《科学研究費補助金(総合研究Ａ)研究集会報告集》

代数的組合せ論
報告集

1986年11月12日～14日

於　愛媛大学理学部

はしがき

この報告書は、1986年11月12日より3日間愛媛大学理学部で開かれた「代数的組合せ論」研究集合の講演記録である。

代数的組合せ論の研究集会は、第1回が1983年に岡山大学、第2回が1985年に大阪市立大学文化交流センターで開かれ、今回が第3回である。

この研究集会では、この報告集でみられるように、研究成果の発表とともに、符号理論、アダマール行列、射影平面、グラフ等についての紹介もおこなわれた。

この集会のプログラム、準備等は主として木村浩氏によりなされた。また会場を提供し、色々と御援助下さった愛媛大学理学部数学教室の方々に感謝の意を表したい。

尚この集会の費用は、科学研究費総合研究A（代表者　白谷克巳）によった。この集会のために色々御尽力頂いた白谷克巳氏にもお礼の言葉を申し述べたい。

1986年12月10日

大山　豪

目　　次

Code理論について

伊藤昇（甲南大理）

1° まえがき

Code理論は日本では主として数学以外の人達によって研究されてきているように見えます。それはそれで理由があるのでしょうが，数学の人達との交流がもっとよかったらと思うのは私だけでしょうか。有名なReed-Muller codeなど，日本で発見されながら逆輸入の形をとって発展したことなども，よくある話のひとつかも知れません。ともかくCode理論の歴史はまだ新らしいので魅力ある問題がいまでも沢山あります。こんなことを思い浮べながらこの話をすることを引受けたのでした。

2° Codeとは

Codeとは有限体$GF(q)$上のベクトル空間$V=\{(a_1,\cdots,a_n),\ a_i\in GF(q),\ 1\leq i\leq n\}$の部分集合のことです。その部分集合が部分空間$C$であるとき$C$はlinearと呼ばれますが，ここではそのようなものに限定します。$q=2$のときCはbinaryと呼ばれますが，ここではそのときに限定します。しかし理

論上からは GF(4) 上のものを考えることも必要になるでしょう。数学的には代数的数体上のベクトル空間で必要な理論を展開しておいて，素イデアルを法としておとすということも考えられていますが，それもまだ充分にまされているとはいえません。

3° Code の特性

V には通常の内積：$a=(a_1,\cdots,a_n)$，$b=(b_1,\cdots,b_n)$ について $a\cdot b=\sum_{1\le i\le n} a_i b_i$ がありますが，code というときには Hamming 距離；$d(a,b)=\#\text{of } i\text{'s};\ a_i\neq b_i$ を考えにいれます。これにより V は距離空間に入ります。また 0 ベクトルからの距離 $d(0,a)=wt(a)$ を a の重さといいます。さらに $d(C)=\min_{0\neq a\in C} wt(a)$ を C の最小重さといいます。$k(C)=\dim C$ とおくとき，$k(C)$ $d(C)$ がともに大きな C を求めるというのが code 理論の基本的問題のひとつです。このとき $C^{\perp}=\{a\in V;\ a\cdot C=0\}$ を C の双対といいますが，C とともに $C^{\perp}$ を考察することは数学の常とよ手段でしょう。つぎに $x\in V$ について $wt(C+x)=\min_{a\in C} d(a,x)$，$t(C)=\max_{x\in V}\min_{a\in C} d(a,x)$ とおいて $t(C)$ を C の coveri

n を radius と呼びます。$k(C)$, $t(C)$ がともに小さな C を求めるということも code 理論の基本的問題のひとつです。そのさい n はある与えられた範囲を動くと考えるべきでしょう。

Code は応用と直接結びついているため有名な code 達はみな好みに構成されています。そのためもっと一般的な定理があってしかるべきだと思われるところがいろいろあるように思います。

4° Code の群

代数と直接関連している部分は沢山ありますが，そのひとつは C の自己同型群です　とくに 23 次元の Mathieu 群と Golay code との結びつきは今では誰もが知っていることでしょう。C の自己同型群は

$$\mathrm{Aut}\,C = \{\sigma \in \mathrm{Sym}\,n \;;\; C\sigma = C \;:\; \text{ただし } (a_1, \cdots, a_i, \cdots, a_n)\sigma = (a_{1\sigma}, \cdots, a_{i\sigma}, \cdots, a_{n\sigma})\}$$

で定義されます。$\mathrm{Aut}\,C$ が大きいということは C に対称性，美しさ，が沢山あると考えられます。実際 C に n-サイクルがあるとき C は cyclic と呼ばれますが，そのとき $V = \dfrac{GF(2)[x]}{(1+x^n)}$，ただし n は奇数とするのが普通です，と見ると C は V のイデアルとなって，

一般論が展開されています。といっても $d(C)$, $t(C)$ に深く立入ることは出来ていません。

5° 文献

最近はCovering radiusについてのものが沢山あります。そこからcode理論に入るというのも良いと思います。若い方に期待しています。

(1) Covering radius - survey and recent results

Cohen, Karpousky, Mattson, Shatz

IEEE IT 31 (1985) 328-343

(2) On the covering radies of codes

Graham, Sloane

IT 31 (1985) 385-401

(3) Furthen results on the covering radius of codes

Cohen, Lobstein, Sloane

IT 32 (1986) 680-694

(4) On the covering radius of cyclic linear codes and arithmetic codes

Helleseth

Discrete Applied Math 11 (1985) 157-173

Hadamard 行列に関する二三の話題

東京女子大文理　山本幸一

Hadamard 行列の研究は大別して，構成の問題と分類の問題に分けることができる．

構成の問題は，Hadamard 行列の無限系列を作り出す原理を探索することに帰着するが，それらのいくつかの原理が，研究者によって次次に提示されてきている．

分類の問題は，Hadamard 行列の同値類を決定することで，与えられた次数の Hadamard 行列の同値性の判定が一つの先決問題になる．そこにはまた何らかの不変量が必要になり，しかも比較的簡単に計算できるものが望ましい．

今回はこの二つの方向で，注目すべき結果を紹介することにする．

§1. 構成の問題

n次の $(1,-1)$-行列 x, y について，それらが正規行列で，互に交換可能であると仮定する．すなわち

$$xx^* = x^*x,\quad yy^* = y^*y,$$

$$xy = yx.$$

このとき $2n$ 次の $(1,-1)$-行列

$$H = \begin{pmatrix} x & y \\ -y^* & x^* \end{pmatrix}$$

は

$$HH^* = \begin{pmatrix} xx^* + yy^* & 0 \\ 0 & xx^* + yy^* \end{pmatrix}$$

を満足するから，この外にもおノルム関係式

$$xx^* + yy^* = 2nI$$

が成立てば，H は $2n$ 次 Hadamard 行列となる

たとえば A, B, C, D が n次 $(1,-1)$-巡回行列（または多重巡回行列：以下同様）で，A, B, C, D は対称行列，

$$x = \begin{pmatrix} A & B \\ -B & A \end{pmatrix},\quad y = \begin{pmatrix} C & D \\ -D & C \end{pmatrix}$$

とすれば，

$$H=\begin{pmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{pmatrix}$$

で，ノルム関係式

$$A^2+B^2+C^2+D^2=4nI$$

ならば，H は 4n次 Williamson型 Hadamard 行列となる

また A，B，C，D が巡回行列で，R は基本的逆巡回行列，

$$\mathfrak{X}=\begin{pmatrix} A & B \\ -B^* & A^* \end{pmatrix},\quad \mathfrak{Y}=\begin{pmatrix} C & DR \\ -DR & C \end{pmatrix}$$

とおけば

$$H=\begin{pmatrix} A & B & C & DR \\ -B^* & A^* & -DR & C \\ -C^* & DR & A^* & -B \\ -DR & -C^* & B^* & A^* \end{pmatrix}$$

で，ノルム関係式

(1) $$AA^*+BB^*+CC^*+DD^*=4nI$$

ならば，H は 4n 次 Hadamard 行列になる．これは，Goethal-Seidel 型 Hadamard 行列の一つの表現である．

事実これの左右から $\mathrm{diag}\{I, R, R, I\}$ を掛けると普通見なれている Goethals-Seidel 行列になる.

