科研基盤 A「統計科学における数理的手法の理論と応用」
研究代表者：谷口正信（早稲田大学）によるシンポジウム
（科研基盤 B「符号および遺伝子解析実験に共在する組合せ構造とアルゴリズムの研究」
研究代表者：神保雅一（名古屋大学）との共催）

「離散数学の統計科学および関連分野への応用」

世話人　神保　雅一（名古屋大・情報科学）
三嶋　美和子（岐阜大・工）

日 時：　2008 年 9 月 16 日（火）13：40 ～ 18 日（木）11：40
場 所：　下呂温泉　ホテルくさかベアルメリア
〒509-2206　岐阜県下呂市幸田 1811
TEL　0576-24-2020（携帯電話から）　0120-305-380（一般電話から）
URL　http://www.armeria.co.jp/index.html

プログラム

9 月 16 日　（火）

13：40 ～ 14：10　Ying Miao（筑波大院・システム情報工）
Difference Triangle Sets and Monotonic Directed Designs

14：10 ～ 14：40　籾原 幸二（名古屋大院・情報科学）
Difference Families of Block Size 4, 5 Related to OOCs and CACs

14：40 ～ 14：50　＜Break＞

14：50 ～ 15：40　Cunsheng Ding（Dept. of CSE, HKUST, Hong Kong）
Binary Sequences with Optimal Autocorrelation and Period $N \equiv 1 \pmod 4$ and $N \equiv 2 \pmod 4$

15：40 ～ 15：50　＜Break＞

15：50 ～ 16：40　Hung-Lin Fu（Dept. of Applied Math., National Chiao Tung Univ, Taiwan）
Grid-Block Designs and Packings

16：40 ～ 16：50　＜Break＞

16：50 ～ 17：20　門脇 聖（島根県立吉賀高校）・景山 三平*（広島工業大・環境）
Affine α-Resolvable PBIB Design の特徴づけと構成

9 月 17 日 （水）

9：30 ～ 10：00　市村 尚代*（阪府大院・工）・丸山 芳人（阪府大院・工）・
田中 秀和（阪府大院・工）・栗木 進二（阪府大院・工）
非小細胞肺ガン患者のデータ解析

10：00 ～ 10：30　谷口 英司（国際自然研）・兵頭 義史（岡山理大院・総合情報・
クワ田 正秀*（広島大院・工）
Balanced Fractional 3^m Factorial Designs of Resolutions R({10,01} S|Ω)

10：30 ～ 10：40　＜Break＞

10：40 ～ 11：10　小林 みどり（静岡県立大・経営情報）・宮内 美樹（NTT）・
中村 義作*（東海大・教育開発研究所）
一般化した実験計画法

11：10 ～ 11：40　小林 みどり*（静岡県立大・経営情報）・宮内 美樹（NTT）・
中村 義作（東海大・教育開発研究所）
アダマール行列の一般化

11：40 ～ 13：40　＜Lunch＞

13：40 ～ 14：10　篠原 聡*（明星大・情報）・宮本 暢子（東京理科大・理工）
直線と Conic の交点と Balanced Array

14：10 ～ 14：40　城本 啓介（愛知県立大・情報科学）
デザイン構造をもつマトロイド

14：40 ～ 14：50　＜Break＞

14：50 ～ 15：40　Walter D. Wallis（Dept. of Math., Southern Illinois Univ., USA）
Single-Change Designs

15：40 ～ 15：50　＜Break＞

15：50 ～ 16：40　Chin-Mei Fu（Dept. of Math., Tamkang Univ., Taiwan）
Decomposing Complete Graphs into Sun Graphs of *n*-Cycle

9 月 18 日 （木）

9：30 ～ 10：00　潮 和彦（近畿大・理工）
Hamilton C_k-Trefoil Designs

10：00 ～ 10：30　吉川 智史*（名古屋大院・情報科学）・神保 雅一（名古屋大院・情報科学）
A Construction of a Cyclic SQS(2p) for Prime p

10：30 ～ 10：40　＜Break＞

10：40 ～ 11：10　藤原 祐一郎（筑波大院・システム情報工）
Translation-Free Steiner Systems and Their Application

11：10 ～ 11：40　藤原 良*（筑波大院・システム情報工）・
藤原 祐一郎（筑波大院・システム情報工）・
Ying Miao（筑波大院・システム情報工）
Perfect Hash Families

＜Close＞

Monotonic Directed Designs

Gennian Ge and Dawei Huang, Zhejiang University, China
Ying Miao, University of Tsukuba, Japan

Let $X = \{x_0, x_1, \ldots, x_{v-1}\}$ be a v-set of points. A transitively ordered k-subset (called directed block) $B = (x_{i_0}, x_{i_1}, \ldots, x_{i_{k-1}})$ of X consists of $\frac{k(k-1)}{2}$ ordered pairs of form (x_{i_s}, x_{i_t}) with $0 \le s < t \le k-1$. Let $\mathcal{B}$ be a collection of transitively ordered k-subset of X. A pair $(X, \mathcal{B})$ is a directed (v, k, λ)-design if any ordered pair of distinct points from X is contained in exactly λ directed blocks.

Let the points of X be linearly ordered by $x_0 \prec x_1 \prec \cdots \prec x_{v-1}$, and $B = (x_{i_0}, x_{i_1}, \ldots, x_{i_{k-1}}) \in \mathcal{B}$ be a directed block of X. Let $pos(x_{i_j})$ denote the position of x_{i_j} in the ordered v-set $(x_{i_0}, x_{i_0+1}, \ldots, x_{v-1}, x_0, x_1, \ldots, x_{i_0-1})$. Then B is a monotonic directed block if $pos(x_{i_0}) < pos(x_{i_1}) < \cdots < pos(x_{i_{k-1}})$.

A monotonic directed (v, k, λ)-design (v, k, λ)-MDD is a pair $(X, \mathcal{B})$, where the points of X are linearly ordered, satisfying the following two conditions:

1. $(X, \mathcal{B})$ is a directed (v, k, λ)-design.

2. Each directed block of $\mathcal{B}$ is monotonic.

The notion of a monotonic directed design was introduced in [1] for the construction of difference triangle sets. An (n, k)-difference triangle set, (n, k)-DΔS, is a set $\Delta = \{\Delta_1, \ldots, \Delta_n\}$, where $\Delta_i = \{a_{i0}, a_{i1}, \ldots, a_{ik}\}$, $1 \le i \le n$, is a set of integers such that $0 = a_{i0} < a_{i1} < \cdots < a_{ik}$, and the differences $a_{il} - a_{ij}$, $1 \le i \le n$, $0 \le j < l \le k$, are all distinct. Let $m(\Delta) = \max\{a_{ik} \mid 1 \le i \le n\}$ be the scope of Δ. An (n, k)-DΔS is regular if $m(\Delta) = \frac{nk(k+1)}{2}$. Let $M(n, k) = \min\{m(\Delta) \mid \Delta \text{ is an } (n, k)\text{-D}\Delta\text{S}\}$. If $m(\Delta) = M(n, k)$, then Δ is said to be optimal. Clearly, any regular DΔS is optimal. Difference triangle sets have applications in various areas (see [2] and references therein). In these applications, in general, better results are obtained from difference triangle sets having small scope. Hence the fundamental problem in the research of difference triangle sets is to construct optimal (n, k)-DΔSs for given pair (n, k).

Let $\mathcal{F} = \{B_1, \ldots, B_t\}$ be a family of k-subsets (called base blocks) of $\mathbf{Z}_v$. $\mathcal{F}$ is a cyclic difference family $(v, k, 1)$-CDF if any element of $\mathbf{Z}_v \setminus \{0\}$ can

be represented in a unique way as a difference of two elements lying in some member of $\mathcal{F}$.

Theorem 1. ([1]) If there exist a $(v, k, 1)$-CDF and a $(k, h, 1)$-MDD, then there exists a regular $(\frac{2(v-1)}{h(h-1)}, h-1)$-D$\Delta$S, Δ, with $m(\Delta) = v - 1$.

Theorem 2. ([1]) If there exists a regular (n, k)-DΔS, then there exists an $(\frac{nk(k+1)}{2} + 1, k + 1, 1)$-MDD.

Theorem 1 shows that the existence of MDDs is crucial for the construction of regular DΔSs. Clearly, if there is a $(v, k, 1)$-MDD, then we have $v \geq k$, $2(v-1) \equiv 0 \pmod{k-1}$, and $2v(v-1) \equiv 0 \pmod{k(k-1)}$. One known non-existence result ([1]) is that there is no $(v, k, 1)$-MDD for $k \geq 6$. However, research on the existence of MDDs is almost non-existent, except for the examples coming from regular DΔSs by Theorem 2. As indicated in [1], an example of $(v, k, 1)$-MDD with $k \geq 4$, not constructed from a regular DΔS, would be of great interest.

In this paper, we investigate monotonic directed designs. We introduce several new concepts related to monotonic directed designs, and describe various constructions for monotonic directed designs and their related designs. The following is the main result of this paper.

Theorem 3. The necessary conditions for the existence of a $(v, 3, 1)$-MDD, namely, $v \geq 3$ and $v \equiv 0, 1, 4, 9 \pmod{12}$, are also sufficient, and the necessary conditions for the existence of a $(v, 4, 1)$-MDD, namely, $v \geq 4$ and $v \equiv 1 \pmod{3}$, are also sufficient with two definite exceptions $v = 4, 10$ and six possible exceptions $v \in \{13, 19, 82, 94, 214, 292\}$.

References

[1] W. Chu, C. J. Colbourn and S. W. Golomb, *A recursive construction for regular difference triangle sets*, SIAM J. Discrete Math., vol. 18, pp. 741-748, 2005.

[2] J. B. Shearer, *Difference triangle sets*, in *Handbook of Combinatorial Designs, Second Edition*, C. J. Colbourn and J. H. Dinitz, Eds., Boca Raton, FL: Chapman & Hall / CRC, pp. 436–440, 2007.

Difference families of block size 4, 5 related to OOCs and CACs

Koji Momihara (E-mail: momihara@math.cm.is.nagoya-u.ac.jp)
Graduate School of Information Science, Nagoya University
Keywords: cyclic δ-support $(n,k)_\mu$ difference family, optical orthogonal code; conflict-avoiding code

1 Introduction. Let $\binom{\mathbb{Z}_n}{k}$ be the set of all k-subsets of $\mathbb{Z}_n$, the residue ring of integers modulo n. An $(n,k,\lambda_a,\lambda_c)$ optical orthogonal code (OOC) is a family $\mathcal{F} \subseteq \binom{\mathbb{Z}_n}{k}$ satisfying:

(i) (*The autocorrelation property*) $|X \cap (X+s)| \le \lambda_a$ for any $X \in \mathcal{F}$ and every $s \in \mathbb{Z}_n \setminus \{0\}$;

(ii) (*The cross-correlation property*) $|X \cap (Y+s)| \le \lambda_c$ for any $X, Y \in \mathcal{F}$ with $X \neq Y$ and every $s \in \mathbb{Z}_n$.

An $(n,k,\lambda_a,\lambda_c)$-OOC without the property (i) is called an (n,k,λ_c) conflict-avoiding code (CAC). An $(n,k,\lambda_a,\lambda_c)$-OOC (or an (n,k,λ_c)-CAC) is called *optimal* if the number of codewords is maximum for given n, k, λ_a and λ_c.

In this paper, we treat only the case when $k=4$. (Some of the results in this paper are generalized to the case when $k=5$. See [1, 2, 3].)

2 Upper bounds on code size. Given a k-subset $X \in \binom{\mathbb{Z}_n}{k}$, we define the list of differences of X by

$$\Delta X = \{a-b \,|\, a,b \in X, a \neq b\}$$

as a multiset, and define the *support* of ΔX, denoted by $\mathrm{supp}(\Delta X)$, as the set of underlying elements in ΔX. Note that $k-1 \le |\mathrm{supp}(\Delta X)| \le k(k-1)$ for any $X \in \binom{\mathbb{Z}_n}{k}$. We define

$$\mu(X) = \max\{m_i(\Delta X) \,|\, i \in \Delta X\},$$

where $m_i(\Delta X)$ denote the multiplicity of i in ΔX. Then we have

$$\mu(X) = \max\{|X \cap (X+s)| : s \in \mathbb{Z}_n \setminus \{0\}\}.$$

From this correspondence, it is easy to see the following:

Lemma 2.1. *Every $(n,k,\lambda_a,1)$-OOC is a family $\mathcal{F} \subseteq \binom{\mathbb{Z}_n}{k}$ satisfying the following conditions:*

(i) $\lambda_a = \max\{\mu(X) \,|\, X \in \mathcal{F}\}$;

(ii) $\Delta X \cap \Delta Y = \emptyset$ *for any distinct* $X, Y \in \mathcal{F}$.

The above conditions (i) and (ii) are corresponding to the auto- and cross-correlation properties, respectively. In order to get tight upper bounds on code size of $(n,4,\lambda_a,1)$-OOCs, we need the following correspondences.

Lemma 2.2. *For $X \in \binom{\mathbb{Z}_n}{4}$, it holds that*

$$|\mathrm{supp}(\Delta X)| = \begin{cases} 3 & \text{iff } X = (\frac{n}{4})\mathbb{Z}_n; \\ 4 & \text{iff } X \subset (\frac{n}{5})\mathbb{Z}_n; \\ 5 & \text{iff } X = \{0, a, n/2, n/2+a\} \text{ or} \\ & \quad X \subset (\frac{n}{6})\mathbb{Z}_n \text{ except for } |\mathrm{supp}(\Delta X)| = 3; \\ 6 & \text{iff } X = \{0, a, 2a, 3a\} \text{ or } X \subset (\frac{n}{7})\mathbb{Z}_n \\ & \quad \text{except for } |\mathrm{supp}(\Delta X)| = 3, 4 \text{ and } 5; \\ 7 & \text{iff } X = \{0, a, n/2, n-a\}, \\ & \quad X = \{0, a, n/2-a, n/2\}, \text{ or } X \subset (\frac{n}{8})\mathbb{Z}_n \\ & \quad \text{except for } |\mathrm{supp}(\Delta X)| = 3, 5 \text{ and } 6; \\ 8 & \text{iff } X = \{0, a, a+b, 2a+b\}, \\ & \quad X = \{0, a, n/3, 2n/3\}, \text{ or } X = \{0, a, 2a, 4a\} \\ & \quad \text{except for } |\mathrm{supp}(\Delta X)| = 3, 4, 5, 6 \text{ and } 7; \\ 9 & \text{iff } X = \{0, a, 2a, n/2\} \\ & \quad \text{or } X = \{0, a, n/2, 3n/4\} \\ & \quad \text{except for } |\mathrm{supp}(\Delta X)| = 3, 5 \text{ and } 7; \\ 10 & \text{iff } X = \{0, a, 2a, 2a+b\} \text{ except for} \\ & \quad |\mathrm{supp}(\Delta X)| = 3, 4, 5, 6, 7, 8 \text{ and } 9; \\ 11 & \text{iff } X = \{0, a, b, n/2\} \text{ except for} \\ & \quad |\mathrm{supp}(\Delta X)| = 3, 5, 7 \text{ and } 9. \end{cases}$$

Lemma 2.3. *For $X \in \binom{\mathbb{Z}_n}{4}$, it holds that*

$$\mu(X) = \begin{cases} 4 & \text{iff } |\mathrm{supp}(\Delta X)| = 3 \text{ or} \\ & \quad 5 \ (X = \{0, a, n/2, n/2+a\}); \\ 3 & \text{iff } |\mathrm{supp}(\Delta X)| = 4, \\ & \quad 5 \ (X = \{0, n/6, n/3, n/2\}, \\ & \quad X = \{0, n/6, n/3, 2n/3\}), \\ & \quad 6 \ (X = \{0, a, 2a, 3a\}) \text{ or} \\ & \quad 8 \ (X = \{\{0, a, n/3, 2n/3\}); \\ 2 & \text{iff } |\mathrm{supp}(\Delta X)| = 6, 7, 8, 9, 10 \text{ or } 11 \\ & \quad \text{except for the case } \mu(X) = 3; \\ 1 & \text{iff } |\mathrm{supp}(\Delta X)| = 12. \end{cases}$$

By the above lemmas, we have the following upper bounds on code size of $(n,4,\lambda_a,1)$-OOCs.

