}'_A = \omega_0\mathbf{Q}_0^{\#} + \omega_1\mathbf{Q}_1^{\#} + \omega_2\mathbf{Q}_2^{\#}, \quad \mathbf{N}_B\mathbf{N}'_B = \xi_0\mathbf{R}_0^{\#} + \xi_1\mathbf{R}_1^{\#} + \xi_2\mathbf{R}_2^{\#}$$

とし，

$$\boldsymbol{\tau} = \begin{pmatrix} \tau_1 \\ \tau_2 \\ \vdots \\ \tau_v \end{pmatrix}$$

とする．

定理 2.1, 定理 2.2 から，次の定理が得られる．

定理 3.1. $\mathbf{N}_1\mathbf{N}'_1$ は固有値 $\omega_0\xi_0$, $\omega_0\xi_1$, $\omega_0\xi_2$, $\omega_1\xi_0$, $\omega_1\xi_1$, $\omega_1\xi_2$, $\omega_2\xi_0$, $\omega_2\xi_1$, $\omega_2\xi_2$ をもち，その重複度は 1, $m-1$, $m(m-3)/2$, $n-1$, $(m-1)(n-1)$, $m(m-3)(n-1)/2$, $n(n-3)/2$, $(m-1)n(n-3)/2$, $m(m-3)n(n-3)/4$ である．

定理 3.2. $\mathbf{N}_2\mathbf{N}'_2$ は固有値 $r_A\xi_0$, $r_A\xi_1$, $r_A\xi_2$ をもち，その重複度は 1, $m-1$, $m(m-3)/2$ である．$\mathbf{N}_3\mathbf{N}'_3$ は固有値 $r_B\omega_0$, $r_B\omega_1$, $r_B\omega_2$ をもち，その重複度は 1, $n-1$, $n(n-3)/2$ である．

定理 3.3. $\mathbf{N}_1\mathbf{N}'_1$, $\mathbf{N}_2\mathbf{N}'_2$, $\mathbf{N}_3\mathbf{N}'_3$ はそれぞれ交換可能である．

定理 3.4. $(\mathbf{Q}_0^{\#} \otimes \mathbf{R}_0^{\#})\boldsymbol{\tau} = \mu\mathbf{1}_v$, $(\mathbf{Q}_1^{\#} \otimes \mathbf{R}_2^{\#})\boldsymbol{\tau} = (\mathbf{Q}_2^{\#} \otimes \mathbf{R}_1^{\#})\boldsymbol{\tau} = (\mathbf{Q}_2^{\#} \otimes \mathbf{R}_2^{\#})\boldsymbol{\tau} = \mathbf{0}$ であり，

$$(\mathbf{Q}_1^{\#} \otimes \mathbf{R}_0^{\#})\boldsymbol{\tau},\ (\mathbf{Q}_2^{\#} \otimes \mathbf{R}_0^{\#})\boldsymbol{\tau},\ (\mathbf{Q}_0^{\#} \otimes \mathbf{R}_1^{\#})\boldsymbol{\tau},\ (\mathbf{Q}_0^{\#} \otimes \mathbf{R}_2^{\#})\boldsymbol{\tau},\ (\mathbf{Q}_1^{\#} \otimes \mathbf{R}_1^{\#})\boldsymbol{\tau}$$

はそれぞれ行処理の主効果 θ_s $(s = 1, 2, \cdots, n)$，行処理の交互作用効果 δ_{st} $(s \neq t, s, t = 1, 2, \cdots, n)$，列処理の主効果 $\varphi_{s'}$ $(s' = 1, 2, \cdots, m)$，列処理の交互作用効果 $\psi_{s't'}$ $(s' \neq t', s', t' = 1, 2, \cdots, m)$，行処理の主効果と列処理の主効果の交互作用効果 $(\theta\varphi)_{ss'}$ $(s = 1, 2, \cdots, n, s' = 1, 2, \cdots, m)$ の contrast を表す．

定理 3.1，定理 3.2，定理 3.3，定理 3.4 から，stratum efficiency factor を求めることができる．

Contrast	No.	I	II	III	IV
θ_s	$n-1$	ω'_1	$1-\omega'_1$	-	-
δ_{st}	$n(n-3)/2$	ω'_2	$1-\omega'_2$	-	-
$\varphi_{s'}$	$m-1$	ξ'_1	-	$1-\xi'_1$	-
$\psi_{s't'}$	$m(m-3)/2$	ξ'_2	-	$1-\xi'_2$	-
$(\theta\varphi)_{ss'}$	$(m-1)(n-1)$	$\omega'_1\xi'_1$	$(1-\omega'_1)\xi'_1$	$\omega'_1(1-\xi'_1)$	$(1-\omega'_1)(1-\xi'_1)$

control-test 対比における diallel cross 実験の最適性

慶應義塾大学大学院理工学研究科　津島 直

diallel cross は動植物の交配実験において，交配品種（line）の遺伝的な特性を研究するために用いられる．通常，p 個の line を考え，line i と line j の交配を cross と呼び，cross (i,j) $(i,j=1,\cdots,p,\ i<j)$ と書く．それぞれの品種が持つ効果 (general combining ability（g.c.a.）effect) の推定に関する最適な実験が，Gupta and Kageyama (1994) などによって研究されてきた．近年では，ある程度効果のわかっている品種（control line）と新しい品種（test line）を交配させる実験が，Choi, Gupta and Kageyama (2004) によって提案された．さらに Das, Gupta and Kageyama (2004) は，control-test 対比に対して A- optimal なデザインの十分条件を与えた．これらの control-test 対比における daillel cross 実験では，control line を一つとして考えている．今回，複数の control line が存在する diallel cross 実験を考え，control-test 対比に対して weakly universally optimal なデザインの十分条件を与える．

p 個の control line と q 個の test line から作られる cross を b 個の block（block size: k）に配置する．実験の総数は $n=bk$ である．block を考慮した実験のモデルは

$$\boldsymbol{Y}=\mu\mathbf{1}_n+\Delta_1\boldsymbol{g}+\Delta_2\boldsymbol{\beta}+\boldsymbol{\varepsilon}$$

となる．ここで，$\boldsymbol{Y}$ はプロットベクトル，μ は一般平均，$\boldsymbol{g}$ は g.c.a. 効果ベクトル，$\boldsymbol{\beta}$ は block 効果ベクトル，$\Delta_1(\Delta_2)$ はプロット × line（block）の計画行列，$\boldsymbol{\varepsilon}$ は平均 $\mathbf{0}$，分散が $\sigma^2 I$ の誤差ベクトルである．このとき，g.c.a. 効果の推定に関する C-行列は，

$$C=\Delta_1'\Delta_1-k^{-1}NN'$$

である．ただし，$N=\Delta_1'\Delta_2=(n_{ij})$ は line × block 結合行列である．

ここで，$P=(-I_p\otimes\mathbf{1}_q \quad \mathbf{1}_p\otimes I_q)$ とおくと，

$$P\boldsymbol{g}=(g_{p+1}-g_1,\cdots,g_{p+1}-g_p,g_{p+2}-g_1,\cdots,g_{p+q}-g_{p+1})'$$

となり，すべての control-test の対比を表現できる．そのとき，$P\boldsymbol{g}$ の最良線型不偏推定量（BLUE）$P\hat{\boldsymbol{g}}$ の分散共分散行列は $\mathrm{Var}(P\hat{\boldsymbol{g}})=\sigma^2PC^-P'$ である．

ここで，次のような集合 $\mathcal{M}$ を考える．

$$\mathcal{M}=\{M=PC^-P'\mid C^-\text{は}C\text{の一般逆行列}\},\quad \bar{\mathcal{M}}:\mathcal{M}\text{の凸閉包}$$

ϕ を $\bar{\mathcal{M}}$ 上で次の条件を満たす関数とする．

(i) $\phi(M)\le\phi(aM)$, $a\ge1$, $M\in\bar{\mathcal{M}}$.

(ii) ϕ は $\bar{\mathcal{M}}$ 上で下に凸な関数.

(iii) Π_1 を $\{1,\cdots,p\}$ 上の置換の集合，Π_2 を $\{p+1,\cdots,p+q\}$ 上の置換の集合としたとき，$\Pi=\Pi_1\times\Pi_2\ni\pi$ を取ると，$\phi(P\pi C^-\pi'P')=\phi(PC^-P')$.

このような ϕ の集合を Φ とする．

定義 1 $\phi\in\Phi$ に対して，$C^*\in\mathcal{C}$ ($\mathcal{C}$ は推定可能な C-行列の集合) が ϕ -optimal であるとは，

$$\phi(PC^{*-}P')=\min_{C\in\mathcal{C}}\phi(PC^-P')$$

であることを言う．

定義 2 $C^*\in\mathcal{C}$ が weakly universally optimal であるとは，任意の $\phi\in\Phi$ に対して C^* が ϕ -optimal であることを言う．

定理 1 C^* が (i) $C^*=\left(\begin{array}{c|c} aI_p+bJ_p & cJ_{pq} \\ \hline cJ_{qp} & dI_q+eJ_q \end{array}\right)$, $a,d>0$, $c\neq0$, (ii) $\mathrm{tr}(PC^{*-}P')=\min_{C\in\mathcal{C}}\mathrm{tr}(PC^-P')$ を満たすならば，C^* は weakly universally optimal である．

定義 3 $\mathcal{U}$ を control line の集合 ($|\mathcal{U}| = p$), $\mathcal{V}$ を test line の集合 ($|\mathcal{V}| = q$), $\mathcal{B}$ を k_1k_2 -部分集合の族 (superblock), $\mathcal{B}'$ を $\mathcal{B}$ の各 superblock を k_2 -部分集合に分割した k_2 部分集合の族 (subblock) としたとき, $(\mathcal{U},\mathcal{V},\mathcal{B},\mathcal{B}')$ が nested balanced bipartite design (NBBD) である $\overset{\text{def}}{\Longleftrightarrow}$

(i) 任意の $u_1,u_2 \in \mathcal{U}$ に対して, u_1 と u_2 が superblock で会合する数を $\lambda_0(u_1,u_2)$, u_1,u_2 を共に含む subblock の数を $\lambda_0'(u_1,u_2)$ とすると,

$$\lambda_0(u_1,u_2) = \lambda_0, \quad \lambda_0'(u_1,u_2) = \lambda_0'$$

である. λ_0, λ_0' は定数.

(ii) 任意の $u \in \mathcal{U}$, $v \in \mathcal{V}$ に対して, u と v が superblock で会合する数を $\lambda_1(u,v)$, u,v を共に含む subblock の数を $\lambda_1'(u,v)$ とすると,

$$\lambda_1(u,v) = \lambda_1, \quad \lambda_1'(u,v) = \lambda_1'$$

である. λ_1, λ_1' は定数.

(iii) 任意の $v_1,v_2 \in \mathcal{V}$ に対して, v_1 と v_2 が superblock で会合する数を $\lambda_2(v_1,v_2)$, v_1,v_2 を共に含む subblock の数を $\lambda_2'(v_1,v_2)$ とすると,

$$\lambda_2(v_1,v_2) = \lambda_2, \quad \lambda_2'(v_1,v_2) = \lambda_2'$$

である. λ_2, λ_2' は定数.

NBBD では次の数も一定となる. 実験で control line i が用いられる数を r_0, test line j が用いられる数を r_1 とする. さらに, 結合行列 $N = (n_{ij})$ に関して, $\sum_{j=1}^{b} n_{ij}^2 = x$, $(i = 1,\cdots,p)$, $\sum_{j=1}^{b} n_{hj}^2 = y$, $(h = p+1,\cdots,p+q)$ である.

定義 4 次の条件が成り立つ NBBD を NBBD_0 と呼ぶ.

$|n_{ij} - n_{i'j'}| \le 1$, $|n_{hj} - n_{h'j'}| \le 1$, $({}^{\forall}i,i' = 1,\cdots,p;\ {}^{\forall}h,h' = p+1,\cdots,p+q;\ {}^{\forall}j,j' = 1,\cdots,b)$

このとき, x,y はそれぞれ最小値 x_0, y_0 を取る.

定理 2

$$\text{tr}(PC^{*-}P') = \frac{kq(p-1)}{p(\lambda_0 - k\lambda_0') + q(\lambda_1 - k\lambda_1')} + \frac{k}{(\lambda_1 - k\lambda_1')} + \frac{kp(q-1)}{p(\lambda_1 - k\lambda_1') + q(\lambda_2 - k\lambda_2')}$$

を最小にするパラメータ $(\lambda_0, \lambda_0', \lambda_1, \lambda_1', \lambda_2, \lambda_2')$ をとる NBBD_0 は, $\mathcal{D}(p,q,b,k)$ において, weakly universally optimal である.

定理 3 $p = 1$ のとき,

$$\text{tr}(PC^{*-}P') = \frac{q}{r - x_0/k} + \frac{(q-1)^2}{2bk - r - qy_0/k - (r - x_0/k)/q}$$

を最小にする r を r_0 としたとき, パラメータ $r_1 = \frac{2bk - r_0}{q}$, $\lambda_1' = \frac{r_0}{q}$, $\lambda_2' = \frac{r_1 - \lambda_1'}{q-1}$, $\lambda_1 = \frac{2kr_0 - x_0}{q}$, $\lambda_2 = \frac{2kr_1 - y_0 - \lambda_1}{q-1}$ の NBBD_0 は, $\mathcal{D}(1,q,b,k)$ において, weakly universally optimal である.

注：この定理は, Das, Gupta, Kageyama (2004) の A-optimal に関する結果を weakly universally optimal に拡張したものである.

さらに, $p = 2$ の場合についても考察する.

参考文献

[1] K.C. Choi, S. Gupta and S. Kageyama (2004). Designs for diallel crosses for test versus control comparisons, *Utilitas Math.*, **65**, 167-180.

[2] A. Das, S. Gupta and S. Kageyama (2004). A-optimal diallel crosses for test versus control comparisons. To appear.

[3] S. Gupta and S. Kageyama (1994). Optimal complete diallel crosses, *Biometrika*, **81**, 420-424.

[4] J. Kiefer and H.P. Wynn (1981). Optimal balanced and latin square designs for correlated observations, *Ann. Statist.*, **9**, 737-757.

