(17)「実験計画法とその周辺における組合せ的構造の開明と推移理論」に関する研究報告

科学技術文書におけるテキスト領域・数式領域切り分け

福岡教育大学・教育　楊肖玉
九州大学・数理　鈴木昌和
福岡教育大学・教育　玉利文和

一．あらまし

現在、市販のOCRは、鮮明に印刷された英語と日本語のテキスト文章を、ほぼ完全に認識する、しかし、数式を含んだ科学技術文書を読み取るOCRは実用化されていない。数式を含んだ科学技術書をディジタル化することは重要である。数式認識を行うためには、文章の中から数式部分を取り出し、数式構造解析を行わなければならない。本講演では、数式を含む英語の教科書や専門雑誌の数式領域/英語領域の切り分けについて発表する。

二．　印刷文書における数式領域切り分けの概要

画像の認識結果に基づいて、数式領域切り分けを行う。具体的には、画像データに含まれた座標や、文字種類の情報を使い、行分割、単語分割を行って、数式単語かテキスト単語かを判断し、TEXの形式で出力する。

三．アルゴリズム概要：

１．　行分割：基本的にＹ座標の重なりを持つ文字を１つ行にする。

２．　行分割の補正：

印刷文書にはほとんど行と行の間に空白がある。しかし、隣接行の文字の間にＹ座標の重なりをもっている時もある。この場合には、行分割の補正を行う。

行分割の補正を行う手順は次のとおりである：

一ページ画像において、すべてのアルファベット小文字の平均縦幅を求めて、その値をAveHeightSizeとする。行分割段階では得られた行の高さがAveHeightSizeより３倍以上になれば、行分割の補正を行う。

上下付属式をもつ記号（lim ,Σ、分数線など）とその付属式（上下添え字、分数線上下の分子と分母)またはアクセント記号とその下にある強調される文字が再分割されないように、それらを１つの文字領域とみなし、１つの文字として扱う。

文字にラベルをつけ、再分割処理を行う。

３．　単語分割：単語間のスペースで単語分割を行う。

一ページ画像においてすべてのアルファベット小文字の平均横幅を求めて、その値をAverageSizeとする。

二つの隣接文字間の空白とAverageSizeの差の絶対値がVarepsilonより小さければ、この隣接文字を１つ単語にする。そうでなければ、二つ単語にする。例えば、Assume that if x is increase ,then y is increase, that is; y = ax. のような文章では、単語分割を行ったあと、次のように分けられる。

Assume that if x is increase, then y is increase, that is, y＝ax.

Assume that if is increase, 等はテキスト単語(つまり、普通の意味がある単語)という。また、y ＝ ax 等は数式単語と言う。

4． 分けられた単語は数式単語か、テキスト単語かを判断する。

4．1．単語分割を行った直後の単語を OldWord と言う。

4．2．単語の両端に点類と括弧類が出てくる可能性があるので、その点類と括弧類を取り除いたあとの単語を NewWord と言う。

4．3．1つの NewWord に対し、テキスト単語かどうか判断する。

①1つ NewWord に対し、数式文字〔関係演算子、二項演算子、ギリシャ文字など〕が一箇所以上現れると、数式単語にする。NewWord の中には、数式文字以外の文字類、即ちアルファベット類、数字類、ピリオド、ハイフン、@、スラッシュ、クォーテーションしか出現しないときにテキスト単語になる可能性がある。

②ピリオド、ハイフン、@、スラッシュ、クォーテーションが出現した場合には、特殊な単語として処理する。

次に、アルファベット類と数字類だけで構成される単語がテキスト単語かどうかを判断する。

③数字が、アルファベットの中に出てくると数式単語にする。

④小文字の後ろに大文字が出てくると数式単語にする。

⑤母音が含まれるかどうかを調べる。母音が1つも含まれていない単語は数式単語にする。

⑥添え字が一箇所以上現れると数式単語にする。

4．4．再判定。

①テキスト単語の直後と直前、関係演算子と二項演算子が現れたら、数式単語に変える。

②点類と括弧類だけの単語に対して前後の単語との関係を見て、数式かどうか判断する。

参考文献：

「1」 岡本正行、東裕之「記号レイオウトに注目した数式構造認識」、信学論、J－78D—II、No.3, pp.474-482, 1995

「2」 能隅進一、福田亮治、玉利文和、鈴木昌和 「絞り込み法による数式文字認識とその日本語・数式領域取り出しへの応用」、信学論、Vol.J83-D-II, No. 3, pp.894-906, 2000.

手書き入力を用いた高等学校数学授業支援システム

福岡教育大学・教育 中村 勝己
九州大学・数理 鈴木 昌和
福岡教育大学・教育 玉利 文和

1 はじめに

数学授業支援ソフトとして、関数電卓や数式処理ソフト (Mathematica,Matlab,Maple) がある。関数電卓は，深い階層のメニューを使用しなくてはならいないなど面倒な手続きが必要である。数式処理は、多くの命令を習得しなくてはならない。

手書き数式入力インターフェースを用いることにより、ノートに書く感覚で自由に数式を書くことができ、その数式を計算したり、グラフの表示ができる。自分で問題を作成し、計算した後、自分の答えが正しいかどうかチェックでき、自学習としても扱える。

入力インターフェースを利用した教育用ソフトの研究・開発を行っている。

2 本研究の目的

1. ペンとノートを使う感覚でシステムを実現する
2. 数式のフォーマットが直感的で、わかりやすい
3. インターフェスの操作が簡単である
4. 入力された数式に対して計算、及びグラフ表示ができる
5. 他の数式フォーマットと互換性を持つ
6. 自学習に利用できる

以上の目標を持って、使いやすさを重視しながら、実際の数学の授業の現場で役立つシステムの作成を目的にしている。

3 システムの概要

このシステムのメインウインドウは、2つのエリアを持っている。上部のエリアは数式の表示、編集、計算などを行うディスプレイエリアで、その下は手書き文字認識、数式認識を行う手書き入力エリアである。

手書き入力エリアでは、ユーザがマウスかデータタブレットかペンディスプレイで数式を手書き入力することができる。書かれた文字が瞬時に認識され、認識された文字が直ちに書かれた文字とほぼ同じ位置に適切な大きさの手書きサンプル文字に置き換えられていく。それと同時に書かれた文字の数式的要素も考慮して、文字の大きさ、お互いの位置関係も自動に判別し、正しい数式のレイアウトで表示される。

手書き入力エリアで数式の入力後、手書き入力エリアにある OK ボタンを押すと、書かれた数式は解析され、その結果は上部のディスプレイエリアに表示される。その表示結果について、ディスプレイエリアで計算、グラフ表示などの命令を実行できる。また、書かれた数式を Mathematica フォーマットでは入出力、TEX フォーマットでは出力できる。

4　文字認識、数式認識について

手書き入力エリアでは逐次自動書換方式を採用している。誤認識が生じた場合は即時にユーザが判断できて、その場で修正を行える。

1. 一文字認識
   認識方法の一つは方向線素特徴量を基本特徴ベクトルとするもので、もう一つは、書かれた文字のストロークを y 座標の極値によって分割して、それぞれの部分を予め、決めた幾つかのパターンで表す。そして、そのパターンの組合せを基本特徴ベクトルとするものである。
2. 数式認識
   システムに一貫性を持たせ、より数式構造解析がスムーズに行えるために、このシステムでは、文字認識と同時に、書かれた文字を適切な位置に配置することを行う。最後に書かれた文字に対して、その1つ前に書かれた文字との関係と前の文字に対する位置関係を分析して、適当な位置に表示する。主な判断基準は文字の位置座標と大きさである。

5　本システムの機能

現在、使用できる主な機能は、数式の計算、グラフ表示、方程式・不等式、2次関数、微分・積分、ベクトル、数列、式のチェック、数式に番号を付ける、である。

数式の計算では、式の計算 (四則演算、積分、積分の中間形式、総和記号 ($\sum$)、極限記号 (lim)、sin、cos、tan、log などの演算記号による単純計算)、因数分解、展開、通分、方程式の計算、連立方程式の計算 (2変数) ができる。

グラフ表示では、入力された数式のグラフを ActiveMathLink の control 上に表示することができる。

方程式・不等式では、方程式、不等式、連立方程式 (2変数・3変数)、連立不等式の計算ができる。

2次関数では、値域、最大値・最小値、平行移動、頂点の座標、標準形、2次方程式を解く (実数解の範囲)、不等式を解く、共有点の個数、2次関数の決定の項目がある。

微分・積分では、微分、積分ができる。

ベクトルでは、ベクトルの計算 (和、差、内積) の計算ができる。

数列では、一般項が与えられた場合、指定した第 m 項から第 n 項を表示することができ、第 m 項から第 n 項の和を計算することができる。

式のチェックでは、選択した複数行の数式に対して、結果、あるいは式変形が正しいかどうかを判定することができる。

数式に番号を付けるでは、数式に番号を付け、その数式の番号を利用することができる。例えば、番号を付けることによって、連立方程式を解く過程を確認できる。

参考文献

[1] 叢 偉、「手書き入力を用いた数学授業支援システム」『福岡教育大学、修士論文』2001 年

[2] 若松 直樹、「オンラインによる文字認識の研究」『福岡教育大学、卒業論文』2001 年

[3] 安座間 万里子、「オンラインによる文字認識の研究」『福岡教育大学、卒業論文』2001 年

Efficient treatment-control designs

大阪府立大・工　西浦珠代
大阪府立大・工　栗木進二

1. 序

V を v 個の treatment の集合とし，$\mathcal{B}$ を V の b 個の部分集合（block という）の集まりとする．各 block の大きさは一定 (k) であるとし，design $(V,\mathcal{B})$ を $\mathrm{D}(v,b,k)$ と記す．特に，$v=p+1$ で，p 個を test treatment といい，$1,2,\cdots,p$ で表し，1 個を control treatment といい，0 で表すとき，$(V,\mathcal{B})$ を treatment-control design といい，$\mathrm{TCD}(p,b,k)$ と記す．ここで，同じ treatment が同じ block に重複して現れる場合も考える．

問題となるのはどのように treatment を配置すれば，test treatment と control treatment の効果の差がうまく比較できるのかということである．ブロック計画における通常のモデルにおいて，

$$\sum_{i=1}^{p}\mathrm{V}(\hat{\tau}_i-\hat{\tau}_0)$$

を最小とする treatment-control design を求めることが考えられ，その design を optimal であるという．ここで，$(V,\mathcal{B})$ は連結であるとし，τ_j は treatment j の treatment 効果で，$\hat{\tau}_j$ は τ_j の最小二乗推定量である $(j=0,1,2,\cdots,p)$.

Optimal な design を求めるために，Bechhofer and Tamhane (1981) によって導入された balanced treatment incomplete block (BTIB) design が有用であり，Majumdar and Notz (1983) は BTIB design の特別なクラスが optimal な treatment-control design を与えることを示した．最近，Das, Dey, Kageyama and Sinha (2000) は $\sum_{i=1}^{p}\mathrm{V}(\hat{\tau}_i-\hat{\tau}_0)$ が小さいという意味で，efficient な treatment-control design の table を与えた．$\mathrm{TCD}(p,b,k)$ において，$2\le k\le p$ のとき，Majumdar and Notz (1983) は $\sum_{i=1}^{p}\mathrm{V}(\hat{\tau}_i-\hat{\tau}_0)$ の下限 $g(t,s)\sigma^2$ を与え，

$$e=\frac{g(t,s)\sigma^2}{\sum_{i=1}^{p}\mathrm{V}(\hat{\tau}_i-\hat{\tau}_0)}$$

が treatment-control design の efficiency として定義されている．$e=1$ のとき，その design は optimal であり，$e\ge 0.95$ のとき，highly efficient であるといわれている．ここでの目的は，cyclic design と generalized cyclic design に注目し，efficient な treatment-control design を与えることである．

2. Efficient treatment-control designs

Cyclic (generalized cyclic) design $\mathrm{D}(p,b,k)$ の各 block に control treatment を f 回反復させることによって，treatment-control design を構成する．このとき，得られた treatment-control design $\mathrm{TCD}(p,b,k+f)$ において，

$$\sum_{i=1}^{p}\mathrm{V}(\hat{\tau}_i-\hat{\tau}_0)=\left\{\sum_{i=1}^{p-1}\frac{p(k+f)}{bk(f+ke_i)}+\frac{p(k+f)}{bkf}\right\}\sigma^2$$

が成り立つ．ここで，$e_1,e_2,\cdots,e_{p-1}$ は cyclic (generalized cyclic) design の canonical efficiency factor である．

Das, Dey, Kageyama and Sinha (2000) は，BIBD, PBIBD を用いて，パラメータ $2\leq k\leq 10$, $r\leq 10$, $k\leq p\leq b\leq 50$ に対して，$e\geq 0.95$ である efficient な treatment-control design $\mathrm{TCD}(p,b,k)$ の table を与えた．ここで，r は各 test treatment の反復回数である．ただし，(p,k) が同じ場合には，条件：(1) block の個数が小さくない．(2) e の値が大きくない．の両方を満たす design は table から除かれる．すなわち，D_1, D_2 を $\mathrm{TCD}(p,b_1,k)$, $\mathrm{TCD}(p,b_2,k)$ とし，その efficiency を e_1, e_2 とするとき，$b_1\leq b_2$ で，$e_1\geq e_2$ である D_2 は table から除かれる．

Cyclic design, generalized cyclic design として，efficient な design を用いると，その結果として得られる treatment-control design も efficient であることが期待され，ここでは，John (1987) によって与えられた efficient な cyclic design の table と Hall and Jarrett (1981) によって与えられた efficient な generalized cyclic design の table を用いることにした．結果として得られる treatment-control design $\mathrm{TCD}(p,b,k)$ について，パラメータ $3\leq k\leq 10$, $r\leq 10$, $k\leq p\leq 50$, $b\leq 50$ をもち，$e\geq 0.95$ である多くの efficient な treatment-control design が得られたが，Das, Dey, Kageyama and Sinha (2000) の table に対して，先の両方の条件を満たす design は除くことにした．また，Das, Dey, Kageyama and Sinha (2000) によって与えられた table の design が，ここで得られた efficient な treatment-control design に対して，先の両方の条件を満たす場合には，その design に “$*$” を付けることにした．

参考文献

Bechhofer, R. E. and Tamhane, A. C. (1981) Technometrics 23,45-57.
Das A., Dey A., Kageyama S. and Sinha K. (2000) submitted for publication.
Hall, W. B. and Jarrett, R. G. (1981) Biometrika 68, 617-627.
Jarrett, R. G. and Hall, W. B. (1978) Biometrika 65, 397-401.
John, J. A. (1987) Cyclic designs. Chapman and Hall, New York.
Majumdar D. and Notz W. I. (1983) Ann. Statist. 11, 258-266.

Split-block designs and affine α-resolvable designs

大阪府立大・工　岡田正和
大阪府立大・工　栗木進二

1. 序

2因子実験を考え，その因子を A, B とし，それぞれのレベルを $A_1,A_2,\cdots,A_l$, $B_1,B_2,\cdots,B_h$ とする．b 個のブロックがあり，そのブロックは p 行 q 列に配列されているとし，各ブロックに対して，因子 A の $p(\leq l)$ 個のレベルを行 (行処理という) に，因子 B の $q(\leq h)$ 個のレベルを列 (列処理という) に割り当てることにする．このようなデザインを split-block design という．ここでは，$p < l$, $q < h$ である incomplete split-block design (ISBD) を考え，行処理，列処理の組合せ A_wB_j $(w = 1, 2, \cdots, l; j = 1, 2, \cdots, h)$ を含むブロックの個数は一定 (r) とする．

モデルとして，処理効果が母数で，ブロック効果，行効果，列効果が確率変数である mixed model を考え，3段階の無作為化，(1) ブロックの無作為化，(2) ブロックの中の行 (列) の無作為化，(3) ブロックの中の列 (行) の無作為化，を考える．i 番目の処理効果 τ_i は $\tau_i = \mu + \alpha_w + \beta_j + (\alpha\beta)_{wj}$, $i = (w-1)h + j$ $(w = 1, 2, ..., l; j = 1, 2, ..., h)$ である．ここで，μ は一般平均，α_w は A_w の主効果，β_j は B_j の主効果，$(\alpha\beta)_{wj}$ は A_w と B_j の交互作用効果である．Multistratum 分析においては，4つの strata, すなわち，(I) inter-block stratum, (II) inter-row (within the blocks) stratum, (III) inter-column (within the blocks) stratum, (IV) inter-plot stratum がある (cf. Houtman and Speed (1983))．このとき，stratum 情報行列 $\mathbf{A}_1$, $\mathbf{A}_2$, $\mathbf{A}_3$, $\mathbf{A}_4$ は

$$\mathbf{A}_1 = \frac{1}{pq}\mathbf{N}_1\mathbf{N}_1' - \frac{r^2}{n}\mathbf{J}_v, \quad \mathbf{A}_2 = \frac{1}{q}\mathbf{N}_2\mathbf{N}_2' - \frac{1}{pq}\mathbf{N}_1\mathbf{N}_1',$$

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

によって与えられる．ここで，$\mathbf{N}_1$, $\mathbf{N}_2$, $\mathbf{N}_3$ は，処理とブロック，行，列の接合行列である．また，$\mathbf{A}_f/r$ $(f = 1, 2, 3, 4)$ の固有値を stratum efficiency factor (cf. Houtman and Speed (1983), Mejza (1992)) といい，それに対応する固有ベクトルを basic contrast (cf. Pearce, Caliński and Marshall (1974)) という．

Hering and Mejza (1997, 2001), Mejza (1998), Ozawa, Jimbo, Kageyama and Mejza (2001) は，ISBD の構成法として，2つのデザインの Kronecker 積を考えた．ここでの目的は，Mejza, Kuriki and Mejza (2001) の結果を一般化し，より小さな ISBD を構成することを考え，その結果として得られる ISBD の統計的性質を調べることである．

2. Affine α-resolvable incomplete block design による ISBD の構成法

Affine α-resolvable incomplete block design (affine α-RIBD と書く) を用いて, ISBD を構成する. ブロックの個数を小さくする方法として, 行列 $\mathbf{C}$, $\mathbf{D}$ が

$$\mathbf{C} = [\mathbf{C}_1 : \mathbf{C}_2 : \cdots : \mathbf{C}_d], \quad \mathbf{D} = [\mathbf{D}_1 : \mathbf{D}_2 : \cdots : \mathbf{D}_d]$$

で表されるとき,

$$\mathbf{C}\tilde{\otimes}\mathbf{D} = [\mathbf{C}_1 \otimes \mathbf{D}_1 : \mathbf{C}_2 \otimes \mathbf{D}_2 : \cdots : \mathbf{C}_d \otimes \mathbf{D}_d]$$

である semi-Kronecker 積 (cf. Mejza, Kuriki and Mejza (2001)) を用いることにする. 同じ個数の α-resolvable class をもつ 2 つの affine α-RIBD から, semi-Kronecker 積を用いて, ISBD $\tilde{\mathcal{D}}$ を構成する. このとき, $\mathbf{N}_1$, $\mathbf{N}_2$, $\mathbf{N}_3$ を表すことができ, $\mathbf{N}_1\mathbf{N}_1'$, $\mathbf{N}_2\mathbf{N}_2'$, $\mathbf{N}_3\mathbf{N}_3'$ の固有値を求めることができる.