ルム関係式の代りに C-行列の条件式

(2) $\quad AA^* + BB^* + CC^* + DD^* = 4(n+1)I - 4J$

および, A, B, C, D の行和に関する条件が満足されれば, H に幅 4 の「縁取り」をつけて $4(n+1)$ 次の Hadamard 行列ができる.

この原理と, 整数論的な手法とを用いて山田 [1] は,

定理. $q = 8k+1$ が素数冪で, $4k$ 次の Hadamard 行列が存在すれば, $4q$ 次の Hadamard 行列が構成できる.

を証明した.

$n \leq 10000$ で存在が未確認の次数 $4n$ のうち, 39 個にこの定理で決着がつく.

しかし, それよりも定理の formulation が, Hadamard 行列の拡大 (dilatation) を示唆するので, 将来の構成問題に対して一つの道を開くものといえよう. 拡大は, 他には T 行列を用いる方向もあるが, ラテン方陣の先蹤から見て, こちらの方により広い拡張が約束されているように思われる.

§2. 分類の問題

ここでは Hall ベクトル不変量について述べる.

$4n$ 次 Hadamard 行列 $H=(a_{ij})_{i,j=1,2,\cdots,4n}$ において, 添数集合 $\{1,2,\cdots,4n\}$ から取った 4 点部分集合 $I=\{i_1,i_2,i_3,i_4\}$ について

$$N(I)=\sum_{k=1}^{4n} a_{i_1k}a_{i_2k}a_{i_3k}a_{i_4k}$$

とおき $N(I)$ が $4m$ になる 4 点部分集合の個数

$$\#\{I;\ N(I)=4m\}=C_m$$

とおいて

$$\begin{cases} D_m=C_m+C_{n-m} & (m\neq\frac{n}{2}) \\ D_{\frac{n}{2}}=C_{\frac{n}{2}} \end{cases}$$

を定義すれば, これらは Hadamard 行列の不変量である.

$$\alpha=(D_0,D_1,\cdots,D_{\frac{n}{2}})$$

を Hall のベクトル不変量という.

なお Hadamard 行列の成分 -1 は凡て 0 でおきかえた行列を, しばらく (a_{ij}) と書いて,

$$N(I)=\sum_{k=1}^{4n}\left((a_{i_1k}+a_{i_2k}+a_{i_3k}+a_{i_4k})\bmod 2\right)$$

として $C_m=\{I;\ N(I)=4m\}$, D_m を上と同様に定義しても, $\alpha=(D_0,D_1,\cdots,D_{\frac{n}{2}})$ は Hadamard 行列の不変量

である. つまりベクトル

$$\alpha=(D_0, D_1, \cdots, D_{\frac{n}{2}})$$

の成分が1つでも違う二つの Hadamard 行列は Hadamard 非同値である.

しかし今上のベクトル不変量が同一であったとするならば, 次のように細分をする

任意の行 i_0 を固定し, $\{1, 2, \cdots, 4n\}-\{i_0\}$ の3要部分集合 $J=\{i_1, i_2, i_3\}$ について

$$C_{i_0}(m)=\#\{J;\ N(i_0, i_1, i_2, i_3)=4m\},$$

$$D_{i_0}(m)=C_{i_0}(m)+C_{i_0}(n-m)$$

とおく. このとき $4n$ 個のベクトル

$$\alpha_0=(D_0(0), D_0(1), D_0(2), \cdots, D_0\left(\tfrac{n}{2}\right)),$$

$$\alpha_1=(D_1(0), D_1(1), D_1(2), \cdots, D_1\left(\tfrac{n}{2}\right)),$$

$$\cdots\cdots$$

$$\alpha_{4n}=(D_{4n}(0), D_{4n}(1), D_{4n}(2), \cdots, D_{4n}\left(\tfrac{n}{2}\right))$$

は, 全体として, すなわち行の入れかえを除いて, 一定になる.

したがって, ベクトルの集合

$$\{\alpha_0, \alpha_1, \cdots, \alpha_{4n}\}$$

が全体として一致するのでなければ Hadamard 行列は非同値である.

この判定条件をパスしたものについては, 2点部分集合 $I_0=\{i_0, i_1\}$ を固定して $\{1, 2, \cdots, 4n\}-I_0$ のすべての2点部分集合 K について

$$C_{I_0}(m) = \#\{K;\ N(I_0 \cup K) = 4m\}$$

とおき,

$$D_{I_0}(m) = C_{I_0}(m) + C_{I_0}(n-m)$$

とおくと, $\binom{4n}{2}$ 個のベクトル

$$\alpha_{0,1} = \left(D_{0,1}(0),\ D_{0,1}(1),\ \cdots\cdots,\ D_{0,1}\left(\frac{n}{2}\right)\right),$$

$$\alpha_{0,2} = \left(D_{0,2}(0),\ D_{0,2}(1),\ \cdots,\ D_{0,2}\left(\frac{n}{2}\right),\right.$$

$$\cdots\cdots$$

$$\alpha_{4n-1,4n} = \left(D_{4n-1,4n}(0),\ D_{4n-1,4n}(1),\ \cdots,\ D_{4n-1,4n}\left(\frac{n}{2}\right)\right)$$

は全体として不変である. すなわち

$$\alpha_{i_0,i_1} = \alpha_{p(i_0),p(i_1)}, \qquad P=\begin{pmatrix}1 & 2 & \cdots & 4n\\ p(1) & p(2) & \cdots & p(4n)\end{pmatrix}$$

ならしめる $\{1, 2, \cdots, 4n\}$ の置換 P が存在するのでなければ, 対応する Hadamard 行列は非同値である

この段階の判定法をパスしたものについては, さらに3点部分集合を取って, 同様のベクトル不変量を考える

ことにする.

$4n=28, 36, 44$ の Goethals-Seidel 型 Hadamard 行列の分類にこの判定法を適用する. (36次のものは, 基礎群が Z_9 と $Z_3 \times Z_3$ に分ける.) そのために計算したベクトル不変量は, もともと同値であると認められるもの, すなわち, 対応する群の自己同型で移り得るもの, 以外は凡て相異ることが分った.

§3. Z_4^s 上の差集合

$v=2^m$ の正規非自明ブロックデザインでは, $v=2^{2s}$, $k=2^{s-1}(2^s-1)$, $\lambda=2^{s-1}(2^{s-1}-1)$ となることが Mann によって知られる. またアーベル群上の差集合に関しては, このパラメーターを持つ差集合が存在するためには, 基礎にあるアーベル群の指数 (exponent) は 2^{s+1} 以下であることが, 筆者の論文 (Pacific Journ. 1963) から分る.

基礎の群が Z_4^s の場合. Z_4 上に s 次拡大環 $\mathfrak{R}=Z_4(\xi)$ を作って, $\mathfrak{R}$ の加法群上で考える. ここに ξ は Z_2 上 s 次原始多項式の係数を Z_4 でおきかえたものの根で, $\xi^{2^s-1}=1$ なるものとしておく.

このとき $\mathfrak{R}$ の正則元全体の乗法群 $\mathfrak{R}^*$ の指数 (index)

2の部分群は上掲のパラメータを持つ差集合の例となる(山田).

なら $\mathbb{Z}_v^*/\{\pm 1\}$ の coset 2^{s-1} の合併集合について, 必ずしも群でなくても, 差集合となるものがあることを, $s=3$, $v=64$; $s=4$, $v=256$ の場合に確められている.

64次では19個(うち群は7個, 非群は12個)あり, 256次では195個(うち群は15個, 非群が180個)ある.

64次の場合12の非群は, 自己同型, 平行移動で互いに移りうるが, 群である7個は3類に落ちるだけである. §2の意味のベクトル不変量は, 群の表わす3類では同一で, 非群の不変量とは相異る. したがって64次の場合, 非同値差集合が少くとも2個存在する.

差集合では, 対応するHadamard行列の行に, もとの群が可移に作用するから, 第2行以下によるベクトル不変数の数値を次に示す.

	D(0)	D(1)	D(2)	D(3)	D(4)	D(5)	D(6)	D(7)	D(8)
群	35	0	0	0	672	0	7168	0	31836
非群	0	0	0	0	42	280	4984	18536	15869

参考

[1] 山田美枝子. 一般四元数型配列の応用から得られる新しい Hadamard 行列の系列. 本報告集.