Lemma 2.4. *(The Johnson bound) It holds that*

$$M(n,4,1,1) \le \lfloor (n-1)/12 \rfloor,$$

where $M(n,k,\lambda_a,\lambda_c)$ means the maximum number of codewords of $(n,k,\lambda_a,\lambda_c)$-OOC.

Lemma 2.5. *Let $n = 2^r 7^s m$, where m is not divisible by 2 and 7. Then it holds that*

$$M(n,4,2,1) \le \begin{cases} \lfloor n/8 \rfloor & \text{if } r \ge 1,\ s = 0; \\ \lfloor (n+1)/8 \rfloor & \text{if } r = 0,\ s \ge 1; \\ \lfloor (n+2)/8 \rfloor & \text{if } r \ge 1,\ s \ge 1; \\ \lfloor (n-1)/8 \rfloor & \text{if } r = s = 0. \end{cases}$$

Lemma 2.6. *Let $n = 5^r 6^s m$, where m is not divisible by 5 and 6. Then it holds that*

$$M(n,4,3,1) \le \begin{cases} \lfloor (n+1)/6 \rfloor & \text{if } r \ge 1,\ s = 0; \\ n/6 & \text{if } r = 0,\ s \ge 1; \\ \lfloor (n+2)/6 \rfloor & \text{if } r \ge 1,\ s \ge 1; \\ \lfloor (n-1)/6 \rfloor & \text{if } r = s = 0. \end{cases}$$

Note that the bound of Lemma 2.6 is also tight when $\gcd(n,30) = 1$ for $(n,4,1)$-CACs.

3 Cyclic difference families. For positive integers δ and μ with $k-1 \le \delta \le k(k-1)$ and $1 \le \mu \le k$, let $\mathcal{F}$ be a family of k-subsets of $\mathbb{Z}_n$ such that $|\mathrm{supp}(\Delta B)| = \delta$ and $\mu(B) \le \mu$ for every $B \in \mathcal{F}$. We say that $\mathcal{F}$ is a cyclic δ-support $(n,k)_\mu$ difference family (briefly δ-supp $(n,k)_\mu$-CDF) if the following are satisfied:

(i) $\Delta B \cap \Delta B' = \emptyset$ for any $B, B' \in \mathcal{F}$ with $B \ne B'$; and

(ii) $\bigcup_{B\in\mathcal{F}} \mathrm{supp}(\Delta B) = \mathbb{Z}_n \setminus \{0\}$.

The members of a δ-supp $(n,k)_\mu$-CDF are called *blocks*. We clearly have $n \equiv 1 \pmod{\delta}$. For any k-subset X of $\mathbb{Z}_n$ with $|supp(\Delta X)| \equiv 1 \pmod 2$, X must contain the element $n/2$ and then n must be divisible by 2. Therefore, any δ-supp $(n,k)_\mu$-CDF with $\delta \equiv 1 \pmod 2$ consists of exactly one block and $n = \delta + 1$ holds. A δ-supp $(n,k)_\mu$-CDF with $\delta = k(k-1)$ is also called a *cyclic $(n,k,1)$ simple difference family* which generates a Steiner 2-design with an automorphism consisting a single cycle of length n.

By the lemmas given in Section 2, we get:

Lemma 3.1. *Any 12-supp $(n,4)_1$-CDF gives an optimal $(n,4,1,1)$-OOC.*

Lemma 3.2. *Any 8-supp $(n,4)_2$-CDF gives an optimal $(n,4,2,1)$-OOC.*

Lemma 3.3. *Any 6-supp $(n,4)_3$-CDF gives an optimal $(n,4,3,1)$-OOC. When $n \not\equiv 25 \pmod{30}$, so is an optimal $(n,4,1)$-CAC.*

The following are new constructions and existence theorems for δ-supp $(n,4)_\mu$-CDFs. Further results are referred to [1, 2, 3].

Theorem 3.4. *For any prime $p \equiv 1 \pmod 8$, there exists an element $c \in \mathbb{Z}_p$ s.t. $\{0,1,c,c+1\} \cdot S$ is an 8-supp $(p,4)_2$-CDF, where S is a complete system of representatives for the cosets of $\{-1,1\}$ in the set of quartic elements of $\mathbb{Z}_p$.*

Theorem 3.5. *Let $\mathcal{F}$ be an 8-supp $(n_1,4)_2$-CDF with $\gcd(n_1,6) = 1$ and let*

$$\mathcal{F}' = \{\{0, a_i, a_i+b_i, 2a_i+b_i\} \mid 1 \le i \le \frac{n_2-1}{8}\}$$

be an 8-supp $(n_2,4)_2$-CDF. Define

$$B_{i,j} = \{0, a_i + jn_2, a_i + b_i + 3jn_2, 2a_i + b_i + 4jn_2\}$$

on $\mathbb{Z}_{n_1 n_2}$. Then,

$$\{B_{i,j} \mid 1 \le i \le \frac{n_2-1}{8}, 0 \le j \le n_1 - 1\} \cup n_2\mathcal{F}$$

over $\mathbb{Z}_{n_1 n_2}$ is an 8-supp $(n_1 n_2, 4)_2$-CDF.

Theorem 3.6. *Let p be a prime $\equiv 1 \pmod{3^{r'}}$. There exists a set S of $\mathbb{Z}_p$ such that $\{0,1,2,3\} \cdot S$ is a 6-supp $(p,4)_3$-CDF iff there exists an integer $r \le r'$ s.t. 2 is 3^{r-1}th power but not 3^rth power in $\mathbb{Z}_p$ and 6 is 3^rth power in $\mathbb{Z}_p$.*

Theorem 3.7. *Let $\mathcal{F}$ be a 6-supp $(n_1,4)_3$-CDF with $\gcd(n_1,6) = 1$ and let*

$$\mathcal{F}' = \{\{0, a_i, 2a_i, 3a_i\} \mid 1 \le i \le \frac{n_2-1}{6}\}$$

be a 6-supp $(n_2,4)_3$-CDF. Define

$$B_{i,j} = \{0, a_i + jn_2, 2(a_i + jn_2), 3(a_i + jn_2)\}.$$

on $\mathbb{Z}_{n_1 n_2}$. Then,

$$\{B_{i,j} \mid 1 \le i \le \frac{n_2-1}{6}, 0 \le j \le n_1 - 1\} \cup n_2\mathcal{F}$$

over $\mathbb{Z}_{n_1 n_2}$ is a 6-supp $(n_1 n_2, 4)_3$-CDF.

References

[1] Momihara, K., Buratti, M., Bounds and constructions of optimal $(n,4,2,1)$ optical orthogonal codes, submitted to *IEEE. Trans. Inform. Theory.*

[2] Momihara, K., Cyclotomic condition and density of cyclic δ-support $(n,k)_\mu$ difference families with $\delta = 2(k-1)$, $\mu = k-1$, and $k = 4, 5$, submitted to *Finite Fields Appl.*

[3] Momihara, K., Strong difference families, difference covers, and their applications for relative difference families, submitted to *Des. Codes Criptogr.*

BINARY SEQUENCES WITH OPTIMAL AUTOCORRELATION AND PERIOD $N \equiv 1 \pmod 4$ AND $N \equiv 2 \pmod 4$

CUNSHENG DING

ABSTRACT

The autocorrelation of a binary sequence $(s(t))$ of period N at shift w is

$$\mathbf{AC}_s(w) = \sum_{t=0}^{N-1} (-1)^{s(t+w)-s(t)}, \tag{1}$$

where each $s(t) \in \{0,1\}$. These $\mathbf{AC}_s(w)$, $w \in \{1,2,\cdots,N-1\}$, are called the out-of-phase autocorrelation values. For various applications, we wish to have binary sequences with minimal value $\max_{1\le w\le N-1} |\mathbf{AC}_s(w)|$.

Throughout this lecture, let $(s(t))$ be a binary sequence of period N. The set

$$C_s = \{0 \le i \le N-1 : s(i) = 1\} \tag{2}$$

is called the *support* of $(s(t))$; and $(s(t))$ is referred to as the *characteristic sequence* of $C_s \subseteq \mathbf{Z}_N$.

The mapping $s \mapsto C_s$ is a one-to-one correspondence from the set of all binary sequences of period N to the set of all subsets of $\mathbf{Z}_N$. Hence, studying binary sequences of period N is equivalent to that of subsets of $\mathbf{Z}_N$.

For any subset C of $\mathbf{Z}_N$, the *difference function* of C is defined as

$$d_C(w) = |(w+C) \cap C|, \ w \in \mathbf{Z}_N. \tag{3}$$

Let $(s(t))$ be the characteristic sequence of C. It is easy to show that

$$\mathbf{AC}_s(w) = N - 4(k - d_C(w)), \tag{4}$$

where $k := |C|$. Thus the study of the autocorrelation property of the sequence $(s(t))$ becomes that of the difference function d_C of the support C of the sequence $(s(t))$.

It follows from (4) that $\mathbf{AC}_s(w) \bmod 4 = N \bmod 4$. Hence we have the following four cases.

Let $N \equiv 3 \pmod 4$. Then $\max_{1\le w\le N-1} |\mathbf{AC}_s(w)| \ge 1$. On the other hand, $\max_{1\le w\le N-1} |\mathbf{AC}_s(w)| = 1$ iff $\mathbf{AC}_s(w) = -1$ for all $w \not\equiv 0 \pmod N$. In this case, the sequence $\{s(t)\}$ is said to have *ideal autocorrelation* and *optimal autocorrelation*.

Let $N \equiv 1 \pmod 4$. There is some evidence that there is no binary sequence of period $N > 13$ with $\max_{1 \le w \le N-1} |\mathbf{AC}_s(w)| = 1$. It is then natural to consider the case $\max_{1 \le w \le N-1} |\mathbf{AC}_s(w)| = 3$. In this case $\mathbf{AC}_s(w) \in \{1, -3\}$ for all $w \not\equiv 0 \pmod N$.

Let $N \equiv 2 \pmod 4$. Then $\max_{1 \le w \le N-1} |\mathbf{AC}_s(w)| \ge 2$. On the other hand, $\max_{1 \le w \le N-1} |\mathbf{AC}_s(w)| = 2$ iff $\mathbf{AC}_s(w) \in \{2, -2\}$ for all $w \not\equiv 0 \pmod N$. In this case, the sequence $\{s(t)\}$ is said to have *optimal autocorrelation*.

Let $N \equiv 0 \pmod 4$. We have clearly that $\max_{1 \le w \le N-1} |\mathbf{AC}_s(w)| \ge 0$. If $\max_{1 \le w \le N-1} |\mathbf{AC}_s(w)| = 0$, the sequence $(s(t))$ is called *perfect*. The only known perfect binary sequence up to equivalence is the $(0, 0, 0, 1)$. It is conjectured that there is no perfect binary sequence of period $N \equiv 0 \pmod 4$ greater than 4. This conjecture is true for all $N < 108900$. Hence, it is natural to construct binary sequences of period $N \equiv 0 \pmod 4$ with $\max_{1 \le w \le N-1} |\mathbf{AC}_s(w)| = 4$.

There are a small number of constructions of binary sequences with optimal autocorrelation and period N for the two cases $N \equiv 0 \pmod 4$ and $N \equiv 3 \pmod 4$. However, for the two cases $N \equiv 1 \pmod 4$ and $N \equiv 2 \pmod 4$, there are only three and two constructions of such sequences respectively. This lecture is focused on the latter two cases.

In this lecture, we shall first introduce cyclotomy and two combinatorial designs: difference sets and almost difference sets. We then describe a bridge between binary sequences with optimal autocorrelation and the two combinatorial designs. Finally, we talk about the known constructions of binary sequences with optimal autocorrelation and period N for the two cases $N \equiv 1 \pmod 4$ and $N \equiv 2 \pmod 4$. We will also introduce five open problems on this topic, and applications of such sequences in statistics, experimental designs, ranging systems, spread spectrum communication systems, coding theory, multi-terminal system identification, code division multiple access communications systems, global positioning systems, software testing, circuit testing, computer simulation, stream ciphers, and physics.

ACKNOWLEDGMENTS

This lecture is supported by JSPS Scientific Research (A)19204009 and (B)18340024.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY, CLEAR WATER BAY, KOWLOON, HONG KONG. EMAIL: CDING@CSE.UST.HK

Title: Grid-Block Designs and Packings

Speaker: Hung-Lin Fu
Department of Applied Mathematics
National Chiao Tung University
Hsin Chu, Taiwan 30050

Abstract (Extended)

For a v-set V, let A be a collection of $r \times c$ arrays with distinct elements in V. A pair (V, A) is called a $r \times c$ grid-block design (packing) if every two distinct elements in V occur exactly (at most) once in the same row or in the same column of an array in A.

From the point of view of Graph Decomposition, the existence of a $r \times c$ grid-block design (packing) of order v is equivalent to a decomposition (packing) of the complete graph of order v into the Cartesian product of $K_r \times K_c$. Therefore, the study of this topic can be approached from Graph Theory and of course from Combinatorial Design.

By direct counting, it is not difficult to see that a $r \times c$ grid-block design of order v exists only if *(a)* $v \geq r \cdot c$, *(b)* $v - 1 \equiv 0 \pmod{r + c - 2}$ *and (c)* $v(v - 1) \equiv 0 \pmod{r \cdot c\,(r + c - 2)}$. It has been shown respectively by Mutoh et al. that this necessary condition is also sufficient for the cases when (r, c) = (2, 3), (3, 3), (2, 4) and (2, 5) in past years. In this talk, I'll report the progress of the research of this topic by noticing the following results:

1. A 4×4 grid-block design of order v exists if and only if $v \equiv 1 \pmod{96}$; and
2. A 3×4 grid-block design of order v exists if and only if $v \equiv 1, 16, 21, 36 \pmod{60}$ except $v = 16$ (does not exist) and possibly $v \in \{60n + 36 : n = 1,2,4,5,10,20,22,26\} \cup \{60n + 16 : n = 2,3,4,7,10,18,23\}$.

The basic tools of obtaining the above results are direct constructions. From previous works we have u to k·u construction and u + 1 to k·u + 1 construction respectively by applying suitable group divisible designs (GDD). So, it is left to construct a few small designs. Mainly, difference method will be the key tool to get the job done. In that case, we utilize group action and a well known theorem by Wilson.