定理 2.1. $\mathbf{N}_1\mathbf{N}_1'$ は固有値 $\beta'\beta''q_2''q_2''t$, $(k'-q_1')(k''-q_1'')$, $\beta'q_2'(k''-q_1'')$, $\beta''(k'-q_1')q_2''$, 0 をもち, その重複度は 1, $(\beta'-1)(\beta''-1)t$, $(\beta''-1)t$, $(\beta'-1)t$, $v'v''-(\beta'-1)(\beta''-1)t-(\beta'-1)t-(\beta''-1)t-1$ である.

定理 2.2. $\mathbf{N}_2\mathbf{N}_2'$ は固有値 $\alpha'\beta''q_2''t$, $\alpha'(k''-q_1'')$, 0 をもち, 重複度は v', $(\beta''-1)v't$, $(v''-(\beta''-1)t-1)v'$ である. また, $\mathbf{N}_3\mathbf{N}_3'$ は固有値 $\alpha''\beta'q_2't$, $\alpha''(k'-q_1')$, 0 をもち, 重複度は v'', $(\beta'-1)v''t$, $(v'-(\beta'-1)t-1)v''$ である.

Stratum efficiency factor を求めるためには, 構成されたデザイン $\tilde{\mathcal{D}}$ が generally balanced (cf. Houtman and Speed (1983)) であることを調べなければならないが, そのための必要十分条件は $\mathbf{N}_1\mathbf{N}_1'$, $\mathbf{N}_2\mathbf{N}_2'$, $\mathbf{N}_3\mathbf{N}_3'$ がそれぞれ交換可能になることである (cf. Mejza (1992)).

定理 2.3. $\tilde{\mathcal{D}}$ は generally balanced である.

定理 2.1, 定理 2.2, 定理 2.3 から, stratum efficiency factor を求めることができ, それらの表が与えられる. なお, 推定の方法として, すべての strata の情報を考慮して推定する方法が Houtman and Speed (1983), Nelder (1968) 等で与えられている. また, 各 stratum ごとに分散分析を行うことができる.

参考文献

Hering, F. and Mejza, S. (1997) Biom. J. 39, 227-238.
Hering, F. and Mejza, S. (2001) (to be published in J. Statist. Plann. Infer.).
Houtman, A. M. and Speed, T. P. (1983) Ann. Statist. 11, 1069-1085.
Mejza, I. (1998) Biom. J. 40, 627-639.
Mejza, I., Kuriki, S. and Mejza, S. (2001) Colloquium Biometryczne 31, 97-103.
Mejza, S. (1992) Statistica. anno LII. 2, 263-278.
Nelder, J. A. (1968) J. Royal Statist. Soc. Ser. B 30, 303-311.
Ozawa, K., Jimbo, M., Kageyama, S. and Mejza, S. (2001) (to be published in J. Statist. Plann. Infer.).
Pearce, S. C., Caliński, T. and Marshall, T. F. de C. (1974) Biometrika 54, 449-460.

Optimal $(v, 4, 1)$ Optical Orthogonal Codes with $v \equiv 0 \bmod 12$

Yanxun Chang
Department of Mathematics
Northern Jiaotong University

Ryoh Fuji-Hara and Ying Miao
Institute of Policy and Planning Sciences
University of Tsukuba

An optical orthogonal code (OOC) is a family of $(0, 1)$ sequences with good auto- and cross-correlation properties. Its study has been motivated by an application in a code division multiple access (CDMA) communication using a fiber optical channel. The lack of a network synchronization requirement and an electronic-optical domain conversion requirement enhances the simplicity and the flexibility of such an optical multiple access system. The high weight of codewords facilitates the detection of the desired signal, and the low auto- and cross-correlations reduce the interference from unwanted signals in the network. OOC's also have applications in mobile radio, neuromorphic networks, and radar and sonar signal design. Recent work has been done on using OOC's for multimedia transmission in fiber-optic LAN's and in multirate fiber-optic CDMA systems, too.

Here is the formal definition of an optical orthogonal code. Let v, k, λ_a and λ_c be positive integers. A $(0, 1)$ sequence of *length* v and *weight* k is a sequence with exactly k 1's and $v - k$ 0's. A $(v, k, \lambda_a, \lambda_c)$ *optical orthogonal code*, or briefly (v, k, λ)-OOC, $\mathcal{C}$, is a family of $(0, 1)$ sequences (called *codewords*) of length v and weight k satisfying the following two properties:

(1) (*The Auto-Correlation Property*)
$\sum_{0 \le t \le v-1} x_t x_{t+i} \le \lambda_a$ for any $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$ and any integer $i \not\equiv 0 \pmod{v}$;

(2) (*The Cross-Correlation Property*)
$\sum_{0 \le t \le v-1} x_t y_{t+i} \le \lambda_c$ for any $\mathbf{x} = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$, $\mathbf{y} = (y_0, y_1, \ldots, y_{v-1}) \in \mathcal{C}$ with $\mathbf{x} \neq \mathbf{y}$, and any integer i.

Aperiodic correlation properties might be more appropriate for the present application. However, in this paper, we will restrict our attention to periodic correlations, i.e., the subscripts in the above definition are reduced modulo v whenever necessary. We will only consider the case $\lambda_a = \lambda_c = \lambda$, for which the notation is abbriviated to (v, k, λ)-OOC.

A (v, k, λ) optical orthogonal code with

$$\lfloor \frac{1}{k} \lfloor \frac{v-1}{k-1} \lfloor \frac{v-2}{k-2} \lfloor \cdots \lfloor \frac{v-\lambda}{k-\lambda} \rfloor \rfloor \rfloor \rfloor \rfloor$$

codewords is said to be *optimal*. The use of an optimal optical orthogonal code enables the largest possible number of asynchronous users to transmit information efficiently and reliably in such a CDMA communication system.

Determining the parameters v, k and λ for which an optimal (v, k, λ)-OOC exists is apparently a difficult task. It was shown [2] that an optimal $(v, 3, 1)$-OOC exists if and only if $v \neq 6t + 2$ with $t \equiv 2$ or $3 \pmod 4$. For $k \geq 4$, although there are some partial results, the existence problem for an optimal $(v, k, 1)$-OOC is far from settled. The only complete congruence classes of v for which the existence of an optimal $(v, 4, 1)$-OOC was solved are, to our best knowlege, $v \equiv 6 \pmod{12}$ and $v \equiv 24 \pmod{48}$ due to Ge and Yin [4], and $v \equiv 0 \pmod{648}$ due to Chang and Miao [1].

It is known ([3]) that an optimal (v, k, λ)-OOC is in fact equivalent to a maximum cyclic $(\lambda + 1)$-$(v, k, 1)$-difference packing. Therefore, instead of constructing optimal optical orthogonal codes directly, we need only to construct the corresponding maximum cyclic t-difference packings.

In this paper, several new direct constructions are presented for maximum cyclic 2-$(v, 4, 1)$-difference packing with $v \equiv 0 \pmod{12}$. Some of the constructions are based on the knowledge of skew starters and Weil's theorem on character sums, and some are obtained by listing the explicit codewords of the optimal optical orthogonal codes. As a consequence, together with some new incomplete difference matrices over Z_v, it is shown that an optimal $(v, 4, 1)$-OOC exists for every positive integer $v \equiv 0 \pmod{24}$. Combining the known results, the existence problem for an optimal $(v, 4, 1)$-OOC is settled at this moment for every positive integer $v \equiv 0, 6, 18 \pmod{24}$.

References

[1] Y. Chang and Y. Miao, *Constructions for optimal optical orthogonal codes,* Discrete Math., to appear.

[2] F. R. K. Chung, J. A. Salehi and V. K. Wei, *Optical orthogonal codes: design, analysis, and applications,* IEEE Trans. Inform. Theory **35** (1989), pp. 595–604. Correction: IEEE Trans. Inform. Theory **38** (1992), pp. 1429.

[3] R. Fuji-Hara and Y. Miao, *Optical orthogonal codes: their bounds and new optimal constructions,* IEEE Trans. Inform. Theory **46** (2000), pp. 2396–2406.

[4] G. Ge and J. Yin, *Constructions for optimal* $(v, 4, 1)$ *optical orthogonal codes,* IEEE Trans. Inform. Theory, to appear, 2001.

Optical Orthogonal Codes from Curves

明星大学 情報学部　篠原 聡 *

1 序

Optical Orthogonal Code は光ファイバーを用いた通信において符号分割多元接続を実現する符号であり、その構成などに組合せデザインが応用されるなど密接な関係を持っている。

Optical Orthogonal Code (以下 OOC と略す) C とは以下の 2 つの性質を持つような、長さ n で重みが w の $(0,1)$-sequences の集まりで、$(n,w,\lambda_a,\lambda_c)$-OOC と書く。

- (*auto-correlation property*) 任意の $(c_0,c_1,\ldots,c_{n-1})\in C$ と任意の $1\leq t\leq n-1$ なる整数 t に対し、$\sum_{i=0}^{n-1}c_ic_{i+t}\leq\lambda_a$
- (*cross-correlation property*) 任意の異なる $(c_0,\ldots,c_{n-1}),(c'_0,\ldots,c'_{n-1})\in C$ と任意の $0\leq t\leq n-1$ なる整数 t に対し、$\sum_{i=0}^{n-1}c_ic'_{i+t}\leq\lambda_c$

ただし c,c' の添字は n で剰余をとる。また $\lambda_a=\lambda_c=\lambda$ のときは、(n,w,λ)-OOC と書く。

C の各元を**符号語**と呼び、より多くの符号語がある事が望ましいとされている。与えられたパラメータ (n,w,λ) に対して、符号語の数が最大であるような OOC を *optimal* であるという。constant weight code に対する Johnson bound より導かれる、OOC の符号語数についての上限式

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

が存在し、この上限を達成する事で Optimal な OOC であると保証できる。

$\lambda=1$ であるような optimal な OOC の構成法は数多く存在するが、$\lambda=1$ では符号語数をあまり増やせない等の欠点がある。λ を大きくすると符号語数が増やせるが、$\lambda=2$ の場合、さらに $\lambda\geq3$ の場合の構成法はあまり多くない。$\lambda=2$ の optimal OOC は cyclic Steiner 3-designs からの構成 [1] と、本報告とは異なる射影幾何を使った方法 [2] しか知られていない。本報告では、$\lambda\geq2$ の OOC を有限射影空間内の曲線を用いて構成する方法を提案し、まず conics から $\lambda=2$ の OOC を構成する事を試み、その性能を検討する。

2 $\lambda=2$ の OOC

以下 q を素数巾とする。

Theorem 1 $\mathcal{C}$ をどの 2 つも高々2 点でしか交わらないような射影平面 $\mathrm{PG}(2,q)$ 上の conic の集合とする。このとき $(q^3+q^2+q+1,q+1,2)$-OOC が存在し、その符号語数は $\#\mathcal{C}+\lfloor\frac{q^3-1}{q^2-1}\rfloor$ となる。

さらに、このような conic の集合を定めるのに以下の方法を示している。

Lemma 2 P を射影平面 $\mathrm{PG}(2,q^2)$ の点であって $\mathrm{PG}(2,q)$ の点ではないものとし、$\mathcal{C}$ を射影平面上の conic であって、かつ点 P を通るような位数 q の有限体上のすべての conic の集合とする。このとき $\mathcal{C}$ の任意の 2 つの conics は $\mathrm{PG}(2,q)$ において高々2 点で交わり、$\#\mathcal{C}=q^3-q^2$ である。

q	n	w	size (1)	bound (2)	(1)/(2)
3	40	4	21	61	0.344262
4	85	5	52	113	0.460177
5	156	6	105	196	0.535714
7	400	8	301	470	0.640426
8	585	9	456	673	0.677563
9	820	10	657	928	0.707974
11	1464	12	1221	1618	0.754635
13	2380	14	2041	2588	0.78864
16	4369	17	3856	4673	0.825166

表 1: Theorem 1 および Lemma 2 より導かれる $(n, w, 2)$-OOC

表 1 では、Theorem 1 と Lemma 2 から導かれる OOC の各パラメータおよび符号語数を、小さな q に対して示し、さらに Johnson bound より得られる上限と比較している。この結果、本報告で示した方法で得られた OOC は、q が大きくなるにつれて漸近的に Johnson bound より得られる符号語数の上限式を達成していると思われる。

3 $\lambda \geq 2$ の OOC

Theorem 1 を一般の次数の曲線に適応させる事により、以下のような定理が導き出せる。

Theorem 3 $\mathcal{C}$ を射影平面上の m 次曲線の集合とする。$\mathcal{C}$ の任意の曲線がちょうど w 個の射影平面 PG$(2, q)$ の点を持ち、さらに $\mathcal{C}$ のどの 2 曲線も PG$(2, q)$ において高々λ 個の点を共有するならば、$(q^3 + q^2 + q + 1, w, m, \lambda)$-OOC が構成できる。ただし、$\lambda \leq m^2$ とする。

さらに曲線だけでなくより高次元の多様体へと一般化する事も可能であると思われるが、これは今後の課題である。また、高々2 点で交わるような平面上の conic を Lemma 2 で示したよりたくさん集める方法や、最大いくつの conic を集められるのかを明らかにする必要もある。他には、3 次曲線で $\lambda = 3$ の OOC を具体的に構成できるかを今後検討していく予定である。

参考文献

[1] C.M. Bird and A.D. Keedwell, "Design and Applications of Optical Orthogonal Codes – a Survey", *Bulletin of the ICA*, Vol. 11, pp. 21–44, 1994.

[2] H. Chung and P.V. Kumar, "Optical orthogonal codes: new bounds and an optimal construction", *IEEE Trans. Inform. Theory*, Vol. 36, pp. 866–873, 1990.

* e-mail: sshinoha@mi.meisei-u.ac.jp

1-Rotationally Resolvable Even-Cycle Systems of $2K_v$

岐阜大学・工　三嶋 美和子
國立交通大学・應數　傅 恆霖

1. Introduction

For a graph G, let $V(G)$ be the vertex-set of G and $\mathcal{C}$ be a collection of cycles of length m (m-*cycles*) whose edges partition the edges of G. Then the pair $(V(G), \mathcal{C})$ is called an m-*cycle system* of G.

Let a pair $(V, \mathcal{C})$ be an m-cycle system of λK_v and Π be an *automorphism group* of the m-cycle system $(V, \mathcal{C})$. If π is an automorphism of order $v-1$ with a single fixed point, then the system $(V, \mathcal{C})$ is said to be 1-*rotational*. For a 1-rotational m-cycle system of λK_v, the vertex-set V can be identified with $\{\infty\} \cup \mathbb{Z}_{v-1}$. In this case, the automorphism can be represented by

$$\pi : \infty \mapsto \infty,\ i \mapsto i+1 \pmod{(v-1)} \quad \text{or} \quad \pi = (\infty)(0, 1, \ldots, v-2)$$

acting on the vertex-set $V = \{\infty\} \cup \mathbb{Z}_{v-1}$.

