「実験計画法およびその周辺領域における組合せ構造の解明とその応用」に関する研究報告

栗木　進二 (大阪府大院・工学研究科)

1. 研究目的

本研究は, 実験計画法およびその周辺領域 (組合せ論, 符号理論, 暗号理論, 乱数等) における組合せ構造の最新の話題に関する研究発表および情報交換を行い, 今後の研究の方向性を様々な観点から見いだすことを目的とした.

2. 研究計画

本研究は, 平成 22 年度に下記シンポジウムを開催し, 関連する研究者が, 統計的計画の最適性, 存在性, 構成法に関する話題, その周辺領域における組合せ構造に関する話題, 通信工学等への応用に関する話題, また, 最新の話題や研究の紹介, 新たな問題の提起などを行うことにより遂行された.

シンポジウム： 実験計画法およびその周辺領域における組合せ構造の解明とその応用
研究分担者　： 栗木　進二 (大阪府大・工学研究科)
期　　日　： 平成 22 年 11 月 29 日 (月) 〜 12 月 1 日 (水)
参 加 人 数　： 38 名
場　　所　： 城崎大会議館 (兵庫県豊岡市城崎町湯島 1062)

3. 研究成果

本シンポジウムにおいては, 上記の目的に沿った 23 件の報告が行われ, 各報告に対して活発な議論がなされた. 講演題目・講演者・講演内容は次のとおりである.

1. 「Special integral and minimal cubature formula」
   澤 正憲 (名古屋大院)：Cubature formula の紹介, およびある最適性をもつ cubature formula に関する最近のいくつかの結果

2. 「円対称性を持つ積分に対する最小求積公式について」
   平尾 将剛 (名古屋大院)：円対称性を持つ積分に対する最小求積公式が存在するための解析的な必要条件の紹介

3. 「射影ド・ブライン原始多項式の存在性について」
   萩田 真理子 (お茶の水大・情報)：射影ド・ブライン原始多項式の存在と最適な誤り訂正符号系列の関係, および射影ド・ブライン原始多項式が存在しないパラメータに関する結果

4. 「Conflict-avoiding codes of weight three」
   Hung-Lin FU (National Chiao Tung Univ., Taiwan)：重み 3 の conflict avoiding code の存在性と構成についてのサーベイと今後の展望

5. 「Balanced (C_5, C_{12})-foil designs and related designs」
   潮 和彦 (近畿大)：均衡型 (C_5, C_{12})-Foil Designs, 均衡型 C_{17}-Foil Designs, 均衡型 (C_{10}, C_{24})-Foil Designs, 均衡型 C_{34}-Foil Designs の構成と存在性

6. 「Recursive constructions of t-SEEDs related to quantum jump codes」
   林 怡伶, 神保 雅一 (名古屋大院)：量子ジャンプ符号の分野で導入された t-SEED の逐次構成法

7. 「アフィン幾何からできるデザインの分解について」
   長谷川 潤 (名古屋大院), 籾原 幸二 (筑波大院), 三嶋 美和子 (岐阜大), 神保 雅一 (名古屋大院)：AG$(2n, 3)$ の平面からできるデザインの部分デザインへの分解

8. 「標数 p^2 のガロア環から得られる差集合族と関連する指標和」
   籾原 幸二 (筑波大院), 山田 美枝子 (金沢大)：ガロア環のヤコビ和の計算による標数 4 のガロア環の単数群上のある分割型差集合族の存在性の決定

9. 「The existence of almost difference families」
Xun WANG (筑波大院)：$k = 4, 5, 6$ の (q, k, λ, t)-almost 差集合族の構成法

10. 「The existence of n-sun systems」
Chin-Mei Kau FU (Tamkang Univ., Taiwan)：n-Sun system と呼ばれるグラフによる完全グラフのグラフ分解の存在性

11. 「A counter-example of Delsarte-Seidel's conjecture on tight Euclidean design」
周 園媛 (名古屋大院)：Tight Euclidean design の新たな例の紹介, および Delsarte-Seidel による tight Euclidean design の存在性予想に対する反証

12. 「s 距離集合と Larman-Rogers-Seidel の定理の一般化」
野崎 寛 (東北大院)：ユークリッド空間上の s 距離集合に対する Larman-Rogers-Seidel の定理の拡張

13. 「低い次元の距離集合の有限性について」
篠原 雅史 (鈴鹿高専)：直線上, および円周上の距離集合の有限・無限の境界

14. 「Optimal fractional factorials under a baseline parametrization」
Rahul MUKERJEE* (Indian Institute of Management Calcutta, India), Boxin TANG (Simon Fraser Univ., Canada)：Optimal two-level factorial fractions under a nonorthogonal baseline parametrization

15. 「On optimal ternary linear codes」
丸田 辰哉 (大阪府大院)：次元 6 の新しい 3 元線形符号の構成方法, およびその他の最新結果

16. 「最適な separable code の構成」
程 民権 (筑波大院), 季 利均 (蘇州大, 中国), 繆 瑩 (筑波大院)：射影平面や差行列などによる長さ 2 及び 3 の最適な $\bar{2}$-分離可能符号の構成

17. 「Existence of affine α-resolvable PBIB designs with some constructions」
門脇 聖 (松江高専), 景山 三平 (広島工大)：2-アソシエートである affine α-分解可能 PBIB デザインの存在性に関する研究成果の報告

18. 「Graham-Winkler によるグラフの等長埋め込み問題とその一般化」
渡部 里織 (名古屋大)：グラフの等長埋め込み問題の観点からの完全グラフの完全多部グラフ分解問題の考察

19. 「Characterization of partially balanced fractional $2^{m_1+m_2}$ factorial designs of resolution $R(\{00, 10, 01, 11\})$」
弓場 弘 (国際自然研), 兵頭 義史 (岡山理科大), クワ田 正秀 (国際自然研)：Simple partially balanced array が, 一般平均, すべての主効果, 二因子交互作用が推定可能な partially balanced fractional $2^{m_1+m_2}$ factorial design となるための必要十分条件

20. 「Characterization of balanced fractional 3^m factorial designs of resolution III」
弓場 弘 (国際自然研), 兵頭 義史 (岡山理科大)：3 シンボル単純配列から導かれる分解能 III の釣合い型一部実施 3^m 要因計画の特徴づけ

21. 「Cyclic design を用いた分割型ユニットをもつ 2 因子実験の構成法」
田口 和規, 栗木 進二 (大阪府大院)：Cyclic design を用いた分割型ユニットをもつ 2 因子実験の構成法とその stratum efficiency factor

22. 「スペクトル拡散通信における同期の問題」
堀田 祐未, 栗木 進二 (大阪府大院)：スペクトル拡散通信におけるプレフィクスコンマフリーを用いた同期の研究

23. 「Mutually M-intersecting K-arcs と光直交符号への応用」
宮本 暢子 (東京理科大), 篠原 聡 (明星大)：有限射影平面上における mutually M-intersecting (K, D)-arcs という集合の構成法, およびそれらと可変重み光直交符号との関係

Cubature formula for some special integral

Masanori Sawa
Graduate School of Information Science, Nagoya University

A main problem of numerical integration is to approximate the integral

$$\int_{\Omega} f(x)d\mu.$$

Here x is an n-dimensional coordinate vector and μ is a probabilistic measure on a domain Ω in $\mathbb{R}^n$. We assume Ω and μ are both invariant under the orthogonal group of degree n. Such a region and a measure define a *spherically symmetric integral*; for instance the Gaussian integral belongs to this class of integral. We shall seek for an approximant by taking a linear combination of the function values of f at specified points $x_1, \cdots, x_N$, namely,

$$\sum_{i=1}^{N} w_i f(x_i). \tag{1}$$

We call (1) a *cubature formula*. The values w_i are the *weights* and x_i are the *points* of a cubature formula. To each formula we assign the set of functions for which it is exact. Most often this set is the space of all polynomials of degree no more than t: In this case a cubature formula is said to be of *degree* t. We refer the readers to the comprehensive monograph [6] for the basic theory of cubature formula.

We require a cubature formula with small number of points to reduce the computational cost. It is well known that the number of points X in a cubature formula of degree t is bounded from below as follows:

$$|X| \geq \dim \mathcal{P}_{[t/2]}. \tag{2}$$

Here $\mathcal{P}_\ell$ is the space of polynomials of total degree at most ℓ. Researchers in combinatorics and statistics usually call (2) *Fisher-type bound*, since it can be obtained essentially by the same way as in Fisher's inequality for the number of blocks in BIB designs. Möller [5] improved (2) for the odd degree case. Namely, he gave the following lower bound for a cubature formula of degree $2k+1$ X:

$$|X| \geq \begin{cases} 2\dim \mathcal{P}_k^* - 1 & \text{if } k \text{ is even and } 0 \in X, \\ 2\dim \mathcal{P}_k^* & \text{otherwise,} \end{cases} \tag{3}$$

where $\mathcal{P}_k^*$ is the space of even polynomials or odd polynomials of total degree at most k according to whether k is even or odd. A cubature formula is *minimal* if the equality holds in one of the above bounds.

In the two-dimensional case there are many literatures where minimal formulae were actually found; see, e.g., [8]. In higher dimensional cases, however, only a few minimal formulae have been found so far: Those examples are of small degrees as well as in low dimensional spaces. It seems to be the conventional belief that there exists no minimal formula of degree t for a d-dimensional spherically symmetric integral for any $t \geq 5$ and $d \geq 3$ with some possible exceptional examples. Part of the belief is supported by a famous theorem of Taylor [7]. Namely, he proved that there exists no minimal formula of even degree for the uniform measure on the $(d-1)$-dimensional unit sphere, using a celebrated theorem

of Bannai and Damerell [1] on the nonexistence of tight spherical designs. There are some recent papers involving the degree $4, 5, 7, 9$ cases, however as far as we know, very little is known on the existence and nonexistence of minimal formulae of degree at least 10 except for Taylor's theorem.

The aim of this talk is to let more and more researchers know the concept of cubature formula which has been extensively studied in various areas of mathematics; see for example [2, 4]. To do so, we explain basic facts and theories of cubature formula. We also give some new results on the structure and the existence of minimal formula of degree $4k+1$ for spherically symmetric integral.

Theorem 1 (Hirao-Nozaki-S.-Vatchev, 2010). Let d, k be positive integers such that $k \geq 2$ and $d \geq \lceil (4k^2 - 4k + 3 + (2k-1)\sqrt{4k^2+12k+1})/2 \rceil$. Assume there exists a d-dimensional minimal formula of degree $4k+1$ for spherically symmetric integral with points X. Then there exists a layer of X over which inner products between pairs of the points are rational numbers, where a layer of X is the intersection of X and some concentric sphere.

The proof uses a famous theorem in geometry called the Larman-Rogers-Seidel theorem [3] which mentions the rationality of the inner products of given points.

Theorem 2 (Hirao-Nozaki-S.-Vatchev, 2010). Let $k = 3, 4, 5, 6$ and $d \geq 2$ be an integer. Then there exists some spherically symmetric integral which does not admit d-dimensional minimal formula of degree $4k+1$.

References

[1] Bannai, Ei., Damerell, R. M.: *Tight spherical designs, II.* J. London Math. Soc., **21**, 13–30 (1980).

[2] Cohn H., Kumar, A.: *Universally optimal distribution of points on spheres.* J. Amer. Math. Soc., **20**, 99–148 (2007).

[3] Larman, D. G., Rogers, C. A., Seidel, J. J.: *On two-distance sets in Euclidean space.* Bull. London Math. Soc., **9**, 261–267 (1977).

[4] Lyons, L., Victoir, V.: *Cubature on Wiener space, Stochastic analysis with applications mathematical finance.* Proc. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. **460**, 169–198 (2004).

[5] Möller, H. M.: *Lower bounds for the number of nodes in cubature formulae.* Numerische Integration (Tagung, Math. Forschungsinst., Oberwolfach, 1978), pp. 221–230, Internat. Ser. Numer. Math., **45**, Birkhäuser, Basel-Boston, Mass., 1979.

[6] Sobolev, S. L., Vaskevich, V. L.: *The Theory of Cubature Formulas.* Mathematics and its Applications, 415. Kluwer Academic Publishers Group, Dordrecht, 1997.

[7] Taylor, M.: *Cubature for the sphere and the discrete spherical harmonic transform.* SIAM J. Numer. Anal., **32**, 667–670 (1995).

[8] Xu, Y.: *Minimal cubature formulae for a family of radial weight functions.* Adv. Comput. Math., **8**, 367–380 (1998).

On minimal cubature formulas for circularly symmetric integrals

名古屋大学大学院情報科学研究科　平尾　将剛
名古屋大学大学院情報科学研究科　澤　正憲

Ω を $\mathbb{R}^2$ 上の回転不変な領域, ω を Ω 上で定義された回転不変な重み関数とし, 積分

$$\mathcal{I}[f] = \frac{1}{V(\Omega)} \int_\Omega f(\mathbf{x})\omega(\|\mathbf{x}\|)d\mathbf{x}, \quad V(\Omega) = \int_\Omega w(\|\mathbf{x}\|)d\mathbf{x}$$

を考える．このような積分には, $\mathbb{R}^2$ 上のガウス重み関数 $e^{-\|\mathbf{x}\|^2}$ や単位円盤上のヤコビ重み関数 $(1-\|\mathbf{x}\|^2)^{1/2}$ のような確率論，統計学などに頻繁に現れるものが含まれる．X を $\mathbb{R}^2$ 上の有限集合，λ を X 上の正値関数とする．t 次までの任意の多項式 f に対して，

$$\mathcal{I}[f] = \sum_{\mathbf{x}\in X} \lambda(\mathbf{x})f(\mathbf{x})$$

が成り立つとき，重み付き集合 (X,λ) は $\mathcal{I}$ に対する t 次の cubature formula (以下, CF と省略) をなすという．CF は数値解析や離散幾何をはじめとする多くの分野で研究されている．主要な研究テーマとして存在問題や構成法，またそれらの応用などがある．中でも存在問題は基本的なものである．Tchakaloff (1957) は点の個数が十分大であれば CF は存在することを示した．また CF が存在するための点の個数の下界については次の代数的評価式が知られている．

定理 1 (Radon (1949), Möller (1979))**.** (X,λ) が $\mathcal{I}$ に対する t 次の CF をなすならば,

$$|X| \geq \begin{cases} \frac{1}{2}(e+1)(e+2) & t=2e \text{ のとき}, \\ \frac{1}{2}(e+1)(e+2)+\lfloor\frac{e+1}{2}\rfloor & t=2e+1 \text{ のとき}. \end{cases} \tag{1}$$

上の評価式において等号を達成する CF を最小 (minimal) であるという．

任意の積分 $\mathcal{I}$ に対して最小 CF が常に存在するとは限らない．しかしながら, Xu により次のような最小 CF を持つ積分が与えられた．

定理 2 ([4])**.** 自然数 e を一つ固定する．このとき, 領域と重み関数がそれぞれ

$$\Omega = \{\mathbf{x}\in\mathbb{R}^2 \| 1 \leq \|\mathbf{x}\| < \infty\}, \quad w_e(\|x\|) = \frac{\sqrt{\|\mathbf{x}\|^2-1}}{\|\mathbf{x}\|^{2e+4}},$$

である積分に対して, $2e-1, 2e$ 次の最小 CF が存在する．

この定理を受け, 我々は他にどのような積分が最小 CF を持つかを示したい．これは次で定義する Euclidean tight design の分類問題として捉えることも出来る: 重み付き有限集合 (X,λ) に対して, 動径集合を $\{\|\mathbf{x}\|^2 \mid R_1 > R_2 > \ldots R_p \geq 0\}$ する．$S_i = \{\mathbf{x}\in\mathbb{R}^2 \mid \|\mathbf{x}\|^2 = R_i\}$, $X_i = X\cap S_i$, $\Lambda_i = \sum_{\mathbf{x}\in X_i}\lambda(\mathbf{x})$ とする．このとき, t 次までの任意の多項式 f に対して,

$$\sum_{i=1}^{p} \Lambda_i \int_{S_i} f(\mathbf{x})d\rho_i(\mathbf{x}) = \sum_{\mathbf{x}\in X}\lambda(\mathbf{x})f(\mathbf{x}),$$

が成り立つとき, 重み付き有限集合 (X,λ) を Euclidean t-design であるという．さらに点の個数が (1) の等号を達成する Euclidean design を tight であるという．

積分 $\mathcal{I}$ に対する t 次の CF は Euclidean t-design であることが知られている．さらに任意の t に対して, Euclidean tight t-design は常に存在する (Bajnok(2005))．したがって, どのような積分に対して最小 CF が存在するかが問題となる:

問題. (X,λ) を Euclidean tight t-design とし, $\mathcal{I}$ をある円対称性を持つ積分とする．このとき, (X,λ) は $\mathcal{I}$ に対する t 次の最小 CF であるか?

我々はこの問題に対して, Euclidean tight design をなす点は p 個のある正多角形上に配置されること ([1]) と Cools-Schmid(1993) での証明のアイデアを組み合わせることにより，最小 CF が存在するための必要条件を直交多項式の因数分解の条件として得た. 以下，簡単のためにガウス積分に対する $t=4k+3$ の場合について主張を記述する.

定理 3. ([3]). $L_k^j(t)$ をパラメータ j の k 次 Laguerre 多項式とする．ガウス積分に関する $4k+3$ 次の最小 CF が存在し，かつその CF の点は $k+1$ 個の円上に配置されると仮定する. このとき，次の (i), (ii) が成り立つ.

(i) ある実数 γ_1,γ_2 が存在して $L_{k+1}^0(t)$ は次のように分解される:

$$\begin{cases} \frac{1}{\binom{2j+1}{j}} L_j^{2j+2}(t)\Big(L_{j+1}^{2j+2}(t)+\gamma_1 L_j^{2j+2}(t)+\gamma_2 L_{j-1}^{2j+2}(t)\Big) & k=2j \text{ のとき,} \\ \frac{1}{\binom{2j+2}{j+1}}\Big(L_{j+1}^{2j+3}(t)+\gamma_1 L_j^{2j+3}(t)\Big)\Big(L_{j+1}^{2j+3}(t)+\gamma_2 L_j^{2j+3}(t)\Big) & k=2j+1 \text{ のとき.} \end{cases}$$

(ii) $\{R_1,\cdots,R_{k+1}\}$ は $L_{k+1}^0(t)$ の零点集合である.

条件 (i) より，$L_{k+1}^0(t)$ とその分解された多項式の間で各項の係数を比較することにより最小 CF の存在性を判定することができる．さらに条件 (i) が成り立つ k に対して条件 (ii) を適用することにより，最小 CF の存在性を判定ことができる.

ガウス積分に対して, 我々は次の最小 CF の存在に関する主張を得た.

定理 4 ([2, 3])**.** ガウス積分に対する t 次の最小 CF で点が $\lfloor t/4\rfloor+1$ 個の円上に配置されるならば, $t\le 5$ である.

References

[1] Bannai, Ei., Bannai, Etsu., Hirao, M., Sawa. M.: *Cubature formulas in numerical analysis and Euclidean tight designs*, European J. Combin. **31**, 423–442 (2010).

[2] Bannai, Ei., Bannai, Etsu., Hirao, M., Sawa. M.: *On the non-existence of minimal cubature formulas for Gaussian measure on $\mathbb{R}^2$ of degree t supported by $[\frac{t}{4}]+1$ circles*, submitted to European J. Combin..

[3] Hirao, M., Sawa, M.: *On minimal cubature formulae of odd degrees for circularly symmetric integrals*, to appear in Adv. Geom..

[4] Xu, Y.: *Minimal cubature formulae for a family of radial weight functions*, Adv. Comput. Math. **8**, 367–380 (1998).

射影ド・ブライン原始多項式の存在性について

お茶の水女子大学大学院　萩田真理子
東京大学大学院　松本眞

周期列で, その連続する部分列の集合が符号をなすものを誤り訂正符号系列という. 射影ド・ブライン系列を係数に持つ原始多項式を用いて m 系列を作ると良いパラメータをもつ誤り訂正符号系列が構成できることが知られているが, 多くのパラメータでそのような原始多項式が存在しないことを示した.

Definition 1 (誤り訂正符号系列) X 上の (N,k,d) 誤り訂正符号系列とは，周期 N の数列

$$a_0a_1a_2\cdots a_{N-1} \qquad a_i = a_{N+i}, \quad a_j \in X$$

で，その連続する k 個の元の集合

$$C := \{a_ia_{i+1}a_{i+2}\cdots a_{i+k-1} | i \in \{0,1,2,\cdots,N-1\}\}$$

の要素がすべて異なり，最小距離

$$d := \min_{0\le s<t\le N-1} \sum_{i=0}^{k-1} \delta(a_{i+s}, a_{i+t}) \text{ ただし } \delta(x,y) = \begin{cases} 1 & (x \neq y) \\ 0 & (x = y) \end{cases}$$

の誤り訂正符号をなすものをいう.

Definition 2 (M 系列) F_q 上の n 次の M 系列とは，原始多項式

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0$$

の係数を用いて作られる漸化式

$$x_{n+i} + a_{n-1}x_{n+i-1} + \cdots + a_0x_i = 0$$

で生成される，周期 q^n-1 の数列 $(x_n) = x_0x_1x_2\cdots$ である.

M 系列は，周期 q^n-1 で，連続する n 個を見たときの最小距離が 1 であるから，$(q^n-1, n, 1)$ 誤り訂正符号系列であるが, 任意の d について十分大きな s について連続する $n+s$ 項を考えれば, $(q^n-1, n+s, d)$ 誤り訂正符号系列でもある. なるべく小さな s で $d=3$ となるための原始多項式の条件を考える.

m 系列に現れる連続する $n+s$ 項は,

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} & 1 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & 1 & \cdots & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & 1 \end{pmatrix}$$

とすると，$A\boldsymbol{x} = 0$ を満たす，0 ベクトル以外のベクトル$\boldsymbol{x}$の全体である.$d \ge 3$ にするためには，行列 A のどの 2 つの列も線型独立でなくてはならない. 線型独立な列の個数は高々 $\dfrac{q^n-1}{q-1}$ 個であるから，s が最も小さくなるのは，$n+s = \dfrac{q^n-1}{q-1}$ のときとわかる.

Definition 3 (射影ド・ブライン系列) s 次の射影ド・ブライン系列とは，$\mathbb{F}_q$ 上の周期 $\dfrac{q^n-1}{q-1}$ の数列で，連続する s 個を見ると，周期の中で全て *0* の列以外のどのパターンもちょうど *1* 回ずつ出ている数列である. だたし, $(x_1x_2\cdots x_s) = k(x_1x_2\cdots x_s)$

射影ド・ブライン系列の存在条件について, 参考文献 [1] で次の 2 つの定理を証明し, その期待値から以下の 2 つの予想を紹介した.

Theorem 1 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ を $\mathbb{F}_q$ 上の射影ド・ブライン系列を係数に持つ多項式とする. この $f(x)$ から M 系列を作ると，$(q^n-1, n+s, 3)$ 誤り訂正符号系列となる.

Theorem 2 (射影ド・ブライン系列の個数) $\mathbb{F}_q$ 上の s 次の射影ド・ブライン系列の個数は

$$\frac{(q!)^{\frac{q^{s-1}-1}{q-1}}}{q^{s-1}}$$

個である.

Conjecture 1 $\mathbb{F}_q (q \geq 3)$ 上の射影ド・ブライン系列を係数に持つ多項式の中には，原始既約であるものが存在する.

この予想が成り立てば，次の予想も成り立つ.

Conjecture 2 *Conjecture1* が正しければ，　$\frac{q^m-1}{q-1}, q^{\frac{q^m-1}{q-1}-m}-1, 3$　誤り訂正符号系列が存在する.

$\mathbb{F}_2$ 上ではこの予想は成り立たず，$(2^{2^n-n-1}-1, 2^n-2, 3)$ 誤り訂正符号系列が存在すると予想されている.

$\mathbb{F}_3$ 上の 3 次と 4 次の射影ド・ブライン原始多項式の存在性については計算機実験（佐藤春菜・お茶の水女子大学大学院）により以下が示されている.