As to the applications of the grid-block designs or resolvable packings, we mainly introduce the use of DNA library screening. The idea is as follows. We place different clones in each spot of a microtiter plate which is an array with size 8×12 (or suitable size) and then every row and every column in the plate is tested in the first stage. Note here that each row or each column forms a pool in group testing. After we have the outcomes by testing each pool, we test each possible positive clone (determined by the response of pools) individually in the second stage. This method is known as the basic matrix method (BMM) which is a very efficient 2-stage group testing.

Characterization and construction of affine α-resolvable block designs

Yoshiga High School Satoru Kadowaki
Hiroshima Institute of Technology Sanpei Kageyama

One of the earliest examples of a resolvable balanced incomplete block (BIB) design is the Kirkman (1850a) school girl problem formulated in 1850 and pursued further in another paper (Kirkman, 1850b). This can be seen as equivalent to finding a resolvable solution of a BIB design with parameters $v = 6t + 3, b = (2t + 1)(3t + 1), r = 3t + 1, k = 3, \lambda = 1$. Kirkman himself gave some solutions and many mathematicians worked on this problem in the late 19th and early 20th century. However, no complete solution was known until Ray-Chaudhuri and Wilson (1971) completely solved the problem. This was a celebrated open problem throughout the period 1850-1970.

Though Yates (1939, 1940) has pointed out some statistical advantages of resolvable designs, the interest in resolvable BIB designs was greatly enhanced by a combinatorial paper by Bose (1942).

A block design BD(v, b, r, k) is said to be α-resolvable if the b blocks of size k each can be grouped into t sets (called α-resolution sets) of β blocks each ($b = \beta t$) such that in each α-resolution set every treatmenat (or point) is replicated α times ($r = \alpha t$). An α-resolvable BD is said to be affine α-resolvable if every two distinct blocks from the same α-resolution set intersect in the same number, say, q_1, of treatments, whereas every two blocks belonging to different α-resolution sets intersect in the same number, say, q_2, of treatments.

In this talk, some characterization of affine α-resolvable block designs are dealt with from a combinatorial point of view. Their topics are concerned with bounds on parameters in designs, the characterization of parameters in a closed form and existence problems. The block designs discuused here are BIB designs and PBIB designs. The basic procedure is based on the number-theoretic and combinatorial approach. Comprehensive and useful results on combinatorics are obtained. Several methods of construction are also newly presented with practical affine resolvable block designs.

Key results

Lemma 1. In an affine α-resolvable BD$(v, b = \beta t, r = \alpha t, k)$ with the incidence matrix N, the matrix $N'N$ has eigenvalues $rk, k\{1 - (\alpha - 1)/(\beta - 1)\}$ and 0, with multiplicities 1, $b - t$ and $t - 1$, respectively.

Lemma 2. In a 2-associate PBIB design, having the incidence matrix N, with parameters v, b, r, k, λ_i, θ_i, ρ_i, $i = 0, 1, 2$, where $\lambda_0 = r, \theta_0 = rk$, $\rho_0 = 1$, θ_1 and θ_2 are the nonnegative eigenvalues (other than rk) of NN' with respective multiplicities ρ_1 and ρ_2, when $\theta_1 > 0$ and $\theta_2 > 0$, the design does not possess a property of affine α-resolvability.

Theorem 1. Let N be the $v \times b$ incidence matrix of an affine α-resolvable 2-associate PBIB design with parameters $v, b = \beta t, r = \alpha t, k, \lambda_1, \lambda_2, q_1 = k(\alpha - 1)/(\beta - 1)$ and $q_2 = k^2/v$, and further let θ_i be eigenvalues of NN' with multiplicities ρ_i, $i = 0, 1, 2$, where $\theta_0 = rk$ and $\rho_0 = 1$. Then

(i) when $\theta_1 > 0$ and $\theta_2 = 0$, $q_1 = k - \theta_1$ and $b = t + \rho_1$ hold;

(ii) when $\theta_1 = 0$ and $\theta_2 > 0$, $q_1 = k - \theta_2$ and $b = t + \rho_2$ hold.

Affine α-resolvable SGD designs

Theorem 2. The existence of an affine α-resolvable SGD($v = nv^*, b = b^* = \beta t, r = r^* = \alpha t, k = nk^*, \lambda_1 = r^*, \lambda_2 = \lambda^*; m = v^*, n = n$) with $q_1 = nk^*(\alpha - 1)/(\beta - 1)$ and $q_2 = n(k^*)^2/v^*$ is equivalent to the existence of an affine α-resolvable BIB($v^*, b^* = \beta t, r^* = \alpha t, k^*, \lambda^*$) with $q_1^* = k(\alpha - 1)/(\beta - 1)$ and $q_2^* = k^2/v$.

Theorem 3. The parameters of an affine α-resolvable SGD design are given by $v = mn, b = \beta(m-1)/(\beta-1), r = \alpha(m-1)/(\beta-1), k = \alpha mn/\beta, \lambda_1 = \alpha(m-1)/(\beta-1), \lambda_2 = \alpha(\alpha m - \beta)/[\beta(\beta-1)]; t = (m-1)/(\beta-1), q_2 = \alpha^2 mn/\beta^2$, where $\alpha m/\beta$ is an integer.

Table 1. Affine resolvable SGD designs

No.	m	n	v	b	r	k	λ_1	λ_2	q_2	Source 1	Source 2	Remark
1	4	2	8	6	3	4	3	1	2	K1+{2}		S6
2	4	3	12	6	3	6	3	1	3	K1+{3}		S27
3	4	4	16	6	3	8	3	1	4	K1+{4}		S61
4	4	5	20	6	3	10	3	1	5	K1+{5}		S106
5	4	6	24	6	3	12	3	1	6	K1+{6}		
6	4	7	28	6	3	14	3	1	7	K1+{7}		
7	4	8	32	6	3	16	3	1	8	K1+{8}		
8	4	9	36	6	3	18	3	1	9	K1+{9}		
9	4	10	40	6	3	20	3	1	10	K1+{10}		
10	6	2	12	10	5	6	5	2	3	Non-E	BIB(6, 3, 2) + {2}	※ 1
11	6	4	24	10	5	12	5	2	6	Non-E	BIB(6, 3, 2) + {4}	※ 1
12	6	6	36	10	5	18	5	2	9	Non-E	BIB(6, 3, 2) + {6}	※ 1
13	8	2	16	14	7	8	7	3	4	K5+{2}		S63
14	8	3	24	14	7	12	7	3	6	K5+{3}		
15	8	4	32	14	7	16	7	3	8	K5+{4}		
16	8	5	40	14	7	20	7	3	10	K5+{5}		
17	9	2	18	12	4	6	4	1	2	K6+{2}		S37
18	9	3	27	12	4	9	4	1	3	K6+{3}		S91
19	9	4	36	12	4	12	4	1	4	K6+{4}		
20	9	5	45	12	4	15	4	1	5	K6+{5}		
21	9	6	54	12	4	18	4	1	6	K6+{6}		
22	10	2	20	18	9	10	9	4	5	Non-E	BIB(10, 5, 4) + {2}	※ 1
23	10	4	40	18	9	20	9	4	10	Non-E	BIB(10, 5, 4) + {4}	※ 1
24	12	2	24	22	11	12	11	5	6	K12+{2}		
25	12	3	36	22	11	18	11	5	9	K12+{3}		
26	14	2	28	26	13	14	13	6	7	Non-E	BIB(14, 7, 6) + {2}	※ 1
27	15	3	45	21	7	15	7	2	5	Non-E	Non-E	※ 2
28	16	2	32	20	5	8	5	1	2	K17+{2}		S74
29	16	2	32	30	15	16	15	7	8	K18+{2}		
30	16	3	48	20	5	12	5	1	3	K17+{3}		
31	16	4	64	20	5	16	5	1	4	K17+{4}		
32	16	5	80	20	5	20	5	1	5	K17+{5}		
33	18	2	36	34	17	18	17	8	9	Non-E	BIB(18, 9, 8) + {2}	※ 1
34	20	2	40	38	19	20	19	9	10	K25+{2}		
35	25	2	50	30	6	10	6	1	2	K28+{2}		S121
36	25	3	75	30	6	15	6	1	3	K28+{3}		
37	25	4	100	30	6	20	6	1	4	K28+{4}		
38	27	2	54	39	13	18	13	4	6	K30+{2}		
39	36	2	72	42	7	12	7	1	2	Non-E	Non-E	※ 3
40	40	2	80	52	13	20	13	3	5	Non-E	BIB(40, 10, 3) ?	※ 4
41	49	2	98	56	8	14	8	1	2	K40+{2}		

One characterization theorem and three construction methods of affine α-resolvable SRGD designs are given with some table. Similar discussions are made for affine α-resolvable L_2 designs with some table.

非小細胞肺ガン患者のデータ解析

大阪府立大学大学院　工学研究科　市村　尚代
大阪府立大学大学院　工学研究科　丸山　芳人
大阪府立大学大学院　工学研究科　田中　秀和
大阪府立大学大学院　工学研究科　栗木　進二

ガン細胞は顕微鏡で見ることによって、腺ガン・扁平上皮ガン・大細胞ガン・小細胞ガンの 4 つの組織型に分類され、その組織型により、性質やできる場所が異なっている。腺ガン・扁平上皮ガン・大細胞ガンを非小細胞ガンと呼び、小細胞ガンと非小細胞ガンとでは、治療法が異なっている。近畿中央胸部疾患センターの川口先生に非小細胞肺ガン患者 25554 人のデータを提供していただき、肺ガン全体の半数以上を占める、腺ガンを中心に解析を行った。今までに読んだ論文の中で、多いものでも 2000 人くらいのデータしかなかったため、今回はかなり標本数が多い状態で解析を行った。データには、患者のいろいろな情報があったが、生存時間に関係しているであろうと思われる、性別・年齢・確診年（ガンと診断された日）・PS（介助を必要とするかや寝たきりかなどの全身状態）・喫煙歴・組織型（ガンの種類）・臨床病気（どこまで転移しているかなどの進行状態）の 7 項目を解析に用いた。

カプラン・マイヤー法
死亡発生時刻を $0 < t_1 < t_2 < \cdots < t_j < \cdots$ とすると、

$$\hat{S(t_{j+1})} = \hat{S(t_j)}(1 - \frac{d_{j+1}}{n_{j+1}})$$

ここで、$d_j : t_j$ での死亡発生数、$n_j : t_j$ での観察対象者数である

Cox 回帰
以下に示す、Cox 比例回帰モデルを用いて解析を行う。

$$h(t) = h_0(t)exp(\beta_1\chi_1 + \cdots + \beta_p\chi_p)$$

ここで、$h(t)$:ハザード関数、$h_0(t)$:基準ハザード関数、χ_i:各項目の値、β_i:各項目の回帰係数である。
ハザードとは、ある時点まで生きた人が、その時点において死亡する危険を表す指数であり、瞬間死亡率と呼ばれているが、実際には確率でないため、1 よりも大きくなり得る。

ハザード関数から生存率を求める公式

$$S(t) = (S_0(t))^{exp[\beta_1\chi_1 + \cdots + \beta_7\chi_7]}$$

ここに、$h(t) = h_0(t)exp(\beta^\top\chi)$ を代入して、

$$S(t) = S_0(t)^{exp(\beta^\top\chi)}$$

よって、基準ハザード関数 $h_0(t)$ に対応する生存率を $S_0(t)$ とすると、生存関数は以下のようになる。

$$S(t) = (S_0(t))^{exp[\beta_1\chi_1+\cdots+\beta_7\chi_7]}$$

ここで各項目を全て 0 とすると $S_0(t)$ となる。

変数（項目）選択
生存率に影響を及ぼす項目を選ぶため、ステップワイズ Cox 回帰法という方法を用いて、項目選択を行った。今回の 7 項目では、7 項目とも全て生存率に影響を及ぼすとして、モデルに含まれた。

Cox 回帰を用いて、1 年生存率と 95 % 信頼区間を求めた。2 年生存率も同じように求めることが出来る。ここで、192 通り全ての 95 % 信頼区間は 5 % くらいに収まっていた。川口先生が仰るには 5 % くらいの違いは誤差の範囲内であるという。これは、標本数が多いため、95 % 信頼区間は狭くなったと考えられる。

ノモグラムの作成
ある関数の計算をグラフィカルに行うために設計された二次元の図表をノモグラムという。まず、回帰係数を用いた点数化を行う。
回帰係数 $\beta_i(i = 0, \cdots, 7)$ の最大値 β_{max} を 100 点とし、各項目について以下のように点数化する。

$$(\frac{\beta_i}{\beta_{max}}) \times 100$$

ここで、β がマイナスになると、ノモグラムが 0 からでなくマイナスの値をとってしまうため、回帰係数が正になるように項目を設定している。
次に、先ほどの回帰係数を点数化したものを用いて、それぞれの型に点数をつける。

$$\text{点数} = \beta_1\hat{\chi}_1 + \cdots + \beta_7\hat{\chi}_7$$

最後に、直線上に各点数を取り、その上に対応する生存関数の値を書き、ノモグラムを描く。今回描いたノモグラムでは、生存率が 3 つのかたまりに分かれた。その原因として、Cox 回帰の結果で、ＰＳと臨床病期のハザード比が他と比べて大きいことにあると考えられる。川口先生が仰るには、ＰＳと臨床病期が生存率に関係しているのではないかと考えていらっしゃったようですが、今回のことで、それを統計的に検証したと考えられる。

モデルの検証
データの 75 % を用いて Cox 回帰し、残りの 25 % を用いてカプラン・マイヤーを行い、検証する。ここで、25554 人のデータを用いても、その 25 その結果､X軸を Cox 回帰の加重平均､Y軸をカプラン・マイヤーとすると、だいたい7割がX=Yの理想線を含んでいた。このことより、生存時間解析に Cox 回帰を適用してもいいのではないかと考えられる。

BALANCED FRACTIONAL 3^m FACTORIAL DESIGNS OF RESOLUTIONS R($\{10,01\} \cup S|\Omega$)

Eiji TANIGUCHI (*International Institute for Natural Sciences*)
Yoshifumi HYODO (*Graduate School of Informatics, Okayama University of Science*)
Masahide KUWADA (*Graduate School of Engineering, Hiroshima University*)

We consider a balanced fractional 3^m factorial (3^m-BFF) design T derived from a simple array SA($m;\{\lambda_{i_0i_1i_2}\}$) with N assemblies (or treatment combinations), where the three-factor and higher-order interactions are assumed to be negligible and $m \geq 4$. Let $\boldsymbol{y}(T)$ be an $N \times 1$ observation vector based on T. Then the ordinary linear model is given by $\boldsymbol{y}(T) = E_T\boldsymbol{\Theta} + \boldsymbol{e}_T$, where E_T is the $N \times \nu(m)$ design matrix, $\boldsymbol{\Theta}$ is the $\nu(m) \times 1$ vector of the non-negligible factorial effects up to the two-factor interaction, and $\boldsymbol{e}_T$ is an $N \times 1$ error vector with mean $\boldsymbol{0}_N$ and variance-covariance matrix $\sigma^2 I_N$. Here $\nu(m) = 1+2m^2$ and $\boldsymbol{\Theta} = (\boldsymbol{\theta}_{00}'; \boldsymbol{\theta}_{10}'; \boldsymbol{\theta}_{01}'; \boldsymbol{\theta}_{20}'; \boldsymbol{\theta}_{02}'; \boldsymbol{\theta}_{11}')'$. The normal equations for estimating $\boldsymbol{\Theta}$ are given by $M_T\hat{\boldsymbol{\Theta}} = E_T'\boldsymbol{y}(T)$, where $M_T (= E_T'E_T)$ is the information matrix of order $\nu(m)$.

