≪科学研究費補助金（総合研究A）研究成果報告書≫

（課題番号　58340001）

研究集会

「代数的組み合せ論の研究」

報告集

研究代表者：　都　筑　俊　郎　（北海道大学理学部）

期　　間：　1983年12月15日～17日

場　　所：　岡　山　大　学　教　育　学　部

ま　え　が　き

この報告書は，1983年12月15日より３日間岡山大学で開かれた「代数的組み合せ論」の研究集会の報告集である。

単純群の分類問題が解決されてより，有限群の研究者達は，それぞれの方向を求めて新しい分野に研究を進めていった。この集会は，代数的な組合せ論をテーマにした最初の研究集会である。

講演には，グラフ，アダマール行列，デザイン，射影平面等に関する新しい結果が発表され盛会裡に終った。

この集会のプログラム，準備等は野田隆三郎（岡山大），木村浩（愛媛大）両氏によりなされた。また会場を提供し，色々と御援助下さった岡山大学数学教室の方々に感謝の意を表したい。

この集会の費用等は科学研究費総合研究Ａ（代表者　都筑俊郎）によった。代表者として御協力下さった都筑氏が病のため参加して頂けなかったことは残念であった。次の集会にはぜひ元気に御参加下さる様祈ってやまない。

大　山　豪

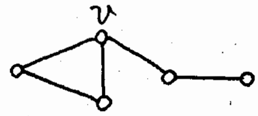
目　　　　次

グラフの因子分解

明石工高専　加納幹雄

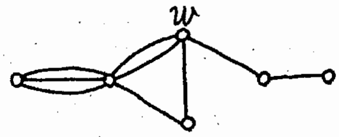
1.はじめに

まず本稿で使う記号，用語について述べよう．グラフGの**点集合**を$V(G)$とかき，**辺集合**を$E(G)$で表わす．2つの点が2本以上の辺で結ばれているとき，この2点を結ぶ辺を**多重辺**という．ここでは，ループはないが，多重辺は許された有限グラフを扱う．このようなグラフはしばしば多重グラフとよばれているが，ここではこれを単に**グラフ**という（図2）．多重辺のないグラフ，すなわちすべての2点間に高々1本の辺しかないグラフを**単純グラフ**とよぶ（図1）．



$d_G(v)=3$

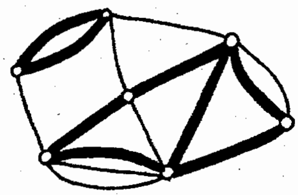
図1．単純グラフG



$d_G(w)=4$

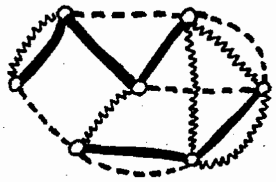
図2．グラフG

グラフGの点vに対し，vと接続する辺の数をvの**次数**（degree）といい$d_G(v)$で表す．部分グラフHとその点vに対し，vと接続するHの辺の数をvのHにおける次数といい$d_H(v)$で表す．グラフGにおいて，Gのすべての点を含む部分グラフ（i.e. $V(H)=V(G)$となる部分グラフH）をGの**全域部分グラフ**（spanning subgraph）という．a, b, rは$0\le a\le b$，$1\le r$となる整数とする．このとき各点vにおいて$a\le d_G(v)\le b$となるグラフGを**[a,b]-グラフ**といい（図3），各点vで$d_{G'}(v)=r$となるグラフG'を**r-正則グラフ**という．同様に各点uにおいて$a\le d_F(u)\le b$となる全域部分グラフを**[a,b]-因子**といい（図3），各点uで$d_{F'}(u)=r$となる全域部分グラフを**r-正則因子**とか**r-因子**という．明らかに，もし$a\le b\le c\le d$なら，[b,c]-グラフ([b,c]-因子)は[a,d]-グラフ([a,d]-因子)でもある．



F={━}

図3．[3,6]-グラフと[2,3]-因子F



F_1={━}, F_2={〰}, F_3={- - -}

図4．3つの[1,2]-因子F_1,F_2,F_3に分解されたグラフ

本稿ではグラフを[a,b]-因子に分解する問題を考える．グラフGに対し，もし

$$E(G)=E(F_1)\cup\cdots\cup E(F_m)$$

$E(F_i)\cap E(F_j)=\phi$，$1\le i<j\le m$，各F_iはGの[a,b]-因子，と分解できればGは**[a,b]-因子分解可能**という．

このとき上の分解を簡単に$G=F_1\cup\cdots\cup F_r$とかき，これをGの$[a,b]$-因子分解という(図4)．グラフの因子分解に関する最も古い結果は次のものである．なお完全グラフとはすべての2点を1つの辺で結んで得られるグラフである．

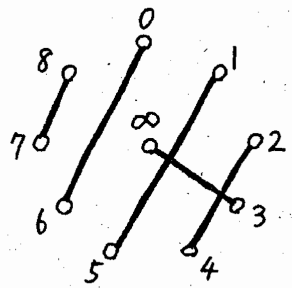


図5. K_{10}の1-因子分解の1-因子F_3.

定理1.(Reiss 1859年[3 定理8.9]) $2m$個の点からなる完全グラフK_{2m}は1-因子分解可能である．

(証) K_{2m}の点集合を$V(K_{2m})=\{0,1,\cdots,2m-2\}\cup\{\infty\}$とおき，各$i$, $0\le i\le 2m-2$に対し$F_i=\{\{i,\infty\},\{i-j,i+j\}\in E(K_{2m})\mid 1\le j\le m-1\}$とおく，ただし$i-j$, $i+j$は$\bmod 2m-1$でとる．(図5)．すると$K_{2m}=F_0\cup\cdots\cup F_{2m-2}$と1-因子に分解できる。

完全グラフの1-因子分解は$2m$組のチームがm個の会場を用いて総当り戦をするときの最適な(日数最小の)試合の組み合せの方法を与えている．もちろん完全グラフの1-因子分解には，これと同型でないものもある．完全グラフの1-因子分解についてはいろいろな研究がされており，代数的(群論的)な方法が有効と思われる問題もある．これらについては近く発表される完全グラフの1-因子分解に関するSurvey[9]を参照してほしい．

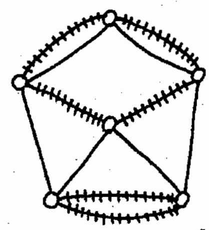


図6(a), 4-正則グラフとその2-因子分解

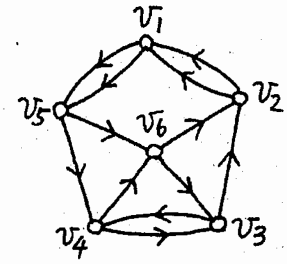
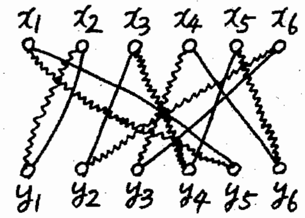


図6(b) Gから作った有向グラフD

さて定理1の次に得られたグラフの因子分解に関する結果は次の定理2である．これはよく知られた有名な定理であるが，これ以後一般のグラフに関する因子分解については，つい最近まで，ほとんど結果が得られなかった．この間約90年の間になされたグラフの因子分解に関する研究は，先に述べた完全グラフとか，これに類似した特殊なグラフの分解に関するものだけであった．



$L_1=\{\sim\}$, $L_2=\{-\}$

図6(c) 2部グラフ$H=(X,Y;E(H))$とその1-因子分解$H=L_1\cup L_2$

定理2.(Petersen 1891年[3 定理8.8]) グラフGが2-因子分解可能であるための必要十分条件は，Gが$2m$-正則グラフであることである．ただしmは正の整数である．

(証) Gがm個の2-因子に分解されるなら，Gは明らかに$2m$-正則グラフとなる．よって$2m$-正則グラフはm個の2-因子に分解できることを示せばよい．Gを$2m$-正則グラフとする．オイラーの一筆書きの定理[3, 定理2.15]によりGのすべての辺を1回通って元に

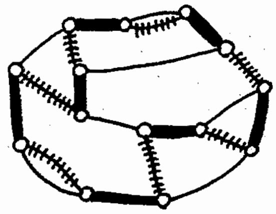


図7. 平面的な2-辺連結3-正則グラフの1-因子分解

もどる閉路 C がある．C の進行方向に沿って各辺に向きをつけ，G から有向グラフ D をつくる．明らかに，D の各点の入次数，出次数は共に n である．次に D から次のようにして $X \cup Y$ を点集合とする2部グラフ $H=(X,Y;E(H))$ をつくる．$V(D)=\{v_1,\cdots,v_m\}$ とするとき $X=\{x_1,\cdots,x_m\}$，$Y=\{y_1,\cdots,y_m\}$ とおき，x_i と y_j を v_i から v_j へ向う D の弧の本数と同じ本数の辺で結ぶ(図6(c))．すると H は n-正則な2部グラフとなる．正則な2部グラフは P.Hallの個別代表系の定理により1-因子分解できる．よって H は $H=L_1\cup\cdots\cup L_m$ と1-因子分解できる．各 L_i に対し L_i に対応する D の弧，それに対応する G の辺を集めると G の2-因子 F_i が得られ，$F_1\cup\cdots\cup F_m$ は G の2-因子分解を与える(図6.(a))．

一般的なグラフの[a,b]-因子分解に関する新しい結果は次の定理3である．なおこの定理は4色定理(平面上の地図は4色で塗れる)と同値である．

定理3. (Appel and Haken 1976年[3 系2.3])平面的な2-辺連結3-正則グラフは1-因子分解できる(図7)．

2. [a,b]-因子分解

[a，b]-因子分解の概念は秋山によって導入され，秋山は次の結果を得た．

定理4. (秋山 1982年[1]) r-正則グラフは[2，3]-因子分解可能である．ただし $r\geq 2$．

正則グラフはグラフの重要なクラスであるが，正則グラフの[a,b]-因子分解は恵羅により完全に解決された．なお以下の定理において，a,b,k,n,r,s,t は整数を表すものとする．

定理5. (恵羅 1983年[4]) もし $r\geq 2k^2+2k$ なら単純な r-正則グラフは $[k,k+1]$-因子分解可能である．ただし $k\geq 1$．

さて，Petersenの2-因子定理は次のように一般化できる．

定理6. ([5]) $0\leq a\leq b$ とする．するとグラフ G が $[2a,2b]$-因子分解可能であるための必要十分条件は G が $[2an,2bn]$-グラフであることである．

これは必要十分条件を与えているが，この他の[a，b]-因子分解において必要十分条件を与えるのはほとんど不可能と思われる．それは例えば $[2a,2b+1]$-因子分解可能な $[2an,(2b+1)n]$ グラフと $[2a,2b+1]$-因子分解できない $[2an,(2b+1)n]$-グラフを識別することがきわめてむつかしいためである．[1，2]-因子分解は，もっとも興味ある問題のひとつである．

定理7. ([5]) $1\leq t$，$0\leq s$ とする．すると $[8t+2s,10t+2s]$ グラフは

このとき上の分解を簡単に $G=F_1\cup\cdots\cup F_r$ とかき，これを G の $[a,b]$−因子分解という（図4）．グラフの因子分解に関する最も古い結果は次のものである．なお完全グラフとはすべての2点を1つの辺で結んで得られるグラフである．

定理1.（Reiss 1859年[3 定理8.9]）$2m$ 個の点からなる完全グラフ K_{2m} は1−因子分解可能である．

(証) K_{2m} の点集合を $V(K_{2m})=\{0,1,\cdots,2m-2\}\cup\{\infty\}$ とおき，各 i, $0\le i\le 2m-2$ に対し $F_i=\{\{i,\infty\},\{i-j,i+j\}\in E(K_{2m})\mid 1\le j\le m-1\}$ とおく，ただし $i-j$, $i+j$ は mod $2m-1$ でとる．（図5）．すると $K_{2m}=F_0\cup\cdots\cup F_{2m-2}$ と1−因子に分解できる。

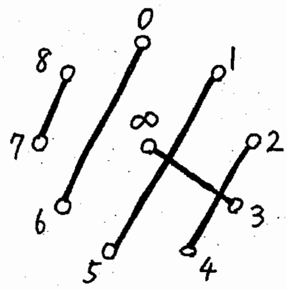


図5. K_{10} の1−因子分解の1−因子 F_3.

完全グラフの1−因子分解は $2m$ 組のチームが m 個の会場を用いて総当り戦をするときの最適な（日数最小の）試合の組み合せの方法を与えている．もちろん完全グラフの1−因子分解には，これと同型でないものもある．完全グラフの1−因子分解についてはいろいろな研究がされており，代数的（群論的）な方法が有効と思われる問題もある．これらについては近く発表される完全グラフの1−因子分解に関するSurvey[9]を参照してほしい．

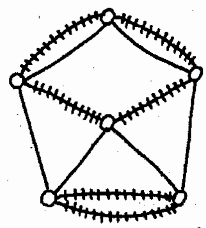


図6(a)，4−正則グラフとその2−因子分解

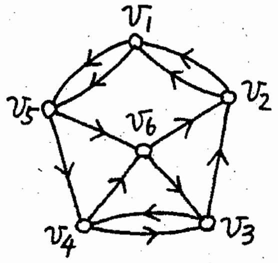
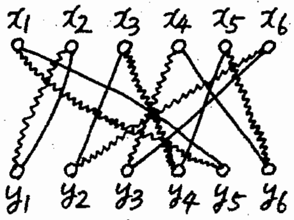


図6(b) G から作った有向グラフ D

さて 定理1の次に得られたグラフの因子分解に関する結果は次の定理2である．これはよく知られた有名な定理であるが，これ以後一般のグラフに関する因子分解については，つい最近まで，ほとんど結果が得られなかった．この間約90年の間になされたグラフの因子分解に関する研究は，先に述べた完全グラフとか，これに類似した特殊なグラフの分解に関するものだけであった．



$L_1=\{\sim\}$, $L_2=\{-\}$

図6(c) 2部グラフ $H=(X,Y;E(H))$ とその1−因子分解 $H=L_1\cup L_2$

定理2.（petersen 1891年[3 定理8.8]）グラフ G が2−因子分解可能であるための必要十分条件は，G が $2n$−正則グラフであることである．ただし n は正の整数である．

(証) G が n 個の2−因子に分解されるなら，G は明らかに $2n$−正則グラフとなる．よって $2n$−正則グラフは n 個の2−因子に分解できることを示せばよい．G を $2n$−正則グラフとする．オイラーの一筆書きの定理[3，定理2.15]により G のすべての辺を1回通って元に

もどる閉路Cがある．Cの進行方向に沿って各辺に向きをつけ，Gから有向グラフDをつくる．明らかに，Dの各点の入次数，出次数は共にnである．次にDから次のようにして$X \cup Y$を点集合とする2部グラフ$H=(X,Y;E(H))$をつくる．$V(D)=\{v_1,\cdots,v_m\}$とするとき$X=\{x_1,\cdots,x_m\}$, $Y=\{y_1,\cdots,y_m\}$とおき，x_iとy_jをv_iからv_jへ向うDの弧の本数と同じ本数の辺で結ぶ(図6(c))．するとHはn-正則な2部グラフとなる．正則な2部グラフはP.Hallの個別代表系の定理により1-因子分解できる．よってHは$H=L_1\cup\cdots\cup L_n$と1-因子分解できる．各L_iに対しL_iに対応するDの弧，それに対応するGの辺を集めるとGの2-因子F_iが得られ，$F_1\cup\cdots\cup F_n$はGの2-因子分解を与える(図6.(a))．

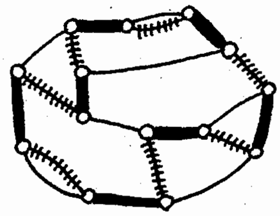


図7. 平面的な2-辺連結3-正則グラフの1-因子分解

一般的なグラフの[a,b]-因子分解に関する新しい結果は次の定理3である．なおこの定理は4色定理(平面上の地図は4色で塗れる)と同値である．

定理3. (Appel and Haken 1976年[3 系2.3])平面的な2-辺連結3-正則グラフは1-因子分解できる(図7).

2. [a,b]-因子分解

[a,b]-因子分解の概念は秋山によって導入され，秋山は次の結果を得た．

定理4. (秋山 1982年[1]) r-正則グラフは[2,3]-因子分解可能である．ただし$r\geq 2$。

正則グラフはグラフの重要なクラスであるが，正則グラフの[a,b]-因子分解は恵羅により完全に解決された．なお以下の定理において，a,b,k,n,r,s,tは整数を表すものとする．

定理5. (恵羅 1983年[4]) もし$r\geq 2k^2+2k$なら単純なr-正則グラフは$[k,k+1]$-因子分解可能である．ただし$k\geq 1$.

さて，Petersenの2-因子定理は次のように一般化できる．

定理6. ([5]) $0\leq a\leq b$とする．するとグラフGが$[2a,2b]$-因子分解可能であるための必要十分条件はGが$[2an,2bn]$-グラフであることである。

これは必要十分条件を与えているが，この他の[a,b]-因子分解において必要十分条件を与えるのはほとんど不可能と思われる．それは例えば$[2a,2b+1]$-因子分解可能な$[2an,(2b+1)n]$グラフと$[2a,2b+1]$-因子分解できない$[2an,(2b+1)n]$-グラフを識別することがきわめてむつかしいためである．[1,2]-因子分解は，もっとも興味ある問題のひとつである．

定理7. ([5]) $1\leq t$, $0\leq s$とする．すると$[8t+2s,10t+2s]$グラフは

$[1,2]$—因子分解可能である。

この結果は$[1,2]$—因子分解できない$[6,8]$—グラフがあることからも，ある程度の良さをもった十分条件を与えているが，まだ改良できると思われる．

グラフの次数の区間の比は$(8t+2s)/(10t+2s)\to\frac{4}{5}$となっているが，この比が$\frac{3}{4}$とか$\frac{3}{2}$とかまで改良できてもおかしくない．

この他の場合については次のような十分条件が得られた．

定理8.（秋山，加納[2]）$s\geq 0$, $t\geq 1$, $k\geq 1$とする．すると$[(12k+2)t+2ks, (12k+4)t+2ks]$—グラフは$[2k,2k+1]$—因子分解可能である．特に$r\geq(12k^2+2k)t$, $t\geq 1$なら$[r, r+2(t-1)k+1]$—グラフは$[2k,2k+1]$—因子分解できる．

定理9.（[6]）$1\leq a\leq b$, $0\leq t$, $0\leq s$, $s+t\geq 1$とする．すると$[(16a-4)t+2as, (16b-2)t+2bs]$—グラフは$[2a-1,2b]$—因子分解可能である．特に$r\geq(16k-4)tk$, $t\geq 1$なら$[r, r+2(t-1)k]$—グラフは$[2k-1,2k]$—因子分解できる．

定理8と定理9から，もし$r\geq 4k^2$ならr—正則グラフ（多重辺があってもよい）は$[k,k+1]$—因子分解できることがわかる．またこれは定理5の簡単な別証明も与えている．（定理5の証明[4]はやや長い）

定理10.（[6]）$1\leq a\leq b$, $t\geq 1$．また整数p, qは$0\leq p\leq q$, $aq\leq bp$, $q+1\geq\frac{2}{3}t$ (or $q+2\geq t$)をみたすものとする．すると$[2at+p, 2bt+q]$—グラフ（単純な$[2at+p, 2bt+q]$—グラフ）は$[2a,2b+1]$—因子分解可能である．

上の定理で$a=b=k$としたものは，正則グラフが$[2k,2k+1]$—因子分解できることしかいっておらず，定理8の結果が良い．また定理8と定理10は，かなり違う方法で証明されている．

3．定理6と定理7の証明について

グラフの$[a,b]$—因子分解を調べるためには，まずグラフの$[a,b]$—因子の存在に関する研究が必要である．グラフの$[a,b]$—因子分解については，前にも述べたように最近まであまり一般的な結果が得られなかったが，$[a,b]$—因子の存在については多くの研究がされてきた．ここではその中でもっとも重要な(g,f)—因子定理とよばれている定理を使う．

グラフGとその点集合$V(G)$上で定義された2つの整数値関数g, fに対し，もしGの各点xで$g(x)\leqq d_F(x)\leqq f(x)$となる$G$の全域部分グラフ$F$があれば，$F$を$G$の$(g,f)$—因子という（図8）．もちろん$(g,f)$—因子が存在するためには，各点$x$で$g(x)\leqq f(x)$となって必要がある．$(g,f)$—因子が存在するための必要十分条件は1970年にLovasz[8]によって得られた．しかし与えられたグラフと2つの関数g, fがこの条件を満たすかどうか確かめるのは一般には容易でない．

補題1.（Lovasz，1970年[8]）グラフGとその点集合$V(G)$上で定義された2つの整数値関数g, fを考える．gとfは任意の点xにおいて$g(x)\leqq f(x)$となるものとする．このときGが(g,f)—因子をもつための必要十分条

件は、任意の$S, T \subset V(G)$, $S \cap T = \phi$ に対し

$$\delta(S,T)=\sum_{t\in T}\{d_G(t)-g(t)\}+\sum_{s\in S}f(s)-e(S,T)-h(S,T)\geq 0$$

となることである．ここで$e(S,T)$はSの点とTの点とを結ぶGの辺の個数を表し，$h(S,T)$は$G-(S\cup T)$の成分Cで，各点$x\in V(C)$において$g(x)=f(x)$となりかつ$\sum_{x\in V(C)}f(x)+e(V(C),T)\equiv 1 \pmod 2$となるものの個数を表す．

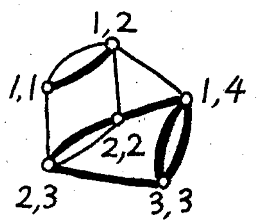


図8. 各数字は $g(x)$ と $f(x)$の値を表す．
$F=\{━\}$は(g,f)−因子

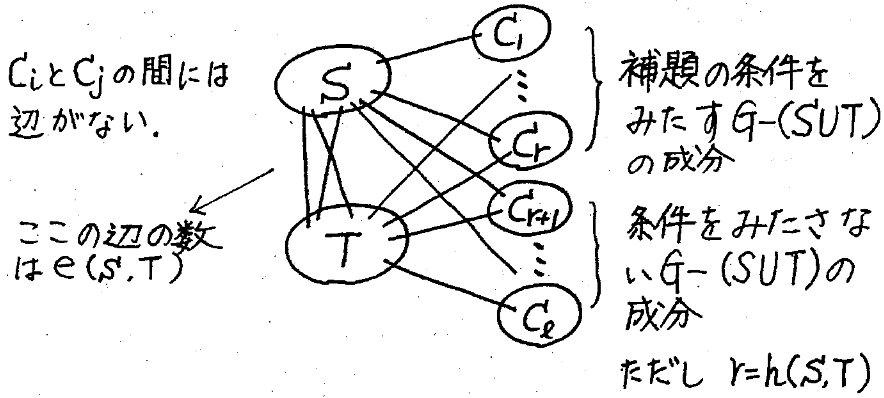


図9.

この補題を用いて，グラフが(g,f)−因子をもつための使いやすい十分条件を与えることができる．なおグラフGがm−辺連結であるとは，Gのどの$m-1$本の辺を除去しても残ったグラフが連結であることである．

補題2.（[5]）Gはm−辺連結なグラフ($m\geq 1$)で，θは$0\leqq\theta\leqq 1$となる実数とする．g, fは$V(G)$上で定義された整数値関数で，各点xにおいて$g(x)\leqq f(x)$となるものとする．このときもし次の条件(1),(2)と{(3a),(3b),(3c)}の中のひとつが満たされれば，Gには(g,f)−因子が存在する．

(1) Gのすべての点xにおいて $g(x)\leqq\theta d_G(x)\leqq f(x)$となるか，または

$$\varepsilon=\sum_{x\in V(G)}\left(\max\{0, g(x)-\theta d_G(x)\}+\max\{0,\theta d_G(x)-f(x)\}\right)<1$$

(2) $g(v)<f(v)$となる点vが少なくともひとつ存在するか，又はすべての点で$g(x)=f(x)$となり，かつ$\sum_{x\in V(G)}f(x)\equiv 0 \pmod 2$となる

(3a) $m\theta\geqq 1$ かつ $m(1-\theta)\geqq 1$

(3b) $\{d_G(x) \mid g(x)=f(x), x\in V(G)\}$ 及び $\{f(x)\mid f(x)=g(x), x\in V(G)\}$が共に偶数だけからなる集合である．

(3c) $\{d_G(x)\mid g(x)=f(x), x\in V(G)\}$が偶数の集合で，$m$は奇数，$(m+1)\theta\geqq 1$，$(m+1)(1-\theta)\geqq 1$となっている．

ここでは，上の補題2の証明はしないが，補題1を用いて2−3ページの計算で証明できる．

定理6の証明 グラフGが$[2a, 2b]$−因子分解可能なら，ある正の整数nが存在し、Gはn個の$[2a, 2b]$−因子に分解できる．このとき明らかにGは$[2an, 2bn]$−グラフである．よって$[2an, 2bn]$−グラフがn個の$[2a,

$2b]$－因子に分解できることを示せばよい．これをnに関する帰納法で証明する．$n=1$のときは明らかだから$n\geq 2$としてよい．また成分ごとに考えればよいから，グラフは連結であるとしてよい．

Gを連結な$[2an, 2bn]$－グラフとする．$\theta = 1/n$とおき，$V(G)$上で定義される整数値関数g, fを次のように定義する．

もし$d_G(x)=2an$なら　$g(x)=f(x)=2a=\theta d_G(x)$

もし$2an<d_G(x)<2bn$なら　$g(x)\leq \theta d_G(x) \leq f(x)$かつ$f(x)-g(x)=1$となるように$g(x), f(x)$をきめる．

もし$d_G(x)=2bn$なら$g(x)=f(x)=2b=\theta d_G(x)$　（下の例参照）．

すると補題２の条件(1),(2),(3b)がみたされるから，Gには(g,f)－因子Fがある．容易にわかるように，$2am<d_G(x)<2bm$となる点xに対しては，$2a<\theta d_G(x)<2b$かつ$2a(m-1)<(1-\theta)d_G(x)<2b(m-1)$となっている．よって$F$は$G$は$[2a, 2b]$－因子で$H=G-E(F)$は$G$の$[2a(m-1), 2b(m-1)]$－因子である．帰納法の仮定により$H$は$m-1$個の$[2a, 2b]$－因子分解されるから$G$は$m$個の$[2a, 2b]$－因子に分解される．

例　$[6, 12]$グラフGを$[2, 4]$－因子に分解するときのg, fの決め方

$d_G(x)$	$g(x)$	$\theta d_G(x)$	$f(x)$	$d_G(x)-d_F(x)$
6	2	2	2	4
7	2	2.33…	3	4　5
8	2	2.66…	3	5　6
9	2	3	3	6　7
10	3	3.33…	4	6　7
11	3	3.66	4	7　8
12	4	4	4	8

$\theta = 1/3$とおき，g, fを左の表のように決める．するとGは(g,f)－因子Fをもつ．$G-E(F)$は$[4, 8]$－グラフとなり，同じ方法で２つの$[2, 4]$－因子に分解できる．

次に定理７の証明について述べる．しかしこの証明は長いので，ここでは定理７の証明で使われるひとつの重要な補題とその証明を述べる．この補題を定理の形で述べる．

定理11． 次数６の点を高々１つ含む３－辺連結な$[4, 6]$－グラフは３つの$[1, 2]$－因子に分解できる．

この証明にも２つの補題が必要である．次の補題３はよく知られている．

補題３．（[7]）奇数個の点からなる$(r-1)$－辺連結なr－正則グラフをGとする．すると各点vに対し$G-v$は１－因子をもつ．

補題４．（[5]）(1) $[3, 4]$－グラフは２つの$[1, 2]$－因子に分解できる．

(2) 次数３の点を少くともひとつ含む連結な$[2, 4]$グラフは，２つの$[1, 2]$－因子に分解できる．

(証) (1) 連結な[3, 4]-グラフをGとおく. $V(G)$上で定義される2つの関数g_1 f_1を次のように定める.