Goethals - Seidel型Hadamard行列

足利工大　喜安善市
名工大　　澤出和江

1. はしがき

Hadamard行列の構成上，一般によく知られている代表的な型には，Paley型，Williamson型，Goethals-Seidel型がある．

Williamson型については，Turyn達によって随分と研究されてきた．しかし，Goethals-Seidel型Hadamard行列については，多少複雑なことなどからあまり研究されていなかった．

本稿では，このGoethals-Seidel型Hadamard行列の簡単で体系的な発見法を述べる。更に，この型のHadamard同値類は透明な状況にあることを指摘し，また4·7，4·11，4·67等の比較的低次数の場合の計算と検討結果とについてもふれる．

2. 用語の定義

定義2.1.　　$h \times h$ $(1,-1)$-直交行列をh次Hadamard行列(略

して，H-行列）と定義する．

定義2.2.　H-行列 H_1, H_2 の中，一方の行や列に符号付き置換を施すと他方に等しくなるとき，H_1 と H_2 はHadamard同値であるといい，$H_1 \sim H_2$ と書く．

定義2.3.　あるH-行列 H_1 に対して，$\mathbb{K}=\{H \mid H \sim H_1\}$ を H_1 のHadamard同値類（略して，H-同値類）という．

定義2.4.　n 次巡回(1,-1)-行列 A, B, C, D が

$$AA^T + BB^T + CC^T + DD^T = 4nI_n$$

を満たすとき，A, B, C, D をGoethals-Seidel行列（略して，GS行列）と定義する．

定義2.5.　GS行列 A, B, C, D と n 次の逆巡回行列 R とから作った行列

$$H=\begin{bmatrix} A & BR & CR & DR \\ -BR & A & -DR & RC \\ -CR & RD & A & -RB \\ -DR & -RC & RB & A \end{bmatrix}$$

をGoethals-Seidel型Hadamard行列（略して，GS型H-行列）という．ただし．

$$R=(r_{ij});\ r_{ij}=\begin{cases} 1, & i+j \equiv 0 \pmod{n} \text{ のとき} \\ 0, & \text{上記以外のとき．} \end{cases}$$

上で定義した行列 H は，$HH^T = 4nI_{4n}$ なるH-行列の条件を自動的に満足させている．

定義2.6.　GS型H-行列Hに対して，H^T, H^*, H^{*T} の3つをそれぞれGS型H-行列Hのひとつのmateと定義する．ただし，

$$H^* = GS^*(A,B,C,D) = \begin{bmatrix} A & BR & CR & DR \\ -BR & A & RD & -RC \\ -CR & -RD & A & RB \\ -DR & RC & -RB & A \end{bmatrix}.$$

定義2.7.　Hのmate関係による類をmate類(略して，family)といい，このfamilyに属する2つの元は互いにmateであるという．

4個の行列(A,B,C,D)がGS行列であれば，次節に述べるようにしてこれらから多数のGS行列が新しく導かれる．これらの新しい行列をもとのGS行列の誘導GS行列という．

3．誘導GS行列とGS型H-行列familyとの関係．

以下で述べるように，1組のGS行列から多数のGS行列が誘導される．これらの誘導GS型H-行列とfamilyの元であるH行列との間のH-同値関係を論じる．まず，記号の説明から始める．

G：位数nの有限アーベル群

A,B,C,D：G上で定義されたn次GS行列

ε：行列A,B,C,Dを要素とする4次の置換

$\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$：A,B,C,Dにそれぞれこの順序に+1または−1スカラー倍する演算子．

$\mu=\varepsilon\cdot S$：行列 A, B, C, D の符号付き置換

τ_i $(i=1,2,3,4)$：A, B, C, D のそれぞれにこの順序に施す転置または恒等置換かのいずれかを示す記号．

θ：群 G の translate．　　σ：群 G の automorphism．

以上で定義した操作を (A, B, C, D) に施して得られた GS型H-行列はもとの H の mate と同値関係にある．これらは次の4命題にまとめられる．

命題3.1. (1) $GS(A,B,C,D)^{\mu}$

$$\sim\begin{cases} GS(A,B,C,D) & \operatorname{sgn}\mu=\operatorname{sgn}\varepsilon\cdot\prod_{i=1}^{4}S_i=1 \text{ のとき} \\ GS^{*}(A,B,C,D) & \operatorname{sgn}\mu=-1 \text{ のとき}. \end{cases}$$

(2) $GS(A^{\tau_1}, B^{\tau_2}, C^{\tau_3}, D^{\tau_4})$

$$\sim\begin{cases} GS(A,B,C,D) & \text{偶数個の } \tau_i \text{ が転置操作} \\ GS^{*T}(A,B,C,D) & \text{奇数個の } \tau_i \text{ が転置操作}. \end{cases}$$

(3) G の位数 n を奇数に限定した場合，$0\leqq h_i<n$, $i=1,2,3,4$ に対して，$GS(\theta^{h_1}(A), \theta^{h_2}(B), \theta^{h_3}(C), \theta^{h_4}(D)) \sim GS(A,B,C,D)$．

(4) $GS(A^{\sigma}, B^{\sigma}, C^{\sigma}, D^{\sigma}) \sim GS(A,B,C,D)$．

証明略．

命題3.1から同じ family の mate 相互間の H-同値について得られた結果は以下のようである．

命題3.2.　対称型行列を巡回置換によって対称行列に変換可能なものと定義する．GS行列の中，少なくとも1つが対称型行列ならば

$$H \sim H^{*T}.$$

命題3.3. 命題3.1の演算を組み合せて，GS行列の中，少なくとも1対の相等しいものが得られるならば

$$H \sim H^{*}.$$

命題3.4. 上の2条件を共有するならば

$$H \sim H^{*} \sim H^{T} \sim H^{*T}.$$

4. 4-complementary sequence と runの分布

H-行列，GS行列など (1,-1)-行列(ベクトルを含む)において，1を0，-1を1としたものをそれらの2進形という．2進形ではGF(2)上の元として扱かう．この節では次のような記号を使う．

p：奇素数	F_G： F上Gの群環
$n = p^s$	r： GF(n)の原始根
$m = \frac{1}{2}(n-1)$	$\oplus$： F_G上の2進和演算子
$G = GF(n)^+$	σ： Gのautomorphism
$F = \mathbb{Z}_2$	θ_h： Gのh-translate

w： F_Gの要素のweight，s.t. $\forall a = \sum_{g \in G} \alpha_g g \in F_G$ に対して

$$w(a) = \#\{g \in G \mid \alpha_g = 1\}.$$

定義4.1. $a, b, c, d \in F_G$ 及び $\forall h \in G - \{0\}$ に対して

$$w(a \oplus \theta_h(a)) + w(b \oplus \theta_h(b)) + w(c \oplus \theta_h(c)) + w(d \oplus \theta_h(d)) = 2n$$

を満たすとき，a, b, c, d をG上の4-complementary sequenceと定義する．

定義 4.2.　2進ベクトルにおいて，連続項が(複)巡回的に同じ数であるとき，その連続項をrun，0のrunの個数をこのベクトルのrunの数という．

定義 4.3.　$\forall a \in F_G$ および $0 \leqslant t < m$ に対して

$$\chi_t = \frac{1}{2} w(a^{\sigma^t} \oplus \theta_1(a^{\sigma^t}))$$

とおいた時

$$\chi = (\chi_0, \chi_1, \ldots, \chi_{m-1})$$

をaのrunベクトルと定義する．(χ_tはa^{σ^t}のrunの数である．)

$\mathcal{Y}$, $\mathcal{Z}$, $\mathcal{V}$ も定義 4.3 と同様にそれぞれこの順に b, c, d の run ベクトルとする．

定理 4.4.　4-complementary sequence (a, b, c, d) が存在すれば，対応する(複)巡回行列 (A, B, C, D) は GS 行列であり，この逆も成立する．

証明略．

定理 4.5.　$a, b, c, d \in F_G$ が G 上の 4-complementary sequence である為の必要十分条件は

$$\chi + \mathcal{Y} + \mathcal{Z} + \mathcal{V} = n\mathcal{E}, \qquad \mathcal{E} = (1, 1, \ldots, 1)$$

である．

証明略．

H-行列の次数 n が 4平方和であらわされたとき，これに対応する GS

行列をすべて求める方法は種々考案されているが，H-同値であるものを予め除外することが重要である．これには第3節の処論によってfamilyの代表元を求めて行けばよい．ここではK-complementary sequenceとrunの方法を採用する．