Let T be an SA($m;\{\lambda_{i_0i_1i_2}\}$), then M_T associated with T is given by

$$M_T = \sum_{a_1a_2}\sum_{b_1b_2}\sum_{\gamma}\kappa_{\gamma}^{a_1a_2,b_1b_2} D_{\gamma}^{\#(a_1a_2,b_1b_2)} + \sum_{u_1u_2}\sum_{v_1v_2}\sum_{i,j}\kappa_{f_{ij}}^{u_1u_2,v_1v_2} D_{f_{ij}}^{\#(u_1u_2,v_1v_2)},$$

where $\kappa_{\gamma}^{a_1a_2,b_1b_2}$ (γ=0,1,2) and $\kappa_{f_{ij}}^{u_1u_2,v_1v_2}$ are given by some linear combinations of $\lambda_{i_0i_1i_2}$. Thus M_T is isomorphic to the symmetric matrices $\|\kappa_{\gamma}^{a_1a_2,b_1b_2}\| (= K_{\gamma}$, say) for γ=0,1,2 and $\|\kappa_{f_{ij}}^{u_1u_2,v_1v_2}\| (= K_f$, say). The a_1a_2-th row block and the b_1b_2-th column one of $D_{\gamma}^{\#(a_1a_2,b_1b_2)}$ are concerned with $A_{\gamma}^{\#(a_1a_2,a_1a_2)}\boldsymbol{\theta}_{a_1a_2}$ and $A_{\gamma}^{\#(b_1b_2,b_1b_2)}\boldsymbol{\theta}_{b_1b_2}$, respectively, and the u_1u_2-th row block and the v_1v_2-th column one of $D_{f_{ij}}^{\#(u_1u_2,v_1v_2)}$ are also concerned with $A_{f_{ii}}^{\#(u_1u_2,u_1u_2)}\boldsymbol{\theta}_{u_1u_2}$ and $A_{f_{jj}}^{\#(v_1v_2,v_1v_2)}\boldsymbol{\theta}_{v_1v_2}$, respectively.

The resulting array given by interchanging all of the symbols 0 and 2 of an SA($m;\{\lambda_{i_0i_1i_2}\}$) is also the SA($m;\{\lambda^*_{k_0k_1k_2}\}$), where $\lambda^*_{k_0k_1k_2} = \lambda_{k_2k_1k_0}$, and it is briefly denoted by (0,2)-ISA. Let K_{β} and $\tilde{K}_{\beta}$ (β=0,1,2,f) be, respectively, the irreducible representations of M_T and $M_{\tilde{T}}$ associated with T and $\tilde{T}$ with respect to the ideals of the MDR algebra, where T and $\tilde{T}$ are an SA($m;\{\lambda_{i_0i_1i_2}\}$) and its (0,2)-ISA, respectively. Then we have the following:

Lemma 1. *Let T and $\tilde{T}$ be an* SA($m;\{\lambda_{i_0i_1i_2}\}$) *and its* (0,2)-ISA, *respectively. Then the relations between K_{β} and $\tilde{K}_{\beta}$ (β=0,1,2,f) are given by $\tilde{K}_{\beta} = \Delta_{\beta}K_{\beta}\Delta_{\beta}$, where Δ_0=diag[1;–1;1;1;1;–1], Δ_1=diag[1;1;–1], Δ_2=1 and Δ_f=diag[–1;1;1;1;–1;–1].*

A necessary and sufficient condition for a parametric function $C\boldsymbol{\Theta}$ of $\boldsymbol{\Theta}$ to be estimable for some matrix C of order $\nu(m)$ is that there exists a matrix X of order $\nu(m)$ such that $XM_T = C$. If $C\boldsymbol{\Theta}$ is estimable, then its BLUE is given by $C\hat{\boldsymbol{\Theta}}$, where $\hat{\boldsymbol{\Theta}}$ is a solution of the normal equations, and its variance-covariance matrix is given by $\sigma^2 XM_TX'$. We impose some restrictions on C such that it is given by some linear combinations of $D_{\gamma}^{\#(a_1a_2,b_1b_2)}$ and $D_{f_{ij}}^{\#(u_1u_2,v_1v_2)}$, and hence we define C as follows:

$$C = D_0^{\#(10,10)} + D_{f_{11}}^{\#(10,10)} + D_0^{\#(01,01)} + D_{f_{11}}^{\#(01,01)} + \sum^*\sum^*\sum^* g_{\gamma}^{a_1a_2,b_1b_2} D_{\gamma}^{\#(a_1a_2,b_1b_2)} + \sum^*\sum^*\sum^* g_{f_{ij}}^{u_1u_2,v_1v_2} D_{f_{ij}}^{\#(u_1u_2,v_1v_2)},$$

where $g_{\gamma}^{a_1a_2,b_1b_2}$ and $g_{f_{ij}}^{u_1u_2,v_1v_2}$ are some constants. Similarly we define X as follows:

$$X = \sum_{a_1a_2}\sum_{b_1b_2}\sum_{\gamma}\chi_{\gamma}^{a_1a_2,b_1b_2} D_{\gamma}^{\#(a_1a_2,b_1b_2)} + \sum_{u_1u_2}\sum_{v_1v_2}\sum_{i,j}\chi_{f_{ij}}^{u_1u_2,v_1v_2} D_{f_{ij}}^{\#(u_1u_2,v_1v_2)},$$

where $\chi_{\gamma}^{a_1a_2,b_1b_2}$ and $\chi_{f_{ij}}^{u_1u_2,v_1v_2}$ are also some constants. Then C and X are isomorphic to Γ_{β} and χ_{β} (β=0,1,2,f), respectively. Thus $XM_T = C$ is also isomorphic to $\chi_{\beta}K_{\beta} = \Gamma_{\beta}$.

Lemma 2. *If $N < \nu(m)$, then the indices $\lambda_{i_0i_1i_2}$ of an* SA *hold that $\lambda_{i_0i_1i_2} = 0$ for $(i_0i_1i_2) \neq (pm–p0)$ ($1 \leq p \leq m$),($0qm–q$) ($1 \leq q \leq m$), ($m–r0r$) ($1 \leq r \leq m$),($11m–2$),($m–211$), ($1m–21$).*

Theorem. *Let T be an* SA($m;\{\lambda_{i_0i_1i_2}\}$), *then we have*

$$K_\beta=(D_\beta F_\beta \Lambda_\beta)\,(D_\beta F_\beta \Lambda_\beta)' \quad \text{for } \beta=0,1,2,f,$$

where D_β *and* Λ_β *are the diagonal matrices whose diagonal elements are non-zero, and* F_β *are some matrices whose elements corresponding to* $\lambda_{i_0i_1i_2}$ *are given by only its suffices* i_0, i_1 *and* i_2.

Theorem A. *There does not exist a* 3^m-BFF *design of resolution* R($\{10,01,20,02\}|\Omega$) *derived from an* SA($m;\{\lambda_{i_0i_1i_2}\geq 0$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(pm\text{–}p0)$ $(1\leq p\leq m)$,$(0qm\text{–}q)$ $(1\leq q\leq m)$,$(m\text{–}r0r)$ $(1\leq r\leq m)$,$(11m\text{–}2)$,$(m\text{–}211)$,$(1m\text{–}21)\}$) *with* $N<\nu(m)$.

Theorem B. *Let T be an* SA($m;\{\lambda_{i_0i_1i_2}\geq 0$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(pm\text{–}p0)$ $(1\leq p\leq m)$, $(0qm\text{–}q)$ $(1\leq q\leq m)$,$(m\text{–}r0r)$ $(1\leq r\leq m)$,$(11m\text{–}2)$,$(m\text{–}211)$,$(1m\text{–}21)\}$) *with* $N<\nu(m)$. *Then there exists only the* 3^4-BFF *design of resolution* R($\{10,01,20,11\}|\Omega$) *derived from the* SA($m=4;\{\lambda_{310}=\lambda_{013}=\lambda_{220}=\lambda_{022}=\lambda_{112}+\lambda_{211}+\lambda_{121}=1$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(310),(013),(220),(022),(112),(211),(121)\}$).

Theorem C. *There does not exist a* 3^m-BFF *design of resolution* R($\{10,01,02,11\}|\Omega$) *derived from an* SA($m;\{\lambda_{i_0i_1i_2}\geq 0$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(pm\text{–}p0)$ $(1\leq p\leq m)$,$(0qm\text{–}q)$ $(1\leq q\leq m)$,$(m\text{–}r0r)$ $(1\leq r\leq m)$,$(11m\text{–}2)$,$(m\text{–}211)$,$(1m\text{–}21)\}$) *with* $N<\nu(m)$.

Theorem D. *There does not exist a* 3^m-BFF *design of resolution* R($\{10,01,20\}|\Omega$) *derived from an* SA($m;\{\lambda_{i_0i_1i_2}\geq 0$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(pm\text{–}p0)$ $(1\leq p\leq m)$,$(0qm\text{–}q)$ $(1\leq q\leq m)$,$(m\text{–}r0r)$ $(1\leq r\leq m)$,$(11m\text{–}2)$,$(m\text{–}211)$,$(1m\text{–}21)\}$) *with* $N<\nu(m)$.

Theorem E. *There does not exist a* 3^m-BFF *design of resolution* R($\{10,01,02\}|\Omega$) *derived from an* SA($m;\{\lambda_{i_0i_1i_2}\geq 0$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(pm\text{–}p0)$ $(1\leq p\leq m)$,$(0qm\text{–}q)$ $(1\leq q\leq m)$,$(m\text{–}r0r)$ $(1\leq r\leq m)$,$(11m\text{–}2)$,$(m\text{–}211)$,$(1m\text{–}21)\}$) *with* $N<\nu(m)$.

Theorem F. *There does not exist a* 3^m-BFF *design of resolution* R($\{10,01,11\}|\Omega$) *derived from an* SA($m;\{\lambda_{i_0i_1i_2}\geq 0$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(pm\text{–}p0)$ $(1\leq p\leq m)$,$(0qm\text{–}q)$ $(1\leq q\leq m)$,$(m\text{–}r0r)$ $(1\leq r\leq m)$,$(11m\text{–}2)$,$(m\text{–}211)$,$(1m\text{–}21)\}$) *with* $N<\nu(m)$.

Theorem G. *Let T be an* SA($m;\{\lambda_{i_0i_1i_2}\geq 0$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(pm\text{–}p0)$ $(1\leq p\leq m)$, $(0qm\text{–}q)$ $(1\leq q\leq m)$,$(m\text{–}r0r)$ $(1\leq r\leq m)$,$(11m\text{–}2)$,$(m\text{–}211)$,$(1m\text{–}21)\}$) *with* $N<\nu(m)$. *Then a necessary and sufficient condition for T to be a* 3^m-BFF *design of resolution* R($\{10,01\}|\Omega$) *is that one of the following holds*:

(I) *When* $m=4$, (i) $\lambda_{112}=1$, *and furthermore*

(1) $\lambda_{031}=\lambda_{301}=\lambda_{211}+\lambda_{121}=1$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(031),(301),(112),(211),(121)$, *or its* (0,2)-ISA, *or*

(2) $\lambda_{013}=\lambda_{310}=\lambda_{121}=1$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(013),(310),(112),(121)$, *or its* (0,2)-ISA,

(ii) $1\leq\lambda_{130},\lambda_{031},\lambda_{103},\lambda_{301}\leq 2$, *and furthermore*

(1) $\lambda_{112}+\lambda_{121}=1$, $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(130),(031),(103),(301),(112),(121)$ *and* $\lambda_{130}+\lambda_{031}+\lambda_{103}+\lambda_{301}\leq 5$, *or its* (0,2)-ISA, *or*

(2) $\lambda_{220}=\lambda_{022}=1$, $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(130),(031),(103),(301),(220),(022)$ *and* $\lambda_{130}+\lambda_{031}+\lambda_{103}+\lambda_{301}\leq 5$,

(iii) $\lambda_{130}=\lambda_{103}=\lambda_{220}=\lambda_{202}=\lambda_{112}+\lambda_{211}+\lambda_{121}=1$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(130),(103),(220),(202),(112),(211),(121)$, *or its* (0,2)-ISA, *or*

(iv) $1\leq\lambda_{130},\lambda_{013},\lambda_{310},\lambda_{103}\leq 2$ *and* $\lambda_{130}+\lambda_{013}+\lambda_{310}+\lambda_{103}\leq 5$, *and furthermore*

(1) $\lambda_{112}+\lambda_{211}+\lambda_{121}=1$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(130),(013),(310),(103),(112),(211),(121)$, *or its* (0,2)-ISA, *or*

(2) $\lambda_{022}=\lambda_{202}=1$ *and* $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(130),(013),(310),(103),(022),(202)$, *or its* (0,2)-ISA,

(II) *when* $m\geq 4$, $\lambda_{1m-10},\lambda_{0m-11},\lambda_{01m-1},\lambda_{m-110},\lambda_{10m-1},\lambda_{m-101}\geq 1$, $\lambda_{i_0i_1i_2}=0$ *for* $(i_0\,i_1\,i_2)\neq(1m\text{–}10),(0m\text{–}11),(01m\text{–}1),(m\text{–}110),(10m\text{–}1),(m\text{–}101)$ *and* $\lambda_{1m-10}+\lambda_{0m-11}+\lambda_{01m-1}+\lambda_{m-110}+\lambda_{10m-1}+\lambda_{m-101}\leq 2m$.