もし$d_G(x)=3$なら　$g_1(x)=1$, $f_1(x)=2$,

もし$d_G(x)=4$なら　$g_1(x)=f_1(x)=2$.

すると$m=1$, $\theta=1/2$, g_1, f_1は補題2の条件(1), (2), (3b)をみたすからGは$(g_1 f_1)$-因子F_1をもつ. 明らかにF_1, $G-E(F_1)$は共にGの[1, 2]-因子だからGは2つの[1, 2]-因子に分解できる.

(2) 与えられたグラフをGとおく. $V(G)$上で定義される2つの関数g_2, f_2を次のように定める.

$d_G(x)$	$g_2(x)$	$\frac{1}{2}d_G(x)$	$f_2(x)$
2	1	1	1
3	1	1.5	2
4	2	2	2

すると$\theta=1/2$, $m=1$, g_2, f_2は補題2の条件(1), (2)(∵次数3の点がある), (3c)をみたす. よってGには(g_2, f_2)-因子F_2がある. 故にGは2つの[1, 2]-因子F_2と$G-E(F_2)$に分解できる.

整数の集合$\{a, b, c\cdots\}$に対し, 各点xにおいて, $d_G(x)\in\{a, b, c\cdots\}$となるグラフを**$\{a, b, c\cdots\}$-グラフ**という.

(定理11の証明)　次数6の点を高々1つ含む3-辺連結な[4, 6]-グラフをGとおく. まずGには次数3又は5の点が少くともひとつあるか, 又は次数3, 5の点はなく(i.e. Gは$\{4, 6\}$-グラフ), 次数4の点が偶数個あるものと仮定する. このときは$\theta=1/4$とおき, $V(G)$上で定義される2つの関数g_1, f_1を次のように決める.

$d_G(x)$	$g_1(x)$	$\theta d_G(x)$	$f_1(x)$	$d_G(x)-d_{F_1}(x)$
4	1	1	1	3
5	1	1.25	2	3　4
6	2	1.5	2	4

すると次数6の点は高々ひとつだから, $m=3$, $\theta=1/4$, g_1, f_1は補題2の条件(1) ($\varepsilon=0$ or $\varepsilon=0.5$), (2), (3c)をみたす. よってGには(g_1, f_1)-因子F_1がある. $G-E(F_1)$は[3, 4]-グラフだから補題4の(1)より2つの[1, 2]-因子に分解できる. 故にGは3つの[1, 2]-因子に分解できる.

次にGは次数4の点を奇数個もつ$\{4, 6\}$-グラフとする. もしGが4-正則グラフなら補題3より, 任意の点vに対し$G-v$は1-因子L_1をもつ. L_1にvと接続するひとつの辺を加えてできるGの[1, 2]-因子をF_1とおく. $H_1=G-E(L_1)$は次数2の点が唯一つの[2, 3]-グラフだから, 各成分には次数3の点が少なくともひとつある. よって補題4の(2)よりH_1は2つの

[1,2]一因子F_2, F_3に分解でき，Gは$G=F_1 \cup F_2 \cup F_3$と3つの[1,2]一因子に分解できる．

次にGには次数6の点がひとつあるものとする．この点をwとおく．2つの関数g_2, f_2を

Gのすべての点xに対し　$g_2(x)=f_2(x)=1$

と定める．すると$m=3$, $\theta=1/4$, g_2, f_2は補題2の条件(1) ($\varepsilon=0.5$), (2)(3)をみたすから(g_2, f_2)一因子L_2がある．L_2に次数6の点wに接続する辺を1本加えて得られる[1,2]一因子をF_1とする．すると$H_2=G-E(F_1)$は次数2と4の点をそれぞれちょうど1つ含む[2,4]一因子となる．よってH_2の各成分には次数3の点が含まれている．補題4の(2)よりH_2は2つの[1,2]一因子F_2とF_3に分解できる．故にGは$G=F_1 \cup F_2 \cup F_3$と[1,2]一因子分解できる．

文　献

[1] J. Akiyama, Factorization and Linear Arboricity of graphs, Doctor thesis, Science University of Tokyo, Feb. (1982)

[2] J. Akiyama and M. Kano, Almost regular factorization of graphs, J. of Graph Theory, to appear.

[3] ベサット他著，秋山，西関訳），"グラフとダイグラフの理論"，共立出版 1979.

[4] H. Era, Semi-regular factorization of graphs, Graphs and Applications (Proc. of the first Colorado symp. of graph theory, ed. F. Harary and J. Maybee) John Wiely, to appear.

[5] M. Kano, [a,b]-factorization of a graph, J. of Graph Theory, to appear.

[6] M. Kano, [a,b]-factorization of a graph II, submitted.

[7] C. H. C. Little, D. D. Grant and D. A. Holton, on detect d-matchings in graphs, Discrete Math. 13 (1975) 41-54

[8] L. Lorasz, Subgraphs with prescribed velercies, J. of Conbinatorial Theory 8 (1970) 391-416

[9] E. Mendelsohn and A. Rosa, One factorization of the complete graph — A survey, J. of Graph Teory, to appear.

Distance-Regular Digraphs

東大 理 情報科学　榎本彦衛

ここでは有向グラフのみを考える。
グラフGの2頂点 x, y に対し、

$$d_G(x,y) := x \text{から} y \text{への(有向)通路の長さの最小値}$$

と定義する。ただし、$x=y$ の時には、$d_G(x,x):=0$ と定義する。有向グラフを考えているので、$d_G(x,y)=d_G(y,x)$ とは限らないし、

$$d_G(x,y)=d_G(z,w) \Rightarrow d_G(y,x)=d_G(w,z)$$

も成り立つとは限らない。(以下、どのグラフを考えているかが明らかな時は添字の G を省略する。)
グラフ G の直径および内周を、

$$d(G) := \max\{d(x,y) \mid x, y \in V(G)\}$$

$$g(G) := G \text{における閉路の長さの最小値}$$

と定義する。また、

$$\Gamma(x) := \{y \in V(G) \mid (x,y) \in E(G)\} \quad (x\text{から出ている辺の行先})$$

$$= \{y \in V(G) \mid d(x,y)=1\}$$

もう少し一般に、

$$\Gamma_i(x) := \{y \in V(G) \mid d(x,y)=i\}$$

と定義します。

定義　$d(x,y)=d(x',y')$ ならば、必ず Gの自己同型写像 σ で、$x^\sigma=x'$, $y^\sigma=y'$ となるものが存在するとき、G は 距離可移 (distance-transitive) と呼ばれる。

(注意) 上の性質を持つグラフを strongly distance-transitive と呼び、

$$d(x,y)=d(x',y') \text{かつ} d(y,x)=d(y',x') \Rightarrow \exists\sigma\in \mathrm{Aut}\, G \text{ s.t. } x^\sigma=x',\ y^\sigma=y'$$

が成り立つとき、weakly distance-transitive と呼ぶ人もいる。

定義　$|\Gamma_i(x)\cap\Gamma(y)|$ が i と $d(x,y)$ だけで決まるような連結グラフは 距離正則 (distance-regular) と呼ばれる

距離可移グラフが距離正則になることは明らかだが、勿論、逆は必ずしも成り立たない。
以下、距離可移グラフの例をいくつかあげておく

(例1) 有向 n 角形 $\overrightarrow{C_n}$

(例2) (Paley トーナメント)

$q \equiv 3 \mod 4$ の時、$S := \{a^2 \mid a \in GF(q) - \{0\}\}$ を平方剰余の全体とし、

$$V(G) := GF(q)$$
$$E(G) := \{(x, y) \mid y - x \in S\} \quad (\text{i.e. } \Gamma(x) = x + S)$$

と定義すると、G は距離可移となる。

(例3) $\overrightarrow{K_{n,n}}$

$$V(G) := \{x_1, \cdots, x_n, y_1, \cdots, y_n\}.$$
$$\Gamma(x_i) := \{y_1, \cdots, y_n\} \quad (1 \leqq i \leqq n)$$
$$\Gamma(y_i) := \{x_1, \cdots, x_n\} \quad (1 \leqq i \leqq n)$$

これらは良く知られた例であるが、実は、直径が2以上の例は(本質的には)これら以外には知られていない。また、距離可移でない距離正則グラフも知られていない。

以下、知られている結果をまとめておくことにする

1) W. M. Kantor は [1] において、直径が2の距離可移グラフは(例2)(例3)のものしかないということを(デザインに関する定理の形で)示した

2) C. W. H. Lam は [2] において、距離可移グラフにおいては、$d(G) = g(G)$ または $d(G) = g(G) - 1$ となること、および、$d(G) = g(G)$ のものと $d(G) = g(G) - 1$ のものとの間に自然な対応がつくことを示した。

3) 坂内-Cameron-Kahn は [3] において、$g(G) = d(G) - 1$ で $g(G)$ が奇数で5以上のものは(例1)のもの以外には存在しないということを示した。

一般の距離正則グラフについては R. M. Damerell [4] を越える結果は何も得られていないようである。[4] において、[2] の結果がほとんどすべて距離正則グラフに対して成り立つことが示された。

以下、G を距離正則グラフ, $d(x, y) = j$ のときの $|\Gamma_i(x) \cap \Gamma(y)|$ の値を p_{ij} と書くことにする。

4) $0<t<g(G)$ ならば

$$d(x,y)=t \iff d(y,x)=g(G)-t$$

5) $d(G)=g(G)$ または $d(G)=g(G)-1$

6) $d(G)=g(G)-1$ の時、任意の集合 M に対し ($|M|\geqq 2$)

$$V(H):=V(G)\times M$$

$$E(H):=\{((x,a),(y,b)) \mid y\in\Gamma_G(x),\ a,b\in M\}$$

と定義すると、Hは距離正則で、$d(H)=g(H)$ となる。

7) $d(H)=g(H)$ となる距離正則グラフ H はすべて(6)の方法により構成される。

以下、$d(G)=g(G)-1$, $g:=g(G)$, $0^*=0$, $g^*=g$, $t^*:=g-t$ $(0<t<g)$ とする。

(4)より $d(x,y)^*=d(y,x)$ となることがわかる。

また、$d(x,y)=k$ の時の

$$\#\{z \mid d(x,z)=i,\ d(z,y)=j\}$$

を p^i_{jk} と書くことにする。特に

$$s_{i^*,j^*}=p^1_{ij}$$

となる。

$$B_i:=(p^i_{jk})_{0\leqq j,k\leqq d}$$

は intersection matrix と呼ばれる。

Γ_i に関する adjacency matrix を A_i とする。i.e.

$$A_i \text{の} (x,y)\text{-要素} := \begin{cases} 1 & d(x,y)=i \text{ の時} \\ 0 & \text{それ以外} \end{cases}$$

この時、

8) $A_1A_i=\sum_{j=0}^{i+1} s_{i^*j^*}A_j \quad (0\leqq i\leqq d-1)$

例えば

$$A_1^2 = s_{g-1,0}A_0 + s_{g-1,g-1}A_1 + s_{g-1,g-2}A_2$$

$$A_1A_2 = s_{g-2,0}A_0+s_{g-2,g-1}A_1+s_{g-2,g-2}A_2+s_{g-2,g-3}A_3$$

特に A_i は A_1 の i 次の多項式として表わされる.

もう少し一般に

$$A_i A_j = \sum_{k=0}^{d} p^i_{jk} A_k$$

9) $A_i \longrightarrow B_i$ は $\langle A_1, \cdots, A_d \rangle_{\mathbb{C}}$ から $\langle B_1, \cdots, B_d \rangle_{\mathbb{C}}$ への algebra としての同型写像を与える.

向きのない距離正則グラフの場合、

$$B_1 = \begin{bmatrix} 0 & 1 & & & & \\ k & a_1 & c_2 & & 0 & \\ & b_1 & a_2 & \ddots & & \\ & & b_2 & \ddots & c_{d-1} & \\ & 0 & & \ddots & a_{d-1} & c_d \\ & & & & b_{d-1} & a_d \end{bmatrix} \qquad (c_i + a_i + b_i = k)$$

という形をしている。従って、自由度は約 $2d$ と考えられる.

有向グラフの場合には

$$B_1 = \begin{bmatrix} 0 & 1 & & & \\ & * & * & 0 & \\ & & \ddots & \ddots & \\ & * & & \ddots & \ddots \\ & & & * & * \\ & & & & * \end{bmatrix}$$

という形になることしかわからず. もっと自由度がありそうに見える. しかし, それほど自由度はないということを坂内氏 [5] が示した.

$B = B_1$ の固有値を $\theta_0 = k, \theta_1, \cdots, \theta_d$, θ_i の $A = A_1$ における重複度を $m_0 = 1, m_1, \cdots, m_d$ とする.

10) $\theta_{i^*} = \overline{\theta_i}$, $m_{i^*} = m_i$ としてよい

11) $\displaystyle\sum_{i=0}^{d} m_i (\theta_i)^j = 0 \quad (1 \leqq j \leqq d)$

∵) 左辺 $= \mathrm{tr}\, A^j$ であるが G には長さ j の閉路が存在しないので 0 になる.

12) $B_i = f_i(B)$ となる i 次の多項式 f_i は B から一意的に決まる.

逆に、f_i より $\mathfrak{B}$ が決まることが (8) よりわかる。

13) $f_i(\theta_j) = f_{i^*}(\overline{\theta_j}) \quad (0 \leqq j \leqq d)$

∵) ${}^tA_i = A_{i^*} = \overline{A_{i^*}}$ よりわかる。

θ_j をすべて決めた時、(13) は f_i と f_{i^*} の係数はスカラー倍を除いて一意的に決まる。この意味で、$\mathfrak{B}$ の(R上の)自由度は約 d であるといえる。

坂内氏は更に

14) $\displaystyle\sum_{l=0}^{d} m_l f_i(\theta_l) f_j(\overline{\theta_l}) = 0 \quad (0 \leqq i < j \leqq d)$

となることを示し、m_l を合わせても $\frac{3}{2}d$ しか自由度がないのにこれらの $\binom{d+1}{2}$ 個の方程式を満たすことは極めて稀だろうから距離正則グラフはほとんど存在しないだろうと主張されました。

しかし、(11) の下では (13) と (14) はほとんど同値になります。たとえば、(13) $\Rightarrow$ (14) は次のようにして証明されます：

$$\sum_{l=0}^{d} m_l f_i(\theta_l) f_j(\overline{\theta_l}) = \sum_{l=0}^{d} m_l f_i(\theta_l) f_{d+1-j}(\theta_l)$$

となりますが、$f_i(\theta_l) f_{d+1-j}(\theta_l)$ は θ_l に関して $d+1+i-j$ $(\leqq d)$ 次の式なので、(11) より 0 となることがわかります。

$k_i := |\Gamma_i(x)|, \quad k = k_1 := |\Gamma(x)|$

とおくと、

$k_i \leqq k^i$

となることは正則グラフについて成り立ちます。向きのないグラフの場合のまねをすると、

$k_i = k^i \quad (1 \leqq i \leqq d)$

が成り立つ時 Moore グラフと呼ぶのは自然ですが、このような

グラフは自明なものしか存在しないことは既に証明されています。向きのない Moore グラフは、もし存在したとすれば距離正則になることはすぐにわかります。従って、(有向グラフの場合にも) 距離正則グラフの中で直径と次数を決めた中で頂点数の最大値を考えるのも自然だと思われます。この場合、[4] より $k_{i^*}=k_i$ となるので、

$$k_i = k^i \quad \left(1 \leqq i \leqq \left\lfloor \frac{d}{2} \right\rfloor\right)$$

が成り立つ時、(距離正則) Moore グラフと呼ぶことになります。しかし、このようなグラフは自明なもの ($k=1$ または $d=2$) 以外に存在しないことが容易にわかります。

∵) $p_{1j}>0$ (となる j) $(2 \leqq j \leqq d-1)$ が存在したとすると、

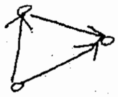
$$p_{1j}k_j = p^{1}_{1^*j^*}k_{j^*} = p^{1^*}_{j^*1^*}k_{1^*}$$

となるが、$k_j \geqq k^2$, $p^{1^*}_{j^*1^*} \leqq k$ なので、$k>1$ ならば

$$p_{1j}=1,\ j=2 \text{ または } j=2^*,\ p^{1^*}_{j^*1^*}=k$$

となるはずだが、$p^{1^*}_{j^*1^*}=k$ とはなれないことがすぐにわかる。

従って、$p_{11^*}>0$ でなくてはならないが、すると、



という部分グラフを含むので、$d=2$ でなくてはならない。

$d=3$ の場合。

$$B = \begin{bmatrix} 0 & 1 & 0 \\ 0 & (k-1)/2 & (k+1)/2 \\ k & (k-1)/2 & (k-1)/2 \end{bmatrix}$$

となることは容易にわかる。特に (kは奇数で) $|V(G)| = 2k+1 \equiv 3 \mod 4$ となる。

また、

$$H := \begin{bmatrix} 1 & 1 \cdots & 1 \\ -1 & & \\ \vdots & \multicolumn{2}{c}{A_0+A_1-A_2} \\ -1 & & \end{bmatrix}$$

が skew Hadamard 行列になることがわかります．逆に skew Hadamard 行列から $g=3$ の距離正則グラフを構成できることも容易に分かります．

$g=4$ の場合．$k=k_1$, $l=k_2$,

$$B = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & a & e & 0 \\ 0 & f & d & b \\ k & a & c & a \end{bmatrix}$$

とすると，

$$a+b = c+d+e = 2a+f+1 = k$$

$$cl = fk, \quad bk = el$$

という関係が成り立ち，自由度は2になります．実際，2つのパラメータ β と γ を使って，

$$k = 2\beta^2\gamma - \beta^2 + \beta\gamma - \gamma$$

$$a = 2\beta\gamma - \beta - \gamma$$

$$b = \beta(2\beta\gamma - \beta - \gamma + 1)$$

$$c = (\beta - 1)\gamma$$

$$d = \beta(2\beta\gamma - \beta - \gamma)$$

$$e = \beta\gamma$$

$$f = (\beta - 1)(2\beta\gamma - \beta - \gamma + 1)$$

$$l = 4\beta^3\gamma - 4\beta^3 + 2\beta^2 + 2\beta - 3\beta\gamma + \gamma - 1 + \frac{\beta^3 - \beta^2}{\gamma}$$

と書け，

$$\theta_1 + \overline{\theta}_1 = a = 2\beta\gamma - \beta - \gamma$$

$$\theta_1 \overline{\theta}_1 = \beta\gamma(2\beta\gamma - \beta - \gamma + 1)$$

$$\theta_2 = d - b = -\beta$$

$\beta=8$ の場合には，Q-polynomial scheme と呼ばれるものになるので，特に興味があるのですが，存在するかどうかわかっていません。$|V(G)|=1+2k+l=484$ となるので，特に 8 が 2冪の時には 2元体上のベクトル空間を使って構成できれば面白いのだがと期待しています。一番小さい場合 $(8=2)$ は，$|V(G)|=64$ で

$$B=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 4 & 4 & 0 \\ 0 & 5 & 8 & 10 \\ 14 & 4 & 2 & 4 \end{bmatrix}$$

となります。

文献

[1] W.M. Kantor, Automorphism groups of designs, Math. Z. 109 (1969) 246–252

[2] C.W.H. Lam, Distance-transitive digraphs, Discrete Math. 29 (1980) 265–274

[3] E. Bannai, P.J. Cameron, J. Kahn, Nonexistence of certain distance-transitive digraphs, J. Combinatorial Theory (B) 31 (1981) 105–110

[4] R.M. Damerell, Distance-transitive and distance-regular digraphs, J. Combinatorial Theory (B) 31 (1981) 46–53

[5] E. Bannai, private communication

$PG(n,q)$ のグラフ論的特徴づけ

岩手大・教育　沼田 稔

位数 q の有限体上の n 次元射影空間 $PG(n,q);(n \geqq 3)$ の直線の交わりの関係をもとにグラフを考える。すなわち $PG(n,q)$ の1次元射影部分空間を点と考え、異なる二つの1次元射影部分空間が交わっている時、対応する2点を辺で結んで作るグラフを考える。このグラフは次の特徴をもっている。

i) 結ばれない2点 α, β に対し、α, β の両方と結ばれる点の全体の作る部分グラフは、2次元正方 *lattice* グラフ $L_2(t)$，$(t \geqq 2$，t は定数$)$ と同型である。

ii) 互いに結ばれない3点 γ, δ, η に対し、これら3点と結ばれる点の間には辺がない。

一般に有限集合 V を点の集合とし、V の順序を考えない異なる2点の組からなるある集合 E を辺の集合とし $\Gamma=(V,E)$ をグラフと呼ぶ。V の2点 α, β の組 (α,β) が E の元である時 α と β は辺で結ばれるといい、そうでないとき α と β は結ばれない，又は離れているという。

上の条件 i) と ii) を満すグラフとして $PG(n,q)$ から作ったグラフ以外に完全グラフの辺を点と考え、異なる二つの辺が1点を共有する時対応する点を辺で結んで出来るグラフ，すなわち *triangle graph* $T(m)$，$(m \geqq 4)$ がある。さらに10次の対称群 S_{10} の部分群 $S_5 \wr Z_2$ による置換表現から作られるグラフも条件 i), ii) を満している。逆に我々は次の定理を得た。

定理　グラフ $\Gamma=(V,E)$ が上の条件 i), ii) を満す時，Γ は次のいずれかと同型である。　a) $PG(n,q)$，$(n \geqq 3)$ から作られるグラフ　b) $T(m)$，$(m \geqq 4)$

c) 対称群 S_{10} の部分群 $S_5 \wr Z_2$ による置換表現から作られるグラフ。

定理の証明の概略.

証明の中心は、例外的なb)及びC)のグラフを除いて、$PG(n,q)$から作られるグラフとなることを示すのである。このために、1916年, O. Veblen, J.W. Young による射影空間の特徴づけに関する定理が使える状態にもっていって証明を終えるのである。

$PG(n,q)$から作ったグラフに対し、$PG(n,q)$の点ひに対応するものとしてひを通る直線全体を考えるとこれはグラフにおいて極大な完全部分グラフを作っている。したがって極大な完全部分グラフ(これを clique と呼ぶ)を考えるのであるが、$PG(n,q)$から作ったグラフでは clique はもう一種類ある。すなわち、ある平面上にのっている直線の全体である。条件 i), ii) を満すグラフは二種類の clique をもつことを証明し、サイズの大きい方の clique の全体とグラフの点の全体が射影空間の公理を満していることを確めるのである。

それでは証明の手順を説明していく。

(イ) Γ は強正則グラフである。

この証明には条件 i) を使うだけである。

(ロ) α, γ を互いに結ばれない2点とする。$\Delta(\alpha)\cap\Delta(\gamma)$ の一つの clique を l とし、l に含まれる2点, β_1, β_2 を取る。この時 $\Delta(\beta_1)\cap\Delta(\beta_2)$ の元 δ は l に含まれるか又は l のすべての元と結ばれている。(ただし $\Delta(\alpha)$ は α と結ばれる点の全体, すなわち $\Delta(\alpha)=\{\beta\in V \mid (\alpha,\beta)\in E\}$)

(ハ) $\alpha, \gamma, \beta_1, \beta_2$ は(ロ)の時と同じとする。その時 $\Delta(\beta_1)\cap\Delta(\beta_2)\cap\Delta(\alpha)\setminus\Delta(\gamma)$ と $\Delta(\beta_1)\cap\Delta(\beta_2)\cap\Delta(\gamma)\setminus\Delta(\alpha)$ は共に完全部分グラフとなる。そして $\Delta(\beta_1)\cap\Delta(\beta_2)\cap\Delta(\gamma)\setminus\Delta(\alpha)$ と $\Delta(\beta_1)\cap\Delta(\beta_2)\cap\Delta(\alpha)\setminus\Delta(\gamma)$ の点はどれも互いに結ばれない。

(ニ) β_1, β_2 を互いに結ばれる点とする。その時, β_1 と β_2 を含む Γ の clique は調度2個ある。これを C_1, C_2 とすると $|C_1\cap C_2|=t$ となる。

(ホ) C を clique, γ を C に含まれない点とする。その時 $|C\cap\Delta(\gamma)|=0$ or t.