Mutually M-intersecting k-arcs の収集法の改良

明星大学 情報学部　　篠原 聡
東京理科大学 理工学部　宮本 暢子

1. はじめに

q を素数巾とする。射影平面 PG$(2,q)$ 上の k 個の点からなる集合で、そのうちどの 3 点も同一直線上にないようなものを *k-arc* という。M を有限個の非負整数の集合とする。k-arc の集まりで、任意の 2 つの k-arc の共有点の個数が M に含まれているとき、この集まりを *mutually M-intersecting k-arcs* と呼ぶことにする。Mutually M-intersecting k-arcs は直交配列や均斉配列の構成に利用することができ、また光ファイバーを用いた符号分割多元接続通信を実現するために利用される光直交符号 (Optical Orthogonal Code) を得るためにも応用できる。

光直交符号では、各符号語とそれぞれを cyclic shift したものとで、自己および相互相関の最大値がある一定値 $(=\lambda)$ 以下となるようにする。この λ や、符号語の長さ n および重み w といった与えられたパラメータ (n,w,λ) に対して、符号語の数が最大であるような光直交符号を *optimal* であるという。符号語数に関しては、constant weight code に対する Johnson bound より導かれる、

$$\Phi(n,w,\lambda) \leq \lfloor \frac{1}{w} \lfloor \frac{n-1}{w-1} \lfloor \cdots \lfloor \frac{n-\lambda}{w-\lambda} \rfloor \cdots \rfloor \rfloor \rfloor \tag{1}$$

によってある上限が与えられており、これを達成する事で optimal な光直交符号であると保証できる。

Mutually $\{0,1,2\}$-intersecting $(q+1)$-arcs を求める方法、およびこの集合から長さが q^3+q^2+q+1、重みが $q+1$、$\lambda=2$ であるような光直交符号が得られる事が筆者らによって示されている [2]。また、より一般的に mutually M-intersecting (k,d)-arcs と光直交符号との関係も明らかにされている [3]。

2. optimal により近い光直交符号を得るために

ある mutually M-intersecting k-arcs $\mathcal{C}$ に対して、$\mathcal{C} \subset \mathcal{C}'$ なる mutually M-intersecting k-arcs $\mathcal{C}'$ が存在しないとき、$\mathcal{C}$ を *maximal* であるという事にする。

Lemma 1 q を素数冪とし、点 P を射影平面 PG$(2,q^2)$ の点で PG$(2,q)$ 以外の点とする。点 P を通る PG$(2,q)$ 上のすべての conic の集合 $\mathcal{C}$ は、maximal な mutually $\{0,1,2\}$-intersecting $(q+1)$-arcs であり、$|\mathcal{C}| = q^3 - q^2$ である。

光直交符号への応用に際し、mutually M-intersecting k-arcs における k-arcs の個数が、符号語数に対応する。また、符号語の cyclic shift は PG$(3,q)$ における Singer cycle と対応付けられるが、ある平面上で Lemma 1 の方法によって得られる mutually $\{0,1,2\}$-intersecting $(q+1)$-arcs を符号語とみなした上で、さらに他の平面上に k-arcs を追加して、符号語数を増やす事は出来ない。そこで、(1) 式の bound により近づけるようにするために、符号語の重みを大きくする事を試みた。

Lemma 2 符号語の長さが q^3+q^2+q+1 であり、$\lambda=2$ であるような光直交符号が q^3-q^2 個の符号語を持つとき、符号語の重みは高々 $q+2$ である。

*E-mail: sshinoha@mi.meisei-u.ac.jp
†E-mail: miyamoto@is.noda.tus.ac.jp

3. hyperoval の交点

q が偶数の素数冪のとき、conic のすべての点における接線が唯一の点で交わり（この点を *nuleus* と呼ぶ)、conic にその nucleus を加えた点集合は $(q+2)$-arc となる。この $(q+2)$-arc を *hyperoval*(超卵型) と呼ぶ。Lemma 1 の方法によって得られる mutually $\{0,1,2\}$-intersecting $(q+1)$-arcs をなす各 conic にそれぞれの nucleus を加えた hyperoval の集合は mutually $\{0,1,2,3\}$-intersecting $(q+2)$-arcs である [3]。この場合 $\lambda=3$ なる光直交符号が対応する。

$\lambda=2$ であるような光直交符号を得るためには、mutually $\{0,1,2\}$-intersecting k-arcs が必要となる。hyperoval からなる mutually $\{0,1,2\}$-intersecting $(q+2)$-arcs を得る方法を探るためにも、hyperoval 同士の交点数を明らかにする必要がある。これまでに、2 つの conic の交わり方による分類をもとに、それぞれに nucleus を加えた hyperoval 同士の交点数を筆者らは明らかにしてきたが、未解決であったケースに関してここで述べる事にする。

q を素数冪とする。$\pi_i=\mathrm{PG}(2,q^i)$ とし、$\pi_i\subset\pi_{i+1}$ であるとする。点 $P\in\pi_3\setminus\pi_2$ が π_1 の直線上にないとき、点 P を通るすべての conic の集合は、mutually $\{1\}$-intersecting $(q+1)$-arcs をなす [1]。q が偶数のとき、これらの conic それぞれに nucleus を加えた hyperoval 同士の交点数に関しての結果が得られた。

Lemma 3 h を奇数とし、$q=2^h$ とする。点 $P\in\pi_3\setminus\pi_2$ が π_1 上の直線上に無いとき、点 P を通る 2 つの conic それぞれに nucleus を加えた 2 つの hyperoval は高々2 点で交わる。

Theorem 4 h を奇数とし、$q=2^h$ とする。このとき q^2+q+1 個の hyperoval からなる mutually $\{1,2\}$-intersecting $(q+2)$-arcs が存在する。

4. q が奇数のとき

q が奇数の素数冪のときには、$q+1$ が k の最大値であるため、同一平面上の点を付加する事により符号語の重みを増やす事は出来ない。そこで、conic を含んでいる平面にない $\mathrm{PG}(3,q)$ の点を加える事を試みた。しかしながら、加える事が可能な点の集合を求めた上でコンピュータによる全探索を試みたところ、どの具体例についてもそのような点集合が存在しない結果となってしまった。

Conjecture 5 q が奇数のとき、Lemma 1 によって得られる mutually $\{0,1,2\}$-intersecting $(q+1)$-arcs に 1 点を加える事で、重みが $q+2$ の光直交符号を得る事は出来ない。

参考文献

[1] R.D. Baker, J.M.N. Brown, G.L. Ebert, and J. C. Fisher, "Projective bundles", *Bull. Belg. Math. Soc.*, Vol. 3, pp. 329–336, 1994.

[2] Nobuko Miyamoto, Hirobumi Mizuno, and Satoshi Shinohara, "Optical orthogonal codes obtained from conics on finite projective planes", *Finite Fields and thier Applications*, Vol. 10, pp.405–411, 2004.

[3] Nobuko Miyamoto and Satoshi Shinohara, "Mutually M-intersecting (k,d)-arcs and its application to optical orthogonal codes", *Congressus Numerantium*, to appear.

平成 16 年 11 月 17 日 (水)

Additive structures of BIB designs I

- 完全行列の分解問題 -

広島大学大学院教育学研究科　樹山廣之

1　完全行列の分解問題

全ての成分が 1 である $v \times b$ 行列 J を完全行列と呼ぶことにする。

＜問題＞

BIBD(v, b, r, k, λ) の s 個の異なる生起行列 N_1, $N_2, \cdots, N_s$ で,

$$N_1 + N_2 + \cdots + N_s = J \quad \cdots\cdots \quad (1.1)$$

を満たすものが存在するか？

s 個の生起行列の和が J になることから，$v/k = b/r = s$ という必要条件が得られる。また $s = 2$ のとき，BIBD の補構造は BIBD であることから $N_2 = {N_1}^c$ とすると $N_1 + N_2 = J$ が得られるので，この問題は $s \geq 3$ について考えていくことにする。

これまでの考察から得られた分解問題の解を紹介する。

定理 1.1. resolvable BIBD

resolvable BIBD$(v = sk, b, r, k, \lambda)$ に対して (1.1) 式を満たす s 個の異なる生起行列 N_1, $N_2, \cdots, N_s$ が存在する。

この定理により，resolvable BIBD に対しては，分解問題の解が与えられた。続いての定理では，non-resolvable BIBD に対しても解を与えている。

定理 1.2. 松原

BIBD$(6m+3, (2m+1)(3m+1), 2m+1, 3, 1)$ の s 個の生起行列 $N_1, N_2, \cdots, N_s$ で (1.1) 式を満たすものが存在する。

この定理で得られる BIBD は Skolem's method(Skolem,1958) と呼ばれる構成法によって構成されるものである。注意したいのは，m の値によって $2m+1$ 個の生起行列が全て non-resolvable であるものも構成されている，ということである。

2 今後の課題

現在は，BIBD$(21,30,10,7,3)$について$N_1+N_2+N_3=J$を満たす3つの生起行列を探している。このパラメータをもつBIBDは全てnon-resolvableであることが分かっているものなので，これを足がかりにnon-resolvable BIBDに対する分解問題に取り組んでいきたい。

参考文献

- Bose, R. C. and Manvel, B. (1984). *Introduction to Combinatorial Theory.* Wiley.
- Calinski, T. and Kageyama, S. (2003). *Block Design : A Randamization Approach, Volume* II *: Design.* Springer-Verlag.
- Colbourn, C.J. and Dinitz,J.H. (ed). (1996). *The CRC Handbook of Combinatorial Design.* CRC Press, Boca Ration, USA.
- Kiyama, H., Matsubara, K., Matsumoto, D.,Sawa, M. and Kageyama, S.(2004). Decomosition of an all-one matrix into incidence matrices of a BIB design. submitted.
- Matsubara, K., Sawa, M.,Matsumoto, D.,Kiyama, H. and Kageyama, S.(2004). An addition structure on incidence matrices of a BIB design. *Ars Combin.*, to appear.
- Raghavarao, D. (1988).*Constructions and Combinatorial Ploblems in Design of Experiments.* Dover.

Additive structures of BIB design II

広島大院・教育　松本大地

「完全行列の分解問題」に『任意の２つの生起行列の加法により得られる行列もまた，BIBD の生起行列になる』という条件を加えた「加法構造」について考える．本発表では，加法構造の定義を提示し，いくつかの系列と，それらを得るためのアイデアについて述べる．

1　加法構造の存在問題

$N_1, N_2, \cdots, N_s$ を BIBD$(v = sk, b, r, k, \lambda)$ の生起行列とするとき，

(1)　$N_i + N_j$: BIBD　$(\forall\, i, j \in \{1, 2, \cdots s\}, i \neq j)$

(2)　$N_1 + N_2 + \cdots + N_s = J$

を満たす $N_1, N_2, \cdots, N_s$ は存在するか？

定義 1.1（加法構造）　ある BIBD が上の条件 (1), (2) を満たす生起行列をもつとき，その BIBD は**加法構造をもつ**という．

補題 1.1　$N_1, N_2, \cdots, N_s$ を BIBD$(v = sk, b, r, k, \lambda)$ の生起行列とするとき，次の (a) と (b) は同値である．

(a)　$N_i + N_j$: BIBD　$(\forall\, i, j \in \{1, 2, \cdots s\}, i \neq j)$

(b)　$N_{i_1} + N_{i_2} + \cdots + N_{i_t}$: BIBD　$(\forall\, i_1, i_2, \cdots, i_t \in \{1, 2, \cdots, s\}, 2 \leq t \leq s-2)$

補題 1.1 より，任意の $i, j \in \{1, 2, \cdots s\}, (i \neq j)$ に対して，$N_i + N_j$ が BIBD となることが確認できれば，$2 \leq t \leq s-2$ に対して，$N_{i_1} + N_{i_2} + \cdots + N_{i_t}$　$(i_1, i_2, \cdots, i_t \in \{1, 2, \cdots, s\})$ は BIBD の生起行列となる．

注 1.1　s の値によっては，任意の２つではなく，いくつかの２つの生起行列の和が，BIBD の生起行列であることを示せば十分である場合もある．

注 1.2　$s = 5$ のときは，$N_i + N_{i+1}$ $(1 \leq i \leq 5)$ を確認すればよい．

実際，$N_1 + N_2$ は BIBD の生起行列であると仮定する．$N_1 + N_2 + N_3 + N_4 + N_5 = J$ から，$N_3 + N_4 + N_5 = J - (N_1 + N_2)$ である．仮定より $N_1 + N_2$ は BIBD の生起行列であるから，$N_3 + N_4 + N_5$ は BIBD の生起行列となる．

したがって，各 N_3, N_4, N_5 での会合数は一定．かつ，$(N_3, N_4), (N_4, N_5), (N_3, N_5)$ の会合数も一定でなければならない．

$(N_3, N_4), (N_4, N_5)$ の会合数は一定より，(N_3, N_5) の会合数も一定である．

注 1.4　$s = 3$ のとき，条件 (1) より $N_{i_1} + N_{i_2} = J - N_{i_3}$ $(i_1, i_2, i_3 \in \{1, 2, 3\})$ であり，N_{i_3} は BIBD の生起行列であるから，$J - N_{i_3}$ も BIBD の生起行列である（補構造なので）．したがって，$N_{i_1} + N_{i_2}$ も BIBD の生起行列である．これより，$s = 3$ のときは，「完全行列の分解問題」と「加法構造の存在問題」は同値である．

2 加法構造をもつ BIBD

加法構造をもつ BIBD の系列をいくつか紹介する.

系列 2.1 p : 素数, $n(\geq 2)$: 整数 に対して, BIBD$(v = p^n, b = p^n(p^n-1), r = p(p^n-1), k = p, \lambda = p(p-1))$ は, 加法構造をもつ.

系列 2.2 p : 奇素数, $n(\geq 2)$: 整数 に対して, BIBD$(v = p^n, b = p^n(p^n-1)/2, r = p(p^n-1)/2, k = p, \lambda = p(p-1)/2)$ は, 加法構造をもつ.

系列 2.3 p : 奇素数, $n(\geq 2)$: 整数 に対して, BIBD$(v = p^n, b = p^n(p^n-1)/2, r = p^{n-1}(p^n-1)/2, k = p^{n-1}, \lambda = p^{n-1}(p^{n-1}-1)/2)$ は, 加法構造をもつ.

ここに挙げた系列は, 次の array(2.1) を用いることによって, 構成できる.

$$\begin{array}{ccccccc}
x & x^2 & x^3 & \cdots & x^{p^n-1} & 0 \\
x^2 & x^3 & x^4 & \cdots & x & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
x^{\frac{p^n-1}{2}} & x^{\frac{p^n-1}{2}+1} & x^{\frac{p^n-1}{2}+2} & \cdots & x^{\frac{p^n-1}{2}-1} & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
x^{p^n-1} & x & x^2 & \cdots & x^{p^n-2} & 0
\end{array}$$

array(2.1)

任意の p 列 を選ぶ. そして, 各行ずつを 1 つブロックとすると,

$$\{x, x^2, \cdots, x^p\}, \{x^2, x^3, \cdots, x^{p+1}\}, \cdots, \{x^{p^n-1}, x, \cdots, x^{p^n+p-2}\}$$

これらのブロックは, 初期ブロックとなる.

参考文献

[1] Bose, R. C. and Manvel, B. (1984). *Introduction To Combinatorial Theory.* Wiley.

[2] Calinski, T. and Kageyama, S. (2003). *Block Designs : A Randomization Approach, Volume II: Design.* Springer-Verlag.

[3] Colbourn, C. J. and Dinitz, J. H. (ed.)(1996). *The CRC Handbook of Combinatorial Designs.* CRC Press, Boca Raton, USA.

[4] Kiyama, H., Matsubara, K., Matsumoto, D., Sawa, M. and Kageyama, S. (2004). Decomposition of an all-one matrix into incidence matrices of a BIB design. submitted.

[5] Matsubara, K., Sawa, M., Matsumoto, D., Kiyama, H. and Kageyama, S. (2004). Addition structure on incidence matrices of a BIB design. *Ars Combin.*, to appear.

[6] Raghavarao, D.(1988). *Constructions and Combinatorial Problems in Design of Experiments.* Dover.

Difference systems of sets and code synchronization

Vladimir D. Tonchev
Department of Mathematical Sciences, Michigan Technological University
Houghton, Michigan 49931, U.S.A.
tonchev@mtu.edu

1 Introduction

A *difference system of sets* (DSS) with parameters $(n, \tau_0, \ldots, \tau_{q-1}, \rho)$ is a collection of q disjoint subsets $Q_i \subseteq \{1, 2, \ldots, n\}$, $|Q_i| = \tau_i$, $0 \leq i \leq q-1$, such that the multi-set

$$\{a - b \pmod{n} \mid a \in Q_i,\ b \in Q_j,\ i \neq j\} \tag{1}$$

contains every number i, $1 \leq i \leq n-1$ at least ρ times.

Difference systems of sets were introduced by Levenshtein [2] in connection with code synchronization. This paper discusses some constructions of difference systems of sets obtained from cyclic difference sets and finite geometry.