実際にrunの概念を適用して，4·67次skew型のHadamard行列を比較的短時間の計算で，数多く発見することが出来た．これによってrunの概念がH-行列の構成に非常に有効であることが実証された．例えば，$67 \equiv 1 \pmod 3$より，GF(67)の22乗剰余類に注目して，$4 \cdot 67 = 13^2+7^2+1^2+1^2$に対応するGoethals-Seidel型かつskew型のものを見つけた．4·67次のskew型H-行列は，これまで未発見のものである．その1つは次のようである．ここでは2進ベクトルa, b, c, dをあらわすのに，その成分が1である座標（C_iを使用）で代用した．

$C_i = (2^i, 2^{22+i}, 2^{44+i} \pmod{67}) \quad (i=0,1,\ldots,21)$

$a = (C_0, C_3, C_5, C_9, C_{13}, C_{14}, C_{16}, C_{17}, C_{18})$

$b = (C_1, C_3, C_4, C_5, C_6, C_8, C_9, C_{17}, C_{20}, C_{21})$

$c = (C_1, C_3, C_6, C_9, C_{11}, C_{13}, C_{14}, C_{16}, C_{18}, C_{20})$

$d = (C_1, C_3, C_5, C_7, C_9, C_{11}, C_{13}, C_{15}, C_{17}, C_{19}, C_{21})$

x = (17, 17, 16, 16, 17, 16, 16, 16, 16, 17, 16)

y = (16, 16, 16, 16, 16, 16, 18, 17, 17, 18, 17)

z = (17, 17, 16, 16, 17, 18, 16, 17, 17, 15, 17)

$\mathbf{v} = (17, 17, 17, 17, 17, 17, 17, 17, 17, 17, 17)$

5. 4·7 と 4·11 次の GS型 H-行列の同値類について

Hadamard同値判定基準は幾つかある．ここでは，特性数と広義の Hall set の濃度分布を利用した．後者の方は，木村浩教授らの研究の一部と同等と思われる．

まず，$h\,(=4n)$ 次 Hadamard 行列 H に対する 2進形を M とする．M の相異なる4行を $\mathbf{h}_i, \mathbf{h}_j, \mathbf{h}_k, \mathbf{h}_\ell$ と書く．いま，$1 \leqq i < j < k < \ell \leqq h$ として

$$\mu(i,j,k,\ell) = \min\left\{\frac{1}{4}\cdot w(\mathbf{h}_i \oplus \mathbf{h}_j \oplus \mathbf{h}_k \oplus \mathbf{h}_\ell),\ n - \frac{1}{4}\cdot w(\mathbf{h}_i \oplus \mathbf{h}_j \oplus \mathbf{h}_k \oplus \mathbf{h}_\ell)\right\}$$

とおく．この μ を使って次のものを定義する．

定義 5.1.　$\mu = \min_{(i,j,k,\ell)} \mu(i,j,k,\ell)$

を H の特性数という．

定義 5.2.　$\zeta_t = \#\{(i,j,k,\ell) \mid \mu(i,j,k,\ell) = t\}$，$0 \leqq t \leqq [\frac{n}{2}]$

に対し，$\sum_{0\leqq t\leqq [\frac{n}{2}]} \zeta_t = \binom{h}{4}$ より，

$$\left\{\zeta_t \mid t = 0, 1, \ldots, [\tfrac{n}{2}]-1\right\}$$

を広義の Hall set の cardinality sequence (略して car. seq.) という．

定理 5.3.　2つの h 次 Hadamard 行列が H-同値ならば，次の2つが成立する．

(1)　2つの行列の特性数は等しい．

(2) 2つの行列の car. seq. も等しい.

前節の結果を利用して，4·7次及び4·11次のGS型H-行列の具体的な形をすべてもとめることが出来たので，定理5.3の対偶を使ってH-同値性を調査した結果，4·7次では6個，4·11次では114個のGS型H-行列が得られ，それらすべて互いにH-非同値(すなわちfamily相互間はH-非同値で，family内では命題3.2と3.3とによるもの以外は非同値)であることがわかった．詳細は別に発表する．

6. むすび

今まで述べたことによって，GS型H-行列の性質が明らかになった．また，GS型に関する限り，runの概念によってそのH-同値類の同定が極めて簡単になった．また4·7および4·11次のGS型の場合のH-同値類の個数を6，114と確定した．なお今後の課題には次のようなものがある．

(1) $4\cdot p^s$次のGS型H-行列に対しては，命題3.2及び3.3の逆が成立すると予想している．この予想は，同値類の決定に極めて有効である．

(2) 伊藤昇教授は，私信で，我々が計算した114個の4·11次GS型H-行列の中の2つは，その自己同型群が自明なものに限られることを指摘された．これに触発されて未発表

の方法で調べた結果，このようなものが 114個のうち，上記のものを入れて 76個あると予想している．この方法の一般化．

(3) GS行列 A, B, C, D を巡回行列以外の高さ一様な行列に拡張すること．

(4) GS行列は T-行列から求める方法もある．これに run の概念を適用すること．

謝辞： この研究について，山本幸一，伊藤昇の両教授，榎本彰衛助教授から多大の御教示を受けた．厚く御礼申し上げます．

文　献

[1] A.V. Geramita and J. Seberry, Orthogonal designs, Lecture Notes in Pure and Applied Mathematics, vol. 45, Dekker, 1979.

[2] 喜安善市，アダマール行列とその応用，電子通信学会，1980．

[3] 喜安善市，符号論序説，情報科学講座 A. 2.8，共立出版，1984．

[4] W.D. Wallis, Anne Penfold Street and Jennifer Seberry Wallis, Combinatorics: Room squares, sum-free sets, Hadamard matrices. Lecture Notes in Math., vol. 292, Springer, New York, 1972.

一般四元数型配列の応用から得られる新しいHadamard行列の系列

東京女子大・文理　山田美枝子

1 序.

本稿の目的は次の定理を証明することである。

定理1　$q \equiv 1 \pmod 8$ が素数中で $\frac{q-1}{2}$ 次Hadamard行列が存在するならば $4q$ 次Hadamard行列が構成できる。

定理2　$q \equiv 5 \pmod 8$ が素数中で $\frac{q+3}{2}$ 次skew-Hadamard行列が存在するならば $4(q+2)$ 次Hadamard行列が構成できる。

定理3　$q \equiv 1 \pmod 8$ が素数中で $\frac{q+3}{2}$ 次対称C行列が存在するならば $4(q+2)$ 次Hadamard行列が構成できる。

定理2、定理3は喜安[3]によりすでに証明されている(未発表)。特に $\frac{q+3}{2}$ が素数中であるとすると喜安[2]の定理9.18になる。喜安はKSW形行列を使って証明したが、こ

ここでは一般四元数型配列の応用と考えられる配列と相対的Gaussの和を使ってこれらの定理を証明する。

$4n = 40000$ 次までの未知のHadamard行列の表[1]のうち次の新しい次数が上記の定理から得られた。

▶定理1から得られる新しい次数

n : 233,809,953,1193,1889,2393,2417,2441,2729,2953,3209,
3593,3617,3881,4049,4217,4721,4889,5657,5849,6073,6089,
6113,6257,6449,6473,6569,6977,7177,7417,7433,7753,7793,
8297,8369,8609,8713,8761,9833.

▶定理2から得られる新しい次数

n : 103,127,151,655,879,1231,1951,1999,2239,2271,2559,2799,
2839,2959,3039,3183,3583,3679,4359,4735,4863,4911,5079,
5311,5503,5815,5983,6199,6639,7519,8119,8223,8679,9279,
9631,9903.

▶定理3から得られる新しい次数

n : 579,2019,3043,4443,6339,7419,8523,9819.

—— は喜安[2]定理9.18から得られる次数

よく使う記号を先にまとめておく。

q : 素数中、$F = GF(q)$: q 個の元からなる有限体、

$K = GF(q^t)$: F の t 次拡大、$t \geq 2$, $K^\times, F^\times$: K, F の乗法群、

S_K : K からのトレース、 S_F : F からのトレース、

$S_{K/F}$ ：KからFへの相対トレース、 ζ：$K^{\times}$の生成元、

A^{*}：行列Aの転置行列、 $\otimes$ ：行列のテンサー積、

I_m：m次単位行列、 J_m：成分がすべて1のm次正方行列、 $J_m(x) = 1 + x + \cdots + x^{m-1}$.