(ヘ)　α, βを互いに結ばれる2点，C_1, C_2をα, βを含む2個のcliqueとする。δを$C_1 \setminus C_2$の元とし$\{\alpha, \delta\}$を含むC_1と異なるcliqueをCとすると　$C \cap C_2 = \{\alpha\}$。

(ト)　α, β, C_1, C_2は(ヘ)の時と同じとする。その時αを含むすべてのcliqueを次のように取ることが出来る。　$D_1, \cdots, D_x$，$F_1, \cdots, F_y$がすべてのαを含むcliqueで　$|D_1| = |D_2| = \cdots = |D_x| = |C_1|$，$|F_1| = |F_2| = \cdots = |F_y| = |C_2|$となり　$x = |C_2| - 1/t-1$，　$y = |C_1| - 1/t-1$　となる。　さらに　$D_i \cap D_j = \{\alpha\}$　$F_k \cap F_\ell = \{\alpha\}$，$(i \neq j, k \neq \ell)$，$|F_k \cap D_i| = t$　となる。$(\cup D_i = \cup F_k = \Delta(\alpha) \cup \{\alpha\})$

以上(ト)までの証明によって$\Delta(\alpha)$の構造は完全に決定された。　これ以後は$x \leqq y$とし，　$x = t$　となることを例外的場合を除いて証明する。そのために，αと結ばれない点の全体を$\Sigma(\alpha)$とし（すなわち　$\Sigma(\alpha) = V \setminus \Delta(\alpha) \setminus \{\alpha\}$）$\Sigma(\alpha)$の点の間の結びつきの関係を調べる。　今$\alpha$を含むすべてのcliqueから$\alpha$を除いた集合を各々$A_1, \cdots, A_x$，$B_1, \cdots, B_y$とする。（$A_i = D_i \setminus \{\alpha\}$，$B_j = F_j \setminus \{\alpha\}$）

(チ)　γを$\Sigma(\alpha)$の点とする。　その時　$A_1, \cdots, A_x$の中からt個，$A_{i_1}, \cdots, A_{i_t}$，$B_1, \cdots, B_y$の中からt個，$B_{j_1}, \cdots, B_{j_t}$を各々選んで　$|A_{i_k} \cap B_{j_\ell} \cap \Delta(\gamma)| = 1$，$(1 \leqq k \leqq t,\ 1 \leqq \ell \leqq t)$　となるように出来る。

γは$A_{i_1}, \cdots, A_{i_t}$，$B_{j_1}, \cdots, B_{j_t}$と会合すると呼ぼう。

(リ)　$A_1 \cap B_1$，$A_1 \cap B_2$，$A_2 \cap B_1$，$A_2 \cap B_2$　の中から各々任意に1つづつ点　$\beta_1, \beta_2, \beta_3, \beta_4$を取る。　その時　$\beta_1, \beta_2, \beta_3, \beta_4$のすべてと結ばれる$\Sigma(\alpha)$の点は唯一つ存在する。

(ヌ)　γが$A_1, \cdots, A_t$，$B_1, \cdots, B_t$と会合している$\Sigma(\alpha)$の点であるとする。$A_1, \cdots, A_t$から2つA_i, A_j，$B_1, \cdots B_t$から2つB_k, B_ℓと取り，$A_i \cap B_k$，$A_i \cap B_\ell$，$A_j \cap B_k$，$A_j \cap B_\ell$から各々1つづつ点$\beta_1, \beta_2, \beta_3, \beta_4$を取る。そして　$\Delta(\beta_1) \cap \Delta(\beta_2) \cap \Delta(\beta_3) \cap \Delta(\beta_4) \cap \Sigma(\alpha) = \{\gamma'\}$　とすると　γ'は$A_1, \cdots, A_t$，$B_1, \cdots, B_t$と会合する。

γ, γ'を$\Sigma(\alpha)$の2つの元で，それぞれ$A_1, \cdots, A_t$，$B_1, \cdots, B_t$及び$A_{i_1}, \cdots, A_{i_t}$，

$B_{j_1}, \cdots, B_{j_t}$ と会合しているとする。

(ル) $|\{A_1, \cdots, A_t\} \cap \{A_{i_1}, \cdots, A_{i_t}\}| = t$ or 1 or 0 となる。

(オ) $\{A_1, \cdots, A_t\} = \{A_{i_1}, \cdots, A_{i_t}\}$, $\{B_1, \cdots, B_t\} \cap \{B_{j_1}, \cdots, B_{j_t}\} = \phi$,

又は $\{A_1, \cdots, A_t\} \cap \{A_{i_1}, \cdots, A_{i_t}\} = \{A_k\}$, $\{B_1, \cdots, B_t\} \cap \{B_{j_1}, \cdots, B_{j_t}\} = \phi$,

又は $\{A_1, \cdots, A_t\} \cap \{A_{i_1}, \cdots, A_{i_t}\} = \{A_k\}$, $\{B_1, \cdots, B_t\} \cap \{B_{j_1}, \cdots, B_{j_t}\} = \{B_\ell\}$

ならば γ と γ' は結ばれない。

(ワ) $\{A_1, \cdots, A_t\} = \{A_{i_1}, \cdots, A_{i_t}\}$, $\{B_1, \cdots B_t\} \cap \{B_{j_1}, \cdots, B_{j_t}\} = \{B_\ell\}$

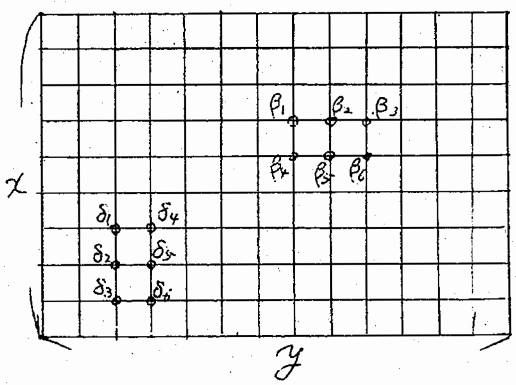
とする。そして $A_i \cap B_\ell \cap A(\gamma) = A_i \cap B_\ell \cap A(\gamma')$, $(1 \leqq i \leqq t)$ である

時 γ と γ' は結ばれる。そうでない時 γ と γ' は結ばれない。

(注, (ル), (オ), (ワ) は A と B を入れ替えても同様に成立する。)

さて, $t=2$ と仮定する。

(カ) 右図のように四角形 $\delta_1, \delta_2, \delta_5, \delta_4$, 四角形 $\delta_2, \delta_3, \delta_6, \delta_5$, 四角形 $\delta_1, \delta_3, \delta_6, \delta_4$ と対応する $\Sigma(\alpha)$ の元を各々 $\gamma_1, \gamma_2, \gamma_3$ とする。$\gamma_1, \gamma_2, \gamma_3$ を含む clique を C とすると C は $\Sigma(\alpha)$ に含まれ, そのサイズは $y+1$ となる。同様に四角形 $\beta_1, \beta_2, \beta_5, \beta_4$,



四角形 $\beta_2, \beta_3, \beta_6, \beta_5$, 四角形 $\beta_1, \beta_3, \beta_6, \beta_4$ に対応する $\Sigma(\alpha)$ の元を各々 $\gamma_1', \gamma_2', \gamma_3'$ とし, それら3つの元を含む clique を C′ とすると C′ は $\Sigma(\alpha)$ に含まれそのサイズは $x+1$ となる。

(ヨ) $2 < x \leqq y$ とすると $x = y$ となる。

(タ) $2 < x = y$ の時 Γ は $x^2, 2(x-1), 4$ のパラメーターをもつ強正則グラフであり, これは $x=5$ の時しか存在し得ない。$x=5$ の時グラフは完全に決まる。

次に, $t>2$ と仮定する。

γとγ'が同じ$A_1, \cdots, A_t, B_1, \cdots, B_t$と会合していると仮定する。$\gamma$と$\gamma'$はどのような時に結ばれるかを調べる。

$A_1, \cdots, A_t, B_1, \cdots, B_t$と会合している$\Sigma(\alpha)$の元全体を$\mathfrak{S}$とする。

(レ) $\mathfrak{S}$のサイズは$(t-1)^4$である。

(ソ) γと結ばれない$\mathfrak{S}\setminus\{\gamma\}$の元は少なくとも$(t-2)^2(t-1)t$個ある。

(ツ) γと結ばれる$\mathfrak{S}$の元は少なくとも$t^2(t-2)$個あり，(ソ)と合わせ考えると調度$t^2(t-2)$個であることになり，γとγ'が結ばれるのはA_{i_0}, B_{j_0}が存在し

$$A_{i_0}\cap B_j\cap\Delta(\gamma) = A_{i_0}\cap B_j\cap\Delta(\gamma'),\quad (1\leqq j\leqq t)$$

$$A_i\cap B_{j_0}\cap\Delta(\gamma) = A_i\cap B_{j_0}\cap\Delta(\gamma'),\quad (1\leqq i\leqq t)$$

となっている時に限る。

(ネ), (ツ)におけるγとγ'を含む2つのcliqueは$A_{i_0}\cap\Delta(\gamma)$と結ばれる$\Sigma(\alpha)$の元全体と$A_{i_0}\cap\Delta(\gamma)$の和集合，及び$B_{j_0}\cap\Delta(\gamma)$と結ばれる$\Sigma(\alpha)$の元全体と$B_{j_0}\cap\Delta(\gamma)$の和集合となる。

(オ), $\gamma_1, \gamma_2, \gamma_3$は互いに結ばれる$\Sigma(\alpha)$の元でそれぞれ$A_{i_1}, \cdots, A_{i_t}, A_{j_1}, \cdots, A_{j_t}$ $A_{k_1}, \cdots, A_{k_t}$と会合し$B_1, \cdots, B_t$と共通に会合していると仮定する。そして
$|\{A_{i_1}\cdots A_{i_t}\}\cap\{A_{j_1}, \cdots, A_{j_t}\}| = |\{A_{j_1}, \cdots, A_{j_t}\}\cap\{A_{k_1}, \cdots, A_{k_t}\}| =$
$|\{A_{k_1}, \cdots, A_{k_t}\}\cap\{A_{i_1}, \cdots, A_{i_t}\}| = 1$とする。$\gamma_1, \gamma_2, \gamma_3$を含むcliqueを$C$とすると$C$は$\Sigma(\alpha)$に含まれ，そのサイズは$y(t-1)+1$となっている。

(ワ) (オ)におけるclique Cの元γ, γ'は共通に会合するA, Bを高々1個しかもたない。よって　Cのサイズは$x+y$より少ない。$t>2$だからこれは(オ)に矛盾する。

以上によって　$t=2$, $x=y=5$の例外を除いて　$t=x$となることが示された。　$t=x=2$の時　Γはtriangle graphとなり　$t=x>2$の時射影空間の公理系を満し，次元が3以上だからデザルグの定理を満し，有限斜体は可換体であるというWedderburnの定理より，定理の証明は完結する。

この問題は，$PG(n,q)$ の k 次元部分射影空間を点と考え、異なる二つの k 次元部分射影空間の共通部分が $k-1$ 次元部分射影空間となるとき、対応する点を辺で結んで出来るグラフを考えると，このグラフは，距離2の位置にある α, β に対して $\Delta(\alpha)\cap\Delta(\beta)$ が $L_2(t)$ と同型となり、さらに条件 ii) を満足する。よって，グラフの直径を一般にして，定理を拡張することが出来ないか。また条件 i) だけだとどうなるのかも興味深い問題である。また $\Delta(\alpha)$ の構造を与えておいてグラフを特徴づけるという方向もある。

Bush型のHadamard行列

伊藤 昇（甲南大理）

1. 成分が± 1である行ベクトルをHadamardベクトル（Hベクトルと略す）と呼ぼう。サイズをnとすると2^n個ある。k個のHベクトルが2つづつ直交している時，その集合をHadamard k-セット（Hk-セットと略す）と呼ぼう。H2-セットの存在の必充条件が$n \equiv 0 \pmod 2$であり，H3-セットの存在の必充条件が$n \equiv 0 \pmod 4$であることは見易い。サイズnが与えられた時，Hk-セットが存在すると，$k \leqq n$であることは明らかであるが，$k = n$というのが存在するというのが，Hadamardの予想と言われ未解決となっている。サイズnのHk-セットがあると，(1, 1)，(1, −1)との直積を作ると，サイズ$2n$のH$2k$-セットが得られる。それで$n = 2^m$の時，予想は正しいが，これはHadamardよりも前に，Sylvesterにより知られていた。Hadamardはその他に$n = 12, 20$の時を解決し，うえの予想となったのかも知れない。とも角いまの構成によると，予想を解決するには，$n = 4u$，u奇数の時だけ考察すればよいので，以下そうすることにする。

2. サイズnが与えられた時，予想解決よりも弱く，なるべく大きなHk-セットを作ろうという問題を考えて見よう。成分位置の置換又はある成分に−1を乗ずることにより，Hk-セットはHk-セットに移る。その様なHk-セットは等価であると呼ばれる。Hk-セットがH$k+1$-セットに拡大されない時，極大（Hk-セット）と呼ぼう。予想解決の困難さは，極大なものが$k = n$の時に限らず，その様なkが沢山あるというところにあるのだろう。サイズuの全1ベクトルをjと書く。その時(j, j, j, j)，$(j, j, -j, -j)$，$(j, -j, j, -j)$，$(j, -j, -j, j)$が極大H4-セットであることは見易い。これに等価なものが最も良く知られた極大H4-セットの例であろう。(1, 1)，(1, −1)との直積は極大性を保存することも注意されてよいかも知れない。次の事実も見易いであろう。$u = vw$とし，サイズwの全1ベクトルをhと書く。サイズ$4v$のHk-セットAがあると，Aの各ベクトルで1，−1をh，$-h$で置き換えると，サイズ$4u$のHk-セットBが得られる。Aが極大とするとき，Bは極大とは限らないだろうが，どこまで拡大出来るか調べることは面白いと思う。そうしてみるとサイズ$4p$，p素数，の時を考察するのが大切に見える。

3. さてBushは文献[1]で次の様な結果を示した。pを$p \equiv 1 \pmod 4$である素数とする。サイズ$p-1$のH$p-1$-セット（次数$p-1$のHadamard行列）の存在を仮定する。そうするとサイズ$4p$の，$4p > k \geqq 2p+2$を満足する極大Hk-セットが存在する。Bushが実際に示したことはH$2p+2$-セットでH$4p$-セットに拡大できないものがあるということで，kの値は決めていない。$p = 5$の時に書いてみる。

+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
+	+	+	+	+	−	−	−	−	+	−	+	+	−	−	−	−	+	+	−
+	−	−	−	−	+	+	+	+	−	+	+	+	−	−	−	−	+	+	−
+	+	+	−	−	+	+	−	−	+	+	+	−	+	+	−	−	−	−	−
+	−	−	+	+	−	−	+	+	+	+	−	+	+	+	−	−	−	−	−
+	+	+	−	−	−	−	+	+	−	−	+	+	+	−	+	+	−	−	−
+	−	−	+	+	+	+	−	−	−	−	+	+	−	+	+	+	−	−	−
+	+	−	+	−	+	−	+	−	−	−	−	−	+	+	+	−	+	+	−
+	−	+	−	+	−	+	−	+	−	−	−	−	+	+	−	+	+	+	−

```
+ + − + − − + − + + + − − − − + + + − −
+ − + − + + − + − + + − − − − + + − + −
+ + + + + + + + + − − − − − − − − − − +
```

美しいパタンなので，興味のある方にとっては，構成の仕組を読み取ることは困難でないであろう。図の場合には，極大でなければならないことはHallの定理により知られている。一般の場合の証明は，Hasse-Minkowski不変数を使う行列のたくみな計算に基づいている。

4．Bushの上の結果では，条件 $p \equiv 1 \pmod 4$ が本質的なのではないだろうか。$p=3$ の時ためしてみる．構成は少しだけ改良が加えられている

```
+ + + + + + + + + + + +
+ + + + + − − − − − − +
+ + + − − + − − − + + −
+ − − + + − + − − + + −
+ + − + − + + + − − − −
+ − + − + + + − + − − −
+ + − − + − − + + + − −
+ − + + − − − + + − + −
```

これはH12-セットに拡大される:

```
+ + − − − − + − + − + +
+ − + − − − + + − + − +
+ − − + − + − − + + − +
+ − − − + + − + − − + +
```

そこでLeon，Longyearとともに $p=7$ の時の分類をこころみた．前提とすることは次数12のHadamard行列と2-(7，4，2)トーナメントの存在である．後者は次数8のskew-Hadamard行列の存在といってもよい．そして $p=3$ の時と同じ様にサイズ28のH16-セットからはじめる．

```
+ + + + + + + + + + + + + + + + + + + + + + + + + + + +
+ + + + + + + + + + + + + − − − − − − − − − − − − − − +
+ + − + − + + + − − − + − + − − − − − + + − − + + + + −
+ − + − + − − − + + + − + − + − − − − + + − − + + + + −
+ + − − + − + + + − − − + + + + − − − − − + + − − + + −
+ − + + − + − − − + + + − + + − + − − − − + + − − + + −
+ + + − − + − + + + − − − + + + + + − − − − − + + − − −
+ − − + + − + − − − + + + + + + + − + − − − − + + − − −
+ + − + − − + − + + + − − − − + + + + + − − − − − + + −
+ − + − + + − + − − − + + − − + + + + − + − − − − + + −
+ + − − + − − + − + + + − + + − − + + + + + − − − − − −
+ − + + − + + − + − − − + + + − − + + + + − + − − − − −
+ + − − − + − − + − + + + − − + + − − + + + + + − − − −
+ − + + + − + + − + − − − − − + + − − + + + + − + − − −
+ + + − − − + − − + − + + − − − − + + − − + + + + + − −
+ − − + + + − + + − + − − − − − − + + − − + + + + − + −
```

これは実際幾通りもの仕方で，H28-セットに拡大される．Leonのアル

ゴリズムによって数え上げたところ，53等価類にわかれたが，これはLeonのアルゴリズムが不備であるためで，14等価類にわかれるものと思われる

5．4．での実験結果を $u\equiv 3\ (\mathrm{mod}\ 4)$，次数 $2u-2$ のHadamard行列と次数 $u+1$ のskew-Hadamard行列の存在の仮定の下で公式化することは可能である．その様にして出て来る次数 $4u$ のHadamard行列をBush型と名付ける．ともかくサイズ $4u$ の H_{2u+2}-セットから出発出来，そのパタンも比較的簡明であるので，H_{4u}-セットへの拡大の可能性が見えるのではないかという夢を持たせる．然し乍ら，出発点になる H_{2u+2}-セットの左半分は u が大きくなるにつれ，ひずみが大きくなる様なので，心配である．細部は文献［2］にまかせたい．尚，Bush型の転置もBush型である．

文献

1. K. A. Bush
   On Hadamard embeddability
   Linear algebra and its application 29 (1980), 39－52.

2. N. Ito
   Hadamard matrices of Bush type

3. N. Ito, J. Leon, Q. Longyear
   Hadamard matrices of order 28 of Bush type.

2，3は準備中である．

四元数型アダマール行列の構成

東京女子大学・文理　山本幸一

1. 成分が ±1 の n 次正方行列 H が $HH^*=nI$ (I: 単位行列) を満たすとき, H を n 次アダマール行列と呼ぶ. 次数 n は 1 と 2 を例外値として, すべて 4 の倍数になる. 成分が ±1, $\pm i$ である n 次正方行列 H が $HH^*=nI$, $H^*={}^t\bar{H}$ を満たすとき, H を n 次の複素アダマール行列と呼ぶ. 次数は 1 の外はすべて偶数になる. またその成分が有理四元数体の極大整環 (Hurwitz 四元数環) の単数である n 次正方行列 H が $HH^*=nI$ を満たすとき, H は n 次の四元アダマール行列と呼ばれる. Hurwitz 四元数環 $\mathcal{O}$ は $a+bi+cj+dk$, $a, b, c, d \in \frac{1}{2}\mathbf{Z}$, $a\equiv b\equiv c\equiv d \pmod 1$ なる四元数から成るものである. $\mathcal{O}$ の単数群は位数 24 で, 四元数群 $U_0=\{\pm1, \pm i, \pm j, \pm k\}$ を正規部分群にもち, また

$$\omega=\frac{-1+i+j+k}{2}, \quad \omega^3=1$$

を含む. さらに単数群 U は U_0 と $\{\omega\}$ の半直積である. $U_0\omega \cup U_0\omega^2$ に属する 16 個の単数はちょうど

$$\frac{\pm1\pm i\pm j\pm k}{2}$$

の形の 16個であるが, H の成分がすべてこの形のものならば, 行列 $2H$ で, $1, i, j, k$ をその 4 次正則表現

$$\begin{pmatrix} 1 & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \end{pmatrix}, \quad \begin{pmatrix} \cdot & 1 & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & -1 \\ \cdot & \cdot & 1 & \cdot \end{pmatrix}, \quad \begin{pmatrix} \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & 1 \\ -1 & \cdot & \cdot & \cdot \\ \cdot & -1 & \cdot & \cdot \end{pmatrix}, \quad \begin{pmatrix} \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & -1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ -1 & \cdot & \cdot & \cdot \end{pmatrix}$$

で置き換えることにより, $4n$ 次アダマール行列

$$\begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix} \tag{1}$$

が得られる．逆に上の行列で A, B, C, D の成分が ± 1 で，しかも

$$\begin{cases} AB^*-BA^*+CD^*-DC^*=0, \\ AC^*-CA^*+DB^*-BD^*=0, \\ AD^*-DA^*+BC^*-CB^*=0, \end{cases}$$

$$AA^*+BB^*+CC^*+DD^*=4nI$$

ならば，それはある四元アダマール行列から得られたものになる．この意味で上の形の $4n$ 次アダマール行列を，四元数型アダマール行列という．

2. 一般に n 次正方行列 M が巡回行列であるというのは，その第1行を次次に巡回的にずらして第2行以下が得られることで，もし

$$T=\begin{pmatrix} 0 & 1 & \cdots & & 0 \\ & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ & & & & 1 \\ 1 & 0 & \cdots & & 0 \end{pmatrix}$$

を基本的巡回行列とすれば，M は T の多項式となる：$M=f(T)$, $f(x) \in \mathfrak{O}[x]$.

巡回的なアダマール行列 $H=f(T)$ の次数は平方数である．

実際，条件 $HH^*=nI$, $f(T)f(T^{-1})=nI$ から T の固有値1に対する関係式 $f(1)^2=n$ が出る．

同様に巡回的な複素アダマール行列の次数は2つの平方数の和であることが分る．さらに巡回的な四元アダマール行列の成分が $\omega U_0 \cup \omega^2 U_0$ に属するならば，同じ議論によって $4n$ が4つの平方数の和になることが分る．このように整数論的には，巡回的な四元アダマール行列を取扱うことが，最も普遍性を持つものと言えよう．なお巡回的な（普通の）アダマール行列は $n=1, n=4$ を除いて一つも知られていないし，Ryser は他の場合は不可能であると推測している．

巡回的な四元アダマール行列から作られた普通の $4n$ 次アダマール行列 (1) では，A, B, C, D は成分が ± 1 の巡回行列で，条件

$$AA^*+BB^*+CC^*+DD^*=4nI$$

をみたすものとして特長づけられる．さらにもし A, B, C, D をすべて対称行列とすれば上の条件は

$$A^2+B^2+C^2+D^2=4nI \tag{2}$$

となる. これを発見者に因んで Williamson 等式と呼ぶ.

3. アダマール行列の構成という見地から見れば, $4n$ 次アダマール行列のうちで n が奇数である場合が最も重要である. 従って以下一般に n は奇数と仮定する. Williamson 等式 (2) に対応する巡回的な四元アダマール行列 H は, 仮定から $H=P\omega+Q\omega^2$ となる. ここに P, Q は成分が四元数群 U_0 に入るかまたは 0 で, P と Q との 0 でない成分を 1 で置き換えた行列 P_0, Q_0 に対しては $P_0+Q_0=J$ はすべての成分が 1 に等しい. なお P, Q は対称である. 故に

$$nI=(P\omega+Q\omega^2)(\omega^2\bar{P}+\omega\bar{Q})=P\bar{P}+Q\bar{Q}+P\omega^2\bar{Q}+Q\omega\bar{P}$$
$$=P\bar{P}+Q\bar{Q}+S(P\omega^2\bar{Q})$$

となる. ここに S は共役和をあらわす. 一般に U_0 の元 ε, η に対して $\varepsilon\omega^2\eta$ は $\frac{\pm1\pm i\pm j\pm k}{2}$ の形であるから $S(\varepsilon\omega^2\eta)=\pm1$ が成立し, 上式を (mod 2) で考察すると

$$I\equiv P_0^2+Q_0^2+S(P_0\omega^2\bar{Q}_0)=P_0^2+Q_0^2+P_0Q_0\equiv P_0^2+Q_0J \pmod 2.$$

H の対角成分を ω と仮定しても一般性を失わないからそう仮定すると $Q_0J\equiv0$ (mod 2) で, $P_0^2\equiv I$ (mod 2), $P_0\equiv I$ (mod 2), $P=\omega I$ を得る. すなわち巡回的な四元アダマール行列 $-\omega H$ は

$$\frac{1+i+j+k}{2}I+A+Bi+Cj+Dk$$

の形である. A, B, C, D は対称行列で, 対角線上は 0, それ以外では, A, B, C, D のただ1つの行列が ±1 なる成分を持ち他は 0 である. 書きかえると

$$\left(\frac{I}{2}+\sum_{m\in\mathcal{A}}e_mT^m\right)+\left(\frac{I}{2}+\sum_{m\in\mathcal{B}}e_mT^m\right)i+\left(\frac{I}{2}+\sum_{m\in\mathcal{C}}e_mT^m\right)j+\left(\frac{I}{2}+\sum_{m\in\mathcal{D}}e_mT^m\right)k$$

で, $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ は添数集合 $\Omega=\{1,2,\cdots,n-1\}$ の分割で, e_m は ±1 なる値を持つ. なお $e_{-m}=e_m$ である. 条件は

$$\left(I+2\sum_{m\in\mathcal{A}}e_mT^m\right)^2+\left(I+2\sum_{m\in\mathcal{B}}e_mT^m\right)^2+\left(I+2\sum_{m\in\mathcal{C}}e_mT^m\right)^2+\left(I+2\sum_{m\in\mathcal{D}}e_mT^m\right)^2=4nI \tag{3}$$

となる. これを簡約化された Williamson 等式と呼ぶ.