Let $D = \{x_1, x_2, \ldots, x_k\}$ be a cyclic (v, k, λ) difference set. Then the collection of singletons $Q_0 = \{x_1\}, \ldots, Q_{k-1} = \{x_k\}$ is a DSS with parameters $n = v, q = k, \rho = \lambda$. The next lemma generalizes this simple construction by using more general partitions of difference sets.

Lemma 1.1 *(Tonchev [5]). Let $D \subseteq \{1, 2, \ldots, n\}$, $|D| = k$, be a cyclic (n, k, λ) difference set. Assume that D is partitioned into q disjoint subsets $Q_0, \ldots, Q_{q-1}$ that are the base blocks of a cyclic design $\mathcal{D}$ with block sizes $\tau_i = |Q_i|$, $i = 0, \ldots, q-1$ such that every two points are contained in at most λ_1 blocks. Then the sets $Q_0, \ldots, Q_{q-1}$ form a DSS with parameters $(n, \tau_0, \ldots, \tau_{q-1}, \rho = \lambda - \lambda_1)$.*

The following theorem gives DSS's obtained as partitions of difference sets of quadratic-residue (QR) type.

Theorem 1.2 *(Tonchev [5]). For every prime $n = 2mq + 1 \equiv 3 \pmod 4$ there exists a DSS with parameters $n, q, \rho = (n - 2m - 1)/4$.*

If n is a prime of the form $n \equiv 1 \pmod 4$, the quadratic residues do not form a difference set. Some results concerning primes $n \equiv 1 \pmod 4$ that explore cyclotomy were obtained recently by Mutoh and Tonchev [4].

2 Difference systems of sets from finite geometry

Let H be a hyperplane in the $2s$-dimensional projective space $PG(2s,p)$ over $GF(p)$. The $(p^{2s}-1)/(p-1)$ points of H form a cyclic difference set with parameters

$$v=\frac{p^{2s+1}-1}{p-1},\ k=\frac{p^{2s}-1}{p-1},\ \lambda=\frac{p^{2s-1}-1}{p-1}$$

in a cyclic group acting regularly on the points of $PG(2s,p)$, known as the Singer difference set. The points of H can be partitioned into disjoint lines $Q_0,\ Q_1,\ldots,\ Q_{q-1}$, where

$$q=\frac{p^{2s}-1}{p^2-1}=p^{2s-2}+\ldots+p^2+1.$$

On the other hand, the collection of all lines in $PG(2s,p)$ is a cyclic 2-$(\frac{p^{2s+1}-1}{p-1},p+1,1)$ design $\mathcal{D}$. If the partition

$$H=Q_0\cup Q_1\cup\ldots\cup Q_{q-1}$$

is chosen so that $Q_0,\ \ldots,\ Q_{q-1}$ are base blocks of $\mathcal{D}$, then by Lemma 1.1 the collection $Q_0,\ Q_1,\ldots,\ Q_{q-1}$ is a DSS with parameters

$$n=\frac{p^{2s+1}-1}{p-1},\ q=\frac{p^{2s}-1}{p^2-1},\ \rho=\frac{p^{2s-1}-p}{p-1}.$$

Hyperplane partitions with the above property were found by Fuji-Hara, Jimbo and Vanstone [1] in $PG(2s,2)$ for $s\leq 5$, and in $PG(2s,3)$ for $s\leq 3$.

Recently, Munemasa [3] found such partitions in $PG(4,p)$ for $p=8$ and $p=9$, and showed that no solution exists in $PG(4,4)$. A solution was also found by the author in $PG(4,5)$.

The existence of solutions in other dimensions or other values of p is an open problem.

References

[1] R. Fuji-Hara, M. Jimbo, and S. Vanstone, Some results on the line partitioning problem in $PG(2k,q)$, *Utilitas Math.* **30** (1986), 235-241.

[2] V. I. Levenshtein, One method of constructing quasilinear codes providing synchronization in the presence of errors, Problems of Information Transmission, vol. 7, No. 3 (1971), 215-222.

[3] A. Munemasa (private communication).

[4] Y. Mutoh and V.D. Tonchev, Difference systems of sets and cyclotomy, *Discrete Math.*, July 21, 2004.

[5] V. D. Tonchev, Difference systems of sets and code synchronization, Rendiconti del Seminario Matematico di Messina, Series II, vol. 9 (2003), 217-226.

Singer difference sets and difference system of sets

東北大学・情報科学　宗政昭弘

1 序

有限射影空間における射影直線の集合、または超平面の集合はいずれも BIBD をなすが、これら相互の関係について考える。特に、Singer cycle で不変な構造から、差集合の一般化である difference system of sets が得られるが、実際に計算機を用いて、$PG(4,8)$ 等について実例が見つかったことを報告する。

まず有限射影空間に関する基本的な用語を説明する。$PG(n,q)$ は、有限体 $GF(q)$ 上の n 次元射影空間を表す。その元は点と呼び、直線は射影直線を意味することとする。$PG(n,q)$ における spread とは、互いに交わらない直線の集合で $PG(n,q)$ 全体の分割になっているものである。Spread が存在するために必要十分条件は n が奇数であることである。Packing （または resolution, parallelism）とは、直線全体の集合の、spread への分割である。n が奇数のとき packing が存在するかどうかは、一般には未解決問題である。

一方、n が偶数のとき、$PG(n,q)$ には spread が存在しないので、当然 packing も存在しないのだが、$PG(n,q)$ の余次元 1 の超平面には spread が存在するので、直線全体の集合をそのような spread に分割することが可能か、という問題は意味を持つ。これが可能なとき、$PG(n,q)$ は $(n-1)$-partitionable であるという。$PG(n,q)$ における直線の総数は

$$\frac{(q^{n+1}-1)(q^n-1)}{(q^2-1)(q-1)} = \frac{(q^{n+1}-1)}{(q-1)} \cdot \frac{(q^n-1)}{(q^2-1)}$$

であり、右辺の第一因子は $PG(n,q)$ における余次元 1 の超平面の総数、第二因子は余次元 1 の超平面における spread を構成する直線の数であるから、上の問題には肯定的な解が期待される。この問題を提起したのは藤原-神保-Vanstone [2] であり、彼らは例えば $(n,q) = (4,2),(4,3),(6,q)$ 等について肯定的に解決している。問題を若干言い換えると、以下のようになる。

問題 1. $PG(2n,q)$ の余次元 1 の各超平面 H に対して、spread S_H が存在して、直線全体の集合を S_H たちの、互いに交わらない和集合として分割することが可能か。

この問題でにおいて、今まで未解決であった $(2n,q)$ の値は例えば $(4,4),(4,5),(4,7)$ 等がある。

このような問題を肯定的に解決する常套手段は、すべての超平面を考えるかわりに、超平面全体の集合に可移に作用する自己同型を用意して、ただ一つの超平面に関する問題に帰着することである。そのような自己同型として、よく知られた Singer cycle というものがある。Singer cycle とは、射影空間の巡回的な自己同型で、点集合にも、余次元 1 の超平面の集合にもただひとつの軌道を持っている。以下、射影空間の次元は偶数 $2n$ とし、$PG(2n,q)$ の Singer cycle を σ とする。今、H を余次元 1 の超平面とし、

$$H = L_1 \cup L_2 \cup \cdots \cup L_s$$

を H の spread とすると、

$$H^\sigma = L_1^\sigma \cup L_2^\sigma \cup \cdots \cup L_s^\sigma$$

は H^σ の spread になる。さらに続けて σ を作用させることによって、すべての超平面の spread が得られる。ただ、これだけでは問題 1 の解になるとは限らない。なぜなら、上記の方法で得られた直線がすべて異なるという保証がないからである。その保証をするためには、H の spread を構成する

$L_1, L_2, \ldots, L_s$ がすべて異なる $\langle\sigma\rangle$ 軌道に属していれば十分である。したがって、Singer cycle を使って問題 1 の解を得るためには、次の問題を解けばよいことになる。

問題 **2.** $PG(2n,q)$ の余次元 1 の任意の超平面を H とする。H の spread S で、S に属する直線がすべて異なる $\langle\sigma\rangle$ 軌道に属しているようなものが存在するか。

このような spread は、以下に定義する、difference system of sets を与えることがわかる。

定義 **3.** G を位数 v の有限群、$\mathcal{S} = \{B_1, B_2, \ldots, B_k\}$ を G の k 個の m 元部分集合とする。Multiset として

$$\{gh^{-1} \mid g \in B_i,\ h \in B_j,\ 1 \le i,j \le k,\ i \ne j\}$$

が $\lambda(G - \{1\})$ に一致するとき、$\mathcal{S}$ を $(v,k,\lambda;m)$ difference system of sets と呼ぶ。

実際、$PG(2n,q)$ とその Singer cycle $G = \langle\sigma\rangle$ を同一視すれば、H の spread $H = L_1 \cup \cdots \cup L_s$ は G の $s = (q^{2n}-1)/(q^2-1)$ 個の $q+1$ 元部分集合の族と考えることができて、

$$(\frac{q^{2n+1}-1}{q-1}, \frac{q^{2n}-1}{q-1}, \frac{q^{2n-1}-q}{q-1}; q+1) \text{ difference system of sets}$$

になることが簡単にわかる。その証明で重要なことは、H が Singer difference set になることと、$\{L_1, \ldots, L_s\}$ が difference family になることである。後者は、$\{L_1, \ldots, L_s\}$ の展開が $PG(2n,q)$ の直線全体の集合に一致することによる。

2 得られた結果

定理 **4.** $PG(4,4)$ には問題 2 の条件を満たす spread は存在しない。

定理 **5.** $PG(4,8), PG(4,9)$ には問題 2 の条件を満たす spread が存在する。

いずれも、計算機によって確かめられた。ここでは、定理 4 の確認方法を簡単に述べる。$PG(4,4)$ の余次元 1 の任意の超平面を H とする。グラフ Γ を次のように定義する。Γ の頂点集合としては H に含まれる直線全体をとる。2 つの直線 L, L' に対して、L, L' が交わらず、また L, L' が同じ $\langle\sigma\rangle$ 軌道に属していないとき、L, L' は Γ において辺で結ぶことにする。このように定義したグラフ Γ においては、17 点の完全部分グラフが問題 2 の条件を満たす spread に対応する。計算代数システム magma [1] を用いて、グラフ Γ を実際に構成し、magma のビルトイン関数 `HasClique` を用いて 17 点完全部分グラフが存在しないことを確認した。

同様の方法で $PG(4,q)$ $(q > 4)$ の場合に *exhaustive search* をするには時間がかかりすぎるため、$\langle\sigma\rangle$ の代わりに $\langle\sigma\rangle$ と Frobenius automorphism で生成された、より大きい群で不変な line partition を探すことにより、定理 5 を得た。

参考文献

[1] Computer Algebra System Magma, `http://magma.maths.usyd.edu.au/`.

[2] R. Fuji-hara, M. Jimbo and S. Vanstone, Some results on the line partitioning problem in $PG(2k,q)$, Utilitas Math. 30 (1986), 235–241.

Self-Orthogonal 3-(56, 12, 65) Designs

Masaaki Harada (Yamagata University)
山形大学・理 原田 昌晃

1 Introduction

Let C be a binary self-dual code of length n, that is, C is an $n/2$-dimensional vector subspace of $\mathbb{F}_2^n$ with $C = C^\perp$ where $C^\perp$ is the dual code under the standard inner product. A self-dual code C is *doubly-even* if all codewords have weights divisible by four. Such codes exist if and only if $n \equiv 0 \pmod 8$. The minimum weight d of a doubly-even self-dual code of length n is upper bounded by $d \leq 4[n/24]+4$. A doubly-even self-dual code meeting the bound is called *extremal*. Recall that two codes are equivalent if one can be obtained from the other by permuting the coordinates. An automorphism of C is a permutation of the coordinates of C which preserves C. The set consisting of all automorphisms of C is called the automorphism group of C.

A t-(v, k, λ) design $\mathcal{D}$ is a set X of v points together with a collection of k-subsets of X (called blocks) such that every t-subset of X is contained in exactly λ blocks. A design $\mathcal{D}$ can be represented by its block-point incidence matrix $A = (a_{ij})$ where $a_{ij} = 1$ if the jth point is contained in the ith block and $a_{ij} = 0$ otherwise. Two designs are isomorphic if the incidence matrix of one design can be obtained from the incidence matrix of the other by permuting rows and columns. An automorphism of $\mathcal{D}$ is any isomorphism of the design with itself and the set consisting of all automorphisms of $\mathcal{D}$ is called the automorphism group of $\mathcal{D}$. The block intersection numbers of $\mathcal{D}$ are the cardinalities of the intersections of any two distinct blocks. A t-(v, k, λ) design is called *self-orthogonal* if the block intersection numbers have the same parity as the block size k (cf. [2]).

2 Motivation

The supports of the codewords of each weight in an extremal doubly-even self-dual code of length $n \equiv 0, 8, 16 \pmod{24}$ form a $5, 3, 1$-design by the Assmus–Mattson theorem, respectively. Such a design is self-orthogonal. For example, the supports of the codewords of minimum weight in an extremal

doubly-even self-dual code of length 32 (resp. 56) form a self-orthogonal 3-design with parameters $(32, 8, 7)$ (resp. $(56, 12, 65)$). Tonchev [2] showed that the code generated by the rows of a block-point incidence matrix of a self-orthogonal 3-$(32, 8, 7)$ design is an extremal doubly-even self-dual code of length 32. Using the classification of such codes, the self-orthogonal 3-$(32, 8, 7)$ designs and quasi-symmetric 2-$(31, 7, 7)$ designs are classified [2].

3 Results

We show that the code generated by the rows of a block-point incidence matrix of a self-orthogonal 3-$(56, 12, 65)$ design is a doubly-even self-dual code of length 56. As a consequence, it is shown that an extremal doubly-even self-dual code of length 56 is generated by the codewords of minimum weight and the 2-rank of a self-orthogonal 3-$(56, 12, 65)$ design is exactly 28. In addition, two inequivalent extremal doubly-even self-dual codes of length 56 give two non-isomorphic self-orthogonal 3-$(56, 12, 65)$ designs. By the construction method developed in [1], we construct extremal doubly-even self-dual $[56, 28, 12]$ codes from the generator matrices of some extremal double circulant doubly-even $[56, 28, 12]$ codes. By comparing with the known codes, it is demonstrated that at least 1151 inequivalent extremal doubly-even self-dual $[56, 28, 12]$ codes exist. From this result, there are at least 1151 non-isomorphic self-orthogonal 3-$(56, 12, 65)$ designs.

References

[1] M. Harada, Existence of new extremal doubly-even codes and extremal singly-even codes, *Des. Codes Cryptogr.* **8** (1996), 273–283.