一般化した実験計画法

静岡県立大学　経営情報学部　小林みどり

NTT　コミュニケーション科学基礎研究所　宮内美樹

東海大学　教育開発研究所　中村義作

これまでの実験計画法は，アダマール行列を用いて行っていた．今回，アダマール行列を一般化することに成功し，それに伴って，実験計画法も一般化が可能となった．すなわちこの一般化したアダマール行列を用いると，従来は不可能とされていた線型関係も解析できることが明らかになった．

	0	1	2	3	4	5	6	7
1	1	1	1	1	1	1	1	1
2	1	-1	1	-1	1	-1	1	-1
3	1	1	-1	-1	1	1	-1	-1
4	1	-1	-1	1	1	-1	-1	1
5	1	1	1	1	-1	-1	-1	-1
6	1	-1	1	-1	-1	1	-1	1
7	1	1	-1	-1	-1	-1	1	1
8	1	-1	-1	1	-1	1	1	-1

表１

	0	1	2	3	4	5	6	7
1	1	1	1	1	n1	n3	-n4	n2
2	1	-1	1	-1	n2	n4	n3	-n1
3	1	1	-1	-1	n3	-n1	-n2	-n4
4	1	-1	-1	1	n4	-n2	n1	n3
5	1	1	-1	-1	-n3	n1	n2	n4
6	1	-1	-1	1	-n4	n2	-n1	-n3
7	1	1	1	1	-n1	-n3	n4	-n2
8	1	-1	1	-1	-n2	-n4	-n3	n1

表２

表１は８×８のアダマール行列で，どの要素も１または－１としたうえ、どの横の２行も，どの縦の２列も直交するようにしたものである．表２はアダマール行列ではないが，どの縦の２列も直交しているという点で，アダマール行列と似ている．ここに，n1，n2，n3，n4 は任意の数でよい．

本稿では、表２を一般化した(８次の)アダマール行列と呼ぶが，その理由はアダマール行列が実験計画法の割り付け止利用されるのにたいし，一般化したアダマール行列が実験計画法の高度な割り付けに利用されるうえ，重回帰分析の効率的な解法にも結びついているからである．

	0	1	2	3	4	5	6	7
1	1	1	1	1	7	3	-1	5
2	1	-1	1	-1	5	1	3	-7
3	1	1	-1	-1	3	-7	-5	-1
4	1	-1	-1	1	1	-5	7	3
5	1	1	-1	-1	-3	7	5	1
6	1	-1	-1	1	-1	5	-7	-3
7	1	1	1	1	-7	-3	1	-5
8	1	-1	1	-1	-5	-1	-3	7

表３

いま（等間隔の）選点直交多項式の０次と１次の簡約係数が

０次：　１，1，１，１，１，１，１，１

１次：－７，－５，－３，－１，１，３，５，７

であることに着目して．表２の n1，n2，n3，n4 を

n1＝７，n2＝５，n3＝３，n4＝１

とおくと，表３を得る．すると、第４列～第７列に１次式が割り付けられるため、それらの列だけを利用すれば重回帰分析の効率的な解析に適用でき，すべての列を利用すれば１次式を含んだ実験計画法の割り付けに適用できる，ここに，重回帰分析の効率的な解析というのは，ふつうの重回帰分析では，分散・共分散行列の逆行列の計算が不可欠なのに，その計算が不要になることを意味する．

本発表では，具体的な数値例を挙げて，重回帰分析と実験計画法への応用の方法を示す．

アダマール行列の一般化

静岡県立大学 経営情報学部　小林みどり
NTT コミュニケーション科学基礎研究所　宮内美樹
東海大学 教育開発研究所　中村義作

1. はじめに

n を正の偶数とする．n 次アダマール行列 $H = (a_{ij})$ とは，n 次正方行列で，$a_{ij} = \pm 1$ $(i, j = 1, 2, \ldots, n)$, $H^T H = nI$ を満たすものをいう．一般化アダマール行列を次のように定義する．n 次一般化アダマール行列 $G = (a_{ij})$ とは，n 次正方行列で，ある整数 l $(1 \quad l \quad n)$ が存在して，

(i) $a_{i1} = 1$ $(i = 1, 2, \ldots, n)$

(ii) $a_{ij} = \pm 1$ $(i = 1, 2, \ldots, n,\ j = 2, 3, \ldots, n \quad l)$

(iii) $\{a_{ij} | i = 1, 2, \ldots, n\} = \{\pm 1, \pm 2, \ldots, \pm(n \quad 1)\}$　　$(j = n \quad l + 1, \ldots, n)$

(iv) G の任意の 2 列は直交する

を満たすものをいう．本稿では，n が 2 冪のときの一般化アダマール行列の構成法を検討する．

2. セットラテン符号方陣の構成

n 次セットラテン方陣とは，記号を成分とする n 次ラテン方陣であり，どの 2 行についても，$\begin{pmatrix} X \\ Y \end{pmatrix}$ があれば $\begin{pmatrix} Y \\ X \end{pmatrix}$ があるものをいう．n 次セットラテン方陣に対応するセット符号方陣とは，成分を $+$, 　とする n 次正方行列で，上記の $\begin{pmatrix} X \\ Y \end{pmatrix}$ と $\begin{pmatrix} Y \\ X \end{pmatrix}$ に対応する 4ヶ所の符号が $\{+, +, +, \ \}$ または $\{\ \ ,\ \ ,\ \ , +\}$ であるものをいう．n 次セットラテン符号方陣とは，n 次セットラテン方陣と，それに対応するセット符号方陣を合わせた行列である．したがって，セットラテン符号方陣は，どの 2 行についても内積が 0 となる．ここで，内積は形式的に計算するものとする．セットラテン符号方陣は，$n = 2, 4, 8$ のとき構成できたが，それ以外の n についての構成は未解決である．次の n 次セットラテン符号方陣を U_2, U_4, U_8 とおき，これらを用いて，次節で一般化アダマール行列を構成する．

$$U_2 = \begin{pmatrix} A & B \\ B & -A \end{pmatrix},\ U_4 = \begin{pmatrix} A & B & C & D \\ B & -A & D & -C \\ -C & D & A & -B \\ D & -C & B & -A \end{pmatrix}$$

$$U_8 = \begin{pmatrix} A & B & C & D & E & F & G & H \\ B & -A & D & -C & F & -E & -H & G \\ -C & D & A & -B & G & H & -E & -F \\ D & -C & B & -A & H & -G & F & -E \\ E & -F & -G & -H & -A & B & C & D \\ F & E & -H & G & -B & -A & -D & C \\ G & H & E & -F & -C & D & -A & -B \\ H & -G & F & E & -D & -C & B & -A \end{pmatrix}$$

3. 一般化アダマール行列の構成

n は 2 冪とする．$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ から Kronecker 積により生成される n 次アダマール行列を H_n とし，H_n を変形して n 次一般化アダマール行列を構成する．ここでは，$n = 16$ を例にしてその構成法を説明する．4 次セットラテン符号方陣 U_4 を利用する．U_4 の成分の A, B, C, D には，それぞ

れ $8,4,2,1$ を代入する．また，

$$H_{16}=\begin{pmatrix}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\
1&1&1&1&1&1&1&1&-1&-1&-1&-1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1&1&1&1&1&-1&-1&-1&-1\\
1&1&1&1&-1&-1&-1&-1&-1&-1&-1&-1&1&1&1&1\\
1&1&-1&-1&1&1&-1&-1&1&1&-1&-1&1&1&-1&-1\\
1&1&-1&-1&1&1&-1&-1&-1&-1&1&1&-1&-1&1&1\\
1&1&-1&-1&-1&-1&1&1&1&1&-1&-1&-1&-1&1&1\\
1&1&-1&-1&-1&-1&1&1&-1&-1&1&1&1&1&-1&-1\\
1&-1&1&-1&1&-1&1&-1&1&-1&1&-1&1&-1&1&-1\\
1&-1&1&-1&1&-1&1&-1&-1&1&-1&1&-1&1&-1&1\\
1&-1&1&-1&-1&1&-1&1&1&-1&1&-1&-1&1&-1&1\\
1&-1&1&-1&-1&1&-1&1&-1&1&-1&1&1&-1&1&-1\\
1&-1&-1&1&1&-1&-1&1&1&-1&-1&1&1&-1&-1&1\\
1&-1&-1&1&1&-1&-1&1&-1&1&1&-1&-1&1&1&-1\\
1&-1&-1&1&-1&1&1&-1&1&-1&-1&1&-1&1&1&-1\\
1&-1&-1&1&-1&1&1&-1&-1&1&1&-1&1&-1&-1&1
\end{pmatrix}$$

の第 1 列から第 16 列までの列ベクトルを，$1,a,b,ab,c,ac,bc,abc,d,ad,bd,abd,cd,acd,bcd,abcd$ とかく．ここで，たとえば，2 つの列ベクトル a,b の積 ab は，a と b の成分ごとの積からなる列ベクトルのことである．H_n の列ベクトル $x_1,x_2,\ldots,x_k$ が独立であるとは，$x_1,x_2,\ldots,x_k$ を並べた $n\times k$ 行列 $(x_1,x_2,\ldots,x_k)$ の行に，(1 1　　1) から (　1　　1　　　1) までの 2^k 通りのパターンが現れることである．

H_{16} の 4 個のベクトル $a,b,c,abcd$ は独立である．そこで，$(a,b,c,abcd)U_4=(h_1,h_2,h_3,h_4)$ とおく．また，ad,bd,cd,abc も独立であるので，同様に $(ad,bd,cd,abc)U_4=(h_5,h_6,h_7,h_8)$ とおく．H_{16} において，$\{a,b,c,abcd\}$ を $\{h_1,h_2,h_3,h_4\}$ で置き換え，$\{ad,bd,cd,abc\}$ を $\{h_5,h_6,h_7,h_8\}$ で置き換え，残りの 8 個のベクトルを左側に寄せる．このようにして，一般化アダマール行列 G_{16} が得られる．すなわち

$$G_{16}=\begin{pmatrix}
1&1&1&1&1&1&1&1&11&-5&15&-13&11&-5&15&-13\\
1&1&1&1&-1&-1&-1&-1&9&-1&7&3&-9&1&-7&-3\\
1&1&-1&-1&1&1&-1&-1&13&-3&-9&11&13&-3&-9&11\\
1&1&-1&-1&-1&-1&1&1&15&-7&-1&-5&-15&7&1&5\\
1&-1&1&-1&1&-1&1&-1&3&11&13&-9&1&15&5&7\\
1&-1&1&-1&-1&1&-1&1&1&15&5&7&-3&-11&-13&9\\
1&-1&-1&1&1&-1&-1&1&5&13&-11&15&7&9&-3&-1\\
1&-1&-1&1&-1&1&1&-1&7&9&-3&-1&-5&-13&11&-15\\
1&-1&-1&1&1&-1&-1&1&-7&-9&3&1&-7&-9&3&1\\
1&-1&-1&1&-1&1&1&-1&-5&-13&11&-15&5&13&-11&15\\
1&-1&1&-1&1&-1&1&-1&-1&-15&-5&-7&-1&-15&-5&-7\\
1&-1&1&-1&-1&1&-1&1&-3&-11&-13&9&3&11&13&-9\\
1&1&-1&-1&1&1&-1&-1&-15&7&1&5&-13&3&9&-11\\
1&1&-1&-1&-1&-1&1&1&-13&3&9&-11&15&-7&-1&-5\\
1&1&1&1&1&1&1&1&-9&1&-7&-3&-11&5&-15&13\\
1&1&1&1&1&-1&-1&-1&-11&5&-15&13&9&-1&7&3
\end{pmatrix}$$

同様の考え方で，次の結果が得られる．$n=2^m$ $(m=1,2,\ldots,8)$ 以外の一般化アダマール行列の構成については現在未解決である．これらの一般化アダマール行列は，正の成分を 1 に，負の成分を 1 に置き換えると，普通のアダマール行列になることが作り方から分かる．

定理　$n=2^m$ $(m=1,2,\ldots,8)$ のとき，n 次一般化アダマール行列が存在する．

直線と Conic の交点と Balanced Array

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 $\mathrm{PG}(2,q)$ 上の k 個の点からなる集合で、そのうちどの $d+1$ 点も同一直線上にないようなものを (k,d)-*arc* といい、$d=2$ のときは特に k-arc という。射影平面上の conic は $(q+1)$-arc である。

S を s 個のシンボルからなる集合とし、S^t を S 上のすべての t 次元ベクトルの集合とする。$N \quad k$ 配列 A が以下の条件を満たすとき、A を強さ t の**均斉配列** *(balanced array)* と呼び、$BA_\mu(N,k,s,t)$ のように書く:

1. どの t 列からなる部分配列においても、任意の $\boldsymbol{a} \in S^t$ が行として $\mu_{\boldsymbol{a}}$ 回現れる。
2. 任意の行ベクトル $\boldsymbol{a} \in S^t$ の成分に対する置換 σ について、$\mu_{\sigma(\boldsymbol{a})} = \mu_{\boldsymbol{a}}$ が成り立つ。

すべての $\boldsymbol{a} \in S^t$ に対して $\mu_{\boldsymbol{a}} = \mu$ であるとき、配列 A は**直交配列**となる。

以下では、射影平面上のある点 P を通るすべての conic の集合と、点 P を通らないすべての直線の集合を用いる事により、強さ 2 の均斉配列が得られる事を示す。

2　conic と 2 直線の交点数

射影平面 $\mathrm{PG}(2,q)$ 上の点 P に対し、$\mathcal{C}$ を点 P を通るすべての conic の集合とし、$\mathcal{L}$ を P を通らないすべての直線の集合とする。$\mathcal{C}$ の conic の数は $|\mathcal{C}| = q^2(q+1)(q-1)$ であり、$|\mathcal{L}| = q^2$ である。$\mathcal{L}$ の異なる 2 直線 l_1 と l_2 に対し、l_1 と α 個の点で交わり、かつ l_2 と β 個の点で交わる $\mathcal{C}$ の conic の数を $\mu_{(\alpha,\beta)}(l_1,l_2)$ で表すものとする。すなわち、$\mu_{(\alpha,\beta)}(l_1,l_2) = |\{C \in \mathcal{C} : |C \cap l_1| = \alpha, |C \cap l_2| = \beta\}|$ とする。以下では、$\mu_{(\alpha,\beta)}(l_1,l_2)$ を求めるために、必要に応じて l_1 と l_2 の交点 R を通るときと通らないときとに場合分けし、l_1,l_2 との交点の個数がそれぞれ α, β であるような conic の集合を定め、その要素の個数についての補題を列挙していく。点 R を l_1 と l_2 の交点とし、$\mathcal{C}_R$ を R を通る $\mathcal{C}$ の conic からなる集合、$\bar{\mathcal{C}}_R$ を R を通らない $\mathcal{C}$ の conic からなる集合とする。

補題 1 $\mathcal{C}_1 = \{C \in \bar{\mathcal{C}}_R : |C \cap l_1| = 2, |C \cap l_2| = 2\}$ としたとき、$|\mathcal{C}_1| = \frac{1}{4}q(q-1)(q-2)(q-3)$ である。

補題 2 $\mathcal{C}_2 = \{C \in \mathcal{C}_R : |C \cap l_1| = 2, |C \cap l_2| = 2\}$ としたとき、$|\mathcal{C}_2| = q(q-1)(q-2)$ である。

補題 3 $\mathcal{C}_3 = \{C \in \bar{\mathcal{C}}_R : |C \cap l_1| = 2, |C \cap l_2| = 1\}$ とすると、$|\mathcal{C}_3| = \frac{1}{2}q(q-1)(q-2)$ である。

補題 4 $\mathcal{C}_4 = \{C \in \mathcal{C}_R : |C \cap l_1| = 2, |C \cap l_2| = 1\}$ とすると、$|\mathcal{C}_4| = q(q-1)$ である。

補題 5 $\mathcal{C}_5 = \{C \in \mathcal{C} : |C \cap l_1| = 2, C \cap l_2 = \emptyset\}$ とすると、$|\mathcal{C}_5| = \frac{1}{4}q^2(q-1)^2$ である。

補題 6 $\mathcal{C}_6 = \{C \in \mathcal{C} : |C \cap l_1| = 1, |C \cap l_2| = 1\}$ とすると、$|\mathcal{C}_6| = q(q-1)$ である。

補題 7 $\mathcal{C}_7 = \{C \in \mathcal{C} : |C \cap l_1| = 1, C \cap l_2 = \emptyset\}$ とすると、$|\mathcal{C}_7| = \frac{1}{2}q^2(q-1)$ である。

補題 8 $\mathcal{C}_8 = \{C \in \mathcal{C} : C \cap l_1 = \emptyset, C \cap l_2 = \emptyset\}$ とする。このとき、$|\mathcal{C}_8| = \frac{1}{4}(q+1)q(q-1)(q-2)$ である。

3 均斉配列との対応

補題 1 から 8 において示されたそれぞれの conic の個数は、l_1 や l_2 の選び方によらない事が言える。よって、次のように交点数を配列の要素に置く事により、均斉配列が得られる。

A を $N \quad k$ 配列 (a_{ij}) とする。ここで、

$$a_{ij} = |C_i \cap l_j|,\ C_i \in \mathcal{C} \text{ and } \ l_i \in \mathcal{L}$$

とする。このとき、A の行の数は $\mathcal{C}$ の conic の数に等しく、列の数は $\mathcal{L}$ の直線の数となる。よって、$N = q^2(q+1)(q-1)$ であり、 $k = q^2$ である。補題 1 から 8 より、以下の定理が言える。

定理 9 配列 A は均斉配列 $BA_\mu(q^2(q+1)(q-1), q^2, 3, 2)$ であり、

$$\mu_{(\alpha,\beta)} = \begin{cases} \frac{1}{4}(q+1)q(q-1)(q-2) & \text{if } (\alpha,\beta) = (0,0) \text{ or } (2,2), \\ \frac{1}{2}q^2(q-1) & \text{if } \alpha - \beta = \quad 1, \\ \frac{1}{4}q^2(q-1)^2 & \text{if } \alpha - \beta = \quad 2, \\ q(q-1) & \text{if } (\alpha,\beta) = (1,1). \end{cases}$$

となる。

参考文献

[1] I.M. Chakravarti, *Fractional replication in asymmetrical factorial designs and partially balanced arrays*, Sankhya, vol. 17, pp. 143-164, 1956.