さらに簡易化して, x は $x^n=1$ を満たす数として $u_m=x^m+x^{-m}$ とおき,

$$\left(1+2\sum_{m\in A} e_m u_m\right)^2+\left(1+2\sum_{m\in B} e_m u_m\right)^2+\left(1+2\sum_{m\in C} e_m u_m\right)^2+\left(1+2\sum_{m\in D} e_m u_m\right)^2=4n \tag{4}$$

の形にしておくのが最も普通である．ここに $e_m=\pm1$ で，A, B, C, D は集合 $\Omega'=\{1,2,\cdots,\frac{n-1}{2}\}$ の分割である．

それはまた n の任意の約数 n' について

$$\left(1+4\sum_{m\in A} e_m\cos\frac{2\pi m}{n'}\right)^2+\left(1+4\sum_{m\in B} e_m\cos\frac{2\pi m}{n'}\right)^2+\left(1+4\sum_{m\in C} e_m\cos\frac{2\pi m}{n'}\right)^2$$
$$+\left(1+4\sum_{m\in D} e_m\cos\frac{2\pi m}{n'}\right)^2=4n \tag{5}$$

が成立つことと同値である．

4．以下簡約化された Williamson 等式をどのようにして解くかを問題にしたい．まず (5) で $n'=1$ の場合は

$$(1+4w_1)^2+(1+4w_2)^2+(1+4w_3)^2+(1+4w_4)^2=4n, \tag{6}$$

$$w_1=\sum_{m\in A} e_m,\quad w_2=\sum_{m\in B} e_m,\quad w_3=\sum_{m\in C} e_m,\quad w_4=\sum_{m\in D} e_m \tag{7}$$

となる．

不定方程式 (6) は Jacobi の定理からちょうど $\sigma(n)$ 個の解 (w_1,w_2,w_3,w_4) を持つ．ここに $\sigma(n)$ は n の約数の和を表わす函数である．また集合 A の中で $e_m=1$ なる m の全体を A_+，$e_m=-1$ なる m の全体を A_- で表わし，B_+, B_- 以下も同様に定義しておくと，(6) の解 (w_1,w_2,w_3,w_4) に対して (7)，すなわち

$$w_1=\#A_+-\#A_-,\quad w_2=\#B_+-\#B_-,\quad w_3=\#C_+-\#C_-,\quad w_4=\#D_+-\#D_- \tag{8}$$

が成立するように，Ω' の分割 $A_+, A_-, B_+, B_-, C_+, C_-, D_+, D_-$ を定める．これではただ各集合の濃度が決まるだけであるが，具体的に分割を決めた上で，(5) あるいは (4) が成立つかどうかを判定しなければならない．たとえば n が素数ならば，(5) はただその n に対してだけ検証することになる．それ以外では他の約数 $\neq1$ についても検証しなければならない．無論 (5) では cos を実数計算で取扱うから誤差が出て，最終的には絞られた候補に対して (4) にまで戻ることになる．アルゴリズムの意味で (4) を簡単化しておく．

Ω' の部分集合 M, L につき，

$$f(M)=\sum_{\substack{m,k\in M\\ m<k}} u_m u_k = \sum_{\substack{m,k\in M\\ m<k}} (u_{m+k}+u_{m-k}), \quad u(M)=\sum_{m\in M} u_m,$$

$$g(M,L)=\sum_{m\in M}\sum_{\ell\in L} u_m u_\ell = \sum_{m\in M}\sum_{\ell\in L}(u_{m+\ell}+u_{m-\ell})$$

とおいて

$$f(A_+)+f(A_-)+u(A_+)+f(B_+)+f(B_-)+u(B_+)+f(C_+)+f(C_-)+u(C_+)+f(D_+)+f(D_-)+u(D_+)$$
$$=g(A_+,A_-)+g(B_+,B_-)+g(C_+,C_-)+g(D_+,D_-)$$

をチェックする。同じことを場合の個数計算と見れば、$r\in\Omega'$ を任意の値として

$$m+k\equiv r,\ m<k;\quad (m,k\in A_+)\vee(m,k\in A_-)\vee(m,k\in B_+)\vee(m,k\in B_-)\vee$$
$$\vee(m,k\in C_+)\vee(m,k\in C_-)\vee(m,k\in D_+)\vee(m,k\in D_-)$$

の解の個数と

$$m-k\equiv r,\ m<k;\quad (m,k\in A_+)\vee\ \cdots\ \vee(m,k\in D_-)$$

の解の個数の和を F_r で表わし、

$$m+\ell\equiv r;\ (m\in A_+,\ell\in A_-)\vee(m\in B_+,\ell\in B_-)\vee(m\in C_+,\ell\in C_-)\vee(m\in D_+,\ell\in D_-)$$

の解の個数と

$$m-\ell\equiv r;\ (m\in A_+,\ell\in A_-)\vee\ \cdots\ \vee(m\in D_+,\ell\in D_-)$$

の個数の和を G_r で表わす。また E_r は特性函数

$$\begin{cases} r\in A_+\cup B_+\cup C_+\cup D_+ & \text{のとき } 1,\\ r\notin A_+\cup B_+\cup C_+\cup D_+ & \text{のとき } 0\end{cases}$$

を表わすとすれば、Williamson 等式は

$$F_r+E_r=G_r \qquad \left(r=1,2,\cdots,\frac{n-1}{2}\right) \tag{9}$$

と変形される。

$\cos$ の実数近似のほか、整数論的近似つまり p進近似によって、"ふるい" をかけることもできる。しばらく $n=p$ を素数として $\zeta_p=e^{2\pi i/p}$ とおき、有理 p進数体に ζ_p を添加した体で $\varpi^{p-1}=-p$ なる素元 ϖ を取り

$$\zeta_p^m\equiv 1+m\varpi+\frac{m^2}{2!}\varpi^2+\cdots+\frac{m^{p-1}}{(p-1)!}\varpi^{p-1} \pmod{\varpi^p}$$

から

$$u_m\equiv 2\left(1+\frac{m^2}{2}\varpi^2+\frac{m^4}{24}\varpi^4+\cdots\right) \pmod{\varpi^p}$$

を得て，Williamson 等式 (4) から

$$(1+4w_1)S_2(A)+(1+4w_2)S_2(B)+(1+4w_3)S_2(C)+(1+4w_4)S_2(D)\equiv 0 \pmod{p} \qquad (10)$$

となる．ここで

$$S_2(A)=\sum_{m\in A} e_m m^2,\ S_2(B)=\sum_{m\in B} e_m m^2 \quad 等.$$

5. Williamson 等式 (4) は 27 以下の奇数について計算がなされている．$n\leq 23$ については Wallis の本 [**9**] に表がある．それ以下の $n=25, n=27$ は沢出 [**2**] によるが，それは (10) と類似する整数論的な screening を使って簡易化されたアルゴリズムに依る．一般に，計算の大きさは $\frac{n-1}{2}!$ のオーダーで急激に増大するから，列挙による方法は大体この辺りが限界であろう．

以上の結果から見て取れるように，$4n$ を 4 つの奇数の平方の和に表わす "整数分解" (6) のどれにでも対応する Williamson 等式が存在するとは限らない．さらに整数分解 (6) の個数が $=\sigma(n)$ であっても，解を具体的に与える簡単な手続きはない．これが広い一般性を持つ Williamson 等式の系列の発見を困難にする原因である．Turyn [**4**] は Paley 2 型のアダマール行列を，Williamson 等式 (2) の形に変形できることを示した．そこでは $2n-1=q$ が素数巾であるという制約がある．そして本質的に，これが現在知られている，唯一の無限系列である．

中間的な立場は，Ω' の分割様式を特定のものに限定することであろう．

$n=p\equiv 1 \pmod 4$ を素数とし，$p=a^2+b^2$, $a\equiv 1 \pmod 4$, $j^2\equiv -1 \pmod p$ として，分割に

$$B_+=jA_+,\ B_-=jA_-,\ D_+=jC_+,\ D_-=jC_-$$

なる制限を置くもの．これが <u>j 型 Williamson 等式</u>である．整数分解は

$$4p=(a+b)^2+(a+b)^2+(a-b)^2+(a-b)^2.$$

山田 [**5**] は $p=37$ に対する解を得て，$p=29, 41$ に対しては解のないことを示した．

$n=p\equiv 1 \pmod 3$ が素数で，$4p=a^2+3b^2$, a, b 奇数とし，$w^3\equiv 1 \pmod p$ なる w に対して，分割様式は

$$C_+=wB_+,\ C_-=wB_-,\ D_+=w^2B_+,\ D_-=w^2B_-$$

となるもの．なお $n=3p$ でもよい．これは W型のWilliamson 等式である．整数分解は

$$4n = a^2 + b^2 + b^2 + b^2$$

沢出・小野［3］は多くの解を得た．$n=39$ は Agayan-Sarukhanyan［1］に載せられないものである．

6．最後に $2n-1$ が2つの平方の和 a^2+b^2 で

$$C_+ = C_- = D_+ = D_- = \emptyset$$

の場合，整数分解

$$4n = (a+b)^2 + (a-b)^2 + 1^2 + 1^2$$

に対応するものを Turyn 型の Williamson 等式という．あるいは 2平方 Williamson 等式と呼ぶ．しばらく記号を少し変えてそれを

$$\Big(\varepsilon + 2\sum_{m\in A} e_m x^m\Big)^2 + \Big(\varepsilon + 2\sum_{m\in B} e_m x^m\Big)^2 = 4n-2, \qquad \varepsilon = (-1)^{(n-1)/2}$$

と書く．ここに A, B は $\Omega = \{1, 2, \cdots, n-1\}$ の分割である．この時

$$A_+ = A \cap 2A,\ A_- = A \cap 2B,\ B_+ = B \cap 2B,\ B_- = B \cap 2A,$$

$$\# A_+ = \tfrac{1}{4}(n-1-\varepsilon+a+2b),\quad \# B_+ = \tfrac{1}{4}(n-1-\varepsilon+a-2b),$$

$$\# A_- = \# B_- = \tfrac{1}{4}(n-1+\varepsilon-a)$$

が成立する．すなわち $\# A_+, \# A_-, \# B_+, \# B_-$ がすべて定まり，また A, B をこの条件の下で指定すれば，符号 e_m の分布は完全に決ってしまう．

$2n-1=q$ が素数巾の場合 Turyn の行った Paley 行列の Williamson 等式 (2) への変形は，簡約化された形では，この二平方 Williamson 等式になる．$2n-1$ が素数巾でない場合の解は一つも知られていない．Turyn は不可能と推測している．このことは沢出により $n \leqq 61$ まで確認された．

Turyn の変形を直接2平方 Williamson 等式へ持ってゆくのに，有限体のガウスの和を使うのが自然である［8］．Paley 型のアダマール行列を，四元数型に持って行けない場合の処置，またガウス和を中心にして四元数型を拡張した，“一般四元数型アダマール行列”等も考えられている（山田［6］）．

文献

1. S. S. Agayan, A. G. Sarukhanyan, Recurrence formulas for the construction of Williamson-type matrices, Math. Notes 30 (1982).
2. K. Sawade, Hadamard matrices of order 100 and 108, Bull. Nagoya Inst. Technology. 29 (1977)
3. 沢出和江, 小野貴生, Williamson 等式の Turyn 解, 名古屋工業大学学報 34 (1982).
4. R. J. Turyn, An infinite family of Williamson matrices, J. Combin. Theory, Ser. A 12 (1972)
5. M. Yamada, On the Williamson type j matrices of orders 4·29, 4·41 and 4·37, J. Comb Theory, Ser. A 27 (1979).
6. 山田美枝子, 有限体のガウスの和とそのアダマール行列への応用, 代数的整数論研究集会報告集 (1983).
7. K. Yamamoto, A generalized Williamson equation, Colloquia Math. Societatis János Bolyai 37 (1983).
8. K. Yamamoto, M. Yamada, Williamson Hadamard matrices and Gauss sums, to appear.
9. W. D. Wallis, A. P. Street, J. S. Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard matrices, Lecture Notes 292, Springer-Verlag 1972.

マトロイドのブラケット環

岡山理科大学　渡辺　守

本稿では，正則マトロイドのNeil L. Whiteのブラケット環による特徴付け　およびそれに関連したことがらについて報告する。

有限集合 S と次の i),ii),iii) をみたす $\mathcal{B} \subseteq 2^S$ の組 $(S, \mathcal{B}) = G$ を S 上のマトロイド(matroid)という：

i) $\mathcal{B} \neq \phi$,

ii) $A, B \in \mathcal{B}$, $A \neq B \Rightarrow A \not\subseteq B$,

iii) $A, B \in \mathcal{B}$, $b \in B \Rightarrow \exists a \in A$ s.t. $(B-b) \cup a \in \mathcal{B}$.

$\mathcal{B}$ の要素を基底，基底の位数を G のランクといい，$r(G)$ とかく。基底の部分集合は独立であるといい，そうでないとき従属であるという。

マトロイドに関する基本的なことについては，[2] [7] 等を参照されたい。

以下，単に G とかけばランク n の S 上のマトロイドを表わすものとする。

1. マトロイドの線形表現

マトロイド G が体 K に座標系をもつ，あるいは K 上で線形表現可能であるとは，写像 $\xi : S \longrightarrow V$ (K 上 n 次元の線形空間) で次をみたすものが存在することをいう： 任意の部分集合 $A \subseteq S$ に対して，

A が G で独立である必要十分条件が $\xi(A)$ は V で一次独立でかつ ξ は A 上単射であることである。

一般にマトロイドは必ずしも線形表現可能ではない。 事実，非パップスマトロイド(図1)や非デザルグマトロイド(図2)はいかなる体の上で

も線形表現できない。

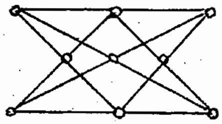
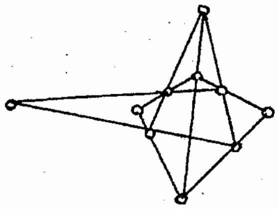
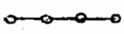
図1 

図2 

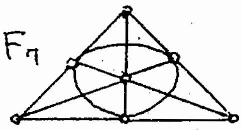
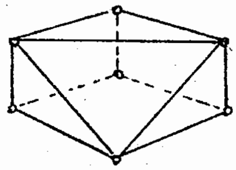
与えられた体 あるいはいくつかの体の各々の上で線形表現可能なマトロイドを特徴付けるという問題はマトロイドの最初の論文 [13] で提起されている。 この問題は2，3を除いて未解決である。

2元体，3元体，またはすべての体の上で線形表現可能なマトロイドをそれぞれ <u>2値マトロイド</u> (binary matroid)，<u>3値マトロイド</u> (ternary matroid)，<u>正則マトロイド</u> (regular matroid) という。 これらについての特徴付けは次のように解かれている。

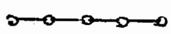
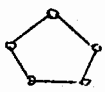
W.T. Tutte (1958 [6])

G 2値マトロイド ⇔ $U_{2,4}$  をマイナ (minor) にもたない

G 正則マトロイド ⇔ Gは2値マトロイドで，かつ Fanoマトロイド F_7 またはその双対 F_7^* をマイナにもたない

F_7  F_7^* 

R.E. Bixby (1979 [1])， P.D. Seymour (1979 [4])

G 3値マトロイド ⇔ F_7，F_7^*，$U_{2,5}$  または $U^*_{3,5}$  をマイナにもたない

P.D. Seymour (1979 [4])

G 正則マトロイド ⇔ 2値 かつ 3値マトロイド.

3値マトロイド，正則マトロイドの新しい特徴づけとして [5] がある。しかし，P元体 (P>3) 上線形表現可能なマトロイドの特徴づけは未解決のままである。

N. White により導入されたブラケット環の概念により，2値マトロイド

および正則マトロイドの新しい特徴づけを与える。上記の特徴付けはいずれも特定のマトロイドをもたないという形，すなわち禁止マトロイドによるものであり，従って幾何学的であるのに対し，White によるものは代数的（環論的）である。ブラケット環はマトロイドの線形表現との関係だけでなく，それ自体非常に興味ある構造をもっており，またマトロイドをそのブラケット環上の加群として表わすことにより線形表現をもたないマトロイドに対しても線形表現に類似した表現，特徴が得られる（[8], [9]）。

2. ブラケット環

G は S 上のランク m のマトロイドとする。S の元の順序付き m 組 $X=(x_1,\cdots,x_m)$ に対し，記号 $[X]=[x_1,\cdots,x_m]$ を対応させ，これを<u>ブラケット</u>（bracket）とよぶ。ブラケット達 $\{[X]\mid X\in S^m\}$ で生成され整数環 $\mathbb{Z}$ 上の可換な多項式環を R_G とする。次の関係式で生成された R_G のイデアル I_G を考え，その商環 $R_G/I_G=B_G$ を<u>ブラケット環</u>とよぶ：

(1)　X が重複元を含むかまたは X が G で従属であるとき，$[X]=0$

(2)　$\{1,2,\cdots,m\}$ 上の任意の置換 σ に対して，$[X]=(\mathrm{sgn}\,\sigma)[\sigma X]$

(3)　$[x_1,\cdots,x_m][y_1,\cdots,y_m]$

$$=\sum_{i=1}^{m}[y_i,x_2,\cdots,x_m][y_1,\cdots,y_{i-1},x_1,y_{i+1},\cdots,y_m]$$

(3) は，$x_1,\cdots,x_m$ を行列の列ベクトル，$y_1,\cdots,y_m$ を単位ベクトルとみなすと小行列式による行列式の Laplace 展開に対応しており，これらの関係式は行列式の性質の抽象化である。

定義より，直ちに　$B_G\ni[X]\neq 0$　である必要十分条件は X が G の基底なことであることがわかる。

環準同型写像 $\eta: B_G \to K$(体) で, G の任意の基底 X に対して $\eta[X] \neq 0$ であるものを体 K への c-準同型写像 (coordinatizing homomorphism) とよぶ。

定理 1 ([9]) $\zeta: S \to V$ を G の K 上の線形表現とするとき,

(#) $\eta[X] = \det \zeta X$ により一意的に c-準同型写像 $\eta: B_G \to K$ が定まる。逆に, Y を G の基底とするとき, どの c-準同型写像 $\eta: B_G \to K$ も $M(\zeta) = (\zeta s_1 \cdots \zeta s_m)$ $(s_i \in S)$ が次の形の(#)をみたす一意的な線形表現 ζ を定める:

$$M(\zeta) = \left[\begin{array}{ccc|c} \alpha & & & \\ & 1 & & \\ & & \ddots & * \\ & & & 1 \end{array}\right], \quad \alpha = \eta[Y] \neq 0$$
$$\underbrace{\hphantom{\alpha\ 1\ \ddots\ 1}}_{Y}\ \underbrace{\hphantom{*}}_{S-Y}$$

ζ_1, ζ_2 が同じ c-準同型写像 η を定める必要十分条件は, $M(\zeta_1) = E\, M(\zeta_2)$ なる $\det E = 1$ の行列 E が存在することである。このとき, $\zeta_1 \sim \zeta_2$ とおくと関係 $\sim$ は同値関係である。

これよりマトロイドの線形表現とブラケット環の c-準同型写像が直ちに結びついて次が得られる.

定理 2 ([10])

$\{G$ の K 上の線形表現 $\zeta: S \to V\}/\sim$

$\underset{1:1}{\longleftrightarrow}$ $\{$c-準同型写像 $\eta: B_G \to K\}$

$\underset{1:1}{\longleftrightarrow}$ $\{B_G$ の c-素イデアル $P\}$

ただし, B_G のイデアル P が c-素イデアル (coordinatizing prime) であるとは, $P = \ker \eta$ となる c-準同型写像 $: B_G \to K$ が存在することをいう。このことは P は B_G の素イデアルで, G のどの基底 X に対しても $P \not\ni [X]$ であることと等価である。

FがGのrpwm-像（rank-preserving-weak-map-image）であるとは，次がみたされるときにいう：

i) F, G は共に S 上のマトロイド，
ii) $r(F) = r(G)$，
iii) すべての $A \subseteq S$ に対して，A が G で従属ならば A は F で従属である．

iii)は Fの基底はGの基底になることを表わしている。この概念により，与えられたマトロイドGを構造のわかりやすい別のマトロイドFに移行して考えることが可能になる。rpwm-像に対する定理との類似が次である。

定理3（[10]）

$$\{G\text{の rpwm-像 } F \text{ の } K \text{ 上の線形表現 } \Im\}/\sim$$
$$\underset{1:1}{\longleftrightarrow} \{\text{準同型写像 } \eta : B_G \longrightarrow K \mid \eta[X] \neq 0 \text{ for some } X \subseteq S\}$$
$$\underset{1:1}{\longleftrightarrow} \{B_G \text{の素イデアル } P \mid P \not\ni [X] \text{ for some basis } X \subseteq S\}$$

さて，
$$c\text{-}rad(B_G) = \cap\{B_G \text{の } c\text{-素イデアル} P\}$$
$$rad(B_G) = \cap\{B_G \text{の素イデアル} P\}$$
と定義すると次が得られる。

定理4（[10]）　Gは2値マトロイドとする。

$c\text{-}rad(B_G)$ は c-素イデアルである。

Gが正則マトロイドのとき，

$$rad(B_G) = c\text{-}rad(B_G)$$
$$= \text{集合}\left\{J-L \;\middle|\; \begin{array}{l} J\text{と}I\text{は同次数のブラケットの積で } \eta_0 J = \eta_0 L, \\ \text{ただし，} \eta_0 \text{は} \eta_0[X] = \pm 1 \text{ なる任意に固定された} \\ B_G \text{から } \mathbb{Z} \text{ への準同型写像} \end{array}\right\}$$

で生成された斉次イデアル

ここに，ブラケットの積 $[X_1]\cdots[X_\ell]$ の次数とは $X_1, \cdots, X_\ell$ 中に現われる元 $s \in S$ の総数を a_s としたとき重複集合 $M = \sum_{s \in S} a_s \cdot s$ のことをいう。

Gが正則マトロイドでないならば

$c\text{-}rad(B_G) =$ 集合 $\{J+L \mid J$とLは同次数のブラケットの積$\}$で
生成された斉次イデアル.

この定理はTutteのホモトピー定理が本質的にきいており,
Whiteによる次のブラケット環論的な変型を用いて導かれる。

定理5([10])

B_Gにおいて恒等式　$K_1[H_1, e] = K_2[H_2, e]$　$e \in S$
が成立する。ここに, H_1, H_2は連結マトロイド$G-e$における
補点(copoint)で, K_1, K_2はeを通らない補点からなる連結パス
(Tutte道)に対応するブラケットの積である。

次が主定理である。

定理6([10])

Gが2値マトロイドであるとき, Gが正則マトロイドであるための
必要十分条件は$rad(B_G)$がB_Gの素イデアルなことである。

定理4が必要条件を与えており, 十分条件はGが正則でない
と仮定して$rad(B_G)$が素イデアルでないことを導くのであるが, その
ために正則マトロイドの先のTutteの禁止マトロイドによる条件
と次のブラケット環の構造についての性質を用いる。

$B_G \cong B_{G^*}$, Gの任意のマイナFについて$B_F \hookrightarrow B_G$。

しかし, 3値マトロイドのブラケット環による特徴づけについては
未解決である。

[10]において, 正則マトロイドGに対して　$rad(B_G)=0$
したがってGが正則であるための必要十分条件はB_Gが整域
であろうと予想されている。

3. ブラケット環の Krull 次元

[10]において、ブラケット環 B_G の Krull 次元 すなわち B_G の素イデアル達の鎖達の中での最大の長さの決定の問題提起がなされているが、[12]においてその解決をみている。

ブラケット環の係数 $\mathbb{Z}$ の代りに体 k をとって考えたブラケット環 B_G^k を考え次の写像を考える。

G の <u>弱い線型表現</u> とは 写像 $\xi : S \longrightarrow V$ (k の適当な拡大体 K 上の n 次元の線形空間)で、ξ が A 上単射でかつ $\xi(A)$ が V で一次独立 なら A が G で独立 なことがすべての $A \subseteq S$ に対していえることをいう。この場合、定理2の類似は次である。

$$\{B_G^k \text{ の素イデアル } P \mid P \not\ni [Z] \text{ for every basis } Z \text{ of } G\}$$

$$\underset{1:1}{\longleftrightarrow} \{G \text{ の弱い線型表現 } \xi : S \to V \mid M(\xi) \text{ が下の形のもの}\}/\sim$$

$$M(\xi) = \Big[\underbrace{\begin{matrix} 1 & & \\ & \ddots & \\ & & 1 \end{matrix}}_{Z} \Big| \underbrace{\;*\;}_{S-Z}\Big] \quad (= M_{P,Z} \text{ とかく})$$

k 上代数的に独立な $M_{P,Z}$ の要素 $(\in K)$ の最大個数を $\mathrm{td}(M_{P,Z})$ とかくとき、B_G^k の Krull 次元は次で与えられる。

<u>定理7</u> ([12]) $$\text{Krull dim}\,(B_G^k) = \max_{\substack{P,\,Z \\ [Z]\notin P}} \mathrm{td}(M_{P,Z})$$

White は[12]の中で B_G^k のイデアルによるすべての飽和降鎖列が同じ長さをもつかどうかを考察している。正則マトロイド G に対しては rad B_G が素イデアルなことより肯定的である。さらに B_G が Macauley 環なら肯定的となるが、B_G が Macauley 環とならないマトロイド G を与えている。

[11] において，マトロイド G の基底単項式環 M_G^k を定義して次の結果を得ている。（k は体）

(1) M_G^k は Macauley 環。

(2) $\text{Krull dim}\,(M_G^k) = |S| - c(G) + 1$

ここに，$c(G)$ は G の連結成分の個数。

(3) 線形表現可能なマトロイド G に対して

$$\text{Krull dim}\,(B_G^k) \geqq \text{Krull dim}\,(M_G^k)$$

ここに，M_G^k は次のように定義される環のことをいう。

多項式環 $k[S]$ を考え，そのすべての単項式 $\prod_{s\in S} s^{e_s}$ $(e_s \in N \cup \{0\})$ からなる乗法的モノイドを $\mathcal{M}$ とする。N を平方因子を含まない単項式 $s_1 s_2 \cdots s_n$（ただし，$s_1, \cdots, s_n$ は G の基底）全体の集合とする。M_G を k と N で生成された $\mathcal{M}$ の部分モノイドとする。k と N で生成された $k[S]$ の部分環 $k[N] = k[M_G]$ を基底単項式環（basis monomial ring）という。

文献

[1] R. E. Bixby, On Ried's characterization of ternary matroids, J. Comb. Theory, Ser B26 (1979), 174–204.

[2] T. Brylawski, D. G. Kelly, Matroid and combinatorial geometries, MAA Studies in Math, vol 17 (1978), 179–217.

[3] P. D. Seymour, The forbidden minors of binary clutters, J. London Math. Soc. (2), 12 (1976), 356–360.

[4] ————, Matroid representation over GF(3), J. Comb. theory, Ser. B26 (1979), 159–173.

[5] K. Truemper, Alpha-balanced graphs and matrices and GF(3)-representability of matroids, J. Comb. Theory, Ser. B 32 (1982), 112-139.

[6] W. T. Tutte, A homotopy theorem for matroids I, II, Trans. Amer. Math. Soc. 88 (1958), 144-174.

[7] D. J. A. Welsh, "Matroid Theory", Academic Press, 1976.

[8] N. White, The bracket ring and combinatorial geometry, Harvard University, Cambridge, Mass., 1971.

[9] ——————, The bracket ring of a combinatorial geometry I, Trans. Amer. Math. Soc., 202 (1975) 79-95.

[10] ——————, The bracket ring of a combinatorial geometry II: unimodular geometries, Trans. Amer. Math. Soc., 214 (1975) 233-248.

[11] ——————, The basis monomial ring of a matroid, Advances in Math., 24 (1977), 292-297.

[12] ——————, The transcendence degree of a coordinatization of a combinatorial geometry, J. Comb. Theory, Ser. B29 (1980), 166-175

[13] H. Whitney, On the abstract properties of linear dependence, Amer. J. Math., 57 (1935), 509-533

(t)-デザインについて

永尾汎．厚見寅司

藤原氏の指摘どおりに統計学では(2)-デザインという概念はすでにgroup divisible designとしてR. M. Wilson [4], Hanani [2]等により研究されていた(ほとんどがgroup divisible designに関する存在定理がおもな結果である). しかし一般の(t)-デザインの場合について我々のような形でsystematicに考えているものはないように思われますので以下の結果を報告します。

岡山で発表した時と少し記号を変えますので注意して下さい。

$V = N\times F$ $\quad N=\{1,2,\cdots,n\}$ $\quad F=\{\alpha,\beta,\cdots\}$ $\quad |F|=q$.