For an m-cycle system of λK_v, $(V, \mathcal{C})$, if the collection $\mathcal{C}$ of cycles can be partitioned into $s(= \lambda(v-1)/2)$ 2-factors (in terms of block designs, *resolution classes*), $R_1, \ldots, R_s$, then the system $(V, \mathcal{C})$ is said to be *resolvable* and $\mathcal{R} = \{R_1, \ldots, R_s\}$ is called a *resolution* of the system. Obviously, for the existence of a resolvable m-cycle system of λK_v, $v \equiv 0 \pmod{m}$ and $\lambda(v-1) \equiv 0 \pmod{2}$ are necessary.

A 1-rotational m-cycle system is said to be 1-*rotationally resolvable* when it admits $\pi = (\infty)(0, 1, \ldots, v-2)$ as an automorphism leaving a resolution invariant.

Rodger [4] surveyed the existence results of m-cycle systems of λK_v and those with several properties including resolvability. Recently the authors [3] proved through 'extended Skolem sequences' that a 1-rotationally resolvable 4-cycle system of $2K_v$ exists if and only if $v \equiv 0 \pmod{4}$.

Our purpose is, generalizing the idea of [3], to establish a necessary and sufficient condition for the existence of a 1-rotationally resolvable even-cycle system of $2K_v$.

2. Equivalent problems

It is known that for any $(2m, 2)$-admissible v, i.e., $v \equiv 0, m \pmod{2m}$, there exists a $2m$-cycle system of $2K_v$. For a $2m$-cycle system of $2K_v$ to be resolvable, it is necessary that $2m$ divides v. On the other hand, by noting that any 1-rotational $2m$-cycle system of $2K_v$ consists of $v/(2m)$ full cycle orbits, $v \equiv 0 \pmod{2m}$ is a necessary condition also for the existence of a 1-rotational $2m$-cycle system of $2K_v$. Accordingly we have the following.

Lemma 2.1 *A necessary condition for the existence of a* 1*-rotationally resolvable* $2m$*-cycle system of* $2K_v$ *is that* $v \equiv 0 \pmod{2m}$.

A *k-extended Skolem sequence* of order t is a sequence $(s_1, \ldots, s_{2t+1})$ of $2t+1$ integers in which $s_k = 0$ and for each $j \in \{1, \ldots, t\}$, there exists a unique $i \in \{1, \ldots, 2t+1\} \setminus \{k\}$ such that $s_i = s_{i+j} = j$. A k-extended Skolem sequence of order t is also represented as a collection of ordered pairs $\{(a_j, b_j) : 1 \le j \le t,\ b_j - a_j = j\}$ with $\cup_{j=1}^{t}\{a_j, b_j\} = \{1, 2, \ldots, 2t+1\} \setminus \{k\}$. If $k = t+1$, the sequence is often referred to as a *Rosa sequence* or a *split Skolem sequence* (see [2]). Baker [1] settled the spectrum of k-extended Skolem sequences of order t.

Theorem 2.2 ([1]) *There exists a* k*-ext* $\mathcal{S}_t$, $1 \le k \le 2t+1$, *if and only if either*
(1) k *is odd and* $t \equiv 0$ *or* $1 \pmod 4$; *or*
(2) k *is even and* $t \equiv 2$ *or* $3 \pmod 4$.

Here we will utilize the same extended Skolem sequences as in [3] to settle the existence problem of 1-rotationally resolvable $2m$-cycle systems of $2K_v$ for general $m \ge 2$.

Without loss of generality, let $v = 2m(t+1)$ and thus $V = \{\infty\} \cup \mathbb{Z}_{2m(t+1)-1}$ for $t \geq 0$. Since any 1-rotationally resolvable $2m$-cycle system of $2K_v$ consists of $v/(2m)$ full cycle orbits, it suffices to find the $v/(2m)$ base cycles which partition the vertex-set of K_v.

Construction I (for the case $t \equiv 0, 3 \pmod 4$). Let $\{(a_j, b_j) : 1 \leq j \leq t\}$ be a $(t+1)$-ext $\mathcal{S}_t$ (as a collection of ordered pairs). Take the following t $2m$-cycles.

$$\begin{aligned}\{(&ma_j - 1, m(b_j+1) - 2, ma_j, m(b_j+1) - 3, \dots, \\ &m(a_j+1) - 3, mb_j, m(a_j+1) - 2, mb_j - 1) : 1 \leq j \leq t\}\end{aligned} \tag{2.1}$$

Besides (2.1), we can take one more cycle consisting of the $2m$ vertices $\{0, \dots, m-2\} \cup \{m(t+1) - 1, \dots, m(t+2) - 2\} \cup \{\infty\}$ so that the rest of the differences, $\pm\{1, 2, \dots, m-1, mt+1, mt+2, \dots, m(t+1) - 1, \infty, \infty\}$, may occur.

Construction II (for the case $t \equiv 1, 2 \pmod 4$). Assume that $\{(a_j, b_j) : 1 \leq j \leq t\}$ is a t-ext $\mathcal{S}_t$ satisfying $(a_t, b_t) = (t+1, 2t+1)$. First we make $t-1$ cycles just as (2.1) but for $1 \leq j \leq t-1$.

$$\begin{aligned}\{(&ma_j - 1, m(b_j+1) - 2, ma_j, m(b_j+1) - 3, \dots, \\ &m(a_j+1) - 3, mb_j, m(a_j+1) - 2, mb_j - 1) : 1 \leq j \leq t-1\}\end{aligned}$$

Two more cycles can be formed to use up the rest of the vertices, $\{0, 1, \dots, m-2\} \cup \{mt - 1, \dots, m(t+2) - 2\} \cup \{m(2t+1) - 1, \dots, m(2t+2) - 2\} \cup \{\infty\}$, and to cover the $4m$ differences $\pm\{1, 2, \dots, m-1, m(t-1)+1, m(t-1)+2, \dots, mt-1, mt, mt, mt+1, mt+1, \dots, m(t+1)-1, m(t+1) - 1, \infty, \infty\}$.

3. Existence results

Since the existence of a $(t+1)$-ext $\mathcal{S}_t$ with $t \equiv 0, 3 \pmod 4$ implies that of a 1-rotationally resolvable $2m$-cycle system of $2K_v$ with $v \equiv 2m, 0 \pmod{8m}$, respectively, Theorem 2.2 and Construction I ensure the following.

Theorem 3.1 *There exists a 1-rotationally resolvable $2m$-cycle system of $2K_v$ whenever $v \equiv 0, 2m \pmod{8m}$.*

Recent result due to the authors [3] almost completes the sufficiency of Lemma 2.1.

Theorem 3.2 ([3]) *Whenever $t \equiv 1, 2 \pmod 4$ and $t \geq 6$, there exists a t-ext $\mathcal{S}_t$ (as a collection of ordered pairs) including the pair $(t+1, 2t+1)$.*

From Theorem 3.2 and Construction II, we can state the following immediately.

Corollary 3.3 *There exists a 1-rotationally resolvable $2m$-cycle system of $2K_v$ whenever $v \equiv 4m, 6m \pmod{8m}$ and $v \geq 14m$.*

Unfortunately there does not exist a t-ext $\mathcal{S}_t$ satisfying the required condition when $t = 1, 2$ and 5, which implies that Construction II cannot be applied for the cases $v = 4m, 6m$ and $12m$. This means that we need to make up for those cases with direct constructions. So far, we proved for the cases $v = 4m$ and $6m$, and can state the following from Theorem 3.1 and Corollary 3.3.

Theorem 3.4 *There exists a 1-rotationally resolvable $2m$-cycle system of $2K_v$ if and only if $v \equiv 0 \pmod{2m}$ with a possible exception $v = 12m$.*

References

[1] C. A. Baker, Extended Skolem sequences, J. Combin. Des. 3 (1995), 363–379.

[2] C. J. Colbourn and A. Rosa, Triple systems, Oxford University Press, New York, 1999.

[3] H.-L. Fu and M. Mishima, 1-Rotationally resolvable 4-cycle systems of $2K_v$, J. Combin. Des., to appear.

[4] C. A. Rodger, "Cycle systems" in The CRC Handbook of Combinatorial Designs, C. J. Colbourn and J. H. Dinitz (Editors), CRC Press, Boca Raton, FL, 1996, pp.266–270.

BIB デザインとpacking/covering デザインの探索のための推論システム

慶應大・理工　佐藤 秀
慶應大・理工　大原 幸多

1　はじめに

近年，実験計画のみならず符号や暗号の分野で組合せデザインが用いられ，情報通信分野での利用についての研究も始まっている．組合せデザインの１つであるBIBデザインの構成法や存在・非存在に関する問題は古くから研究がなされており，有限アフィン幾何・有限射影幾何を用いる構成法，有限体を用いる構成法，逐次構成法などの多くの構成法が知られている．これらの構成法を用いて作られたBIBデザインの表が統計学辞典などにまとめられている．しかし，符号・暗号等の情報通信分野ではこれらの表のパラメータの値を越えた大きなデザインを用いることが多い．従って，与えられたパラメータを持つデザインを構成して出力するシステムの構築が必要とされる．

昨年，存在・非存在に関する既知の定理を組み込むことによりユーザーによって与えられた入力パラメータに対応するBIBデザインの存在・非存在を判定する推論システム“DesNavi”を構築したが，本研究ではさらに，BIBデザインが存在する場合は実際にそのデザインを構成する機能を加えた．また，packingデザイン，coveringデザインに関する定理も組み込んでいる．

2　DesNavi(Design Navigation system)

DesNaviは，ブラウザによってサーバとクライアントを接続するためにJava言語を用い，有限体と因数分解の計算，素数判定にMathematica4.1を使い，C言語によって核の部分が記述されている．C言語によって，より高速な計算が可能となり，MathLinkによりC-Mathematica間の通信が実現されている．クライアント側にはJavaアプレットを採用したため，Java対応のWebブラウザのみでこのシステムを使用することが可能である．(図１)

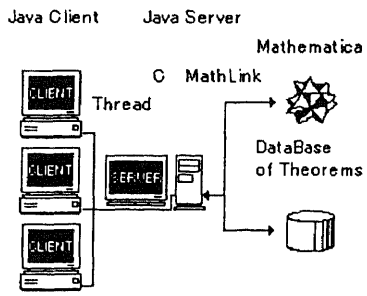

図 1: DesNavi system

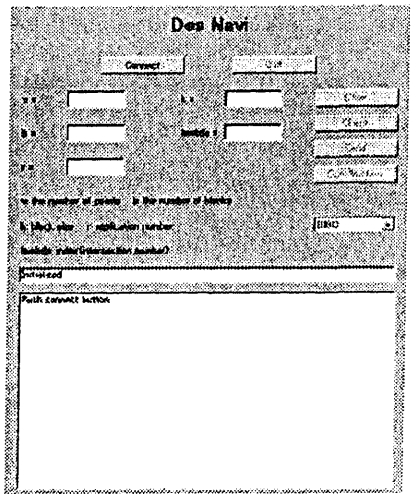

図 2: クライアント画面

クライアントによって送られたパラメータに対して，合致する存在･非存在定理をサーバが探索を行い，もしデザインが存在すれば，実際のデザインを構成し結果を定理とともにクライアントへ返す．ここでクライアントに返される定理は，探索過程で最初にパラメータに合致した定理である．竹内 (1989)，Beth, Jungnichel, and Lenz (1986)，Mathon and Rosa(1996) らによる BIB デザインの表はこのシステムに組み込まれた定理群から導出される．DesNavi に組み込まれているどの定理にも合致せず，かつデータベースに蓄積されていないパラメータに対しては“unknown”をクライアントに返す．BIB デザインの構成については，現状で有限アフィン幾何・有限射影幾何による方法，有限体による方法，cyclic difference family, cyclic difference set による方法をシステムに組み込んでいる．また，packing，covering デザインに関しては，クライアントより送られたパラメータ v, k, λ を持つデザインは多数存在する．サーバは packing (covering) デザインの最大 (最小) ブロック数に関する定理を探索し，ブロック数が Johnson bound (Schönheim bound) で与えられる上限 (下限) と一致するデザインが存在すれば，そのブロック数を定理とともにクライアントへ返す．存在しないときは，最大 (最小) ブロック数のとりうる値の範囲を返す．

3 動作例

図 3 はクライアントが点の数 $v = 1464$，ブロックサイズ $k = 12$，会合数 $\lambda = 1$ を入力したときの BIB デザインの存在・非存在の判定と構成の結果である．この BIB デザイン $B[12, 1; 1464]$ は $PG_1(3, 11)$ で構成されることがわかり，初期ブロックが表示される．DesNavi においては一般に，デザインの構成は初期ブロックを表示する．

```
==========================================
B[12,1;1464] is made from PG_1(3,11)
==========================================
PG_1(3,11) is B[12,1;1464].
The base blocks :
( 0 1 4 530 548 675 698 874 984 1105 1330 1412)
( 0 11 44 105 172 358 443 576 830 892 1438 1454)
( 0 2 252 282 394 494 623 702 711 971 1078 1371)
( 0 22 146 174 402 433 441 501 997 1042 1308 1406)
( 0 5 108 189 478 635 713 815 850 954 1017 1350)
( 0 55 181 210 246 523 566 615 866 939 1129 1188)
( 0 6 48 207 513 633 673 724 774 961 1244 1276)
( 0 66 83 323 508 528 644 813 860 1107 1194 1251)
( 0 7 84 158 170 281 413 519 712 931 1324 1395)
( 0 13 109 234 275 498 652 1003 1067 1281 1300 1315)
( 0 25 97 143 785 915 1086 1110 1124 1199 1289 1316)
( 0 122 244 366 488 610 732 854 976 1098 1220 1342)
mod 1464
```

図 3: B[12, 1; 1464] の判定結果

Partially balanced fractional $2^{m_1+m_2}$ factorial designs of resolution IV

Subir Ghosh (Univ. California)　　栗田 正秀 (広島大・総合科学)
兵頭 義史 (岡山理大・理, 国際自然研)　　弓場 弘 (国際自然研)

単純部分均斉配列 SPBA$(m_1+m_2;\{\lambda_{i_1i_2}\})$ (i.e. PBA$(N, m_1+m_2, 2, m_1+m_2; \{\lambda_{i_1i_2}\})$) から得られる $2^{m_1+m_2}$-PBFF 計画 T を考える. ただし, 3 因子以上の高次交互作用は無視可能とし, $m_1, m_2 \geq 2$ とする. このとき, T に基づく線形模型は, $\varepsilon[\boldsymbol{y}(T)] = E_T\Theta$, $\mathrm{Var}[\boldsymbol{y}(T)] = \sigma^2 I_N$ で与えられる. ただし, $\boldsymbol{y}(T)$: $N\times 1$ 観測値ベクトル, E_T : $N\times\nu(m_1,m_2)$ 計画行列, $\Theta = (\Theta'_{00};\Theta'_{10};\Theta'_{01};\Theta'_{20};\Theta'_{02};\Theta'_{11})'$: 2-因子交互作用までの $\nu(m_1,m_2)\times 1$ 要因効果ベクトル, $\nu(m_1,m_2) = 1+m_1+m_2+\binom{m_1+m_2}{2}$ である.

ETMDPB アソシエーション代数 $\Omega = [D^{\#(a_1a_2,b_1b_2)}_{\beta_1\beta_2}]$ の性質を用いて, 情報行列 $M_T\,(=E'_TE_T)$ は,

$$M_T = \sum_{\beta_1\beta_2}\sum_{a_1a_2}\sum_{b_1b_2}\kappa^{a_1a_2,b_1b_2}_{\beta_1\beta_2}D^{\#(a_1+\beta_1a_2+\beta_2,b_1+\beta_1b_2+\beta_2)}_{\beta_1\beta_2}$$

で与えられる. ただし, 実対称行列 $K_{\beta_1\beta_2} = [\kappa^{a_1a_2,b_1b_2}_{\beta_1\beta_2}]$ の各要素は, 指標 $\lambda_{i_1i_2}$ のある線形式として与えられる. また M_T は, 次のブロック対角行列と相似である :

$$\mathrm{diag}(K_{00};\overbrace{K_{10},\cdots,K_{10}}^{\phi_{10}};\overbrace{K_{01},\cdots,K_{01}}^{\phi_{01}};\overbrace{K_{20},\cdots,K_{20}}^{\phi_{20}};\overbrace{K_{02},\cdots,K_{02}}^{\phi_{02}};\overbrace{K_{11},\cdots,K_{11}}^{\phi_{11}})$$

ただし, $K_{00}: 6\times 6$; $K_{10}: 3\times 3\,(m_1\geq 3)$, $2\times 2\,(m_1=2)$; $K_{01}: 3\times 3\,(m_2\geq 3)$, $2\times 2\,(m_2=2)$; $K_{20}: 1\times 1\,(m_1\geq 4)$; $K_{02}: 1\times 1\,(m_2\geq 4)$; $K_{11}: 1\times 1$, $\phi_{\beta_1\beta_2} = \left\{\binom{m_1}{\beta_1}-\binom{m_1}{\beta_1-1}\right\}\left\{\binom{m_2}{\beta_2}-\binom{m_2}{\beta_2-1}\right\}$ である.