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

Multi-Structured Designs

筑波大学大学院 システム情報工学研究科
fujihara@sk.tsukuba.ac.jp
藤原　良 (Ryoh Fuji-Hara)

1　はじめに

世の中には，　Nested designs, Balanced nested designs, Splitting designs, Directed designs, Row and column designs,... などの名前をもった組合わせ的デザインがある．これらのデザインに共通なのは，単なるブロックデザインではなく，**その各ブロック内に更なる構造を持っている**という点である．これらは，異なるアプリケーション先で定義され，微妙に異なる組合わせ条件を持っているが，多くの共通部分をも持っている．　また構成法に関しても共通に使われている手法が多々ある．この種の組み合わせ的デザインを個別に独立して構成するのではなく，統一的に解析し，より一般的な構成法に整理することが期待される．これらのブロックデザインを**多重構造デザイン** (*multi-structured designs*) と呼ぶことにし，まずは統一的に定義することにしよう．

2　定義

まずブロックデザイン $(V, \mathcal{B})$ を次のように定義する．

- V : 有限な点の集合, $|V| = v$
- $\mathcal{B} = \{B_1, B_2...., B_b\}$ ブロックの集り, $B_i \subseteq V$
- バランス条件：(b1) V のどの点も r 個のブロックに含まれる．(b2) V の任意の異なる 2 点に関して，それらを同時に含むブロックが必ず λ 個存在する．

多重構造デザインは基本的には

1. 親デザイン (Super design). $(V, \mathcal{B})$
2. m 個の子デザイン (Sub-designs), $(V, \mathcal{B}_0), (V, \mathcal{B}_1), ..., (V, \mathcal{B}_{m-1})$
3. 個々の子デザインのバランス条件
4. 子デザイン間のバランス条件

からなる．B の各ブロック B は次のように部分ブロックに分割されている．

$$(C_0, C_1, ..., C_{m-1}),\ C_i \subseteq B,\ 0 \leq |C_i| \leq |B|$$

ここでは $C_0, C_1, ..., C_{m-1}$ がブロック B の分割になっている場合のみをあつかう．(ϕ でもよい) そして，第 i 番目の部分ブロックのみを集めたものを $\mathcal{B}_i$ と書く．

それでは既に研究されている数々のデザインと統一的定義での分類と比較しながら多重構造デザインの各種タイプを定義しよう．

Type I (Nested design$_1$)

1. $(V, \mathcal{B})$ はブロックデザイン

2. 各 $(V, \mathcal{B}_i)$ はブロックでサイン

Type II (Nested design$_2$)

1. $(V, \mathcal{B})$ はブロックデザイン

2. $(V, \mathcal{B}_*)$ はブロックデザイン.　但し $\mathcal{B}_* = \mathcal{B}_0 \cup \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_{m-1}$

Type III (Nested design$_3$)

1. $(V, \mathcal{B})$ はブロックデザイン

2. 各 $(V, \mathcal{B}_i)$ および $(V, \mathcal{B}_*)$ はブロックデザイン

つぎに相対バランス条件 (relative balance condition) に関して整理しよう.
異なる V の2点 a, b に対し，$a \in C_i$, $b \in C_j$ となっていて，親ブロックの数を $\lambda_{ij}(a, b)$ と書く. いまもし s, b の取り方に依存しないとき，すなわち任意の異なる $a, b \in V$ に対し $\lambda_{ij}(a, b) = \lambda_{ij}$ なら，$\mathcal{B}_i$ と $\mathcal{B}_j$ は**バランスしている**という.

Type IV (Balanced Nested design)

1. $(V, \mathcal{B})$ はブロックデザイン

2. 各 $(V, \mathcal{B}_i)$ はブロックでサイン

3. 任意の i, j に対して，$\mathcal{B}_i$ と $\mathcal{B}_j$ はバランスしている

このデザインはまた均整配列（直交配列の一般系）と同値になる. また，相対バランスの総和が一定という条件（任意の異なる $a, b \in V$ に対し $\sum_{i \neq j} \lambda_{ij}(a, b) = \mu$ であるとき）*Splitting design* などと呼ばれている.
また相対バランス条件を任意の i, j ではなく，(1) $i \leq i < j \leq m-1$ や (2) $i, i+1 (mod\ m)$ などの特定の間のみバランス条件を要求し，各部分ブロックはサイズが1のものを *directed design* などと呼んでいる.

次に親ブロックのサイズか固定で $k_1 k_2$ としよう. 各ブロックは2つの分割を持っている:

$$(C_0, C_1, ..., C_{k_2-1}),\ |C_i| = k_1\ ,\ (D_0, D_1, ..., D_{k_1-1}),\ |D_i| = k_2$$

そして,,　$|C_i \cap D_j| = 1$ をみたす. このようなデザインを Matrix 型多重構造デザインということにする.

また $V = \mathbb{Z}_v$ としてサイクリックな多重構造デザインを考えるとき，各種の系列問題と同値になり，Comma-free code, Frequency hopping sequence など多くのアプリケーションと結びつく.

3　構成法

この多重構造デザインの各種のタイプに対して，共通に使える手法が多々有る. 最も有効的に働く構成は法は Wilson の定理に基づく構成法である. "Design Theory, Second Edition" T.Beth, D.Jungnickel and H.Lenz, VII §5 参照. また有限幾何，特にアフィン幾何の平行類の構造はこの多重構造デザインの構成には極めて有効である. また再帰的構成法も共通に使えるものがあるはずである.

Some Infinite Classes of 5-Sparse Steiner Triple Systems

Department of Mathematics, Keio University, Yuichiro Fujiwara

A *Steiner triple system* S of *order* v, briefly STS(v), is an ordered pair $(V, \mathcal{B})$, where V is a finite set of v elements called *points*, and $\mathcal{B}$ is a set of 3-element subsets of V called *blocks*, such that each unordered pair of distinct elements of V is contained in exactly one block of $\mathcal{B}$. It is well-known that an STS(v) exists if and only if $v \equiv 1, 3 \pmod 6$; such orders are called *admissible*.

$G^{(3)}(n; m)$ denotes a 3-graph of n vertices and m 3-tuples called edges. In 1976, Erdös [2] conjectured that there is an integer $v_0(r)$ so that for every $v > v_0(r)$, $v \equiv 1, 3 \pmod 6$, there exists a Steiner triple system on v elements containing no $G^{(3)}(k+2; k)$ for every $1 < k \leq r$. Such an STS is said to be *r-sparse*. Since every $G^{(3)}(k+2; k)$ for $1 < k \leq 3$ has two edges containing the same pair of points, every STS(v) is 3-sparse. Obviously, every r-sparse STS(v) is also $(r-1)$-sparse.

The problem of characterizing those v for which there exists an r-sparse STS(v) has been studied for a long time. One direction is regarding the problem as one of extremal problem on hypergraphs. In fact, Erdös posed this conjecture as a problem relating with extremal set theory on hypergraphs. The other direction, in which we shall study in this talk, is to construct an r-sparse STS for all possible orders. When we construct an STS, $G^{(3)}(k; l)$ appearing in an STS is often called a "configuration".

A *(k, l)-configuration* in an STS is a set of l blocks whose union contains precisely k points. Two particular configurations are of interest here. The unique $(6, 4)$-configuration, called the *Pasch configuration*, is described by 6 distinct points on 4 blocks $\{a, b, c\}$, $\{a, d, e\}$, $\{f, b, d\}$ and $\{f, c, e\}$. One of two $(7, 5)$-configurations is called the *mitre*, described by 7 distinct points on 5 blocks $\{a, b, e\}$, $\{a, c, f\}$, $\{a, d, g\}$, $\{b, c, d\}$ and $\{e, f, g\}$; a is referred to as the *centre* or *central element* of the mitre and the unique pair of blocks with no common point, that is, $\{b, c, d\}$ and $\{e, f, g\}$, are referred to as the *parallel blocks*. The other $(7, 5)$-configuration, the *mia*, is obtained by joining two noncollinear points in a Pasch configuration: $\{a, b, c\}$, $\{a, d, e\}$, $\{f, b, d\}$, $\{f, c, e\}$ and $\{g, c, d\}$. Since the only $G^{(3)}(6; 4)$s which may occur in an STS are Pasch configurations, an STS(v) is 4-sparse if and only if it contains no Pasch configuration. Similarly, since containing no Pasch configuration implies no mia configuration neither, an STS(v) is 5-sparse if and only if it contains neither Pasch nor mitre configuration.

The constructive methods for an STS containing no particular configuration, especially no $(k+2, k)$-configuration, have been studied for a lomg time. In particular, Ling, Colbourn, Grannell and Griggs [6] extended substantially the spectrum of known 4-sparse STS and the existence problem was settled by Grannell, Griggs and Whitehead [4].

Theorem 1 (Grannell, Griggs and Whitehead) [4] *There exists a* 4*-sparse* STS(v) *if and only if* $v \equiv 1, 3 \pmod 6$ *and* $v \neq 7, 13$.

Thus, Erdös' conjecture is true for $r = 4$ and $v_0(4) = 13$. Also, substantial progress has been made on STS containing no mitre configuration, we call such an STS *anti-mitre*, due to Colbourn, Mendelsohn, Rosa and Širáň [1], Ling [5] and the author [3]. However, the existence problem for 5-sparse STS, that is, STS containing neither Pasch nor mitre configuration appears to be much more difficult and remains far from settled. In fact, less is known about 5-sparse STS and no example is known for r-sparse STS with $r \geq 6$. Only one infinite class is known for 5-sparse STS due to Colbourn, Mendelsohn, Rosa and Širáň [1] and a recursive construction is developed by Ling [5].

In this talk we present new constructions for anti-mitre STS and an extention for 5-sparse ones which extend substantially the spectrum of known such systems. As a consequence of these constructions we can cover anti-mitre systems for at least 13/14 of the admissible orders and can construct 5-sparse STS for two residue classes modulo 54.

For 5-sparse STS, we present a construction utilizing 4-sparse STS.

Lemma 2 *If there exists a* 4*-sparse* STS(v)*, then there also exists a* 5*-sparse* STS($9v - 8$).

Combining Theorem 1 with Lemma 2 gives:

Theorem 3 *There exists a* 5*-sparse* STS(v) *for every* $v \equiv 1, 19 \pmod{54}$ *except for* $v = 55, 109$.

As far as the author knows, this is the first result on the existence of 5-sparse STS covering a residue class completely.

References

[1] C. J. Colbourn, E. Mendelsohn, A. Rosa, and J. Širáň, Anti-mitre Steiner triple systems, Graphs Combin. **10** (1994) 215-224.

[2] P. Erdös, Problems and results in combinatorial analysis, Creation in Math. **9** (1976) 25.

[3] Y. Fujiwara, Constructions for anti-mitre Steiner triple systems, J. Combin. Des. to appear.

[4] M. J. Grannell, T. S. Griggs, and C. A. Whitehead, The resolution of the anti-Pasch conjecture, J. Combin. Des. **8** (2000) 300-309.

[5] A. C. H. Ling, A direct product construction for 5-sparse triple systems, J. Combin. Des. **5** (1997) 443-447.

[6] A. C. H. Ling, C. J. Colbourn, M. J. Grannell, and T. S. Griggs, Construction techniques for anti-Pasch Steiner triple systems, J. London Math. Soc. (2) **61** (2000) 641-657.

Additive structures of BIB designs with III

澤正憲（広島大学大学院理学研究科）

1. 加法構造をもつBIBDの分類

BIBD$(v=sk,b,r,k,\lambda)$が**加法構造**をもつとは、s個の異なるincidence matrixN_i $(i=1,\ldots,s)$が条件 (1)$\sum_{i=1}^{s}=J$, (2)$\forall i,\forall j$, に対してN_i+N_jがBIBD$(v=sk,k',\lambda')$の異なるincidence matrixになる、を満たす時をいう [1, 2]。ただしJは$v\times b$で全ての成分が1であるような行列を意味する。明らかに、(1) は各N_iが行列の成分として互いに排反なことを保証しているため$k'=2k$を満たす。加法構造をもつための必要条件として次を示した [3].

定理1: s個の異なるN_iが条件 (1)、(2) を満たすならば、

$$2\lambda\equiv 0 \mod k-1.$$

定理2: $k>\lambda$とする. 加法構造をもつBIBD$(v=sk,\ b,\ r,\ k,\ \lambda)$は次の二つに限られる：

(I) $v=sk,b=s(sk-1)/2,r=(sk-1)/2,k,\lambda=(k-1)/2,$

(II) $v=sk,b=s(sk-1),r=sk-1,k,\lambda=k-1,$

ただし、(I) で$k\equiv s\equiv 1 \bmod 2$.

定理3: $k=\lambda$とする。加法構造をもつBIBD$(v=sk,\ b,\ r,\ k,\ \lambda)$は次の二つに限られる：

(III) $v=2s,b=2s(2s-1),r=2(2s-1),k=2,\lambda=2,$

(IV) $v=3(2l+1),b=3(2l+1)(3l+1),r=3(3l+1),k=3,\lambda=3,$ $l\geq 1$.

2. 相互直交ラテン方格を利用した解の構成法

定理4: sが奇素数または奇素数べきならば、BIBD$(s^n,\ s(s^n-1)/2,$ $(s^n-1)/2,\ s^{n-1},\ (s^{n-1}-1)/2)$で加法構造をもつものが存在する.

定理5: sが2のべきならば、BIBD$(2^n,\ 2^{n-1}(2^n-1),\ (2^n-1)/2,\ 2,\ 1)$で加法構造をもつものが存在する.

定理5は相互直交ラテン方格を利用した直接的構成法による [3]。定理4の系列は定理1(I) に属する. これはn次元アフィン空間から再帰的に得られる [3]. 一般に (I) に属するBIBDの解が得られればそのincidence matrixの並置によって (II) に属するBIBDの解が得られることがわかる. 従って、この系列から (II) に属する系列も得る. 一方定理5の系列は (II) に属し、並置をとることで (III) に属する系列も得る.

3. Resolvable BIBD の分類

$s=3$ の時は条件 (1) と条件 (2) は同値な概念である ([2])。また一般に resolvable BIBD は条件 (1) を満たす ([1]) . $s=3$ の時先の (I) に属する resolvable BIBD は affine resolvable となる.

定理 7 [3]: $v=3k$, $k=2\lambda+1$ とすると, Resolvable BIBD は affine でそのパラメタは、

(V) $v=9(2p+1), b=3(9p+4), r=9p+4, k=3(2p+1), \lambda=3p+1$,
ただし、$p \geq 0$.

$v=3^n$ に対して (V) に属する系列が得られている ([2])。一方 3 のべき以外の v に対しては (V) に属する indivisual な例すら得られておらず、$v \leq 224$ なる全ての v に対する非存在が確かめられている。$v=225=3^2 5^2$ の時、パラメタ $v=225$, $b=336$, $r=112$, $k=75$, $\lambda=37$ の resolvable BIBD の存在性については知られていない.

4. 今後の課題

(III) の解で v が 2 のべきでないものとして現在までに知られているのは次の 2 つだけである :

・$v=6$, $b=30$, $r=10$, $k=2$, $\lambda=2$

・$v=10$, $b=90$, $r=18$, $k=2$, $\lambda=2$

(IV) については v が 3 のべきならば解の存在性を示した ([2]). 先と同様に v が 3 のべきでない解として現在までに知られているのは 1 つだけである :

・$v=21$, $b=210$, $r=30$, $k=3$, $\lambda=3$

今後の課題として (III), (IV) の解でその存在性が未知な最小の s に対する BIBD をあげておく :

次のパラメタをもつ BIBD は加法的な解をもつか

問題 1: $v=12$, $b=132$, $r=22$, $k=2$, $\lambda=2$,

問題 2: $v=15$, $b=105$, $r=21$, $k=3$, $\lambda=3$.

参考文献

[1] Kiyama, H., Matsubara, K., Matsumoto, D., Sawa, M. and Kageyama, S.(2004). Decomposition of an all-one matrix into incidence matrices of a BIB design. submitted.

[2] Matsubara, K., Sawa, M., Matsumoto, D., Kiyama, H. and Kageyama, S.(2004). An addition structure on incidence matrices of a BIB design. Ars Combin., to appear.

[3] Sawa, M., Matsubara, K., Matsumoto, D., Kiyama, H. and Kageyama, S.(2004). The spectrum of BIB designs with additive structure.