とし, $V\supset S$ に対し $S_N=\{i\in N \mid \exists\alpha\in F \text{ s.t. } (i,\alpha)\in S\}$ (Nへのprojection)とする。また $S=\{(i_1,\alpha_1),\cdots,(i_k,\alpha_k)\}$ が[k]-setというのは $|S|=|S_N|=k$ (i.e. $i_1,\cdots,i_k$ はすべて異なる)と定義する。

定義 $\mathcal{B}$ を[k]-setのあるfamilyとするとき. $(V,\mathcal{B})$ が[t]-$(n\times q, k, \lambda)$ design $\overset{d}{\Longleftrightarrow}$ $\forall$[t]-set T を含む $B\in\mathcal{B}$ の個数が丁度λ個であるとき.

注意 上の定義で $q=1$ のとき t-design, $k=n$ のとき orthogonal array, $t=2$ のとき Hanani 等のいう group divisible design である。

以下の2つの例は多分 well-known であろう。

例1. $N=\mathbb{F}_q^n$, $F=\mathbb{F}_q^m$ $\quad V=N\times F$: $n+m$次元のaffine空間

block B として V の r次元 affine subspace で $\dim B=\dim B_N=r$ となるものをとる. $(r\leqq n)$ $\quad \mathcal{B}$: blockの全体とする。

$(V,\mathcal{B})$ $\quad$ [2]-$(q^n\times q^m,\ q^r,\ \lambda)$ design となる

ただし $\lambda = q^{m(r-1)} \dfrac{(q^{n-1}-1)\cdots\cdots(q^{n-r+1}-1)}{(q^{r-1}-1)\cdots\cdots(q-1)}$

例2. $V' = \mathbb{F}_q^n$ とする. V' に次のような座標をいれる. 原点Oを通る直線上の点は同じ座標をもつ.

原点を通らない r 次元 subspace を block, その全体を $\mathcal{B}$ とすると

$$(V\ \ \mathcal{B}) : [2]-\left(\frac{q^n-1}{q-1}\times(q-1),\ q^r,\ \lambda\right) \text{ design}$$

ただし, $V = V' - \{0\}$, $\lambda = q^{r-1}\dfrac{(q^{n-2}-1)\cdots\cdots(q^{n-r}-1)}{(q^{r-1}-1)\cdots\cdots(q-1)}$.

例3. (新しい例と思われる)

$(N, \mathbb{C})$: $t-(n, k, \lambda)$ design と $F = \mathbb{F}_q \supsetneq A \neq \phi$ を与えたとき.

$\mathcal{B} := \{B \subseteq N\times F \mid B_N \in \mathbb{C}$, かつ $\sum_{(i,\alpha_i)\in B}\alpha_i \in A\}$ とおくと.

$(N\times F, \mathcal{B})$ は $[t]-(n\times q,\ k,\ \lambda q^{k-t-1}|A|)$ design である.

Prop.1 $(V\ \ \mathcal{B}) : [t]-(n\times q,\ k,\ \lambda)$ design

$\Rightarrow (V\ \ \mathcal{B}) : [i]-$ design $\quad i \leq t$.

証.

$\forall I$: $[i]$-set とし, I を含む blocks の個数を λ_i とすると

J : $[t-i]$-set $\qquad I_N \cap J_N = \phi$

$\{(J, B) \mid J : [t-i]\text{-set},\ J\cup I \subseteq B \in \mathcal{B}\}$ の元の個数を2通りに数える。

$$\binom{n-i}{t-i} q^{t-i}\lambda = \lambda_i \binom{k-i}{t-i} \quad \therefore\ \lambda_i = \frac{\binom{n-i}{t-i}}{\binom{k-i}{t-i}} q^{t-i}\lambda$$

$(V, \mathcal{B}) : [t]-(n\times q,\ k,\ \lambda)$ design. I : $[i]$-set, J : $[j]$-set, $i+j \leq t$ とし, また $I_N \cap J_N = \phi$ とする。

Prop.2. $\Gamma_I^J = \{B \in \mathcal{B} \mid I \subset B,\ B_N \cap J_N = \phi\}$ とすれば $|\Gamma_I^J|$ は

iとjのみできまり，これをμ_i^jで表せば $\mu_i^j = \mu_i^{j-1} - q\mu_{i+1}^{j-1}$ が成立する。

証．$j=0$ のときは自明．　$j>0$ とし j に関する induction．$J_N \ni l$ を一つきめ，
$x=(l,\delta)\in J$ とし　$J' = J - \{x\}$．$F=\{\alpha_1,\cdots,\alpha_q\}$ とするとき $y_i = (l\ \alpha_i)$
とし，$I_i' = I \cup \{y_i\}$ とする。$\mathcal{C}_I^{J'} \ni B$ に対し $B_N \ni l \Longrightarrow B \ni$ some y_i だから
$B\in \mathcal{C}_{I_i'}^{J'}$ for some i.　　　　$B_N \not\ni l \Longleftrightarrow B \in \mathcal{C}_I^J$

$$\therefore\quad \mathcal{C}_I^{J'} = \Big(\bigsqcup_{i=1}^{q} \mathcal{C}_{I_i'}^{J'}\Big) \sqcup \mathcal{C}_I^J$$

disjoint

$$\therefore\ |\mathcal{C}_I^J| = |\mathcal{C}_I^{J'}| - q|\mathcal{C}_{I_1'}^{J'}| \qquad \text{帰納法より}$$

$$\mu_i^j = \mu_i^{j-1} - q\mu_{i+1}^{j-1}.$$

Prop. 3 (Chaudhuri－Wilson の定理の拡張)(新しい結果と思われる)

$\exists\ (V, \mathbb{B}) : [2s]\text{-}(n\times q, k, \lambda)$ design　　$n \geqq k+s$

$\Rightarrow\quad b \geqq \binom{n}{s} q^s$　　　ただし，$b = |\mathbb{B}|$

証．$\mathcal{S} = \{S : [s]\text{-set}\}$ を basis とする $\mathbb{R}$上の vector space を
$W = \bigoplus_{S\in\mathcal{S}} \mathbb{R}S$ とする。　　$\dim W = \binom{n}{s}q^s$．　　$\mathbb{B}\ni B$ に対し
$\zeta_B := \sum_{\mathcal{S}\ni S\subset B} S$　とし，$W = \langle \zeta_B \mid B \in \mathbb{B}\rangle$ を示せばよい。
$\mathcal{S}\ni S_0$ を一つfixし，$0\leqq i\leqq s$ なる i に対して
$\xi_i := \sum_S{}' S$　(ここで S は $|S\cap S_0| = |S_N \cap (S_0)_N| = s-i$ なる
S をわたる)とおく．明らかに $\xi_0 = S_0$

注意　$|S\cap S_0| = |S_N\cap(S_0)_N|\ (= s-i)$

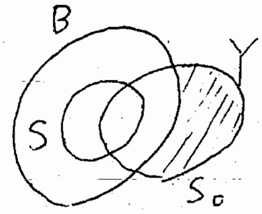
$\Leftrightarrow\ (S-(S\cap S_0))_N \cap (S_0-(S\cap S_0))_N = \phi$.

$\Leftrightarrow\ S_N \cap (S_0 - (S\cap S_0))_N = \phi \ \Leftrightarrow\ S\cup S_0$ が $[s+i]$-set

また $\eta_i := \sum_B \zeta_B$　(B は $|B\cap S_0| = |B_N\cap(S_0)_N| = s-i$ をみたすもの)

$= \sum_{S} \mu_S S$ とおけば

$$\mu_S = \#\{B \in \mathbb{B} \mid \underbrace{S \subset B,\ |B \cap S_0| = |B_N \cap (S_0)_N| = s-i}_{条件㊟とする.}\}$$



○ いま. S, B は条件㊟をみたすとする。
$Y = S_0 - (B \cap S_0)$ とおくと, Y は $[i]$-set
$B_N \cap Y_N = \phi$, $S \cup S_0 - Y \subset B$, $|S \cap S_0| = |S_N \cap (S_0)_N|$ が成り立つ

○ 逆に $|S \cap S_0| = |S_N \cap (S_0)_N| = s - r$ なる $[s]$-set S と
$S_0 - (S \cap S_0) \supset Y$, $|Y| = i$ なる Y に対して $B \in \mathbb{B}$ が
(**) $B_N \cap Y_N = \phi$, $S \cup S_0 - Y \subset B$ をみたせば, S. B は条件㊟をみたす. ここで上のような Y は $\binom{r}{i}$ 個, 各 Y に対し
$((S \cup S_0) - Y)_N \cap Y_N = \phi$ より (**) をみたす B の個数は μ^i_{s+r-i}.
よって $\mu_S = \binom{r}{i} \mu^i_{s+r-i}$ となる。よって

(***) $$\eta_i = \sum_{r=i}^{s} \binom{r}{i} \mu^i_{s+r-i} \xi_r \qquad (0 \le i \le s)$$

係数の行列は三角行列で対角線上には μ^i_s がならぶ.
ここで $\mu^i_s > 0$
(∵) $k + s \le n$ より $B \in \mathbb{B}$ に対し $|N - B_N| = n - k \ge s$.
$0 \le i \le s$ に対し $\exists Y$: $[i]$-set s.t. $B_N \cap Y_N = \phi$
$|B_N| = k > t = 2s$ より $\exists\, X \subset B$ s.t. $|X| = s$, このとき
$X_N \cap Y_N = \phi$ で $X \subset B$, $B_N \cap Y_N = \phi$ $\therefore \mu^i_s > 0$

よって (***) を解いて $\xi_0 = S_0$ は $\{\eta_i\}$ の l. comb. 特に
$S_0 \in \langle \xi_B \mid B \in \mathbb{B} \rangle$.

Prop.3. (Cameron-Bush の結果の拡張) (新しい結果と思われる)
$\exists\ (V, \mathbb{B})$: $[t]$-$(n \times q, k, 1)$ design $\Longrightarrow$

(1) $1<q$, $1\leq t+1<k\leq n$ のとき $(t+1)(k-t-1)\leq(n-t-1)q$

(2) $q=1$, $1\leq t<k<n$ のとき $(t+1)(k-t)\leq n-t-1$.

対称的[2]-design

定義 $(V\ \mathbb{B})$ $[2]-(n\times q;k,\lambda)$ design とする。

$(V\ \mathbb{B})$ 対称的 $\overset{d.}{\Longleftrightarrow}$ $(V\ \mathbb{B})$ の dual が同じパラメータをもつ $[2]-(n\times q,k,\lambda)$ design.

例2′ 例2で $r=n-1$ のとき $(V\ \mathbb{B})$ は 対称的 $[2]-\left(\frac{q^{n}-1}{q-1}\times(q-1),\ q^{n-1},\ q^{n-2}\right)$ design である。

[t]-design の拡大

$(V,\mathbb{B})$ $[t]-(n\times q,k,\lambda)$ design とする。 $V\ni(1,\alpha)$

$V-\{(1\ \beta)\mid\beta\in F\}=V_{(1,\alpha)}$ とおく, $\mathbb{B}'=\{B\in\mathbb{B}\mid(1\ \alpha)\in B\}$

とすると $(V_{(1\alpha)},\mathbb{B}')$ は $[t-1]-((n-1)\times q,\ k-1,\ \lambda)$ design になる。

上の $(V_{(1\alpha)},\mathbb{B}')$ は $(V\ \mathbb{B})_{(1,\alpha)}$ と表わす。

$(V\ \mathbb{B})$ [t]-design に対して [t+1]-design $(V^*\ \mathbb{B}^*)$ が存在して $(V^*\ \mathbb{B}^*)_{(l,\alpha)}=(V\ \mathbb{B})$ for some $(l\ \alpha)\in V^*$ のとき $(V\ \mathbb{B})$ は拡大可能であるという。

Prop.4 $(V\ \mathbb{B})$ $[t]-(n\times q,k,\lambda)$ design 拡大可能

$\Rightarrow b(n+1)q\equiv 0 \pmod{k+1}$

Prop.5 対称的 $[2]-(n\times q,\ k,\ \lambda)$ design 拡大可能

$\Rightarrow 2(\lambda q+1)(\lambda q+2)\equiv 0 \pmod{k+1}$

次の結果は orthogonal array に置換群を作用させることより [t]-design がつくれることを示す。多分 well-known であろう

Prop. 6. $A=(a_{ij})$ $N\times k$ 行列 $a_{ij}\in\mathbb{F}_q$
A $(N, k, q, 2)$ orthogonal array (index λ),
G 2重可移群 on $\Omega=\{1,2,\cdots,n\}$ $n>k$ とする。
Aの列全体をGでpermuteさせれば（列がない時 $a_{i,j'}=a_{i,g(j)}$ $g\in G$ とおく） $[2]-(n\times q, k, \lambda')$ designが出来る。

References

1. T. Atsumi, A study of orthogonal arrays from the point of view of design theory, J. Combinatorial Theory A 35 (1983), 241−251.
2. H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255−369.
3. H. Nagao, 群とデザイン 岩波書店 1974
4. R. M. Wilson, An existence theory for pairwise balanced designs I, J. Combinatorial Theory A 13 (1972) 220 − 245.
5. ——————, An existence theory for pairwise balanced designs II, J. Combinatorial Theory A 13 (1972) 246 − 273.

Codes and Designs in Association Schemes

Tatsuro Ito

1. Introduction I should like to discuss a few topics about codes and designs in association schemes, which I am currently interested in. The first topic is perfect codes in symmetric groups S_n. I shall discuss Nomura's Theorem [10] which states how perfect 1-codes are distributed to cosets $S_k \backslash S_n$. As a corollary to Nomura's Theorem, we have a stronger version of the sphere packing condition. This kind of theorem holds for perfect e-codes in the Hamming schemes $H(n, q)$ (Munemasa [9]) and is expected to hold for perfect e-codes in association schemes whose automorphism groups contain regular subgroups G and "good" subgroups H of G.

The second topic is designs in symmetric groups S_n. Associated with a permutation representation of S_n, we shall consider designs in S_n which are defined algebraically and can be interpretated geometrically as a generalization of orthogonal permutation arrays.

The third topic is perfect codes and tight designs in (P and Q)-polynomial association schemes. We shall discuss the properties of Lloyd/Wilson polynomials, namely they are balanced ${}_4\varphi_3$ (Askey-Wilson polynomials) and have their roots all rational. We believe these properties are strong enough to eliminate perfect e-codes and tight t-designs in the known (P and Q)-polynomial association schemes for sufficiently large e and t.

The fourth topic is the geometric meaning of t-designs in the known (P and Q)-polynomial association schemes. We consider meet semi-lattices with certain regularity to interpretate t-designs geometrically. These meet semi-lattices are closely related to and seem to be constructed by certain maximal cliques in the (P and Q)-polynomial association schemes.

The reader who is unfamiliar with association schemes can be referred to §2.2 and 2.3 of [1].

2. Perfect Codes in Symmetric Groups Let X be a finite group and $C_0=\{1\}, C_1, \cdots, C_d$ the conjugacy classes of X. Define the relations R_i on X $(0 \le i \le d)$ by

$$(x,y) \in R_i \Longleftrightarrow x^{-1}y \in C_i \qquad \text{for } x, y \in X.$$

Then $\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$ is a commutative association scheme. Let $\chi_0 = 1, \chi_1, \cdots, \chi_d$ be the irreducible characters of X over $\mathbb{C}$. Then the 1st eigenmatrix $P = (p_i(j))$ and the 2nd eigenmatrix $Q = (q_i(j))$ are given by

$$p_i(j) = \frac{k_i\, \chi_j(x_i)}{f_j},$$

$$q_i(j) = f_i\, \overline{\chi_i(x_j)},$$

where $k_i = |C_i|$, $f_i = \chi_i(1)$ and $x_i \in C_i$ (see §2.7 [1]).

For a subset M of $\{0, 1, \cdots, d\}$ which contains 0, we set

$$\Sigma(x) = \{ y \in X \mid (x,y) \in R_i \text{ for some } i \in M \}.$$

A subset Y of X is said to be an <u>M-code</u> if

$$\Sigma(x) \cap \Sigma(y) = \phi \qquad \text{for distinct } x, y \in Y.$$

An M-code Y is <u>perfect</u> if $X \times X$ is the disjoint union of $\Sigma(x)$ $(x \in Y)$. Since $|\Sigma(x)| = \sum_{i \in M} k_i$, an M-code Y satisfies the sphere packing bound $\quad |Y| \leq |X| / \sum_{i\in M} k_i$

with the equality holding if and only if Y is perfect. In particular, $\sum_{i\in M} k_i$ divides $|X|$ if Y is a perfect M-code. Another necessary condition for the existence of a perfect M-code Y is derived from the distribution of Y to $C_0, C_1, \cdots, C_d$:

Theorem of Lloyd type $\quad$ Let Y be a perfect M-code in X. Then there exist at least $|M|-1$ irreducible characters χ of X over $\mathbb{C}$ such that

$$\sum_{i\in M} \frac{k_i \chi(x_i)}{\chi(1)} = 0,$$

where $k_i = |C_i|$ and $x_i \in C_i$.

Now, let X be the symmetric group S_n of degree n. For $x, y \in X$, let $\partial(x, y)$ be the minimum number of transpositions whose product is $x^{-1}y$. Then $\partial(\ ,\ )$ is a distance in X. For a positive integer e, let $\Sigma_e(x)$ be the e-ball with centre x :

$$\Sigma_e(x) = \{ y \in X \mid \partial(x, y) \leq e \}.$$

A subset Y of X is called an e-code if

$$\Sigma_e(x) \cap \Sigma_e(y) = \phi \qquad \text{for distinct } x, y \in Y.$$

The e-ball $\Sigma_e(1)$ with centre the identity 1 is a union of conjugacy classes C_i $(i \in M)$ and e-codes are nothing but M-codes.

When M. Deza visited Japan in 1978 (it may be in 1977, I cannot remember exactly), he proposed E. Bannai, who was then in Gakushuin University, to classify perfect e-codes in symmetric groups, but his definition of distance was slightly different : $\partial(x, y)$ is the number of letters actually moved by $x^{-1}y$.

The present definition of $\partial(\ ,\ )$ and the formulation of the perfect e-code problem are due to E. Bannai and M. Yoshizawa. They first tried to classify perfect 1-codes Y in S_n but got stuck with $n = 11$. The sequence of n which satisfy the sphere packing condition $n!/\{1+\binom{n}{2}\} \in \mathbb{Z}$ is 6, 11, 18, 27, 37, 38, ---, including an infinite sequence m^2+2. The consideration of Y's distribution to C_i $(0 \le i \le d)$ eliminates $n=6$ but not $n=11$, and they suspected that there might exist perfect 1-codes in S_{11} related to the Mathieu group M_{11}. Recently, Nomura [10] eliminated the case $n=11$ by considering the distribution of a perfect 1-code to the cosets $S_k \backslash S_n$.

Theorem (Nomura) Let Y be a perfect 1-code in S_n. Let H be a subgroup of S_n isomorphic to S_k $(k \ge [\frac{n}{2}]+1)$, embedded naturally in S_n. Then Y is distributed evenly to the cosets $H \backslash S_n$:

$$|H \cap Y| = |Hx \cap Y| \qquad \text{for all } x \in S_n.$$

In particular, $1+\binom{n}{2}$ divides $k!$.

This theorem improves the sphere packing condition $n!/\{1+\binom{n}{2}\} \in \mathbb{Z}$ and eliminates perfect 1-codes in S_n for $n = 6, 11, 18$. So S_{27} is the smallest symmetric group in which the existence of perfect 1-codes is unknown.

Nomura's theorem is expected to hold for perfect e-codes in association schemes whose automorphism groups have regular subgroups G and "good" subgroups H of G, e.g., Hamming schemes, association schemes of bilinear forms / classical forms (see §3.6 [1]). For Hamming schemes, Munemasa [9] showed

<u>Theorem</u> (Munemasa) Let Y be a perfect e-code in the Hamming scheme $H(n,q)$. Let u be the minimum zero of the Lloyd polynomial $\sum_{i=0}^{e} K_i(x)$, where $K_i(x)$ is the Krawtchouk polynomial of degree i:

$$K_i(x) = \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{x}{j}\binom{n-x}{i-j}.$$

Equip the underlying space $X = \overbrace{F \times \cdots \times F}^{n}$ ($|F| = q$) with a group structure such as the direct product of n copies of F, and let H be a subgroup of X isomorphic to $\overbrace{F \times \cdots \times F}^{k}$ ($k \geq n-u+1$), embedded naturally in X. Then Y is distributed evenly to $H\backslash X$:

$$|H \cap Y| = |Hx \cap Y| \qquad \text{for all } x \in X.$$

In particular, $\sum_{i=0}^{e} \binom{n}{i}(q-1)^i$ divides q^k.

Notice that u is a positive integer by the Lloyd theorem. Munemasa's theorem is an improvement of the sphere packing condition $q^n / \sum_{i=0}^{e} \binom{n}{i}(q-1)^i \in \mathbb{Z}$. Perfect e-codes in $H(n,q)$ have been completely classified for $e \geq 3$ and remain unclassified for $e = 1, 2$, mainly because the Lloyd theorem is useful for $e \geq 3$ but not for $e = 1, 2$. For $e = 2$, Munemasa's theorem claims $q^{n-u+1} / \{1 + n(q-1) + \binom{n}{2}(q-1)^2\}$ is an integer, where

$$u = \frac{1}{q}\left\{2 + n(q-1) - \frac{q}{2} - \sqrt{\frac{q^2}{4} + (q-1)(n-2)}\right\},$$

and we hope this is a useful information to classify perfect 2-codes in $H(n,q)$; the ternary Golay code is the only known perfect 2-code.

Coming back to perfect 1-codes in S_n, the theorem of Lloyd type is that there exists an irreducible character χ of S_n over $\mathbb{C}$ such that

$$1 + \binom{n}{2}\frac{\chi(x)}{\chi(1)} = 0 \qquad \text{for a transposition } x.$$

H. Enomoto and T. Saito ran computers to make the list of such χ for $n \leq 30$. There were lots of such χ, but all of them were found to belong to the principal 2-block if n satisfies the sphere packing condition $\frac{n!}{1+\binom{n}{2}} \in \mathbb{Z}$. This fact seems interesting itself.

<u>Question</u> Let χ be an irreducible character of S_n over $\mathbb{C}$ such that $1 + \binom{n}{2}\frac{\chi(x)}{\chi(1)} = 0$ for a transposition x. Then does χ belong to the principal 2-block, if $1+\binom{n}{2}$ divides $n!$?

3. <u>Designs in Symmetric Groups</u> Let $\mathcal{X} = (X, \{R_i\}_{0\leq i\leq d})$ be a commutative association scheme. Let Y be a subset of X. The <u>inner distribution</u> of Y is $\mathbb{a} = (a_0, a_1, \cdots, a_d)$ with

$$a_i = \frac{1}{|Y|}\,|Y\times Y \cap R_i| \qquad (0 \leq i \leq d),$$

and the <u>dual</u> of $\mathbb{a}$ is $\mathbb{a}' = (a_0', a_1', \cdots, a_d')$ with

$$a_i' = \frac{1}{|Y|}\sum_{j=0}^{d} a_j\, q_i(j) \qquad \left(\text{i.e., } \mathbb{a}' = \frac{1}{|Y|}\mathbb{a}Q\right),$$

where $Q = (q_i(j))$ is the 2nd eigenmatrix of $\mathcal{X}$. Delsarte [2] showed

<u>Delsarte Condition</u> $\quad a_i' \geq 0 \qquad (0 \leq i \leq d)$,

and defined that Y is a <u>T-design</u> for $T \subseteq \{1, 2, \cdots, d\}$ if

$$a_i' = 0 \qquad \text{for } i \in T.$$

Now, let X be a finite group and $\mathcal{X} = (X, \{R_i\}_{0\leq i\leq d})$ the association scheme on X as in the previous section. Then for a subset Y of X, the dual inner distribution $\mathbb{a}' = (a_0', a_1', \cdots, a_d')$ of Y is given by

$$a_i' = \frac{\chi_i(1)}{|Y|^2} \sum_{x,y\in Y} \chi_i(x^{-1}y),$$

and so Y is a T-design if and only if

$$\sum_{x,y\in Y} \chi_i(x^{-1}y) = 0 \qquad \text{for } i \in T.$$

Let X act on a set Ω transitively and π the permutation character. Let T be the set of indices i such that $i \neq 0$ and the irreducible character χ_i actually appears in π. Then by the Delsarte condition, $Y \subseteq X$ is a T-design if and only if

$$1 = \frac{1}{|Y|^2} \sum_{x,y\in Y} \pi(x^{-1}y).$$

For a subset Y of X, set

$$n_{\alpha\beta} = \#\{x \in Y \mid x(\alpha) = \beta\} \qquad (\alpha, \beta \in \Omega).$$

Counting the number of $(\alpha, \beta, x) \in \Omega\times\Omega\times Y$ such that $x(\alpha) = \beta$, we have

$$\sum_{\alpha,\beta\in\Omega} n_{\alpha\beta} = |Y|\cdot|\Omega|.$$

In particular,

$$\sum_{\alpha,\beta\in\Omega} n_{\alpha\beta}^2 \geq |Y|^2,$$

where the equality holds if and only if $n_{\alpha\beta} = |Y|/|\Omega|$ for all $\alpha, \beta \in \Omega$. On the other hand, counting the number of $(\alpha, \beta, x, y) \in \Omega\times\Omega\times Y\times Y$ such that $x(\alpha) = y(\alpha) = \beta$, we have

$$\sum_{\alpha,\beta\in\Omega} n_{\alpha\beta}^2 = \sum_{x,y\in Y} \pi(x^{-1}y).$$

Thus we get

<u>Lemma</u> (Enomoto - Ito) Y is a T-design if and only if

$$n_{\alpha\beta} = \frac{|Y|}{|\Omega|} \qquad \text{for all } \alpha, \beta \in \Omega.$$

In particular, if $|Y|$ is a T-design, then $|Y|/|\Omega| \in \mathbb{Z}$ and

<u>Inequality of Fisher type</u> $\quad |Y| \geq |\Omega|$.

If the equality holds, Y is said to be a <u>tight</u> T-design.

Let X be the symmetric group S_n of degree n and π_k the permutation character of X acting on the ordered k-tuples $\alpha_1, \cdots, \alpha_k$ $\underbrace{(\alpha_i \neq \alpha_j \text{ for } i \neq j)}_{\text{of } \{1,2,\cdots,n\}}$. Let Y be a subset of X. Y forms a $|Y| \times n$ permutation array whose (x,i) entry is $x(i)$ $(x \in Y,\ i \in \{1,2,\cdots,n\})$. By the previous lemma, Y is a T-design associated with π_k if and only if the permutation array is <u>orthogonal with strength k</u>, i.e., the rows of any $|Y| \times k$ subarray contains each ordered k-tuple $\alpha_1, \cdots, \alpha_k$ $(\alpha_i \neq \alpha_j$ for $i \neq j)$ $\dfrac{|Y|}{n(n-1)\cdots(n-k+1)}$ times. Orthogonal permutation arrays of strength k are a generalization of k-ply transitive groups. Given a T-desing Y, we may assume Y contains the identity, because Yx and xY are also T-designs for all $x \in X$. In this sense, I should like to ask

<u>Question</u> Is a T-design Y $(Y \ni 1)$ associated with π_k necessarily a subgroup of X for sufficiently large k ?