本報告では, ETMDPB アソシエーション代数の性質および行列方程式を用いて, 次の (A)~(E) の場合について, それらの要因効果ベクトルが推定可能となる分解能 IV の $2^{m_1+m_2}$-PBFF 計画を与えた :

(A) $\Theta^{\mathrm{A}} \equiv (\Theta'_{00};\Theta'_{10};\Theta'_{01};\Theta'_{20};\Theta'_{02})'$
(B) $\Theta^{\mathrm{B}} \equiv (\Theta'_{00};\Theta'_{10};\Theta'_{01};\Theta'_{20};\Theta'_{11})'$ (or $(\Theta'_{00};\Theta'_{10};\Theta'_{01};\Theta'_{02};\Theta'_{11})'$)
(C) $\Theta^{\mathrm{C}} \equiv (\Theta'_{00};\Theta'_{10};\Theta'_{01};\Theta'_{20})'$ (or $(\Theta'_{00};\Theta'_{10};\Theta'_{01};\Theta'_{02})'$)
(D) $\Theta^{\mathrm{D}} \equiv (\Theta'_{00};\Theta'_{10};\Theta'_{01};\Theta'_{11})'$
(E) $\Theta^{\mathrm{E}} \equiv (\Theta'_{00};\Theta'_{10};\Theta'_{01})'$

(A) の場合

定理 1　$\Theta^{\mathrm{A}} \equiv (\Theta'_{00};\Theta'_{10};\Theta'_{01};\Theta'_{20};\Theta'_{02})'$: 推定可能 $\iff$ $K_{20}(=\kappa^{00,00}_{20})\neq 0$ $(m_1\geq 4)$, $K_{02}(=\kappa^{00,00}_{02})\neq 0$ $(m_2\geq 4)$ および次の条件 (I) または (II) が成り立つ :

(I) $\det(K_{00})\neq 0$ のとき
　(i) $\det(K_{10})\neq 0$ かつ
　　(a) $\det(K_{01})\neq 0 \implies K_{11}(=\kappa^{00,00}_{11}) = 0$ or
　　(b) $\det(K_{01}) = 0 \implies m_1 = 2n_1\,(n_1\geq 1)$, $\det(K^{\mathrm{A}}_{01}(11))\neq 0$, $\kappa^{10,10}_{01} = 0$ or
　(ii) $\det(K_{10}) = 0 \implies m_2 = 2n_2\,(n_2\geq 1)$, $\det(K^{\mathrm{A}}_{10}(11))\neq 0$, $\kappa^{01,01}_{10} = 0$, $\det(K_{01})\neq 0$
(II) $\det(K_{00}) = 0$ のとき
　$m_1 = 2n_1\,(n_1\geq 1)$, $m_2 = 2n_2\,(n_2\geq 1)$, $\det(K^{\mathrm{A}}_{00}(11))\neq 0$, $\kappa^{11,11}_{00} = 0$, $\det(K_{10})\neq 0$, $\det(K_{01})\neq 0$

ただし, $K^{\mathrm{A}}_{00}(11)$: K_{00} の最初の 5×5 部分行列 ; $K^{\mathrm{A}}_{10}(11)$: K_{10} の最初の $2\times 2\,(m_1\geq 3)$, $1\times 1\,(m_1=2)$; $K^{\mathrm{A}}_{01}(11)$: K_{01} の最初の $2\times 2\,(m_2\geq 3)$, $1\times 1\,(m_2=2)$

[注意] ある $\eta_1\eta_2\,(=00,10,01,11)$ に対して, $\det(K_{\eta_1\eta_2})\neq 0 \implies A^{\#(11,11)}_{\eta_1\eta_2}\Theta_{11}$ も推定可能となる. ただし, $A^{\#(a_1a_2,b_1b_2)}_{\beta_1\beta_2}$: $D^{\#(a_1a_2,b_1b_2)}_{\beta_1\beta_2}$ の $n(a_1a_2)\times n(b_1b_2)$ 部分行列 $(n(a_1a_2) = \binom{m_1}{a_1}\binom{m_2}{a_2})$

例 1 T を SPBA$(2+2;\{\lambda_{00}=\lambda_{01}=\lambda_{02}=\lambda_{11}=\lambda_{20}=\lambda_{22}=1\,,\ \lambda_{10}=\lambda_{12}=\lambda_{21}=0\})$ とする．このとき，

$$K_{00}=\begin{bmatrix} 10 & -2\sqrt{2} & 0 & 2 & -2 & 0 \\ -2\sqrt{2} & 12 & 0 & -2\sqrt{2} & 2\sqrt{2} & 0 \\ 0 & 0 & 8 & 0 & 0 & 0 \\ 2 & -2\sqrt{2} & 0 & 10 & 6 & 0 \\ -2 & 2\sqrt{2} & 0 & 6 & 10 & 0 \\ 0 & 0 & 0 & 0 & 0 & 16 \end{bmatrix} \qquad K_{10}=\begin{bmatrix} 8 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\det(K_{10})=0$$

$$K_{01}=\begin{bmatrix} 12 & -4\sqrt{2} \\ -4\sqrt{2} & 8 \end{bmatrix}$$

$$\det(K_{01})=64$$

$$\det(K_{00})=524288 \qquad K_{11}(=\kappa_{11}^{00,00})=16$$

$\Longrightarrow$ $\det(K_{00})\neq 0$, $\det(K_{10})=0$, $K_{10}^{\mathrm{A}}(11)$ $(=\kappa_{10}^{00,00})\neq 0$, $\kappa_{10}^{01,01}=0$, $\det(K_{01})\neq 0$ であるから Θ^{A} は推定可能である．さらに $\det(K_{00})\neq 0$, $\det(K_{01})\neq 0$, $K_{11}(=\kappa_{11}^{00,00})\neq 0$ より $A_{00}^{\#(11,11)}\Theta_{11}$, $A_{01}^{\#(11,11)}\Theta_{11}$, $A_{11}^{\#(11,11)}\Theta_{11}$ も推定可能となる．

(B) の場合

定理 2 $\Theta^{\mathrm{B}}\equiv(\Theta_{00}';\Theta_{10}';\Theta_{01}';\Theta_{20}';\Theta_{11}')'$: 推定可能 $\Longleftrightarrow$ $\det(K_{10}^{\mathrm{B}})\neq 0$,
$K_{20}^{\mathrm{B}}(=\kappa_{20}^{00,00})\neq 0$ $(m_1\geq 4)$, $K_{11}^{\mathrm{B}}(=\kappa_{11}^{00,00})\neq 0$ および次の条件 (I) または (II) が成り立つ：

(I) $\det(K_{00}^{\mathrm{B}})\neq 0$ のとき

(i) $\det(K_{01}^{\mathrm{B}})\neq 0 \Longrightarrow m_2\geq 4$, $K_{02}^{\mathrm{B}}(=\kappa_{02}^{00,00})=0$ or

(ii) $\det(K_{01}^{\mathrm{B}})=0 \Longrightarrow m_2=2n_2$ $(n_2\geq 2)$, $\det(K_{01}^{\mathrm{B}}(11))\neq 0$, $\kappa_{01}^{01,01}=0$

(II) $\det(K_{00}^{\mathrm{B}})=0$ のとき

$m_2=k_2^2$ $(k_2\geq 2)$, $\det(K_{00}^{\mathrm{B}}(11))\neq 0$, $\kappa_{00}^{02,02}=0$, $\det(K_{01}^{\mathrm{B}})\neq 0$

ただし，$K_{00}^{\mathrm{B}}(11)$: K_{00}^{B} の最初の 5×5 部分行列；$K_{01}^{\mathrm{B}}(11)$: K_{01}^{B} の最初の 2×2 $(m_2\geq 3)$

例 2 T を SPBA$(2+4;\{\lambda_{03}=\lambda_{11}=\lambda_{13}=\lambda_{21}=\lambda_{23}=1\,,\ \lambda_{00}=\lambda_{01}=\lambda_{02}=\lambda_{04}=\lambda_{10}=\lambda_{12}=\lambda_{14}=\lambda_{20}=\lambda_{22}=\lambda_{24}=0\})$ とする．このとき，

$$K_{00}^{\mathrm{B}}=\begin{bmatrix} 28 & 4\sqrt{2} & 4 & -4 & -4\sqrt{2} & 0 \\ 4\sqrt{2} & 24 & -4\sqrt{2} & 4\sqrt{2} & 8 & 0 \\ 4 & -4\sqrt{2} & 28 & 4 & 4\sqrt{2} & 0 \\ -4 & 4\sqrt{2} & 4 & 28 & -4\sqrt{2} & 0 \\ -4\sqrt{2} & 8 & 4\sqrt{2} & -4\sqrt{2} & 24 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \qquad K_{10}^{\mathrm{B}}=\begin{bmatrix} 32 & 0 \\ 0 & 32 \end{bmatrix}$$

$$\det(K_{10}^{\mathrm{B}})=1024$$

$$K_{01}^{\mathrm{B}}=\begin{bmatrix} 28 & 4\sqrt{2} & 4\sqrt{2} \\ 4\sqrt{2} & 24 & -8 \\ 4\sqrt{2} & -8 & 56 \end{bmatrix}$$

$$\det(K_{01}^{\mathrm{B}})=32768$$

$$\det(K_{00}^{\mathrm{B}})=0\,,\quad \det(K_{00}^{\mathrm{B}}(11))=4194304$$

$$K_{02}^{\mathrm{B}}(=\kappa_{02}^{00,00})=0\,,\quad K_{11}^{\mathrm{B}}(=\kappa_{11}^{00,00})=32$$

$\Longrightarrow$ $\det(K_{00}^{\mathrm{B}})=0$, $\det(K_{00}^{\mathrm{B}}(11))\neq 0$, $\kappa_{00}^{02,02}=0$, $\det(K_{10}^{\mathrm{B}})\neq 0$, $\det(K_{01}^{\mathrm{B}})\neq 0$, $K_{11}^{\mathrm{B}}(=\kappa_{11}^{00,00})\neq 0$ であるから Θ^{B} は推定可能である．さらに $\det(K_{01}^{\mathrm{B}})\neq 0$ より $A_{01}^{\#(02,02)}\Theta_{02}$ も推定可能となる．

(C)～(E) の場合に関する定理および例については省略する．

GA-optimal balanced fractional 2^m factorial designs of resolution R($\{0,1\}|3$)

広島大・総合科学　　桒田 正秀
岡山理大・理, 国際自然研　兵頭 義史
国際自然研　　弓場 弘

次のような線形模型を考える：

$$\varepsilon[\boldsymbol{y}(T)] = E_T\boldsymbol{\theta},\ \mathrm{Var}[\boldsymbol{y}(T)] = \sigma^2 I_N$$

ただし, T: SA$(m;\{\lambda_i\})$, $\boldsymbol{y}(T)$: 観測値ベクトル $(N\times 1)$, E_T: 計画行列 $(N\times\nu_3)$, $\boldsymbol{\theta} = (\theta_\phi;\boldsymbol{\theta}_1';\boldsymbol{\theta}_2';\boldsymbol{\theta}_3')'$: 3-因子交互作用までの要因効果ベクトル $(\nu_3\times 1)$; $N = \sum_{i=0}^{m}\binom{m}{i}\lambda_i$, $\nu_3 = \sum_{i=0}^{3}\binom{m}{i}$ である.

TMDPB アソシエーション代数 $\Omega = [D_\beta^{\#(a,b)}]$ の性質を用いて, 情報行列 $M_T(=E_T'E_T)$ は,

$$M_T = \sum_{\beta=0}^{3}\sum_{a=0}^{3-\beta}\sum_{b=0}^{3-\beta}\kappa_\beta^{a,b}D_\beta^{\#(a+\beta,b+\beta)}$$

で与えられる. ただし, 実対称行列 $K_\beta = ||\kappa_\beta^{a,b}||$ の各要素は, 指標 λ_i のある線形式として与えられる. この M_T は, 次のブロック対角行列と相似である:

$$\mathrm{diag}(K_0;\overbrace{K_1,\cdots,K_1}^{\phi_1};\overbrace{K_2,\cdots,K_2}^{\phi_2};\overbrace{K_3,\cdots,K_3}^{\phi_3})$$

ただし, K_β: $(4-\beta)$ 次行列; $\phi_\beta = \binom{m}{\beta} - \binom{m}{\beta-1}$ である.

TMDPB アソシエーション代数および行列方程式を用いて, 次を得る:

定理　単純配列 SA$(m,\{\lambda_i\})$ を用いた 2^m-BFF 計画 T を考える. ただし, 4 因子以上の高次交互作用は無視可能とし, $N<\nu_3$ とする. このとき, 少なくとも一般平均と主効果が推定可能となる計画は, 次の (1)〜(8) の指標に関する条件を満たすものに限られる:

分解能 R($\{0,1\}|3$) の計画

(1) (a) $m=2n+1(n\geq 3)$; $\lambda_0,\lambda_1,\lambda_{n+1},\lambda_m>0$, その他の指標: 0,
(b) $m=2n+1(n\geq 3)$; $\lambda_0,\lambda_n,\lambda_{m-1},\lambda_m>0$, その他の指標: 0,

(2) (a) $\lambda_0+\lambda_m>0$,$\lambda_1,\lambda_2,\lambda_{m-1}>0$, その他の指標: 0,
(b) $\lambda_0+\lambda_m>0$,$\lambda_1,\lambda_{m-2},\lambda_{m-1}>0$, その他の指標: 0,

(3) $\lambda_0+\lambda_m>0$,$\lambda_1,\lambda_{m-1},\lambda_i>0(i(\neq\frac{m}{2})\in\{3,\cdots,m-3\})$,
その他の指標: 0,

分解能 R($\{0,1,2\}|3$)(i.e., 分解能 VI) の計画

(4) $m=2n(n\geq 3)$; $\lambda_0+\lambda_m>0,\lambda_1,\lambda_n,\lambda_{m-1}>0$, その他の指標: 0,

(5) $m=6$; $\lambda_1,\lambda_3,\lambda_5>0$, その他の指標: 0,

(6) $m=6$; $\lambda_0,\lambda_2,\lambda_4,\lambda_6>0$, その他の指標: 0,

(7) (a) $\lambda_0+\lambda_m>0$, $\lambda_1,\lambda_2,\lambda_{m-2}>0$, その他の指標: 0,
(b) $\lambda_0+\lambda_m>0$, $\lambda_2,\lambda_{m-2},\lambda_{m-1}>0$, その他の指標: 0,

(8) $\lambda_0,\lambda_m\geq 0$, $\lambda_1,\lambda_2,\lambda_{m-2},\lambda_{m-1}>0$, その他の指標: 0.

定義 単純配列 T を $C(\alpha)\Theta$ が推定可能な 2^m-BFF 計画とする. このとき, 与えられた (N,m) に対して, $S_T(\alpha)$ が最小となる計画を GA_α-最適計画という. ただし,

$$\Theta:\ c\text{-因子交互作用までの要因効果ベクトル},$$

$$C(\alpha)=\sum_{\beta=0}^{a}\sum_{p=\beta}^{a}D_\beta^{\#(p,p)}+\sum_{\beta=0}^{c}\sum_{q=g(\beta)}^{b(\beta)}x_\beta^q(\alpha)\Big\{D_\beta^{\#(q,q)}+\sum_{r=b(\beta)+1}^{c}w_\beta^{q,r}D_\beta^{\#(q,r)}\Big\},$$

$$S_T(\alpha)=\frac{1}{\sigma^2}\mathrm{tr}(\mathrm{Var}[C(\alpha)\hat{\Theta}])$$

$$=\sum_{\beta=0}^{c}\phi_\beta\mathrm{tr}(X_\beta(K_\beta^{(b(\beta)-\beta+1)})^{-1}X_\beta),$$

$$X_\beta=\begin{cases}\mathrm{diag}(I_{g(\beta)-\beta};x_\beta^{g(\beta)}(\alpha);\cdots;x_\beta^{b(\beta)}(\alpha)) & (0\le\beta\le a),\\ \mathrm{diag}(x_\beta^{g(\beta)}(\alpha);\cdots;x_\beta^{b(\beta)}(\alpha)) & (a+1\le\beta\le c).\end{cases}$$

$x_\beta^q(\alpha)$: 任意定数, $w_\beta^{q,r}$: 既知定数, $b(\beta)=\mathrm{rank}[K_\beta]+(\beta-1)$, $g(\beta)=\max[\beta,a+1]$, $K_\beta^{(r)}$:K_β の最初の $r\times r$ 部分行列とする. ここでは, $\det(K_\beta)\neq 0$ のとき, $w_\beta^{u,v}=0$ と規約する.

本報告では, $x_\beta^b(\alpha)$ として,

$$x_\beta^b(0)=1,\quad x_\beta^b(1)=\Big\{1+\textstyle\sum_{q=1}^{c}|w_\beta^{b,q}|\Big\}^{-1},$$

$$x_\beta^b(2)=\Big\{1+\textstyle\sum_{q=1}^{c}(w_\beta^{b,q})^2\Big\}^{-\frac{1}{2}}$$

を用いた場合の GA_α-最適計画を与えた (結果は省略).