	3 次 (10 次式)	4 次 (36 次式)
ProjectiveDeBruijn の個数 (調べた個数)	144 (144)	6510819 (2000)
既約多項式の個数	12	65
原始多項式の個数	0	29
モニックで定数項 $\neq 0$ の多項式の総数	39366	1.00×10^{17}
原始多項式の総数	2640	1.19×10^{15}

3 次の Projective DeBruijn 系列では原始多項式は存在せず, Conjecture1 の反例となる結果となっている．4 次の結果から,「一般の多項式の中の原始多項式の割合」と「Projective DeBruijn 系列から作った多項式の中の原始多項式の割合」を比較してみると，以下のようになる.

$$\frac{\mathbb{F}_3\text{上 } 36 \text{ 次の原始多項式の個数}}{\mathbb{F}_3\text{上 } 36 \text{ 次の多項式の個数}} = \frac{\phi(3^{36}-1)/36}{2 \cdot 3^{35}} = 0.00399\cdots$$

$$\text{(原始多項式)/(Projective DeBruijn 系列から作った多項式)}=\frac{29}{2000} = 0.0145$$

このように，Projective DeBruijn 系列から作った多項式の方が原始多項式の割合が高いと期待できる結果となった．Projective DeBruijn 系列から作った多項式の方がランダムに係数を選んだ多項式よりも原始多項式になりやすいと仮定すると，Projective DeBruijn 系列を係数とする原始多項式の個数の期待値は,

$$(\mathbb{F}_q \text{ 上 } s \text{ 次の Projective DeBruijn 系列の個数}) \times \frac{\mathbb{F}_q\text{上 } n \text{ 次の原始多項式の個数}}{\mathbb{F}_q\text{上 } n \text{ 次の多項式の個数}}$$

$$= \frac{(q!)^{\frac{q^{s-1}-1}{q-1}}}{q^{s-1}} \cdot \frac{\phi(q^n-1)/n}{(q-1)q^{n-1}}, \quad \text{ただし } n = \frac{q^s-1}{q-1} - s$$

個以上となる．これらのことから, $q = 3$ の 3 次 $(s = 3, n = 10)$ 以外では存在すると期待されていたが, 奇数次数や $q > 3$ では存在できないことがわかった.

Theorem 3 射影ド・ブライン系列を係数とする多項式は $\mathbb{F}_3$ 上偶数次の場合を除いて原始多項式ではない.

本研究は科学研究費補助金 19204002（基盤研究（A）研究代表者　松本眞），20740051（若手研究（B）研究代表者　萩田真理子）の補助を受けて行われました.

参考文献

[1] Mariko Hagita, Makoto Matsumoto, Fumio Natsu, Yuki Ohtsuka: "Error Correcting Sequence and Projective De Bruijn Graph", Graphs and Combinatorics(2008)24:185-194

Optimal Conflict Avoiding Codes of Weight three

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

A conflict-avoiding code (CAC) of length n and weight k is defined as a set $C \subseteq \{0,1\}^n$ of binary vectors, called codewords, all of Hamming weight k such that the distance of arbitrary ***cyclic*** shifts of two distinct codewords in C is at least $2k - 2$. We denote the class of all the CACs of length n and weight k by CAC(n, k). Note that a code $C \in$ CAC(n, k) can be viewed as an (n, k, 1) optical orthogonal code without the autocorrelation property.

A code of maximum size (maximum number of codewords) is said to be optimal. We use M(n) = M(n,3) to denote the maximum size of a CAC of length n and weight 3. The following results are known so far.

Theorem 1 (Levenshtein and Tonchev, 2005)

If n ≡ 2 (mod 4), then M(n) = (n-2)/4. Furthermore, the optimal code obtained is an equi-difference (centered) code.

Theorem 2 (Jimbo et al., IEEE T. Information Theory 2007)

Let $n = 16m + 8$. The maximum size M(n) of a code $C \in$CAC(n) is (7n-8)/32 if m ≡ 1 (mod 2); (7n-24)/32 if m ≡ 0,2 (mod 6) and (7n+8)/32 if m ≡ 4 (mod 6).

Theorem 3 (Fu, Mishima and Uruno, DCC 2009)

The maximum size M(n) = M(16m) of a code in CAC(n) is M(n) = 7n/32 if m ≡ 0 (mod 2); (7n-16)/32 if m ≡ 1, 5 (mod 6); and (7n+16)/32 if m ≡ 3 (mod 6), with the exceptions M(48) = 10 and M (64) = 13.

Theorem 4 (Fu, Lin and Mishima, IEEE T. Information Theory 2010)

The maximum size M(n) = M(8n+4) of a code in CAC(n) is M(n) = (7n+4)/32 if m ≡ 0 (mod 4); (7n+12)/32 if m ≡ 1 (mod 12); (7n-12)/32 if m ≡ 2,6 (mod 12); (7n-4)/32 if m ≡ 3 (mod 4); (7n-20)/32 if m ≡ 5,9 (mod 12) and (7n+20)/32 if m ≡ 10 (mod 12).

Based on the above four theorems optimal conflict-avoiding codes of even length and weight 3 have been constructed successfully. So, it is left to consider the case when n is odd. In the direction of constructing these codes the following results are obtained though there is a long way to go.

Theorem 5 Let $G_c(n)$ denote the graph obtained from the set of differences $\{1, 2, \ldots, (n-1)/2\}$ with the edges correspond to centered codewords. Then $M(n) = [(n-1)/4]$ if G contains at most one odd cycle.

Theorem 6 Let $n = p^r$ where p is not a Wieferich prime. Then the maximum size of a conflict-avoiding code of length n is $(n - 1 - r \cdot O(p))/2$ where O(p) is the number of odd cycles in $G_c(n)$.

For general n, we can also obtain a formula by using the principle of inclusion and exclusion. But, it depends on the number of odd cycles in $G_c(p)$ where p is an odd prime.

References

1 M. Jimbo, M. Mishima, S. Janiszewski, A.Y. Teymorian, and V.D. Tonchev, On conflict-avoiding codes of length n = 4m for three active users, IEEE Trans. Inf. Theory, vol. 53, 2732 – 2742, Aug. 2007.

2 V.I. Levenshtein, Optimal conflict-avoiding codes for three active users, in Proc. IEEE Int. Symp. Inform. Theory, Adelaide, Australia, Sep. 2005, 535 – 537.

3 M. Mishima, H.-L Fu, and S. Uruno, Optimal conflict-avoiding codes of length n ≡ 0 (mod 16) and weight 3, Des, Codes Cryptogr., vol. 52, no. 3, 275 – 291, Sep. 2009.

4 K. Momihara, Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three, Des, Codes Cryptogr., vol. 45, no. 3, 379 – 390, Dec. 2007.

5 Hung-Lin Fu, Yi-Hean Lin, and Miwako Mishima, Optimal conflict-avoiding codes of even length and weight 3, IEEE Trans. Inf. Theory, vol. 56, 5747 - 5756, Nov. 2010.

Balanced (C_5, C_{12})-Foil Designs and Related Designs

Department of Informatics, Kinki University Ushio, Kazuhiko

In graph theory, the decomposition problem of graphs is a very important topic. Various type of decompositions of many graphs can be seen in the literature of gaph theory. This paper gives balanced (C_5, C_{12})-foil designs, balanced C_{17}-foil designs, balanced (C_{10}, C_{24})-foil designs, and balanced C_{34}-foil designs.

1. Balanced (C_5, C_{12})-Foil Designs

Let K_n denote *the complete graph* of n vertices. Let C_5 and C_{12} be *the* 5-*cycle* and *the* 12-*cycle*, respectively. *The* (C_5, C_{12})-$2t$-*foil* is a graph of t edge-disjoint C_5's and t edge-disjoint C_{12}'s with a common vertex and the common vertex is called *the center of the* (C_5, C_{12})-$2t$-*foil*. When K_n is decomposed into edge-disjoint sum of (C_5, C_{12})-$2t$-foils, we say that K_n *has a* (C_5, C_{12})-$2t$-*foil decomposition*. Moreover, when every vertex of K_n appears in the same number of (C_5, C_{12})-$2t$-foils, we say that K_n *has a balanced* (C_5, C_{12})-$2t$-*foil decomposition* and this number is called *the replication number*. This decomposition is to be known as *a balanced* (C_5, C_{12})-$2t$-*foil design*.

Theorem 1. K_n has a balanced (C_5, C_{12})-$2t$-foil decomposition if and only if $n \equiv 1 \pmod{34t}$.

Example 1.1. Balanced (C_5, C_{12})-2-foil decomposition of K_{35}.

$\{(35, 1, 16, 32, 14), (35, 5, 8, 18, 26, 13, 20, 11, 23, 21, 10, 4)\}$. (17 edges, 17 all lengths)

This starter comprises a balanced (C_5, C_{12})-2-foil decomposition of K_{35}.

Example 1.2. Balanced (C_5, C_{12})-4-foil decomposition of K_{69}.

$\{(69, 1, 30, 62, 28), (69, 9, 14, 34, 49, 24, 37, 61, 43, 40, 18, 7)\} \cup$

$\{(69, 2, 32, 63, 27), (69, 10, 16, 35, 51, 25, 39, 22, 45, 41, 20, 8)\}$. (34 edges, 34 all lengths)

This starter comprises a balanced (C_5, C_{12})-4-foil decomposition of K_{69}.

2. Balanced C_{17}-Foil Designs

Let K_n denote *the complete graph* of n vertices. Let C_{17} be *the* 17-*cycle*. *The* C_{17}-t-*foil* is a graph of t edge-disjoint C_{17}'s with a common vertex and the common vertex is called *the center of the* C_{17}-t-*foil*. When K_n is decomposed into edge-disjoint sum of C_{17}-t-foils, it is called that K_n *has a* C_{17}-t-*foil decomposition*. Moreover, when every vertex of K_n appears in the same number of C_{17}-t-foils, it is called that K_n *has a balanced* C_{17}-t-*foil decomposition* and this number is called *the replication number*. This decomposition is to be known as *a balanced* C_{17}-t-*foil design*.

Theorem 2. K_n has a balanced C_{17}-t-foil decomposition if and only if $n \equiv 1 \pmod{34t}$.

Example 2.1. Balanced C_{17}-decomposition of K_{35}.

$\{(35, 1, 16, 32, 14, 19, 5, 8, 18, 26, 13, 20, 11, 23, 21, 10, 4)\}$. (17 edges, 17 all lengths)

This stater comprises a balanced C_{17}-decomposition of K_{35}.

Example 2.2. Balanced C_{17}-2-foil decomposition of K_{69}.

$\{(69, 2, 32, 63, 27, 36, 9, 14, 34, 49, 24, 37, 61, 43, 40, 18, 7),$

$(69, 1, 30, 62, 28, 38, 10, 16, 35, 51, 25, 39, 22, 45, 41, 20, 8)\}$. (34 edges, 34 all lengths)

This stater comprises a balanced C_{17}-2-foil decomposition of K_{69}.

3. Balanced (C_{10}, C_{24})-Foil Designs

Let K_n denote *the complete graph* of n vertices. Let C_{10} and C_{24} be *the* 10-*cycle* and *the* 24-*cycle*, respectively. *The* (C_{10}, C_{24})-$2t$-*foil* is a graph of t edge-disjoint C_{10}'s and t edge-disjoint C_{24}'s with a common vertex and the common vertex is called *the center of the* (C_{10}, C_{24})-$2t$-*foil*. When K_n

is decomposed into edge-disjoint sum of (C_{10}, C_{24})-$2t$-foils, we say that K_n *has a* (C_{10}, C_{24})-$2t$-*foil decomposition*. Moreover, when every vertex of K_n appears in the same number of (C_{10}, C_{24})-$2t$-foils, we say that K_n *has a balanced* (C_{10}, C_{24})-$2t$-*foil decomposition* and this number is called *the replication number*. This decomposition is to be known as *a balanced* (C_{10}, C_{24})-$2t$-*foil design*.

Theorem 3. K_n has a balanced (C_{10}, C_{24})-$2t$-foil decomposition if and only if $n \equiv 1 \pmod{68t}$.

Example 3.1. Balanced (C_{10}, C_{24})-2-foil decomposition of K_{69}.

$\{(69, 1, 30, 62, 28, 55, 27, 63, 32, 2),$
$(69, 9, 14, 34, 49, 24, 37, 61, 43, 40, 18, 7, 15, 8, 20, 41, 45, 22, 39, 25, 51, 35, 16, 10)\}$.
(34 edges, 34 all lengths)
This starter comprises a balanced (C_{10}, C_{24})-2-foil decomposition of K_{69}.

Example 3.2. Balanced (C_{10}, C_{24})-4-foil decomposition of K_{137}.

$\{(137, 1, 58, 122, 56, 111, 55, 123, 60, 2), (137, 3, 62, 124, 54, 107, 53, 125, 64, 4)\} \quad \cup$
$\{(137, 17, 26, 66, 95, 46, 71, 119, 83, 78, 34, 13, 27, 14, 36, 79, 85, 120, 73, 47, 97, 67, 28, 18),$
$(137, 19, 30, 68, 99, 48, 75, 121, 87, 80, 38, 15, 31, 16, 40, 81, 89, 44, 77, 49, 101, 69, 32, 20)\}$.
(68 edges, 68 all lengths)
This starter comprises a balanced (C_{10}, C_{24})-4-foil decomposition of K_{137}.

4. Balanced C_{34}-Foil Designs

Let K_n denote *the complete graph* of n vertices. Let C_{34} be *the* 34-*cycle*. *The* C_{34}-t-*foil* is a graph of t edge-disjoint C_{34}'s with a common vertex and the common vertex is called *the center of the* C_{34}-t-*foil*. When K_n is decomposed into edge-disjoint sum of C_{34}-t-foils, it is called that K_n *has a* C_{34}-t-*foil decomposition*. Moreover, when every vertex of K_n appears in the same number of C_{34}-t-foils, it is called that K_n *has a balanced* C_{34}-t-*foil decomposition* and this number is called *the replication number*. This decomposition is to be known as *a balanced* C_{34}-t-*foil design*.

Theorem 4. K_n has a balanced C_{34}-t-foil decomposition if and only if $n \equiv 1 \pmod{68t}$.

Example 4.1. Balanced C_{34}-decomposition of K_{69}.

$\{(69, 2, 32, 63, 27, 36, 9, 14, 34, 49, 24, 37, 61, 43, 40, 18, 7, 15, 8, 20, 41, 45, 22, 39, 25, 51, 35, 16, 10,$
$38, 28, 62, 30, 1)\}$. (34 edges, 34 all lengths)
This stater comprises a balanced C_{34}-decomposition of K_{69}.

Example 4.2. Balanced C_{34}-2-foil decomposition of K_{137}.

$\{(137, 4, 64, 125, 53, 70, 17, 26, 66, 95, 46, 71, 119, 83, 78, 34, 13, 27, 14, 36, 79, 85, 120, 73, 47, 97, 67,$
$28, 18, 72, 54, 124, 62, 3),$
$(137, 2, 60, 123, 55, 74, 19, 30, 68, 99, 48, 75, 121, 87, 80, 38, 15, 31, 16, 40, 81, 89, 44, 77, 49, 101, 69,$
$32, 20, 76, 56, 122, 58, 1)\}$. (68 edges, 68 all lengths)
This stater comprises a balanced C_{34}-2-foil decomposition of K_{137}.

References

[1] K. Ushio and H. Fujimoto: "Balanced bowtie and trefoil decomposition of complete tripartite multigraphs,", *IEICE Trans. Fundamentals*, vol.E84-A, pp.839–844, 2001. [2] —— : "Balanced foil decomposition of complete graphs,", *IEICE Trans. Fundamentals*, vol.E84-A, pp.3132–3137, 2001. [3] —— : "Balanced bowtie decomposition of complete multigraphs,", *IEICE Trans. Fundamentals*, vol.E86-A, pp.2360–2365, 2003. [4] —— : "Balanced bowtie decomposition of symmetric complete multi-digraphs,", *IEICE Trans. Fundamentals*, vol.E87-A, pp.2769–2773, 2004. [5] —— : "Balanced quatrefoil decomposition of complete multigraphs,", *IEICE Trans. Information and Systems*, vol.E88-D, pp.19–22, 2005. [6] —— : "Balanced C_4-bowtie decomposition of complete multigraphs,", *IEICE Trans. Fundamentals*, vol.E88-A, pp.1148–1154, 2005. [7] —— : "Balanced C_4-trefoil decomposition of complete multigraphs,", *IEICE Trans. Fundamentals*, vol.E89-A, pp.1173–1180, 2006.

Recursive constructions of t-SEEDs related to quantum jump codes

Yiling Lin* and Masakazu Jimbo
Graduate School of Information Science, Nagoya University

A new class of combinatorial design, called a t-SEED, was introduced by Beth *et al.* (2003). A t-SEED has close relation with t-error correcting quantum jump code. For an n-set V and $\mathcal{B}^{(i)} \subset \binom{V}{k}$ $(i = 1, \cdots, m)$, a system $(V; \mathcal{B}^{(1)}, \mathcal{B}^{(2)}, \cdots, \mathcal{B}^{(m)})$ is called a *t-spontaneous emission error design*, denoted by t-$(n, k; m)$ SEED if the following conditions are satisfied:

(i) For any $i \neq j$, $\mathcal{B}^{(i)} \cap \mathcal{B}^{(j)} = \emptyset$,

(ii) For any i, $u \leq t$, $T \in \binom{V}{u}$, $\dfrac{\lambda_T}{|\mathcal{B}^{(i)}|} = \mu_T$ holds,
where $\lambda_T = |\{T \subset B | B \in \mathcal{B}^{(i)}\}|$.

A t-(n, k, λ) *design* is a pair $(V, \mathcal{B})$, where V is an n-set of points and $\mathcal{B}$ is a collection of k-tuple of V (*blocks*), such that every t-tuple of V is contained in exactly λ blocks. A *large set* of t-designs, denoted by $LS_\lambda(t, k, n)$, is a partition of the complete design (i.e. the set of all k-subsets of V) into disjoint t-(n, k, λ) designs.

It is clear that the definition of t-SEED is less restrictive than that of t-design by allowing a local parameter μ_T rather than the usual λ_t. If λ_T are constant not depending on T, then the t-SEED is a collection of t-designs.

Example 1 Any t-(n, k, λ) design $(V, \mathcal{B})$ can be seen as a t-$(n, k; 1)$ SEED.

Example 2 If a large set $LS_\lambda(t, k, n)$ exists, then there exists a t-$(n, k; \dfrac{\binom{n-t}{k-t}}{\lambda})$ SEED.

A t-$(n, k; m)$ SEED $(V; \mathcal{B}^{(1)}, \mathcal{B}^{(2)}, \cdots, \mathcal{B}^{(m)})$ is said to be *s-resolvable* if each design $\mathcal{B}^{(i)}$ is partitioned into h subfamilies $\mathcal{B}^{(i,1)}, \mathcal{B}^{(i,2)}, \cdots, \mathcal{B}^{(i,h)}$ and a $(V; \mathcal{B}^{(1,1)}, \mathcal{B}^{(1,2)}, \cdots, \mathcal{B}^{(m,h)})$ forms an s-$(n, k; mh)$ SEED.

*Email: lin@jim.math.cm.is.nagoya-u.ac.jp

A $k \times \lambda q^t$ array of q symbols is called an *orthogonal array* $OA_\lambda(t,k,q)$ if every one of the possible q^t ordered t-tuples of symbols occurs in exactly λ columns in any t rows of the array. When $\lambda = 1$, we write $OA(t,k,q)$. A *large set* of orthogonal arrays $LOA_\lambda(t,k,q)$ is a collection $\{A_r\}_{r\in R}$ of $OA_\lambda(t,k,q)$s such that every possible k-tuple of symbols occurs in exactly one of the OA's in the collection. We write $LOA(t,k,q)$ when $\lambda = 1$. Note that $|R| = q^{k-t}$. The following is known (see, for example, Raghavarao [2]).

Lemma 1 For any prime power q, there exists a $LOA(t,k,q)$.

Now we give some recursive constructions of t-SEEDs that we found.

Theorem 1 (Direct product construction) If there are a t-$(n,k;m)$ SEED and a t-$(n',k';m')$ SEED, then there is a t-$(nn',kk';mm')$ SEED.

Theorem 2 (LOA construction) If there are a t-$(n,k;m)$ SEED and an $LOA(t,k,q)$, then there is a t-$(nq,k;mq^{k-t})$ SEED.

Theorem 3 If there is a $\lfloor \frac{t}{2} \rfloor$-resolvable t-$(n,k;m)$ SEED, then there exists a $\lfloor \frac{t}{2} \rfloor$-resolvable t-$(nv,kk';h^{k'-1}m^{k'})$ SEED for any v, $k' \geq 2$, where h is the number of subfamilies $\mathcal{B}^{(i,j)}$ in $\mathcal{B}^{(i)}$.

Theorem 4 If there are a $\lfloor \frac{t}{2} \rfloor$-resolvable t-$(n,k;m)$ SEED and an $LOA(t,k',q)$, then there is a $\lfloor \frac{t}{2} \rfloor$-resolvable t-$(nv,kk';q^{k'-t}h^{k'-1}m^{k'})$ SEED for any $v \geq 2$, where h is the number of subfamilies $\mathcal{B}^{(i,j)}$ in $\mathcal{B}^{(i)}$.

In this report, we found several recursive constructions. By applying our constructions to known large set of t-designs, we obtain many series of t-SEEDs. Beth *et al.* gave an upper bound for m of a t-$(n,k;m)$ SEED. It is obvious that a large set $LS_\lambda(t,k,n)$ attain the upper bound. But even now, we cannot find a t-SEED attaining the upper bound except for a large set of t-designs.

References

[1] T. Beth, C. Charnes, M. Grassl, G. Alber, A. Delgado, M. Mussinger, A new class of designs which protect against quantum jumps. *Designs, Codes and Cryptography,* **29** (2003), 51–70.

[2] D. Raghavarao, *Constuctions and Combinatorial Problems in Design of Experiments.* Wiley, New York (1971).

アフィン幾何からできるデザインの分解について

長谷川 潤 (名古屋大院・情報科学), 籾原 幸二 (筑波大院・システム情報)
三嶋美和子 (岐阜大・工), 神保 雅一 (名古屋大院・情報科学)

1. Preliminary

It is well known that the set of t-flats in $\mathrm{AG}(n,q)$ yields a 2-design for a prime power q and a positive integer n. Especially, let $V=\mathrm{GF}(q^n)$ and $\mathcal{B}$ be the set of planes (2-flats) of $\mathrm{AG}(n,q)$. Then $(V,\mathcal{B})$ is a 2-$(q^n,q^2,(q^{n-1}-1)/(q-1))$ design.

Let $\sigma_a : x\mapsto ax$ for $a\in\mathrm{GF}(q^n)^\times$ and $G=\langle\sigma_\alpha\rangle$ for a primitive element α of $\mathrm{GF}(q^n)$. Moreover, let $T=\{\tau_b \mid \tau_b : x\mapsto x+b, b\in\mathrm{GF}(q^n)\}$ be the group of translations and $H=G\ltimes T=\{\tau_b\sigma_a : x\to ax+b \mid \sigma_a\in G,\tau_b\in T\}$. Then $\mathcal{B}$ is decomposed into block orbits $\mathcal{O}_j$ by the action of H and the following decomposition of the design is known.