2 一般四元数型配列の応用

一般四元数型配列の応用を使った次の定理がある。

定理4　4次正方行列L, M, Nを次のように定義する。

$$L = \begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}, \quad M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}, \quad K = -\frac{1}{2}LM.$$

これらは4次Hadamard行列であることに注意する。

Hを4n次正方行列

$$H = \begin{pmatrix} A & B & C & D \\ -B^{*} & A^{*} & -D^{*} & C^{*} \\ -C^{*} & D & A^{*} & -B \\ -D^{*} & -C & B^{*} & A \end{pmatrix}$$

で、成分行列A, B, C, Dが次を満足するとする。

(1) A, B, C, Dは成分が1か-1のn次正規行列.

(2) $AB = BA$, $AC = CA$, $AD = DA^{*}$, $BC = C^{*}B$, $BD^{*} = DB^{*}$, $CD = DC$,

$A^{*}B = BA^{*}$, $A^{*}D^{*} = D^{*}A$, $CB = BC^{*}$, $B^{*}D = D^{*}B$, $C^{*}D = DC^{*}$.

(3) $AA^* + BB^* + CC^* + DD^* = 4(n+1)I_n - 4J_n$.

(4) $Ae = 2e$, $Be = Ce = De = 0$. ただし e は成分がすべて1の n 次列ベクトル.

このとき

$$N = \begin{pmatrix} 1 \otimes L & e^* \otimes K \\ e \otimes M^* & H \end{pmatrix}$$

は $4(n+1)$ 次 Hadamard 行列となる。

(証明) 条件(1)-(4)を使って NN^* を計算する.

成分行列 A, B, C, D が巡回行列である場合は、行列 H は四元数環をさらに四元数拡大した環のある元の右正則表現になる.([6]参照)。その意味から行列 H は一般四元数型配列の応用と考えられる。

3 有限体の相対的 Gauss の和

有限体の Gauss の和と相対的 Gauss の和を定義する。

<u>定義</u> χ を F の指標、$\zeta_p = e^{2\pi i/p}$ とする。Gauss の和 $\tau_F(\chi)$ は

$$\tau_F(\chi) = \sum_{\alpha \in F} \chi(\alpha) \zeta_p^{S_F \alpha}$$

で定義される。

$\chi=1$、単位指標のとき、$\tau_F(\chi)=-1$ である。$\chi\neq 1$ ならば $\tau_F(\chi)\overline{\tau_F(\chi)}=q$ である。χ が K の単位指標でないとき、

$$\vartheta_{K/F}(\chi)=\frac{\tau_K(\chi)}{\tau_F(\chi)}$$

を<u>χ に付随する相対的 Gauss の和</u>という。

相対的 Gauss の和に関する次の定理は重要である。

<u>定理5</u>　$\chi=\chi_K$ を K の指標、χ_F を χ を F に制限したときの指標とする。$\mathfrak{L}$ を次のような $K^\times/F^\times$ の完全代表系とする。

$$\mathfrak{L}=\mathfrak{L}_0+\mathfrak{L}_1\ ;\ \mathfrak{L}_0=\{\beta : S_{K/F}\beta=0\},\ \mathfrak{L}_1=\{\beta : S_{K/F}\beta=1\}.$$

このとき

$$\sum_{\beta\in\mathfrak{L}_1}\chi(\beta)=\begin{cases}\sum_{\beta\in\mathfrak{L}}\chi(S_{K/F}\beta)\chi(\beta)=\vartheta_{K/F}(\beta) & (\chi_F\neq 1\text{ のとき}),\\ -\frac{1}{q}\tau_K(\chi) & (\chi_F=1,\ \chi_K\neq 1\text{ のとき}),\\ q^{t-1} & (\chi_K=1\text{ のとき}).\end{cases}$$

である。

(証明) [7], [8]参照.

4 補助定理(その1)

以後 $t=2$、すなわち有限体の2次拡大をとり扱う。

χ を K の指標、$\chi(\xi)=\zeta_{q-1}$ で ζ_{q-1} は 1 の原始 $q-1$ 乗根とする。

$$\chi\left(\frac{S_{K/F}\xi^m}{2\xi^m}\right)=\zeta_{q-1}^{z_m} \qquad m\not\equiv\frac{q+1}{2}\pmod{q+1}$$

で z_m を定義する。さらに多項式 $f(x)$ を

$$f(x)\equiv\sum_{\substack{m=0\\ m\not\equiv\frac{q+1}{2}}}^{q} x^{z_m} \pmod{x^{q-1}-1}$$

で定義する。次の補助定理が成りたつ。

<u>補助定理1</u> (1) $f(x)$ は x^{z_m} を $x^0=1$ を除いて丁度2個含む。

(2) $f(x)f(x^{-1})\equiv q+(q+1)J_{q-1}(x)-J_{(q-1)/2}(x^2) \pmod{x^{q-1}-1}$.

(証明) 定理5を使って証明する。詳細は[6]参照。

<u>補助定理2</u> $f(x)\equiv f_0(x^2)+xf_1(x^2) \pmod{x^{q-1}-1}$ とおく。

$f_0(x^2)$ と $f_1(x^2)$ の x^2 を x でおきかえて多項式

$$\varphi_0(x)\equiv f_0(x)-J_{(q-1)/2}(x) \pmod{x^{(q-1)/2}-1},$$

$$\varphi_1(x)\equiv f_1(x)-J_{(q-1)/2}(x) \pmod{x^{(q-1)/2}-1},$$

を定義する。このとき次が成りたつ。

$$\varphi_0(x)\varphi_0(x^{-1})+\varphi_1(x)\varphi_1(x^{-1})\equiv q-2J_{(q-1)/2}(x) \pmod{x^{(q-1)/2}-1}.$$

(証明) 補助定理1から求まる。詳細は[6]参照。

5 補助定理（その2）

$q \equiv 1 \pmod 4$、$n = \frac{q+1}{2}$、i を1の原始4乗根、ψ を F の平方剰余指標とする。多項式 $g(x)$ を次で定義する。

$$g(x) \equiv \sum_{m=0}^{q} \psi(S_{K/F}\xi^m) i^m x^m \pmod{x^n - 1}.$$

n が奇数であることから変数変換をして $g(x)$ は

$$g(x) \equiv \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^{4m}) x^m + i^n \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^{4m+n}) x^m \pmod{x^n - 1}$$

と書くことができる。そこで多項式

$$\alpha(x) \equiv \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^{4m}) x^m \pmod{x^n - 1},$$

$$\beta(x) \equiv \sum_{m=0}^{n-1} \psi(S_{K/F}\xi^{4m+n}) x^m \pmod{x^n - 1}$$

を定義すると $g(x) \equiv \alpha(x) + i^n \beta(x) \pmod{x^n - 1}$ で、$\alpha(x)$, $\beta(x)$ は次のような性質をもつ。

<u>補助定理3</u> (1) $\alpha(x^{-1}) \equiv \alpha(x)$, $\beta(x^{-1}) \equiv \beta(x) \pmod{x^n - 1}$.

(2) $\alpha(x)\alpha(x^{-1}) + \beta(x)\beta(x^{-1}) \equiv q \pmod{x^n - 1}$.

(証明) 定理5を使って証明する。詳細は[7]参照.

6 定理1の証明の概略

補助定理2における多項式 $\varphi_0(x)$、$\varphi_1(x)$ を使って行列 A, B を次のように定義する。

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varphi_0(T) + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I_{(q-1)/2},$$

$$B = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \varphi_1(T),$$

とする。ただしTは $\frac{q-1}{2}$ 次基本巡回行列.