定理の (1)-(a) の場合:

$$\begin{aligned}C(\alpha) &= \textstyle\sum_{i=0}^{3}D_0^{\#(i,i)}+\Big\{D_1^{\#(1,1)}+x_1^2(\alpha)\Big(D_1^{\#(2,2)}-\sqrt{n-1}D_1^{\#(2,3)}\Big)\Big\}\\ &\quad +x_2^2(\alpha)\Big\{D_2^{\#(2,2)}+\frac{1}{\sqrt{2n-3}}D_2^{\#(2,3)}\Big\}+D_3^{\#(3,3)},\\ S_T(\alpha) &= \mathrm{tr}(K_0^{-1})+\phi_1\mathrm{tr}\left(\begin{bmatrix}1&0\\0&x_1^2(\alpha)\end{bmatrix}\begin{bmatrix}\kappa_1^{0,0}&\kappa_1^{0,1}\\ \kappa_1^{1,0}&\kappa_1^{1,1}\end{bmatrix}^{-1}\begin{bmatrix}1&0\\0&x_1^2(\alpha)\end{bmatrix}\right)\\ &\quad +\frac{\phi_2(x_2^2(\alpha))^2}{\kappa_2^{0,0}}+\frac{\phi_3}{\kappa_3^{0,0}}.\end{aligned}$$

また, $x_1^2(\alpha)$, $x_2^2(\alpha)$ は次の通りである:

$$x_1^2(\alpha)=\begin{cases}1 & (\alpha=0),\\ \frac{1}{1+\sqrt{n-1}} & (\alpha=1),\\ \frac{1}{\sqrt{n}} & (\alpha=2),\end{cases}\qquad x_2^2(\alpha)=\begin{cases}1 & (\alpha=0),\\ \frac{\sqrt{2n-3}}{\sqrt{2n-3}+1} & (\alpha=1),\\ \frac{\sqrt{2n-3}}{\sqrt{2(n-1)}} & (\alpha=2).\end{cases}$$

定理の (2)~(8) については省略する.

参 考 文 献

[1] Ghosh, S., Kuwada, M., 2001. Some estimable parametric functions for balanced fractional 3^m factorial designs. Statistical Reserch Group, TR #01-6, Hiroshima University, Higashi-Hiroshima, Japan

[2] Ghosh, S., Kuwada, M., 2001. Estimable parametric functions for balanced fractional 2^m factorial designs. Statistical Reserch Group, TR #01-7, Hiroshima University, Higashi-Hiroshima, Japan

MEP.3 計画の構成について

神戸市立工業高専　末次武明
神戸大学発達科学部　白倉暉弘

1．はじめに

2^m $(m \geq 6)$ 要因計画で，T_1 : weight(1 の数) が $0, 1, m-1$ の処理組合せを全部集めた計画とするとき、$T = T_1 + T_2$（"+" は２つの計画の並置）が MEP.3 計画（主効果が全て推定可能で，２因子交互作用から高々３個の未知効果が検索できる）であるような計画 T_2 を構成することを考える．

この問題は、Shirakura, Suetsugu and Tsuji(To appear) が MEP.2 計画を構成したのと同様の仕組みを考えて，MEP.3 plan の構成を目指すものである．

誤差がないという仮定の下で，Srivastava (1975) の基本定理は，この場合，次のように表される．

「T が MEP.3 計画であるための必要十分条件は，$s \neq s'$ なら $1 \leq p_s < q_s \leq m$, $(p_s, q_s) \neq (p_{s'}, q_{s'})$ であるような、どんな (p_s, q_s), $1 \leq s \leq 6$ の選び方に対しても，行列 $G = [\mathbf{1}_N, \mathbf{g}_1, \cdots, \mathbf{g}_m, \mathbf{g}_{p_1q_1}, \mathbf{g}_{p_2q_2}, \mathbf{g}_{p_3q_3}, \mathbf{g}_{p_4q_4}, \mathbf{g}_{p_5q_5}, \mathbf{g}_{p_6q_6}]$ が　rank $G = m + 1 + 6$ $\cdots$ (1)　であることである.」

さらに、T の列ベクトル $\mathbf{t}_i$ について，$\mathbf{t}_{ju} = \mathbf{t}_j * \mathbf{t}_u$ とするとき，行列 $U = [\mathbf{1}_N, \mathbf{t}_1, \ldots, \mathbf{t}_m, \mathbf{t}_{p_1q_1}, \mathbf{t}_{p_2q_2}, \mathbf{t}_{p_3q_3}, \mathbf{t}_{p_4q_4}, \mathbf{t}_{p_5q_5}, \mathbf{t}_{p_6q_6}]$ を考えると，$\mathbf{t}_j$, $\mathbf{t}_{ju}$ が $\mathbf{g}_j$, $\mathbf{g}_{ju}$ の１次式で表されるので，rank G = rank U だから，(1) の条件を，T から直接作った U を使って，調べることができる．

2．この計画の特徴づけ

2.1 T_1 から言えること

上記の条件 (1) について、T_1 から、どれだけのことが言えるかを探る．まず、対応する行列 U_1 で，$(\mathbf{t}_{p_1q_1}, \cdots, \mathbf{t}_{p_6q_6})$ の rank が 6 であればよい事がわかる．さらに、$\mathbf{e}_{ju}$ は j 番目と u 番目が 0 で 他は 1 であるベクトルだとすると、

定理 1　U_1 で，$\left(\mathbf{e}_{p_1q_1} \quad \mathbf{e}_{p_2q_2} \quad \mathbf{e}_{p_3q_3} \quad \mathbf{e}_{p_4q_4} \quad \mathbf{e}_{p_5q_5} \quad \mathbf{e}_{p_6q_6} \right)$ の rank は 4 以上である．

さらに，$\lambda_1\mathbf{e}_{p_1q_1} + \lambda_2\mathbf{e}_{p_2q_2} + \lambda_3\mathbf{e}_{p_3q_3} + \lambda_4\mathbf{e}_{p_4q_4} + \lambda_5\mathbf{e}_{p_5q_5} + \lambda_6\mathbf{e}_{p_6q_6} = 0$ を考えると，一次従属の可能性のあるのは，p_i, q_i が次のような文字の組合せの場合だけである．

・「rank$(V_1) = 4$ の場合」

a) ４文字で，各文字の出現回数 (3,3,3,3)　b) ５文字で，各文字の出現回数 (3,3,2,2,2)

・「rank$(V_1) = 5$ の場合」

c) ５文字で，各文字の出現回数 (4,2,2,2,2)　d) ６文字で，各文字の出現回数 (2,2,2,2,2,2)
e) ５文字で，各文字の出現回数 (4,3,2,2,1)　f) ６文字で，各文字の出現回数 (4,2,2,2,1,1)
g) ６文字で，各文字の出現回数 (3,3,2,2,1,1)　h) ７文字で，各文字の出現回数 (3,2,2,2,1,1,1)
i) ７文字で，各文字の出現回数 (2,2,2,2,2,1,1)　j) ８文字で，各文字の出現回数 (2,2,2,2,1,1,1,1)

2.2 さらに，T_2 が ST-array を含むことで言えること

Shirakura,T. and Suetsugu,T and Tsuji,T(To appear) で，上記の T_1 に対して、MEP.2 計画になる T_2 は、「どの４列を取っても，$\binom{1}{1}, \binom{1}{0}, \binom{0}{1}, \binom{0}{0}$ が全て含まれているような２行が存在する」という条件を満たす行列 (ST-array) であることを示した．

さらに、彼らの結果から，次の ST-array の３つのタイプを考える．

・ Linear code を使う (LC タイプと呼ぶことにする)
・ BIBD の転値行列を使う (BI タイプ)
・ Q.R. を利用する (QR タイプ)

次に，上記の T_1 について、T_2 が ST-array を含むときに，成り立つことを探る．

定理 2 T_2 が ST-array を含むとき，U の部分行列 $V=(\mathbf{t}_{p_1q_1}\ \mathbf{t}_{p_2q_2}\ \mathbf{t}_{p_3q_3}\ \mathbf{t}_{p_4q_4}\ \mathbf{t}_{p_5q_5}\ \mathbf{t}_{p_6q_6})$ の rank は 5 以上である.

さらに、次のことが成り立つ.

1) 「 (a) の場合は，$\mathrm{rank}(V)=6$ 」

2) 「(e),(f),(g),(h),(i),(j) の場合は同じ構造で，$\mathrm{rank}(V)=6$ 」

3) 「T_2 が ST-array を含んでも，(c) の場合は $\mathrm{rank}(V)=5$ の場合が存在する.」

$m=6$ の場合に反例がある.

4) 「T_2 が QR や BI や LC タイプでは，(b), (c) の場合も $\mathrm{rank}(V)=5$ の場合はなく，$\mathrm{rank}(V)=5$ の可能性があるのは，(d) の 6 文字の場合に限る.」 (証明まだ)

5) (d) の 6 文字の場合に $\mathrm{rank}(V)=6$ になる (一次従属にならない) ためには，もとの T_2 で，次のどの条件かを満たす行があればよい.

	a	a	b	c	d	e
	b	c	d	e	f	f
λ	1	−1	−1	1	1	−1

を仮定する.

・weight 2 のとき：T_2 で 1 になる列が，{a,b}，～，{e,f} のペアのどれかであるとき

・weight 3 のとき：T_2 で 1 になる列が，{a,b}，～，{e,f} のペアのどれかと，もう 1 文字がその 2 文字の入らないペアにあるとき

・weight 4 のとき：T_2 で 1 になる列が，{a,b}，～，{e,f} のペアのうち，λ の符号の同じ 2 組であるとき

3．MEP.3 plan の例

1) 「T_2 として，複数のタイプを併置する構成にすると，MEP.3 plan になる」

例) m=7 のとき，QR タイプ $(7*7)$ に，LC タイプ $(6*8)$ より 1 列をカットしたものを併置して T_2 とすると，MEP.3 plan になる.

0	1	1	0	1	0	0
0	0	1	1	0	1	0
0	0	0	1	1	0	1
1	0	0	0	1	1	0
0	1	0	0	0	1	1
1	0	1	0	0	0	1
1	1	0	1	0	0	0
0	0	0	0	1	1	1
0	0	1	1	0	0	1
0	1	0	1	0	1	0
0	0	1	1	1	1	0
0	1	0	1	1	0	1
0	1	1	0	0	1	1

2) 「m : 素数, $m>20$ のとき，T_2 が Q.R. タイプであれば，MEP.3 plan になる」

・ m=7 (× の数:28), m=11(○:MEP.3 plan), m=13(× の数:39), m=17(○), m=19(× の数:57)

・m=23(○), m=29(○), m=31(○), m=37(○), m=41(○), m=43(○)

4．おわりに

まだ，3 節であげた MEP.3 plan の例が，MEP.3 plan であるという数学的証明ができていない.

また， MEP.3 plan になるための，T_2 の条件もまだ，煮詰まっていない．だから，これらの点を進めて，完成することが今後の課題になる.

参考文献

Shirakura,T. and Suetsugu,T and Tsuji,T(To appear). Construction of main effect plus two plans for 2^m factorials

Srivastava,J.N.(1975). Designs for searching non-negligible effects, in: A Survey of Statistical Design and Linear Model (ed. J.N.Srivastava),507-519, North- Holland, Amsterdam.

多水準過飽和実験の評価について

— 2列間の非直交性の尺度 —

慶應義塾大学 理工学部 管理工学科 飯田孝久

1. 過飽和実験の評価について

過飽和実験では、全ての要因に対する計画行列がランク落ちするため、計画全体としての評価ができない。そこで、部分の評価を総合して計画を評価することになる。多くの場合、2列に対する評価を用いているが、当然ながら3列以上の評価も重要である。

部分の評価基準には、通常の実験計画で用いられるA－、D－、E－、G－基準などが考えられる。総合化の段階では、全ての組合せに対して何らかの意味でこれらの平均をとる。一般には算術平均を用いることが多いが、場合によっては幾何平均や調和平均をとることもある。ここでは、2列に対するD最適基準に相当する量（内積の平方）を採用し、この量の2列の組合せ全体に対する算術平均で全体を評価することとする。

2. 2水準因子の評価—水準出現数が等しい場合

全ての列が2水準で、2つの水準の出現数が等しい場合は、列の水準値を1と－1にとることで各列が一般平均列と直交する。そこで、D最適基準に相当する量として、2列の内積の平方を用いることができる。ここで、どの評価基準もこの値の単調変換であることに注意する。総合評価にはこの値の平均を用いる。

内積の平均平方については、以下に示す様に評価値の下限が与えられている。ここで、実験数をn、列（因子）数をp、計画行列をXとする。過飽和実験から、$p \geqq n$である。

内積の平均平方の下限

$$\begin{aligned} &\{\mathrm{tr}(X'XX'X) - pn^2\}/p(p-1) \\ =&\{\mathrm{tr}(XX'XX') - pn^2\}/p(p-1) \\ \geqq&\{p^2n^2/(n-1) - pn^2\}/p(p-1) \\ =&n^2(p-n+1)/(n-1)(p-1) \end{aligned}$$

この下限を達成する計画を最適計画と呼ぶことにする。アダマール行列の半分実施計画や、同じサイズで同一の列が存在しないアダマール行列を並べた計画は最適である。

3. 2水準因子の評価—水準出現数が異なる場合

各列が2水準であるが、2つの水準出現数が異なる場合は、水準値を1と－1にすると一般平均列と直交しない。そこで、和が0平方和がnとなるように水準値を設定する。第1水準の出現数が$k(\leqq n/2)$のとき、水準値は$\sqrt{\{(n-k)/k\}}$と$-\sqrt{\{k/(n-k)\}}$であ

る。この列は、一般平均列と直交しかつ長さが等しいので、評価に内積の平方を用いることができる。この値は、水準値をデータと見たときの相関係数の平方と同等である。

この場合、総合評価値の下限については、水準出現数が等しい場合と同じ結果が得られることが知られている（昨年の研究集会で発表）。同様の結果は、過飽和回帰で各列が和＝0、平方和＝nと基準化されている場合にも成立する。

ＢＩＢＤから導かれた計画やそれらの結合計画が、下限を達成するという意味で最適計画であることは明らかである。

4．　多水準因子の評価について

3水準以上の列に対する評価を考える。各列の値は名義尺度のため、そのままでは説明変数行列Ｘとして用いることはできない。また、列空間を表現する（水準数－1）列の選び方は、直交系に限定しても一意ではない、という問題がある。

ここでは、要因効果列を、和が0で平方和がnで互いに直交する水準数－1個のベクトルで表現したときの、2要因の各ベクトル間の内積の平方和を用いることとする。この基準は、Ｄ最適基準に対応し、説明変数の列空間の角度の余弦の平方を拡張したものと解釈できる。

多水準の2列の直交性は、二元表の直交性の検定統計量で測ることができる、これは、二元表での各セルの出現数をn_{ij}、期待度数を$m_{ij}=n_{i.}\times n_{.j}/n$としたとき、

$$\Sigma_i\Sigma_j\,(n_{ij}-m_{ij})^2/m_{ij}$$

で表される量であり、周辺度数を与えたときの非直交性を計る尺度である。

これら2つの尺度については、次の関係が成立する。

定理1

次の2つの評価基準は本質的に同等である

1）列空間を長さの等しい直交系に分解した後の内積の平方和

2）直交性の検定統計量

5．　多水準過飽和実験の総合評価

内積の平方を用いる場合には、ｐ＝(水準数の合計)−(因子数)　とおけば、2水準の場合と同じ下限が与えられる。ただし、この総合化は、2列の評価の平均ではなく、（水準数−1）個の母数化後の列組合せに対する平均であることに注意する必要がある。この組合せの中には、同じ要因内の列組合せ（内積は0）を含んでいるので、過小評価になっている。

6．　まとめ

多水準の過飽和実験に対する評価方法を示した。この基準が、二元表での直交性を測る統計量と本質的に同等であることを示した。この基準のもとでの下限が与えられ、その値は2水準の場合の下限と同じであることを示した。

順序制約下の母数推測のための最適実験計画

明星大学理工学部　広津　千尋

1．序論

順序制約下にある母数に対する推定，検定については既に多くの論文があるが，一方，最適実験計画を扱った論文は意外に少ない．その理由としては，順序制約問題で想定されるのは圧倒的に単調制約が多いこと，そして単調制約の場合，少なくとも検出力に関する限り両端に総実験数の半分ずつを割り振る自明な実験計画が最適になってしまうためと思われる．著者等は以前に 1 元配置の設定で単調仮説の検定問題をあつかったが，そこでは自明な最適計画の least favorable case に対する検出力は確保したまま，出来る限り標本を内側に配分する maxmin 検定（最小検出力最大化検定）を導いた（Hirotsu & Herzberg, 1987; Hirotsu, 2001 参照）．新薬臨床試験の分野では，薬効のあること自体の証明として用量反応関係を示すことが求められると同時に，臨床至適用量の推測が求められる．そのような場合に，検定の検出力を確保したまま，やや内側の水準に可能な限りの例数を割り振るという考え方が正当化される．本論はこの考えを凹性仮説の検定に拡張する．