[2] R. Fuji-Hara, S. Kageyama, S. Kuriki, Y. Miao and S. Shinohara, "Balanced nested designs and balanced arrays", *Discrete Mathematics*, Vol. 259, pp.91–119, 2002.

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

[4] N. Miyamoto, H. Mizuno and S. Shinohara, "Optical orthogonal codes obtained from conics on finite projective planes", *Finite Fields and Their Applications*, vol. 10, pp. 405-411, 2004.

[5] N. Miyamoto and S. Shinohara, "Mutually M-intersecting (k,d)-arcs and its application to optical orthogonal codes", *Congressus Numerantium*, vol. 169, pp. 23–31, 2004.

[6] J.A. Rafter and E. Seiden, *Contributions to the theory and construction of balanced arrays*, Ann. Statest, vol. 2, pp. 1256–1273, 1974.

[7] J.N. Srivastava, *Some general existence conditions for balanced arrays of strength t and 2 symbols*, J. Combin. Theory Ser. A, vol. 13, pp. 198-206, 1972.

デザイン構造をもつマトロイドについて[1]

愛知県立大学　情報科学部　城本 啓介

q-元体 $\mathbb{F}_q$ 上の線形符号と組合せデザインの間には深い関係があり，古くから考察されている．特に，様々な符号を用いて 5-デザインをはじめとした組合せデザインを構成する研究は有名である（[1] 等）．また，マトロイドと組合せデザインにも関連性はあり，マトロイドを用いた組合せデザインの構成などが研究されている．一方で，マトロイドは符号の概念を拡張した離散構造を考えることができることから（[3] 等），これらの 3 つの数理構造を統一的に考察することで各分野における研究への新たなアプローチを行うことが本研究の目的である．ここでは，以下の問題について考察する．

問題 1 デザイン構造をもつマトロイドはどのような特徴をもつか？

以下のマトロイドの一つの定義を記す．なお，マトロイド理論の詳細は [4] や [5] を参照されたい．

定義 2 マトロイド（*matroid*）とは，有限集合 E と写像 $\rho : 2^E \to Z_{\geq 0}$ の順序対 $\mathcal{M} = (E, \rho)$ であり，以下の 3 条件を満たすものである：

(R1) $X \subseteq E$ ならば $0 \leq \rho(X) \leq |X|$,
(R2) $X \subseteq Y \subseteq E$ ならば $\rho(X) \leq \rho(Y)$,
(R3) $X, Y \subseteq E$ ならば $\rho(X \cup Y) + \rho(X \cap Y) \leq \rho(X) + \rho(Y)$

マトロイド $\mathcal{M} = (E, \rho)$ に対して，$X (\subseteq E)$ が i-flat であるとは，$\rho(X) = i$ であり，任意の $x \in E - X$ に対して，$\rho(X \cup \{x\}) = \rho(X) + 1$ が成立することである．特に，極大な flat を $\mathcal{M}$ の hyperplane という．以後，$\mathcal{M}$ の hyperplane の集合を $\mathcal{H}$ で表す．さらに，$C (\subseteq E)$ が circuit であるとは，任意の $x \in C$ に対して，$\rho(C) = |C| - 1 = \rho(C - \{x\})$ が成立することである．$\mathcal{M}$ の citcuit の集合を $\mathcal{C}$ で表す．また，$\mathcal{F}_i$ を i-flat の集合，$\mathcal{C}_i$ は位数 i である circuit の集合とする．以下に，組合せデザインと関連した構造を持つマトロイドについて考察する．

任意のマトロイド $\mathcal{M}$ とその hyperplane 族 $\mathcal{H}$ に対して，$\mathcal{C}^* = \{E - H \ : \ H \in \mathcal{H}\}$ を circuit 族とするマトロイドを $\mathcal{M}$ の双対マトロイドといい，$\mathcal{M}^*$ で表す．さらに，以下の概念を導入する．

$$
\begin{aligned}
p(\mathcal{M}; \lambda) &:= \sum_{X \subseteq E} (-1)^{|X|} \lambda^{\rho(\mathcal{M}) - \rho(X)} \\
A_{\mathcal{M}}(i, \lambda) &:= \sum_{X \in \binom{E}{i}} p(\mathcal{M}.X; \lambda) \\
\mathcal{R}_{M,t} &:= \{j \in \{1, \ldots, n-t\} \ : \ A_{\mathcal{M}^*}(j, \lambda) \neq 0\}, \\
d_{\mathcal{M}} &:= \min\{|X| \ : \ X \in \mathcal{C}(\mathcal{M})\}
\end{aligned}
$$

このとき，以下の Assmus-Mattson 型の定理が成立する（[2]）．

定理 3 次の条件を満たす整数 t $(0 < t < d_{\mathcal{M}})$ が存在するとき，任意の i に対して $(E, \mathcal{C}_i)$ は t-design となる．

1. $|\mathcal{R}_{\mathcal{M},t}| < d_{\mathcal{M}} - t$
2. すべての $T \in \binom{E}{t}$ と $l = 1, \ldots, n-t$ に対して，$A_{\mathcal{M}^*}(l, \lambda) = 0$ である場合は $A_{\mathcal{M}^*/T}(l, \lambda) = 0$

[1]本研究は Thomas Britz 氏 (University of New South Wales, Australia) との共同研究の一部である．

逆に，組合せデザインから構成されるマトロイドについては，以下のことが知られている．

定義 4 マトロイド $\mathcal{M} = (E, \rho)$ が *perfect matroid design* (PMD) であるとは，すべての i-flat の位数が等しいときである．

PMD の構成法についてはそれほど多くは知られておらず，射影幾何やアフィン幾何の直線集合からの構成法が有名であり，現在でも様々な離散構造からの構成法を提案することが研究されている．特に，PMD と組合せデザインの関係としては，以下の結果が知られている．

命題 5 (Young-Edmonds ([6])) $t = \min\{|X| : X \in \mathcal{C}\} - 1$ とする．このとき，$\mathcal{M}$ が PMD ならば，各 i, j に対して $(E, \mathcal{F}_i)$ と $(E, \mathcal{C}_i)$ はともに t-design をなす．

また，PMD の組合せデザインによる構成法としては，以下の定理が知られている．

定理 6 (Young-Edmonds ([6])) $(E, \mathcal{H})$ を t-$(v, k, 1)$ design とする．このとき，$\mathcal{H}$ を hyperplane 族とするマトロイド $\mathcal{M}$ は PMD であり，$(E, \mathcal{C}_{t+1})$ と $(E, \mathcal{C}_{t+2})$ はそれぞれ t-$(v, t+1, k-t)$, t-$(v, t+2, \frac{(v-k)(v-(t+1)(v-t+1))}{2})$ designs である．特にこの場合 $\mathcal{C} = \mathcal{C}_{t+1} \cup \mathcal{C}_{t+2}$ である．

ここで，考えたい問題としてはこの定理の逆が成立するかと言うことである．つまり，以下の問題を考察したい．

問題 7 与えられた t-$(v, t+1, k-t)$ design $(E, \mathcal{C}_{t+1})$ と t-$(v, t+2, \frac{(v-k)(v-(t+1)(v-t+1))}{2})$ design $(E, \mathcal{C}_{t+2})$ に対して，$\mathcal{C} = \mathcal{C}_{t+1} \cup \mathcal{C}_{t+2}$ を circuit 族とするマトロイドは存在するか？また存在した場合は PMD であるか？

手始めに，$\mathcal{C}_{t+2} = \emptyset$ となる場合，つまり，$v - (t+1)(v-t+1) = 0$ の場合に限定して考察を進めた．この場合，$t = 5$ とすると，$v = 12\,(k = 6), 18\,(k = 7), 24\,(k = 8), 30\,(k = 9), 36\,(k = 10), 42\,(k = 11), 48\,(k = 12), \ldots$ である．ここで，個別にデザインのパラメータを考察することで現時点では以下のことが判明した．

命題 8 $(E, \mathcal{C})$ が 5-$(12, 6, 1)$ または 5-$(24, 6, 3)$ design ならば，対応するマトロイドは PMD である．

ちなにみ，$v = 18, 30$ では上記のような事実が成立しないことが分かった．今後の課題としては，上記の事実が成立するようなデザインのパラメータに関して統一的考察を行い，より一般的なパラメータの形で記述を行うことである．

References

[1] E. F. Assmus and H. F. Mattson, New 5-designs, *J. Combin.* **6** (1969), 122–151.

[2] T. Britz, G. Royle and K. Shiromoto, Designs from matroids, submitted.

[3] C. Greene, Weight enumeration and the geometry of linear codes, *Stud. Appl. Math.* **55** (1976), pp. 119–128.

[4] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.

[5] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.

[6] P. Young and J. Edmonds, Matroid designs, *J. Res. Nat. Bur. Stand. B* **77B** (1973), 15–44.

Single-Change Covering Designs

W. D. Wallis, Southern Illinois University

Given positive integers v, k and λ, a (v, k, λ)-*covering design* is a collection of k-subsets (blocks) of a given v-set V in which every pair of elements of V occur together in at least λ of the blocks.

An *ordered* (v, k, λ)-*covering design* or $OC(v, k, \lambda)$ is a (v, k, λ)-covering design together with a way to order the blocks of the design.

Suppose the blocks of an ordered covering design are (in order) $B_1, B_2, \ldots, B_n$. The *cost* of B_i $(i > 1)$ is c_i,

$$c_i = |B_i \backslash B_{i-1}|;$$

that is, the cost is the number of changes from the preceding block. The cost of S is defined to be

$$c(S) = \sum_{i=2}^{n} c_i \, .$$

Ordered covering designs arise in the testing of electrical components for compatibility. The testing device takes several components and tests them simultaneously, so a block consists of the set of components which are tested together. The test is electrical, and the cost is negligible; but the (mechanical) insertion and removal of components has a signficant cost (in terms of operator time). For this application, low-cost ordered covering designs are needed.

We define $c(v, k)$ to be the minimum, for all $OC(v, k, 1)$-designs S, of $c(S)$. We would like:

(i) to find $c(v, k)$;

(ii) to find an $OC(v, k, 1)$, call it $S = S(v, k)$ such that $c(S) = c(v, k)$;

(iii) if (i) or (ii) cannot be achieved, to find a lower bound on $c(v,\, k)$ and to find a design S such that $c(S)$ is close to the bound, for given v and k.

Suppose an $OC(v, k, \lambda)$ contains the successive blocks

$$B_0 = \{a_1,\, a_2,\, \ldots,\, a_{c-1},\, a_c,\, x_1,\, x_2,\, \ldots,\, x_d\}$$
$$B_c = \{b_1,\, b_2,\, \ldots,\, b_{c-1},\, b_c,\, x_1,\, x_2,\, \ldots,\, x_a\}.$$

The total cost is unchanged if we insert between these two $B_1,\, B_2,\, \ldots,\, B_{c-1}$, where

$$B_i = \{b_1,\, b_2,\, \ldots,\, b_i,\, a_{i+1},\, \ldots,\, a_c,\, x_1,\, x_2,\, \ldots,\, x_d\}.$$

In other words, given any $OC(v,\, k,\, \lambda)$, there will be an $OC(v,\, k,\, \lambda)$ of the same cost in which each block has cost 1. We call such a design a *single change covering design.* (SCCD) So we concentrate on single change $OC(v,\, k,\, 1)s$. If one has b blocks, denote it by $SC(v,\, k,\, b)$, or just $SC(v,\, k)$. Usually discuss $f(v,\, \lambda) = c(v,\, \lambda) + 1$, the *minimum number of blocks*, rather than the minimum cost.

Trivially, the addition of $l - k$ new elements to every block of an $SC(v + k,\, k,\, b)$ results in an $SC(v + l,\, l,\, b)$. So:

Lemma 1. *$f(v + k,\, k) \geq f(v + l,\, l)$ when $k \leq l$.*

Lemma 2. *The number of blocks in an $SC(v,\, k)$ is at least*

$$m(v, k) = \left\lceil \left\{ \binom{v}{2} - \binom{k-1}{2} \right\} / (k-1) \right\rceil . \tag{1}$$

We call an $SC(v,\, k)$ *economical* if it attains the bound (1). We say case $(v,\, k)$ is *tight* (TSCCD) if $k - 1$ divides $\binom{v}{2} - \binom{k}{2}$. In this case, denote the design $TSC((v,\, k)$. If the number of blocks is b, then

$$\binom{v}{2} - \binom{k}{2} = (b-1)(k-1).$$

Theorem 1. *There is an economical $SC(v,\, 3)$ for all $v \geq 3$.*

This theorem shows that $f(v,\, 3) = m(v,\, 3)$ for all $v \geq 3$. This is not true in general: for example, economical $SC(v,\, k)$ do *not* exist in the tight cases $v = 6,\, 7,\, 9$, for $k = 4$.

In this talk we shall prove some of these results and indicate some directions for further research.

Decomposing complete graphs into sun graphs of n-cycle

Chin-Mei Fu
Department of Mathematics, Tamkang University
cmfu@mail.tku.edu.tw

Let G be a graph with at least three vertices and suppose $V(G) = \{v_1, v_2, v_3, \ldots, v_n\}$. Add n new vertices $\{w_1, w_2, w_3, \ldots, w_n\}$ to G together with edges $\{v_i, w_i\}$, for $1 \le i \le n$. The resulting graph on $2n$ vertices is called a sun graph of G, denoted by $S(G)$. (Note that $\deg_{S(G)} w_i = 1$ for all i, $1 \le i \le n$.) A sun graph of n-cycle, $S(C_n)$, is a graph with 2n vertices $v_1, v_2, v_3, \ldots, v_{2n}$ and 2n edges $\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_n, v_1\}, \{v_1, v_{n+1}\}, \{v_2, v_{n+2}\}, \ldots, \{v_n, v_{2n}\}$, i.e. $S(C_n)$ is the union of one n-cycle C_n and one 1-factor. A graph G is decomposable into subgraphs $H_1, H_2, \ldots, H_m$ of G if no H_i (i = 1, 2, .., n) has isolated vertices and the edge set E(G) can be partitioned into the subsets $E(H_1)$, $E(H_2)$, …, $E(H_m)$. If $H_i \cong S(C_n)$ for all i, then G is called $S(C_n)$-decomposable.

First we consider n = 3.