Additive structures of BIB design IV

—加法構造をもつBIBDの構成法について—

広島大学大学院　教育学研究科　松原和樹

1　はじめに

ここでは加法構造をもつBIBDの具体的な構成法を紹介し，小さいパラメータのBIBDに関しての加法構造の存在に関するリストをあげる．

2　再帰的構成法

定理 1 sが奇素数または奇素数巾のとき，加法構造をもつBIBD$(v = sk, b, r, k, \lambda)$が存在するならば，加法構造をもつBIBD$(v^* = s^2k, b^* = s(s-1)[(s+1)r - s\lambda]/2, r^* = (s-1)[(s+1)r - s\lambda]/2, k^* = sk, \lambda^* = (s-1)r/2)$が存在する．

系 1 sが奇素数または奇素数巾のとき，加法構造をもつBIBD$(v^* = s^2, b^* = s(s+1)(s-1)^2/4, r^* = (s+1)(s-1)^2/4, k^* = s, \lambda^* = (s-1)^2/4)$が存在する．

定理 2 sが奇素数または奇素数巾のとき，BIBD$(v = sk, b, r, k, \lambda)$に対して分解問題の解が存在するならば，加法構造をもつresolvable BIBD$(v^* = sk, b^* = s^2(s-1)r/2, r^* = s(s-1)r/2, k^* = k, \lambda^* = s(s-1)\lambda/2)$が存在する．

定理 3 $s-1$が奇素数または奇素数巾のとき，BIBD$(v = sk, b, r, k, \lambda)$に対して分解問題の解が存在するならば，加法構造をもつBIBD$(v^* = sk, b^* = s(s-1)(s-2)r/2, r^* = (s-1)(s-2)r/2, k^* = k, \lambda^* = (s-1)(s-2)\lambda/2)$が存在する．

定理 4 sが奇素数または奇素数巾のとき，resolvable BIBD$(v = sk, b, r, k, \lambda)$が存在するならば，加法構造をもつresolvable BIBD$(v^* = sk, b^* = s($

$1)r/2, r^* = (s-1)r/2, k^* = k, \lambda^* = (s-1)\lambda/2)$ が存在する．また s が 2 の巾であるとき，resolvable BIBD$(v = sk, b, r, k, \lambda)$ が存在するならば，加法構造をもつresolvable BIBD$(v^* = sk, b^* = s(s-1)r, r^* = (s-1)r, k^* = k, \lambda^* = (s-1)\lambda)$ が存在する．

3 直接的構成法

定理 5 加法構造をもつBIBD$(v = p^n, b = p^n(p^n-1)/2, r = p(p^n-1)/2, k = p, \lambda = p(p-1)/2)$ は存在する．ただし，p は素数，n は 2 以上の整数である．

定理 6 $2s-1$ が奇素数または奇素数巾のとき，加法構造をもつ BIBD$(2s, s(s-1)(2s-1), (s-1)(2s-1), 2, s-1)$ が存在する．

定理 7 加法構造をもつBIBD$(s^n, s(s^n-1)/2, (s^n-1)/2, s^{n-1}, (s^{n-1}-1)/2)$ は存在する．ただし，s は奇素数または素数巾であり，n は 2 以上の整数である．

参考文献

[1] Bose, R.C. and Manvel, B. (1984). *Introduction To Combinatorial Theory.* Wiley.

[2] Calinski, T. and Kageyama, S. (2003). *Block Design : A Randamization Approach, Volume* II*: Design.* Springer-Verlag.

[3] Colbourn, C. J. and Dinitz, J. H. (ed.) (1996). *The CRC Handbook of Combinatorial Designs.* CRC Press, Boca Raton, USA.

[4] Kiyama, H., Matsubara, K., Matsumoto, D., Sawa, M. and Kageyama, S. (2004). Decomposition of an all-one matrix into incidence matrices of a BIB design. submitted.

[5] van Lint, J. H. and Wilson, R. M. (1994). *A Course in Combinatrics.* Cambridge Univ. Press.

[6] Matsubara, K., Sawa, M., Matsumoto, D., Kiyama, H. and Kageyama, S. (2004). An addition structure on incidence matrices of a BIB design. ARS Combin., to appear.

完全二部グラフを用いた clutter ordering の構成法

東邦大学理学部　　足立 智子

1. はじめに

RAID (redundant arrays of independent disks)とは，ディスクの読み込み・書き込みを複数のディスクで並列に行うことにより，処理速度と安全性を高める技術である．アクセスコストを低減するために，RAID の information disk と check disk を完全グラフの辺と頂点に対応させて information disk の順序付けを考察する cluttered ordering という概念が，Cohen 等(2001)によって導入された．Mueller 等(2004)は，二次元の RAID を完全二部グラフに対応させることで，数理モデル化をおこなった．本稿では，Mueller 等の研究をさらに発展させ，効率的な RAID を構築するために，完全二部グラフの cluttered ordering の構成法について報告する．

2. 二次元の RAID の数理モデル化

まず，information disk には保存したいデータを分割して格納し，check disk には information disk 内のデータが破損した場合に復旧するための冗長データを格納するとする．今，n個の information disk と c個の check disk があるとする．本稿で扱う二次元の RAID では，information disk，check disk を縦横の二次元に配列するので，information disk の個数 $n=m_1\times m_2$ に対し，check disk の個数は $c=m_1+m_2$ となる．本稿では $m_1=m_2$ $(=m)$の場合を扱う．

この二次元のRAIDのcheck diskを頂点，information diskを辺とみなすことで，RAID を完全グラフで表現することができる．$n=m^2$個の information disk，$c=2m$ 個の check disk を持つ二次元の RAID は，上下に m 個づつ計 $c=2m$ 個の頂点，$n=m^2$ 本の辺をもつ完全二部グラフ $K_{m,m}$ に対応する．

図１では，４個の information disk を縦２行，横２列の二次元に配列しているので，対応する check disk は縦方向に２個，横方向２個の計４個となり，完全二部グラフ $K_{2,2}$ で表現できる．

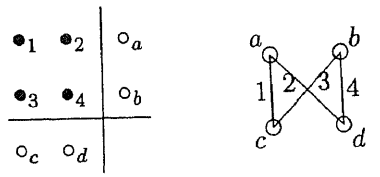

図１．二次元の RAID と完全二部グラフ

3. Cluttered Ordering

あるグラフ $G=(V,E)$について $c=|V|$, $E=\{e_0, e_1, \cdots, e_{n-1}\}$とする．n より小さい正の整数 d を考え，window と呼ぶ．$\{0, 1, \cdots, n-1\}$上の置換 π に対して $V_i^{\pi,d}$ を $\{e_{\pi(i)}, e_{\pi(i+1)}, \cdots, e_{\pi(i+d-1)}\}$の各辺に含まれる点の集合とする．インデックスは mod n で計算し，$0\leq i\leq n-1$ である．d本の辺を持つ部分グラフのアクセスコストをその部分グラフの頂点数で測るのだが，上限(d-最大アクセスコストは $\max_i |V_i^{\pi,d}|$で与えられる．d-最大アクセスコストが f となる辺の順序付けを(d,f)-cluttered ordering と呼ぶ．

完全二部グラフ $K_{3,3}$ の(3,4)-cluttered ordering を図２に示す．

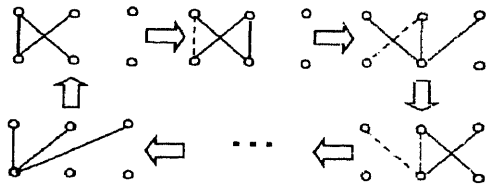

図２．$K_{3,3}$ の(3,4)-cluttered ordering

4. 二部グラフでの Cluttered Ordering

完全グラフにおける cluttered ordering の構成法は Cohen 等(文献[2]および[3])によって与えられた．また，Steiner triple system での cluttered ordering の構成法は Cohen 等(文献[1])によって与えられた．本稿では，二次元の RAID に自然に対応するように，Mueller 等(文献[4])によって与えられた完全二部グラフの cluttered ordering の構成法について述べる．そのために，wrapped Δ-labelling と(d;f)-movement という２つの概念を導入する．

二部グラフ $H=(U,E)$について $U = V\cup W$, $d=|E|$とする．

写像 $\delta : U \rightarrow Z_d \times Z_2$ が

$$\delta(V) \subset Z_d \times \{0\},\ \delta(W) \subset Z_d \times \{1\}$$

を満たし，Z_dの各要素が

$$\{\delta(v) - \delta(w) \mid v \in V, w \in W, (v,w) \in E\}$$

に一つずつ存在するとき，この写像δのことを H のΔ-labelling と呼ぶ．Δ-labelling δは，二部グラフHの頂点をZ_dの各要素でラベル付けしている．

更に，Uの部分集合X, Yに対して，$Z_d \times Z_2$において

$$\delta(Y) = \delta(X) + (\kappa, 0),\quad (\kappa, d) = 1$$

を満たす整数κが存在するとき，このΔ-labelling δをHの wrapped Δ-labelling と呼ぶ．

次に，(d,f)-movement について述べる．同形な二つの二部グラフ $H=(U, E)$, $H'=(U', E')$ について

$U = V \cup W$, $U' = V' \cup W'$, $|V|=|V'|$, $|W|=|W'|$,

$E=\{e_0, e_1, \cdots, e_{d-1}\}$, $E'=\{e'_0, e'_1, \cdots, e'_{d-1}\}$

とする．$\{0, 1, \cdots, d-1\}$上の置換πを用いて，完全二部グラフGを

$$H_0 := H,\quad H_i := (U_i, E_i),\ 1 \leqq i \leqq d$$

と d+1 個の部分グラフに分割する．但し，

$E_i := (E_{i-1} \setminus \{e_{\pi(i-1)}\}) \cup \{e'_{\pi(d+i-1)}\}$,

U_iはE_iの各辺に含まれる頂点の集合

とする．このとき，$H_d = H'$となり，$\max_{0 \leqq i \leqq d} |U_i| = f$ ならば，πをHからH'への(d,f)-movement と呼ぶ．

ここで，wrapped Δ-labelling と(d,f)-movement を用いることにより，完全二部グラフにおける(d,f)- cluttered ordering の存在に関して，次の定理が得られる．

定理 1.（文献[4]） 同形な二部グラフ H, H'に対し，wrapped Δ-labelling と(d,f)-movement が存在するならば，完全二部グラフ $K_{d,d}$において(d,f)-cluttered ordering は存在する．

5. 特別な場合の構成法

本章では，自然数 h, t をパラメータとして，次で与えられる特別な二部グラフ $H(h;t)=(U,E)$について考察する．

頂点集合 $U = V \cup W$は，次のように，各 h(t+1)個の頂点を持つ２つの部分集合 V, W に分けられるとする．

$V := \{v_i \mid 0 \leqq i < h(t+1)\}$,

$W := \{w_i \mid 0 \leqq i < h(t+1)\}$

頂点の個数は，$|U| = 2h(t+1)$となる．

辺集合Eは，次のようにt個の部分集合E_s ($0 \leqq s < t$) に分割されると定める．さらに，部分集合E_sは，それぞれ，E_s', E_s'', E_s'''の３つの部分集合に分けられるとする．

$E_s' := \{\{v_i, w_j\} \mid s \times h \leqq i, j < s \times h + h\}$,

$E_s'' := \{\{v_i, w_{h+j}\} \mid s \times h \leqq j \leqq i < s \times h + h\}$,

$E_s''' := \{\{v_{h+i}, w_j\} \mid s \times h \leqq i \leqq j < s \times h + h\}$,

$E_s := E_s' \cup E_s'' \cup E_s'''$,　$0 \leqq s < t$

$E := \cup_{0 \leqq s \leqq t-1} E_s$

辺の本数は，$|E| = t \times (h^2 + h(h+1)/2 + h(h+1)/2) = th(2h+1)$ となる．

ここで，二部グラフ H(h;t)に関して，自然数 h, t (但し $t \geqq 2$)に対して，次の定理により，(d,f)-movement の存在が保証される．

定理２．（文献[4]） 自然数 h, t (但し $t \geqq 2$)に対して，$d = h(2h+1)$, $f = 4h$ とすれば，二部グラフ H(h;t)に関して E_0 から E_{t-1}への(d,f)-movement が存在する．

よって，H(h;t)に関して，同型な二部グラフへの wrapped Δ-labelling の構成法を与えれば，定理１および定理２より，対応する完全二部グラフにおける cluttered ordering が与えられる．

定理３．（文献[4]） 自然数h, tに対して，二部グラフH(h;t)の任意の wrapped Δ-labelling から，完全二部グラフ $K_{m,m}$の(d,f)-cluttered ordering が得られる．このとき，パラメータの値は，$m = th(2h+1)$, $d = h(2h+1)$, $f = 4h$ となる．

Mueller 等は，H(1;t), H(2;t), H(h;1)に対して，それぞれに同形な二部グラフへの wrapped Δ-labelling の構成法を与えた．本稿では，この構成法を紹介するとともに，さらに研究を発展させ，H(h;2) に関して，同形な二部グラフへの wrapped Δ-labelling の構成法の予想を与える．

文　献

[1] M. Cohen, and C. Colbourn, Optimal and Pessimal Orderings of Steiner Triple Systems in Disk Arrays, Theoretical Computer Science, vol.297, Issues 1-3, pp.103-117, March 2003.

[2] M. Cohen, and C. Colbourn, Ladder orderings of pairs and RAID performance, Discrete Applied Mathematics, vol.138, no.29, pp.35-46, March 2004.

[3] M. Cohen, C. Colbourn, and D. Froncek, Cluttered orderings for the complete graph, COCOON 2001: Lect. Notes Comp. Sci. 2108, pp.420-431, Springer- Verlag, 2001.

[4] M. Mueller, T. Adachi, and M. Jimbo, Cluttered orderings for the Complete Bipartite Graph, Discrete Applied Mathematics, submitted.