次に $\frac{q-1}{2}$ 次Hadamard行列 H_0 が存在するので H_0 を使って行列C、Dを定義する。

$$C = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes H_0,$$

$$D = C \quad \text{あるいは} \quad D = C^*.$$

A, B, C, Dが定理4の条件(1)-(4)を満たすことを示す。

- 条件(1)は明らか.
- 条件(2). 行列 $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ と $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ の積が0になることから

$$BC = C^*B,\ CB = BC^*,\ BD^* = DB^*,\ B^*D = D^*B$$

はすべて0になり成りたつ。$D = C$ あるいは $D = C^*$ なので

$$CD = DC,\quad C^*D = DC^*$$

は明らか. $\varphi_0(T)$, $\varphi_1(T)$ が巡回行列であることから

$$AB = BA,\quad A^*B = BA^*$$

が成りたつ. さらに

$$AC = CA = A^*C = CA^* = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes H_0,$$

$$AC^* = C^*A = A^*C^* = C^*A^* = 2\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes H_0^*$$

から

$$AC = CA,\quad AD = DA^*,\quad A^*D^* = D^*A$$

を得る。

• 条件(3). 補助定理2から

$$AA^*+BB^*+CC^*+DD^* = 2\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes\varphi_0(T)\varphi_0(T^{-1}) + 2\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes I_{(q-1)/2}$$
$$+2\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes\varphi_1(T)\varphi_1(T^{-1})+4\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes H_0H_0^*$$
$$= 2\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes(qI_{(q-1)/2}-J_{(q-1)/2})+2\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes I_{(q-1)/2}$$
$$+2\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes(q-1)I_{(q-1)/2}$$
$$= 4qI_{q-1}-4J_{q-1}$$

が求まる。

• 条件(4) m が偶数(奇数)のとき Z_m も偶数(奇数)なので

$$f_0(1)=\frac{q+1}{2},\quad f_1(1)=\frac{q-1}{2},$$
$$\varphi_0(1)=f_0(1)-\frac{q-1}{2}=1,\quad \varphi_1(1)=f_1(1)-\frac{q-1}{2}=0.$$

である。従って $\mathbf{e}$ を成分が1の $q-1$ 次列ベクトルとすると

$$A\mathbf{e}=2\mathbf{e},\quad B\mathbf{e}=0$$

を得る。定義から

$$C\mathbf{e}=D\mathbf{e}=0$$

である。

以上から定理4を使って $4q$ 次Hadamard行列が構成できる。

7 定理2. 定理3の証明の概略

補助定理3の多項式 $\alpha(x)$, $\beta(x)$ を使って行列 A, B を次

のように定義する。

$$A=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes\beta(T)+\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes I_{(g+1)/2},$$

$$B=\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes\alpha(T).$$

ただし T は $\frac{g+1}{2}$ 次基本巡回行列.

次に、定理2では $\frac{g+3}{2}$ 次skew-Hadamard行列 Q が存在し Q を次のように変形する。

$$Q=\begin{pmatrix}1&\mathbf{e}^*\\-\mathbf{e}&S+I_{(g+1)/2}\end{pmatrix}.$$

ただし $\mathbf{e}$ は成分がすべて1の $\frac{g+1}{2}$ 次列ベクトル. Q が skew-Hadamard行列であることから

$$S\mathbf{e}=0,\quad SS^*=\frac{g+1}{2}I_{(g+1)/2}-J_{(g+1)/2}$$

が成りたつ。S を使って行列 C, D を次のように定義する.

$$C=\begin{pmatrix}1&1\\1&1\end{pmatrix}\otimes S+\begin{pmatrix}1&-1\\-1&1\end{pmatrix}\otimes I_{(g+1)/2},$$

$$D=C\quad\text{あるいは}\quad D=C^*.$$

定理3では $\frac{g+3}{2}$ 次対称C行列 R が存在し、R を同じように変形する。

$$R=\begin{pmatrix}0&\mathbf{e}^*\\\mathbf{e}&U\end{pmatrix}.$$

U についても同様に

$$U\mathbf{e}=0,\quad UU^*=\frac{g+1}{2}I_{(g+1)/2}-J_{(g+1)/2}$$

が成りたつ。行列C、Dを定理2と同様に

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes U + \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes I_{(g+1)/2},$$

$$D = C \quad \text{あるいは} \quad D = C^*.$$

で定義する。こうして定義されたA, B, C, Dが定理4の条件(1)-(4)を満たすことから定理2、定理3が証明される。

参考文献

[1] A.V.Geramita & J.Seberry, Orthogonal designs, Lecture Notes in Pure and Applied Math. 45, Marcel Dekker, New York-Basel, 1979.

[2] Z.Kiyasu, An Hadamard matrix and its applications, Denshi-Tsushin Gakkai, Tokyo, 1980 (in Japanese).

[3] Z.Kiyasu, private communication.

[4] E.Spence, Hadamard matrices from relative difference sets, J. Comb. Theory (A) 19 (1975), 287-300.

[5] A.L.Whiteman, Hadamard matrices of order 4(2p+1), J. Number Thoery 8 (1976), 1-11.

[6] M.Yamada, Hadamard matrices generated by an adaptation of generalized quaternion type array, Graphs and Combinatorics 2 (1986), 179-187.

[7] K.Yamamoto & M.Yamada, Williamson Hadamard matrices and Gauss sums, J. Math. Soc. Japan 37 (1985), 703-717.

[8] K.Yamamoto, On congruences arising from relative Gauss sums, in:Number Theory and Combinatorics Japan 1984, 423-446, World Scientific Publ., Singapore, 1985.

アダマール行列と code 理論

長崎大・教養　小関 道夫(Ozeki Michio)

§1　Introduction

アダマール行列について

± 1 のみを係数に持つ n 次の正方行列 H が

$$H^{t}H = nI_n \qquad (I_n \text{ は単位行列})$$

をみたすとき、n 次の Hadamard 行列という。

以後 $n \equiv 0 \pmod 4$ の場合に話を限定する。

2つの n 次のアダマール行列 H_1, H_2 は

(i) H_1 のある行(又は列)に -1 を掛ける。

(ii) H_1 のある2つの行(又は列)をとり換える。

及び (i), (ii) の操作の何回かの結合によって H_1 から H_2 が得られるとき、H_1 と H_2 とは H-equivalent であるという。(アダマール行列には他にもいくつかの同値関係が定義される。) 任意の n 次のアダマール行列 H_n は次の形に同値である。

$$NH_n = \begin{pmatrix} -1 & 1 & 1 & \cdots & 1 \\ 1 & & & & \\ \vdots & & * & & \\ 1 & & & & \end{pmatrix} \qquad (1)$$

我々はこれを正規化されたアダマール行列と言うことにする。

Remark. 通常 アダマール行列の正規形と言うと、第一行と第一列とをすべて 1 にしたものを言うが、我々の議論には(1)の方が適している。

code について

$GF(2) = \mathbb{F}_2 = \{\bar{0}, \bar{1}\}$ 上の m 次元 vector space $\mathbb{F}_2^m$ の k 次元 subspace を $[m, k]$ binary code という。

$\mathbb{F}_2^m \ni \underline{x} = (x_1, x_2, \cdots, x_n)$ の non-zero coordinates の個数を $\underline{x}$ の Hamming weight といい、$wt(\underline{x})$ と書く。

$\mathbb{F}_2^m \ni \underline{x}, \underline{y} = (y_1, y_2, \cdots\cdots, y_m)$ について通常の内積

$$(\underline{x}, \underline{y}) = \sum_{i=1}^{m} x_i y_i$$ 及び

vector product

$$\underline{x} \cdot \underline{y} = (x_1 y_1, x_2 y_2, \cdots\cdots, x_m y_m) \in \mathbb{F}_2^m$$

が定義される。

非負の整数 $\underline{x} * \underline{y} = wt(x \cdot y)$ を $\underline{x}$ と $\underline{y}$ との intersection number ということにすると、次の関係が成り立つ。

$$wt(\underline{x} + \underline{y}) = wt(\underline{x}) + wt(\underline{y}) - 2\underline{x} * \underline{y} \qquad (2)$$

これは inclusion - exclusion principle の特別な場合である。

$[m, k]$ binary code C があるとき、その dual

$$C^{\perp} = \left\{ \underline{u} \in \mathbb{F}_2^m \mid (\underline{u}, \underline{x}) = 0 \quad \forall \underline{x} \in C \right\}$$

が定義される。 $\dim C^{\perp} = m - k$

code C は $C \subset C^{\perp}$ であるとき、self - orthogonal、$C = C^{\perp}$ であるとき、self - dual であるという。self - orthogonal code C の各 codeword の weight は偶数であることはすぐに分る。$[m, k]$ binary code C が self - dual であって、C の各元の weight が 4 で割り切れるとき、C は doubly even self - dual code であるという。(以下 略記して DESD binary code と書くことにする。) C が DESD binary code ならば、m は 8 の倍数で、$k = \frac{m}{2}$ となることはよく知られている結果である。

本講演では 次の定理 1 を主として解説する。

定理 1、 $n \equiv 4 \pmod 8$ のとき、正規化されたアダマール行列 (1) から DESD binary code $C(NH_n) = [2n, n]$ が定義される。

さらに次の定理 2 も証明されて、アダマール行列と

DESD binary code との深い関連を示唆するが、証明には立入らない。

定理2、$n \equiv 4 \pmod 8$ で 二つのH-同値な正規化された n 次のアダマール行列 $NH(1)$, $NH(2)$ から定義される $C(NH_{(1)})$ $C(NH_{(2)})$ は code として同値である。

§2 $C(NH_n)$ の定義と性質

NH_n を 正規化されたアダマール行列とする。

$K_n = \frac{1}{2}(NH_n + J_n)$ とおく。

ここで J_n は all 1 square matrix.