2．定式化

1 元配置のモデル

$$y_{ij}=\mu_i+\varepsilon_{ij},\ i=1,\cdots,a,\ j=1,\cdots,n_i$$

において，凹性仮説

$$H:\ \mu_{i+2}-2\mu_{i+1}+\mu_i\le 0,\ i=1,\cdots,a-2$$

に対する線形 maxmin 検定を考える．すなわち，総実験数 n を与えられたものとして n_i の

最適配分を考える．仮説 H は凸錐をなし，その $a-2$ 個のコーナーベクトル $\mathbf{m}_k, k=1,\cdots,a-2$，の第 k 要素は C_k を規準化定数として

$$C_k\{2a-k-1+jy_k+(k-j+1)x_k\},\ j\le k,$$
$$C_k\{2a-k-1+jy_k\},\ j\ge k+1$$

で与えられる．ただし，

$$x_k=-a(a-1)/\{k(k+1)\},\ y_k=-(3a-2k-1)/(a+1)$$

である．すなわち，$\mathbf{m}_k$ は k 点を境とするスロープ変化モデルを形成するという特徴がある(Hirotsu & Marumo, 2001)．ここで，Hirotsu & Herzberg(1987) に従い，線形検定を

$$\left(\sum \lambda_k \mathbf{m}_k\right)' NQ'\bar{\mathbf{y}}$$

と表し，コーナーベクトル$\mathbf{m}_k$, $k=1,\cdots,a-2$, に対する 線形 maxmin 検定を考える．ただし，$N=\mathrm{diag}\left(\sqrt{n_i}\right)Q'$ は適当な$(a-2)\times a$ 直交行列，$\bar{\mathbf{y}}$ は観測値平均ベクトル，そしてλは Lagrange 未定係数である．その解はaの値に依存し，次節で$a\leq 16$ の場合の結果について述べる．

3. $a\leq 16$ の場合の結果

まず，maxmin の性質から$n_j = n_{a-j+1}$がいえ，両端のコーナーベクトル，つまり k = 1 および a-2 が least favorable case，かつ最適検定が$\lambda_1 = \lambda_{a-2}$，その他のλは 0 で与えられることが分かる．このとき，対立仮説$\mathbf{m}_k$ に対する非心度をγ_k とすると

$$\gamma_1 = C_1 a(a-1)\left\{n^2/16 - (n_1 - n/4)^2\right\}$$

$$\gamma_k = C_k n_1 x_k\left\{-k+2(kn_1 + (k-1)n_2 + \cdots 1n_k)\right\},\ k=2,\cdots,n-2$$

となる．明らかに least favorable case が$n_1 = n/4$で最適化されることが分かる．その他の水準に対するn_iは不等式$\gamma_k \geq \gamma_1$を満たす範囲で最適検定の最小検出力を下回ることなく自由に選べる．その中で中間の例数をすべて 0 とし，中央に n/2 を配分するのが overall の意味での検出力最適化計画になる．

4．考察

線形最強力検定で達成される検出力の最小値を低下させることなく，実験数を満遍なく割り振るという当初の目的は達成されたが，次の点において単調仮説の場合と異なることに注意する必要がある．

（1） 当該検定が least favorable case に対する最強力検定でないため，ここで得た解はあくまで線形 maxmin 検定である．

（2） least favorable case がaの値によって変わる．,

参考文献

Hirotsu, C.(2001). On an optimal design for an isotonic inference. To appear in *J. Statist. Planning and Inference.*

Hirotsu, C. and Herzberg, A. M.(1987). Optimal allocation of observations for inference on k ordered normal population means. *Australian J. Statit.*, 29, 151-165.

Hirotsu, C. and Marumo, K.(2001). Changepoint analysis as a method for isotonic inference. To appear in *Scandinavian J. Statist.*

Balanced (C_3, C_4)-$2t$-Foil System

Kinki University Kazuhiko Ushio

1. Introduction

Let K_n denote *the complete graph* of n vertices. Let C_k be *the k-cycle. The (C_3, C_4)-$2t$-foil* is a graph of t edge-disjoint 3-cycles and t edge-disjoint 4-cycles with a common vertex and the common vertex is called *the center of the (C_3, C_4)-$2t$-foil.*
When K_n is decomposed into edge-disjoint sum of (C_3, C_4)-$2t$-foils, we say that K_n *has a (C_3, C_4)-$2t$-foil decomposition.* Moreover, when every vertex of K_n appears in the same number of (C_3, C_4)-$2t$-foils, we say that K_n *has a balanced (C_3, C_4)-$2t$-foil decomposition* and this number is called *the replication number.* This decomposition is to be known as *a balanced (C_3, C_4)-$2t$-foil system.*

It is a well-known result that K_n has a C_3 decomposition if and only if $n \equiv 1$ or 3 (mod 6). This decomposition is known as *a Steiner triple system.* See Colbourn and Rosa[1] and Wallis[3]. Horák and Rosa[2] proved that K_n has a C_3-bowtie decomposition if and only if $n \equiv 1$ or 9 (mod 12). This decomposition is known as *a bowtie system.*

2. Balanced (C_3, C_4)-$2t$-foil decomposition of K_n

Notation. We denote a (C_3, C_4)-$2t$-foil passing through $v_1 - v_2 - v_3 - v_1 - v_4 - v_5 - v_6 - v_1$, $v_1 - v_7 - v_8 - v_1 - v_9 - v_{10} - v_{11} - v_1$, $v_1 - v_{12} - v_{13} - v_1 - v_{14} - v_{15} - v_{16} - v_1$, ..., $v_1 - v_{5t-3} - v_{5t-2} - v_1 - v_{5t-1} - v_{5t} - v_{5t+1} - v_1$ by $\{(v_1, v_2, v_3), (v_1, v_4, v_5, v_6)\} \cup \{(v_1, v_7, v_8), (v_1, v_9, v_{10}, v_{11})\} \cup \{(v_1, v_{12}, v_{13}), (v_1, v_{14}, v_{15}, v_{16})\} \cup \ldots \cup \{(v_1, v_{5t-3}, v_{5t-2}), (v_1, v_{5t-1}, v_{5t}, v_{5t+1})\}$.

Theorem. K_n has a balanced (C_3, C_4)-$2t$-foil decomposition if and only if $n \equiv 1 \pmod{14t}$.

Proof. **(Necessity)** Suppose that K_n has a balanced (C_3, C_4)-$2t$-foil decomposition. Let b be the number of (C_3, C_4)-$2t$-foils and r be the replication number. Then $b = n(n-1)/14t$ and $r = (5t+1)(n-1)/14t$. Among r (C_3, C_4)-$2t$-foils having a vertex v of K_n, let r_1 and r_2 be the numbers of (C_3, C_4)-$2t$-foils in which v is the center and v is not the center, respectively. Then $r_1 + r_2 = r$. Counting the number of vertices adjacent to v, $4tr_1 + 2r_2 = n - 1$. From these relations, $r_1 = (n-1)/14t$ and $r_2 = 5(n-1)/14$. Therefore, $n \equiv 1 \pmod{14t}$ is necessary.

(Sufficiency) Put $n = 14st + 1$. When $s = 1$, we consider 9 cases.
Case 1. $n = 15$. Construct 15 (C_3, C_4)-2-foils as follows:
$B_i = \{(i, i+1, i+7), (i, i+2, i+13, i+3)\}$ $(i = 1, 2, ..., 15)$.
Case 2. $n = 29$. Construct 29 (C_3, C_4)-4-foils as follows:
$B_i = \{(i, i+1, i+12), (i, i+3, i+24, i+5)\} \cup \{(i, i+2, i+15), (i, i+4, i+26, i+6)\}$ $(i = 1, 2, ..., 29)$.
Case 3. $n = 43$. Construct 43 (C_3, C_4)-6-foils as follows:
$B_i = \{(i, i+1, i+17), (i, i+4, i+35, i+7)\} \cup \{(i, i+2, i+20), (i, i+5, i+37, i+8)\} \cup \{(i, i+3, i+22), (i, i+6, i+39, i+9)\}$ $(i = 1, 2, ..., 43)$.
Case 4. $n = 57$. Construct 57 (C_3, C_4)-8-foils as follows:
$B_i = \{(i, i+1, i+27), (i, i+5, i+46, i+9)\} \cup \{(i, i+2, i+23), (i, i+6, i+48, i+10)\} \cup \{(i, i+3, i+25), (i, i+7, i+50, i+11)\} \cup \{(i, i+4, i+28), (i, i+8, i+52, i+12)\}$ $(i = 1, 2, ..., 57)$.
Case 5. $n = 71$. Construct 71 (C_3, C_4)-10-foils as follows:

$B_i = \{(i, i+1, i+34), (i, i+6, i+57, i+11)\} \cup \{(i, i+2, i+28), (i, i+7, i+59, i+12)\}$
$\cup \{(i, i+3, i+32), (i, i+8, i+61, i+13)\} \cup \{(i, i+4, i+31), (i, i+9, i+63, i+14)\} \cup$
$\{(i, i+5, i+35), (i, i+10, i+65, i+15)\}$ $(i = 1, 2, ..., 71)$.

Case 6. $t \equiv 2$ **(mod 4),** $t \geq 6$ **and** $n = 14t + 1$.

Construct n C_3-t-foils B_i $(i = 1, 2, ..., n)$ as follows:

$B_i = \{(i, i+1, i+(25t+2)/4), (i, i+t/2, i+7t+1), (i, i+t, i+13t/2)\}$
$\cup \{(i, i+2j, i+11t/2+j) \mid 1 \leq j \leq (t-2)/2\}$
$\cup \{(i, i+2j+1, i+(13t+2)/2+j) \mid 1 \leq j \leq (t-6)/4\}$
$\cup \{(i, i+t/2+2j, i+(27t-2)/4+j) \mid 1 \leq j \leq (t-2)/4\}$.

Construct n C_4-t-foils B'_i $(i = 1, 2, ..., n)$ as follows:

$B'_i = \{(i, i+t+j, i+11t+2j, i+2t+j) \mid 1 \leq j \leq t\}$.

Construct n (C_3, C_4)-$2t$-foils $B_i \cup B'_i$ $(i = 1, 2, ..., n)$.

Case 7. $t \equiv 3$ **(mod 4),** $t \geq 7$ **and** $n = 14t + 1$.

Construct n C_3-t-foils B_i $(i = 1, 2, ..., n)$ as follows:

$B_i = \{(i, i+1, i+(25t+5)/4), (i, i+(t-1)/2, i+7t+1), (i, i+t, i+(13t+1)/2)\}$
$\cup \{(i, i+2j, i+(11t+1)/2+j) \mid 1 \leq j \leq (t-1)/2\}$
$\cup \{(i, i+2j+1, i+(13t+3)/2+j) \mid 1 \leq j \leq (t-7)/4\}$
$\cup \{(i, i+(t-1)/2+2j, i+(27t-1)/4+j) \mid 1 \leq j \leq (t-3)/4\}$.

Construct n C_4-t-foils B'_i $(i = 1, 2, ..., n)$ as follows:

$B'_i = \{(i, i+t+j, i+11t+2j, i+2t+j) \mid 1 \leq j \leq t\}$.

Construct n (C_3, C_4)-$2t$-foils $B_i \cup B'_i$ $(i = 1, 2, ..., n)$.

Case 8. $t \equiv 0$ **(mod 4),** $t \geq 8$ **and** $n = 14t + 1$.

Construct n C_3-t-foils B_i $(i = 1, 2, ..., n)$ as follows:

$B_i = \{(i, i+1, i+(25t+4)/4), (i, i+(t-2)/2, i+7t), (i, i+t, i+13t/2)\}$
$\cup \{(i, i+2j, i+11t/2+j) \mid 1 \leq j \leq (t-2)/2\}$
$\cup \{(i, i+2j+1, i+(13t+2)/2+j) \mid 1 \leq j \leq (t-8)/4\}$
$\cup \{(i, i+(t-2)/2+2j, i+(27t-4)/4+j) \mid 1 \leq j \leq t/4\}$.

Construct n C_4-t-foils B'_i $(i = 1, 2, ..., n)$ as follows:

$B'_i = \{(i, i+t+j, i+11t+2j, i+2t+j) \mid 1 \leq j \leq t\}$.

Construct n (C_3, C_4)-$2t$-foils $B_i \cup B'_i$ $(i = 1, 2, ..., n)$.

Case 9. $t \equiv 1$ **(mod 4),** $t \geq 9$ **and** $n = 14t + 1$.

Construct n C_3-t-foils B_i $(i = 1, 2, ..., n)$ as follows:

$B_i = \{(i, i+1, i+(25t+7)/4), (i, i+(t-3)/2, i+7t), (i, i+t, i+(13t+1)/2)\}$
$\cup \{(i, i+2j, i+(11t+1)/2+j) \mid 1 \leq j \leq (t-1)/2\}$
$\cup \{(i, i+2j+1, i+(13t+3)/2+j) \mid 1 \leq j \leq (t-9)/4\}$
$\cup \{(i, i+(t-3)/2+2j, i+(27t-3)/4+j) \mid 1 \leq j \leq (t-1)/4\}$.

Construct n C_4-t-foils B'_i $(i = 1, 2, ..., n)$ as follows:

$B'_i = \{(i, i+t+j, i+11t+2j, i+2t+j) \mid 1 \leq j \leq t\}$.

Construct n (C_3, C_4)-$2t$-foils $B_i \cup B'_i$ $(i = 1, 2, ..., n)$.

By Cases 1–9, K_{14t+1} has a balanced (C_3, C_4)-$2t$-foil decomposition. Therefore, in general, when $n = 14st + 1$, K_n has a balanced (C_3, C_4)-$2st$-foil decomposition. Decompose each (C_3, C_4)-$2st$-foil into s (C_3, C_4)-$2t$-foils. Then they comprise a balanced (C_3, C_4)-$2t$-foil decomposition of K_n. This completes the proof.

References

[1] C. J. Colbourn and A. Rosa, Triple Systems. Clarendom Press, Oxford (1999).

[2] P. Horák and A. Rosa, Decomposing Steiner triple systems into small configurations, *Ars Combinatoria* 26 (1988), pp. 91–105.

[3] W. D. Wallis, Combinatorial Designs. Marcel Dekker, New York and Basel (1988).

自己補ブロックの数え上げ

田澤新成（近畿大学・理工）
金應烈（南開大・組合数学）

1 序

本講演で自己補グラフの数え上げ問題を扱う。特にブロックの場合に制限しての話題である。点集合 X に対し、集合 $X^{(2)}=\{\{i,j\}\subset X|i\neq j\}$ を定める。X と $X^{(2)}$ の部分集合 E との対 (X,E) をグラフと呼ぶ。$|X|$ をこのグラフの位数という。グラフ $G=(X,E)$ に対し $\overline{E}=X^{(2)}-E$ を取り構成されるグラフ $(X,\overline{E})$ は G の補グラフと呼ばれ、$\overline{G}$ と書かれる。グラフ G とその補グラフ $\overline{G}$ が同型ならば G は自己補グラフといわれる。点の個数をパラメータとする自己補グラフの数え上げは Read[2] により与えられた。切断点をもたない位数 ≥ 2 のグラフはブロックといわれる。ここでは次数列をパラメータとする自己補ブロック（ブロック型自己補グラフ）の数え上げを行う。

$X=\{1,2,...,n\}$、$Y=\{0,1\}$ とし、写像 $f:X^{(2)}\to Y$ は位数 n の 1 つのグラフ $G(f)$ を表す。ここで 2 点の隣接関係は「$\{i,j\}$ が $G(f)$ の辺 $\Leftrightarrow$ $f(\{i,j\})=1$」である。時々 f 自身をグラフとよぶ。A を X 上の対称群とし、$\alpha\in A$ に対し $X^{(2)}$ 上の置換 α' を $\alpha'\{i,j\}=\{\alpha i,\alpha j\}$ $(\{i,j\}\in X^{(2)})$ により定める。$A^{(2)}=\{\alpha'|\alpha\in A\}$ は対群と呼ばれる。B を Y 上の対称群とする。$\alpha\in A,\beta\in B$ に対し $Y^{X^{(2)}}$ 上の置換 $(\alpha';\beta)$ を $((\alpha';\beta)f)(\{i,j\})=\beta f(\{\alpha i,\alpha j\})$ $(f\in Y^{X^{(2)}},\ \{i,j\}\in X^{(2)})$ により定める。$B^{A^{(2)}}=\{(\alpha';\beta)|\alpha\in A,\beta\in B\}$ は $Y^{X^{(2)}}$ 上の冪群と呼ばれる。グラフ f に対し、f が自己補グラフであるための必要十分条件は $(\alpha';\beta_1)f=f$ を満たす置換 $\alpha\in A$ が存在することである。ただし β_1 は Y の元 0 と 1 を交換する置換である。この f は $(\alpha';\beta_1)$ の固定元と呼ばれる。