If $k=1$, Latin squares are counterexamples. For $k=2$, there are also counterexamples constructed from projective planes. Starting with the permutation character $\tilde{\pi}_k$ of X acting on the k-subsets of $\{1,2,\cdots,n\}$, we can consider a similar T-design problem :

<u>Question</u> Is a $\tilde{T}$-design Y associated with $\tilde{\pi}_k$ necessarily a T-design associated with π_k for sufficiently large k ?

If Y is a subgroup, the answer is affirmative for $k \geq 5$ [7].

Tight designs associated with $\tilde{\Pi}_k$ are counterexamples. So I should like to ask

Question Do there exist tight designs associated with $\tilde{\Pi}_k$ $(k \geq 2)$?

4. Perfect Codes and Tight Designs in (P and Q)-polynomial Association Schemes

Let $\mathcal{X} = (X, \{R_i\}_{0 \leq i \leq d})$ be a symmetric association scheme. Let A_i and E_i $(0 \leq i \leq d)$ be the adjacency matrices of $\mathcal{X}$ and the primitive idempotents of the adjacency algebra, respectively. $\mathcal{X}$ is said to be a P-polynomial association scheme w.r.t. the ordering $A_0, A_1, \cdots, A_d$ if $A_i = v_i(A_1)$ $(0 \leq i \leq d)$ in the adjacency algebra $\mathfrak{A}$ for polynomials $v_i(x)$ of degree i, or equivalently if the graph $\Gamma = (X, R_1)$ is distance-regular, i.e., x and y $(x, y \in X)$ have distance i in the graph Γ if and only if $(x, y) \in R_i$. $\mathcal{X}$ is said to be a Q-polynomial association scheme w.r.t. the ordering $E_0, E_1, \cdots, E_d$ if $E_i = v_i^*(E_1)$ $(0 \leq i \leq d)$ in the dual adjacency algebra $\hat{\mathfrak{A}}$ for polynomials $v_i^*(x)$ of degree i (the multiplication of $\hat{\mathfrak{A}}$ is the Hadamard product, i.e., the entry wise product). We shall give examples of them in the next section.

In what follows, we only consider $\{0, 1, \cdots, e\}$-codes in P-polynomial association schemes and $\{1, 2, \cdots, t\}$-designs in Q-polynomial association schemes. Such codes and designs are simply called e-codes and t-designs, respectively. There are well-known inequalities for e-codes and t-designs [2]:

Sphere Packing Bound $\displaystyle\sum_{i=0}^{e} k_i \leq \frac{|X|}{|Y|}$ for an e-code Y,

Inequality of Fisher Type $\displaystyle\sum_{i=0}^{[t/2]} m_i \leq |Y|$ for a t-design Y, where k_i is the valency of R_i and m_i is the rank of E_i. The bound-achieving e-codes (resp. t-designs) are called <u>perfect</u> (resp. <u>tight</u>). There are well-known necessary conditions for the existence of perfect e-codes and tight t-designs [2] :

<u>Theorem of Lloyd Type</u> If there exists a perfect e-code, then the polynomial $\sum_{i=0}^{e} v_i(x)$ divides $\sum_{i=0}^{d} v_i(x)$. If there exists a tight t-design, then $\sum_{i=0}^{s} v_i^*(x)$ divides $\sum_{i=0}^{d} v_i^*(x)$, where $s=[\frac{t}{2}]$.

The polynomials $\sum_{i=0}^{e} v_i(x)$ and $\sum_{i=0}^{s} v_i^*(x)$ are called the <u>Lloyd polynomial</u> and the <u>Wilson polynomial</u>, respectively.

Now, let $\mathcal{X}=(X, \{R_i\}_{0\le i\le d})$ be a (P and Q)-polynomial association scheme. Leonard [6] showed that $v_i(x)$ and $v_i^*(x)$ are <u>balanced ${}_4\varphi_3$</u> (<u>Askey-Wilson polynomials</u>), including certain limiting cases (see §3.5 [1]). Namely, let

$$u_i(x) = {}_4\varphi_3\left(\begin{matrix} q^{-i},\ s^*q^{i+1},\ q^{-y},\ sq^{y+1} \\ r_1q,\ r_2q,\ r_3q \end{matrix}; q, q\right) \qquad (r_1r_2r_3 = ss^*)$$

$$\text{with} \quad x = \mu(y) = k_1 + \frac{h(1-q^y)(1-sq^{y+1})}{q^y},$$

where $${}_r\varphi_s\left(\begin{matrix} a_1, \cdots, a_r \\ b_1, \cdots, b_s\end{matrix}; q, x\right) = \sum_{t=0}^{\infty} \frac{(a_1;q)_t \cdots (a_r;q)_t}{(b_1;q)_t \cdots (b_s;q)_t} \frac{x^t}{(q;q)_t}$$

$$\text{with} \quad (a;q)_t = \begin{cases} (1-a)(1-aq)\cdots(1-aq^{t-1}) & \text{for } t=1,2,\cdots, \\ 1 & \text{for } t=0. \end{cases}$$

Then $u_i(x)$ is a polynomial of degree i in x with parameters $q, s, s^*, r_1, r_2, r_3, h, k_1$ and it holds that $v_i(x) = k_i u_i(x)$. If we change (s, s^*, h, k_i) to (s^*, s, h^*, m_i), we get $v_i^*(x)$.

$\{u_i(x)\}_{0\le i\le d}$ are orthogonal polynomials w.r.t. the weight $w(x)$, where

$$w(\mu(i)) = m_i = \frac{1}{(s^*q)^i}\,\frac{1-sq^{2i+1}}{1-sq}\,\frac{(sq;q)_i}{(q;q)_i}\prod_{\nu=1}^{3}\frac{(r_\nu q;q)_i}{(\frac{sq}{r_\nu};q)_i} \qquad (0\le i\le d)$$

and $w(x)=0$ for $x \notin \{\mu(0), \mu(1), \cdots, \mu(d)\}$.

Let $V_i(x) = v_0(x) + v_1(x) + \cdots + v_i(x)$. Then $V_d(x)$ has root $\mu(i)$ $(1 \le i \le d)$ and $\{V_i(x)\}_{0 \le i \le d-1}$ are orthogonal polynomials w.r.t. the weight $\tilde{w}(x) = (\mu(0) - x)w(x)$ (see [2]). Setting

$$\tilde{\mu}(y) = \mu(y+1),$$

$$\tilde{s} = sq^2, \quad \tilde{s}^* = s^*q, \quad \tilde{h} = \frac{h}{q}, \quad \tilde{r}_\nu = r_\nu q \quad (\nu = 1, 2, 3),$$

it holds that

$$\tilde{\mu}(y) = \tilde{\mu}(0) + \frac{\tilde{h}(1-q^y)(1-\tilde{s}q^{y+1})}{q^y},$$

$$\tilde{w}(\tilde{\mu}(i)) = c\,\frac{1}{(\tilde{s}^*q)^i}\,\frac{1-\tilde{s}q^{2i+1}}{1-\tilde{s}q}\,\frac{(\tilde{s}q;q)_i}{(q;q)_i}\prod_{\nu=1}^{3}\frac{(\tilde{r}_\nu q;q)_i}{(\frac{\tilde{s}q}{\tilde{r}_\nu};q)_i} \qquad (0 \le i \le d-1)$$

$$\text{with} \quad c = \frac{hs}{q^2}(1-sq^2)(1-sq^3)\prod_{\nu=1}^{3}\frac{1-r_\nu q}{r_\nu - sq}$$

and $\quad \tilde{w}(x) = 0 \quad$ for $x \notin \{\tilde{\mu}(0), \tilde{\mu}(1), \cdots, \tilde{\mu}(d-1)\}$.

Thus we have

<u>Theorem</u>
$$\frac{V_i(x)}{V_i(\tilde{\mu}(0))} = {}_4\varphi_3\left(\begin{matrix} q^{-i},\ \tilde{s}^*q^{i+1},\ q^{-y},\ \tilde{s}q^{y+1} \\ \tilde{r}_1q,\ \tilde{r}_2q,\ \tilde{r}_3q \end{matrix};\, q, q\right) \qquad (0 \le i \le d-1)$$

$$\text{with} \quad x = \tilde{\mu}(y) = \tilde{\mu}(0) + \frac{\tilde{h}(1-q^y)(1-\tilde{s}q^{y+1})}{q^y}.$$

So Lloyd polynomials $V_e(x)$ are also balanced ${}_4\varphi_3$. Similarly Wilson polynomials $V_s^*(x) = \sum_{i=0}^{s} v_i^*(x)$ are also balanced ${}_4\varphi_3$.

In §3.7 [1], it is shown that $\mu(i)$ $(0 \le i \le d)$ are rational integers for (P and Q)-polynomial association schemes. On the other hand, if there exists a perfect e-code, then $V_e(x)$ divides $V_d(x)$ by the Lloyd theorem. Thus we have

<u>Corollary</u> If there exists a perfect e-code in a (P and Q)-polynomial association scheme, then the roots of the polynomial (in x)

$$ {}_4\varphi_3\left(\begin{matrix} q^{-e}, \ \tilde{s}^* q^{e+1}, \ q^{-y}, \ \tilde{s} q^{y+1} \\ \tilde{r}_1 q, \ \tilde{r}_2 q, \ \tilde{r}_3 q \end{matrix} ; q, q \right) $$

$$ \text{with} \quad x = \tilde{\mu}(y) = \tilde{\mu}(0) + \frac{\tilde{h}(1-q^y)(1-\tilde{s}q^{y+1})}{q^y} $$

are contained in $\{\tilde{\mu}(i) \mid 0 \le i \le d-1\} \subseteq \mathbb{Z}$.

For tight t-designs, a similar corollary holds, changing $e, \tilde{s}^*, \tilde{s}, \tilde{h}, \tilde{\mu}(0)$ to $s = [\frac{t}{2}]$, sq, s^*q^2, $\frac{h^*}{q}$, $\tilde{\mu}^*(0)$, respectively; the only difference is that $\tilde{\mu}^*(i)$ are not necessarily rational integers but rational numbers.

In §3.6 [1], there is the list of parameters $q, s, s^*, r_1, r_2, r_3, h, h^*, k_1, m_1$ for the known (P and Q)-polynomial association schemes and in §3.5 [1], it is also shown how to calculate $v_i(x)$ and $v_i^*(x)$ in the limiting cases of balanced ${}_4\varphi_3$, i.e., how to take the limits of the parameters.

We believe that the above corollary is strong enough to eliminate the existence of perfect e-codes and tight t-designs in the known (P and Q)-polynomial association schemes for sufficiently large e and t. In fact, perfect e-codes and tight t-designs have been, by this method, proved not to exist for large e and t in the Hamming scheme $H(n, q)$ (Bannai et al.) and in the association schemes of bilinear forms (personal communication). It is also known that for fixed $t \ge 8$, there are only finitely many tight t-designs in the Johnson scheme $J(v, k)$ (Bannai); for $t = 4, 6$, we need more involved argument to complete the classification (Petersen for $t=6$, N. Ito et al. for $t=4$).

5. <u>The Geometric Meaning of t-Designs in the Known (P and Q)-polynomial Association Schemes</u> Let $L = \bigcup_{i=0}^{d} X_i$ (a disjoint union) be a partially ordered set satisfying the following conditions :

(i) L has the infimum ϕ and $X_0 = \{\phi\}$.

(ii) For any $x \in L$, there exists a sequence $\phi = x_0 < x_1 < \cdots < x_{r-1} < x_r = x$ with no elements between x_i and x_{i+1} and such sequences have the same length $r = r(x)$. Furthermore

$$X_i = \{ x \in L \mid r(x) = i \} \qquad (0 \le i \le d).$$

(iii) Any $x, y \in L$ have the meet $x \wedge y$, i.e., the greatest lower bound.

(iv) Set $X = X_d$ and define relations R_i on X $(0 \le i \le d)$ by

$$(x, y) \in R_i \iff x \wedge y \in X_{d-i}.$$

Then $\mathcal{X}(L) = (X, \{R_i\}_{0 \le i \le d})$ is a (P and Q)-polynomial association scheme.

We call such L a <u>regular semi-lattice</u>. Notice L is different from Delsarte's regular semi-lattices [3]. The known (P and Q)-polynomial association schemes are obtained from regular semi-lattices as below:

(1) Let V be a set of cardinality v and X_i the set of i-subsets of V. Set $L = \bigcup_{i=0}^{d} X_i$ $(d \le [\frac{v}{2}])$ and define $x \le y$ $(x, y \in L)$ if and only if y includes x. $\mathcal{X}(L)$ is the Johnson scheme $J(v, d)$.

(2) Let V be a vector space of dimension v over $GF(q)$ and X_i the set of i-dimensional subspaces of V. Set $L = \bigcup_{i=0}^{d} X_i$ $(d \le [\frac{v}{2}])$ and define $x \le y$ $(x, y \in L)$ if and only if y includes x. $\mathcal{X}(L)$ is the q-analogue of $J(v, d)$.

(3) Let V be a vector space of dimension v over $GF(q)$ equipped with a non-degenerate classical form, i.e., one of alternating, hermitian and quadratic forms. Let X_i be the set of i-dimensional totally isotropic subspaces of V and d the dimension of maximal totally isotropic subspaces. Set $L = \bigcup_{i=0}^{d} X_i$ and define $x \leq y$ $(x, y \in L)$ if and only if y includes x. $\mathcal{X}(L)$ is the association scheme of dual polar spaces.

(4) Let F be a set of cardinality v and X_i the set of mappings $f : I \longrightarrow F$ from i-subsets I of $\{1, 2, \cdots, d\}$ to F. Set $L = \bigcup_{i=0}^{d} X_i$ and define $f \leq g$ $(f, g \in L)$ if and only if g is an extension of f. $\mathcal{X}(L)$ is the Hamming scheme $H(d, v)$.

(5) Let V and W be vector spaces of dimension d and n $(d \leq n)$ over $GF(q)$, respectively. Let X_i be the set of bilinear mappings $f : U \times W \longrightarrow GF(q)$, where U runs through i-dimensional subspaces of V. Set $L = \bigcup_{i=0}^{d} X_i$ and define $f \leq g$ $(f, g \in L)$ if and only if g is an extension of f. $\mathcal{X}(L)$ is the association scheme of bilinear forms.

(6) (a) Let V be a vector space of dimension d over $GF(q^2)$ and X_i the set of sesquilinear mappings $f : U \times V \longrightarrow GF(q^2)$ such that the restriction of f to $U \times U$ is hermitian, where U runs through i-dimensional subspaces of V. Set $L = \bigcup_{i=0}^{d} X_i$ and define $f \leq g$ $(f, g \in L)$ if and only if g is an extension of f. $\mathcal{X}(L)$ is the association scheme of hermitian forms.

(b) Let V be a vector space of dimension n $(d = [\frac{n}{2}])$ over $GF(q)$ and X_i the set of bilinear mappings $f : U \times V \longrightarrow GF(q)$ such that the restriction of f to $U \times U$ is alternating, where U runs through the subspaces of V with $\dim V - \dim U = 2d - 2i$. Set $L = \bigcup_{i=0}^{d} X_i$ and define $f \leq g$ $(f, g \in L)$ if and only if g is an extension of f.

$\mathcal{X}(L)$ is the association schemes of alternating bilinear forms.

(7) Let V be a vector space of dimension $n-1$ ($d=[\frac{n}{2}]$) over $GF(q)$. If q is odd, let X_i be the set of bilinear mappings $f: U\times V \longrightarrow GF(q)$ such that the restriction of f to $U\times U$ is symmetric, where U runs through the subspaces of V with $\dim V - \dim U = 2d-2i$ or $2d-2i-1$. If q is even, let X_i be the set of pairs (f, Q) of bilinear mappings $f: U\times V \longrightarrow GF(q)$ and quadratic forms $Q: U \longrightarrow GF(q)$ such that $f(x,y) = Q(x+y) - Q(x) - Q(y)$ for $x, y \in U$, where U runs through the subspaces of V with $\dim V - \dim U = 2d-2i$ or $2d-2i-1$. Set $L = \overset{d}{\underset{i=0}{\cup}} X_i$ and define $f \le g$ (resp. $(f, Q) \le (g, R)$) if and only if g (resp. g and R) is an extension of f (resp. f and Q). $\mathcal{X}(L)$ is the association scheme of quadratic forms [4].

The regular semi-lattices $L = \overset{d}{\underset{i=0}{\cup}} X_i$ in the above examples (1) - (5) have the following property:

(v) For $x \in X_j$,

$$N_i(j) = \#\{ y \in X_i \mid y \le x \}$$

is independent of the choice of $x \in X_j$. Moreover, for a fixed i, $N_i(d-j)$ is a polynomial of degree i either in j or in q^{-j}.

In fact, let $\binom{n}{r}_q = \prod_{\nu=0}^{r-1} \frac{q^n - q^\nu}{q^r - q^\nu}$. Then

$$N_i(d-j) = \begin{cases} \binom{d-j}{i} & \text{for Examples (1), (4),} \\ \binom{d-j}{i}_q & \text{for Examples (2), (3), (5).} \end{cases}$$

On the other hand, let $Q_i(j)$ be the (j,i) entry of the second eigenmatrix Q of $\mathcal{X}(L)$. In the above examples (1) – (5), $Q_i(j)$ is a polynomial of degree i either in j (Examples (1), (4)) or in q^{-j} (Examples (2), (3), (5)) (see §3.6 [1]). Hence, regarding $N_i(d-y)$ and $Q_i(y)$ as polynomials, Examples (1) – (5) satisfy

(vi) The linear span of $N_0(d-y), N_1(d-y), \cdots, N_t(d-y)$ over $\mathbb{C}$ equals that of $Q_0(y), Q_1(y), \cdots, Q_t(y)$.

<u>Theorem</u> Let $L = \bigcup_{i=0}^{d} X_i$ be a regular semi-lattice satisfying (v) and (vi). For a subset Y of $X = X_d$ and an element z of X_i, let $\lambda_i(z)$ be the number of $y \in Y$ such that $z \le y$. Then Y is a t-design in $\mathcal{X}(L)$ if and only if $\lambda_i(z)$ is independent of the choice of $z \in X_i$ and determined only by i for $0 \le i \le t$.

<u>Proof</u> Let $\mathfrak{a} = (a_0, a_1, \cdots, a_d)$ be the inner distribution of Y:

$$a_j = \frac{1}{|Y|} \# \{ (x,y) \in Y \times Y \mid x \wedge y \in X_{d-j} \}.$$

Counting the number of $(z,x,y) \in X_i \times Y \times Y$ such that $z \le x \wedge y$, we get

$$\sum_{z \in X_i} \lambda_i(z)^2 = \sum_{j=0}^{d} |Y| \, a_j \, N_i(d-j).$$

Counting the number of $(z,y) \in X_i \times Y$ such that $z \le y$, we get

$$\sum_{z \in X_i} \lambda_i(z) = |Y| \, N_i(d).$$

So we have

<u>Lemma</u> Let λ_i be the average of $\lambda_i(z)$, i.e., $\lambda_i = \dfrac{|Y| \, N_i(d)}{|X_i|}$.

Then

$$\sum_{z \in X_i} (\lambda_i(z) - \lambda_i)^2 = |Y| \left\{ \sum_{j=0}^{d} a_j \, N_i(d-j) - \lambda_i \, N_i(d) \right\}.$$

Apply the lemma for X. Then

$$0 = |X| \left\{ \sum_{j=0}^{d} k_j N_i(d-j) - \frac{|X|}{|X_i|} N_i(d)^2 \right\},$$

where k_i is the valency of R_i. So the lemma can be rewritten as

$$\sum_{z \in X_i} (\lambda_i(z) - \lambda_i)^2 = \frac{|Y|}{|X|} \sum_{j=0}^{d} (|X| a_j - |Y| k_j) N_i(d-j).$$

By (vi), the right hand side is zero for $0 \leq i \leq t$ if and only if

$$\sum_{j=0}^{d} (|X| a_j - |Y| k_j) Q_i(j) = 0 \qquad (0 \leq i \leq t).$$

Since $\sum_{j=0}^{d} k_j Q_i(j) = |X| \delta_{i0}$ by $k_j = P_j(0)$ and $PQ = |X| I$, the above identity is equivalent to

$$\sum_{j=0}^{d} a_j Q_i(j) = |Y| \delta_{i0} \qquad (0 \leq i \leq t),$$

which is the definition for Y to be a t-design. Q.E.D.

In Example (6) (a), $N_i(d-j) = \binom{d-j}{i}_{q^2}$ is a polynomial of degree $2i$ in $(-q)^{-j}$ $(q>0)$, while $Q_i(j)$ is a polynomial of degree i in $(-q)^{-j}$. In Example (6) (b), $N_i(d-j) = \binom{2(d-j)}{2i}_q$ or $\binom{2(d-j)+1}{2i+1}_q$, which is a polynomial of degree $2i$ or $2i+1$ in q^{-2j}, while $Q_i(j)$ is a polynomial of degree i in q^{-2j}. These facts imply that t-designs Y in Examples (6) (a) (b) satisfy $\lambda_i(z) = \lambda_i$ for $0 \leq i \leq [\frac{t}{2}]$. In Example (7), $N_i(d-j)$ depends on the choice of $x \in X_{d-j}$.

Finally, I should like to make remarks about the relation between regular semi-lattices $L = \bigcup_{i=0}^{d} X_i$ and certain maximal cliques of $\mathcal{H}(L)$. Let M be a subset of $\{0, 1, \cdots, d\}$ containing 0. A subset Y of X is said to be an <u>M-clique</u> if $Y \times Y \subseteq \bigcup_{i \in M} R_i$. For $z \in X_i$, let $X(z)$ be the set of $x \in X = X_d$ such that $z \leq x$.

Then it seems true that in most of the known regular semi-lattices, $X(z)$ is an M_{d-i}-clique of maximum size, where $M_j = \{0, 1, \cdots, j\}$, and conversely any M_{d-i}-clique of maximum size is $X(z)$ for some $z \in X_i$, establishing a one-to-one correspondence from X_i to the set of M_{d-i}-cliques of maximum size. Among M_j-cliques of maximum size, M_{d-1}-cliques seem essential in the sense that the others are obtained from them in most cases as follows. Let Y and Y' be M_{d-1}-cliques of maximum size. Then $Y \cap Y'$ is an M_{d-2}-clique of maximum size and any M_{d-2}-clique of maximum size is obtained in this manner. Inductively, let Y and Y' be M_j-cliques of maximum size which are contained in an M_{j+1}-clique of maximum size. Then $Y \cap Y'$ is an M_{j-1}-clique of maximum size and any M_{j-1}-clique of maximum size is obtained in this manner.

For the size of M_{d-1}-cliques, there is an upper bound computable by the adjacency matrices. Let $\mathcal{X} = (X, \{R_i\}_{0 \le i \le d})$ be a symmetric association scheme. Let λ_{min} be the minimum eigenvalue of the d-th adjacency matrix A_d of $\mathcal{X}$ and k_d the valency of R_d. Let Y be an M_{d-1}-clique in $\mathcal{X}$. Then it holds that

<u>Lovász Bound</u> [8] $$|Y| \le \frac{|X|}{1 - \frac{k_d}{\lambda_{min}}}.$$

In most of the known (P and Q)-polynomial association schemes, there exist M_{d-1}-cliques which attain the upper bounds, and the upper bounds are given by ${}_2\varphi_1$ (see [11]). The problem of determining maximal M_j-cliques, which has the origin in Erdös-Ko-Rado Theorem [5], is known important to characterize graphs, and I should like to emphasize that it is also important in relation to designs.

References

1. E. Bannai and T. Ito, *Algebraic Combinatorics I*, Benjamin, 1984.

2. P. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Research Reports Supplements, No. 10 (1973).

3. P. Delsarte, *Association schemes and t-designs in regular semilattices*, J. of Combinatorial Theory (A), 20 (1976), 230–243.

4. Y. Egawa, *Association schemes of quadratic forms*, to appear in J. of Combinatorial Theory (A).

5. P. Erdös, Chao Ko and R. Rado, *Intersection theorems for systems of finite sets*, Quart. J. Math. (Oxford), 12 (1961), 313–320.

6. D. Leonard, *Orthogonal polynomials, duality, and association schemes*, SIAM J. Math. Anal. 13 (1982), 656–663.

7. D. Livingstone and A. Wagner, *Transitivity of finite permutation groups on unordered sets*, Math. Z. 90 (1965), 393–403.

8. L. Lovász, *On the Shannon capacity of a graph*, IEEE Trans. Inform. Theory IT-25 (1979), 1–7.

9. A. Munemasa, *A necessary condition for the existence of a perfect e-error-correcting code*, preprint.

10. K. Nomura, *On perfect 1-codes in symmetric groups*, preprint.

11. D. Stanton, *Some Erdös-Ko-Rado theorems for Chevalley groups*, SIAM J. Alg. Disc. Methods 1 (1980), 160–163.

ON RESOLUTIONS IN FINITE GEOMETRIES

Ryoh Fuji-Hara
Institute of Socio Economic Planning
The University of Tsukuba

A <u>resolution</u> R in a finite geometries G is defined to be a partition of the lines into classes $R_1, R_2, \ldots, R_t$ such that each point of G is incident with exactly one line of each class R_i, $1 \leq i \leq t$. It is well known that any affine geometry AG(n,q) has a resolution defined by the equivalence relation of parallelism. We are here interested in another types of resolutions which we call a skew resolution and a strong skew resolution in an affine geometry and also a resolution in a projective geometry. In this paper, we survey these resolutions.

A <u>skew resolution</u> is defined to be a resolution of the lines in AG(n,q) such that no two lines in any class of the resolution are parallel lines. The following is a readily established result concerning skew resolutions.

THEOREM 1. If there exists a resolution of the line in PG(n,q), then there exist a skew resolution in AG(n,q).

The proof of this result can be easily seen by considering the affine geometry which is obtained by deleting a hyperplane from PG(n,q). The resolution in PG(n,q) induces a skew resolution in AG(n,q).

Resolutions are known to exist in the following projective geometries.

(a) PG(2n+1,2), $n \geq 1$ (Baker(1975), Zaitxev,Zinovjev and Semakov(1973)).

(b) PG(n,q), $n=2^i-1$, $i\geq 2$, q a prime power (Beutelspacher(1974)).

These result prove the following theorem.

THEOREM 2. There exist a skew resolution in AG(n,q) for

(a) $n\geq 3$ and odd, and $q=2$

(b) $n=2^i-1$, $i\geq 2$, q a prime power.

In Fuji-Hara and Vanstone (1981), The following two recursive constructions of skew resolutions are shown.

THEOREM 3. If there exist skew resolutions in AG(m,q) and $AG(n,q^m)$, then there exists a skew resolution in AG(mn,q).