A sun graph of 3-cycle, $S(C_3)$, is a graph with six vertices $v_1, v_2, v_3, v_4, v_5, v_6$ and edges $\{v_1, v_2\}, \{v_2, v_3\}, \{v_3, v_1\}, \{v_1, v_4\}, \{v_2, v_5\}, \{v_3, v_6\}$ which is formed a 3-cycle (v_1, v_2, v_3) and a 1-factor $\{\{v_1, v_4\}, \{v_2, v_5\}, \{v_3, v_6\}\}$, thus we denote it as $[(v_1, v_2, v_3), v_4, v_5, v_6]$. Since $S(C_3)$ is a tripartite graph, we will consider what is the necessary and sufficient condition such that the complete tripartite graph $K_{p,q,r}$ can be $S(C_n)$-decomposable. First we obtain that if $K_{p,q,r}$ is $S(C_3)$-decomposable then $6 \mid (pq+qr+pr)$ and $r \ge \max\{\frac{p}{3}, \frac{pq}{p+q}\}$. Then we get the necessary and sufficient condition for the complete tripartite graph $K_{p,p,r}$.

Theorem 1. $K_{p,p,r}$ is $S(C_3)$-decomposable if and only if $\frac{p}{2} \le r \le \frac{5p}{2}$ and one of the following condition holds:

(1) $p \equiv 0 \pmod 6$. (2) p and $r \equiv 2 \pmod 6$. (3) p and $r \equiv 4 \pmod 6$.

By using Theorem 1 and the construction of Steiner triple system, we prove the following results.

Theorem 2. K_n is $S(C_3)$-decomposable if and only if $n \equiv 0, 1, 4, 9 \pmod{12}$.

After this, we try to embed a Steiner triple system into $S(C_3)$-system.

Theorem 3. A Steiner triple system of order 6m+1 can be embedded into $S(C_3)$-system of order 12m+1.

Next, we consider n = 4.

A sun graph of 4-cycle, $S(C_4)$, is a graph with eight vertices v_1, v_2, v_3, v_4, v_5, v_6, v_7, v_8 and edges $\{v_1, v_2\}$, $\{v_2, v_3\}$, $\{v_3, v_4\}$, $\{v_4, v_1\}$, $\{v_1, v_5\}$, $\{v_2, v_6\}$, $\{v_3, v_7\}$, $\{v_4, v_8\}$ which is formed a 4-cycle (v_1, v_2, v_3, v_4) and a 1-factor $\{\{v_1, v_5\}, \{v_2, v_6\}, \{v_3, v_7\}, \{v_4, v_8\}\}$, thus we denote it as $[(v_1, v_2, v_3, v_4), v_5, v_6, v_7, v_8]$. Since $S(C_4)$ is a bipartite graph, we will consider what is the necessary and sufficient condition such that the complete bipartite graph $K_{p,q}$ can be $S(C_4)$-decomposable. First we obtain the following results:

Theorem 4. Let p and q be integers greater than or equal to 4 and $p \geq q$. $K_{p,q}$ is $S(C_4)$-decomposable if and only if $8 \mid pq$ except $q=4$, $p \equiv 2 \pmod 4$, $q = 5$.

From this decomposition we can get the following result.

Theorem 5. K_n is $S(C_4)$-decomposable if and only if $n \equiv 0, 1 \pmod{16}$.

In this talk, I will show the construction of each theorem. In the follows, one can show the extension of these results to $n > 4$.

Hamilton C_k-Trefoil Designs

Kazuhiko Ushio
Department of Informatics
Faculty of Science and Technology
Kinki University

Let K_n denote *the complete graph* of n vertices. *The complete multi-graph* λK_n is the complete graph K_n in which every edge is taken λ times. Let C_k be *the k-cycle* (or *the cycle* on k vertices). *The C_k-trefoil* is a graph of 3 edge-disjoint C_k's with a common vertex and the common vertex is called *the center of the C_k-trefoil*. In particular, a C_k-trefoil satisfying $n = 3(k-1)+1$ is called *the Hamilton C_k-trefoil* because the C_k-trefoil spans λK_n.
When λK_n is decomposed into edge-disjoint sum of Hamilton C_k-trefoils, we say that λK_n *has a Hamilton C_k-trefoil decomposition*. This Hamilton C_k-trefoil decomposition of λK_n is called *a Hamilton C_k-trefoil design*.

Theorem 1. If λK_n has a Hamilton C_k-trefoil decomposition, then (i) $n = 3(k-1)+1$ and (ii) $\lambda \equiv 0 \pmod{k}$ for odd k, $\lambda \equiv 0 \pmod{k}$ for $k \equiv 0 \pmod 4$, $\lambda \equiv 0 \pmod{k/2}$ for $k \equiv 2 \pmod 4$.

Theorem 2. If λK_n has a Hamilton C_k-trefoil decomposition, then $(s\lambda)K_n$ has a Hamilton C_k-trefoil decomposition for every s.

Theorem 3. Let n be prime. When $n = 3(k-1)+1$, $\lambda \equiv 0 \pmod{k}$, and k odd, λK_n has a Hamilton C_k-trefoil decomposition.

Example 3.1. Hamilton C_3-trefoil of $3K_7$.
$(n, g) = (7, 3)$ n-orbit : $1, 3, 2, 6, 4, 5, 1$.
$H = (7, 1, 3) \cup (7, 2, 6) \cup (7, 4, 5)$.
This starter comprises a Hamilton C_3-trefoil decomposition of $3K_7$.

Example 3.2. Hamilton C_5-trefoil of $5K_{13}$.
$(n, g) = (13, 2)$ n-orbit : $1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1$.
$H = (13, 1, 2, 4, 8) \cup (13, 3, 6, 12, 11) \cup (13, 9, 5, 10, 7)$
$H = (13, 2, 4, 8, 3) \cup (13, 6, 12, 11, 9) \cup (13, 5, 10, 7, 1)$.
These 2 starters comprise a Hamilton C_5-trefoil decomposition of $5K_{13}$.

Example 3.3. Hamilton C_7-trefoil of $7K_{19}$.
$(n, g) = (19, 2)$ n-orbit : $1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1$.
$H = (19, 1, 2, 4, 8, 16, 13) \cup (19, 7, 14, 9, 18, 17, 15) \cup (19, 11, 3, 6, 12, 5, 10)$
$H = (19, 2, 4, 8, 16, 13, 7) \cup (19, 14, 9, 18, 17, 15, 11) \cup (19, 3, 6, 12, 5, 10, 1)$
$H = (19, 4, 8, 16, 13, 7, 14) \cup (19, 9, 18, 17, 15, 11, 3) \cup (19, 6, 12, 5, 10, 1, 2)$.
These 3 starters comprise a Hamilton C_7-trefoil decomposition of $7K_{19}$.

Example 3.4. Hamilton C_{11}-trefoil of $11K_{31}$.
$(n, g) = (31, 3)$ n-orbit : $1, 3, 9, 27, 19, 26, 16, 17, 20, 29, 25, 13, 8, 24, 10, 30, 28, 22, 4, 12, 5, 15, 14, 11, 2, 6, 18, 23, 7, 21, 1$.
5 starters comprise a Hamilton C_{11}-trefoil decomposition of $11K_{31}$.

Example 3.5. Hamilton C_{13}-trefoil of $13K_{37}$.
$(n, g) = (37, 2)$ n-orbit : $1, 2, 4, 8, 16, 32, 27, 17, 34, 31, 25, 13, 26, 15, 30, 23, 9, 18, 36, 35, 33, 29, 21,$

$5, 10, 20, 3, 6, 12, 24, 11, 22, 7, 14, 28, 19, 1$.
6 starters comprise a Hamilton C_{13}-trefoil decomposition of $13K_{37}$.

Example 3.6. Hamilton C_{15}-trefoil of $15K_{43}$.
$(n, g) = (43, 3)$ n-orbit : $1, 3, 9, 27, 38, 28, 41, 37, 25, 32, 10, 30, 4, 12, 36, 22, 23, 26, 35, 19, 14, 42, 40,$
$34, 16, 5, 15, 2, 6, 18, 11, 33, 13, 39, 31, 7, 21, 20, 17, 8, 24, 29, 1$.
7 starters comprise a Hamilton C_{15}-trefoil decomposition of $15K_{43}$.

Example 3.7. Hamilton C_{21}-trefoil of $21K_{61}$.
$(n, g) = (61, 2)$ n-orbit : $1, 2, 4, 8, 16, 32, 3, 6, 12, 24, 48, 35, 9, 18, 36, 11, 22, 44, 27, 54, 47, 33, 5, 10, 20,$
$40, 19, 38, 15, 30, 60, 59, 57, 53, 45, 29, 58, 55, 49, 37, 13, 26, 52, 43, 25, 50, 39, 17, 34, 7, 14, 28, 56, 51, 41,$
$21, 42, 23, 46, 31, 1$.
10 starters comprise a Hamilton C_{21}-trefoil decomposition of $21K_{61}$.

Example 3.8. Hamilton C_{23}-trefoil of $23K_{67}$.
$(n, g) = (67, 2)$ n-orbit : $1, 2, 4, 8, 16, 32, 64, 61, 55, 43, 19, 38, 9, 18, 36, 5, 10, 20, 40, 13, 26, 52,$
$37, 7, 14, 28, 56, 45, 23, 46, 25, 50, 33, 66, 65, 63, 59, 51, 35, 3, 6, 12, 24, 48, 29, 58, 49, 31, 62, 57,$
$47, 27, 54, 41, 15, 30, 60, 53, 39, 11, 22, 44, 21, 42, 17, 34, 1$.
11 starters comprise a Hamilton C_{23}-trefoil decomposition of $23K_{67}$.

Example 3.9. Hamilton C_{25}-trefoil of $25K_{73}$.
$(n, g) = (73, 5)$ n-orbit : $1, 5, 25, 52, 41, 59, 3, 15, 2, 10, 50, 31, 9, 45, 6, 30, 4, 20, 27, 62, 18, 17,$
$12, 60, 8, 40, 54, 51, 36, 34, 24, 47, 16, 7, 35, 29, 72, 68, 48, 21, 32, 14, 70, 58, 71, 63, 23, 42, 64, 28,$
$67, 43, 69, 53, 46, 11, 55, 56, 61, 13, 65, 33, 19, 22, 37, 39, 49, 26, 57, 66, 38, 44, 1$.
12 starters comprise a Hamilton C_{25}-trefoil decomposition of $25K_{73}$.

References

[1] K. Ushio, G-designs and related designs, *Discrete Math.*, Vol. 116, pp. 299–311, 1993.
[2] 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.
[3] 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.
[4] 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.
[5] K. Ushio and H. Fujimoto, Balanced foil decomposition of complete graphs, *IEICE Trans. Fundamentals*, Vol. E84-A, No. 12, pp. 3132–3137, December 2001.
[6] K. Ushio and H. Fujimoto, Balanced bowtie decomposition of complete multigraphs, *IEICE Trans. Fundamentals*, Vol. E86-A, No. 9, pp. 2360–2365, September 2003.
[7] K. Ushio and H. Fujimoto, Balanced bowtie decomposition of symmetric complete multidigraphs, *IEICE Trans. Fundamentals*, Vol. E87-A, No. 10, pp. 2769–2773, October 2004.
[8] K. Ushio and H. Fujimoto, Balanced quatrefoil decomposition of complete multigraphs, *IEICE Trans. Information and Systems*, Vol. E88-D, No. 1, pp. 19–22, January 2005.
[9] K. Ushio and H. Fujimoto, Balanced C_4-bowtie decomposition of complete multigraphs, *IEICE Trans. Fundamentals*, Vol. E88-A, No. 5, pp. 1148–1154, May 2005.
[10] K. Ushio and H. Fujimoto, Balanced C_4-trefoil decomposition of complete multigraphs, *IEICE Trans. Fundamentals*, Vol. E89-A, No. 5, pp. 1173–1180, May 2006.

A construction of a cyclic SQS($2p$) for prime p

名古屋大学大学院　情報科学研究科　吉川智史　神保雅一

本報告では、奇素数 p に対し、$\mathbf{Z}_{2p}$ のすべての unit を multiplier として持つ巡回的 Steiner quadruple system の構成法について考える。

V を v 個の要素からなる有限集合（要素を点（point）と呼ぶ）とし、$\mathcal{B}$ を V の 4 元部分集合族（$|\mathcal{B}| = b$、要素を block と呼ぶ）とする。このとき、任意の異なる 3 点が、ただ 1 つの block に現れるような $(V, \mathcal{B})$ の組を Steiner quadruple system (SQS) と呼び、SQS(v) と書く。また SQS が存在するための条件は、$v \equiv 2, 4 \pmod 6$ である。

SQS(v) $(V, \mathcal{B})$ に長さ v の巡回自己同型変換 σ が存在するとき、**cyclic** SQS という。$(V, \mathcal{B})$ が cyclic SQS のとき、V を $\mathbf{Z}_v$、σ を $x \mapsto x + 1 \pmod v$ とすることができる。また G を SQS の自己同型群の部分群とするとき、block orbit $orb_G(B) = \{B^G \mid g \in G\}$ を B の G-orbit と呼ぶ。特に $G = \langle\sigma\rangle$ のとき、$orb_{\langle\sigma\rangle}(B)$ を単に $orb_\sigma(B)$ と書き、**cyclic orbit** と呼ぶ。$|orb_\sigma(B)| = v$ のとき、orbit は **full** であるという。さらに、すべての cyclic orbit が full であるような SQS を **strictly cyclic** とであるといい、**sSQS** と書く。また orbit の代表元を **base block** と呼ぶ。

$\mathbf{Z}_v$ 上の cyclic SQS(v) において、任意の $B \in \mathcal{B}$ に対して $xB \in \mathcal{B}$ である $x \in \mathbf{Z}_v$ を **multiplier** という。乗法群 $\mathbf{Z}_v^\times$ のすべての要素が multiplier となるとき、SQS は Hol($\mathbf{Z}_v$)-**invariant** であるという。ただし、$\mathrm{Hol}(\mathbf{Z}_v) = \mathbf{Z}_v \rtimes \mathrm{Aut}(\mathbf{Z}_v)$ であり、$G = \mathrm{Hol}(\mathbf{Z}_v)$ とする。

なお過去にも Köhler [1]、Siemon [2–6]、Bitan ら [7]、Chu ら [8]、Feng ら [9] による cyclic SQS、sSQS の構成方法が考えられているが、本報告では、Hol($\mathbf{Z}_{2p}$)-invariant sSQS($2p$) (p は素数、$p \equiv 1, 5 \pmod{12}$) の構成について考える。

点の集合を $V = \mathbf{Z}_{2p}$ とする。$\mathbf{Z}_{2p} \simeq \mathbf{Z}_2 \quad \mathbf{Z}_p = \{(x, y) \mid x \in \mathbf{Z}_2, y \in \mathbf{Z}_p\}$ と書けるので、$V_x = \{(x, y) \mid y \in \mathbf{Z}_p\}$ とすると、$V = V_0 \cup V_1$ とできる。また V 上の加法を $(x, y) + (x', y') \equiv (x + x', y + y') \pmod{(2, p)}$、乗法を $(x, y)(x', y') \equiv (xx', yy') \pmod{(2, p)}$ と定義する。このとき、SQS の block は次の 3 種類に分類される。