Lemma 1 *The 2-design formed by the set of planes in $AG(n,q)$ is decomposed into*

(i) $\frac{q^{n-1}-1}{q^2-1}$ *disjoint* 2-$(v=q^n,k=q^2,\lambda=q+1)$ *designs* $(V,\mathcal{O}_j)$ *for* $i=1,2,\ldots,\frac{q^{n-1}-1}{q^2-1}$ *when n is odd.*

(ii) $\frac{q^{n-1}-q}{q^2-1}$ *disjoint* 2-$(v=q^n,k=q^2,\lambda=q+1)$ *designs* $(V,\mathcal{O}_j)$ *for* $i=1,2,\ldots,\frac{q^{n-1}-q}{q^2-1}$ *and a single* 2-$(v=q^n,k=q^2,\lambda=1)$ *design* $(V,\mathcal{O}_0)$ *when n is even.*

A set $\mathcal{L}$ of lines in $\mathrm{PG}(n-1,q)$ is called an *s-spread* if each point of $\mathrm{PG}(n-1,q)$ is covered exactly s times by lines in $\mathcal{L}$. A 1-spread is simply called a *spread*. A 2-design $(V,\mathcal{O}_j)$ of planes in $\mathrm{AG}(n,q)$ is equivalent to an s-spread $\mathcal{L}_j$ of lines in $\mathrm{PG}(n-1,q)$, where $s=1$ for $\mathcal{L}_0$ and $s=q+1$ for $\mathcal{L}_j$, $j=1,2,\ldots$. Here, a block B_j in $\mathcal{O}_j$ including 0 and 1 is called a *baseblock* of $\mathcal{O}_j$. For a baseblock $B_j\in\mathcal{O}_j$, $B_j^H=\{B_j^h \mid h\in H\}=\mathcal{O}_j$ holds. Similarly, a line (block) L_j in $\mathcal{L}_j$ such that L_j includes 1 is called a *baseblock* of $\mathcal{L}_j$ and for a baseblock $L_j\in\mathcal{L}_j$, $L_j^G=\{L_j^g \mid g\in G\}=\mathcal{L}_j$ holds.

For $e|\frac{q^n-1}{q-1}$ and $\beta=\alpha^e$, let $G_e=\langle\sigma_\beta\rangle$ and $H_e=G_e\ltimes T$. In this report, we consider the case that the orbits of H_e form subdesigns. That is, we try to devide a $(q+1)$-spread $\mathcal{L}_j$ into s'-spreads with $s'\mid q+1$ by the action of G_e. For this purpose, $\gcd(e,q+1)>1$ must hold. Since $\gcd(q+1,\frac{q^n-1}{q-1})=q+1$, or 1 according as n is even or odd, we assume that n is even. Munemasa [1] counted the number of spreads for $q=2$ by examining the orbit structure of $\mathrm{PG}(2n-1,2)$ derived by the action of G_e for $e=3$.

Lemma 2 (Munemasa [1]) *The number of lines in $PG(2n-1,2)$ whose orbit under the subgroup G_3 in the Singer group G is a spead is given by*

$$\frac{(2^{2n}-1)(2^n+(-1)^{n+1})^2}{27}.$$

In general, it follows from Lemma 1 that the number of full orbits is $\frac{2^{2n-1}-2}{3}$. Among these, there are $\frac{1}{27}\{(2^n+(-1)^{n+1})^2\}-\frac{1}{3}\rho_n$ orbits which can be partitioned into three spreads, where $\rho_n=0$ or 1 depending on n. Hence, we obtain the following:

Corollary 3 *The 3-design formed by the set of 2-flats in $AG(2n,2)$ is decomposed into*

$$\frac{2^{2n-1}-2}{3}-\frac{(2^n+(-1)^{n+1})^2}{27}+\frac{\rho_n}{3}$$

2-$(2^{2n},4,3)$ *designs and*

$$\frac{(2^n+(-1)^{n+1})^2}{9}-\rho_n+1$$

2-$(2^{2n},4,1)$ *designs, where $\rho_n=0$ if $n\equiv 0 \pmod 3$, and $\rho_n=1$ otherwise. These designs are disjoint.*

2. Decomposition of a 2-$(3^{2n}, 9, 4)$ design into subdesigns

Now, we consider the decomposition of the 2-design derived from planes of AG$(2n, 3)$. In this case, each block orbit $\mathcal{O}_j$ of planes in AG$(2n, 3)$ contains a baseblock of form

$$B = \{0, 1, x, x+1, x-1, -1, -x, -x-1, -x+1\},$$

which corresponds to a line

$$L = \{1, x, x+1, x-1\}$$

in PG$(2n-1, 3)$.

By letting $C_0^e = \langle\beta\rangle$ and $C_j^e = \alpha^j C_0^e$, we define the three sets $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_2'$ of quadruples of form $\{1, x, x+1, x-1\}$ as follows:

(i) $\mathcal{M}_1$ to be the set of quadruples such that $\{1, x, x+1, x-1\}$ is a complete system of representatives for the cyclotomic cosets C_j^4, $j = 0, 1, 2, 3$.

(ii) $\mathcal{M}_2$ to be the set of quadruples such that two of $1, x, x+1, x-1$ are contained in C_0^2 and the other two are in C_1^2.

(iii) $\mathcal{M}_2^{'}$ to be the set of quadruples such that two of $1, x, x+1, x-1$ are contained in C_0^4 and the other two are in C_2^4.

Lemma 4 (i) *If a line L is a quadruple in $\mathcal{M}_1$, then $\mathcal{L} = L^G$ is decomposed into four spreads L^{G_4}, $L^{\sigma_\alpha G_4}$, $L^{\sigma_\alpha^2 G_4}$ and $L^{\sigma_\alpha^3 G_4}$.*

(ii) *If a line L is a quadruple in $\mathcal{M}_2$, then $\mathcal{L}$ is decomposed into two 2-spreads L^{G_2} and $L^{\sigma_\alpha^2 G_2}$.*

(iii) *If a line L is a quadruple in $\mathcal{M}_2'$, then $\mathcal{L}$ is decomposed into two 2-spreads $L^{G_4} \cup L^{\sigma_\alpha G_4}$ and $L^{\sigma_\alpha^2 G_4} \cup L^{\sigma_\alpha^3 G_4}$.*

Evaluation of $|\mathcal{M}_1|, |\mathcal{M}_2|$ and $|\mathcal{M}_2'|$ can be reduced to calculation problem of Jacobi sums on two multiplicative characters of $\mathbb{F}_{3^{2n}}$, which enables us to establish the following theorem.

Theorem 5 (Main Theorem) *The 2-design formed by the set of 2-flats in AG$(2n, 3)$ is decomposed into $((3^{2n-1}-3)/8 - K_2)$ 2-$(3^{2n}, 9, 4)$ designs, $2(K_2 - K_1)$ 2-$(3^{2n}, 9, 2)$ designs and $(4K_1 + 1)$ 2-$(3^{2n}, 9, 1)$ designs, where*

$$K_2 = \frac{9}{512}(3^{2n}+1) - \frac{1}{256}\left\{(5(-1)^n+2)3^n + (3(-1)^n - 2)\left((1-i2\sqrt{2})^n + (1+i2\sqrt{2})^n\right)\right\} - \frac{1}{4}\mu_n,$$
$$K_1 = \frac{1}{256}(3^{2n}+1) - \frac{1}{128}\left\{(5(-1)^n-2)3^n + ((-1)^n - 2)\left((1-i2\sqrt{2})^n + (1+i2\sqrt{2})^n\right)\right\} - \frac{1}{4}\nu_n$$

with

$$\mu_n = \begin{cases} 0, & \text{if } n \equiv 0 \pmod 4, \\ 1, & \text{otherwise,} \end{cases} \qquad \nu_n = \begin{cases} 0, & \text{if } n \text{ is even,} \\ 1, & \text{if } n \text{ is odd.} \end{cases}$$

These designs are disjoint.

Reference

[1] A. Munemasa, Flag-transitive 2-designs arising from line-spreads in PG$(2n-1, 2)$, *Geometriae Dedicata*, **77** (1999), 209–213.

Difference families from Galois rings with characteristic p^2 and related character sums

Koji Momihara (E-mail: momihara@sk.tsukuba.ac.jp)
Graduate School of Systems and Information Engineering, University of Tsukuba
Mieko Yamada (Email: myamada@kenroku.kanazawa-u.ac.jp)
Institute of Science and Engineering, Kanazawa University

1 Introduction. Let G be a finite abelian group and $\mathcal{F} = \{B_i \mid 1 \quad i \quad b\}$ be a collection of subsets of G. Define $\Delta B_i := \{ab^{-1} \mid a, b \in B_i; a \neq b\}$ for each B_i and set $K = \{|B_i| \mid 1 \quad i \quad b\}$. We say that $\mathcal{F}$ is a $(G, N, K, \mu, \ )$ divisible di erence family (simply DDF) if there exist $\ , \mu \in \mathbb{N}$ and $N \quad G$ such that the list $\bigcup_{i=1}^{b} \Delta B_i$ contains every element of $G \setminus N$ exactly $\ $ times and contains every element of $N \setminus \{1_G\}$ exactly μ times. If the size of each B_i is constant, say k, it is denoted as $(G, N, k, \mu, \ )$-DDF. If $\mu = \ $, the concept of a $(G, N, K, \mu, \ )$-DDF coincides with that of an ordinary $(G, K, \ )$ di erence family (simply DF).

In [3], the following construction of di erence families was given.

Proposition 1.1. *Let $\mathbb{F}_q$ be the finite field with q elements and N denote the set of non-zero squares in $\mathbb{F}_q$. Define $B_1 := (N+1) \cap N$ and $B_2 := (N \quad 1) \cap N$. Then, $\mathcal{F} = \{B_1, B_2\}$ forms an $(N, (q \quad 3)/4, (q \quad 7)/4)$-DF.*

2 Generalized Szekeres's construction. The following provides a generalization of Szekeres's construction of di erence families.

Proposition 2.1. *Let $\mathbb{R}$ be a commutative ring with G and H as its additive and unit groups, respectively, having unity $1 := 1_{\mathbb{R}}$. Let $N \quad H$ and let S be a complete system of representatives for H/N. Furthermore, let A_i, $1 \quad i \quad b$, be u_i-subsets of S. Assume that there is a $(G, K, \ )$-DF $\mathcal{F} = \{D_i \mid 1 \quad i \quad b\}$, in which each D_i has the form $D_i = (\bigcup_{x \in A_i} xN) \cup C_i$, where each C_i is a subset of $I := G \setminus H$. For a subgroup $L \quad N$, assume that $\mathcal{F}$ satisfies the following properties:*

(i) $C_i = tC_i$ for any $1 \quad i \quad b$ and $t \in N$,

(ii) $\sum_{i=1}^{b} |D_i \cap (D_i \quad t+1) \cap (I+1)| = \mu_1$ for any $t \in L \setminus \{1\}$ and $= \mu_2$ for any $t \in N \setminus L$.

Then, the family $\mathcal{F}' = \{y^{-1}(D_i \quad 1) \cap N \mid 1 \quad i \quad b; y \in S\}$ forms an $(N, L, \{k_{i,y} \mid 1 \quad i \quad b; y \in S\}, \quad \mu_1, \quad \mu_2)$-DDF, where $k_{i,y} = |(N+y) \cap D| + |y^{-1}(C_i \quad 1) \cap N|$.

We apply generalized Szekeres's construction to some known series of cyclotomic di erence sets.

Example 2.2. *It is known [2] that for the cases when (i) $e = 2$ and $q \equiv 3 \pmod 4$; (ii) $e = 4$ and $q = 1 + 4t^2$ with $t \equiv 1 \pmod 2$; (iii) $e = 8$ and $q = 9 + 64a^2 = 1 + 8b^2$ with $a \equiv b \equiv 1 \pmod 2$, the set E of non-zero eth powers of $\mathbb{F}_q$ forms an $(\mathbb{F}_q^+, k = (q \quad 1)/e, \ = (q \quad e \quad 1)/e^2)$ difference set. Applying generalized Szekeres's construction to these difference sets as $(G, N, D_1, C_1) = (\mathbb{F}_q^+, E, E, \emptyset)$, we obtain (i) a $(\mathbb{Z}_{(q-1)/2}, (q \quad 3)/4, (q \quad 7)/4)$-DF; (ii) a $(\mathbb{Z}_{(q-1)/4}, (q \quad 5)/16, (q \quad 21)/16)$-DF; (iii) a $(\mathbb{Z}_{(q-1)/8}, (q \quad 9)/64, (q \quad 73)/64)$-DF, respectively, where we used the fact $k_{1,y} = |(N+y) \cap N| = \ $. Form (i), we obtain Szekeres's difference families by noting that $((N+1) \cap N)^{-1} = \ (N \quad 1) \cap N$.*

3 Application of generalized Szekeres's construction to Hadamard difference sets over $GR(4, m)$. Let $GR(p^2, m)$ denote the Galois ring with characteristic p^2 and degree m, which is a Galois extension with degree m of $\mathbb{Z}/p^2\mathbb{Z}$. The ring $\mathbb{R} = GR(p^2, m)$ is a local ring having the unique maximal ideal $p\mathbb{R}$ and the residue class field $\mathbb{R}/p\mathbb{R} = \{\overline{0}, \overline{g^0}, \overline{g^1}, \ldots, \overline{g^{p^m-2}}\}$ is isomorphic to $\mathbb{F}_{p^m}$. We take $\mathcal{T} = \{0, g^0, g^1, \ldots, g^{p^m-2}\}$ as a set of representatives of $\mathbb{R}/p\mathbb{R}$. An arbitrary element $\alpha \in \mathbb{R}$ is uniquely written as $\alpha = a + pb$, $a, b \in \mathcal{T}$.

Let $A := \{\overline{x} \in \mathbb{F}_{2^m}^+ \mid \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\overline{bx}) = \overline{0}\}$ for $\overline{b} \in \mathbb{F}_{2^m}^*$ such that $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2}(\overline{b}) = \overline{0}$ and let $D = \{a(1+2b) \mid a \in \mathcal{T} \setminus \{0\}; b \in A\}$. Note that D is a subgroup of order $2^{m-1}(2^m \quad 1)$ of the unit group

$\mathbb{R}^*$ of $\mathbb{R}$. In [4], it is shown that D forms an $(\mathbb{R}^+, 2^{m-1}(2^m \quad 1), 2^{m-1}(2^{m-1} \quad 1))$ di erence set. By applying Proposition 2.1 to this Hadamard di erence set as $N \quad D$ and $C_1 = \emptyset$, we obtain the following theorem, see [1] for its proof.

Theorem 3.1. *There exists a* $(\mathbb{Z}_{(2^m-1)/e} \times \mathbb{Z}_{2^s}, \{0\} \times \mathbb{Z}_{2^s}, K, 2^m(2^{m-2} \quad 1), 2^{m-1}(2^{m-1} \quad 1) \quad 2^{m-2})$*-DDF for any* $e \mid 2^m \quad 1$ *and* $s \quad m$*. In particular, if* $e = 1$ *and* $s = m \quad 1$*, it has the parameter* $(\mathbb{Z}_{2^m-1} \times \mathbb{Z}_{2^{m-1}}, \{0\} \times \mathbb{Z}_{2^{m-1}}, 2^{m-1}(2^{m-1} \quad 1), 2^m(2^{m-2} \quad 1), 2^{m-1}(2^{m-1} \quad 1) \quad 2^{m-2})$.

Note that $k_y = |(N + y) \cap D| \in K$ for $y \in S$ a complete system of representatives for $\mathbb{R}^*/N$ in Theorem 3.1 by the construction of Proposition 2.1.

4 Computation of k_y's and Jacobi sums. Any multiplicative character ψ of $GR(p^2, m)^*$ is uniquely written as $\psi = \psi_P \psi_T$ for some ψ_P and ψ_T, which are multiplicative character of $GR(p^2, m)$ trivial on $\mathcal{T}$ and P, respectively. Put $\alpha = a(1 + pb) \in GR(p^2, m)^*$. Obviously, the multiplicative character $\psi_P = \psi_{P,\ell}$ for $\ell \in \mathcal{T}$ of $GR(p^2, m)$ is given by $\psi_{P,\ell}(\alpha) = \psi_{P,\ell}(1 + pb) = \chi_{\overline{\ell}}(\overline{b})$, where $\chi_{\overline{\ell}}$ is an additive character of $\mathbb{F}_{p^m}$. Also, the multiplicative character $\psi_T = \psi_{T,i}$ for $0 \quad i \quad p^m \quad 1$ of $GR(p^2, m)$ is given by $\psi_{T,i}(\alpha) = \psi_{T,i}(a) = \quad_i(\overline{a})$, where $\quad_i$ is a multiplicative character of $\mathbb{F}_{p^m}$. We extend the domain of ψ to all elements of $GR(p^2, m)$ as $\psi_{P,\ell}(\alpha) = 0$ for any $\alpha \in p\mathbb{R}$ and for any $\ell \in \mathcal{T}$ and as $\psi_{T,i}(\alpha) = 0$ for any $\alpha \in p\mathbb{R}$ and for any $1 \quad i \quad p^m \quad 1$ and $\psi_{T,0}(\alpha) = 1$ for any $\alpha \in p\mathbb{R}$. The sum $J(\psi_1, \psi_2) := \sum_{\alpha \in \mathbb{R}} \psi_1(\alpha)\psi_2(1 \quad \alpha)$ for multiplicative characters ψ_1 and ψ_2 is called a Jacobi sum of $GR(p^2, m)$.

Proposition 4.1. *Let* $p = 2$ *and let* $\psi_1 = \psi_{P,\ell_1}\psi_{T,m_1}$ *and* $\psi_2 = \psi_{P,\ell_2}\psi_{T,m_2}$*. If* ψ_{P,ℓ_1}*,* ψ_{P,ℓ_2}*, and* $\psi_{P,\ell_1}\psi_{P,\ell_2}$ *are non-trivial, it holds that* $J(\psi_1, \psi_2) = 2^m \chi_{\overline{1}}(\overline{(\ell_1\ell_2)}^{2^{m-1}}) \quad_{m_1}^{-1}(\overline{1 + \ell_1^{-1}\ell_2}) \quad_{m_2}^{-1}(\overline{\ell_1\ell_2^{-1} + 1})$.

Using Proposition 4.1, we obtain the following theorem.

Theorem 4.2. *Assume that* $m \quad s \mid m$ *and* b *satisfies* $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{m-s}}}(\overline{b}) = \overline{0}$*. Let* $N = M \times L \quad \mathbb{R}^*$ *for the multiplicative subgroup* M *of index* e *of* $\mathcal{T} \setminus \{0\}$ *and* $L = \{\overline{x} \in \mathbb{F}_{2^m} \mid \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{m-s}}}(\overline{bx}) = \overline{0}\}$*. Set* $y^{-1} := g(1 + 2h)$ *and* $z := \gcd(e, (2^m \quad 1)/(2^{m-s} \quad 1))$*. Then, if* $\overline{a}(:= \mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{m-s}}}(\overline{bh})) = \overline{0}$*,*

$$k_y = \begin{cases} \frac{2^{s-1}}{e}(2^m \quad 1 \quad e) + \frac{2^{s-1}}{e}(z(2^{m-s} \quad 1) \quad e) & \text{if } g \text{ is } e\text{th power;} \\ \frac{2^{s-1}}{e}(2^m \quad 1) + \frac{2^{s-1}}{e}z(2^{m-s} \quad 1) & \text{if } g \text{ is } z\text{th power but not } e\text{th power;} \\ \frac{2^{s-1}}{e}(2^m \quad 1) & \text{if } g \text{ is not } z\text{th power.} \end{cases}$$

If $\overline{a} \neq \overline{0}$*,*

$$k_y = \begin{cases} \frac{2^{s-1}}{e}(2^m \quad 1 \quad e) + \frac{2^{s-1}z}{e}(\quad 1 \quad \chi_{\overline{1}}'(\overline{a}) + \sum_{u=1}^{e/z-1} J_u) & \text{if } g \text{ is } e\text{th power;} \\ \frac{2^{s-1}}{e}(2^m \quad 1) + \frac{2^{s-1}z}{e}(\quad 1 \quad \chi_{\overline{1}}'(\overline{a}) + \sum_{u=1}^{e/z-1} \quad_{\frac{u(2^m-1)}{e}}^{-1}(\overline{g})J_u) & \text{if } g \text{ is } z\text{th power} \\ & \quad \text{but not } e\text{th power;} \\ \frac{2^{s-1}}{e}(2^m \quad 1) & \text{if } g \text{ is not } z\text{th power,} \end{cases}$$

where $J_u := \sum_{\bar{d} \in \mathbb{F}_{2^{m-s}} \setminus \{\bar{0}, \bar{1}\}} \chi_{\overline{1}}'(\overline{a(d+1)})\eta_{uz(2^{m-s}-1)/e}(\bar{d})\eta_{uz(2^{m-s}-1)/e}^{-1}(\overline{d+1})$ *and* $\eta_{z(2^{m-s}-1)/e}$ *is a multiplicative character of order* e/z *of* $\mathbb{F}_{2^{m-s}}$*. In particular, if* $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_{2^{m-s}}}(\overline{bh}) \neq \overline{0}$*,* $|J_u| \quad 2^{(m-s+2)/2}$ *follows for non-trivial* $\eta_{zu(2^{m-s}-1)/e}$ *and it holds that*

$$\frac{2^{\frac{m+3s}{2}}(e \quad z) + 2^{s-1}(2z + e)}{e} \quad k_y \quad \frac{2^{s-1}(2^m \quad 1)}{e} \quad \frac{2^{\frac{m+3s}{2}}(e \quad z)}{e}.$$

References

1. K. Momihara, M. Yamada, Group divisible difference families from $GR(p^2, n)$ and related character sums–Generalized Szekeres's difference families and Jacobi sums, preprint.
2. T. Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Mathematics, 2, Markham Publishing Company, (1967).
3. G. Szekeres, Tournaments and Hadamard matrices, *Enseignement Math.*, 15, pp. 269–278, (1969).
4. K. Yamamoto, M. Yamada, Hadamard difference sets over an extension of $Z/4Z$, *Util. Math.*, 34, pp. 169–178, (1988).

The Existence of Almost Difference Families

Xun, Wang
Graduate School of Systems and Information Engineering, University of Tsukuba

Abstract. Almost difference families (ADFs) were introduced by Ding and Yin as a useful generalization of almost difference sets (ADSs), and a number of infinite classes of almost difference families had been constructed. In this paper, by using Weil's theorem on character sums estimates and computer searching, some known results on almost difference families by Ding and Yin are improved.

Given an Abelian group G of order q. Let $F = \{D_1, D_2, \cdots, D_s\}$ be a family of k-subsets of G. Define the difference list ΔD_j of D_j to be the multi-set

$$\{a - b : a, b \in D_j \text{ and } a \neq b\},$$

in which each object may occur with a certain multiplicity. The formal sum of the difference list ΔD_j of D_j is called the difference list of F, and is denoted by ΔF.

F said to be an almost difference family, or a (q, k, λ, t)-ADF, if some t nonzero elements of G occur exactly λ times each in the difference list ΔF, while the remaining $q - t - 1$ nonzero elements of G occur exactly $\lambda + 1$ times each in ΔF. Furthermore, if G is a cyclic group of order q, then we call the (q, k, λ, t)-ADF cyclic.

Suppose q is a prime power. To construct combinatorial designs in F_q, one often needs to find an element $x \in F_q \setminus \{0\}$, such that some polynomials in $F_q[x]$ of degree one or two satisfying certain conditions. Weil's theorem on character sum estimates is very useful to do this.

Theorem 1.1. Let ψ be a multiplicative character of F_q of order $m > 1$ and let $f \in F_q[x]$ be an monic polynomial of positive degree that is not an m-th power of a polynomial. Let d be the number of distinct roots of f in its splitting field over F_q, then for every $a \in F_q$, we have

$$\left| \sum_{c \in G} \psi(af(c)) \right| \leq (d-1)\sqrt{q}.$$

In order to construct optimal optical orthogonal codes, Chang and Ji (2004) presented the following result.

Theorem 1.2. Let q be a prime, $q \equiv 1 \pmod{e}$ and

$$q-[\sum_{r=0}^{s-2}\binom{s}{r}(s-r-1)(e-1)^{s-r}]\sqrt{q}-se^{s-1}>0$$

Then, for any given s-tuple $(i_1,i_2,\cdots,i_s)\in(1,2,\cdots,e-1)^s$ and any given s-tuple $(c_1,c_2,\cdots,c_s)$ of pairwise distinct elements of F_q, there exists an element $x\in F_q$ such that $x+c_r\in C_{i_r}^e$ for each r.

For our purpose, Theorem 1.2. is generalized to the following result.