K_n は NH_n の係数のうち 1 を 1 に、-1 を 0 にして得られる (0,1) 行列。$n \times 2n$ 行列 C_n を次により定義する。

$$C_n = (I_n \ K_n)$$

C_n の行ベクトル $\underline{x}_1, \underline{x}_2, \cdots\cdots, \underline{x}_n$ を $\mathbb{F}_2^{2n}$ のベクトルと見て、$\underline{x}_1, \cdots\cdots \underline{x}_n$ により $\mathbb{F}_2$ 上 張られるベクトル空間を $C(NH_n)$ とする。明らかに $\underline{x}_1, \cdots\cdots, \underline{x}_n$ は 一次独立であるから $C(NH_n)$ は $[2n, n]$ binary code である。$C(NH_n)$ が $n \equiv 4 \pmod 8$ のとき DESC code であることを主張するために NH_n の性質を利用する。

$NH_n = (s_{ij})$ とし、ξ_i を NH_n の i 番目の行ベクトルとする。$\nu_1(i)$ (resp. $\nu_2(i)$) を ξ_i の最後の $n-1$ 個の要素中の 1 (resp. -1) の個数とする。定義により次のことは容易に分る。

$$\nu_1(1) = n-1 \quad , \qquad \nu_2(1) = 0 \tag{3}$$

ξ_1 と ξ_i $(i \geqq 2)$ との直交性より

$$\nu_1(i) = n/2 \tag{4-1}$$

$$\nu_2(i) = n/2 - 1 \tag{4-2}$$

が導かれる。さらに $1 \leqq i < h \leqq n$ に対して

$$\mu_1(i,h) = \#\{j \mid S_{ij} = S_{hj} = 1 \qquad 2 \leqq j \leqq n\}$$

$$\mu_2(i,h) = \#\{j \mid S_{ij} = 1, S_{hj} = -1 \qquad 2 \leqq j \leqq n\}$$

$$\mu_3(i,h) = \#\{j \mid S_{ij} = -1, S_{hj} = 1 \qquad 2 \leqq j \leqq n\}$$

$$\mu_4(i,h) = \#\{j \mid S_{ij} = S_{ij} = -1 \qquad 2 \leqq j \leqq n\}$$

とおくと 次のことは 定義から直ちに導かれる性質である。

$$\mu_1(i,h) + \mu_2(i,h) = \nu_1(i) = n/2 \tag{5-1}$$

$$\mu_3(i,h) + \mu_4(i,h) = \nu_2(i) = n/2 - 1 \tag{5-2}$$

$$\mu_1(i,h) + \mu_3(i,h) = \nu_1(h) = n/2 \tag{5-3}$$

$$\mu_2(i,h) + \mu_4(i,h) = \nu_2(h) = n/2 - 1 \tag{5-4}$$

ξ_i と ξ_h $(2 \leqq i < h \leqq n)$ との直交性より

$$\sum_{j=1}^{n} s_{ij} s_{hj}$$

$$= 1 + \mu_1(i,h) + \mu_4(i,h) - \mu_2(i,h) - \mu_3(i,h) = 0 \quad (6)$$

(5-1) ~ (6) から

$$\mu_1(i,h) = \mu_2(i,h) = \mu_3(i,h) = n/4$$
$$\mu_4(i,h) = n/4 - 1 \qquad 2 \leqq i < h \leqq n \qquad (7)$$

$\underline{x}_i, \cdots\cdots, \underline{x}_n$ の定義と ξ_i の符号分布とより、次のことが分る。

$$wt(\underline{x}_1) = n$$
$$wt(\underline{x}_i) = 2 + \nu_1(i) = 2 + n/2 \quad (i \geqq 2)$$

故に $n \equiv 4 \pmod 8$ のとき

$$wt(\underline{x}_i) \equiv 0 \pmod 4 \quad (1 \leqq i \leqq n) \qquad (8)$$

を得る。さらに (4-1) より

$$(\underline{x}_1, \underline{x}_i) = \nu_1(i)\,\overline{1} = \overline{0} \qquad i \geqq 1 \qquad (9\text{-}1)$$

又 (7) より

$$(\underline{x}_i, \underline{x}_h) = \left[1 + \mu_1(i,h)\right]\overline{1} = \overline{0} \quad 1 \leqq i < h \leqq n \quad (9\text{-}2)$$

Remark 2. (9-2) 及び (8) は $n \equiv 4 \pmod 8$ のときにのみ成り立つ。$n \equiv 0 \pmod 8$ については $C(NH_n)$ は定義は同じであるが良い code にならない。

$C = C(NH_n)$ は $\dim C = n$. 又 (8), (9-1), (9-2) より C は self-orthogonal であることは明らか。$C \subset C^{\perp}$ で $\dim C = \dim C^{\perp}$ より $C = C^{\perp}$ よって C は self-dual.

V. Pless の教科書 [9] の §2.4 を引用する。

Proposition 1 (Theorem 4 in Pless [9]). If the rows of a generator matrix G for a binary (n,k) code C have weights divisible by 4 and are orthogonal to each other, then C is self-orthogonal and all weights in C are divisible 4.

(8) と (9-1), (9-2) とより、$C = C(NH_n)$ は 上の prop. の条件をみたしているから doubly even である。以上により $C = C(NH_n)$ は DESD $[2n, n]$ binary code である。これで定理1の証明は済んだ。

実例

ex. 1

$$NH_4 = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

は標準化された4次のアダマール行列

$$C(NH_4) = \left(\begin{array}{cccc|cccc} 1 & & & & 1 & 1 & 1 \\ & 1 & & & 1 & & 1 & 1 \\ & & 1 & & 1 & 1 & & 1 \\ & & & 1 & 1 & 1 & 1 & \end{array}\right)$$

これは Hamming $[8,4,4]$ code (minimal weight=4)

ex. 2 H_{12} を任意の12次のアダマール行列とすると、$C(NH_{12})$ は長さ24の binary Golay code $[24,12,8]$ (minimal weight = 8) になることが証明できる。

ex. 3 Hall [5] により 20次の Hadamard 行列は 3つの

同値類より成り、それらの類から代表をとり、$NH_{20}^{(1)}$, $NH_{20}^{(2)}$, $NH_{20}^{(3)}$ とする。(正規化する) $C(NH_{20}^{(1)})$, $C(NH_{20}^{(2)})$, $C(NH_{20}^{(3)})$ はいずれも DESD $[40, 20, 8]$ binary code である。$C(NH_{20}^{(1)})$ は Mac Williams - Sloane で知られている code に同値な code で $C(NH_{20}^{(2)})$, $C(NH_{20}^{(3)})$ は新しい code 達である。(3つは互いに同値でない)。同値でないことの証明には Assmus - Mattson の定理 ([2]) を適用する。

ex. 4 $n = 36 \equiv 4 \pmod 8$ に対する H_{36} から作られる code $[72, 36]$ の code の minimal weight をいくつかの H-同値類について計算してみたが minimal weight が 16 の DESD code の存在という Sloane の問題に解答を与えるアダマール行列は今の所、見つかっていない。しかし、36次のアダマール行列の同値類の個数は猛烈に沢山あるので $C(NH_{36})$ $[72, 36, 16]$ code を得る望みも捨てたものではない。(少なくとも群論的アプローチ — Pless, Conway, Thompson 達がとっている — よりは hopeful ではないか)。

ex.5　$n=28$ のときの アダマール行列の分類は Tonchev, Kimura によって かなり進展している。Paley 行列 P_{28} から得られる code $C(NP_{28})$ が $[56, 28, 12]$ binary code として唯一知られているもの（同値を除いて）。