Type 1 : V_0、V_1 の 2 点ずつからなる block
Type 2 : V_0、V_1 の一方から 3 点、もう一方の 1 点からなる block
Type 3 : V_0 もしくは V_1 の 4 点からなる block

ただし本報告では、Type 3 は除外し、Type 1 と Type 2 のみで SQS を構成する。また block の各要素に $(1, 0)$ を加えてできる block も SQS の block になる。したがって、V_0、V_1 を区別する必要が無い。よって Type 1 の block $\{(0, a_1), (0, a_2), (1, b_1), (1, b_2)\}$ を、$\{a_1, a_2; b_1, b_2\}$ と略記し、Type 2 の block $\{(0, a_1), (0, a_2), (0, a_3), (1, b_1)\}$、$\{(1, a_1), (1, a_2), (1, a_3), (0, b_1)\}$ を、$\{a_1, a_2, a_3; b_1\}$ と略記する。また本報告では、Type 2 の base block は 1 つしか存在しないと仮定する。

さらに $\{0, 1, a\} = \{(x, 0), (x, 1), (x, a)\}$ を **pure triple** と呼び、$\{0, 1; b\} = \{(x, 0), (x, 1), (x + 1, b)\}$ を **mixed triple** と呼ぶ。ただし、$x \in \mathbf{Z}_2$ とする。

ここで、まず Hol($\mathbf{Z}_{2p}$)-invariant sSQS($2p$) が満たすべき条件・性質を補題の形で列挙する。

補題 1 Hol($\mathbf{Z}_{2p}$)-invariant SQS($2p$) は base block $\{0, 1, -1; 0\}$ を持つ。

補題 2 Type 1 の base block は $\{0, 1; \alpha, \beta\}$ となる。ただし α, β は、$2X^2 - 2X + 1 \equiv 0 \pmod p$ の解とする。

ここで $2X^2 - 2X + 1 \equiv 0 \pmod p$ が解を持つための条件は、$p \equiv 1 \pmod 4$ であり、SQS の存在条件と合わせて、$p \equiv 1, 5 \pmod{12}$ が得られる。

補題 3 $B=\{0,1,a;b\}$ を Type 2 の base block とするとき、次が成り立つ。

(i) $orb_G(B)$ には、pure triple $\{0,1,x\}$ が、$x=a,1-a,a^{-1},1-a^{-1},(1-a)^{-1},1-(1-a)^{-1}$ の 6 個存在する。

(ii) $orb_G(B)$ には、mixed triple $\{0,1;y\}$ が、$y=b,1-b,a^{-1}b,1-a^{-1}b,(1-a)^{-1}(1-b),(1-(1-a)^{-1})(1-a^{-1}b)$ の 6 個存在する。

このとき、pure triple の各 x が異なるための条件は次の通りである。

補題 4 補題 4 において、$a,1-a,a^{-1},1-a^{-1},(1-a)^{-1},1-(1-a)^{-1}$ がそれぞれ異なるためには、$a^2-a+1\not\equiv 0 \pmod p$ でなければならない。

$a^2-a+1\equiv 0 \pmod p$ は、$p\equiv 5 \pmod{12}$ では解を持たないが、$p\equiv 1 \pmod{12}$ では解を持つ。そのため、$p\equiv 1 \pmod{12}$ では次の補題の base block を補わなければならない。

補題 5 $p\equiv 1 \pmod{12}$ のとき、$\mathrm{Hol}(\mathbf{Z}_{2p})$-invariant sSQS($2p$) は、$(0,1,\gamma;(\delta+1)^{-1})$ を特殊な base block として持つ。ただし γ,δ は、$X^2-X+1\equiv 0 \pmod p$ の解とする。

これらの補題に注意して、$\mathrm{Hol}(\mathbf{Z}_{2p})$-invariant sSQS($2p$) を計算機によって求めたところ、$p=13$ を除く $p<200$ の素数 (ただし、$p\equiv 1,5 \pmod{12}$) で $\mathrm{Hol}(\mathbf{Z}_{2p})$-invariant sSQS($2p$) が構成出来た。

定理 6 $\mathrm{Hol}(\mathbf{Z}_{2p})$-invariant sSQS($2p$) ($p$ は素数、$p\equiv 1,5 \pmod{12}$) は、
$p=5,17,29,37,41,53,61,73,89,97,101,109,113,137,149,157,173,181,193,197$ に対して存在する。

$p>200$ の素数については、このような SQS を得るためには計算の高速化をはかる必要があり、また理論的に $\mathrm{Hol}(\mathbf{Z}_{2p})$-invariant sSQS($2p$) の構成を見いだすのも今後の課題である。

参考文献

[1] E. Köhler. Zyklische Quadrupelsysteme. *Abh. Math. Sem. Univ. Hambrug*, **48**, 1-24, 1978.

[2] H. Siemon. Some remarks on the construction of cyclic Steiner Quaduple Systems. *Arch. Math.*, **49**, 166-178, 1987.

[3] H. Siemon. Infinite families of strictly cyclic Steiner quadruple systems. *Discrete Math.*, **77**, 307-316, 1989.

[4] H. Siemon. On the existence of cyclic Steiner quadruple systems SQS($2p$). *Discrete Math.*, **97**, 377-385, 1991.

[5] H. Siemon. Cyclic Steiner quadruple systems and Köhler's orbit graphs. *Designs, Codes and Cryptography*, **1**, 121-132, 1991.

[6] H. Siemon. A number theoretic conjecture and the existence of S-cyclic Steiner quadruple systems. *Designs, Codes, and Cryptography*, **13**, 63-94, 1998.

[7] S. Bitan and T. Etzion. The last packing number of quadruples, and cyclic SQS. *Designs, Codes, and Cryptography*, **3**, 283-313, 1993.

[8] W. Chu and C.J. Colbourn. Recursive constructions for optimal (n, 4, 2)-OOCs. *JCD*, **12**, 333-345, 2004.

[9] T. Feng, Y. Chang and L. Ji. Constructions for strictly cyclic 3-designs and applications to optimal OOCs with $\lambda=2$. *JCT*, to appear 2008.

Translation-free Steiner systems and their application

Yuichiro Fujiwara
Graduate School of System and Information Engineering
University of Tsukuba

A *Steiner t-design* of *order* v, briefly $S(t,k,v)$, 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 k-element subsets of V called *blocks*, such that each t-tuple of distinct elements of V is contained in exactly one block of $\mathcal{B}$. An $S(2,3,v)$ is often called a *Steiner triple system* and referred to as an STS(v). For the sake of simplicity, we assume that V is the set of positive integers less than or equal to v.

A Steiner t-design $(V,\mathcal{B})$ on the point set V is said to have a *translation-free* expression over $\boldsymbol{Z}_w$ if for any block $B=\{a,b,\ldots,c\}\in\mathcal{B}$ and any $i\in V$ it holds that $B+i=\{a+i,b+i,\ldots,c+i\}\in\mathcal{B}$, where all elements in k-tuples are taken modulo w. When $w\geq 2v$, we say that the $S(t,k,v)$ has a translation-free expression over N. In what follows, we simply say that a Steiner t-design is translation-free if it has a translation-free expression.

This special property of Steiner systems stems from synthesis of X-tolerant convolutional compactors, in which translation freeness guarantees better error detection ability and higher X-tolerance for BIST (Built-in self-test) than trasitional methods (See Fujiwara and Colbourn [1], Mitra and Kim [2], and Rajsky and Tyszer [3]).

We focus on excistence of translation-freene $S(t,k,v)$ over N or $\boldsymbol{Z}_w$ for $w\geq v$. By employing a simple probabilistic methods, we asymptotically solved the case $k\geq 5$:

Theorem 1 *Let k be an integer greater than or equal to five. Then for every sufficiently large admissible order v there exists a translation-free $S(2,k,v)$ over $\boldsymbol{Z}_v$.*

It appears to be difficult to settle the case when the block size k is small. Among other results, we have so far obtained the following recursive construction:

Theorem 2 *If there exist a translation-free* STS$(v-1)$ *over* N *or* $\boldsymbol{Z}_v$ *and a translation-free* STS$(w-1)$ *over* $\boldsymbol{Z}_w$*, then there exists a translation-free* STS$(vw-1)$ *over* N *or* $\boldsymbol{Z}_{vw}$*, respectively.*

By using the trivial Steiner triple system of order 3, we have a doubling construction:

Corollary 3 *If there exist a translation-free* STS$(v-1)$ *over* N *or* $\boldsymbol{Z}_v$*, then there exists a translation-free* STS$(2v-1)$ *over* N *or* $\boldsymbol{Z}_{2v}$ *respectively.*

Infinitely many translatin-free Steiner systems can be obtained from other techniques such as trancation of larger Steriner systems having particular automorphisms. Not a few sporadic examples can be found with the aid of computers. We do not know, however, the complete spectrum of orders for which a translation-free $S(2,k,v)$ exits.

References

[1] Y. Fujiwara, C. J. Colbourn, X-tolerant compaction circuits: A combinatorial approach, submitted to IEEE Trans. inform. Theory.

[2] S. Mitra, K. S. Kim, X-compact: An efficient response compaction technique, IEEE Trans. Comput. Des. **23** (2004) 421–432.

[3] J. Rajsky, J. Tyszer, Synthesis of X-tolerant convolutional compactors, Proc. 23rd IEEE VLSI Test Symposium 1, May 5 (2005), 114–119.

Perfect Hash Families
– Strength Three with Three Rows –

筑波大学　システム情報工学研究科　藤原　良
筑波大学　システム情報工学研究科　藤原　祐一郎
筑波大学　システム情報工学研究科　繆　いん

1 Introduction

Perfect Hash Family (PHF) とはサイズ k の定義域 A からサイズ v の値域 B への関数の集まり $\mathcal{H}$, $|\mathcal{H}| = N$, で, 次の条件を満たさなければならない.

- サイズが t の任意の A の部分集合 X に対し，$\mathcal{H}$ の中に X で制限されたとき $(h|_X)$ 単射になるような関数 $h \in \mathcal{H}$ が少なくとも 1 つ存在する.

この関数の集合 $\mathcal{H}$ を Perfect Hash Family と呼び，$PHF(N; k, v, t)$ と書く．列を定義域 A に，行を $\mathcal{H}$ の関数に，配列要素を関数の値に対応させて，N　v の配列に表現することが出来る.
例　$PHF(3; 12, 4, 2)$,　$h_i : \mathbb{Z}_{12} \to \mathbb{Z}_4$

$\mathbb{Z}_{12}$	0	1	2	3	4	5	6	7	8	9	10	11
h_1	0	0	0	1	1	1	2	2	2	3	3	3
h_2	3	0	2	1	2	3	1	0	3	2	0	1
h_3	2	1	3	0	2	1	1	2	3	0	0	3

この問題は 1980 年代初頭に，K. Mehlhorn[3] や M. L. Fredman and J. Komlos[2] や　N. Alon などによって提案された問題であるが，１０年ほど前から暗号，グループ・テスト，放送キー問題などへの応用が次々発見され，PHF の構成問題に再び脚光があたってきた．特に最近 Walker II and Colbourn[1] で，多くの構成法が提案された.

2 Bound

$PHF(N;, k, v, t)$ が存在する，最小の N を $PHFN(k, v, t)$ と書く．$t = 2$ の場合は自明なので，$t \geq 3$ に対して　K. Mehlhorn(1982)[3] によって次の上界が与えられている.

$$PHFN(k, v, t) \geq \frac{\log k}{\log v}$$

Fredman and Komlos(1984)[2] によって，少し改良されたが，基本的にはこの大きさである．N を固定した場合には　$k \leq v^N$ となる.

3 構成

関数 $h \in \mathcal{H}$ の定義域をポイント集合 V とし，ブロック集合 $\mathcal{B}$ を

$$\mathcal{B} = \{B_{i,b} \mid 1 \leq i \leq |\mathcal{H}|,\ b \in B\},\quad B_{i,b} = \{a \mid h_i(a) = b\}$$

と定義する.　但し，$h_i : A \to B$　とする.　このように点とブロックからなるシステムと見ると，次のような条件を満たすシステムと同値となる.

1. 有限集合 V とその部分集合の集まり $\mathcal{B}$ からなる．

2. $\mathcal{B}$ は分割され，その各クラス (平行類) は V を分割している

3. A の任意の t-部分集合 X に対し，その t 個の点が異なるブロックに含まれている平行類が少なくとも一つある．

このシステムを t-Separating Resolvable Block Design (t-SRBD) と呼んでいる．次に，$t = 3$ で関数の数が $N = 3$ の場合を考えよう，この場合が非自明な最も小さなケースである．定義域のサイズの上界は　$k \leq v^3$ であるが，このバウンドはかなり非現実的でこの上界に近い FHS は発見されていない．

定理 3.1　3 クラスの *3-SRBD* になるための必要十分条件は，X に対して 3 つの *secant* ブロックが存在するような定義域の部分集合 X は存在しない.

X に対する secant ブロック とは　A の部分集合 X と 2 点以上で交わるブロックのことである．この条件を満たすデザインを PG$(4, q)$ 上の Quadrics と PG$(3, q^2)$ 上のエルミット多様体を使って構成する．まず PG$(4, q)$ 上の Quadrics, Q(4,q) は，PG$(4, q)$ 上の点を $P = (x_0, x_1, x_2, x_3, x_4), x_i \in GF(q)$ と表現したとき，

$$x_0^2 + x_1x_2 + x_3x_4 = 0$$

の標準形で表せる．この式を満たす点は $(q^2 + 1)(q + 1)$, 直線は $(q^2 + 1)(q + 1)$ 本存在する．そして直線上に $q + 1$ 点，各点に $q + 1$ 直線が結合する構造を持ち，直線が 3 角形を作ることはない．この Q(4,q) に平行類が存在しなければならないが，互いに交わらない直線の最大数は，Q(4,3) の場合，計算の結果最大 7 しかない（平行類には 10 本必要）．そこで Q(4,q) の双対系, $Q(4, q)^*$, を考えると次の結果が得られた．

定理 3.2 任意の素数べキ q, $q \geq 3$ に対して，　*PHF(*$3, q^2(q + 1), q^2, 3$ *)* が存在する．

この結果は $q = 3, 4$ の場合には現在発見されているものよりは大きい定義域のサイズ k を与えるが，それ以上の q に対しては現存サイズを超えない．
次に PG$(3, q^2)$ 上のエルミット多様体，　$H(3, q^2)$，を使った構成法を考える．$H(3, q^2)$ は

$$x_0^{q+1} + x_1^{q+1} + x_2^{q+1} + x_3^{q+1} = 0$$

の形の標準形で表現できる．そして $(q^2+1)(q^3+1)$ 個の点と $(q+1)(q^3+1)$ 本の直線からなる．この $H(3, q^2)$ から次の PHF が構成できる．

定理 3.3 任意の素数べキ q に対して，*PHF(*$3 : q^5, q^3, 3$*)* が存在する．

この構成法は現在発見されている同パラメータでは最も定義域のサイズが大きい．

参考文献

[1] R.A.Walker II and C.J.Colbourn , Perfect Hash Families: Constructions and Existence, J. of Math, Crypto. (2007)

[2] M. L. Fredman and J. Komlos, On the size of separating systems and families of pegect hash functions, SIAM J. Algebraic Discrete Methods 5 (1984), 61-68.

[3] K. Mehlhorn, “On the program size of perfect and universal hash functions,” Proc. 23rd Annual IEEE Symposium on Foundations of Computer Science, 1982, pp. 170-175.