Theorem 1.3. Let q be a prime, $q\equiv 1(\mathrm{mod}\ e)$ and

$$q-[\sum_{r=2}^{s}\binom{s}{r}(r-1)(e-1)^r+\sum_{u=1}^{t}\binom{t}{u}(2u-1)(e-1)^u+\sum_{r=1}^{s}\sum_{u=1}^{t}\binom{s}{r}\binom{t}{u}(r+2u-1)(e-1)^{r+u}]\sqrt{q}-ste^{s+t-1}>0$$

For s-tuple $(i_1,i_2,\cdots,i_s)\in(1,2,\cdots,e-1)^s$ and t-tuple $(h_1,h_2,\cdots,h_t)\in(1,2,\cdots,e-1)^t$, and for any given s-tuple $(c_1,c_2,\cdots,c_s)$ of pairwise distinct elements of F_q, $((a_1,b_1),(a_2,b_2),\cdots,(a_t,b_t))\in(F_q\times F_q)^t$, there exists an element $x\in F_q$ such that $x+c_r\in C_{i_r}^e, 1\le r\le s$, $x^2+a_u x+b_u\in C_{h_u}^e$, where $x^2+a_u x+b_u$ are irreducible in $F_q[x]$ and pairwise coprime, $1\le u\le t$.

By using this bound and computer searching, some results on almost difference families by Ding and Yin (2008) are improved as follows.

Theorem 1.4. Let $q\equiv 1(\mathrm{mod}\,8)$ be a prime and $q>9$. Then there exist a cyclic $(q,4,1,(q-1)/2)$-ADF in F_q.

Theorem 1.5. For each prime $q\equiv 1(\mathrm{mod}\ 6)$ and $q>7$, there exists a cyclic $(q,5,3,2(q-1)/3)$-ADF in F_q.

Theorem 1.6. Let $q\equiv 1(\mathrm{mod}\ 8)$ be a prime and $q>9$. Then there exist a cyclic $(q,5,1,(q-1)/2)$-ADF in F_q.

[1] Chang, Y., Ji, L., 2004. Optimal (4up, 5, 1) optical orthogonal codes. J. Combin. Des. 12, 346–361.

[2] Ding, C., Yin, J., 2008. Constructions of almost difference families. Discrete Math. 308, 4941–4954.

[3] Wang, X., Wu, D., 2009. The existence of almost difference families, J. Statist. Plann. Inference 139, 4211–4216.

On the Existence of k-sun Systems

C.-M. Fu, N.-H. Jhuang, Y.-L. Lin and H.-M. Sung
Department of Mathematics, Tamkang University,
Tamsui, Taipei County, Taiwan, R.O.C.

For a graph G, let $V(G)$ be the vertex set of G and $E(G)$ be the edge set of G and let K_n be the complete graph of order n. A k-cycle is a cycle of length k, denoted by C_k. A matching of size k or a k-matching in G is a set of k mutually non-adjacent edges, denoted by M_k. If M_k covers all vertices of G, then M_k is called a perfect matching of G. A k-sun graph $S(C_k)$ is obtained from C_k by adding a pendent edge to each vertex of C_k. Thus each k-sun graph $S(C_k)$ contains exactly one C_k and one matching M_k.

Let G be a simple graph. A decomposition $\mathcal{D}$ of G is a collection of edge-disjoint subgraphs $G_1, G_2, \cdots, G_t$ of G such that every edge of G belongs to exactly one G_j for $j = 1, 2, \cdots, t$. $\mathcal{D}$ is called a Γ-decomposition of G if each member of $\mathcal{D}$ is isomorphic to Γ. A Γ-decomposition of G is also called a (G, Γ)-design. In particular, if G is K_n and Γ is C_k with $k \geq 3$ then a (K_n, C_k)-design is known as a k-cycle system of order n. If Γ is $S(C_k)$ then a $(K_n, S(C_k))$-design is called a k-sun system of order n. In 2008, Anitha and Lekshmi decomposed K_{2k} into $k-1$ k-sun graphs and a perfect matching when k is odd and $k-2$ k-sun graphs, a perfect matching, and a Hamilton cycle when k is even. This motivates us to study the existence of k-sun systems.

Assume $\mathcal{D}$ to be a (K_n, G)-design. An automorphism group of $\mathcal{D}$ is a group of permutations on $V(K_n)$ leaving the collection $\mathcal{D}$ of G invariant. A (K_n, G)-design is said to be cyclic (respectively 1-rotational) if there is an automorphism of order n (respectively $n-1$ with one fixed point). So far, if G is C_k, then there are many results about cyclic or 1-rotational k-cycle systems. If G is a graph obtained from C_k by adding m (≥ 1) distinct pendent edges to the vertices of C_k, denoted by $\Theta_m C_k$ then Wu and Lu proved the following.

Theorem 1. *For any positive integers k and m with $k \geq 3$, there exists a cyclic $(K_{2(k+m)+1}, \Theta_m C_k)$-design. Moreover, if k is even, then there exists a cyclic $(K_{2p(k+m)+1}, \Theta_m C_k)$-design for any positive integer p.*

Since $S(C_k)$ can be viewed as $\Theta_k C_k$, we have

Corollary 2. *For any positive integer $k \geq 3$, there exists a cyclic k-sun system of order $4k+1$. Moreover, if k is even, then there exists a cyclic k-sun system of order v where $v \equiv 1 \pmod{4k}$.*

In order to settle the existence problem of n-sun systems we need the following lemma (necessary conditions).

Lemma 3. *If an k-sun system of order n exists, then $n \geq 2k$ and $2k | \binom{n}{2}$.*

In 1988, Jian-Xing Yin and Bu-Sheng Gong proved the following result.

Lemma 4. *There exists a 3-sun system of order n, if and only if $n \equiv 0, 1, 4, 9$ (mod 12).*

Let G be a simple graph. We shall assume that the vertex set of K_n is $\mathbb{Z}_n$ when we consider cyclic (K_n, G)-design with the automorphism

$$\pi : i \mapsto i + 1 \pmod{n} \text{ or } \pi = (0, 1, 2, \cdots, n-1)$$

or $\mathbb{Z}_{n-1} \cup \{\infty\}$ when we consider 1-rotational (K_n, G)-design with the automorphism

$$\pi : \infty \mapsto \infty, i \mapsto i + 1 \pmod{n-1} \text{ or } \pi = (\infty)(0, 1, 2, \cdots, n-2).$$

We use difference method to obtain k-sun systems of all possible orders for $k = 3, 4, 5, 6, 10, 14$ and 2^t where $t(\geq 2)$ is a positive integer. More precisely, we obtain cyclic k-sun systems of odd order and 1-rotational k-sun systems of even order except those orders less than $4k$.

Theorem 5. *If $n \equiv 1 \pmod{12}$, then there exists a cyclic 3-sun system of order n. If $n \equiv 0 \pmod{12}$, then there exists a 1-rotational 3-sun system of order n.*

Next we consider 4-sun systems. By counting the edges, we get that if there exists a 4-sun system of order n then $n \equiv 0, 1 \pmod{16}$. From Corollary 2, we have that if $n \equiv 1 \pmod{8k}$, then there exists a cyclic $2k$-sun system of order n.

Lemma 6. *If $n \equiv 0 \pmod{16}$ then there exists a 1-rotational 4-sun system of order n.*

From Lemma 6, we can construct and obtain the following result.

Lemma 7. *Let $k > 2$ be an integer. If $v \equiv 0 \pmod{8k}$ then there exists a 1-rotational $2k$-sun system of order v.*

Theorem 8. *Let $t \geq 2$ be an integer. There exists a 2^t-sun system of order v if and only if $v \equiv 0, 1 \pmod{2^{t+2}}$.*

Next we can construct cyclic or 1-rotational k-sun systems of order n, for $k = 6$, 10 and 14.

Lemma 9. *If $n \equiv 9 \pmod{24}$ then there exists a cyclic 6-sun system of order n.*

Lemma 10. *If n is a positive integer, and $v \equiv 16 \pmod{24}$ then there exists a 1-rotational 6-sun system of order n.*

Theorem 11. *There exists a cyclic or 1-rotational 6-sun system of order n if and only if $n \equiv 0, 1, 9, 16 \pmod{24}$ except possiblen $= 16$.*

Theorem 12. *There exists a cyclic or 1-rotational 10-sun system of order v if and only if $n \equiv 0, 1, 16, 25 \pmod{40}$ except possible $n = 25$.*

Theorem 13. *There exists a cyclic or 1-rotational 14-sun system of order n if and only if $n \equiv 0, 8, 49 \pmod{56}$ except $v = 49$.*

A counter-example of Delsarte-Seidel's conjecture on tight Euclidean design

Masatake Hirao, Masanori Sawa, Yuanyuan Zhou
Graduate School of Information Science, Nagoya University

A spherical t-design is a nite subset X in the unit sphere S^d which is used to approximate the integral of any polynomial f of at most degree t over S^d by the average of values of f at X. Generalizing the concept of spherical designs, Neumaier and Seidel [6] de ned a Euclidean t-design in $\mathbb{R}^{d+1}$.

Let $d,\ t$ be positive integers, and S_r^d be the sphere with radius r in $\mathbb{R}^{d+1}$ whose center is at the origin. A Euclidean t-design is a system of a nite subset X in $\mathbb{R}^{d+1}$ and a weight function w on X such that

$$\sum_{r\in R} \frac{\sum_{\boldsymbol{x}\in X\cap S_r^d} w(\boldsymbol{x})}{\int_{S^d} d} \int_{\boldsymbol{x}\in S^d} f(r\boldsymbol{x})d \ = \sum_{\boldsymbol{x}\in X} w(\boldsymbol{x})f(\boldsymbol{x}) \tag{1}$$

holds for every polynomial f of degree at most t over $\mathbb{R}^{d+1}$, where R is the set of the ordinary Euclidean norms of X and is the uniform measure on the unit sphere S^d. With $|R| = p$, this system is called a *$(d+1)$-dimensional Euclidean t-design on p concentric spheres*. In particular, a Euclidean design with $R = \{1\}$ and $w(\boldsymbol{x})$ 1 is a spherical t-design.

Euclidean designs always exist if the designs have large number of points. Thus we are interested in Euclidean designs with smaller number of points. It is well known [4, 5] that the number of points X in a $(d+1)$-dimensional Euclidean t-design on p concentric spheres is bounded from below as follows:

$$|X| \geq \sum_{k=1}^{p} \left(\binom{\lfloor t/2 \rfloor + d - 2(k-1)}{d} + \binom{\lfloor (t-1)/2 \rfloor + d - 2(k-1)}{d} \right). \tag{2}$$

A Euclidean t-design on p concentric spheres is said to be tight if it attains the bound (2). In the 2-dimensional case, in nitely many tight Euclidean t-designs have been already found for t and p [1, 4]. However, in higher dimensional cases $(d \geq 2)$, little is known on the existence of tight Euclidean designs even for small values of t and p, though many researchers have tried this problem.

In this talk we present a 4-dimensional tight Euclidean 5-design on 3 concentric spheres whose existence was previously unknown. As far as the authors know, this is the rst and the only known example of tight Euclidean t-designs with $0 \notin X,\ t \geq 4,\ d \geq 3$ and $p \geq 3$. In fact all known results of tight Euclidean

designs with $0 \notin X$, $t \geq 4$, $d \geq 2$ and $p \geq 2$, are updated since the last survey paper by Bannai and Bannai [3].

The set of all transpositions of coordinates in $\mathbb{R}^{d+1}$ forms a nite group G, called the Weyl group of type A_d, $d \geq 1$. Let σ be the involution on $\mathbb{R}^{d+1}$ de ned by $x^\sigma = -x$ and H be the semidirect product of G and $\langle\sigma\rangle$. Then it is obvious that H is a subgroup of the Weyl group of type B_{d+1}, say $W(B_{d+1})$, and so the order of H is $2 \cdot (d+1)!$. For $x \in \mathbb{R}^{d+1}$ we denote by $\mathrm{Orb}_H(x)$ the orbit of x under H, that is, $\mathrm{Orb}_H(x) = \{x^\tau \mid \tau \in H\}$.

Theorem 1 There exists a 4-dimensional tight Euclidean 5-design (X, w) on 3 concentric spheres which has the form

$$\sum_{x\in X} w(x)f(x) = w_0 \sum_{x\in \mathrm{Orb}_H((p_0,p_0,p_0,p_0))} f(x) + w_1 \sum_{x\in \mathrm{Orb}_H((p_1,p_1,p_1,q_1))} f(x) + w_2 \sum_{x\in \mathrm{Orb}_H((p_2,p_2,q_2,q_2))} f(x), \tag{3}$$

where $p_0, p_1, p_2, q_1, q_2, w_0, w_1, w_2$ are positive real numbers such that

$$2p_0^2 - 3p_1^2 > 0, \quad -3p_1 = q_1, \quad p_2 = \frac{(\sqrt{2}-1)p_0p_1}{\sqrt{2p_0^2 - 3p_1^2}},$$
$$q_2 = -\frac{(\sqrt{2}+1)p_0p_1}{\sqrt{2p_0^2 - 3p_1^2}}, \quad w_0 = \frac{3p_1^4}{4(7p_0^4 - 18p_0^2p_1^2 + 15p_1^4)},$$
$$w_1 = \frac{p_0^4}{8(7p_0^4 - 18p_0^2p_1^2 + 15p_1^4)}, \quad w_2 = \frac{(2p_0^2 - 3p_1^2)^2}{8(7p_0^4 - 18p_0^2p_1^2 + 15p_1^4)}.$$

References

[1] B. Bajnok, On Euclidean designs, *Adv. in Geom.* **6** (2006), 423–438.

[2] B. Bajnok, Orbits of the hyperoctahedral group as Euclidean designs, *J. Algebraic Combin.* **25** (2007), 375–397.

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

[4] Ei. Bannai, Et. Bannai, M. Hirao, M. Sawa, Cubature formulas in numerical analysis and Euclidean tight designs, *European J. Combin.* **31** (2010), 423–441.

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

[6] A. Neumaier, J. J. Seidel, Discrete measures for spherical designs, eutactic stars and lattices, *Nederl. Akad. Wetensch. Proc. Ser. A* **91** (1988), 321–334.

Few distance sets and a generalization of Larman-Rogers-Seidel's theorem

東北大学大学院情報科学研究科　野崎　寛
Graduate School of Information Sciences, Tohoku University, Japan
Nozaki, Hiroshi

ユークリッド空間 $\mathbb{R}^d$ 上，またはその球面 S^{d-1} 上の,「良い」有限集合として，s 距離集合という概念がある．$X \subset \mathbb{R}^d$ が s 距離集合と呼ばれるのは，互いに異なる 2 点間の距離の種類が，ちょうど s 個のときである．つまり，

$$A(X) = \{d(x,y) \mid x,y \in X, x \neq y\} \text{ （ここで } d(x,y) \text{ はユークリッド距離）}$$

としたとき，$|A(X)| = s$ となる X を s 距離集合と呼ぶ．s 距離集合の主な問題のひとつは，s と d を固定した時に，最大の元の個数を持つ s 距離集合を与えること，または分類することである．
s 距離集合には元の個数について，次の上界が知られている．

Theorem 1 (Bannai-Bannai-Stanton(1983), Delsarte-Goethals-Seidel(1977)). (1) $X \subset \mathbb{R}^d$ が s 距離集合のとき，$|X| \leq \binom{d+s}{s}$.

(2) $X \subset S^{d-1}$ が s 距離集合のとき，$|X| \leq \binom{d+s-1}{s} + \binom{d+s-2}{s-1}$.

1 距離集合に対しては，それらの上界を達成する例として，$d+1$ 点の Regular simplex が存在している．ユークリッド空間上の上界を達成する例については，Lisoněk(1997) が与えた，$\mathbb{R}^8$ 上 45 点 2 距離集合のみである．その他の例は知られておらず，存在性についても，ほとんど分かっていない．球面上の上界を達成する例については，存在性がほとんどの場合に決定されており，s が 3 以上のとき，存在しないことが知られている．s が 2 のときは，$d = 2, 6, 22$ のとき，一意的に存在しており，その他のほとんどの次元については，未解決のまま残されている．

$M_d(s)$（resp. $M_d^*(s)$）を d 次元ユークリッド空間（resp. 球面）上の s 距離集合の元の個数の最大値とする．知られている結果は次の表の通りである．

d	2	3	4	5	6	7	8
$M_d(2)$	5	6	10	16	27	29	45

s	2	3	4	5
$M_2(s)$	5	7	9	12

$M_3(3) = 12$

d	2	3	4	5	6	$7 \cdots 21$	22	$24 \cdots 39$
$M_d^*(2)$	5	6	10	16	27	$\frac{d(d+1)}{2}$	275	$\frac{d(d+1)}{2}$

表に見られるように，距離集合の最大値の決定は，極めて難しいものであるが，$s = 2$ の場合はいくらかの結果が得られている．それは，2 距離集合においては，単純グラフからの良い埋め込みの方法が知られていることと，次にあげる Larman-Rogers-Seidel の定理に依るところが大きい．

Theorem 2 (Larman-Rogers-Seidel(1977)). $X \subset \mathbb{R}^d$ を 2 距離集合とし，$A(X) = \{a_1, a_2\}(a_1 > a_2)$ とする．$|X| \geq 2d+4$ のとき，ある正整数 k $(2 \leq k \leq 1/2 + \sqrt{d/2})$ が存在して，$a_2^2/a_1^2 = (k-1)/k$ となる．

この定理の一般化に，任意の s について成功した．

Theorem 3 ([1]). $X \subset \mathbb{R}^d$ を s 距離集合とし，$A(X) = \{a_1, a_2, \ldots, a_s\}$ とする．$|X| \geq 2\binom{d+s-1}{s-1} + 2\binom{d+s-2}{s-2}$ のとき，それぞれの $i \subset \{1, 2, \ldots, s\}$ について，

$$\prod_{j=1,2,\ldots,s, j\neq i} \frac{a_j^2}{a_j^2 - a_i^2}$$

が整数となる．また，その整数の絶対値は s と d のある関数で抑えられる．

これと同様の定理を，Johnson scheme や Hamming scheme など（一般に二点等質空間）においても，自然に与えることが出来る．

Theorem 3 を用いて，球面上の 3 距離集合の上界を改善することに成功した．特に $M_8^*(3) = 120$, $M_{22}^*(3) = 2025$ となることを示した [2]．8 次元球面最大 3 距離集合は，E_8 root system の部分集合であり，そのような集合は同型を除いても沢山ある．22 次元球面最大 3 距離集合は，Leech 格子の最小ノルムの 22 次元超平面上の部分集合から得られており，それは Q 多項式アソシエーションスキームの構造を持つことが知られている．その集合は一意であることが予想されるが，未解決である．

論文 [2] では，次の上界と Theorem 3，線形計画法による上界を組み合わせることで，球面上の s 距離集合の上界を改善する方法を任意の s について与えている．

Theorem 4 ([3])**.** $X \subset S^{d-1}$ を s 距離集合とし，その互いに異なる二点間の内積の集合を $\{b_1, b_2, \dots, b_s\}$ とする．多項式 $\prod_{i=1}^{s}(t - b_i)$ をゲーゲンバウワー多項式 $\{G_k(t)\}$ 展開したものを $\sum_{i=0}^{s} f_i G_i(t)$ とする．そのとき

$$|X| \le \sum_{i:f_i>0} h_i.$$

ここで，$h_i = \binom{d+s-1}{s} - \binom{d+s-3}{s-2}$.

Theorem 4 において，全ての f_i が正のとき，この上界は Theorem 1 (2) における上界と一致しており，内積の集合に依存することで，真に Theorem 1 (2) における上界を改善している．

論文 [2] における方法において，Theorem 4 の上界を達成する集合は最大距離集合の候補となり，その集合の特徴づけは重要な課題であった．最近の進展として，その特徴づけに成功した．

Theorem 5. $\mathcal{I} := \{l \mid f_l > 0\}$ とし，$X \subset S^{d-1}$ を上界 $|X| \le \sum_{i\in\mathcal{I}} h_i$ を達成する s 距離集合とする．互いに異なる $i, j \in \mathcal{I}$ について，

$$\sum_{x,y\in X} G_k^{(d)}(\langle x, y\rangle) = 0,$$

ここで k は $|i-j| \le k \le i+j$, $k \equiv i+j \pmod 2$ を満たす任意の整数である．また $\langle x, y\rangle$ は標準内積を表わしている．

$\sum_{x,y\in X} G_k^{(d)}(\langle x, y\rangle) = 0$ が $1 \le k \le t$ で成り立つことは，集合 X が球面 t デザインであることと同値である．つまり，Theorem 4 の上界を達成する集合は，一般には球面デザインではないものの，その部分的な性質満たす集合として特徴づけられる．

この定理を用いることで，下の次元の球面上の最大 2 距離集合の分類に成功した．

Theorem 6. (1) $8 \le d \le 39$, $d \ne 22, 23, 26, 37$ において，$d(d+1)/2$ 点最大 2 距離集合は同型を除いて一意的である．

(2) 7 次元 28 点最大 2 距離集合は同型を除いて 467 種類存在する．

(1) については，Regular simplex の辺の中点を全て取ってきた集合である．(2) については，E_8 root system の 7 次元超平面上の部分集合として与えらる．

$d = 26, 37$ については，最大 3 距離集合が強正則グラフの構造を持つことが分かっている．そのパラメーターは $d = 26$ のとき，$(351, 50, 25, 4)$，$(351, 140, 73, 44)$，$d = 37$ のとき，$(703, 72, 36, 4)$，$(703, 182, 81, 35)$ である．$(351, 50, 25, 4)$，$(703, 72, 36, 4)$ については，分類が完了しているが，残りの二つのパラメーターについては存在性さえも分かっていない．その存在性は興味深い未解決問題として残されている．

References

[1] H. Nozaki, A generalization of Larman-Rogers-Seidel's theorem, preprint, arXiv:0912.2387.

[2] O. Musin and H. Nozaki, Bounds on three- and higher-distance sets, preprint, arXiv:1005.2639.

[3] H. Nozaki and M. Shinohara, On a generalization of distance sets, *J. Combin. Theory, Ser. A*, 117 (2010), no. 7, 810–826.

Finiteness of distance sets in few dimensional spaces

鈴鹿工業高等専門学校　教養教育科　篠原雅史

d-次元ユークリッド空間 $\mathbb{R}^d$ 上の有限部分集合 X が k-距離集合であるとは, X の中の相異なる二点間の距離が丁度 k 種類出てくるときをいう. つまり, $A(X) = \{d(x,y)|x,y \in X, x \neq y\}$ としたときに, $|A(X)| = k$ となるとき, X を k-距離集合という. ここで $d(x,y)$ は $x,y \in X$ の二点間のユークリッド距離を表す. 有限集合を相似変換によって別の有限集合に移すとき, 距離の関係は保たれているのでので, 相似な 2 つの配置を同型とし, 以後その同型類について考える.

次元 d と距離の種類 k を固定した場合, 大きな頂点数を持つ距離集合をよいものとし, 次元 d と頂点数を固定した場合, 少ない距離の種類を持つ距離集合をよいものとする. そのとき, よい距離集合を特徴づけたいというのが, 距離集合における主な研究目標である. (距離の種類を固定したときの最大頂点数について, 下の表のような結果が知られている.)

平面上の距離集合対して, 次のような予想がある.

予想 (Erdős and Fishburn, 1996)
平面上の k-距離集合 ($k \geq 7$) のうち, 最大の頂点数を与えるような k-距離集合は L_Δ の部分集合である. ここで, $L_\Delta = \{a(1,0) + b(1/2, \sqrt{3}/2) : a,b \in \mathbb{Z}\}$.

この予想に関して, $k = 5,6,7$ における例を下の図に記す. この予想は, 平面上の距離集合に関して重要なものであるが, 現在のところ解決の兆しも見えないというのが現状であろう. そこで, 思い切って次元を下げて直線上で考えてみたらどうなるか, というのが本講演の一つのテーマであった. 一方, 平面上の凸集合（凸 n 角形を作るような n 点集合）における距離集合について, 次のような背景がある.