2部グラフにおける自己補グラフの数え上げについて

近畿大学理工　田澤新成

有限集合Vに対し、点対の集合$\binom{V}{2}=\{\{x,y\}\subset V|x\neq y\}$の部分集合$K$を考える。$V$と$K$および$K$の部分集合$E$との組$(V,K,E)$は$V$を点集合、$E$を辺集合とするグラフである。グラフ$G=(V,K,E)$について、グラフ$(V,K,K-E)$を$G$の$K$に関する補グラフといい、$\overline{G}$とかく。$G$と$\overline{G}$が同型であるとき、$G$は$K$に関する自己補グラフといわれる。本稿では、互いに同型でないKに関する自己補グラフの個数を求める公式を考える。特に、Kの特別な場合である2部グラフにおける自己補グラフの個数を求める公式を与える。

集合$W=\{0,1\}$に対し、写像$f:K\to W$は1つのグラフを表現する。隣接関係は、$\{x,y\}\in K$に対し、$f(x,y)=1$のとき、2点x,yを隣接させ、$f(x,y)=0$のとき、x,yは隣接させない。$\{\{x,y\}\in K|f(x,y)=1\}$が$f$の表すグラフの辺集合である。

AをV上の置換群とする。$\alpha\in A$に対し、$\alpha'\{x,y\}=\{\alpha x,\alpha y\}$により定義される$\alpha'$は$K$上の置換であり、$A'=\{\alpha'|\alpha\in A\}$は$K$上の置換群である。$\mathfrak{S}_2$を$W$上の対称群とする。$\alpha'\in A',\tau\in\mathfrak{S}_2$に対し、写像$(\alpha';\tau):W^K\to W^K$を$(\alpha';\tau)f(z)=\tau f(\alpha z),z\in K$により定義すると、$\mathfrak{S}_2^{A'}=\{(\alpha';\tau)|\alpha'\in A',\tau\in\mathfrak{S}_2\}$は$W^K$上の置換群である。$f,g\in W^K$に対し、$(\alpha';\tau)f=g$となる$(\alpha';\tau)\in\mathfrak{S}_2^{A'}$が存在するならば、$f$と$g$は同値であるといわれる。ここで、$\tau$が$\mathfrak{S}_2$の単位元ならば、$f$と$g$は同型であるといわれる。もちろん、同型ならば、同値である。同値関係により、W^Kは類別され、各類は$\mathfrak{S}_2^{A'}$による軌道と呼ばれる。置換$\alpha'\in A'$の型を$(j_1(\alpha'),j_2(\alpha'),...,j_m(\alpha'))$と書く。ここに、$m=|K|$であり、$j_k(\alpha')$は$\alpha'$を巡回成分に分解した場合の長さ$k$の巡回成分の個数である。

多項式

$$Z(A';s_1,s_2,...,s_m)=\frac{1}{|A'|}\sum_{\alpha'\in A'}s_k^{j_k(\alpha')}$$

はA'の巡回指数と呼ばれる。$s_1=s_2=\cdots=s_m=2$とおき、式$Z(A';2,2,...,2)$はKの部分集合を辺集合にもつグラフの個数を表す。次の定理が知られている（p.137, [1]）。

定理 1. W^Kの置換群$\mathfrak{S}_2^{A'}$による軌道の個数$N(\mathfrak{S}_2^{A'})$は

$$N(\mathfrak{S}_2^{A'})=\frac{1}{2}\{Z(A';2,2,2,...)+Z(A';0,2,0,2,...)\}\tag{1}$$

で与えられる。

$N(\mathfrak{S}_2^{A'})$はKに関しての補グラフを除いての位数$|V|$のグラフ（辺集合はKの部分集合）の個数を表している。$2N(\mathfrak{S}_2^{A'})$はKの部分集合を辺集合にもつグラフの個数であるが、ただし次の事柄が観察される。

- グラフがKに関して自己補グラフならば、それは重複して（2度）数えられている。
- そうでなければ、ただ1度だけ数えられている。

したがって、Kに関する自己補グラフの個数$s(K)$は

$$s(K)=2N(\mathfrak{S}_2^{A'})-Z(A';2,2,...,2)\tag{2}$$

となる。それ故

定理 2. K に関する自己補グラフの個数 $s(K)$ は

$$s(K) = Z(A'; 0, 2, 0, 2, ...) \tag{3}$$

で与えられる。

$K = \binom{V}{2}$ のときは $A = \mathfrak{S}_n$、$(n = |V|)$ を考え、$s(K)$ は Read[2] によって与えられたものである。有限集合 X, Y をとり、$K = X \times Y$ を考える。この場合は X, Y を部集合とする 2 部グラフを考察の対象にしている。$p = |X|, q = |Y|$ とおく。$\mathfrak{S}_p$ を X 上の対称群、$\mathfrak{S}_q$ を Y 上の対称群とし、$\mathfrak{S}_p \times \mathfrak{S}_q$ の巡回指数は

$$Z(\mathfrak{S}_p \times \mathfrak{S}_q) = \frac{1}{p!q!} \sum_{(\alpha,\beta)\in \mathfrak{S}_p \times \mathfrak{S}_q} \prod_{r,t=1}^{p,q} s_{\ell(r,t)}^{d(r,t) j_r(\alpha) j_t(\beta)}$$

で与えられる。ここで、$d(r,t)$ は r と t の最大公約数、$\ell(r,t)$ は最小公倍数を表す。必要とする A' の巡回指数は

$$Z(A') = \begin{cases} Z(\mathfrak{S}_p \times \mathfrak{S}_q) & (p \neq q \text{ のとき}) \\ \frac{1}{2}(Z(\mathfrak{S}_q \times \mathfrak{S}_q) + \\ \quad \frac{1}{p!} \sum_{\alpha \in \mathfrak{S}_p} \prod_{k:odd} s_k^{j_k(\alpha)} \prod_k s_{2k}^{k\binom{j_k(\alpha)}{2} + [k/2] j_k(\alpha)} \prod_{r<t} s_{2\ell(r,t)}^{d(r,t) j_r(\alpha) j_t(\alpha)}) & (p = q \text{ のとき}) \end{cases}$$

で与えられる。したがって、定理 2 を用いて、$X \times Y$ に関する自己補グラフ（2 部グラフにおける自己補グラフ）の個数が求められる。以下にその数値例を記載する。

p	q	$s(X \times Y)$
2	3	3
2	4	6
2	5	6
2	6	10
2	7	10
3	4	7
3	5	0
3	6	14

p	q	$s(X \times Y)$
3	7	0
4	5	37
4	6	114
4	7	147
5	6	196
5	7	0
6	7	2439

p	p	$s(X \times X)$
1	1	0
2	2	2
3	3	0
4	4	16
5	5	0
6	6	649
7	7	0

参考文献

[1] F. Harary and E.M.Palmer, Graphical Enumeration, Academic Press, New York 1973

[2] R.C. Read, On the number of self-complementary graphs and digraphs, Journal London Math. Soc. **38**(1963), 99-104.

A New Paradigm of Hybrid Encryption Scheme

Kaoru Kurosawa[1] and Yvo Desmedt[2]

[1] Ibaraki University, Japan
kurosawa@cis.ibaraki.ac.jp
[2] Dept. of Computer Science, University College London, UK, and
Florida State University (USA)

Abstract. In this paper, we show that a key encapsulation mechanism (KEM) does not have to be IND-CCA secure in the construction of hybrid encryption schemes, as was previously believed. That is, we present a more efficient hybrid encryption scheme than Shoup [3] by using a KEM which is not necessarily IND-CCA secure. Nevertheless, our scheme is secure in the sense of IND-CCA under the DDH assumption in the standard model. This result is further generalized to universal$_2$ projective hash families.

Keywords: hybrid encryption, KEM, standard model

1 Background

Cramer and Shoup showed the first provably secure practical public-key encryption scheme in the standard model [1, 2]. It is secure against adaptive chosen ciphertext attack (IND-CCA) under the Decisional Diffie-Hellman (DDH) assumption. They further generalized their scheme to projective hash families [2]. (In the random oracle model, many practical schemes have been proven to be IND-CCA, for example, OAEP+, SAEP, RSA-OAEP, etc. However, while the random oracle model is a useful tool, it does not rule out all possible attacks.)

On the other hand, a hybrid encryption scheme uses public-key encryption techniques to derive a shared key that is then used to encrypt the actual messages using symmetric-key techniques.

For hybrid encryption schemes, Shoup formalized the notion of a key encapsulation mechanism (KEM), and an appropriate notion of security against adaptive chosen ciphertext attack [3, 2]. A KEM works just like a public key encryption scheme, except that the encryption algorithm takes no input other than the recipient's public key. The encryption algorithm can only be used to generate and encrypt a key for a symmetric-key encryption scheme. (One can always use a public-key encryption scheme for this purpose. However, one can construct a KEM in other ways as well.) A secure KEM, combined with an appropriately secure symmetric-key encryption scheme, yields a hybrid encryption scheme which is secure in the sense of IND-CCA [3].

Shoup presented a secure KEM under the DDH assumption [3]. As a result, his hybrid encryption scheme is secure in the sense of IND-CCA under the DDH assumption in the standard model [3].

2 Our Contribution

In order to prove the security of hybrid encryption schemes, one has believed that it is essential for KEM to be secure in the sense of IND-CCA, as stated in [2, Remark 7.2, page 207].

In this paper, however, we disprove this belief. That is, it is shown that KEM does not have to be CCA secure, as was previously believed. On a more concrete level, we present a more efficient hybrid encryption scheme than Shoup [3] by using a KEM which is not necessarily secure in the sense of IND-CCA. Nevertheless, we prove that the proposed scheme is secure in the sense of IND-CCA under the DDH assumption in the standard model.

In a typical implementation, the underlying Abelian group may be a subgroup of Z_p^*, where p is a large prime. In this case, the size of our ciphertexts is $|p|$ bits shorter than that of Shoup [3]. The number of exponentiations per encryption and that of per decryption are also smaller. (Further, our scheme is more efficient than the basic Cramer-Shoup scheme [1, 2].)

This shows that one can start with a weak KEM and repair it with a hybrid construction. Eventually, more efficient hybrid encryption schemes could be obtained.

Our KEM is essentially a universal$_2$ projective hash family [2]. We present a generalization of our scheme to universal$_2$ projective hash families also.

The only (conceptual) cost one pays is that one needs to assume a simple condition on the symmetric encryption scheme. Namely, any fixed ciphertext is rejected with overwhelming probability, where the probability is taken over keys K. This property is already satisfied by the symmetric encryption scheme SKE which is used in the hybrid construction of Shoup [3]. Hence the SKE can be used in our hybrid construction too.

Our result gives new light to Cramer-Shoup encryption schemes [1, 2] and opens a door to design more efficient hybrid encryption schemes.

References

1. R. Cramer and V. Shoup, "A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack," *Advances in Cryptology - CRYPTO'98*, Lecture Notes in Computer Science Vol. 1462, H. Krawczyk ed., Springer-Verlag, 1998.
2. R. Cramer and V. Shoup, Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack, SIAM Journal on Computing, Volume 33, Number 1, pp. 167-226 (2003)
3. V. Shoup, Using Hash Functions as a Hedge against Chosen Ciphertext Attack, EUROCRYPT 2000, pp.275-288 (2000)

グループ鍵共有における安全性の検討

慶應義塾大学大学院 理工学研究科　　小田 哲

1　内部不正

多対多の通信で起こりうる内部不正の存在を考える。そして、鍵の共有の途中で、不正者同士が結託してほかのユーザーに誤った鍵を共有させようとする内部不正者の攻撃を想定し、起こりうる不正を定義する。さらにユーザー同士が結託する結託攻撃を定義し、不正者たちのチャレンジとなる不正検知回避、及び不正者検知回避を定義する。これらを使って、不正者たちの有利さを示すアドバンテージを $Adv^{\text{不正検知回避}-\text{結託攻撃}}, Adv^{\text{不正者検知回避}-\text{結託攻撃}}$ として定義する。さらに、グループ鍵共有プロトコルを提案し、ある条件のもとでこの提案プロトコルが結託攻撃に対する不正検知回避や結託攻撃に対する不正者検知回避に対して安全であることを証明する。

2　アドバンテージ

2.1　定義：アルゴリズム

- $A_{E_m}^{\text{不正}}$ は、確率的アルゴリズムで、t ラウンド目において $^{\forall}U_n \in E_m$ は、$t-1$ ラウンド目までの公開鍵と、E_m に所属するメンバーの秘密鍵、および公開情報 s を用いて不正を行うかどうか決定し、$atk_{E_m}^{(t)}$ を出力する。
- $k_I()$ は決定的アルゴリズムで、t ラウンド目において公開鍵と秘密鍵をそのまま $atk_I^{(t)}$ として出力する。
- $K()$ は決定的アルゴリズムで、t ラウンド目において全員の公開鍵と秘密鍵のセット $atk_\Omega^{(t)}$ を入力するとプロトコルに従い、次のラウンドの公開鍵、秘密鍵、公開情報を出力する。
- $B_k^{\text{不正検知}}$ は決定的アルゴリズムで、公開鍵 $\mathbf{Pk}$ とユーザー k が知る秘密鍵 $\mathbf{Sk}_k$、及び公開情報を入力すると、プロトコルが正常に動作しているか異常があるかを判定してその結果を出力する。
- $B_k^{\text{不正者検知}}$ は決定的アルゴリズムで、公開鍵 Pk とユーザー k が知る秘密鍵 Sk_k、及び公開情報を入力すると、全ての $U_k \in \Omega$ に対して U_k が不正者か否かを判定したリストを出力する。

2.2　定義：攻撃とチャレンジ

- $U_n \in E_m$ が不正を行ったときに、全ての監視者 $d \in D$ が不正を検知できないようにするというチャレンジを不正検知回避と呼ぶ。
- 不正が検知されたもとで、任意の $d \notin E_m$ が用いる不正者検知アルゴリズム $B_d^{\text{不正者検知}}$ において E_m に所属する少なくとも一人のメンバー U_n が不正を行っていないと判定させる、もしくは E_m に属さないユーザー U_k が不正を行ったと判定させるというチャレンジを不正者検知回避と呼ぶ。

2.3　不正検知回避に対するアドバンテージ

ある不正者グループ E_m が結託攻撃を行ったという条件のもとで $\mathcal{E}$ のアドバンテージを t ラウンド目に監視者 $d \in D$ が騙される確率を用いて定義する。

$$\Pr_k^{(t)}[G^{(t)};\ Atk^{(t)} \neq \{\mathbf{Pk}^{(t)}, \mathbf{Sk}^{(t)}\} :\ B_k^{\text{不正検知}}(\mathbf{Pk}^{(t+1)}, \mathbf{Sk}_k^{(t+1)}, s^{(t+1)}) = \text{正常}]$$

ただし t ラウンド目における事象 $G^{(t)}$ を次のように置く。

$$G^{(t)} = [^{\forall}E_m \in \mathcal{E},\ atk_{E_m}^{(t)} \leftarrow A_{E_m}^{\text{不正}}(\mathbf{Pk}^{(t-1)}, \mathbf{Sk}_{E_m}^{(t-1)}, s^{(t-1)});\ atk_I^{(t)} = k(pk_I^{(t)}, sk_I^{(t)});\ (\mathbf{Pk}^{(t+1)}, \mathbf{Sk}^{(t+1)}, s^{(t+1)}) = K(atk_\Omega^{(t)})]$$

これを用いて

$$Adv^{\text{不正検知回避}-\text{結託攻撃}} =$$

$$\Pr[^{\forall}t, G^{(t)};$$
$$Atk^{(T)} \neq \{\mathbf{Pk}^{(T)}, \mathbf{Sk}^{(T)}\} :$$
$$^{\forall}d \in D, ^{\forall}t \leq T \text{で正常を出力}]$$

2.4 不正者検知回避に対するアドバンテージ

$$Adv^{\text{不正者検知回避}-\text{結託攻撃}}(k) =$$
$$\Pr[^{\forall}t, G^{(t)};$$
$$Atk^{(T)} \neq \{\mathbf{Pk}^{(T)}, \mathbf{Sk}^{(T)}\};$$
$$C'_{\Omega} = B_d^{\text{不正者検知}}(\mathbf{Pk}^{(t+1)}, \mathbf{Sk}_d^{(t)}, s^{(t+1)}) :$$
$$^{\exists}k, C'_k \neq C_k]$$

3 提案プロトコル

D による結託攻撃のもとでの生成中不正検知を可能にするプロトコルとして、次のようなグループ鍵生成プロトコルを提案する。U_k は、

(0) $r \leftarrow_R \{0,1\}^p, sk_k^{(1)} = r$

(1) $pk_k^{(t)} = \alpha^{sk_k^{(t)}}$

(2) $(pk_k^{(t)}||t||$ 鍵交換 $ID)$ に U_k の署名を付け、$U_{\overline{k}}$ の公開鍵で暗号化して $U_{\overline{k}}$ に送信する。

(3) $U_{\overline{k}}$ から受信したデータを自分の秘密鍵で復号し、$U_{\overline{k}}$ の署名があることを確認し、$pk_{\overline{k}}$ を取り出す。

(4) $h_k^{(t)} = Hash(pk_k^{(t)}||k||$ 鍵交換 $ID)$ を TA に預託する。

(5) $^{\forall}k, h_k^{(t)}$ が預託されたら、TA は $pk_k^{(t)}$ を要求するので、U_k の署名を付けて $pk_k^{(t)}$ を送信する。

(6) $sk_k^{(t+1)} = (pk_{\overline{k}})^{sk_k^{(t)}}$

(7) $t := T$ でなければ $t := t+1$,(1) へ

(5) と (6) との間で、TA は、全ての預託されたハッシュ値が、$^{\forall}k, h_k^{(t)}$ となるかどうかを調べ、ならなかった場合は、不正が起きたと判定する。不正が起きたと判定した場合、TA は全員から $\mathbf{sk}^{(1)}$ を取得し、次のような $B_{TA}^{\text{不正者検知}}$ を動作させる。

- 全員に○をつける。
- プロトコルを提出された $\mathbf{sk}^{(1)}$ を元に TA 内部だけで実行する。
- 預けられた $pk_k^{(t)}$ が正しく $pk^{(t+1)_k}$ が正しくない場合、$pk_{\overline{k}^{(t)}}$ を k に提出させる。
- $pk_{\overline{k}^{(t)}}$ の $\overline{k}$ の署名が正当ならば $\overline{k}$ に×をつける。
- $pk_{\overline{k}^{(t)}}$ の $\overline{k}$ の署名が正当でない場合、k に×を付け、$U_{\overline{k}}^{(t)}$ に $sk_{\overline{k}}^{(t)}$ と $pk_{k^{(t)}}$ を提出させる。$pk_{k^{(t)}}$ の署名が正当でない、もしくは $pk_{\overline{k}^{(t+1)}} \neq (pk_k^{(t)})^{sk_{\overline{k}}^{(t)}}$ にならない場合は、$\overline{k}$ に×をつける。

最終ラウンドまでこれを繰り返し、最終的に×を付けられた人のみと通信をしている人に△を付ける。ただし、U_n が $sk_n^{(t)}$ を提出しなかった場合、U_n に×を付け、$U_{\overline{n}} = U_k$ に $sk_k^{(t+1)}$ を提出させて、続きを実行する。

4 安全性の検討

この提案プロトコルにおけるアドバンテージが、ハッシュ関数が偶然衝突する確率、もしくは時間 s 以内に電子署名が偽造出来る確率よりも小さいことを証明する。

参考文献

[1] G. Ateniese, M. Steiner and G. Tsudik: New multiparty authentication services and key agreement protocols. *IEEE Journal of Selected Areas in Communications*, 18-4, **628-639**, 2000.