A の各置換 α は共通の文字を含まない巡回置換の積に分解し、$j_k(\alpha)$ を長さ k の巡回置換の個数とする（$k=1,2,...,n$）。

補題 1. n を $n\equiv 0,1(\mathrm{mod}\ 4)$ を満たす自然数とする。このとき．$B^{A^{(2)}}$ の元 $(\alpha';\beta_1)$ が固定元をもつための必要十分条件は各 $k=2,3,...,n$ に対し

$$j_1(\alpha)\leq 1 \quad \text{かつ} \quad j_k(\alpha)\begin{cases} \geq 1 & k\equiv 0(\mathrm{mod}\ 4)\text{のとき} \\ =0 & \text{そうでないとき}\end{cases}$$

が成り立つことである。

ここで巡回置換の書式を規定する。すなわち z を巡回置換として z 内の最初の文字が z の中で最小になるように z を記述する。巡回置換 z の偶数番目の位置にある文字の集合を $e(z)$、奇数番目の位置にある文字の集合を $o(z)$ と書く。

整数係数をもつ多項式環 $R=Z[x_1,x_2,...,x_n]$ を取り、関数 $w:Y^{X^{(2)}}\to R$ を

$$w(f)=\prod_{\{i,j\}\in X^{(2)}}(x_ix_j)^{f(\{i,j\})},\qquad f\in Y^{X^{(2)}}$$

により定める。このとき、$w(f)$ における x_i の指数はグラフ f の点 i の次数をあらわす。補題 1 の関係式を満たす A の置換 α に対し Z_ℓ,Z_m をそれぞれ α の長さ ℓ,m の互いに共通の文字をもたない巡回置換とする。このとき 3 つの式を定義する：

(i) $\ell>1$、$m=1$ のとき。$Z_m=(j)$ と書いて $F_1(Z_\ell)=\{\prod_{i\in o(Z_\ell)}x_i+\prod_{i\in e(Z_\ell)}x_i\}x_j^{\frac{\ell}{2}}$

(ii)$\ell>1$、$m>1$のとき

$$F_2(Z_\ell,Z_m) = \{(\prod_{i\in o(Z_\ell)} x_i^{\frac{2m}{d(\ell,m)}} + \prod_{i\in e(Z_\ell)} x_i^{\frac{2m}{d(\ell,m)}}) \prod_{j\in Z_m} x_j^{\frac{\ell}{d(\ell,m)}} + \prod_{i\in Z_\ell} x_i^{\frac{m}{d(\ell,m)}} (\prod_{j\in o(Z_m)} x_j^{\frac{2\ell}{d(\ell,m)}} + \prod_{j\in e(Z_m)} x_j^{\frac{2\ell}{d(\ell,m)}})\}^{\frac{d(\ell,m)}{2}}$$

ここで$d(\ell,m)$はℓとmの最大公約数である。

(iii)$\ell>1$のとき。$F_3(Z_\ell) = 2^{\frac{\ell}{4}}\{\prod_{i\in Z_\ell} x_i\}^{\frac{\ell}{4}}\{\prod_{i\in o(Z_\ell)} x_i^2 + \prod_{i\in e(Z_\ell)} x_i^2\}^{\frac{\ell-4}{4}}\{\prod_{i\in o(Z_\ell)} x_i + \prod_{i\in e(Z_\ell)} x_i\}$

グラフの次数列は通常非増大順に記述される。与えられた次数列をもつ位数nの自己補グラフの個数を決定する母関数を$C(x_1,x_2,...,x_n)$とする。ここで$x_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$ $(d_1\geq d_2\geq\cdots\geq d_n)$の係数は次数列$d_1,d_2,...,d_n$をもつ自己補グラフの個数である。

線形写像$\theta: R\to R$を次のように定義する。θは、Rの各単項式を変数の増大順に並べたとして指数を非減少順に置き換える役目をする。たとえば$\theta(x_3^4x_1^2x_2^3x_4)=x_1^4x_2^3x_3^2x_4^1$となる。

Parthasarathy and Sridharan[1]は自己補グラフの数え上げとして母関数

$$C(x_1,x_2,...,x_n)=\frac{1}{n!}\sum_{\alpha\in A}\sum_{f=(\alpha';\beta_1)f}\theta(w(f))$$

を与えた。ここで$\sum_{(\alpha';\beta_1)f=f} w(f) =$

$$= \begin{cases} \prod_{Z_\ell} F_1(Z_\ell)\cdot\prod_{Z_\ell,Z_m} F_2(Z_\ell,Z_m)\cdot\prod_{Z_\ell} F_3(Z_\ell), & \alpha\text{が長さ}1\text{の巡回置換をもつとき,} \\ \prod_{Z_\ell,Z_m} F_2(Z_\ell,Z_m)\cdot\prod_{Z_\ell} F_3(Z_\ell), & \alpha\text{が長さ}1\text{の巡回置換をもたないとき.} \end{cases}$$

2 自己補ブロックの数え上げ

$B(x_1,x_2,...,x_n)$を位数nの自己補ブロックの数え上げを与える母関数とする。ここで各項$x_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$の係数は次数列$d_1,d_2,...,d_n$ $(d_1\geq d_2\geq\cdots\geq d_n)$をもつ自己補グラフの個数を与える。次の補題を与える。

補題 2. Gを位数≥ 4の自己補グラフとする。このときGがブロックでないならば、Gは次数1の点を少なくとも1つはもつ。

この補題は次のことを示している:次数1の点を少なくとも1つはもつ自己補グラフは、$C(x_1,...,x_n)$においてx_nの指数が1である項に対応する。このことは次の主要な結果を導く。

定理 1.

$$B(x_1,x_2,...,x_n)=C(x_1,...,x_n)-x_n\left(\frac{\partial C}{\partial x_n}\Big|_{x_n=0}\right),$$

ここで$\frac{\partial C}{\partial x_n}$は$x_n$に関しての$C(x_1,...,x_n)$の偏微分である。

参考文献

[1] K.R. Parthasarathy and M.R. Sridharan, Enumeration of self-complementary graphs and digraphs, Journal Math. Phys. Sci., Madras **3**(1969), 410-414.

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

ある種の Graph design の存在性

慶応大・理工　武藤幸康

1　はじめに

V を要素数 v の集合とし V の要素を頂点 (vertex) と呼ぶ．E を V のすべての異なる 2 頂点の非順序対 (edge, 辺) の集合とする．このとき $K_v = (V, E)$ を頂点数 v の完全グラフと呼ぶ．次に w を E から $\mathbb{Z}$ への写像とし，$w(e)$ を辺の重みと呼ぶ．このとき $G = (K_v, w)$ を重み付きグラフ G と呼ぶ．$w(e)$ が一定 $(= \lambda)$ のとき (K_v, w) の代わりに λK_v と書くことにする．また，重み付きグラフ $G = (K_v, w)$ と $G' = (K_{v'}, w')$ の和 $G \cup G'$ を $(K_v \cup K_{v'}, w + w')$ と定義する．ただし，$K_v = (V, E)$，$K_{v'} = (V', E')$ に対して，$K_v \cup K_{v'} = (V \cup V', E \cup E')$ と定義する．また，$e \in E' \setminus E$ のとき $w(e) = 0$ と定義する．w' についても同様である．

V を頂点数 v の集合とし $G = (K_k, w)$ を頂点数 k の重み付きグラフとする．φ_i を K_k から K_v への写像とする．このとき写像 $\mathcal{B} = \{\varphi_1, \cdots, \varphi_b\}$ が存在し，$\cup_{i=1}^{b} \varphi_i(G) = \lambda K_v$ が成り立つとき λK_v は G で分割可能といい，$(V, G, \mathcal{B})$ を会合数 λ をもつ G-デザインであるという．

2　有限体を用いた G-デザインの構成法

q を素数巾，$GF(q)$ を要素数 q の有限体 (ガロア体) とし，$V = GF(q)$ とする．また，α を $GF(q)$ の原始元とする．さらに，$m | q-1$ のとき $H_i^m = \{\alpha^t | \, t \equiv i \pmod m\}$ とおき，$\mathcal{H}^m = \{H_0^m, H_1^m, \cdots, H_{m-1}^m\}$ とする．

$G = (K_k, w)$ を重み付きグラフとし，E を K_k の辺の集合とする．次に Φ を K_k から $GF(q)$ への写像の集合とし，$\varphi \in \Phi$ に対し $B = \varphi(G)$ とする．$e \in E$ としたとき B 上で e に隣接する $GF(q)$ 上の元を x，y とする．このとき

$$\chi_i(e) = \begin{cases} 2 & x - y \in H_i^m \text{ かつ } y - x \in H_i^m \\ 1 & x - y \in H_i^m \text{ または } y - x \in H_i^m \text{ のどちらか一方が成立} \\ 0 & \text{それ以外} \end{cases}$$

と定義する．このとき次の定理が成り立つ．

定理 1 すべての $0 \le i \le m-1$ において $\sum_{e \in E} w(e)\chi_i(e)$ が一定 $(= \lambda)$ となる B が存在するとき，$\mathcal{B} = \{hB + x | \, h \in H_0^m, \, x \in GF(q)\}$ とおけば $(V, G, \mathcal{B})$ は会合数 λ をもつ G-デザインとなる．

また $-1 \in H_0^m$ のとき $\mathcal{B}' = \{hB + x \,|\, h \in H_0^m/\{1,-1\},\, x \in GF(q)\}$ とすれば $(V, G, \mathcal{B}')$ は会合数 $\frac{\lambda}{2}$ をもつ G-デザインとなる.

3 G-デザインの存在性

P_r を $1, \cdots, r$ からなる順序対の集合 $\{(i,j) | 1 \leq i < j \leq r\}$ とする. C を P_r から $\mathcal{H}^m$ への写像とする. このとき $(a_1, a_2, \cdots, a_r) \in GF(q)^r$ が C について *consistent* であるとは, すべての $1 \leq i < j \leq r$ に対して $a_j - a_i \in C(i,j)$ が成立することである.

R.M. Wilson により次の補題が知られている.

補題 1 (Wilson (1972)) $q = mf + 1$ は素数巾で, $q > m^{r(r-1)}$ とする. このとき任意の写像 C において *consistent* な $(a_1, a_2, \cdots, a_r) \subset GF(q)$ が存在する.

この補題 1 を用いることにより次の定理を得る.

定理 2 $G = (K_k, w)$ を重み付きグラフとし, E を K_k の辺の集合, $W = \sum_{e \in E} w(e) > 0$ を重みの総和とする. また $\{w_1, w_2, \cdots, w_d\}$ を G の異なる重みの集合とし, $\{n_1, n_2, \cdots, n_d\}$ を重みが w_j $(1 \leq j \leq d)$ となる G の辺の数とする. λ_0 を λ と $2W$ の最大公約数とし, $\frac{2W}{\lambda_0}$ が偶数のとき $m = \frac{W}{\lambda_0}$, 奇数のとき $m = \frac{2W}{\lambda_0}$ とする. C を E から $\mathcal{H}^m$ への写像とし, $\mu_j^{(i)}$ を $C(e) = H_i^m$ となる重み w_j の辺の数とする. さらに下のいずれか一方の条件を満たすとする.

(i) q が奇素数巾で $\frac{2W}{\lambda_0}$ が偶数のとき

$$\sum_{j=1}^{d} w_j \mu_j^{(i)} = \lambda_0 \quad (1 \leq i \leq m), \qquad \sum_{i=1}^{m} \mu_j^{(i)} = n_i \quad (1 \leq j \leq d)$$

を満たす非負整数解 $\mu_j^{(i)}$ $(1 \leq i \leq m, 1 \leq j \leq d)$ が存在する.

(ii) q が奇素数巾で $\frac{2W}{\lambda_0}$ が奇数のとき, または q が 2 の巾乗のとき

$$\sum_{j=1}^{d} w_j \mu_j^{(i)} = \frac{\lambda_0}{2} \quad (1 \leq i \leq m), \qquad \sum_{i=1}^{m} \mu_j^{(i)} = n_i \quad (1 \leq j \leq d)$$

を満たす非負整数解 $\mu_j^{(i)}$ $(1 \leq i \leq m, 1 \leq j \leq d)$ が存在する.

このとき q が $q > (\frac{2W}{\lambda_0})^{k(k-1)}$ を満たす素数巾で, かつ, $\lambda(q-1) \equiv 0 \pmod{2W}$ を満たすとき会合数 λ の G-デザインが存在する.

DNA library screeningのためのcombinatorial design

池田 真穂，武藤 幸康，神保 雅一（慶応大・理工）
e-mail: jimbo@math.keio.ac.jp

DNA library screeningでは、たくさんの塩基列(A, T, C, Gの列)の中から，ある試験に対して陽性(positive)反応を示す塩基列を見出す試験がよく行なわれる．このテストの際に，v個の各塩基列を一つ一つテストするとv回のテストが必要になるが，複数の塩基列をひとつにまとめてそのグループに対して、反応試験を行なうと、そのグループが陰性(negative)であった場合には，同時に複数の塩基列の陰性を1回のテストで判定できる．この方法をグループテストと読んでいる。DNA library screeningでは，図1のようなmicrotiter plateと呼ばれる2次元配列の各スポット(wellと呼ぶ)に塩基列を入れてPCR法と呼ばれる方法で塩基列のcloneをたくさん作り，作られたcloneを各行、各列ごとにグループとしてグループテストを行う．このテストでpositiveと判定されたcloneは真にpositiveである場合と，それ自身はnegativeであるが，同じグループにpositiveのcloneが混在していたためにpositiveと判定される場合がある．そのためグループテストでpositiveと判定されたcloneについて，2段階目で個々にテストを行い，positiveなcloneを見出す方法が取られることが多い．この方法をBasic Matrix method(BMM試験)と呼ぶ．

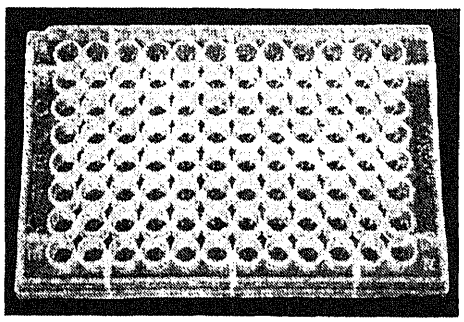

図 1: 8 × 12wellをもつmicrotiterplate

BMM試験において，テストの平均回数を出来る限り少なくすることが必要であり，そのために第1段階でのグループテストについて，*unique collinearity condition*と呼ばれる性質が成り立つことが要求される．

(C1) Unique collinearity condition: どの2つの異なるcloneも配列の同じ行か同じ列のいずれかで高々1回ずつ会合する．

unique collinearity conditionの必要性はBalliot et al.[1], Berger[2]により，シミュレーションあるいは理論的に示されている．

通常，DNA library screeningでは，数万種 ($= v$ 種) の塩基列がテストされることが少なくない．そのため，多くのmicrotiter plateが用いられる．その際に，各塩基が，複数個 ($= t_i$) のplateの行と列でテストされ，各塩基のテストの回数は $2t_i$ となる．われわれのシミュレーションにより，下記の性質が必要であることが見出された．

(C2) Equal replication condition: どのcloneも同じ回数 ($= t$ 回) ずつplateに配置される．

また，Berger[2]により，最適な配列のサイズ $r \times c$ および最適なreplicationの回数 t は，cloneの中のpositiveなcloneの比率 p によって決まることが示されている．

Hwang[5]は，$v = rc$ の場合に，*square lattice design* を用いることを提案した．square lattice designは条件 (C1) を満足しており，$v = rc$ であることより，(C2) も自然に満足していることがわかる．Fu, Hwang, Jimbo, Mutoh and Shiue[4]は，$v > rc$ の場合に，$K_r \times K_c$ decompositon of K_v という組合せ構造をBMM試験に用いることを提案し，いくつかの構成法を与えた．$K_r \times K_c$ decopositon of K_v は (C1) の条件は満たす．しかし，(C2) の条件は全配列を用いた際には満たされるが，一部の配列を用いた際には，必ずしも満たさない．

ここでは，(C1), (C2) の条件を満たすa resolvable $K_r \times K_c$ packing (into K_v) という概念を定義し，この組合せ構造をDNA library screeningに用いることを提案し，その構成法を与える．

参考文献

[1] E. Balliot, B. Lacroix and D. Cohen (1991), Theoretical analysis og library screening using an N-dimensional pooling strategy, Oxford University Press.

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

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

[4] H-L. Fu, F.K. Hwang, M. Jimbo, Y. Mutoh and C.L. Shiue (2001), Decomposing complete graphs into $K_r \times K_c$'s, submitted.

[5] F.K. Hwang (1995), An isomorphic factorization of the complete graph, J. Graph Theory, **19**, 333-337.