予想 (Erdős, 1946)
$(2n+1)$ 点からなる平面上の凸 n-距離集合は, 正 $(2n+1)$-角形の頂点集合に限られる.

この予想は, Altman (1963) によって解決され, さらに Fishburn (1995) は次のことを示した.

定理 (Fishburn, 1995)
$2n$ 点からなる平面上の凸 n-距離集合は, 正 $(2n+1)$-角形の部分集合か正 $2n$-角形となる.

そこで次のような問題が自然と湧きあがってくる.

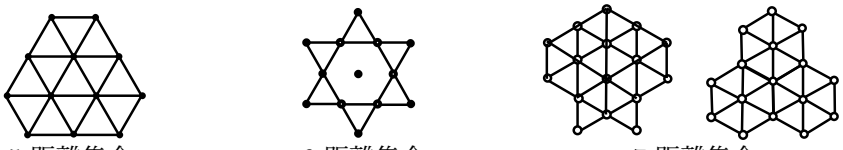
問題 (Fishburn, 1995)
与えられた n に対し, $2n$ 点からなる平面上の凸 $(n+k)$-距離集合が必ず正多角形の部分集合となるような k の最大値 $f(n)$ を求めよ.

この問題に関しても, 思い切って円周 S^1 上に限定し, そのときの最大値 $f^*(n)$ の値について考える.

d	1	2	3	4	5	6	7	8
Max	3	5	6	10	16	27	29	45

k	2	3	4	5	6
Max	5	7	9	12	13(?)

表：$k = 2$, $d = 2$ のときの最大頂点数



5-距離集合　6-距離集合　7-距離集合

図：平面上のよい距離集合（最大頂点数を与える, 最大頂点数を与える候補）の例

本講演における主結果は以下の通りである.

定理 1 直線上の k-距離集合 $X \subset \mathbb{R}^1$ ($|X| = n$) が $k \leq \lfloor \frac{3n-5}{2} \rfloor$ を満たす時, $X \subset Path(m)$ となる m が存在する. ここで $Path(m)$ は, 等間隔に並んだ m 点集合のこと.

定理 1 について, 任意の k に対して, $k = \lfloor \frac{3n-3}{2} \rfloor$ となる n 点 k-距離集合で $Path(m)$ の部分集合とはならないものが (無限個) 構成できる. またこの定理より次の系が得られる.

系 2 円周上の $2n$ 点 k-距離集合 $X \subset S^1$ が $k \leq \lfloor \frac{3n-2}{2} \rfloor$ を満たす時, X は正多角形の部分集合である.

この場合も定理 1 のときと同じように, 任意の k に対して $k = \lfloor \frac{3n}{2} \rfloor$ となる k-距離集合で正多角形の部分集合とはならないものが (無限個) 構成できる. つまり $f^*(n) = \lfloor \frac{n}{2} \rfloor - 1$ である.

最後に, 本講演のタイトルにもある, 距離集合の有限性に関する結果を述べさせていただく. 一般の d, k に対する有限性に関する結果は長い間知られていなかったが, 最近, 野崎氏によって次の結果が示された.

定理 (Nozaki, preprint)
$N = \binom{d+k-1}{k-1} + \binom{d+k-2}{k-2}$ とする. $\mathbb{R}^d$ 上の k-距離集合で $2N$ 点以上のものは同型を除いて高々有限個である.

この定理は任意の d, k に対して, 無限個存在するための頂点数の限界を与えている意味で強力である. しかし, 有限との境界を与えるには $2N$ と k の開きが大きい. $k = 2$ の場合は, 次のような結果がある.

定理 (Einhorn-Schoenberg, 1966)
$\mathbb{R}^d$ 上の 2-距離集合で $d + 2$ 点以上のものは同型を除いて高々有限個である.

任意の次元 d に対して $d + 1$ 点からなる $\mathbb{R}^d$ 上の 2-距離集合は無限個存在するため, $k = 2$ の場合, 有限と無限の境界がはっきり分かったことになる. 定理 1, 系 2 の証明をまねることで, 次のことが示せる. またこれらは境界を与えていることもわかる.

系 3 直線上の n 点 k-距離集合で $k \leq \lfloor \frac{3n-5}{2} \rfloor$ となるものは, 同型を除いて高々有限個である.

系 4 円周上の $2n$ 点 k-距離集合で $k \leq \lfloor \frac{3n-2}{2} \rfloor$ となるものは, 同型を除いて高々有限個である.

References

1 S. J. Einhorn and I. J. Schoenberg, On Euclidean sets having only two distances between points I, II, *Nederl Akad. Wetensch. Proc. Ser. A69=Indag. Math.* **28** (1966), 479–488, 489–504.

2 P. Erdős, On sets of distances of n points, *Amer. Math. Monthly*, **53** (1946), 248–250.

3 P. Erdős and P. Fishburn, Maximum planar sets that determine k distances, *Discrete Math.* , **160** (1996), 115–125.

4 P. Erdős and P. Fishburn, Distinct distances in finite planar sets, *Discrete Math.* **175** (1997), 97–132.

5 P. Fishburn, Convex nonagons with five intervertex distance, *Discrete Math.* **252** (2002), 103–122.

6 M. Shinohara, Classification of three-distance sets in two dimensional Euclidean space, *Europ. J. Combinatorics*, **25** (2004) 1039–1058.

7 M. Shinohara, Uniqueness of maximum planar five-distance sets, *Discrete Math.* **308** (2008), 3048–3055.

Optimal Fractions of Two-level Factorials under a Baseline Parametrization

Rahul Mukerjee
Indian Institute of Management Calcutta, Joka, Diamond Harbour Road, Kolkata 700 104, India
and
Boxin Tang
Department of Statistics and Actuarial Science, Simon Fraser University, Burnaby, BC V5A 1S6, Canada

Optimal fractional factorial designs have received significant attention in recent years. Traditionally, they have been studied under specific model assumptions. More recently, there has been emphasis on model robustness and optimal designs under the minimum aberration (MA) and related criteria have been explored. See Mukerjee and Wu (2006) and Xu, Phoa and Wong (2009) for reviews with focus on the regular and nonregular cases respectively.

While the aforesaid body of work is based on the foundation of the usual orthogonal parametrization (OP) for the factorial contrasts, the present paper aims at exploring optimal two-level factorial fractions under a nonorthogonal baseline parametrization (BP) which arises naturally in many practical situations. So far, full factorials under BP have been studied in microarray experiments; see Banerjee and Mukerjee (2008) and the references therein. Fractional factorials, which are often of compelling interest from consideration of experimental economy, are yet to be investigated under BP. Their study poses two challenges: (i) regular and nonregular designs have to be treated at par because of nonorthogonal parametrization, (ii) isomorphism is more complex than in OP as levels of factors are not interchangeable.

Consider a 2^m factorial with factors $F_1,\ldots,F_m$, each at levels 0 and 1. Let $\tau(j_1\ldots j_m)$ denote the effect of a typical treatment combination $j_1\ldots j_m$. Suppose there is a null state or baseline level, say 0, of each factor. Then under BP, $\tau(00\ldots0)=\theta_0$ is the baseline effect, while we have

$$\tau(100\ldots0)=\theta_0+\theta_1,\qquad \tau(010\ldots0)=\theta_0+\theta_2,\qquad \tau(110\ldots0)=\theta_0+\theta_1+\theta_2+\theta_{12},$$

etc., where θ_1 is the main effect of F_1, θ_2 is the main effect of F_2, θ_{12} is the interaction effect F_1F_2, and so on. Note that these main and interaction effects are contrasts in the $\tau(j_1\ldots j_m)$ but not orthogonal contrasts. The BP is appropriate if there is a null state or baseline level of each factor – e.g., in a toxicological study with binary factors, each representing the presence or absence of a particular toxin, the state of absence can be the natural baseline level of each factor. Indeed, a baseline level can be interpreted in a broad sense. It need not strictly mean the zero level on some scale but may as well refer to a standard or control level like the one currently used in practice. Thus in an industrial experiment on quality improvement via a change in the settings of several machines, the current settings may constitute the control levels.

In order to develop our theory, we first find optimal main effect plans under BP assuming the absence of all interactions and then, from the perspective of model robustness, minimize the contamination due to possible presence of interactions. Consider *N* experimental runs $j_{u1}\ldots j_{um}$, $1\le u\le N$. Let *Z* be an $N\times m$ array obtained by writing each run as a row. As usual, the observations are assumed to be uncorrelated with common variance σ^2.

Proposition 1. *Suppose all interactions are absent. If an N-run design keeps each of* $\theta_1,\ldots,\theta_m$ *estimable, then* $Var(\hat{\theta}_i)\ge(4/N)\sigma^2$, *where* $\hat{\theta}_i$ *is the* BLUE *of* θ_i, $1\le i\le m$. *This lower bound is attained for every* i *if and only if* Z *forms an orthogonal array* OA(*N*, *m*, 2, 2).

Proposition 2. *Suppose all interactions are absent. If Z forms an* OA(*N*, *m*, 2, 2) *then the associated design is universally optimal among all N-run designs for inference on* $\theta_1,\ldots,\theta_m$.

Because the main effects are of primary importance, we continue with designs such that the array Z forms an OA of strength two. No assumption is made now about the absence of interactions and we proceed to quantify the resulting bias of $(\hat{\theta}_1,...,\hat{\theta}_m)'$. Let Ω_s be the collection of s-tuples $g_1...g_s$, $1 \le g_1 < ... < g_s \le m$. For any $s \ge 2$ and $g_1...g_s \in \Omega_s$, define $\alpha(g_1...g_s)$ as the number of times (1 1 … 1) occurs as a row in the $N \times s$ subarray given by the g_1th,…, g_sth columns of Z. Let B_s be a certain $m \times \binom{m}{s}$ matrix with elements dictated by the $\alpha(g_1...g_s)$ and $\theta^{(s)}$ be vector of the $\binom{m}{s}$ s-factor interaction effects.

Theorem 1. *If no assumption is made about the absence of interactions then the bias or contamination of* $(\hat{\theta}_1,...,\hat{\theta}_m)'$ *as an estimator of* $(\theta_1,...,\theta_m)'$ *is given by* $\Sigma_{s=2}^{m} B_s\theta^{(s)}$.

With a view to keeping the contamination small, under the effect hierarchy principle, we look for a design that sequentially minimizes the sizes of $B_2,...,B_m$ as given by $K_s = \mathrm{tr}(B_sB_s')$; vide Tang and Deng (1999) who worked under OP. Thus the MA criterion under BP calls for sequential minimization of $K_2,...,K_m$. One can work out explicit expressions for $K_2,...,K_m$ and verify that beyond the first term K_2, no general connection exists with the corresponding sequence under OP. The values of $K_2,...,K_m$ remain unaffected under row or column permutations of Z but can get affected if the symbols in some of the columns of Z are interchanged. This shows that the class of nonisomorphic designs under BP is much larger than that under OP. Based on the detailed expressions of $K_2,...,K_m$, one can tabulate MA designs under BP for N = 8, 12 and 16. Moreover, the following result holds.

Theorem 2. *Let* $N = 4t$, $m = 4t-1$ *or* $4t-2$ *and suppose an* OA$(4t, m, 2, 2)$ *exists. Then a design has MA under BP if and only if the associated Z is an* OA$(4t, m, 2, 2)$ *with one row consisting only of zeros.*

In general, however, MA designs under BP are not characterized by Z with one row consisting only of zeros, and a counterexample exists for N = 8, m =4, where no design with such Z can have MA.

Many open problems emerge from the present work. These concern the development of more theoretical results and extension of tables to higher values of N. The former is complicated because a connection with Hadamard matrices that facilitates the proof of the Theorem 2 ceases to hold in a manageable form when one goes beyond the saturated and nearly saturated cases. The latter becomes challenging because not all combinatorially nonisomorphic OA(N, m, 2, 2) are as yet known for higher values of N. Furthermore, general factorials including mixed factorials deserve attention. There, even in the absence of all interactions, orthogonal arrays may not be optimal under BP and balanced arrays seem to be more promising.

References

[1] Banerjee, T. and Mukerjee, R. (2008). Optimal factorial designs for cDNA microarray experiments. *Ann. Appl. Statist.* **2**, 366-385.

[2] Mukerjee, R. and Wu, C.F.J. (2006). *A Modern Theory of Factorial Designs*. Springer, New York.

[3] Tang, B. and Deng, L.Y. (1999). Minimum G_2-aberration for non-regular fractional factorial designs. *Ann. Statist*. **27**, 1914-1926.

[4] Xu, H., Phoa, F.K.H. and Wong, W.K. (2009). Recent developments in nonregular fractional factorial designs. *Statist. Surveys* **3**, 18-46.

On optimal ternary linear codes

大阪府立大学大学院 理学系研究科　丸田 辰哉

An $[n,k,d]_q$ code $\mathcal{C}$ is a linear code of length n, dimension k and minimum weight d over $\mathbb{F}_q$, the field of q elements. The *weight* of a vector $\boldsymbol{x} \in \mathbb{F}_q^n$, denoted by $wt(\boldsymbol{x})$, is the number of nonzero coordinate positions in $\boldsymbol{x}$. We only consider *non-degenerate* codes having no coordinate which is identically zero.

A fundamental problem in coding theory is to find $n_q(k,d)$, the minimum length n for which an $[n,k,d]_q$ code exists. See [2] for the updated tables of $n_q(k,d)$ for some small q and k. For ternary linear codes, $n_3(k,d)$ is known for $k \leq 5$ for all d, but the value of $n_3(6,d)$ is unknown for many integer d. It is known that $n_3(6,d) = g_3(6,d)$ or $g_3(6,d)+1$ for $253 \leq d \leq 267$, $n_3(6,d) = g_3(6,d)+1$ or $g_3(6,d)+2$ for $310 \leq d \leq 312$ and $g_3(6,d) \leq n_3(6,d) \leq g_3(6,d)+2$ for $d = 302$, 303, 307-309, where $g_3(k,d) = \sum_{i=0}^{k-1} \lceil d/3^i \rceil$ is the Griesmer bound, see [3]. An $[n,k,d]_q$ code attaining the Griesmer bound is called a *Griesmer code*. Our purpose is to construct some new codes as follows.

Theorem 1. *There exist codes with parameters* $[385,6,255]_3$, $[389,6,258]_3$, $[393,6,261]_3$, $[398,6,264]_3$, $[402,6,267]_3$, $[457,6,303]_3$, $[466,6,309]_3$, $[470,6,312]_3$.

Corollary 2. (1) $n_3(6,d) = g_3(6,d)$ *for* $253 \leq d \leq 267$.
(2) $n_3(6,d) = g_3(6,d)+1$ *for* $310 \leq d \leq 312$.
(3) $n_3(6,d) = g_3(6,d)$ *or* $g_3(6,d)+1$ *for* $301 \leq d \leq 303$ *and* $307 \leq d \leq 309$.

It was shown in [3] that at least three non-equivalent Griesmer $[406,6,270]_3$ codes exist. We construct the codes in Theorem 1 from one of the $[406,6,270]_3$ codes. We refer to [3] for the geometric method to investigate linear codes over $\mathbb{F}_q$ through the projective geometry. We use the notations θ_j, γ_0, C_i, λ_i, $m_{\mathcal{C}}(S)$, $\gamma_j(\Pi)$, $\gamma_j = \gamma_j(\Sigma)$ and a_i as defined in [3].

Five of our new codes are constructed applying the following lemma.

Lemma 3. *Let* $\mathcal{C}$ *be an* $[n,k,d]_q$ *code and let* $\cup_{i=0}^{\gamma_0} C_i$ *be the partition of* $\Sigma = \mathrm{PG}(k-1,q)$ *obtained from* $\mathcal{C}$. *If* $\cup_{i \geq 1} C_i$ *contains a* t*-flat* Π *and if* $d > q^t$, *then there exists an* $[n-\theta_t, k, d-q^t]_q$ *code.*

Lemma 4. *Let* $\mathcal{C}$ *be a* $[109,5,72]_3$ *code with* $a_i = 0$ *for all* $i \notin \{1,10,19,28,37\}$ *and let* $C_0 \cup C_1 \cup C_2$ *be the partition of* $\Sigma = \mathrm{PG}(4,3)$ *obtained from* $\mathcal{C}$. *Then* $C_1 \cup C_2$ *contains a line. Furthermore, for any line* $l_1 \subset C_1 \cup C_2$, *there are two more lines* $l_2, l_3 \subset C_1 \cup C_2$ *such that* l_1, l_2, l_3 *are skew.*

Lemma 5. *Let* $\mathcal{C}$ *be a* $[136,5,90]_3$ *code and let* $C_0 \cup C_1 \cup C_2$ *be the partition of* $\Sigma = \mathrm{PG}(4,3)$ *obtained from* $\mathcal{C}$. *Then*
(1) $a_i = 0$ *for all* $i \notin \{10,19,28,37,46\}$.
(2) $C_1 \cup C_2$ *contains a plane if* $\lambda_0 = |C_0| \leq 18$.

Let $\mathcal{C}$ be a Griesmer $[406, 6, 270]_3$ code with spectrum $(a_{82}, a_{109}, a_{136}) = (1, 12, 351)$ found in [3] and let $C_0 \cup C_1 \cup C_2$ be the partition of $\Sigma = \mathrm{PG}(5, 3)$ obtained from $\mathcal{C}$. Then it is known from [3] that $(\lambda_0, \lambda_1, \lambda_2) = (51, 220, 93)$, where $\lambda_i = |C_i|$. Note that 109-hyperplanes and 136-hyperplanes correspond to $[109, 5, 72]_3$ codes and $[136, 5, 90]_3$ codes, respectively. Let Π_{109} be a 109-hyperplane. Since any j-solid in a 136-hyperplane satisfies $j \in \{10, 19, 28, 37, 46\}$ by Lemma 5, it can be checked that any j-solid in Π_{109} satisfies $j \in \{1, 10, 19, 28, 37\}$. Hence, we can take two skew lines containing no 0-points in Π_{109} by Lemma 4(1). It follows from Lemma 3 that a $[402, 6, 267]_3$ code and a $[398, 6, 264]_3$ code exist. Let b_i be the number of hyperplanes Π of Σ with $|\Pi \cap C_0| = i$. With the aid of a computer, we get

$$(b_{42}, b_{27}, b_{24}, b_{21}, b_{18}, b_{15}) = (1, 12, 12, 12, 120, 207). \tag{1}$$

Let Π_{82} be the 82-hyperplane. Since the Π_{82} contains at least 39 0-points, it contains exactly 42 0-points from (1). It can be also checked that the 109-hyperplanes contain exactly 27 0-points. Hence, a hyperplane containing exactly 18 or 15 0-points is a 136-hyperplane and it has a plane contained in $C_1 \cup C_2$ by Lemma 5. Since the number of 4-flats through a fixed plane in Σ is $\theta_2 = 13$, one can take a 136-hyperplane Π_1 through a plane δ_1 contained in $C_1 \cup C_2$ and a 109-hyperplane Π_2 so that $\Pi_2 \cap \delta$ is a line, say l_1. Actually, taking

$$\delta = \langle 120000, 001210, 110111 \rangle \subset C_1 \cup C_2,$$

it turns out that all 4-flats through δ are 136-hyperplanes, and applying Lemma 3 gives a $[393, 6, 261]_3$ code with spectrum

$$(a_{78}, a_{105}, a_{123}, a_{132}) = (1, 12, 13, 338).$$

From Lemma 4(2), we can take two lines l_2 and l_3 in Π_2 such that l_1, l_2, l_3 are skew and that $l_1 \cup l_2 \cup l_3$ is contained in $C_1 \cup C_2$. Hence we get a $[389, 6, 258]_3$ code and a $[385, 6, 255]_3$ code applying Lemma 3 again. Indeed, taking $l_2 = \langle 010101, 100001 \rangle$, we get a $[389, 6, 258]_3$ code with spectrum

$$(a_{77}, a_{101}, a_{104}, a_{119}, a_{122}, a_{128}, a_{131}) = (1, 2, 10, 1, 12, 37, 301),$$

and taking $l_3 = \langle 110000, 000101 \rangle$ gives a $[385, 6, 255]_3$ code with spectrum

$$(a_{76}, a_{97}, a_{103}, a_{118}, a_{121}, a_{124}, a_{127}, a_{130}) = (1, 2, 10, 2, 11, 2, 70, 266).$$

Applying the following well-known lemma, we get a $[457, 6, 303]_3$ code, a $[466, 6, 309]_3$ code and a $[470, 6, 312]_3$ code.

Lemma 6 ([1]). *Let $\mathcal{C}_1$ be an $[n_1, k, d_1]_q$ code and $\mathcal{C}_2$ be an $[n_2, k-1, d_2]_q$ code. If $\mathcal{C}_1$ has a codeword c with $wt(c) \geq d_1 + d_2$, then an $[n_1 + n_2, k, d_1 + d_2]_q$ code $\mathcal{C}_3$ exists.*

References

[1] R. Hill, D.E. Newton, Optimal ternary linear codes, *Des. Codes Cryptogr.* **2** (1992) 137–157.

[2] T. Maruta, Griesmer bound for linear codes over finite fields, http://www.geocities.jp/mars39geo/griesmer.htm.

[3] M. Takenaka, K. Okamoto, T. Maruta, On optimal non-projective ternary linear codes, *Discrete Math.* **308** (2008) 842–854.

On Separable Codes

Department of Social Systems and Management Faculty of Systems and Information Engineering, University of Tsukuba: Minquan Cheng

School of Mathematical Sciences, Suzhou University: Lijun Jin

Department of Social Systems and Management Faculty of Systems and Information Engineering, University of Tsukuba Ying Miao

Coding providing certain forms of traceability to protect multimedia contents against piracy has been extensively studied in recent years [2, 8]. In order to hinder averaging attack which is one of the commonly used collusion attacks, the notion of a t-resilient AND anti-collusion code (t-AND-ACC) was proposed by Trappe et al. [11, 12] to detect, with code modulation, up to t malicious users taking part in the averaging attack. Several constructions for t-AND-ACCs can be found in, for example, [11, 12, 5, 7, 3]. Unfortunately, the number of codewords in a t-AND-ACC, which corresponds to the number of fingerprints assigned to authorized users, is too small to be used in a multimedia fingerprinting system with a large number of users .

To overcome the shortcomings but keep the advantages of t-AND-ACCs, Cheng and Miao [3] introduced a new concept of t-resilient logical anti-collusion code (t-LACC). t-LACCs have weaker requirements than t-AND-ACCs but they have the same traceability as t-AND-ACCs do. In [3], Cheng and Miao also introduced the definition of a $\bar{t}$-separable code ($\bar{t}$-SC), showed that a binary $\bar{t}$-SC is in fact equivalent to a t-LACC, and explained how $\bar{t}$-SCs can be used to construct t-LACCs. Their efficient detection algorithm [3] based on a special type of t-LACCs works well for a large multimedia fingerprinting system to identify up to t malicious users taking part in the averaging attack.

In this paper, we focus our attention on combinatorial constructions of $\bar{t}$-SCs. Combinatorial constructions for other types of collusion-secure codes can be found in [10, 9]. We first exhibit some basic definitions of collusion-secure codes used in multimedia fingerprinting, then show several preliminary results on $\bar{t}$-SCs, including several upper bounds on the number of codewords in a $\bar{t}$-SC. The composition construction for binary $\bar{t}$-SCs, that is, t-LACCs, stimulates us to investigate $\overline{2}$-SCs with short lengths. We also investigate $\overline{2}$-SCs of length 2, and show that any projective plane can yield an optimal $\overline{2}$-SC of length 2. Optimal $\overline{2}$-SCs of length 3 will been explicitly constructed by means of cyclic difference matrices.

Theorem 0.1 (1) There exists an optimal $\overline{2}$-SC$(2, M, q)$ with $M = \frac{q(1+\sqrt{4q-3})}{2}$ for any prime power $\frac{\sqrt{4q-3}-1}{2}$.

(2) $M(\overline{2}, 2, 43) \leq 300$; $M(\overline{2}, 2, 111) \leq 1220$.