THEOREM 4 If there is a skew resolution in AG(m+1,q) and $AG(n,q^m)$, then there exist a skew resolution in AG(mn+1,q).

These construction can be applied in various way to produce new families of skew resolutions. The two recursive constructions along with Theorem 2 are combined to give the next result.

THEOREM 5. For all $i,j\geq 2$, $k\geq 1$, q a prime power, there exist a skew resolutions in AG(n,q) where $n=[(2^i-1)^k-1][2^j-1]+1$.

Using theorem 2 and 5, we can show that, for all prime power q and $n\leq 100$, we can construct a skew resolution in AG(n,q) where n=3,7,9,15,19,21,25,27, 31,39,43,45,49,55,57,61,63,75,79,81,85,87,91,93 and 99. A skew resolution in AG(5,q), except q=2, is still unkown. If this exists, we can construct skew resolutions in affine geometries for all odd dimensions less than 100, except 17. Since we can not obtain a skew resolution by theorem 1 in even dimension, it was a question whether there exists a skew resolution in affine geometry of even dimension or not. But rcently a computer search answered this question.

THEOREM 6. There exists a skew resolution in AG(4,2).

This result gives us many skew resolutions in AG(n,2), n even, but existence of a skew resolution in AG(n,q), n even, q odd, is still a question.

Theorem 6 implies that the converse of theorem 1 is generally false. But it may be able to construct a resolution in PG(n,q) from a skew resolution in AG(n,q) if the skew resolution satisfies some conditions. We now define a skew resolution with conditions. A skew resolution class S of AG(n,q) is called <u>strong</u> if the points of hyperplane H at infinity which are not incident with any line of S are the points of a PG(n-2,q). Denote this space by K(H,S). A <u>strong skew resolution</u> (SSR) of AG(n,q) is a skew resolution of the geometry in which each class is strong and if S and S' are distinct class of the resolution then $K(H,S) \neq K(H,S')$.

We so far have the following results on the existence of strong skew resolutions, Fuji-Hara and Vanstone (1984).

THEOREM 7. Any skew resolution of AG(3,q) is strong.

THEOREM 8. There exists a strong skew resolution in $AG(2^{k+1}-1,q)$ for all $k \geq 1$, q a prime power.

THEOREM 9. If there exists a strong skew resolution in AG(m,q) and a strong skew resolution in $AG(n,q^m)$, then there is a strong skew resolution in AG(mn,q).

A strong skew resolution is not only a important step to construct a resolution of a projective geometry, but also it has an application by itself to statistics, see Gosh and Shah (1983).

We define another line problem in PG(n,q). A set of lines in PG(n,q) is called a t-partition if these lines partition the points of a t-flat (i.e. a PG(t,q) contained in the geometry). The lines of PG(n,q) are said to be <u>t-partitionable</u> if the lines can be partitioned into t-partitions each of which is associated with a distinct t-flat. A necessary condition for the lines of PG(n,q) to be t-partitionable is t odd. We can now state a partial converse to theorem 1.

THEOREM 10. If the lines in PG(n-1,q) are (n-2)-partitionable and there exists a strong skew resolution in AG(n,q), then there exists a resolution in PG(n,q).

The existence question for t-partitionings in PG(n,q) is an open problem. Ofcourse, for special values of t (i.e. t=1 or n) the question is trivially answered. Of most interest presently is the case t=n-1. We have the following results.

THEOREM 11.

(a) PG(4,2) and PG(4,3) are 3-partitionable,

(b) PG(6,2) and PG(6,3) are 5-partitionable,

(c) PG(8,2) is 7-partitionable.

THEOREM 12. PG(2^i,q) is (2^i-1)-partitionable for $i\geq 2$, q a prime power.

The concept of t-partitioning can be extended to balanced incomplete block designs. A (v,k,λ)-BIBD **D** is said to be t-partitionable if each block of **D** can be partitioned into t-subsets such that the resulting collection of blocks forms a (v,t,λ')-BIBD **D'**. **D** and **D'** are also known as <u>nested designs</u>. There are numerous examples of nested designs, but the existence of a nested design with parameters $v=(q^{n+1}-1)/(q-1)$, $k=(q^n-1)/(q-1)$, $\lambda = (q^{n-1}-1)/(q-1)$, $t=q+1$, $\lambda' = 1$ which is equivalent to a (n-1)-partition of PG(n,q) is unknown.

If the lines in PG(2k,q) are (2k-1)-partitionable for all $k\geq 2$ then the theorm 10 would implies the existence of infinitely many new resolution in projective geometris. The smallest unsolved case is a resolution in PG(5,3). If a strong skew resolution exists in PG(5,3) then theorem 10 and 11 produce a resolution of PG(5,3). The next open case is PG(9,3). By theorem 9 a strong skew resolution exists in AG(9,3). Unfortunately, it is not known whether the lines in PG(8,3) are 7-partitionable.

REFERENCES

[1] Baker, R.D., Partitioning the planes of $AG_{2m}(2)$ into 2-designs, Discrete Math. 15 (1976) 205-211

[2] Beutelspacher, A., On parallelisms in finite projective spaces, Geometricae Dedicata 3 (1974) 35-40

[3] Fuji-Hara, R. and Vanstone, S.A., Recursive constructions for skew resolutions in affine geometries, Aequationes Mathmaticae 23 (1981) 242-251

[4] Fuji-Hara, R. and Vanstone, S.A., Affine geometries obtained from projective planes and skew resolutions of AG(3,q), Annals of Discrete Math. 18 (1982)

[5] Fuji-Hara, R. and Vanstone, S.A., Strong skew resolutions and packings with an application, London Journal Math. (submitted)

[6] Fuji-Hara, R. and Vanstone, S.A., Skew resolutions in AG(n,q) and their applications, Utilitas Math (submitted)

[7] Gosh, S. and Shah, K.R., On the optimality of the generalized Room squares, Commun. Statis. -Theor. Meth. 12(18), 2119-2125 (1983)

[8] Zaitsev, G.V.,Zinovjev, V.A. and Semakov, N.V., Interrelations preparate and Hamming codes and extension of Hamming codes to new double-error-correcting codes. In Proc. 2ed Internat. Symp. on Information Theory Tsahkadsor, Armenia 1071 Budapest 1973

二,三の組合せ論的問題について

慶応大学(高) 芳沢光雄

① $\mathbb{D}$を Steiner system $S(t,k,v)$ としたとき、$\mathbb{D}$が block-schematic であるとは、$\mathbb{D}$の blocks の集合$\mathbb{B}$が intersection numbers に関して association scheme をなすときにいいます。すなわち、$0 \leqq {}^\forall h \leqq k$ に対し $|B_1 \cap B_2| = h$ となる $B_1, B_2 \in \mathbb{B}$ があるとき $|\{B \in \mathbb{B} : |B_1 \cap B| = i, |B_2 \cap B| = j\}|$ は B_1, B_2 のとり方によらず i, j, h のみにより定まる $(0 \leqq i, j \leqq k)$。例として $S(2,k,v)$ とか Mathieu 群から作れるいくつかの Steiner systems 等があります。

これについては次のような結果が得られています。

(原見[1]) $S(t,k,v)$ が block-schem. $\Rightarrow v \leqq k^4 \binom{k}{[\frac{k}{2}]}$

(芳沢[10]) 各 $n \geqq 1$ に対し、$k-t=n$ となる block-schem. $S(t,k,v)$ $(t \geqq 3)$ は有限個。

以上の結果をふまえると、各 $t(\geqq 3)$ に対し block-schem. $S(t,k,v)$ はどうなっているか、ということが自然に問題になってきます。それについて最近次のような結果を得ました。

Th. ${}^\forall \varepsilon$ (real) >0 fix。各 $t\left(\frac{2}{\varepsilon}+2\right)$ に対し $v > k^{3+\varepsilon}$ となる block-schem. $S(t,k,v)$ は有限個。又、各 t $(\geqq 3)$ に対し $v < k^{2-\varepsilon}$ となる block-schem. $S(t,k,v)$ も有限個。

さてこの定理の証明では最初に次の Lem. を示した。

Lem. $\mathbb{D}$ を $k \geqq 2(t-1)$ をみたす Steiner system $S(t,k,v)$ とする。ここで $(t,k,v) \neq (4,7,23)$, $(2, n+1, n^2+n+1)$ $(n \geqq 2)$ ならば、

$\exists B_1, B_2, B_3 \in \mathbb{B}$ s.t. $|B_1 \cap B_2| = |B_1 \cap B_3| = t-1$, $|B_2 \cap B_3| = 0$.

定理の証明は、x_i $(i=0,1,\cdots,k)$ を一つの block B と i 点で交わる blocks の個数とすれば、Mendelsohn の結果[6] より x_i は B のとり方によらず、さらに block-schem. 性および Lem. より $x_0 \leqq x_{t-1}^2$ が成立する。この式の両辺をうまく評価して定理の主張が得られた。($\lim_{k \to \infty}(1-\frac{1}{k})^k = \frac{1}{e} > 0$ でぎりぎり救われた所もあった。)

⑪ $Gal_{\mathbb{Q}}(f) = PSL(2,7)$ となる f として $f(x) = x^7 - 154x + 99$ を見つけた Erbach, Fisher, Mckay の研究 [3] の方法は次のようなものであった。

$f(x) = x^7 + ax + b$ $(a, b \in \mathbb{Z})$ とおき次の条件をみたす a, b を探す。

(1) $f(x)$: irred. ($Gal(f)$ の可移性に対応)。
(多分 Eisenstein 型としたと思われる ⑦)

(2) $disc(f)$ = 平方数 ($Gal(f) \leqq A_7$ に対応)。

(3) $f(x)$ は丁度 3 実根もつ ($Gal(f)$ は 3 点 fix の invol. をもつ)。

(4) $\Phi_3(x) =: \prod_{\substack{\{\alpha_1,\alpha_2,\alpha_3\} \subseteq \Omega \\ (*)}} (x-(\alpha_1+\alpha_2+\alpha_3)) \in \mathbb{Z}[x]$ が可約 (fの根の集合)

($\Omega^{(3)}$ の上に $Gal(f)$ は可移でない，すなわち $Gal(f) \cong PSL(2,7)$ に対応)

(4)のような方法が今のところ"$f(x) \rightleftarrows$ ガロア群"の問題を計算機で解くとき大いに役立っている。他にも[9]にも述べられていたが、次のような結果がある。

(Jensen & Yui [4]) $f(x)$: p (prime) 次 irred. $/\mathbb{Q}$，$Gal(f) \neq$ regular gp. のとき，$Gal(f) \cong D_p \iff \Phi_2(x)$ は $\frac{p-1}{2}$ 個の($\mathbb{Q}$上)既約な p 次式の積に分解。

($\Phi_2(x) \in \mathbb{Q}[x]$ は $\Phi_3(x)$ の 3根 $\{\alpha_1,\alpha_2,\alpha_3\}$ を 2根 $\{\alpha_1,\alpha_2\}$ に変えたもの。)

この結果を拡張する形で、Frobenius gp. という立場から考えると、やさしく次のことが最近分かった。

<u>Th.</u> $f(x)$: p次 irred. $/\mathbb{Q}$.　$\Omega = \{\alpha_1, \cdots, \alpha_p\}$: fの根の集合。

$\varphi(x) =: \prod_{1 \leqq i \neq j \leqq p} (x-(\alpha_i - \alpha_j)) \in \mathbb{Q}[x]$ とおくと次のことが成り立つ。

$\varphi(x)$ の根は全て異なり，$\varphi(x)$ は $\frac{p-1}{m}$ 個 $(1 \leqq m \leqq p-1)$ の次数 mp の($\mathbb{Q}$上)既約式の積に分解し、

$m = p-1 \iff Gal(f)$ は 2-trans.，$m=1 \iff Gal(f)$: regular gp.，

$1 < m < p-1 \iff Gal(f)$ は order mp の Frob. gp.

今後の問題として、上に述べた方法で計算機を使って色々と探すこともあろうが、計算機の"速さ"を考えれば、もっといい方法を見つけることが必要と思う。

Ⅲ いわゆる additive number theory として色々と研究されている有限(可換)群における組合せ論的な問題の中で、面白そうな問題を一つ上げてみた。

G：有限アーベル群.

$s=s(G)$：次のような条件(＊)をみたす s の中での最小値。

(＊) 重複を許して、G の任意の s 個の元 $g_1, \cdots, g_s$ に対して、ある $1 \leq i_1 < \cdots < i_t \leq s$ があって、$g_{i_1} g_{i_2} \cdots g_{i_t} = 1$ となる。

問題：$s(G)$ を決めよ。

この問題は元来数論的に、"G を algebraic number field F の class group としたとき、$s(G)$ は F の irred. (algebraic) integer の prime ideals への分解をしたときの、(重複を含めての) prime ideals の最大数" という意味があって、Davenport (1966) により出された。Olson [8] が最初に G が p-群として解き、その後 [5], [2] にあるような研究はあるが、まだ一般には解けてないようである。

Ⅳ $\mathbb{D}$ を $\mathrm{Aut}(\mathbb{D})$ が block 集合上可移な t-design とすると、$\mathrm{Aut}(\mathbb{D})$ は点集合上 $[\frac{t}{2}]$-homogeneous (ほとんど $[\frac{t}{2}]$-trans. と同じ) になるという野田氏の結果 [7] は、単純群分類をふまえた上では、"block-transitive な t-design の研究はほぼ終り" ということも主張できるのである。ところが置換群の上に design がある

ような群については、今のところ分からないことがいくつかある。例えば、

問題：G：(単なる) permutation gp. on Ω.
$\Omega \ni {}^{\forall}\alpha_1, \underset{(\neq)}{\cdots}, {}^{\forall}\alpha_t$ に対し $G_{\alpha_1 \cdots \alpha_t}$ は丁度 k (定数 $> t$) 点 fix する, ($S(t, k, |\Omega|)$ が作れる。) と仮定。
このときの G を決定せよ。

この問題については $t=2$ てすると G は Ω 上可移になることがいえると(私は)思うが、今のところ $G_{\alpha_1 \cdots \alpha_t}$ に何か条件をつけないと結果は出ていません。

References

[1] T. Atsumi ; An extension of Cameron's result on block schematic Steiner systems, J. Comb. Theory Ser. A 27 (1979), 388-391.

[2] R.C. Baker ; Diophantine problems in variables restricted to the values 0 and 1, J. Number Theory 12 (1980), 460-486.

[3] D.W. Erbach, J. Eischer, and J. Mckay ; Polynomials with PSL(2,7) as Galois group, J. Number Theory 11 (1979), 69-75.

[4] C.U. Jensen and N. Yui ; Polynomials with D_p as a Galois group, J. Number Theory 15 (1982), 347-374.

[5] H.B. Mann ; Additive group theory - A progress report, Bull. Amer. Math. Soc. 79 (1973), 1069-1075.

[6] N. S. Mendelsohn; A theorem on Steiner systems, Canad. J. Math. 22 (1970), 1010-1015.

[7] R. Noda; Some inequalities for t-designs, Osaka J. Math. 13 (1976), 361-366.

[8] J. E. Olson; A combinatorial problem on finite abelian groups, I, J. Number Theory 1 (1969) 8-10.

[9] 山崎圭次郎；ガロア群の計算，「群論とその応用の総合的研究」(1981).

[10] M. Yoshizawa; Block intersection numbers of block designs, Osaka J. Math. 18 (1981), 787-799.

Weakly transitive translation plane について

大阪大学 教養部　平峰 豊

§1. Spread と Translation plane

Vを標数 p の有限体 $GF(q)$ 上の $2n$ 次元ベクトル空間とする。Vの n 次元 $GF(q)$-部分空間のある集合 Γ が <u>spread</u> であるとは、次の条件がみたされることをいう。

$$V-\{0\} = \bigcup_{W\in\Gamma} W-\{0\} \quad (\text{ただし disjoint sum とする})$$

従って Γ が spread ならば $|\Gamma| = (q^{2n}-1)/(q^n-1) = q^n+1$ である。

Γ に対応して affine plane が次のように定義される。

点 ： V のベクトル全体

直線 ： 剰余類 $W+w$ $(W\in\Gamma,\ w\in V)$ の全体

Incidence ： 包含関係 "$\in$"

affine plane が、上で定義されたある $\pi(\Gamma)$ と同型であるとき <u>translation plane</u> とよばれる。q^n を $\pi(\Gamma)$ の <u>order</u> という。

$\pi=\pi(\Gamma)$ の点を点に、直線を直線に 1対1 に移す写像が incidence 関係を保つとき <u>自己同型</u> という。π の自己同型全体がつくる群を <u>$\mathrm{Aut}(\pi)$</u> で表す。$\pi=\pi(\Gamma)$ は各 $w\in V$ に対して次のような自己同型 t_w をもつ。

$$t_w : \begin{array}{ccc} V & \longrightarrow & V \\ \Psi & & \Psi \\ v & \longmapsto & v+w \end{array} \quad , \quad \begin{array}{ccc} \bigcup_{W\in\Gamma} V/W & \longrightarrow & \bigcup_{W\in\Gamma} V/W \\ \Psi & & \Psi \\ W+v & \longmapsto & W+v+w \end{array}$$

このとき $T=\{t_w \mid w\in V\}$ は、$\mathrm{Aut}\,\pi$ の正規部分群となり、V上

regular に作用する。T を $\pi(\Gamma)$ の translation group という。$C=(\mathrm{Aut}\,\pi)_0$ とおけば $\mathrm{Aut}\,\pi = T\cdot C$ (semi-direct product) が成りたつことは明らかである。C ($=C(\pi)$) を π の translation complement という。$C(\pi)$ はベクトル 0 を固定するので Γ に含まれる q^n+1 個の部分ベクトル空間の置換を引起す。よく知られているように desarguesian plane や Lüneburg plane ([6] 参照) では $C(\pi)$ が Γ 上 2重可移に作用しており, semifield plane ([2] 参照) では $C(\pi)$ は Γ の q^n 個の上に可移で、残りの 1 個を固定している。

§2. (G,Γ,n,q)-plane

translation plane $\pi(\Gamma)$ に対して その translation complement, $C(\pi)$ が Γ の置換を引起すことは上に述べたが, V. Jha は [3] で 次の性質をもつ translation plane $\pi(\Gamma)$ を考察した。

(*) $C(\pi)$ の部分群 G と Γ の subset Δ が存在して, $|\Delta|=q+1$ で Δ は G-invariant かつ $\Gamma-\Delta$ 上 G は可移。

(*) をみたす plane $\pi(\Gamma)$ を (G,Γ,n,q)-plane といい, $\pi=\pi(G,\Gamma,n,q)$ と表す。

知られている (G,Γ,n,q)-plane には次のものがある。

(1) $V=GF(q^2)\times GF(q^2)$; $GF(q)$-ベクトル空間とみる.

Γ = V を $GF(q^2)$ 上のベクトル空間とみて, 1次元部分空間の全体

$\cup$

$\Delta=\langle(0,1)\rangle \cup \{\langle(1,x)\rangle \mid x\in GF(q)\}$

$G_0=\left\{\begin{pmatrix} a & b\\ 0 & c\end{pmatrix}\in GL(2,q)\right\}\le G\le \Gamma L(2,q)$

この例では $\pi(\Gamma)$ は desarguesian plane of order q^2 に同型で、$(G, \Gamma, 2, q)$-plane になっている。

(2) order q^2 の Hall plane.

これは適当な G と Γ に対して $(G, \Gamma, 2, q)$-plane となることが知られている。

(3) Narayana Rao と Satyanarayana により構成された order 5^{2n} (n は奇数) の translation plane [7]

これも適当な G と Γ に対して $(G, \Gamma, 2, 5^n)$-plane となることが知られている。

(4) $V = GF(q^3) \times GF(q^3)$; $GF(q)$-ベクトル空間とみる.

Γ = V を $GF(q^3)$ 上のベクトル空間とみて, 1次元部分空間の全体

$\overset{\cup}{\Delta} = \langle(0,1)\rangle \cup \{\langle(1,x)\rangle \mid x \in GF(q)\}$

$G_0 \leq G \leq \Gamma L(2, q)$

ただし $G_0 = \{M \in GL(2, q) \mid \det M$ が $GF(q)^*$ の 2-element$\}$

この例では $\pi(\Gamma)$ は desarguesian plane of order q^3 に同型で、$(G, \Gamma, 3, q)$-plane になっている。

(5) Lorimer-Rahilly plane (LR-16) と Johnson-Walker plane (JW-16). ([5])

これは適当な G, Γ に対して $(G, \Gamma, 4, 2)$-plane であることが知られている。

G を適当にとることにより (1)(2)(3)(5) では次が成りたつ。

(α) $O_p(G) \neq 1$.

とくに (1)(2)(3) では次が成りたつ

(α′) $O_p(G)$ は G の p-Sylow群である.

同様に，適当な G を選ぶことにより (2)(3)(5) では次が成りたつ。

(β) G は Δ の少くとも 2元を固定する。(ただし (3) では $n \neq 1$ とする)

$q=p$ (素数) の場合．つまり (G, Γ, n, p)-plane が (α′)(β) をみたすとき この plane は <u>Δ-transitive</u> であるという。また (β) をみたすとき <u>weakly transitive</u> であるという.

[4] において次のことが示されている。

<u>定理</u> (V. Jha) $\pi(\Gamma)$ が Δ-transitive ならば $n=2$，つまり $\pi(\Gamma)$ の order は p^2 である.

(注) Δ-transitive plane は order p^2 の Hall plane だけである と予想されている。また weakly transitive plane は order p^2 の Hall plane と JW-16, LR-16 であろうと 予想されているが．まだ証明されていない。

(注) 先にあげた (G, Γ, n, q)-plane の例 (1)～(5) では "n" の値は $2 \leqq n \leqq 4$ であり．一般に (G, Γ, n, q)-plane に対して このことが正しいのではないかと考えられる。上の Jha の定理 からも そのように類推される。

§3. Weakly transitive translation plane

(G, Γ, n, p)-plane (pは素数) に関して次のことが証明 できた。

定理1（[1]）πが(G,Γ,n,p)-planeならば次のいずれかが成りたつ。

(i) Δの元Aを適当に選べば$O_p(G)$は$\Delta-\{A\}$上semi-regularである。

(ii) $n=2$.

(iii) $n=3$. さらにΔ上のG-orbitの長さは$|\Delta|$又は$\frac{1}{2}|\Delta|$でとくに$p\equiv -1 \pmod 4$のときは長さは$|\Delta|$である。

この定理によりJhaの定理は次のように拡張される。

定理2（[1]）. πがweakly transitiveで$O_p(G)\neq 1$ならば$n=2$ つまりπのorderはp^2である。

（注）LR-16とJW-16は定理1の(i)をみたす例となっている。又(ii)をみたす例としてorder p^2のHall planeの他に§2の例(3)でのべたplaneでorder 5^2 ($n=1$)のものがある。(iii)の例としてはorder 27のdesarguesian planeがあるが、これ以外にないことが確かめられる。

また(iii)の例でorder 27以外のもの，つまり$p\geqq 5$の場合はもし存在すればnon-desarguesian planeであることが容易に分かる。

§4. (G,Γ,n,q)-planeの一般的性質

最後に(G,Γ,n,q)-planeに関する結果を集会では述べることのできなかったことを含めて次に紹介する。

整数 $a, n > 1$ に対して次の条件をみたす整数 $t > 0$ を $a^n - 1$ の <u>a-primitive divisor</u> という。

$$t \mid a^n - 1 \quad , \quad t \nmid a^i - 1 \quad \forall i \in \{1, 2, 3, \cdots, n-1\}$$

次が知られている。

<u>定理</u>（Zsigmondy, [6] p27）次の場合を除いて $a^n - 1$ の prime a-primitive divisor が存在する。

(1) $n = 2$ かつ $a + 1 = 2^r \quad \exists r$

(2) $n = 6$ かつ $a = 2$

この定理を用いて次が示される。 $q = p^m$ とおくとき

<u>補題3</u> 次の場合を除いて $p^{m(n-1)} - 1$ の prime p-primitive divisor が存在する。

(1) $(m, n) = (1, 3), (2, 2)$ かつ p は Merssene prime

(2) $(m, n) = (1, 2)$

(3) $p = 2$ で $(m, n) = (1, 7), (2, 4), (3, 3), (6, 2)$ かつ $O_2(G)$ は ある $A \in \Delta$ に対して $\Delta - \{A\}$ 上 semi-regular.

(G, Γ, n, q)-plane の定義より G は $\Gamma - \Delta$ 上可移であるから．

$|\Gamma - \Delta| = q(q^{n-1} - 1) \mid |G|$ 　とくに $p^{m(n-1)} - 1 \mid |G|$ である。

補題3により (1) (2) (3) を除いて $p^{m(n-1)} - 1$ の prime p-primitive divisor が必ず存在する。これを t とするとき $p^{m(n-1)} - 1 \mid |G|$ より G の t-Sylow 群 R は $R \neq 1$ である。次が示される。

<u>補題4</u> $R \geq X \neq 1$, $O_p(G) \geq Y$, $[X, Y] = 1$ かつ XY がある $A \in \Delta$ を固定すれば．次のいずれかが成りたつ。

(1) $C_A(X) \neq C_A(Y)$ かつ $|C_A(Y)| \geq q^{n-1}$

(2) $n = 2$ かつ ある $B \in \Delta - \{A\}$ に対して $X \leq G_{(B, 0A)}$.

(注) $\pi(\Gamma)$ に対応する射影平面を $\bar{\pi}(\Gamma)$ とするとき $\bar{\pi}(\Gamma)$ の無限遠直線 l_∞ 上の点と Γ とは同一視される。従って補題4(2)の $G(B, OA)$ は B を center とし OA を axis とする G の homology のつくる部分群を意味するものとする。以下では Γ と l_∞ を同一視する。

この補題を用いて次が示される

<u>補題5</u>　$n \neq 2$ とするとき次のいずれかが起る.

(1) $O_p(G)$ は、ある $A \in \Delta$ に対して $\Delta - \{A\}$ 上 semi-regular である.

(2) $n = 3$ かつ R は Δ 上 semi-regular である。

上の補題では $p^{m(n-1)} - 1$ の prime p-primitive divisor の存在を仮定したが、$q^n \equiv -1 \pmod 4$ のときはこの仮定なしで次が示される.

<u>補題6</u>　$q^n \equiv -1 \pmod 4$ のとき S を G の 2-Sylow 群とすれば次が成りたつ

(1) S は dihedral 又は semidihedral で $Z(S)$ は Γ の元をすべて固定する.

(2) $|S| \geq 4(q+1)_2$,　$S_A \simeq 1$ or $Z_2 \times Z_2$　$\forall A \in \Delta$
(ただし $(q+1)_2$ は $q+1$ を割る 2 の最高巾とする)

これらの補題を用いて次の定理を得る。ただし、記号を次のように定める。

$\Phi = p^{m(n-1)} - 1$ の prime p-primitive divisor 全体の集合

$(q+1)_t = q+1$ を割る素数 t の最高巾.

$$\theta(n, q) = \begin{cases} \prod_{t \in \Phi} (q+1)_t & (q \equiv 1 \pmod 4 \text{ のとき}) \\ \prod_{t \in \Phi \cup \{2\}} (q+1)_t & (q \equiv -1 \pmod 4 \text{ のとき}) \end{cases}$$

定理7. π を (G, Γ, n, q)-plane とし $q=p^m$ とする。
次のいずれかが起こる.