ファイル共有のためのグループ鍵暗号システム

慶應義塾大学　理工学研究科　矢尻えみ子
e-mail　emiko@jimmy.math.keio.ac.jp
デンソークリエイト　陳志松

1. グループ鍵暗号システムの概要

複数のユーザーでグループを作り、鍵を共有することを考える。鍵は、それぞれのグループで生成する。その場合、ユーザーは、自分が属しているグループ分の鍵を記憶しなければならない。しかし、ここでは、ユーザーは自分の秘密鍵のみを保存し、それを使って、グループ鍵を計算することを考える。

ユーザーは、グループで共通鍵を生成する際、自分の公開鍵も生成し、ユーザーは、公開鍵に秘密鍵をかけることにより、共通鍵を求められるようにする。

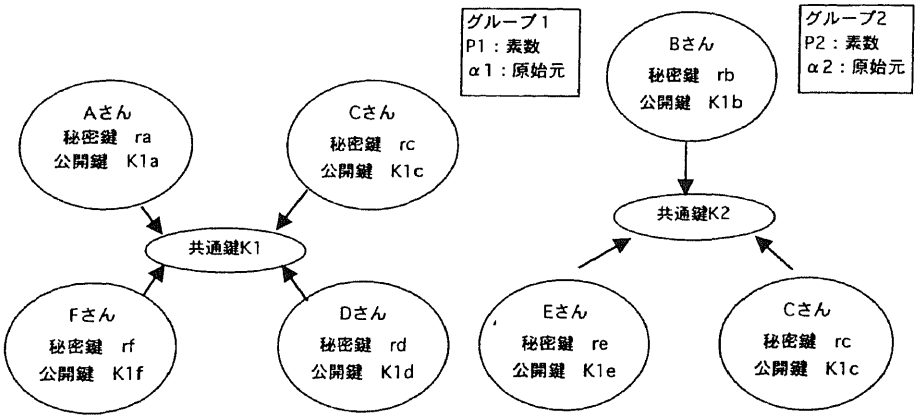

図１：グループ鍵暗号システム

2. グループ鍵生成プロトコル(Burmester と Dexmedt の方法)

センターは、素数 $P(P > r_i)$ とその原始元 α を生成する。

STEP1

各ユーザー $U_i(i = 1,\cdots,n)$ は、秘密鍵 $r_i(i = 1,\cdots,n)$ から $z_i = \alpha^{r_i} \bmod P$ を計算し、z_i をブロードキャストする。

STEP2

各ユーザー $U_i(i = 1,\cdots,n)$ は、X_i を計算し、ブロードキャストする。

$$X_i \equiv (z_{i+1} / z_{i-1})^{r_i} \bmod P$$

STEP3

各ユーザー $U_i(i = 1,\cdots,n)$ は、グループ鍵 K を計算する。

$$K \equiv (z_{i-1})^{nr_i} \cdot X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2} \bmod P$$

3．グループ鍵生成プロトコルの改良版

センターは、素数$P(P>r_i)$とその原始元αを生成する。($(\alpha, P-1)=1$であること。)

STEP1

各ユーザー$U_i(i=1,\cdots,n)$は、秘密鍵$r_i(i=1,\cdots,n)$から$z_i=\alpha^{r_i} \bmod P$を計算し、z_iをブロードキャストする。

STEP2

各ユーザー$U_i(i=1,\cdots,n)$は、X_iを計算し、ブロードキャストする。

$$X_i \equiv (z_{i+1}/z_{i-1})^{r_i} \bmod P$$

STEP3

各ユーザー$U_i(i=1,\cdots,n)$は、自分の公開鍵K_iを計算する。

$$K_i \equiv (z_{i-1})^n \cdot (X_i^{n-1} \cdot X_{i+1}^{n-2} \cdots X_{i-2})^{r_i^{-1}} \bmod P$$

ここで、$r \cdot r_i^{-1}=1 \bmod P-1$とする。

4. ファイルの共有について

あるユーザー A が他のユーザーにファイルを公開する場合、ユーザー A は、グループ鍵Kでファイルを暗号化する。そして、そのファイルに他のユーザーの公開鍵K_iも添付する。ユーザーは、公開鍵に自分の秘密鍵$r_i(i=1,\cdots,n)$をかけることにより、グループ鍵Kを得ることができ、ファイルを復号化し、読むことができる。

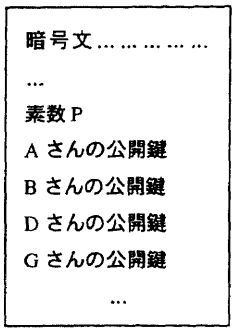

図 2：ファイルのイメージ

5. 参考文献

Mike Burmester, Yvo Desmedt: A Secure and Efficient Conference Key Distribution System. In:A. De Santis(Ed.): Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science 950. Berlin; Springer 1995, pp.275-286

射影幾何により生成されるquorum systemのfailure polynomial

慶應大・理工　足立智子, 上原啓明

1. はじめに

quorum systemとは，任意の2つの集合が空でない共通部分を必ず持つという集合系であり，排他制御など分散システムの分野に広く応用されている([5]他)．このquorum systemsがどの程度有用なものかを判断する基準として，failure polynomialやcondorcetがある([4])．Maekawa([3], 1985)はquorum systemに有限射影平面を用いる方法を見出したが，Peleg and Wool([4], 1995)によりcondorcetの性質を満たさないことがわかった．Colbourn, Dinitz, Stinson([2], 2001)は，より一般的に$\lambda = 1$の(v, k, λ)-BIBデザインからquorum systemを構成する方法を見出した．この手法では，パラメータv, kの値が大きくなると計算が煩雑となり，計算機を用いて$k = 3$かつ$v \leq 15$のBIBデザインについてfailure polynomialを計算したが，この計算は非常に煩雑なものであり一般のBIBデザインについて有用であるとはいえない．

本報告では，射影幾何を用いてBIBデザインから構成したquorum systemのfailure polynomialについて考察する．

2. quorum system

Xをn個の点の集合，$\mathcal{A}$をXの部分集合の族$(m = |\mathcal{A}|)$とする．$\mathcal{A}$の任意の異なる2つの部分集合が空でない共通部分を必ず持つならば，$(X,\mathcal{A})$を(n, m)-quorum systemと呼ぶ．

一方，Yをn'個の点の集合，$\mathcal{B}$をYの部分集合の族$(m' = |\mathcal{B}|)$とする．Yの任意の2点を含む$\mathcal{B}$のブロックの数が1以上ならば，$(Y,\mathcal{B})$を(n', m')-covering systemと呼ぶ．また，$v = |Y|$，$\mathcal{B}$がYのk-部分集合の族，Yの任意の2点を含む$\mathcal{B}$のブロックの数がλであるならば，$(Y, \mathcal{B})$を(v, k, λ)-BIBデザインと呼ぶ．

このとき，(n, m)-quorum systemのdual systemは(m, n)-covering systemとなることが知られている([2])．(v, k, λ)-BIBデザインはcovering systemであり，そのdual systemはquorum systemとなる．

3. failure polynomial

$\mathcal{Q} = (X, \mathcal{A})$を$(n, m)$-quorum systemとする．$X$の部分集合$W$に対して，

$$\mathbf{fail}(W) = \begin{cases} 1 & W \cap A \neq \emptyset \quad \text{for all } A \in \mathcal{A} \\ 0 & \text{上記以外} \end{cases}$$

と定義する．各点は独立に確率pで失敗するという仮定の下で，$\mathcal{Q}$のfailure probabilityは

$$F_{\mathcal{Q}}(p) = \sum_{W \subseteq X} \mathbf{fail}(W) p^{|W|} (1-p)^{(|X|-|W|)}$$

と定義される．この次数nのpの多項式$F_{\mathcal{Q}}(p)$をfailure polynomialと呼ぶ．また，このとき$\mathcal{Q}$のdual system $(Y, \mathcal{B})$は(m, n)-covering systemとなる．Yの部分集合

Z, $0 \leq i \leq m, 0 \leq j \leq n$ に対して,

$$\mathbf{span}(Z) = \{B \in \mathcal{B} : B \cap Z \neq \emptyset\}$$

$$a_{i,j} = |\{Z \subseteq Y : |Z| = i, |\mathbf{span}(Z)| = j\}|$$

と定義すると,

$$F_Q(p) = \sum_{i=0}^{m} \sum_{j=0}^{n} (-1)^i a_{i,j} (1-p)^j$$

となる ([2]). $F_Q(p)$ が condorcet であるとは, $p < \frac{1}{2}$ のとき, $F_Q(p) \to 0\,(n \to \infty)$ を満たすことである. PG(2,q) から生成される quorum system は, $q \to \infty$ のときに condorcet の性質を満たさないことが知られている ([4]). そこで, PG(t,q) において, $t \to \infty$ の場合を考える.

4. 射影幾何により生成される quorum system の failure polynomial

Assmus and Mattson([1]) により, perfect code の 0 でない最小重みの符号語を集めて, 座標を点, 符号語をブロックとみると, t-デザインとなることが知られている. たとえば, $t = 2$ の場合には, Hamming code がその例であり, 最小重みの符号語は BIB デザインを成し, 長さ $2^m - 1$ のハミング符号の重み 3 の符号語は, $PG(m-1, 2)$ の直線に対応する.

そこで, 我々は, binary Hamming code から生成された $(2^m - 1, 3, 1)$-BIB デザインにより構成した quorum system について, $m = 3, 4, 5$ の場合の failure polynomial を求めた. 我々の手法では, $(15, 3, 1)$-BIB デザインから構成された quorum system の failure polynomial は, 計算機を用いずに求めることができた. さらに, $(31, 3, 1)$-BIB デザインから構成された quorum system についても, 煩雑さを軽減し, その failure polynomial を求めた. これらより, $PG(m-1, 2)$ において, p が十分小さいとき, $F_Q(p) \to 0\,(m \to \infty)$ が予想される.

参考文献

[1] E. F. Assmus, Jr., H. F. Mattson, Jr., On tactical configutations and error-correcting codes, *J. of Combinatorial Theory*, **2**(1967) 243-257.

[2] C. J. Colbourn, J. H. Dinitz, D. R. Stinson, Quorum systems constructed from combinatorial designs, *Information and Computation*, **169**(2001) 160-173.

[3] M. Maekawa, A $\sqrt{N}$ algorithm for mutual exclusion in decentralized systems, *ACM Transactions on Computing Systems*, **3**(1985) 145-159.

[4] D. Peleg, and A. Wool, The availability of quorum systems, *Information and Computation*, **123**(1995) 210-223.

[5] M. Raynal, Algorithms for Mutual Exclusion, *MIT Press*, 1986.

直交配列の拡大について

筑波大学　社会工学系　藤原　良

1　直交配列

$S=\{0,1,...,s-1\}$ としたとき，**直交配列**とは $N\times m$ は配列 A で，次の条件を満たす．

1. A の各セルは S の要素をひとつとる．
2. A の任意の2列には S の全ての順序対 $(a,b)\in S^2$ が行として同数回 (λ) 現れる．

直交配列は互いに直交するラテン方格や有限射影平面の問題と同値で，応用も実験計画法を始め，情報，通信，電子工学など多方面で利用されている．構成法に関しても，Euler（１８世紀）以来，数多くの方法が研究されている．

そんな中で，あるひとつの（あるいは複数個の）直交配列を元に何らかの組合せ構造を触媒的に使ってより大きな直交配列を作る手法（再帰的方法という）が以前から盛んに研究されている．ここではその再帰的構成法のひとつを提案する．元になる直交配列 A のサイズを $N\times m$ としたとき，同じ S を使うとして，行数を増やすのは比較的簡単だが，列数を拡大するのは一般的により難しいとされている．今までの拡大法で，行数拡大に比較してもっとも列数拡大の大きい例は，行数が N から sN に拡大したとき，列数は m から $sm+1$ に拡大する例である．

もっともよく知られている再帰的方法は差行列 (Difference Matrix) と呼ばれるある代数的性質を持った行列を使う方法である．ここでは差行列による方法をより一般化した組合せ構造を提案する．

2　中国人のアダマール行列

Y. S. Zhang らによって試みられている方法で，アダマール行列，あるいは差行列をより一般化して，その構造を使って直交配列を拡大しようとしている．まず，

$$C=\{1,-1\}\ ,\ X=\{x_1,x_2,...,x_m\}$$

X は不定元の集合と考える．そして $C\times X$ 上で次のように掛け算 $\bullet$ を定義する．

$$(c,x_i)\bullet(c',x_j)=\begin{cases} cc' & \text{if } x_i=x_j \\ 0 & \text{if } x_i\neq x_j \end{cases}$$

この $C\times X$ 上の要素からなる $n\times m$ 行列を H とする．このとき足し算は整数上で計算するとして，もし H が次の条件を満たすとき，H を**中国人のアダマール行列**と呼ぶことにしよう．

$$H^TH=mI$$

例：

$$H_1=\begin{pmatrix} x_1 & x_1 & x_2 \\ x_1 & -x_1 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}\qquad H_2=\begin{pmatrix} x_1 & x_1 & x_2 & x_2 & x_3 & x_3 \\ x_1 & -x_1 & x_2 & -x_2 & x_3 & -x_3 \end{pmatrix}$$

行数を n,X の大きさを m としたとき，H の列数は最大いくつまで作れるかは興味ある問題でるが，おそらくは nm が最大であると予想される．もし $n\times n$ の普通のアダマール行列 D が存在するなら，クロネッカー積

$$D\otimes(x_1,x_2,...,x_m)$$

によって簡単に $n\times nm$ の中国人のアダマール行列が構成できる．

中国人のアダマール行列を使った直交配列の再帰的構成は次のように行う．まず，元の直交配列（サイズは $N\times m$，$S=\{0,1\}$）を A とする．そして，H を m 個の不定元 $x_1,x_2,...,x_m$ を持つサイ

ズ $n \times M$ の中国人のアダマール行列とする．つぎに直交配列 A の列を不定元 $x_1, x_2, ..., x_m$ に対応させる．そして一種のクロネッカー積

$$A \otimes' H$$

を作る．すなわち，A の x_i 列を H の不定元 x_i の部分に埋め込む．ただし係数が -1 の時はシンボル $\{0,1\}$ を反転させて埋め込む．

3 多値の直交配列の拡大

この中国人のアダマール行列の定義を多値の直交配列の拡大にも適応できるよう一般化してみよう．3値の場合で説明する．いま $C = \{\xi_0, \xi_1, \xi_2\}$ の3つの係数を考える．これらは

$$\xi_0 = \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 2 & 2 \end{pmatrix}, \ \xi_1 = \begin{pmatrix} 0 & 1 \\ 1 & 2 \\ 2 & 0 \end{pmatrix}, \ \xi_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \\ 2 & 1 \end{pmatrix}$$

これらを，左列から右列への置換と考える．また行を順序対と見て，対の集合と見ることもできる．その場合 $\{0,1,2\}$ のすべての順序対が一回づつ現れている．

いま $\{0,1,2\}$ の要素からなり，2列の配列 E があるとする．そしてそのふたつの列はまったく同じ列であるとする．そこで C の要素同士の掛け算 $\cdot$ を次のように定義する．

$$\xi_i \cdot \xi_j = \xi_k$$

は E の左列の要素に置換 ξ_i を，右列の要素に置換 ξ_j をほどこしたとき置換された配列 E に行として現れるペアの集合は ξ_k に現れる順序対の集合と同値である．掛け算表にしてみると次のようになる．(ξ_0 を 1 と表示する)：

$\cdot$	1	ξ_1	ξ_2
1	1	ξ_1	ξ_2
ξ_1	ξ_2	1	ξ_1
ξ_2	ξ_1	ξ_2	1

この掛け算は一見群にみえるが，結合律を満たさない．また非可換である．係数集合 C 上でこの演算をつかい，$C \times X$ 上の掛け算を同様に行うことができる．そして，$1 + \xi_1 + \xi_2 = 0$ の条件を付け加えて，中国人のアダマール行列を同様に定義する．

直交配列の拡大に使うときは，2値の場合係数が -1 のとき $\{0,1\}$ の値を反転させたが，こんどは置換 $\{\xi_0 = 1, \xi_1, \xi_2\}$ をほどこすことによって，2値の場合と同様に再帰的な構成に使える．

4 均斉配列への応用

$C \times X$ 上で足し算をするときに，$1 + \xi_1 + \xi_2 = 0$ の条件を付け加えたが，この代わりに，$\xi_1 + \xi_2 = 0$ とし，中国人のアダマール行列の定義を次のように変更する．

$$H^T H = \mu J + (n - \mu) I$$

このとき，μ は C 上の式，J はすべて 1 の行列．

このような条件を満たす $C \times X$ 上の行列 H を構成することによって，ある直交配列から，サイズを拡大しながら均斉配列を構成することができる．問題はこのような行列 H を行数に対してできるだけ列数の大きい行列をいかに構成するかである．ひとつのアイデアは多値の等距離符号を使う方法が考えられる．　一般的に均斉配列の再帰的拡大は難しく．行拡大にたいし，列拡大があまり多くできていない．差行列による構成法は，均斉配列には応用するのは難しい．C のような置換の集合に特殊な演算を定義することによって，より柔軟な応用が可能になっている．

5 参考文献

[1] Y. S. Zhang, S. Q. Pang and Y. P. Wang, Orthogonal arrays obtained by generalized Hadamard product. Designs, codes and finite geometries, Discrete Math. 238 (2001), 151-170.

[2] Y. S. Zhang, Y. Q. Lu and S. Q. Pang, Orthogonal arrays obtained by orthogonal decomposition of projection matrices, Statist. Sinica 9 (1999), 594-604.