Theorem 0.2 There exists an optimal $\overline{2}$-SC$(3, q^2 + \frac{q(q-1)}{2}, q)$ for any odd integer q.

Theorem 0.3 There exists an optimal $\overline{2}$-SC$(3, q^2 + \frac{q(q-1)}{2}, q)$ for any even integer q.

References

[1] S. R. Blackburn, "Frameproof codes," *SIAM J. Discrete Math.*, vol. 16, no. 3, pp. 499-510, 2003.

[2] D. Boneh and J. Shaw, "Collusion-secure fingerprinting for digital data," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1897-1905, 1998.

[3] M. Cheng and Y. Miao, "On anti-collusion codes and detection algorithms for multimedia fingerprinting," *IEEE Trans. Inform. Theory*, conditionally accepted, 2010.

[4] C. J. Colbourn and J.H. Dinitz (Eds.), "CRC Handbook of Combinatorial Designs," CRC Press, Boca Raton, FL, 1996, pp. 270-287.

[5] J. Dittmann, P. Schmitt, E. Saar, J. Schwenk and J. Ueberberg, "Combining digital watermarks and collusion secure fingerprints for digital images," *SPIE J. Electron. Imag.*, vol. 9, no. 4, pp. 456-467, 2000.

[6] D.-Z. Du and F. K. Hwang, "Pooling Designs and Nonadaptive Group Testing: Important Tools for DNA Sequencing," World Scientific, Singapore, 2006.

[7] Q. Li, X. Wang, Y. Li, Y. Pan and P. Fan, "Construction of anti-collusion codes based on cover-free families," in *2009 Sixth Int. Conf. Inform. Tech.: New Generations*, pp. 362-365, Las Vegas, NV, 2009.

[8] K. J. R. Liu, W. Trappe, Z. J. Wang, M. Wu and H. Zhao, "Multimedia Fingerprinting Forensics for Traitor Tracing," Hindawi, NY, 2005.

[9] J. N. Staddon, D. R. Stinson and R. Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 3, pp. 1042-1049, 2001.

[10] D. R. Stinson, Tran van Trung and R. Wei, "Secure frameproof codes, key distribution patterns, group testing algorithms and related structures," *J. Statist. Planning Inferenece*, vol. 86, pp. 595-617, 2000.

[11] W. Trappe, M. Wu and K. J. R. Liu, "Collusion-resistant fingerprinting for multimedia," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process.*, pp. 3309-3321, Orlando, FL, 2002.

[12] W. Trappe, M. Wu, Z. J. Wang and K. J. R. Liu, "Anti-collusion fingerprinting for multimedia," *IEEE Trans. Signal Process.*, vol. 51, no. 4, pp. 1069-1087, 2003.

Existence of affine α-resolvable PBIB designs with some constructions

松江工業高等専門学校　　門脇　聖
広島工業大学環境学部　　景山　三平

ブロックデザインにおける分解可能性の構造は，数学的には 1850 年に考えられ，その統計的利用は 1939 年より始まった．また，この概念は 1963 年に α-分解可能性へと一般化されている．一方，実験計画法における種々のブロックデザインの中で，釣合い型不完備ブロックデザイン（Balanced Incomplete Block design, 以下 BIB デザイン）と部分釣合い型不完備ブロックデザイン（Partially BIB デザイン，以下 PBIB デザイン）がよく扱われ，多くの研究者によってそれらのデザインの特徴づけや構成に関する研究が行われてきた．

アフィン α-分解可能 PBIB デザインの特徴づけ及び存在問題について，特にアフィン 1-分解可能 2-アソシエート PBIB デザインの構成に関して Clatworthy は，2-アソシエート PBIB デザインの存在性を v　100 かつ r, k　10 の範囲内でその結果をまとめている．しかし，Clatworthy による研究ではデザインの具体的な解が与えられているものの，その構成法が詳述されていないために，パラメータ値の適用範囲を拡大できないという制約があった．多くの研究者によって一般的な構成法に関する研究が行われてきたが，体系としてまとめるまでには至っていない．そこで門脇，景山は，r, k を 20 まで拡大して，アフィン 1-分解可能 2-アソシエート PBIB デザインの特徴づけ及び存在性に関する研究を行った．

2-アソシエートである PBIB design は主に group divisible（GD），Triangular，Latin-square（L_2），cyclic の４つのタイプに分類され，GD はさらに SGD，SRGD，RGD の３つの部分クラスに分類される．これらのデザインについて，affine α-分解可能の性質をもつデザインの不存在性について，以下の定理が示される．

Theorem 1.1. 任意の α　1 に対して，affine α-分解可能 cyclic 2-アソシエート PBIB デザイン は存在しない．ただし，α　1.

Theorem 1.2 (Kageyama, 2007, 2008b). 1　α　10 の場合，affine α-分解可能 triangular デザインは存在しない．

Theorem 1.4 (Kageyama, 2008a). 任意の α　1 に対して，affine α-分解可能 RGD デザインは存在しない．

以上のことから，affine α-分解可能の性質をもつ SGD，SRGD，L_2 のデザインの存在性について考察した．

パラメータの特徴付けとして，まず affine α-分解可能 SGD デザインに対して次の結果が得られた．

Theorem 2.1.2. affine α-分解可能 SGD デザインのパラメータは

$$v = mn, b = \frac{\beta(m \quad 1)}{\beta \quad 1}, r = \frac{\alpha(m \quad 1)}{\beta \quad 1}, k = \frac{\alpha mn}{\beta}, \lambda_1 = \frac{\alpha(m \quad 1)}{\beta \quad 1}, \lambda_2 = \frac{\alpha(\alpha m \quad \beta)}{\beta(\beta \quad 1)};\ t = \frac{m \quad 1}{\beta \quad 1}, q_2 = \frac{\alpha^2 mn}{\beta^2}$$

によって与えられる．ただし，$\alpha m/\beta$ は整数である．

この結果から，v　100 かつ r, k　20 の範囲での affine α-分解可能 SGD デザインの $\alpha = 1$ の場合に限定したパラメータの表が得られた．

次に，affine α-分解可能 SRGD デザインに対しても同様に，パラメータの特徴付けを行い，次の結果を得た．

Theorem 2.2.1. affine α-分解可能 SRGD デザインのパラメータは

$$v = mn, b = \frac{\beta m(n \quad 1)}{\beta \quad 1}, r = \frac{\alpha m(n \quad 1)}{\beta \quad 1}, k = \frac{\alpha mn}{\beta}, \lambda_1 = \frac{\alpha m(\alpha n \quad \beta)}{\beta(\beta \quad 1)}, \lambda_2 = \frac{\alpha^2 m(n \quad 1)}{\beta(\beta \quad 1)}; t = \frac{m(n \quad 1)}{\beta \quad 1}, q_2 = \frac{\alpha^2 mn}{\beta^2}$$

によって与えられる．ただし，$\alpha n/\beta$ は整数である．

この結果より，affine α-分解可能 SGD デザインの場合と同様，$v \quad 100$ かつ $r, k \quad 20$ の範囲での affine α-分解可能 SRGD デザインの $\alpha = 1$ の場合に限定し，そのデザインが存在可能であるパラメータを導き，これまでに存在が不明であったいくつかのデザインの構成方法についての考察を行った．その考察からいくつかの結果を得ることができた．次はその結果の一つである．

Theorem 2.2.2. 位数 $2x$ のアダマール行列が存在することとパラメータ $v = b = 4x, r = k = 2x, \ _1 = 0, \ _2 = x, q_1 = 0, q_2 = x; m = 2x, n = 2$ をもつ affine 分解可能対称型 SRGD デザインが存在することは同値である．

以上の結果から，$v \quad 100$ かつ $r, k \quad 20$ の範囲での affine α-分解可能 SRGD デザインの $\alpha = 1$ の場合に限定したパラ－メータの表が得られた．

さらに，$r + (s \quad 2) \ _1 \quad (s \quad 1) \ _2 = 0$ かつ $r \quad 2 \ _1 + \ _2 > 0$ を満たす affine α-分解可能 L_2 デザインに対しても同様に，パラメータの特徴付けを行い，次の結果を得た．

Theorem 2.3.1. $r + (s \quad 2) \ _1 \quad (s \quad 1) \ _2 > 0$ かつ $r \quad 2 \ _1 + \ _2 > 0$ であるならば，任意の $\alpha \quad 1$ に対して affine α-分解可能 L_2 デザインは存在しない．

この結果より，affine α-分解可能 SRGD デザインの場合と同様に $r + (s \quad 2) \ _1 \quad (s \quad 1) \ _2 = 0$ かつ $r \quad 2 \ _1 + \ _2 > 0$ または $r + (s \quad 2) \ _1 \quad (s \quad 1) \ _2 > 0$ かつ $r \quad 2 \ _1 + \ _2 = 0$ を満たす $\alpha = 1$ の affine α-分解可能 L_2 デザインが存在可能であるパラメータを導き，これまでに存在が不明であったいくつかのデザインの構成方法についての考察を行った．その考察から，以下の結果を得た．

Theorem 2.3.2. パラメータ $v = b = n^2, r = k = n, \ _1 = 0, \ _2 = 1, q_1 = 0, q_2 = 1; m = n$ をもつ affine 分解可能対称型 SRGD デザインが存在することとパラメータ $v^* = n^2, b^* = n(n \quad 1), r^* = n \quad 1, k^* = n, \ ^*_1 = 0, \ ^*_2 = 1, q_1^* = 0, q_2^* = 1$ をもつ $r + (s \quad 2) \ _1 \quad (s \quad 1) \ _2 = 0$ かつ $r \quad 2 \ _1 + \ _2 > 0$ を満たす affine α-分解可能 L_2 デザインが存在することは同値である．

Theorem 2.3.3. パラメータ $v = \beta^2, b = 2\beta, r = 2, k = \beta, \ _1 = 1, \ _2 = 0, q_1 = 0, q_2 = 1$ をもつ $r + (s \quad 2) \ _1 \quad (s \quad 1) \ _2 > 0$ かつ $r \quad 2 \ _1 + \ _2 = 0$ を満たす affine 分解可能 L_2 デザインが存在する．

以上の結果から，2-アソシエートである affine α-分解可能 PBIB デザインの $\alpha = 1$ の場合に限定した存在性に関して，$v \quad 100$ かつ $r, k \quad 20$ の範囲で存在が不明であるデザインは 3 つ（SRGD デザインが 2 つ，L_2 デザインが 1 つ）のみという結果を得た．

Graham-Winkler によるグラフの等長埋め込み問題とその一般化

渡部里織　名古屋大学　情報文化学部
澤正憲　名古屋大学　情報科学研究科

グラフの分解問題は，数学だけでなく工学など様々な分野において盛んに研究されてきた．その１つである完全グラフの分解問題は，グラフ理論やデザイン理論などの組合せ数学の分野において特に重要である．

定理 1 完全グラフ K_n を互いに辺素な完全二部グラフ（必ずしも同型でない）に分解すると，その分解に必要な二部グラフの個数は $n-1$ 以上になる．

この問題は，グラフの等長埋め込み問題に帰着させて解くことができる．d を通常のグラフ距離とする．$A_q = \{0, 1, \cdots, q-1, *\}$ とし，その L 重直積を A_q^L とする．$a = (a_1, a_2, \cdots, a_L), b = (b_1, b_2, \cdots, b_L) \in A_q^L$ に対して, $d_H(a, b) = |\{i : 1 \leq i \leq L, a_i \neq b_i, a_i \neq *, b_i \neq *\}|$ と定義する．グラフ G の頂点集合を V とする．任意の $v_i, v_j \in V$ について，

$$d(v_i, v_j) = d_H(a_i, a_j)$$

となるように符号語 $a_i, a_j \in A_q^L$ を割り当てられるとき，G は長さ L の q- アドレス付け可能であるという．$q = 2$ のときこの問題は Graham と Pollak によって提示された [2]．我々はそれを q シンボルに拡張した．q シンボルに拡張する意義は，グラフの最小符号長 $N_q(G)$ を小さくできる場合があるということである．まず，N_q についての評価下界を紹介する．$\mathrm{diam}(G)$ を G の直径とする．つまり，$v, u \in V$ のとき $\mathrm{diam}(G) = \max d(v, u)$.

定理 2 $n_+(G), n_-(G)$ をそれぞれ G の距離行列の正の固有値の数，負の固有値の個数とする．

$$N_q(G) \geq \max\left\{\left\lceil \frac{n_+(G)}{q-1} \right\rceil, \left\lceil \frac{n_-(G)}{q-1} \right\rceil, \mathrm{diam}(G)\right\}$$

この評価不等式は $q = 2$ のとき，Graham と Pollak によって示されている [2]．頂点数 n の木 T_n や完全グラフ K_n に対して，$N_2(T_n) = n-1$，$N_2(K_n) = n-1$ であることがよく知られている．

次に Graham と Winkler による等長埋め込み問題に触れる [3]．有限集合 X, Y に対して，距離空間 $(X, d_X), (Y, d_Y)$ 考える．(X, d_X) が (Y, d_Y) に等長埋め込み可能であるとは，ある写像 $f : X \to Y$ が存在し，任意の $x, x' \in X$ に対して $d_X(x, x') = d_Y(f(x), f(x'))$ が成り立つということである，グラフの等長埋め込み問題とは，$(V(G), d)$ が $(\{0, 1, \cdots, q-1\}^L, d_H)$ に等長埋め込み可能であるような G を分類し，それが可能である場合最小の符号長 L を決定するというものである．L を埋め込み次元と言い，$\dim(G)$ と表す．この問題は，前に登場した Graham と Pollak の問題の $*$ を用いない場合である．定理 2 から $\dim(G)$ に関して次のような評価不等式が得られる．

定理 3

$$\dim(G) \geq \max\left\{\left\lceil \frac{n_+(G)}{q-1} \right\rceil, \left\lceil \frac{n_-(G)}{q-1} \right\rceil, \mathrm{diam}(G)\right\}$$

次に最小の q 値アドレス付けの系列を与えよう．K_r が木のように高々１点を共有しながら連結しているグラフを r-hypertree という [5]．次のことを示した．

定理 4 G が r-hypertree ならば，$n_+(G) = 1, n_-(G) = |V(G)| - 1$ である．

定理 4 は r-hypertree の構造に関わらず成り立つことを注意しておく．また，定理 4 と定理 2 より G が r-hypertree ならば $N_q(G) \geq \left\lceil \frac{|V(G)|-1}{q-1} \right\rceil$ であることがわかる．さらに特別な q に対して等号が成り立つ．

系 1 G を r-hypertree とする．このとき，
(i) $N_r(G) = \left\lceil \frac{|V(G)|-1}{r-1} \right\rceil$
(ii) r が奇数のとき，$N_{\frac{r+1}{2}}(G) = \left\lceil \frac{|V(G)|-1}{\frac{r+1}{2}} \right\rceil$

最後に，定理 1 とグラフの等長埋め込み問題との等価性を考える．完全二部グラフ分解された K_n から埋め込み行列 (行ベクトルが各頂点に割り当てられている符号語である行列) を作ることができる．これは逆も成り立つ．よって分解の個数は $N_2(K_n) = n - 1$ 以上になることが分かる．また，次のことも示した．

定理 5

$$N_q(K_n) = \left\lceil \frac{n-1}{q-1} \right\rceil$$

定理 5 から K_n の完全 q 部グラフ分解に必要な q 部グラフの最小個数は $\lceil (n-1)/(q-1) \rceil$ であることがわかる．

参考文献

[1] J. H. van Lint, R. M. Wilson. *A Course in Combinatorics* (2nd ed.). Cambridge University Press, 2001.

[2] R. L. Graham, H. O. Pollak. On the addressing problem for loop switching. *Bell System Tech. J.*, **50** (1971), 2495–2519.

[3] R. L. Graham, P. M.Winkler. On isometric embeddings of graphs. *Trans. Amer. Math. Soc.,* **288** (1985), 527–536.

[4] J. R. Elzinga, A. D. Gregory, M. Vander, N. Kevin. Addressing the Petersen graph. *Discrete Math.*, **286** (2004), 241–244.

[5] Sivasubramanian, Sivaramakrishnan. q-analogs of distance matrices of 3-hypertrees. *Linear Algebra Appl.*, **431** (2009), 1234–1248.

CHARACTERIZATION OF PARTIALLY BALANCED FRACTIONAL $2^{m_1+m_2}$ FACTORIAL DESIGNS OF RESOLUTION R({00,10,01,11})

Hiromu Yumiba[1], Yoshifumi Hyodo[1,2] and Masahide Kuwada[1]

[1] *International Institute for Natural Sciences*
[2] *Okayama University of Science*

The concept of a balanced array (BA), which is a generalization of an orthogonal array, was first introduced by Chakravarti (1956; *Sankhya*) as a partially BA. However it is a generalization of the BIB design rather than the PBIB design. Thus Srivastava and Chopra (1971; *AMS*) called it a BA. As a special case of an asymmetrical BA given by Nishii (1981; *HMJ*), a partially BA (PBA) of 2 symbols and m_1+m_2 constraints was introduced by Kuwada (1988; *JSPI*). A PBA of full strength is said to be simple, and it is briefly denoted by SPBA(m_1+m_2;{ λ_{i_1,i_2} }), where λ_{i_1,i_2} are the indices of an SPBA.

Let T be a fractional factorial design with m_1+m_2 factors each at two levels and N assemblies (or treatment combinations), where $m_k \geq 2$ (k=1,2), and non-negligible factorial effects are the general mean(=$\boldsymbol{\theta}_{00}$, say), the main effect(=$\boldsymbol{\theta}_{10}$, say) of the m_1 factors, the main effect(=$\boldsymbol{\theta}_{01}$, say) of the m_2 factors, and the two-factor interaction(=$\boldsymbol{\theta}_{11}$, say) between the m_1 and m_2 factors. Then the linear model is given by $\boldsymbol{y}(T)=E_T\boldsymbol{\Theta}+\boldsymbol{e}_T$, where $\boldsymbol{y}(T)$ is the $N\times 1$ observation vector, E_T is the design matrix of size $N\times\nu(m_1,m_2)$, $\boldsymbol{\Theta}'=(\boldsymbol{\theta}_{00}';\boldsymbol{\theta}_{10}';\boldsymbol{\theta}_{01}';\boldsymbol{\theta}_{11}')$ is the $\nu(m_1,m_2)\times 1$ vector of non-negligible factorial effects, 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 $\nu(m_1,m_2)=(m_1+1)(m_2+1)$ and A' denotes the transpose of a matrix A. Thus 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 $\nu(m_1,m_2)$.

Consider the matrices $D_{\beta_1\beta_2}^{\#(a_1a_2,b_1b_2)}$ given by some linear combination of the ordered association matrices $D_{\alpha_1\alpha_2}^{(a_1a_2,b_1b_2)}$ of order $\nu(m_1,m_2)$ of the extended triangular multidimensional partially balanced (ETMDPB) association scheme, where if $\beta_1\beta_2$=00, then a_1a_2,b_1b_2=00,10,01,11, if $\beta_1\beta_2$=10, then a_1a_2, b_1b_2=10,11, if $\beta_1\beta_2$=01, then a_1a_2,b_1b_2=01,11, and if $\beta_1\beta_2$=11, then $a_1a_2=b_1b_2$=11.

Let $\mathcal{A}=[\,D_{\alpha_1\alpha_2}^{(a_1a_2,b_1b_2)}]$, then $\mathcal{A}=[\,D_{\beta_1\beta_2}^{\#(a_1a_2,b_1b_2)}]$. Note that $\mathcal{A}$ is called the ETMDPB association algebra. Further let $\mathcal{A}_{00}=[\,D_{00}^{\#(a_1a_2,b_1b_2)} \mid a_1a_2,b_1b_2=00,10,01,11]$, $\mathcal{A}_{10}=[\,D_{10}^{\#(a_1a_2,b_1b_2)} \mid a_1a_2,b_1b_2=10,11]$, $\mathcal{A}_{01}=[\,D_{01}^{\#(a_1a_2,b_1b_2)} \mid a_1a_2,b_1b_2=01,11]$ and $\mathcal{A}_{11}=[\,D_{11}^{\#(11,11)}]$. Then we have the following (e.g., Kuwada (1988); *JSPI*):

Proposition. (I) *The* ETMDPB *association algebra* $\mathcal{A}$ *generated by twenty-five matrices* $D_{00}^{\#(a_1a_2,b_1b_2)}$, $D_{10}^{\#(a_1a_2,b_1b_2)}$, $D_{01}^{\#(a_1a_2,b_1b_2)}$ *and* $D_{11}^{\#(11,11)}$ *is the semisimple and completely reducible matrix algebra containing the identity matrix of order* $\nu(m_1,m_2)$.
(II) *The* $\mathcal{A}_{\beta_1\beta_2}$ ($\beta_1\beta_2$=00,10,01,11) *are the minimal two-sided ideals of* $\mathcal{A}$.
(III) *The* $\mathcal{A}$ *is decomposed into the direct sum of four two-sided ideals* $\mathcal{A}_{\beta_1\beta_2}$ *of* $\mathcal{A}$.
(IV) *The ideals* $\mathcal{A}_{00}$, $\mathcal{A}_{10}$, $\mathcal{A}_{01}$ *and* $\mathcal{A}_{11}$ *have* $D_{00}^{\#(a_1a_2,b_1b_2)}$, $D_{10}^{\#(a_1a_2,b_1b_2)}$, $D_{01}^{\#(a_1a_2,b_1b_2)}$ *and* $D_{11}^{\#(11,11)}$ *as their bases*, *respectively*, *and they are isomorphic to the complete* 4×4, 2×2, 2×2 *and* 1×1 *matrix algebras with multiplicities* 1(=ϕ_{00}, *say*), m_1-1(=ϕ_{10}, *say*), m_2-1(=ϕ_{01}, *say*) *and* $(m_1-1)(m_2-1)$(=ϕ_{11}, *say*), *respectively*.

The information matrix M_T is given by $M_T=\sum_{\beta_1\beta_2}\sum_{a_1a_2}\sum_{b_1b_2}\kappa_{\beta_1\beta_2}^{a_1a_2,b_1b_2}D_{\beta_1\beta_2}^{\#(a_1a_2,b_1b_2)}$, where T is an SPBA(m_1+m_2;{ λ_{i_1,i_2} }) and $\kappa_{\beta_1\beta_2}^{a_1a_2,b_1b_2}$ are given by some linear combination of λ_{i_1,i_2}. From Proposition, M_T is isomorphic to $\|\kappa_{\beta_1\beta_2}^{a_1a_2,b_1b_2}\|$(= $K_{\beta_1\beta_2}$, say), and hence we get the following:

Lemma 1. *Let* T *be an* SPBA(m_1+m_2;{ λ_{i_1,i_2} }). *Then the information matrix* M_T *is non-singular*, *i.e.*, T *is a partially balanced fractional* $2^{m_1+m_2}$ *factorial* ($2^{m_1+m_2}$-PBFF) *design of resolution* R({00,10,01,11}), *if and only if* $K_{\beta_1\beta_2}$ ($\beta_1\beta_2$=00,10,01,11) *are non-singular*, *i.e.*, rank{K_{00}}=4, rank{K_{10}}=rank{K_{01}}=2 *and* rank{K_{11}}=1.