[2] J. Pieprzyk, and Huaxiong Wang: Malleability Attacks on Multi-Party Key Agreement Protocols. *Progress in Computer Science and Applied Logic*, Vol. 23 **277-288**, 2004.

[3] Y. Kim, A. Perrig, and G. Tsudik: Simple and fault-tolerant key agreement for dynamic collaborative groups. *Thechnical Report 2, USC Technical Report* **00-737**, 2000.

Bayesian network を用いた positive detecting algorithm の収束性と組合せ構造との関係について

上原 啓明（慶應義塾大学大学院・理工学研究科）
神保 雅一（名古屋大学大学院・情報科学研究科）

1 はじめに

DNA library screening では、たくさんの DNA の断片 (A, T, G, C の塩基列) の中から，ある試験に対して陽性 (positive) 反応を示す塩基列 (clone と呼ぶ) を見出す試験が行なわれる．現状では，この試験の結果に false positive, false negative などの判定誤りが起こることは避けられない．それらの誤りの存在を仮定して，その下で判定誤りの確率を小さくする実験の計画および識別アルゴリズムの開発が重要である．

2 2段階グループテスト

そのための一つの方法として，2段階グループテストと呼ばれる検査方法が用いられることがある ([1], [2], [3], [4], [5])．n 種の各 clone を一つ一つテストすると n 回のテストが必要になるが，通常，positive clone の割合は，0.0001〜0.005 程度のことが少なくない．このような場合，複数の塩基列をひとつにまとめてそのグループ (pool と呼ぶ) に対して，反応試験を行い，その結果が negative の場合には，その pool に含まれるすべての塩基列が negative であることを 1 回のテストで判定できる．また，positive の場合には，その中のいずれかの clone が positive であるとわかる．このように，さまざまな組合せの pool に対してテストを行い，その結果から positive の確率が高い clone を抽出して，それらの clone にのみ個別にテストを行って positive clone を識別する方法を2段階グループテストと呼び，テストに用いられるさまざまな clone の集合からなる pools の族を pooling design と呼んでいる．

したがって，2段階グループテストにおける positive 識別の手順は，

(i) pooling design の計画
(ii) グループテストによる実験
(iii) グループテストの判定結果から positive の確率が高い clone を抽出
(iv) (iii) で抽出された各クローンに対して個別テスト

となる．(ii), (iv) の実験精度は，実際に行われる実験に依存するため，ここでは，(i) の実験の計画と (iii) の識別アルゴリズムに注目し，

(1) 与えられた clone の数と positive 識別アルゴリズムに対して，pool の数が少なく positive clone を識別する能力が高くなる pooling design の計画と
(2) pooling design と実験結果が与えられた際に，高速に精度良く positive clone を識別するアルゴリズムの開発

の両面から研究を行う．

3 BNPD の収束性と組合せ構造との関係

本研究では，ベイジアンネットワークを用いたアルゴリズムBNPD (Bayesian network pool results decoder) の収束性と組合せ構造との関係を調べている．そこで，どのような pooling design を用いた場合に収束せずに振動が起きてしまうのかを考える．例えば，この問題を簡略化するとある条件の下では漸化式

$$A^{(t+1)} = 1 - \frac{1-2q}{1-q}\left\{1 - \frac{p}{(1-p)A^{(t)k-1} + p}\right\}^{r-1}$$

を満たすような数列 $\{A^{(t)}\}_{t=0}^{\infty}$ の収束性を調べる必要があることがわかる．ここで，p は各 clone が positive であるという先見確率，q は実験での誤り確率，k は1つの clone が属する pool の数，r は1つの pool に属する clone の数を表している．この数列に対しては次の定理が成り立つ．

定理 1. $k \geq 3$, $r \geq 3$ に対して，上の数列 $\{A^{(t)}\}_{t=0}^{\infty}$ が収束しないような p と q が存在する．

本発表では，本定理の証明の概略を説明し，また，本定理から BNPD の計算結果が収束しない場合でも p や q を変えることによってよりよい値に収束するようにできる可能性があることをシミュレーションを行うことによって示した．

参考文献

[1] E. Balliot, B. Lacroix and D. Cohen (1991), Theoretical analysis of library screening using an N-dimensional pooling strategy, *Nucleic Acids Res.*, **19**, 6241-6247.

[2] T. Berger, J. W. Mandell and P. Subrahmanya (2000), Maximally efficient two-stage screening, *Biometrics*, **56**, 833-840.

[3] D-Z. Du and F. K. Hwang (2000), *Combinatorial group testing and its application*, World Scientific Pub. Co.

[4] E. Knill, A. Schliep and D. C. Torney (1996), Interpretation of pooling experiments using the Markov chain Monte Carlo method, *Journal of Computational Biology*, **3**, 395-406.

[5] P. Sham, J. S. Bader, I. Craig, M. O'Donovan and M. Owen (2002), DNA pooling: A tool for large-scale association studies, `www.nature.com/reviews/genetics`, **3**, 862-871.

A construction of OA$(s^t, t+1, s, t)$s by polynomials and their classification

Shintaro Yagi (Keio University)
Masakazu Jimbo(Nagoya University)

An $N \times k$ array A with entries from S is said to be an *orthogonal array with s levels, strength t, k constraints (or factors) and index λ* if every $N \times t$ subarray of A contains each t-tuple based on S exactly λ times as a row. The orthogonal array is denoted by OA$(\lambda s^t, k, s, t)$ or OA(N, k, s, t). In this talk, we show a non-linear construction theorem of an OA$(s^t, t+1, s, t)$, and classify the OA$(4^4, 5, 4, 4)$s that are constructed by our theorem by isomorphism. Now, we give the definition of isomorphism.

Definition 1 *Let A and B be orthogonal arrays. A is said to be isomorphic to B if A coincides with B by the following three operations:*
(i) permutation of rows
(ii) permutation of columns
(iii) permutation of symbols in each column

Next, we define the relationship between orthogonal arrays and functional representations.

Definition 2 *Let A be an $OA(s^t, t+1, s, t)$. A function $f : GF(q)^t \to GF(q)$ is called an explicit functional representation of A if, for each row $(\alpha_0, \cdots, \alpha_t)$ of A,*

$$\alpha_0 = f(\alpha_1, \cdots, \alpha_t)$$

holds. Also, if, for each row $(\alpha_0, \cdots, \alpha_t)$ of A,

$$F(\alpha_0, \cdots, \alpha_t) = 0$$

holds, then $F(\cdot)$ is called an implicit functional representation of A.

Note that, for an explicit functional representation f of A, $F(x_0, \cdots, x_t) = x_0 - f(x_1, \cdots, x_t)$ is an implicit functional representation.

Definition 3 *For a function $f : GF(q)^t \to GF(q)$, let*

$$H = \{(\alpha_0, \cdots, \alpha_t) \in GF(q)^{t+1} | \alpha_0 = f(\alpha_1, \cdots, \alpha_t)\}.$$

If there exist functions

$$x_i = f^{(i)}(x_0, \cdots, x_{i-1}, x_{i+1}, \cdots, x_t)$$

for any i such that

$$H^{(i)} = \{(\alpha_0, \cdots, \alpha_t) \in GF(q)^{t+1} | \alpha_i = f^{(i)}(\alpha_0, \cdots, \alpha_{i-1}, \alpha_{i+1}, \cdots, \alpha_t)\}$$

coincides with H, then f is said to be invertible.

Now, we can prove the following theorem.

Theorem 1 *A function f is an explicit functional representation of an $OA(s^t, t+1, s, t)$, if and only if f is invertible.*

The case of $s = 2$, Cheng (1995) classified any orthogonal arrays with $k = t+1, t+2$ and for any index λ. Moreover, in the case of $s = 3$, Hedayat (1997) showed that all $\mathrm{OA}(3^t, t+1, 3, t)$s are isomorphic whose standard forms are $f(x_1, \cdots, x_t) = x_1 + \cdots + x_t$. Also, in the case of s = 4, Mimura (2004) classified $\mathrm{OA}(4^t, t+1, 4, t)$ for $t \leq 3$. In this talk, generalizing Mimura (2004)'s construction, we obtain the following non-linear construction of OAs.

Theorem 2 *Let $g(x_1, \cdots, x_t)$ be a polynomial over $GF(p^l)$, where l is a multiple of p, such that g is linear for each variable x_i and coefficients of g are in $GF(p)$. And let $r(x) = x + x^p + \cdots + x^{p^{l-1}}$. Then,*

$$x_0 = f(x_1, \cdots, x_t) \stackrel{def}{=} x_1 + \cdots + x_t + g(r(x_1), \cdots, r(x_t))$$

is a functional representation of an $OA(s^t, t+1, s, t)$, where $s = p^l$.

By virtue of Theorem 2, we can construct many OAs by choosing different $g(\cdot)$s. Now, we consider $\mathrm{OA}(4^4, 5, 4, 4)$s constructed by Theorem 2 and classify them by isomorphism. The classification is proceeded as follows:
(i) Let Ω be the set of $\mathrm{OA}(4^4, 5, 4, 4)$s constructed by Theorem 2.
(ii) Identify OAs that are isomorphic by the permutation of variables.
(iii) Find isomorphic OAs by invertibility.
(iv) Find isomorphic OAs by permutation $\sigma : x \to x + \alpha$.
Then, we get the following theorem.

Theorem 3 *There are at least 17 nonisomorphic $OA(4^4, 5, 4, 4)$s that are not linear.*

References

[1]C.-S. Cheng(1995). Some projection properties of orthogonal arrays. *Annals of Statistics* 23 1223-1233.
[2] A. S. Hedayat, J. Stufken and G. Su(1997). On the construction and existence of orthogonal arrays with three levels and indexes 1 and 2. *Annals of Statistics* 25 2044-2053.
[3]K. Mimura(2004). Master's thesis in Keio university.

GA-optimal Partially Balanced Fractional $2^{m_1+m_2}$ Factorial Designs of Resolution R({00,10,01,20}|Ω) with $2 \leqq m_1, m_2 \leqq 4$

Masahide KUWADA[1], Shujie LU[2], Yoshifumi HYODO[3] and Eiji TANIGUCHI[3]

[1] Faculty of Integrated Arts and Sciences, Hiroshima University
[2] Graduate School of Engineering, Hiroshima University
[3] Graduate School of Informatics, Okayama University of Science

We consider a fractional $2^{m_1+m_2}$ factorial design, T, say, with N assemblies, where the three-factor and higher-order interactions are assumed to be negligible. Let $(\theta_{00}', \theta_{10}', \theta_{01}', \theta_{20}', \theta_{02}', \theta_{11}')(=\boldsymbol{\theta}'$, say) be the $1 \times \nu(m_1,m_2)$ vector of the non-negligible factorial effects, where $\nu(m_1,m_2)=1+(m_1+m_2)+(m_1+m_2) \times (m_1+m_2-1)/2$. Then the linear model based on T is given by

$$y(T) = E_T\boldsymbol{\theta} + e_T,$$

where $y(T)$, E_T and e_T are an $N \times 1$ vector of observations, the $N \times \nu(m_1,m_2)$ design matrix whose elements are either 1 or -1 and an $N \times 1$ error vector with mean 0_N and variance-covariance matrix $\sigma^2 I_N$, respectively. The normal equations for estimating $\boldsymbol{\theta}$ are given by $M_T\hat{\boldsymbol{\theta}} = E_T'y(T)$, where $M_T(=E_T'E_T)$ is the information matrix of order $\nu(m_1,m_2)$.

Let T be a $2^{m_1+m_2}$-PBFF design derived from an SPBA$(m_1+m_2;\{\lambda_{i_1,i_2}\})$. Then by using the algebraic structure of the extended triangular multidimensional partially balanced (ETMDPB) association scheme, the information matrix M_T is isomorphic to $\| \kappa_{\beta_1\beta_2}^{a_1a_2,b_1b_2} \| (= K_{\beta_1\beta_2}$, say), where $\kappa_{\beta_1\beta_2}^{a_1a_2,b_1b_2}$ are given by some linear combinations of the indices λ_{i_1,i_2} of an SPBA. Furthermore $K_{\beta_1\beta_2}$ are given by

$$K_{\beta_1\beta_2} = (D_{\beta_1\beta_2} F_{\beta_1\beta_2} \Lambda_{\beta_1\beta_2})(D_{\beta_1\beta_1} F_{\beta_1\beta_2} \Lambda_{\beta_1\beta_2})',$$

where $D_{\beta_1\beta_2}$ and $\Lambda_{\beta_1\beta_2}$ are non-singular diagonal matrices, and the elements of $F_{\beta_1\beta_2}$ corresponding to $\lambda_{a,x}$ $(\beta_1 \leqq a \leqq m_1-\beta_1;\ \beta_2 \leqq x \leqq m_2-\beta_2)$ are given by some functions of the suffixes a and x of $\lambda_{a,x}$.

A parametric function $C\boldsymbol{\theta}$ of $\boldsymbol{\theta}$ is estimable for some matrix C of order $\nu(m_1,m_2)$ if and only if there exists a matrix X of order $\nu(m_1,m_2)$ such that $XM_T=C$. If $C\boldsymbol{\theta}$ is estimable, then its unbiased estimator is given by $C\hat{\boldsymbol{\theta}}$, where $\hat{\boldsymbol{\theta}}$ is a solution of the normal equations, and furthermore $\mathrm{Var}[C\hat{\boldsymbol{\theta}}] = \sigma^2 XM_TX'$.