(1) ある $A \in \Delta$ に対して $O_p(G)$ は $\Delta-\{A\}$ 上 semi-regular.

(2) $n=2$

(3) $n=3$ かつ q は奇数である。さらに Δ 上の G-orbit の長さはすべて $\theta(3,q)$ で割りきれる。

定理8. π が (G, Γ, n, q)-plane で $q^n \equiv -1 \pmod 4$, かつ $O_p(G) \neq 1$ ならば $n=3$ である.

定理7は定理1の一般化となっている。Jha の定理や定理2の一般化である次の定理が定理7よりただちに得られる.

定理9. π が (G, Γ, n, q)-plane で $O_p(G) \neq 1$ かつ G が Δ の少くとも2点を fix すれば $n=3$ である。

参考文献

[1] Y. Hiramine : On weakly transitive translation planes, to appear

[2] D. R. Hughes and F. C. Piper : Projective Planes, Springer-Verlag, Berlin-Heidelberg-New York, 1973

[3] V. Jha and M. J. Kallaher : On spreads admitting projective linear groups, Canadian J. Math. 33 (1981), 1487-1497.

[4] V. Jha : On Δ-transitive translation planes, Arch. Math. 37(1981), 377–384.

[5] P. Lorimer : A projective plane of order 16, Journal of Combinatorial Theory (A) 16, 334–347 (1974).

[6] H. Lüneburg : Translation planes, Springer-Verlag, Berlin-Heidelberg-New York, 1980

[7] M.L. Narayana Rao and K. Satyanarayana : A new class of square order planes, J. Combin. Theory (A) 35 (1983), 33–42

Quasifields

大阪教育大　大山　豪

n次元$GF(q)$－ベクトル空間$V(n,q)$上の一般線形群$GL(V(n,q))$のq^n-1個の元と0からなる集合Σが，

任意の$\sigma_1, \sigma_2 (\neq) \in \Sigma$に対して，$\sigma_1 - \sigma_2 \in GL(V(n,q))$.

をみたすとき，Σを spread set という。

order q^n の translation plane はすべてこの spread set Σ を用いて，つぎのように$V(2n,q)$の中で構成される。

$V(2n,q) = V(n,q) \oplus V(n,q)$. とおく.

point は $V(2n,q)$のすべての vector (u,v), $u,v \in V(n,q)$

line は $V(\infty) = \{(0,v) \mid v \in V(n,q)\}$；

$V(\sigma) = \{(v, v^{\sigma}) \mid v \in V(n,q)\}$, $\sigma \in \Sigma$

とおくとき，すべての coset $V(2n,q)/V(\infty)$ 及び $V(2n,q)/V(\sigma)$, $\sigma \in \Sigma$.

結合関係は．$V(2n,q)$ の包含関係に従う.

特に，spread set Σ は単位行列を含むとしてよい．又Σの定義より，任意の$u, v \in V(n,q) \setminus \{0\}$に対して，$u^{\sigma} = v$ となるσがΣにただ1つ存在する。

従ってΣにより translation plane が定まり，このΣを用いて2つの演算$+$と$\circ$をもつ order q^n の quasifield Q がつぎのように作られる。

Qは集合として，$V(n,q)$の vector よりなる.

$+$；$V(n,q)$の vector の和

$\circ$；$e(\neq 0) \in V(n,q)$を固定し，$v \in V(n,q)$に対して，$e^{\sigma} = v$である$\sigma \in \Sigma$を$\sigma(v)$とおく．このとき $u \circ v = u^{\sigma(v)}$

ここで quasifield $Q(+,\circ)$ とは

1) $Q(+)$; 可換群

2) $(a+b)\circ c = a\circ c + b\circ c$

3) 任意の $a\in Q$ に対して $a\circ 0 = 0$

4) $a(\neq 0)\in Q$ に対して, $\exists^1 x\in Q$; $a\circ x = c$

5) $a, b, c\in Q$, $a\neq b$ に対して, $\exists^1 x\in Q$; $x\circ a - x\circ b = c$

6) 任意の $a\in Q$ に対して, $\exists 1\in Q\setminus\{0\}$; $1\circ a = a\circ 1 = a$

逆に, order q^n の quasifield より, translation plane が作られるが, 同型でない quasifield より同型な translation plane を作ることはおこる。

以下で order q^n の quasifield を, $GF(q^n)$ の中で構成する方法について述べる。

$$W = \begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \end{pmatrix}$$ を $n\times n$ 行列

$x\in GF(q^n)$ に対して, $x^{(0)} = x$, $x^{(1)} = \bar{x} = x^q$, $x^{(i)} = x^{q^i}$,

$\mathfrak{A} = \{A\in GL(n, q^n) \mid \bar{A} = AW\}$, 但し $A = (a_{ij})$ に対して $\bar{A} = (\overline{a_{ij}})$

とす.

Lemma 1.

(1) 任意の $A_0\in\mathfrak{A}$ により, $\mathfrak{A} = GL(n,q)A_0$

(2) A を $GF(q^n)$ 上の $n\times n$ 行列とする。

$$A\in\mathfrak{A} \iff A = \begin{pmatrix} a_0 & a_0^{(1)} & \cdots & a_0^{(n-1)} \\ a_1 & a_1^{(1)} & \cdots & a_1^{(n-1)} \\ \vdots & \vdots & & \vdots \\ a_{n-1} & a_{n-1}^{(1)} & \cdots & a_{n-1}^{(n-1)} \end{pmatrix}$$

且つ, $\{a_0, a_1, \cdots, a_{n-1}\}$ は $GF(q)$ 上一次独立

証明は，単に行列の計算をすればよい。

いま$V(n,q)$の basis 及び$\mathfrak{A}$の元 A を固定する。

$$V(2n,q)A = V(n,q)A \oplus V(n,q)A$$
$$= \{(uA, vA) \mid u, v \in V(n,q)\}$$

は，$GF(q)$-vector space として$V(n,q)$と同型である。

$v=(x_0, x_1, \cdots, x_{n-1}) \in V(n,q)$ に対して

$$vA = (x, \bar{x}, \cdots, x^{(n-1)}),\quad x = \sum_{i=0}^{n-1} x_i a_i,\quad A = \begin{pmatrix} a_0 & \cdots \\ a_1 & \cdots \\ \vdots & \\ a_{n-1} & \cdots \end{pmatrix}$$

より，$(x, \bar{x}, \cdots, x^{(n-1)}) = ((x))$ とおくと，

加法群として，$GF(q^n)$ と $V(n,q)A$ は，写像 $x \longmapsto ((x))$ により，同型である．この対応において $\widehat{((x))} = x$ とおく．

Lemma 2

Xを$GF(q^n)$上の $n\times n$ 行列とする。

$$\bar{X} = X^W \iff X = \begin{pmatrix} x_0 & x_{n-1}^{(1)} & \cdots & x_1^{(n-1)} \\ x_1 & x_0^{(1)} & \cdots & x_2^{(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ x_{n-1} & x_{n-2}^{(1)} & \cdots & x_0^{(n-1)} \end{pmatrix}$$

この証明も，単に行列の計算による。このときXは第1列によりきまるから

$$X = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix}$$ とも表すことにする。

Lemma 3

$$GL(n,q)^A = \{X \in GL(n,q^n) \mid \bar{X} = X^W\} = \left\{ \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix} \in GL(n,q^n) \right\}$$

証明

$M \in GL(n,q)$ に対して，$\overline{M^A} = M^{\bar{A}} = (M^A)^W$ である。

逆に，$X \in GL(n,q^n)$，$\bar{X} = X^W$ のとき，$\overline{X^{A^{-1}}} = \bar{X}^{\bar{A}^{-1}} = X^{WW^{-1}A^{-1}}$

$= X^{A^{-1}}$ より，$X^{A^{-1}} \in GL(n,q)$ である。

spread set $\Sigma=\{0\}\cup\{M\in GL(n,q)\}$ に対して, $\Sigma^*=\Sigma^A$ とおく。$\forall u, v\in V(n,q)\setminus\{0\}$ に対して, $uM=v$ となるMが唯1つ存在する。したがって $\forall uA, vA\in V(n,q)A-\{0\}$ に対して $uA\cdot M^A=(uM)A$ であるから, $uA\cdot M^A=vA$ となるM^AがΣ^*に唯1つ存在する。

従って $((x))=(x,\bar{x},\cdots,x^{(n-1)})\in V(n,q)A$ に対して, $((1))M^A=((x))$ となるM^Aが唯1つΣ^*に存在する。ここで

$$M^A=\begin{bmatrix}x_0\\x_1\\\vdots\\x_{n-1}\end{bmatrix} とすると, (1,\cdots,1)\begin{bmatrix}x_0\\x_1\\\vdots\\x_{n-1}\end{bmatrix}=(\Sigma x_i,\cdots,\Sigma x_i^{(n-1)})$$

$\Sigma x_i=x$ である。従ってこのM^Aを $M^A=[x]$ とおく。

このとき, 写像 $x\longmapsto M^A=[x]$ により, 全単射 $GF(q^n)\to\Sigma^*$ が定義でき, $\widehat{[x]}=x$ とおく。

以上のことより, 次のようにして spread set が定義される。

$\Sigma^*=\{[x]\mid x\in GF(q^n)\}$ は

(1) $[x]=\begin{bmatrix}x_0\\\vdots\\x_{n-1}\end{bmatrix}\in GL(n,q^n)$, $[0]=\begin{bmatrix}0\\\vdots\\0\end{bmatrix}$, $[1]=\begin{bmatrix}1\\0\\\vdots\\0\end{bmatrix}$

よりなり,

(2) 任意の $x,y(\neq)\in GF(q^n)$ に対して,

$$\det([x]-[y])\neq 0$$

をみたすとき, Σ^*を spread set という。

このΣ^*を用いて, quasifield Q が次のように定義される。

quasifield $Q=Q(n,q^n,\Sigma^*)$ とは

(1) 集合として, $Q=GF(q^n)$

(2) $Q(+)=GF(q^n)(+)$

(3) $x\circ y=\widehat{((x))[y]}=\sum_{i=0}^{n-1}x^{(i)}y_i$, $[y]\in\Sigma^*$

なお quasifield の同型についての Maduram の定理を，つぎのように書くことができる。

定理 (D. M. Maduram)

quasifield $Q_1 = Q(n, q^n, \Sigma_1^*)$, $Q_2 = Q(n, q^n, \Sigma_2^*)$ が同型

$\Longleftrightarrow$ $\exists N \in GL(n, q)^A$, $\exists \theta \in \mathrm{Aut}\, GF(q^n)$; $\Sigma_2^* = \Sigma_1^{*\theta N}$, $((1))N = ((1))$.

spread set の例

(1) 有限体 $GF(q^n)$ は quasifield $Q(n, q^n, \Sigma^*)$, $\Sigma^* = \left\{ [a] = \begin{bmatrix} a \\ 0 \\ \vdots \\ 0 \end{bmatrix} \middle| \; a \in GF(q^n) \right\}$ である。

(2) quasifield $Q(n, q^n, \Sigma^*)$ において，$\sigma(a) : x \mapsto (x \circ a) \cdot a^{-1}$ (但し・は $GF(q^n)$ における積) が $GF(q^n)$ の同型のとき，Q を generalized André quasifield という。このとき Q は次の様に Σ^* により定義される。

$k \in GF(q)$ に対して，$k \circ a = ((k))\widehat{[a]} = \sum k a_i = k \sum a_i = ka$

$\therefore$ $(k \circ a) a^{-1} = k$ 　従って $\sigma(a) \in \mathrm{Aut}_{GF(q)} GF(q^n)$

$\therefore$ $(x \circ a) a^{-1} = x^{q^{\rho(a)}} = x^{(\rho(a))}$

$\therefore$ $x \circ a = x^{(\rho(a))} a$

一方 $x \circ a = \sum x^{(i)} a_i$ であるから，上の式を用いて

$a_0 x + a_1 x^{(1)} + \cdots + (a_{\rho(a)} - a) x^{(\rho(a))} + \cdots + a_{n-1} x^{(n-1)} = 0$

がすべての $x \in GF(q^n)$ に対して成立する。

$\therefore$ $a_{\rho(a)} = a$, $a_i = 0$ $(i \neq \rho(a))$

$\therefore$ $[a] = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ a \\ 0 \\ \vdots \\ 0 \end{bmatrix} \cdots \rho(a)+1$

以上より

$$\Sigma^* = \left\{ [a] = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ a \\ 0 \\ \vdots \\ 0 \end{bmatrix} \middle| \begin{array}{l} a \in GF(q^n),\ a, b\ (\neq 0) \text{ に対して} \\ \det([a] - [b]) \neq 0 \end{array} \right\}$$

○Examples （大阪教育大学 松本誠）

例として，Hall quasifield の spread set による特徴づけを述べる．以下では次の記号を用いる．

$$\mathfrak{M}=\left\{\begin{bmatrix}\alpha\\ \beta\end{bmatrix};\alpha,\beta\in GF(q^2)\right\}(\cong M_2(q))\quad \text{ただし，}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{pmatrix}\alpha & \bar{\beta}\\ \beta & \bar{\alpha}\end{pmatrix}$$

$\mathfrak{G}=\mathfrak{M}\cap GL(2,q^2)\ (\cong GL(2,q))$

$\mathfrak{M}\supset\Sigma$: spread set (s.t. $|\Sigma|=q^2$, $\Sigma\ni O, I$) について

$Q(\Sigma)$: Σ より構成される位数 q^2 の quasifield，つまり

$Q(\Sigma)(+)=GF(q^2)(+)$，

乗法は，$\alpha\circ\beta=\alpha\beta_1+\bar{\alpha}\beta_2$ (if $\beta=\beta_1+\beta_2$, $\begin{bmatrix}\beta_1\\ \beta_2\end{bmatrix}\in\Sigma$)

Q: quasifield のとき，$k(Q)$: kernel of Q

定義：[Trans. Am. Math. Soc. 54, 229 ~ 277 (1943)]

$\left.\begin{array}{l}Q(+,\circ)\text{: quasifield s.t. } |Q|=q^2,\ k(Q)\supseteq GF(q)\\ f(x)=x^2-ax-b: GF(q)\text{-既約多項式}\end{array}\right\}$ について

Q: Hall quasifield w.r.t. $f(x)$

$\underset{def.}{\Longleftrightarrow}$ i) $Q\ni\alpha$, $k(Q)\ni k\Rightarrow\alpha\circ k=k\circ\alpha$

ii) $Q\setminus k(Q)\ni\alpha\Rightarrow f(\alpha)=0$

Hall quasifield は次のように特徴づけできる．

Q: 位数 q^2 の Hall quasifield w.r.t. $f(x)$

$\Longleftrightarrow$ $\mathfrak{M}\supset\Sigma$: spread set ($|\Sigma|=q^2$, $\Sigma\ni O, I$)

s.t. i)′ $\Sigma\supset\mathfrak{Z}(\mathfrak{G})$

ii)′ $f(\eta)=0$ (at $GF(q^2)$) なる η について

$\Sigma\setminus(\mathfrak{Z}(\mathfrak{G})\cup\{0\})$ は $\begin{bmatrix}\eta\\ 0\end{bmatrix}$ を含む $\mathfrak{G}$-共役類．

について，$Q\cong Q(\Sigma)$

証明
$\mathfrak{M} \supset \Sigma$ について $Q(\Sigma)$ が i), ii) をみたせば i)′, ii)′ をみたすことを示す. i)′ は容易.
ii)′ を示すには, $\mathcal{G} \ni X, Y$ について

$$\mathrm{trace}\,X = \mathrm{trace}\,Y,\ \det X = \det Y \iff X, Y : \mathcal{G}\text{-共役}$$

に注意する. 以下では $q>2$ とする. ($q=2$ の場合は明らか)
$\Sigma \setminus (\mathfrak{Z}(\mathcal{G})) \ni \begin{bmatrix}\alpha_1\\ \alpha_2\end{bmatrix}$ とすれば, $\alpha_1+\alpha_2 \in Q(\Sigma)\setminus k(Q(\Sigma))$
$\because\ \alpha_1+\alpha_2 \in k(Q(\Sigma)) \Rightarrow GF(q) \subsetneq k(Q(\Sigma)) \Rightarrow Q(\Sigma)$: 体 → 矛盾.
従って, $f(\alpha_1+\alpha_2)=0$. $Q(\Sigma)$ の乗法の定義から これは

$$\alpha_1^2+\alpha_1\alpha_2+\bar{\alpha}_1\alpha_2+\alpha_2\bar{\alpha}_2 - a(\alpha_1+\alpha_2)-b=0$$

$$\therefore\ (\alpha_1+\bar{\alpha}_1-a)(\alpha_1+\alpha_2)-b-\alpha_1\bar{\alpha}_1+\alpha_2\bar{\alpha}_2=0$$

$$\left.\begin{array}{l}\alpha_1+\alpha_2 \in GF(q^2)\setminus GF(q),\\ \alpha_1+\bar{\alpha}_1-a,\ b+\alpha_1\bar{\alpha}_1-\alpha_2\bar{\alpha}_2 \in GF(q)\end{array}\right\}\text{より}\ \left\{\begin{array}{l}\alpha_1+\bar{\alpha}_1=a\\ \alpha_1\bar{\alpha}_1-\alpha_2\bar{\alpha}_2=-b\end{array}\right.$$

$$\therefore\ \mathrm{trace}\begin{bmatrix}\alpha_1\\ \alpha_2\end{bmatrix}=a=\mathrm{trace}\begin{bmatrix}\eta\\ 0\end{bmatrix},\ \det\begin{bmatrix}\alpha_1\\ \alpha_2\end{bmatrix}=-b=\det\begin{bmatrix}\eta\\ 0\end{bmatrix}$$

$\begin{bmatrix}\eta\\ 0\end{bmatrix}^{\mathcal{G}} \cup \mathfrak{Z}(\mathcal{G}) \cup \{0\}$ は実際に spread set の条件をみたす.
$\Leftarrow$ は直接確められる.

証終

一般に, $Q(\Sigma)$ $(\Sigma \subset \mathfrak{M})$ が上の条件 i) をみたせば

$$\Sigma \supset \mathfrak{Z}(\mathcal{G}),\ \Sigma\setminus(\mathfrak{Z}(\mathcal{G})\cup\{0\}) \subset \bigcup_{\eta\in GF(q^2)\setminus GF(q)} \begin{bmatrix}\eta\\ 0\end{bmatrix}^{\mathcal{G}}$$

例えば $q=5^r$ (r: 奇数) について $\lambda\in GF(q^2)$ s.t. $\lambda^2+2\lambda-2=0$,
$M(b)=\begin{bmatrix}1-(b^2-1)(\lambda-2)\\ (b^2-1)(\lambda-2)\end{bmatrix} \in \mathcal{H}=\left\{\begin{bmatrix}\alpha\\ \beta\end{bmatrix}\in\mathcal{G};\ \alpha+\beta=1\right\}$ $(b\in GF(q)^*)$,
$\mathcal{L}$: 5-Sylow subgrp. of $\mathcal{H}$ とすると,

$$\Sigma=\mathfrak{Z}(\mathcal{G})\cup\{0\}\cup\bigcup_{b\in GF(q)^*}\begin{bmatrix}b^{-1}\lambda\\ 0\end{bmatrix}^{M(b)\mathcal{L}}$$

は Rao plane (を座標づける quasifield) の spread set である. [J. of Combinatorial Theory (A) 35, 33~42 (1983)]

23, 27のアダマールデザインについて

愛媛大　理　木村浩
愛媛大　教育　大森博之

2−(27, 13, 6) デザインで3個のブロックの共通元の個数は高々5である事は容易にわかりますが、今、それが5である場合のデザインを計算機を用いて構成する事を考えます。

1. 条件を満すデザインは一般性を失う事なく下図のように配置出来ますが点の集合を下記のように名称づけます。

$$\begin{array}{llcccccccc}
 & & \overbrace{1\cdots5}^{X} & \overset{B}{6} & \overset{C}{7} & \overset{D}{8} & \overbrace{9\cdots14}^{F} & \overbrace{15\cdots20}^{G} & \overbrace{21\cdots26}^{H} & \overset{E}{27} \\
\text{ブロック} & 1 & |\cdots| & | & | & & |\cdots| & & & \\
〃 & 2 & |\cdots| & | & & | & & |\cdots| & & \\
〃 & 3 & |\cdots| & & | & | & & & |\cdots| &
\end{array}$$

ここで行番号はブロックを列番号は点を表わします。

2. 第4番目のブロックの候補者を決めるのに X, B, C, D, E, F, G, H 部分からそれぞれ x, b, c, d, e, f, g, h 個の点をとるとします。このとき関係式

$$x+b+c+d+e+f+g=13$$

$$x+b+c+f=6,\quad x+b+d+g=6,\quad x+c+d+h=6$$

を得ますが これより $2x+b+c+d=5+e$ が成立します。

3．上の関係式より非負整数解として以下の解の組が得られます。

$$\begin{aligned}(x,b,c,d,e,f,g,h) &= (3,0,0,0,1,3,3,3)\\ &= (2,0,0,1,0,4,3,3)\\ &= (2,0,1,0,0,3,4,3)\\ &= (2,0,1,1,1,3,3,2)\\ &= (2,1,0,0,0,3,3,4)\\ &= (2,1,0,1,1,3,2,3)\\ &= (2,1,1,0,1,2,3,3)\\ &= (1,1,1,1,0,3,3,3)\end{aligned}$$

上の解の組を持つブロックを上から順に type1 ～ type8 と名付けます。

4．デザインの第4番目以降のブロックを決定するのに，type 1 ～ type 8 のブロックがそれぞれ何個あるかを決定する必要があります。そこで type1 ～ type8 のブロックの個数をそれぞれ $a_1 \sim a_8$ とします。このとき X 部分から

$$5\times 3+3a_1+2(a_2+\cdots+a_7)+a_1=5\times 13$$
$$a_1+\cdots+a_8=24,\quad 3\cdot{}_5C_2+a_1\cdot{}_3C_2+(a_2+\cdots+a_7)=6\cdot{}_5C_2$$

なる関係式が得られ これより $a_1=4,\ a_2+\cdots+a_7=18,\ a_8=2$ がわかります。

更に B,C,D 部に注目して

$a_2+\cdots+a_7=18$, $a_2+a_5+a_6+4=13$, $a_3+a_5+a_7+4=13$, $a_4+a_6+a_7+4=13$

より $a_2=a_7$, $a_3=a_6$, $a_4=a_5$ がわかります。

又 B,C 部分から $a_7+3=6$ ∴ $a_7=3$, 同様にして C,D 部分より $a_4=3$, A,C 部分より $a_6=3$ がわかります。

5。以上の事を踏まえ

(イ) type 1 の4個のブロックを第4番目〜第7番目のブロックにもってくる事にし、その時の配置の名称を下図のようにします。

	X		F	G	H
ブロック 4 〜 ブロック 7	X*		F*	G*	H*

この時、同型なデザインを除く為 行及び列の置換を適当に行う事により X* は17個、F*, G*, H* はそれぞれ 328個の pattern に分類出来る事がわかります。(別表A はその一部を記したものです。)

(ロ) (イ)で求めた pattern の組合せのうち、第8番目以降のブロックが決定出来るのは 1033通りである事がわかりますが、同型なものを除くと 430通りの組合せがある事がわかります。(別表B はその一部を記したものです。)

(ハ) (ロ)で求めた430通りの各々について type 8の2個のブロックを決定し、それを才8番目、才9番目のブロックとします。ここでも(見掛け上)同型でない才8番目、才9番目のブロックの候補者がたくさんありますが、その各々の場合について、才10番目次降のブロックを次々と決定していきます。例えば別表Bの(*)の場合で、才1番目から才9番目までのブロックを固定した場合、才10番目から才27番目までのブロックの決定の仕方は968通りあります。つまり(*)の場合のデザインが968個出来る事になります。

6。 最終的には、(ロ)の430通りの各々の場合について求めたものが、我々の条件を満す27－アダマールデザインのすべてですが、この中には同型なものが含まれていると思われます。これは一つのデザインには、ブロック会合数が5である3個のブロックの組は、一般的には、たくさんあり、その各々の組について 1。～5。の手順を施こす事により、(ロ)の430通りの組合せのうちのどれかになる事によります。

7。 そこで、我々の作ったこれらのデザインを分類する問題が出て来ますが、数万個、数十万個のデザインを分類する事は至難です。

しかし，アダマール デザインという特殊性に注目し，構成したデザインをアダマール行列にし，そのアダマール行列で分類する事が考えられますが，現在の所まだ完成はしていません。尚，位数28のアダマール行列H，素数Pに対し $P \mid |Aut(H)|$ とすると $P = 2, 3, 7, 13$ であり，$|Aut(H)|$ が7，13で割り切れる場合のアダマール行列の分類がTonchevによってなされています。

8。所で2つのデザインの同型を，計算機を用いて，わりと容易に判別出来る方法として点及びブロックごとに，その内部構造，外部構造のブロック交合数を同時に調べる事です。例えば伊藤昇氏に送っていただいた75通りの2-(23,11,5)デザインのうち，dual designとして同型なものが14対，判定不明なものが2対，残りすべてが同型でない事がわかりました。この方法の欠点は，デザインの自己同型群の位数が高い場合のように思われます。

（別表A）

X^*のパターン

① ---- ⑩	⑪ ---- ⑰ (⑪)	⑰
1 2 3	1 2 3	1 2 3
1 4 5	3 4 5	2 4 5
1 4 5	3 4 5	2 3 4
1 2 3	1 2 3	1 4 5

F^*, G^*, H^* のパターン

① -----, ⑫⑥ ⑫⑦ ------ ③②⑧

⑫⑥	⑫⑦	③②⑧
1 2 3	1 2 3	1 2 3
1 2 4	1 2 4	4 5 6
3 4 5	3 4 5	4 5 6
1 4 6	3 4 6	4 5 6

（別表 B）

① (10, 127, 154, 313)
② (10, 127, 256, 289)
③ (10, 128, 154, 311)
⋮
④③⓪ (17, 163, 256, 257)

ここで (i, j, k, l) とすると、iは X^*のパターンのi番目を、j, k, lは F^*, G^*, H^*のパターンのそれぞれの番号を示す。又 j番目のパターンに出て来る数字に8, k番目には14, l番目には20をそれぞれ加えた数字がそれぞれブロックをなす点の番号となる。

参考文献

1. T.D. Tonchev "Hadamard Matrices of Order 28 with Automorphisms of order 13" To appear
2. T.D. Tonchev "Hadamard Matrices of order 28 with Automorphisms of Order 7" To appear