Let T be an SPBA(m_1+m_2;{ λ_{i_1,i_2} }), and further let F_{00}, F_{10}, F_{01} and $\boldsymbol{F}_{11}$ be a $4\times(m_1+1)(m_2+1)$ matrix, a $2\times(m_1-1)(m_2+1)$ one, a $2\times(m_1+1)(m_2-1)$ one and a $1\times(m_1-1)(m_2-1)$ vector such that a 4×1 vector $\boldsymbol{F}_{00}(x,y)$ of F_{00}, a 2×1 one $\boldsymbol{F}_{10}(x,y)$ of F_{10}, a 2×1 one $\boldsymbol{F}_{01}(x,y)$ of F_{01} and an element $F_{11}(x,y)$ of F_{11} are given by $\boldsymbol{F}_{00}(x,y)=\sqrt{\lambda_{x,y}}\,(1\ \ m_1-2x\ \ m_2-2y\ \ (m_1-2x)(m_2-2y))'$ for $(x,y)\in V_{00}$, $\boldsymbol{F}_{10}(x,y)=\sqrt{\lambda_{x,y}}\,(1\ \ m_2-2y)'$ for $(x,y)\in V_{10}$, $\boldsymbol{F}_{01}(x,y)=\sqrt{\lambda_{x,y}}\,(1\ \ m_1-2x)'$ for $(x,y)\in V_{01}$ and $F_{11}(x,y)=\sqrt{\lambda_{x,y}}$ for $(x,y)\in V_{11}$, respectively. Here $V_{\beta_1\beta_2}$ are the sets of the lattice points (x,y) such that $V_{00}=\{(x,y) \mid 0\leq x\leq m_1,\ 0\leq y\leq m_2\}$, $V_{10}=\{(x,y) \mid 1\leq x\leq m_1-1,\ 0\leq y\leq m_2\}$, $V_{01}=\{(x,y) \mid 0\leq x\leq m_1,\ 1\leq y\leq m_2-1\}$ and $V_{11}=\{(x,y) \mid 1\leq x\leq m_1-1,\ 1\leq y\leq m_2-1\}$, where x and y are non-negative integers. Then we have the following (e.g., Kuwada *et al*. (2006); *JJSS*):

Theorem 1. *Let T be an* SPBA($m_1+m_2;\{\lambda_{i_1,i_2}\}$), *where* $m_k\geq 2$ (k=1,2). *Then the matrices* $K_{\beta_1\beta_2}$ ($\beta_1\beta_2$ =00,10,01,11) *can be expressed as* $K_{\beta_1\beta_2}=(D_{\beta_1\beta_2}F_{\beta_1\beta_2}\Lambda_{\beta_1\beta_2})(D_{\beta_1\beta_2}F_{\beta_1\beta_2}\Lambda_{\beta_1\beta_2})'$, *where* $D_{\beta_1\beta_2}$ *and* $\Lambda_{\beta_1\beta_2}$ *are some non-singular diagonal matrices*.

It follows from Theorem 1 that rank$\{K_{\beta_1\beta_2}\}$=r-rank$\{F_{\beta_1\beta_2}\}$ ($\beta_1\beta_2$=00,10,01,11), where r-rank$\{A\}$ denotes the row rank of a matrix A. Thus from Lemma 1, the following is immediately:

Lemma 2. *Let T be an* SPBA($m_1+m_2;\{\lambda_{i_1,i_2}\}$). *Then T is a* $2^{m_1+m_2}$-PBFF *design of resolution* R({00,10, 01,11}) *if and only if* r-rank$\{F_{00}\}$=4, r-rank$\{F_{10}\}$=r-rank$\{F_{01}\}$=2 *and* r-rank$\{F_{11}\}$=1.

Let $SV_{\beta_1\beta_2}$ ($\beta_1\beta_2$=00,10,01,11) be the subsets of $V_{\beta_1\beta_2}$ such that the indices $\lambda_{x,y}$ of an SPBA are non-zero for $(x,y)\in V_{\beta_1\beta_2}$. Then we obtain the following:

Lemma 3. *Let T be an* SPBA($m_1+m_2;\{\lambda_{i_1,i_2}\}$). *Then* r-rank$\{(\boldsymbol{F}_{00}(x_1,y_1)\ \boldsymbol{F}_{00}(x_2,y_2)\ \boldsymbol{F}_{00}(x_3,y_3)\ \boldsymbol{F}_{00}(x_4,y_4))\}$ =r-rank$\{F_{00}((x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4))\}$ *for* $(x_i,y_i)\in SV_{00}$ (i=1,2,3,4), r-rank$\{(\boldsymbol{F}_{10}(x_1,y_1)\ \boldsymbol{F}_{10}(x_2,y_2))\}$ =r-rank$\{F_{10}((x_1,y_1),(x_2,y_2))\}$ *for* $(x_i,y_i)\in SV_{10}$ (i=1,2), r-rank$\{(\boldsymbol{F}_{01}(x_1,y_1)\ \boldsymbol{F}_{01}(x_2,y_2))\}$=r-rank$\{F_{01}((x_1,y_1),(x_2,y_2))\}$ *for* $(x_i,y_i)\in SV_{01}$ (i=1,2) *and* r-rank$\{\boldsymbol{F}_{11}(x,y)\}$=r-rank$\{F_{11}(x,y)\}$=1 *for* $(x,y)\in SV_{11}$, *where*
$F_{00}((x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4))$=(*the* i^{th} *column vector*=$(1\ x_i\ y_i\ x_iy_i)'$ (i=1,2,3,4)) *for* $(x_i,y_i)\in SV_{00}$,
$F_{10}((x_1,y_1),(x_2,y_2))$=(*the* i^{th} *column vector*=$(1\ y_i)'$ (i=1,2)) *for* $(x_i,y_i)\in SV_{10}$, *and*
$F_{01}((x_1,y_1),(x_2,y_2))$=(*the* i^{th} *column vector*=$(1\ x_i)'$ (i=1,2)) *for* $(x_i,y_i)\in SV_{01}$.

From Lemmas 2 and 3, we get the following useful lemma:

Lemma 4. *Let T be an* SPBA($m_1+m_2;\{\lambda_{i_1,i_2}\}$). *Then*
(I) r-rank$\{F_{00}\}$=4 *if and only if there exist at least four indices* λ_{x_i,y_i} (i=1,2,3,4) *such that* $|F_{00}((x_1,y_1),(x_2,y_2),(x_3,y_3),(x_4,y_4))|\neq 0$ *for* $(x_i,y_i)\in SV_{00}$, *where* $|A|$ *denotes the determinant of a matrix* A, *i.e.*,
 (i) *if* $\alpha x_p+\beta y_p=\alpha x_q+\beta y_q=\alpha x_r+\beta y_r(=d_{pqr}$, *say) for some* α *and* β, *then* $\alpha x_s+\beta y_s\neq d_{pqr}$, *where* $\alpha\beta\neq 0$ *and* $\{p,q,r,s\}=\{1,2,3,4\}$, *and*
 (ii) *if any three of four* $\alpha^* x_i+\beta^* y_i$ *are not all the same for any* α^* *and* β^*, *and furthermore*
  (1) *if* $x_p=x_q\neq x_r$ ($y_p\neq y_q$), *then* $y_s\neq y_r$ (*and* $x_s\neq x_p(=x_q)$),
  (2) *if* $y_p=y_q\neq y_r$ ($x_p\neq x_q$), *then* $x_s\neq x_r$ (*and* $y_s\neq y_p(=y_q)$), *and*
  (3) *if* $x_i\neq x_j$ *and* $y_i\neq y_j$ *for any* $\{i,j\}\subset\{1,2,3,4\}$, *then* $2h_{pqr}x_sy_s+2f_{pqr}x_s+2g_{pqr}y_s+c_{pqr}\neq 0$, *where* $2h_{pqr}=|$*the* i^{th} *column vector*=$(1\ x_i\ y_i)'$ (i=p,q,r)$|$, $2f_{pqr}=|$*the* i^{th} *column vector*=$(1\ y_i\ x_iy_i)'$ (i=p,q,r)$|$, $2g_{pqr}=-|$*the* i^{th} *column vector*=$(1\ x_i\ x_iy_i)'$ (i=p,q,r)$|$, *and* $c_{pqr}=-|$*the* i^{th} *column vector*=$(x_i\ y_i\ x_iy_i)'$ (i=p,q,r)$|$,
(II) r-rank$\{F_{10}\}$=2 *if and only if there exist at least two indices* λ_{x_i,y_i} (i=1,2) *such that* $|F_{10}((x_1,y_1),(x_2,y_2))|\neq 0$ *for* $(x_i,y_i)\in SV_{10}$, *i.e.*, $y_1\neq y_2$,
(III) r-rank$\{F_{01}\}$=2 *if and only if there exist at least two indices* λ_{x_i,y_i} (i=1,2) *such that* $|F_{01}((x_1,y_1),(x_2,y_2))|\neq 0$ *for* $(x_i,y_i)\in SV_{01}$, *i.e.*, $x_1\neq x_2$, *and*
(IV) r-rank$\{F_{11}\}$=1 *if and only if there exists at least one index* $\lambda_{x,y}$ *such that* $(x,y)\in SV_{11}$.

Let N_{00}, N_{10}, N_{01} and N_{11} be the cardinal number of $SV_{00}-\{SV_{10}\cup SV_{01}\cup SV_{11}\}(=SV_{00}^*$, say), $SV_{10}-SV_{11}(=SV_{10}^*$, say), $SV_{01}-SV_{11}(=SV_{01}^*$, say) and $SV_{11}(=SV_{11}^*$, say), respectively. Note that $SV_{\beta_1\beta_2}^*$ ($\beta_1\beta_2$ =00,10,01,11) are mutually disjoint and $SV_{00}=SV_{00}^*\cup SV_{10}^*\cup SV_{01}^*\cup SV_{11}^*$. Then from Lemma 4, we establish the main theorem of this paper as follows:

Theorem 2. *Let T be an* SPBA($m_1+m_2;\{\lambda_{i_1,i_2}\}$), *where* $m_k\geq 2$ (k=1,2). *Then T is a* $2^{m_1+m_2}$-PBFF *design of resolution* R({00,10,01,11}) *if and only if there exist at least four indices* λ_{x_i,y_i} (i=1,2,3,4) *such that they satisfy the conditions of* Lemma 4.(I), *where* $(x_i,y_i)\in SV_{00}$, *and* $N_{11}\geq 1$, *and moreover*
(I) *if* N_{11}=1, *then* $N_{10}\geq 1$ *and* $N_{01}\geq 1$,
(II) *if* N_{11}=2, *and furthermore*
 (i) *if* $x_i=x_j$ ($y_i\neq y_j$), *where* $(x_i,y_i),(x_j,y_j)\in SV_{11}^*$ *for* $\{i,j\}\subset\{1,2,3,4\}$, *then* $N_{01}\geq 1$,
 (ii) *if* $y_i=y_j$ ($x_i\neq x_j$), *where* $(x_i,y_i),(x_j,y_j)\in SV_{11}^*$ *for* $\{i,j\}\subset\{1,2,3,4\}$, *then* $N_{10}\geq 1$, *and*
 (iii) $x_i\neq x_j$ *and* $y_i\neq y_j$, *where* $(x_i,y_i),(x_j,y_j)\in SV_{11}^*$ *for* $\{i,j\}\subset\{1,2,3,4\}$, *and*
(III) $N_{11}\geq 3$.

Characterization of balanced fractional 3^m factorial designs of resolution III

Hiromu Yumiba[1] and Yoshifumi Hyodo[1,2]
[1]International Institute for Natural Sciences
[2]Graduate School of Informatics, Okayama University of Science

A balanced array (BA) of strength t, size N, m constraints, three symbols and index set $\{\mu_{j_0 j_1 j_2} | j_0 + j_1 + j_2 = t\}$ is briefly denoted by BA$(N, m, 3, t; \{\mu_{j_0 j_1 j_2}\})$. As a special case of a BA, a BA of strength m (i.e., full strength) and index set $\{\lambda_{i_0 i_1 i_2} | i_0 + i_1 + i_2 = m\}$ is called a simple array (SA) and it is denoted by SA$(m;\{\lambda_{i_0 i_1 i_2}\})$ for brevity. Under the assumption that the $(\ell + 1)$-factor and higher-order interactions are negligible, if all the factorial effects up to the ℓ-factor interaction are estimable, then a design is said to be of resolution $(2\ell + 1)$. If the variance-covariance matrix of the estimators of the factorial effects to be of interest is invariant under any permutation on the factors, then the design is said to be balanced.

In this paper, we present a necessary and sufficient condition for an SA$(m; \{\lambda_{i_0 i_1 i_2}\})$ to be a balanced fractional 3^m factorial (3^m-BFF) design of resolution III ($\ell = 1$) by use of a decomposition of the irreducible representations of the information matrix.

We consider a fractional 3^m factorial design T derived from SA$(m; \{\lambda_{i_0 i_1 i_2}\})$, where the two-factor and higher-order interactions are assumed to be negligible and $m \geq 2$. Then an $N \times 1$ observation vector $\boldsymbol{y}(T)$ based on T is expressed as $\boldsymbol{y}(T) = E_T \boldsymbol{\theta} + \boldsymbol{e}_T$, where E_T, $\boldsymbol{\theta}$ and $\boldsymbol{e}_T$ are the $N \times (1 + 2m)$ design matrix, the $(1 + 2m) \times 1$ vector of the non-negligible factorial effects, and an $N \times 1$ error vector with mean $\boldsymbol{0}_N$ and variance-covariance matrix $\sigma^2 I_N$, respectively. Here $\boldsymbol{\theta} = (\boldsymbol{\theta}'_{00}; \boldsymbol{\theta}'_{10}; \boldsymbol{\theta}'_{01})'$ and $N = \sum_{i_0+i_1+i_2=m} \{m!/(i_0!i_1!i_2!)\} \lambda_{i_0 i_1 i_2}$. Then 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 $1 + 2m$ and A' denotes the transpose of a matrix A. Note that if M_T is non-singular, then T is of resolution III.

Let T be an SA$(m; \{\lambda_{i_0 i_1 i_2}\})$. Then the information matrix M_T associate with T is isomorphic to the symmetric matrices $\|\kappa_0^{a_1 a_2, b_1 b_2}\| (= K_0$, say) of order 3 and $\|\kappa_f^{u_1 u_2, v_1 v_2}\| (= K_f$, say) of order 2, i.e., there exists an orthogonal matrix P of order $1 + 2m$ such that

$$P' M_T P = \mathrm{diag}[K_0; \overbrace{K_f, \ldots, K_f}^{m-1}]. \tag{1}$$

Here that the matrices K_β $(\beta = 0, f)$ are called the irreducible representations of M_T, where $\kappa_0^{a_1 a_2, b_1 b_2}$ (or $\kappa_f^{u_1 u_2, v_1 v_2}$) are given by some linear combinations of $\lambda_{i_0 i_1 i_2}$.

Theorem 1. *Let T be an* SA$(m; \{\lambda_{i_0 i_1 i_2}\})$, *then the matrices K_β $(\beta = 0, f)$ can be expressed as*

$$K_\beta = (D_\beta F_\beta \Lambda_\beta)(D_\beta F_\beta \Lambda_\beta)'. \tag{2}$$

Here $D_0 = \mathrm{diag}[1; 1/\sqrt{m}; 1/\sqrt{m}]$ and $D_f = \mathrm{diag}[-1; 3]$, the column vector $\boldsymbol{F}_0(x, y)$ of F_0 which is of size $3 \times \binom{m+2}{2}$ and the 2×2 submatrix $F_f(x, y)$ of F_f which is of size $2 \times (m-1)(m+4)$ concerned with $\lambda_{m-x-yxy}$ are given by

$$\boldsymbol{F}_0(x, y) = \sqrt{\lambda_{m-x-yxy}} (1 \ -(m - x - 2y) \ m - 3x)' \ ((x, y) \in V_0) \text{ and} \tag{3}$$

$$F_f(x, y) = \sqrt{\lambda_{m-x-yxy}} \begin{pmatrix} -2\sqrt{y(m-x-y)} & (m-x-2y)\sqrt{x} \\ 0 & (m-x)\sqrt{x} \end{pmatrix} ((x, y) \in V_f), \tag{4}$$

respectively, and the diagonal element of the diagonal matrix Λ_0 and the 2×2 block diagonal one of the diagonal matrix Λ_f concerned with $\lambda_{m-x-yxy}$ are given by

$$\sqrt{m!/\{(m-x-y)!x!y!\}} \ ((x, y) \in V_0) \text{ and}$$
$$\sqrt{m!/\{(m-x-y)!x!y!\}} \mathrm{diag}[\sqrt{1/\{(m-1)(m-x)\}}; \sqrt{1/\{m(m-1)(m-x)\}}] \ ((x, y) \in V_f),$$

respectively, where $V_0 = \{(x, y) \in \boldsymbol{N}_0^2 | x + y \leq m\}$ and $V_f = V_0 \setminus \{(0, 0), (m, 0), (0, m)\}$.

It follows from (2) that rank$\{K_\beta\}$ =r-rank$\{F_\beta\}$ for $\beta = 0, f$, where r-rank $\{A\}$ denotes the row rank of a matrix A. Then the following is obtained:

Lemma 1. *Let T be an* SA$(m; \{\lambda_{i_0 i_1 i_2}\})$, *where $m \geq 2$. Then a necessary and sufficient condition for T to be a* 3^m-BFF *design of resolution* III *is that* r-rank$\{F_0\} = 3$ *and* r-rank$\{F_f\} = 2$.

By (3) and (4), the following can be easily proved:

Lemma 2. *Let T be an* SA$(m; \{\lambda_{i_0 i_1 i_2}\})$, *where $m \geq 2$. Then the following hold*:

(I) r-rank$\{\boldsymbol{F}_0(x,y)\} = 1$ *if* $\lambda_{m-x-yxy} \neq 0$ *for* $(x,y) \in V_0$ *and*

(II) $$\text{r-rank}\{F_f(x,y)\} = \begin{cases} 1 & \text{if } \lambda_{m-x-yxy} \neq 0 \text{ for } (x,y) \in V_f^1, \\ 2 & \text{if } \lambda_{m-x-yxy} \neq 0 \text{ for } (x,y) \in V_f^2, \end{cases}$$

where $\boldsymbol{F}_0(x,y)$ and $F_f(x,y)$ are given by (3) *and* (4), *respectively, and* $V_f^2 = \{(x,y) \in \boldsymbol{N}^2 \mid x + y \leq m-1\}$ *and* $V_f^1 = V_f \setminus V_f^2 = \{(x,0) | 1 \leq x \leq m-1\} \cup \{(0,y) | 1 \leq y \leq m-1\} \cup \{(x,y) | m - x - y = 0, 1 \leq x \leq m-1\}$.

From Lemma 2, we have the following:

Lemma 3. *Let T be an* SA$(m; \{\lambda_{i_0 i_1 i_2}\})$, *where $m \geq 2$. Then we have*

(I) r-rank$\{F_0\} = 3$ *if and only if there exist at least three non-zero indices* $\lambda_{m-x_i-y_i x_i y_i}$ $((x_i, y_i) \in V_0$ $(i = 1,2,3))$ *such that* $|F_0((x_1,y_1),(x_2,y_2),(x_3,y_3))| \neq 0$, *where* $F_0((x_1,y_1),(x_2,y_2),(x_3,y_3)) = \begin{pmatrix} 1 & 1 & 1 \\ y_1 & y_2 & y_3 \\ x_1 & x_2 & x_3 \end{pmatrix}$ *and* $|A|$ *denotes the determinant of a matrix* A,

(II) r-rank$\{F_f\} = 2$ *if and only if one of the following holds*:

(i) *There exists at least one non-zero index* $\lambda_{m-x-yxy}((x,y) \in V_f^2)$, *or*

(ii) *there exist at least two non-zero indices* $\lambda_{m-x_i-y_i x_i y_i}((x_i,y_i) \in V_f^1$ $(i = 1,2))$ *such that* $\binom{x_1}{x_2} \neq \boldsymbol{0}_2, \binom{y_1}{y_2} \neq \boldsymbol{0}_2$ *and* $\binom{m-x_1-y_1}{m-x_2-y_2} \neq \boldsymbol{0}_2$, *where* $\lambda_{m-x-yxy} = 0$ *for all* $(x,y) \in V_f^2$.

Let $F_0^*((x_1,y_1),(x_2,y_2),(x_3,y_3))$ be a 3×3 submatrix of F_0 concerned with three non-zero indices $\lambda_{m-x_i-y_i x_i y_i}$ $(i = 1,2,3)$, where $(x_i,y_i) \in V_0$, and $F_f^*((x_1,y_1),\cdots,(x_n,y_n))$ be a $2 \times 2n$ submatrix of F_f concerned with n non-zero indices $\lambda_{m-x_i-y_i x_i y_i}$ $(i = 1,\ldots,n)$, where $(x_i,y_i) \in V_f$. Then from (3), (4) and Lemma 3, we have the following:

Lemma 4. *Let T be an* SA$(m; \{\lambda_{i_0 i_1 i_2}\})$, *where $m \geq 2$. Then* r-rank$\{F_0\} = 3$ *and* r-rank$\{F_f\} = 2$ *if and only if there exist at least three non-zero indices* $\lambda_{m-x_i-y_i x_i y_i}$ $(i = 1,2,3)$ *such that* (i) r-rank$\{F_0^*((x_1,y_1),(x_2,y_2),(x_3,y_3))\} = 3$ *and* r-rank$\{F_f^*((x_1,y_1))\} = 2$ *for* $(x_1,y_1) \in V_f^2$ *and* $(x_k,y_k) \in V_0$ $(k = 2,3)$, *or* (ii) r-rank$\{F_0^*((x_1,y_1),(x_2,y_2),(x_3,y_3))\} = 3$ *and* r-rank$\{F_f^*((x_1,y_1),(x_2,y_2))\} = 2$ *for* $(x_k,y_k) \in V_f^1$ $(k = 1,2)$ *and* $(x_3,y_3) \in V_0$.

Lemmas 1, 3 and 4 lead us to the main result of this paper as follows:

Theorem 2. *Let T be an* SA$(m; \{\lambda_{i_0 i_1 i_2}\})$, *where $m \geq 2$, and further let* $N_f^2(S) = \#\{(x,y) \in S | (x,y) \in V_f^2\}$, *where* $S = \{(x,y) \in V_0 | \lambda_{m-x-yxy} \neq 0\}$. *Then T is a* 3^m-BFF *design of resolution* III *if and only if there exist at least three non-zero indices* $\lambda_{m-x_i-y_i x_i y_i}$ $(i = 1,2,3)$ *such that they satisfy the following conditions*:

(I) *If* $N_f^2(\{(x_1,y_1),(x_2,y_2),(x_3,y_3)\}) = 0$, *then* $(x_k,y_k) \in V_f^1$ $(k = 1,2)$ *and* $(x_3,y_3) \in V_0$, *where* $\binom{x_1}{x_2} \neq \boldsymbol{0}_2, \binom{y_1}{y_2} \neq \boldsymbol{0}_2$ *and* $\binom{m-x_1-y_1}{m-x_2-y_2} \neq \boldsymbol{0}_2$, *and*

(II) *if* $N_f^2(\{(x_1,y_1),(x_2,y_2),(x_3,y_3)\}) \geq 1$, *i.e.,* $(x_1,y_1) \in V_f^2$, *then* $(x_k,y_k) \in V_0$ $(k = 2,3)$, *where* $|F_0((x_1,y_1),(x_2,y_2),(x_3,y_3))| \neq 0$. *Here* $F_0((x_1,y_1),(x_2,y_2),(x_3,y_3))$ *is given in* Lemma 3.