Definition 1. Under the assumption that the three-factor and higher-order interactions are negligible, if $\theta_{00}, \theta_{10}, \theta_{01}, \theta_{20}$ and some linear combinations of the effects of θ_{02} and of θ_{11} are estimable, then a design is said to be of **resolution R({00,10,01,20}|Ω)**, where Ω={00,10,01,20,02,11}.

In this paper, we focus on obtaining a $2^{m_1+m_2}$-PBFF design of resolution R({00,10,01,20}|Ω) derived from an SPBA$(m_1+m_2;\{\lambda_{i_1,i_2}\})$ with $N<\nu(m_1,m_2)$. Thus we consider a design such that C is isomorphic to $\Gamma_{\beta_1\beta_2}$, where $\Gamma_{00}=\mathrm{diag}[I_4; \Gamma_{00}^*]$, $\Gamma_{10}=\mathrm{diag}[I_2; g_{10}^{1111}]$ (if $m_1 \geqq 3$) (or $\mathrm{diag}[1; g_{10}^{1111}]$ (if $m_1=2$)), $\Gamma_{01}=\mathrm{diag}[1; \Gamma_{01}^*]$ (if $m_2 \geqq 3$) (or $\mathrm{diag}[1; g_{01}^{1111}]$ (if $m_2=2$)), $\Gamma_{20}=1$ (if $m_1 \geqq 4$) (or vanish (if $m_1=2,3$)), $\Gamma_{02}=g_{02}^{02,02}$ (if $m_2 \geqq 4$) (or vanish (if $m_2=2,3$)) and $\Gamma_{11}=g_{11}^{1111}$. Here $\Gamma_{\gamma_1\gamma_2}^* = \| g_{\gamma_1\gamma_2}^{a_1a_2,b_1b_2} \|$ $(\gamma_1\gamma_2=00,01;\ a_1a_2,b_1b_2=02,11)$ and $g_{\beta_1\beta_2}^{a_1a_2,b_1b_2}$ are some constants. Further consider a matrix X of order $\nu(m_1,m_2)$ such that X is iso-

morphic to $\| \chi_{\beta_1\beta_2}^{a_1a_2,b_1b_2} \|$ ($=X_{\beta_1\beta_2}$, say). Then $XM_T=C$ is isomorphic to $X_{\beta_1\beta_2}K_{\beta_1\beta_2}=\Gamma_{\beta_1\beta_2}$. The matrix equations $X_{\beta_1\beta_2}K_{\beta_1\beta_2}=\Gamma_{\beta_1\beta_2}$ with parameter matrices $X_{\beta_1\beta_2}$ have a solution if and only if rank$\{K_{\beta_1\beta_2}'\}$ =rank$\{(K_{\beta_1\beta_2}'; \Gamma_{\beta_1\beta_2}')\}$. Thus we have the following:

Theorem. *Let T be an* SPBA($m_1+m_2;\{\lambda_{i_1i_2}\}$) *with* $N<\nu(m_1,m_2)$, *where* $2\leqq m_1,m_2\leqq 4$. *Then T is a* $2^{m_1+m_2}$-PBFF *design of resolution* R($\{00,10,01,20\}|\Omega$) *if and only if one of the following holds*:

(I) *When* $2\leqq m_1\leqq 4$ *and* $m_2=2$, *there does not exist a design of resolution* R($\{00,10,01,20\}|\Omega$),

(II) *when* $m_1=2$ *and* $m_2=3$ ($\nu(2,3)=16$), $\lambda_{0,1}\geqq 1$, $\lambda_{1,0}\geqq 1$, $\lambda_{1,3}\geqq 1$, $\lambda_{2,2}\geqq 1$, *at least two of* $\{\lambda_{0,0},\lambda_{0,3},\lambda_{2,0},\lambda_{2,3}\}$ *except for* $\{\lambda_{0,0},\lambda_{2,3}\}$ *and* $\{\lambda_{0,3},\lambda_{2,0}\}$ *are nonzero*, $3(\lambda_{0,1}+\lambda_{2,2})+2(\lambda_{1,0}+\lambda_{1,3})+\lambda_{0,0}+\lambda_{0,3}+\lambda_{2,0}+\lambda_{2,3}\leqq 15$ *and* $\lambda_{0,2}=\lambda_{1,1}=\lambda_{1,2}=\lambda_{2,1}=0$, *or its* FCA,

(III) *when* $m_1=m_2=3$ ($\nu(3,3)=22$), $\lambda_{0,1}\geqq 1$, $\lambda_{3,2}\geqq 1$, *at least three of* $\{\lambda_{1,0},\lambda_{1,3},\lambda_{2,0},\lambda_{2,3}\}$ *are nonzero*, $1\leqq \lambda_{0,0}+\lambda_{0,3}+\lambda_{3,0}+\lambda_{3,3}$, $3(\lambda_{0,1}+\lambda_{1,0}+\lambda_{1,3}+\lambda_{2,0}+\lambda_{2,3}+\lambda_{3,2})+\lambda_{0,0}+\lambda_{0,3}+\lambda_{3,0}+\lambda_{3,3}\leqq 21$ *and* $\lambda_{0,2}=\lambda_{a,x}=\lambda_{3,1}=0$ ($1\leqq a, x\leqq 2$), *or its* FCA,

(IV) *when* $m_1=4$ *and* $m_2=3$ ($\nu(4,3)=29$), $\lambda_{0,1}\geqq 1$, $\lambda_{4,2}\geqq 1$ *and* $\lambda_{0,2}=\lambda_{a,x}=\lambda_{4,1}=0(1\leqq a\leqq 3;\ 1\leqq x\leqq 2)$, *and in addition*

(i) $\lambda_{2,0}=\lambda_{2,3}=1$, *and furthermore*

(1) *exactly one of* $\{\lambda_{1,0},\lambda_{1,3},\lambda_{3,0},\lambda_{3,3}\}$ *is nonzero*, $1\leqq\lambda_{0,0}+\lambda_{0,3}+\lambda_{4,0}+\lambda_{4,3}$ *and* $3(\lambda_{0,1}+\lambda_{4,2})+4(\lambda_{1,0}+\lambda_{1,3}+\lambda_{3,0}+\lambda_{3,3})+\lambda_{0,0}+\lambda_{0,3}+\lambda_{4,0}+\lambda_{4,3}\leqq 16$, *or its* FCA,

(2) $(\lambda_{1,0},\lambda_{1,3},\lambda_{3,0},\lambda_{3,3})=(1,1,0,0),(1,0,1,0),(0,1,0,1),(0,0,1,1)$ *and* $3(\lambda_{0,1}+\lambda_{4,2})+\lambda_{0,0}+\lambda_{0,3}+\lambda_{4,0}+\lambda_{4,3}\leqq 8$, *or its* FCA, *or*

(3) $(\lambda_{1,0},\lambda_{1,3},\lambda_{3,0},\lambda_{3,3})=(1,0,0,1),(0,1,1,0)$, $1\leqq\lambda_{0,0}+\lambda_{0,3}+\lambda_{4,0}+\lambda_{4,3}$ *and* $3(\lambda_{0,1}+\lambda_{4,2})+\lambda_{0,0}+\lambda_{0,3}+\lambda_{4,0}+\lambda_{4,3}\leqq 8$, *or its* FCA, *or* .... ,

(V) *when* $m_1=m_2=4$ ($\nu(4,4)=37$), ...

Let $\sigma^2V_T(\alpha)$ be the variance-covariance matrix of the linearly independent estimators in $C\hat{\boldsymbol{\theta}}$. Then put $g_{\gamma_1\gamma_2}^{02,02}(=g_{\gamma_1\gamma_2}^{02,02}(\alpha)$, say)=1 if $\alpha=0$, $1/(1+|w_{\gamma_1\gamma_2}^*|)$ if $\alpha=1$ and $1/\{1+(w_{\gamma_1\gamma_2}^*)^2\}^{1/2}$ if $\alpha=2$ for $\gamma_1\gamma_2=00,01$, where $w_{00}^*=\{2(m_2-1)/m_1\}^{1/2}w_{00}$ and $w_{01}^*=\{(m_2-2)/m_1\}^{1/2}w_{01}$.

Definition 2. If $\mathrm{tr}\{V_T(\alpha)\}\leqq\mathrm{tr}\{V_{T^*}(\alpha)\}$ for any T^*, where T and T^* are $2^{m_1+m_2}$-PBFF designs of resolution R($\{00,10,01,20\}|\Omega$) derived from an SPBA($m_1+m_2;\{\lambda_{i_1i_2}\}$) and an SPBA($m_1+m_2;\{\lambda_{i_1i_2}^*\}$) with N assemblies, $N<\nu(m_1,m_2)$ and $2\leqq m_k$, respectively, then T is said to be **GA_α-optimal** for $\alpha=0,1,2$.

Using the properties of the ETMDPB association algebra, we can obtain GA_α-optimal $2^{m_1+m_2}$-PBFF designs of resolution R($\{00,10,01,20\}|\Omega$).

Table. GA_α-optimal 2^{2+3}-PBFF designs

N	$\boldsymbol{\lambda}'$	$\mathrm{tr}\{V_T(0)\}$	$\mathrm{tr}\{V_T(1)\}$	$\mathrm{tr}\{V_T(2)\}$
12	110110010010	1.61111	1.40400	1.44444
13	110110010011	1.40327	1.19617	1.23661
14	110110011011	1.19691	0.98980	1.03024
15	210110011011	1.15585	0.94874	0.98918

２因子と３因子交互作用に対する検索可能計画の構成

神戸市立工業高専　　末次武明
神戸大学発達科学部　　白倉暉弘

１．はじめに

2^m 要因計画を考え，T_1 ： weight(1 の数) が $0, 1, m-1$ の処理組合せを集めた計画とするとき，$T = T_1 + T_2$（"+" は２つの計画の並置）が，２因子と３因子交互作用から高々２個の未知効果が検索でき（但し，３因子交互作用からの未知効果は高々１個しか含まない），主効果と共に推定可能であるような T_2 を構成したい．

このとき，Srivastava の基本定理に相当する次のような定理が導かれる．

定理１　T が上記の計画であるための必要条件は，T の計画行列において，一般平均と各主効果に対応する $m+1$ 列と，２因子と３因子交互作用に対応する４列を選んだ（但し，３因子交互作用に対応する列は２列までしか取れない）部分行列を G とすると，

$$\text{rank } G = m + 1 + 4$$

であることである．特に、誤差がない場合には十分条件になる。

２．この計画の特徴付け

上記のように，交互作用に対応する列からの４列の取り方には，次の３通りがある．

１）２因子交互作用に対応する列から４列を選ぶ場合

Shirakura,T., Suetsugu,T and Tsuji,T(2002) は，この場合に対して，T が定理１を満たすような T_2 の満たすべき条件を導き，これを満たす次のような行列を ST-array と名付けた．

定義　D を $n \times m$ の (0,1) 行列だとすると，D が n 行，m 列の **ST-array** (ST-array(n,m)) であるのは，T_2 のどの４列を取っても，$\binom{1}{1}, \binom{1}{0}, \binom{0}{1}, \binom{0}{0}$ が全て含まれているような２行が存在するときである．(言い換えれば、同じでもなく 0,1 反転 (complement) でもない２行が存在するときである)

さらに，T_2(ST-array) として，Linear code を使う (LC タイプと呼ぶことにする)，BIBD の転置行列を使う (BI タイプ)，Q.R. を利用する (QR タイプ) という３種の構成方法を示した．

２）２因子交互作用に対応する列から３列，３因子交互作用に対応する列から１列を選ぶ場合

このときは，２因子交互作用に対応する３列の独立性だけを考えれば良いことが出てくるので，G の rank が落ちることはないことが示される．

３）２因子交互作用に対応する列から２列，３因子交互作用に対応する列から２列を選ぶ場合

G の rank が落ちないためには，３因子交互作用に対応する列からどの２列を取っても独立であることを示せばよいことが出てくる．さらに，$\mathbf{g}_i$ を主効果 i に対応する列だとすると，$\mathbf{c}_{ijk} = \mathbf{g}_i * \mathbf{g}_j * \mathbf{g}_k - \mathbf{g}_i - \mathbf{g}_j - \mathbf{g}_k$ を考えて，$\mathbf{c}_{ijk} \neq \mathbf{c}_{lmn}$ （但し，i, j, k と l, m, n には同じものがあっても良い）であればよいことが導かれる．

さらに，$c_{ijk} \neq c_{lmn}$ になるには，T_2 に戻して考えると，ijk の３列で weight が 0 or 1 (タイプ A とする) であり，lmn の３列で weight が 2 or 3 (タイプ B とする) である行が存在するか，または，ijk の３列で タイプ B, lmn の３列で タイプ A である行が存在すればよい．

以上のことから，次の定理が導かれる．

定理2　上記の T_1 に対し，$T = T_1 + T_2$ が2因子交互作用・3因子交互作用から高々2個の未知効果が検索でき（但し，3因子交互作用からの未知効果は高々1個しか含まない），主効果と共に推定可能であるための必要条件は，T_2 が ST-array であり，T_2 から任意に3列と3列を選んだ時，タイプAとタイプBの行が存在するか，またはタイプBとタイプAの行が存在することである．特に、誤差がない場合には十分条件になる。

次に，定理を満たす例を構成するために，定理の条件を満たさない3列と3列の組合せを調べておく．

1) 3因子交互作用に対応する列で，1文字も重ならない場合（$\mathbf{g}_{ijk}$ と $\mathbf{g}_{lmn}$ のとき）

$\mathbf{c}_{ijk} = \mathbf{c}_{lmn}$ となるタイプA－A，タイプB－Bの行を考えると、T_2 からの6列のどの行についても，次のような 1,0 の組合せの 32 通りがある．

i	j	k	l	m	n
0	0	0	0	0	0
1	0	0	0	0	0
			$\sim$		
0	1	1	1	1	1
1	1	1	1	1	1

2) 3因子交互作用に対応する列で，1文字が重なった場合（$\mathbf{g}_{ijk}$ と $\mathbf{g}_{imn}$ のとき）

1) で、$i = l$ となった場合を考えればよく、20通りがある．

3) 3因子交互作用に対応する列で，2文字が重なった場合（$\mathbf{g}_{ijk}$ と $\mathbf{g}_{ijm}$ のとき）

T_2 が ST-array であれば，rank が落ちることはないことが示される．

3．計画の例

T_2 として，ST-array の LC タイプ，BI タイプで，定理の条件を満たすことが示される．

1) LC タイプのとき

$(\binom{m}{1} + \binom{m}{2}) \times 2^m$ の LC タイプでは，上半分の m 行で任意に3列と3列を取った時，タイプA－A，タイプB－Bである行は上記の32通りであるが，下半分の $\binom{m}{2}$ 行（上記 m 行の中の2行の mod 2 での和）でもタイプA－A，タイプB－Bであることから，上記 m 行の取り方はさらに制限され，どの4列でも，同じでなく complement でもない weight2 の行が必ず2行存在するという ST-array の条件に矛盾することが示される．

2) BI タイプのとき

T_2 の6列について2列ずつの内積を考えると，内積の値は一定（会合数）であるが，これらを組み合わせると，この中の4列で、weight2 の行の数が0であることが示され，どの4列でも，同じでなく complement でもない weight2 の行が必ず2行存在するという ST-array の条件に矛盾することが示される．

参考文献

Shirakura,T., Suetsugu,T. and Tsuji,T(2002). Construction of main effect plus two plans for 2^m factorials, J.Statist.plann.Inf.,105,405-415

Ghosh,S. , Shirakura,T. and Srivastava,J.N.(to appear). Model identification using search linear models and search designs, in: Entropy and Search (ed. G.O.H.Katona), the series Bolyai mathematical Studies, János Bolyai mathematical Society.