Cyclic design を用いた分割型ユニットをもつ２因子実験の構成法

大阪府立大学　工学研究科　田口　和規
大阪府立大学　工学研究科　栗木　進二

２因子実験を考え，その因子を A, B とし，各々の因子の水準（処理ともいう）を $A_1, A_2, \cdots, A_a$, $B_1, B_2, \cdots, B_b$ とする．k_0 個の superblock があり，各 superblock は k_1 行 k_2 列からなる k_1k_2 個の wholeplot に分割され，各 wholeplot は k_3 個の subplot に分割される．因子 A の処理 $A_1, A_2, \cdots, A_a$ が wholeplot に対して施され，因子 B の処理 $B_1, B_2, \cdots, B_b$ が subplot に対して施される．このような実験を分割型ユニットをもつ２因子実験という．この２因子実験のモデルとして，処理効果が母数であり，superblock 効果，行効果，列効果，wholeplot 効果，subplot 効果が確率変数である混合モデル

$$\boldsymbol{y} = \boldsymbol{\Delta\tau} + \mathbf{R}\boldsymbol{\rho} + \mathbf{D}_1\boldsymbol{\omega} + \mathbf{D}_2\boldsymbol{\chi} + \mathbf{G}\boldsymbol{\eta} + \boldsymbol{\theta} + \boldsymbol{\epsilon}$$

を考える．ここで，$\boldsymbol{y}, \boldsymbol{\tau}, \boldsymbol{\rho}, \boldsymbol{\omega}, \boldsymbol{\chi}, \boldsymbol{\eta}, \boldsymbol{\theta}, \boldsymbol{\epsilon}$ はそれぞれ観測値，処理効果，superblock 効果，行効果，列効果，wholeplot 効果，subplot 効果，観測誤差からなる列ベクトルで，$\boldsymbol{\Delta}$, $\mathbf{R}$, $\mathbf{D}_1$, $\mathbf{D}_2$, $\mathbf{G}$ は処理組合せ，superblock，行，列，wholeplot に対するデザイン行列である．また，４段階の無作為化，(1) superblock の無作為化，(2) superblock 内の行の無作為化，(3) superblock 内の列の無作為化，(4) wholeplot 内の subplot の無作為化を考える．i 番目の処理効果 τ_i は

$$\tau_i = \mu + \alpha_\ell + \beta_m + (\alpha\beta)_{\ell m}, \quad i = (\ell - 1)b + m$$

$(\ell = 1, 2, \cdots, a; m = 1, 2, \cdots, b)$ である．ここで，μ は一般平均，α_ℓ は A_ℓ の主効果，β_m は B_m の主効果，$(\alpha\beta)_{\ell m}$ は A_ℓ と B_m の交互作用効果である．Multistratum 分析において，分割型ユニットをもつ２因子実験では，(I) inter-superblock stratum, (II) inter-row stratum, (III) inter-column stratum, (IV) inter-wholeplot stratum, (V) inter-unit stratum の５つの strata があり，その stratum 情報行列 $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4, \mathbf{A}_5$ は

$$\mathbf{A}_1 = \frac{1}{k_1k_2k_3}\mathbf{N}_0\mathbf{N}_0' - \frac{1}{k_0k_1k_2k_3}\boldsymbol{r}\boldsymbol{r}',$$

$$\mathbf{A}_2 = \frac{1}{k_2k_3}\mathbf{N}_1\mathbf{N}_1' - \frac{1}{k_1k_2k_3}\mathbf{N}_0\mathbf{N}_0',$$

$$\mathbf{A}_3 = \frac{1}{k_1k_3}\mathbf{N}_2\mathbf{N}_2' - \frac{1}{k_1k_2k_3}\mathbf{N}_0\mathbf{N}_0',$$

$$\mathbf{A}_4 = \frac{1}{k_3}\mathbf{N}_3\mathbf{N}_3' - \frac{1}{k_1k_3}\mathbf{N}_2\mathbf{N}_2' - \frac{1}{k_2k_3}\mathbf{N}_1\mathbf{N}_1' + \frac{1}{k_1k_2k_3}\mathbf{N}_0\mathbf{N}_0',$$

$$\mathbf{A}_5 = \boldsymbol{r}^\delta - \frac{1}{k_3}\mathbf{N}_3\mathbf{N}_3'$$

によって与えられる．ここで，$\mathbf{N}_0, \mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_3$ はそれぞれ処理組合せと superblock，処理組合せと行，処理組合せと列，処理組合せと wholeplot の生起行列であり，$\boldsymbol{r}$ は各処理組合せの反復回数を表すベクトル，$\boldsymbol{r}^\delta$ は $\boldsymbol{r}$ の要素を対角要素に並べた対角行列である．Stratum 情報行列 $\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4, \mathbf{A}_5$ に対して，

$$\mathbf{A}_f \boldsymbol{x}_i = \lambda_{f,i} \boldsymbol{r}^{\delta} \boldsymbol{x}_i \quad (f = 1, 2, 3, 4, 5)$$

を満たす $\lambda_{f,i}$ を stratum efficiency factor といい，$\boldsymbol{x}_i' \boldsymbol{r}^{\delta} \boldsymbol{\tau}$ は basic contrast と呼ばれている (cf. Pearce, Caliński and Marshall (1974))．ただし，$\boldsymbol{x}_i \neq \mathbf{1}_v$ である．ここで，$\boldsymbol{\tau}$ は処理効果を表す列ベクトルである．これらの詳細については，Kachlicka and Mejza (1996) が参照される．Kachlicka and Mejza (2004), Mejza, Kuriki and Kachlicka (2009) は因子 A の design として，Youden square を用い，因子 B の design として，BIBD, group divisible design を用いて，分割型ユニットをもつ２因子実験を構成し，その stratum efficiency factor を与えた．ここでの目的は，因子 A の design として， cyclic design を用い，因子 B の design として，ある design を用いて，分割型ユニットをもつ２因子実験を構成し，その stratum efficiency factor を与えることである．

Cyclic design CD (v_A, b_A, r_A, k_A) $\mathcal{D}_{\mathcal{A}}$ のいくつかの cyclic class を順に横に並べ，k_A 行 b_A 列からなる１つの superblock を作る．ただし，それぞれの cyclic class の各行には，$\mathcal{D}_{\mathcal{A}}$ のすべての処理が１回ずつ現れるようにする．この superblock のすべての wholeplot の中に，ある design D (v_B, b_B, r_B, k_B) $\mathcal{D}_{\mathcal{B}}$ の各ブロックを割りつけ，b_B 個の superblock を作り，分割型ユニットをもつ２因子実験 $\mathcal{D}$ を構成する．$\mathcal{D}$ のパラメータは $a = v_A$, $b = v_B$, $k_0 = b_B$, $k_1 = k_A$, $k_2 = b_A$, $k_3 = k_B$ である．$\mathcal{D}_{\mathcal{A}}$, $\mathcal{D}_{\mathcal{B}}$ の生起行列を $\mathbf{N}_A$, $\mathbf{N}_B$ とすると，

$$\boldsymbol{r}\boldsymbol{r}' = r_A^2 r_B^2 \, \mathbf{J}_{v_A} \otimes \mathbf{J}_{v_B}, \quad \boldsymbol{r}^{\delta} = r_A r_B \, \mathbf{I}_{v_A} \otimes \mathbf{I}_{v_B},$$

$$\mathbf{N}_0 \mathbf{N}_0' = r_A^2 \, \mathbf{J}_{v_A} \otimes \mathbf{N}_B \mathbf{N}_B', \quad \mathbf{N}_1 \mathbf{N}_1' = \frac{r_A^2}{k_A} \, \mathbf{J}_{v_A} \otimes \mathbf{N}_B \mathbf{N}_B',$$

$$\mathbf{N}_2 \mathbf{N}_2' = \mathbf{N}_A \mathbf{N}_A' \otimes \mathbf{N}_B \mathbf{N}_B', \quad \mathbf{N}_3 \mathbf{N}_3' = r_A \, \mathbf{I}_{v_A} \otimes \mathbf{N}_B \mathbf{N}_B'$$

となり，分割型ユニットをもつ２因子実験 $\mathcal{D}$ の stratum efficiency factor が次の表によって与えられる．

Type of contrasts	Number of contrasts	Strata				
		I	II	III	IV	V
A	ρ_A	0	0	$1 - \varepsilon_{Ai}$	ε_{Ai}	0
B	ρ_B	$1 - \varepsilon_{Bj}$	0	0	0	ε_{Bj}
$A \times B$	$\rho_A \rho_B$	0	0	$(1 - \varepsilon_{Ai})(1 - \varepsilon_{Bj})$	$\varepsilon_{Ai}(1 - \varepsilon_{Bj})$	ε_{Bj}

ここで，$\rho_A = v_A - 1$, $\rho_B = v_B - 1$, $\varepsilon_{Ai} = 1 - \theta_i/(r_A k_A)$ $(i = 1, 2, \cdots, v_A - 1)$, $\varepsilon_{Bj} = 1 - \omega_j/(r_B k_B)$ $(j = 1, 2, \cdots, v_B - 1)$ であり，θ_i, ω_j はそれぞれ $\mathbf{N}_A \mathbf{N}_A'$, $\mathbf{N}_B \mathbf{N}_B'$ の固有値である．

参考文献

Kachlicka, D. and Mejza, S. (1996) Computational Statistics & Data Analysis 21, 293-305.

Kachlicka, D. and Mejza, S. (2004) Colloquium Biometryczne 34, 103-110.

Mejza, S., Kuriki, S. and Kachlicka, D. (2009) Journal of Statistics and Applications (to appear).

Pearce, S.C., Caliński, T. and Marshall, T.F. de C. (1974) Biometrika 61, 449-460.

スペクトル拡散通信における同期の問題

大阪府立大学大学院　工学研究科　堀田　祐未
大阪府立大学大学院　工学研究科　栗木　進二

スペクトル拡散通信は、ユーザーコードと呼ばれる個々に与えられた暗証番号のようなものを、自分が送りたいデータにかけあわせることによって広い帯域に拡散させて送信し、受信側で同じユーザーコードを使って元のデータを復元するという仕組みになっている。Eshima, N. and Kohda, T. (2006), Eshima, N., Kohda, T. and Tabata, M. (2007), Eshima, N. and Kohda, T. (2008) によれば、このユーザーコードは $(X_0, X_1, X_2, \ldots, X_{N-1})$ と表され、N はコードの長さ、$\Pr(X_i = -1) = \Pr(X_i = -1) = \frac{1}{2}$ である。同様にユーザーデータは $(d_0, d_1, \ldots)$ と表され、送るデータの数は任意で、$d \in -1, 1$ である。この X と d をかけあわせたものを ${y_t}^{(j)} = X_{t-m} d_{t-m} (m = 0, 1, 2, \ldots, N-1)$ と表す。この m は、自分がデータを送りたい人を基準としたときに j 番目の人との間に生じる「通信を始めた時間のずれ」である。この y を使うと、各ユーザーの信号は $j = 0, 1, \ldots, J$ として

$$r_j(t) = \sqrt{2} \sum_{k=-\infty}^{\infty} {y_k}^{(j)} u(t - k - m_j) \cos(\omega t) \tag{1}$$

と表され、$u(t)$ は $0 \leq t < 1$ の時 1 となり、他では 0 となる。よって、全体の受信信号は J 人の信号と雑音をあわせて $r(t) = \sum_{j=0}^{J} r_j(t) + e(t)$ となる。この $r(t)$ を使って $k = 0, 1, 2, \ldots, N-1; a = 0, 1, 2, \ldots; T = N$ として信号の基本受信系列は次のように表される。

$$r_{aN+k} = \frac{\sqrt{2}}{T\omega} \int_{aN+k}^{aN+k+1} r(t) \cos(\omega t) dt \tag{2}$$

さて、受信した信号は、相関器 $Z(a, i)$ で基準となる人のユーザーコードと内積を行う。この $Z(a, i)$ は $Z(a, i) = \sum_{k=0}^{N-1} X_k r_{aN+i+k} (i = 0, 1, 2, \ldots, N-1)$ と表し、この $Z(a, i)$ が ζN より大きい場合に i 番目に同期とする。ここで、ζ は閾値で、N はコードの長さである。次に、$Z(1, i), Z(2, i), \ldots, Z(A, i)$ の中で、ζN より大きい Z を見つけ、その個数を $n(A, i)$ とし、$N-1$ 番目までの和を $n(A, +) = \sum_{i=0}^{N-1} n(A, i)$ と表す。ここで、$Z(a, i)$ は a 行 N 列の行列となることに注意しておきたい。また、同期の時に Z が漸近的に正規分布 $N(N, NJ)$ に従うことから $NJ \to \infty$ の時に

$$\alpha = \int_{\zeta N}^{+\infty} \frac{1}{\sqrt{2\pi NJ}} exp\left(-\frac{(z-N)^2}{2NJ}\right) dz \tag{3}$$

とし、同様に 非同期の時には漸近的に正規分布 $N(0, NJ)$ に従うことから $NJ \to \infty$ の時に

$$\beta = \int_{\zeta N}^{+\infty} \frac{1}{\sqrt{2\pi NJ}} exp\left(-\frac{z^2}{2NJ}\right) dz \tag{4}$$

とする。これらを使って i 番目が同期で、他は非同期の同時確率関数は $\mathbf{n}^{(Na)} = (n(a, 0), n(a, 1), \ldots, n(a, N-1))$ として $\eta_i(\mathbf{n}^{(Na)}) \propto \alpha^{n(a,i)} (1-\alpha)^{a-n(a,i)} \beta^{n(a,+)-n(a,i)} (1-\beta)^{a(N-1)-n(a,+)+n(a,i)}$ となる。i 番目が同期の確率は $i = 0, 1, 2, \ldots, N-1$ の時に

$$\Pr(i|\mathbf{n}^{aN}) = \frac{\eta_i(\mathbf{n}^(aN))}{\sum_{j=0}^{N-1} \eta_j(\mathbf{n}^(aN))} \tag{5}$$

となり、この確率を用いたアルゴリズムが以下である。
1．$\gamma < 1$ とする。2．$\eta_i(\mathbf{n}^{(Na)}) = max\{\eta_0(\mathbf{n}^{(Na)}), \eta_1(\mathbf{n}^{(Na)}), \ldots, \eta_{N-1}(\mathbf{n}^{(Na)})\}$ 3．$\Pr(i|\mathbf{n}^{aN}) \geq \gamma$ ならば、i 番目で同期として取得する。逆に $\Pr(i|\mathbf{n}^{aN}) < \gamma$ ならば、もう 1 度 2 の作業に戻って a の数を 1 つ増やして同様に考える。

さて、今回はコンマフリーコードの 1 つであるプレフィクスコンマフリーをユーザーコードに用いた。コンマフリーコードとは符号語で同期符号とされているもので、2 つの符合語を $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ と $\mathbf{b} = (b_1, b_2, \ldots, b_n)$ とした時、オーバーラップ $(a_{k+1}, a_{k+2}, \ldots, a_n b_1, b_2, \ldots, b_n)$（ただし、$1 \leq k \leq n-1$）が符合語でないものである。また、プレフィクスコンマフリーとは、各コードのはじめに共通な一定のパターンをもつものである。このシミュレーションを上記したアルゴリズムを使い $\omega = \pi$、$e(t) = 0$ として、様々な数値を変えて行った。

N	CF	Eshima	ζ
15	966	842	0.1
31	953	920	0.4
63	966	924	0.017

Table 1

data	CF	Eshima
100	966	842
200	945	870
300	620	301

Table 2

ζ	CF	Eshima
0.08	966	922
0.09	958	898
0.10	945	842
0.11	905	747
0.12	848	651

Table 3

user	CF	Eshima
3	717	525
4	898	771
5	966	842
6	951	871
7	948	880

Table 4

γ	CF	Eshima
0.99	966	842
0.95	898	808
0.90	871	768
0.85	873	769
0.80	878	757

Table 5

CF は comma-free の略である。上記の表は、Table 1 ではコードの長さを、Table 2 ではデータ数を、Table 3 では ζ の値を、Table 4 ではユーザー数を、Table 5 では γ の値を変化させてシミュレーションを 1000 回繰り返した時の正しくコードを取得する回数を示している。また、全てのシミュレーションにおいて変化させる数値以外は $N = 15, d = 100, \zeta = 0.1, J = 5, \gamma = 0.99$ として考えた。結果として、いずれも従来の方法よりプレフィクスコンマフリーを用いることで同期の正確さが高まるということを確かめることが出来た。

[1] Eshima, N. and Kohda, T. (2006) Statistical Approach to the Code Acquisition Problem in Direct-Sequence Spread-Spectrum Communication Systems, IMA Journal of Mathematical Control and Information, 23, 149-163.
[2] Eshima, N., Kohda, T. and Tabata, M. (2007) Statistical solution to the capacity problem in the DS/CDMA communication systems, IMA Journal of Mathematical Control and Information, 24, 289-298.
[3] Eshima, N. and Kohda, T. (2008) Low-complexity code acquisition method in DS/CDMA communication systems: Application of the maximum likelihood method to propagation delay estimation, IEICE Transactions on Communications 91-B, 1472-1479.

Mutually M-intersecting K-arcs と光直交符号への応用

東京理科大学 理工学部　宮本 暢子*
明星大学 情報学部　篠原 聡†

1. はじめに 位数 q の有限体上の射影平面 PG$(2,q)$ において，どの $d+1$ 点も同一直線上にないような k 点からなる集合を (k,d)-*arc* と呼ぶ．ただし，d　2 とし，特に $d=2$ のとき，k-*arc* と書く．k-arc が存在するための k の最大値は，q が奇数のときは $q+1$ であり，q が偶数のときは $q+2$ である．また，任意の conic は $(q+1)$-arc であることが良く知られている．q が偶数のとき，conic の各点の接線は一点で交わり，この点を *nucleus* と呼び，任意の conic 上の点とその nucleus を合わせた点集合が $(q+2)$-arc になることは容易に示される．

Definition 1 M を非負整数，K,D をそれぞれ正整数の順序集合で $|K|=|D|$ とする．任意の $k_i,k_j \in K$ に対して，(k_i,d_i)-*arc* と (k_j,d_j)-*arc* の交点が m 個，ただし $m \in M$ であるとき，この *arc* の集まりを mutually M-intersecting (K,D)-arcs であるという．

簡単のために，$D=\{2,2,\ldots,2\}$ のときは mutually M-intersecting K-arcs のように表わし，$K=\{k\}$ ならば mutually M-intersecting (k,d)-arcs や mutually M-intersecting k-arcs と表わすことにする．

また，重み $w_i \in W$ が一定でない光直交符号は Yang [2] によって 1996 年に提案された．n を符号長，$W=\{w_0,\ldots,w_p\}$ を重みの列とし，$Q=\{q_0,\ldots,q_p\}$ を重み w_j の符号語の全体に占める割合 q_j の分布を表わす列，$L=(\ {}^{0}_{a},\ldots,\ {}^{p}_{a})$ を重み w_j を持つ符号語の auto-correlation の上限値 ${}^{j}_{a}$ の列，${}_{c}$ を cross-correlation の上限値とするような符号 C を以下のように定義する．

Definition 2 C が以下の性質を満たすとき，C を可変重み光直交符号 *(variable-weight OOC)* と呼び，$(n,W,L,\ {}_{c},Q)$-*OOC* と書く．

- *(*auto-correlation property*)* 重みが w_j である任意の符号語 $c=(c_0,c_1,\ldots,c_{n-1}) \in C$ に対して，
$$\sum_{i=0}^{n-1} c_i c_{i+t} \qquad {}^{j}_{a}$$
が 1　t　n　1 なる任意の t と任意の j について成り立つ．
- *(*cross-correlation property*)* 異なる符号語 $c=(c_0,c_1,\ldots,c_{n-1})$ と $c'=(c'_0,c'_1,\ldots,c'_{n-1})$ に対して，
$$\sum_{i=0}^{n-1} c_i c'_{i+t} \qquad {}_{c}$$
が 0　t　n　1 なるすべての t に対して成り立つ．

ただし，添字は n で剰余をとる．

本報告では，mutually M-intersecting K-arcs のいくつかの構成法をのべ，mutually M-intersecting (K,D)-arcs と可変重み光直交符号との関係を示した上で，新たな符号系列を与える．

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

2. Mutually M-intersecting K-arcs 点 $P=(a,b,c)$ を $\mathrm{PG}(2,q)$ 上にない $\mathrm{PG}(2,q^2)$ 上の点，l_P を P を通る F_q 上の多項式で定義される直線とする．l_P は $\mathrm{PG}(2,q)$ 上の直線となり，また $\mathrm{PG}(2,q^2)$ では $P^q=(a^q,b^q,c^q)$ を通る．以下では，素数べき q は偶数とする．$\mathcal{C}$ を点 P を通る全ての conic の集合とし，N を l_P 上にない $\mathrm{PG}(2,q)$ の点とするとき，次のような $\mathcal{C}$ の 3 つの部分集合を考える．$\mathcal{C}_N$ を点 N を通る $\mathcal{C}$ のすべての conic の集合，$\hat{\mathcal{C}}_N$ を N を nucleus として持つような $\mathcal{C}$ のすべての conic の集合，$\bar{\mathcal{C}}_N$ を $\mathcal{C}$ の $\mathcal{C}_N$ と $\hat{\mathcal{C}}_N$ 以外の conic の集合，すなわち $\bar{\mathcal{C}}_N=\mathcal{C}\setminus\{\mathcal{C}_N\cup\hat{\mathcal{C}}_N\}$ とする．定義より，$\mathcal{C}_N,\hat{\mathcal{C}}_N$ および $\bar{\mathcal{C}}_N$ は互いに排反であることに注意する．

$\mathcal{C}_0=\{C\setminus\{N\}:C\in\mathcal{C}_N\}$ とし，$\mathcal{C}_1=\{C\cup\{N\}:C\in\hat{\mathcal{C}}_N\}$ とする．さらに，$\mathcal{C}_2=\bar{\mathcal{C}}_N$ とする．このとき以下の補題や定理が成り立つ．

Lemma 3 $\mathcal{C}_0$ は *mutually* $\{0,1\}$*-intersecting* q*-arcs* である．また，$\mathcal{C}_0$ の要素の個数は $|\mathcal{C}_0|=(q+1)(q\quad 1)$ である．

Lemma 4 $\mathcal{C}_1$ は *mutually* $\{1\}$*-intersecting* $(q+2)$*-arcs* である．また，$\mathcal{C}_1$ の要素の個数は $|\mathcal{C}_1|=q\quad 1$ である．

Lemma 5 $\mathcal{C}_2$ は *mutually* $\{0,1,2\}$*-intersecting* $(q+1)$*-arcs* である．また，$\mathcal{C}_2$ の要素の個数は $|\mathcal{C}_2|=(q+1)(q\quad 1)(q\quad 2)$ である．

Lemma 6 $\mathcal{C}_0\cup\mathcal{C}_1$ は *mutually* $\{0,1,2\}$*-intersecting* $\{q,q+2\}$*-arcs* である．$\mathcal{C}_0\cup\mathcal{C}_2$ は *mutually* $\{0,1,2\}$*-intersecting* $\{q,q+1\}$*-arcs* である．$\mathcal{C}_1\cup\mathcal{C}_2$ は *mutually* $\{0,1,2\}$*-intersecting* $\{q+1,q+2\}$*-arcs* である．

Theorem 7 $\mathcal{C}_0\cup\mathcal{C}_1\cup\mathcal{C}_2$ は *mutually* $\{0,1,2\}$*-intersecting* $\{q,q+1,q+2\}$*-arcs* である．

3. Mutually M-intersecting K-arcs を用いた可変重み光直交符号の構成 Miyamoto and Shinohara [1] では，mutually M-intersecting k-arcs と重み一定の光直交符号との対応を示し，またその一例として $_a$ と $_c$ が異なる光直交符号を hyperoval の集合から得る方法を示した．同様の考え方で，mutually M-intersecting (K,D)-arcs より可変重み光直交符号が得られる．

Theorem 8 q を素数べきとし，$\mathcal{M}$ を $\mathrm{PG}(2,q)$ 上の *mutually* M*-intersecting* (K,D)*-arcs* とする．このとき，$\#\mathcal{M}$ 個の符号語からなる $(q^3+q^2+q+1,W,L,\ _c,Q)$*-OOC* が存在する．ここで，$_c=\max(D\cup M)$ であり，$W=K$,$L=D$ である．なお，$\#\mathcal{M}$ は $\mathcal{M}$ の要素の個数を表わし，重み分布 $Q=\{q_i\}$, q_i は $\mathcal{M}$ の (k_i,d_i)*-arc* の数と $\mathcal{M}$ 全体の *arc* の数の割合，を持つものとする．

この Theorem 8 と Theorem 7 より，可変重み光直交符号が構成できる．

Theorem 9 任意の $q=2^i$, $i=1,2,\ldots,$ に対して，$q^3\quad q^2$ 個の符号語からなる $(q^3+q^2+q+1,(q,q+1,q+2),2,2,(\frac{q+1}{q^2},\frac{(q+1)(q-2)}{q^2},\frac{1}{q^2}))$*-OOC* が存在する．

参考文献

[**1**] 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.

[**2**] G. C. Yang, “Variable-weight optical orthogonal codes for CDMA networks with multiple performance requirements,” *IEEE Trans. Commun.*, vol. 44, no. 1, pp. 47–55, 1996.