残された問題としては

(I) $n \equiv 0 \pmod 8$ のときに n 次のアダマール行列から DESD binary $[2n, n]$ code を定義する方法はないか？

(II) $n \equiv 4 \pmod 8$ で codes $C(NH_n^{(1)})$ と $C(NH_n^{(2)})$ とが同値ならば $NH_n^{(1)}$ と $NH_n^{(2)}$ とは H-equivalent か？

(III) DESD $[2n, n]$ codes の中で code $C(NH_n)$ の特徴付けを行なえ。良い特徴付けができれば、アダマール行列の基本予想（$n \equiv 0 \pmod 4$ なら n 次のアダマール行列 H_n が必ず存在する）に使えるかも知れない。

(IV) $[72, 36, 16]$ binary code が $C(NH_{36})$ として得られるか？

(I) に対するコメント

(i) 20次のアダマール行列の3つの同値類に対応して、3つの互いに同値でない $[40, 20, 8]$ binary code があるように、16次のアダマール行列では5つの同値類があり、一方では

[3] から分っているように 5つの DESD[32, 16, 8] codes の同値類があり、この2種の対象に何らかの関連があると考えたくなる誘惑から逃れ難い。

(ii) 長さ16の DESD indecomposable binary code の生成行列の一つは次によって与えられる。

(I_8, K_8) ただし $K_8 =$

$$\begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

この K_8 と8次の正規化されたアダマール行列(複数個)との比較によって 一つのゲームを思いついた。7行7列のマス目を考え、2つの記号 A, B を用意し、次のような規則(1)~(5)に従う配置を作る。$(1 \leqq i, j \leqq 7)$

(1) どのマス目も A または B または空白が入る。

(2) 第 i 行に並ぶ A の個数、B の個数をそれぞれ i_A, i_B とすると、ただ一つの i_0 を除くと $i_B - i_A = 2$ が成り立つ。その i_0 については $i_{0A} - i_{0B} = 2$

(3) 第 j 行についても(2)に相当したことが成り立つ。(j_0 を使う)

(4) (i_0, j_0) のマス目には A が入らない。

(5) ある斜めの列に A が2つ並び、その斜めの他のマス

目を $(i_1, j_1)(i_2, j_2)$ とする。ただし $i_1+j_1 = i_2+j_2 = t$。

例えば

				A		A
	A	B	B	B		
	B	A		B	B	
A				B	B	B
A	B	B				B
		B				B
	B		B			

は (1)～(5) をみたす。このとき

$K = (k_{ij})$ $0 \leqq i, j \leqq 7$ を次により定める。

$k_{00} = 0$, $k_{0j} = 1$ $1 \leqq j \leqq 7$

$k_{i0} = 1$, $(1 \leqq i \leqq 7)$

$k_{i_0 j_0} = 0$, $k_{i_0 j} = 1$ $j \neq j_0$

$k_{i j_0} = 1$ $i \neq i_0$

$k_{ij} = 1$ $i + j = t$

それ以外の $k_{ij} = 0$

上の例の配置の場合得られた K は K_8 と一致する。

このゲームを $n \equiv 0 \pmod 8$ なる各 n に定式化できれば問題(I)の一つの接近法になりうる。

参考文献

[1] S.S. Agaian, Hadamard matrices and their applications, Lect. Notes Math. No. 1168 Springer

[2] E.F. Assmus, Jr. and H.F. Mattson, Jr., New

5-designs, J. Comb. Th. 6 (1966), 122-151

[3] J.H. Conway and V.Pless, On the enumeration of self-dual codes, J. Comb. Th. Ser.A 28(1980)26-53

[4] M. Hall, Jr., Hadamard matrices of order 16, Jet Propulsion Laboratory Research Summary No.36-10, 1 (1961) 21-26

[5] M.Hall, Jr., Hadamard matrices of order 20, Jet Propulsion Laboratory Technical Report No.32-761, (1965)

[6] M.Hall, Jr., Combinatorial Theory (2nd ed.) Wiley-Interscience Series (1986)

[7] F.J. MacWilliams & N.J.A.Sloane, The Theory of Error-Correcting Codes, North Holland (1977)

[8] M.Ozeki, Hadamard matrices and doubly even self-dual error-correcting codes, to be published by J. Comb. Th. Ser.A

[9] V.Pless, Introduction to the Theory of Error-Correcting Codes, Wiley-Interscience Series (1982)
(和訳「符号理論入門」伊藤昇訳 ワイリー・ジャパン)

[10] W.D. Wallis, A.P. Street & J.S. Wallis, Com-

binatorics: Room Squares, Sum-Free Sets, Hadamard Matrices. Lect. Notes Math. No. 292 Springer

Hadamard行列とそのK-行列について

愛媛大理　木村　浩

Hadamard行列の問題は(1)構成と(2)分類にある.〔1〕と〔2〕で28次の行列の作り方とその分類の方法を示した.

以下次数は28次とする.　HをHadamard行列とし,K(H)をそのK-行列とする(定義は〔1〕,次数$n>28$に対しても同様に定義できる.このときはHall setを数えるだけでなく次数によって決まる自由度がある.その自由度個のK-行列(みたいなもの)が作れ,それらは同値類のinvaliantである.　28次のときは自由度は1であることを注意しておく).K-行列による分類で新しい行列を約450個作った.　またK-行列の形から$Aut\,H$が自明である.(i.e. $|Aut\,H|=2$)行列もそれらの内に沢山あることもわかった.

この講演ではK-行列による分類が

どの程度正確であるかを考えたものである.
$K(H)$ が異なる行を多くもてば良い方法な気がする. しかし $K(H)=0$ なる H は唯一つしか見つかっていない (QR-type).
Toncher の H_2, H_3 [3] は $K(H_2)=K(H_3)$ であった. これを区別する方法がないか考えてみた.

$H=(h_{ij})$ とおく. 異なる6行に対して

$$\#\{j \mid \#\{i \in \{i_1 \cdots i_6\}; h_{ij}=1\}=6 \text{ or } 22\}$$

を考える.

i を fix しておく. i を含む6行を取ることによって K-行列を作ったのと同様にして 27×26 形の行列 K_i を得る. さらに $K_1, \cdots K_{28}$ に辞書的順序をつける.

$KB(H)=\{K_1, \cdots, K_{28}\}$ を H に associate した K-Box ということにする.

作り方より

$$H \sim H' \Rightarrow KB(H)=KB(H').$$

この判定法によって K-行列が同じで K-Box の異なる行列を5個揚げる.

(他に知らない. 才1, 2が Tonchev のもの).
なお〔2〕で作ったH－行列とそれらのK－行列の表を〔4〕で発表の予定である.

$K(H)=K({}^{T}H)=($ 28 .....111)

Table of H-matrices and K_2-matrices

2st row - 28th row of H

$K_2(H)$	$K_2({}^{T}H)$
126935357 52835175 76976859 250958145	221053343 143243085 54642643
26204577 260836977 179407527 12209495	237157777 154359353 205671405
156739669 32780169 40688157 147092663	173966635 102721157 130227215
91788517 69594219 233497091 48963833	72956723 186153163 0
Mul= 28	Mul= 28
6 CCGGGGGGIIIIKKKKOOOOOOSSSS	6 EEGGGGGGIIIIKKMMMMMMMOOQQUU
6 EEGGGGGGIIKKKKMMMMOOOOOOSS	6 EEGGGGIIKKKKMMMMMMMMMOOOOOO
6 EGGIIIIIIIKKKKKKMMMMOOOOOS	6 EEGGIIIIIIIKKKKKMMMMMOOOUU
6 GGGGIIIIKKKKKKMMMMMMMMOOOO	6 GGGGGGIIIIIIKKMMMMOOOOOOQQ
3 IIIIKKKKKKKKMMMMOOOOOOSSSS	3 IIIIKKKKMMMMMMMMOOOOOOQQQQ
32511 2064767 132121023 149130767	252024377 159132213 178974771
40478689 27696081 228101347 181225689	238686925 109989669 75029785
60373771 220424553 189941587 239384903	55826597 104279187 89055883
148256169 210887573 153965959 83186275	97203285 62186573 0
Mul= 4	Mul= 4
3 ..OOOOOOOOOOOOOOOOOOOOOO	
18 EEGGGGHHIIIKMMNNNNOOOOOOOO	
6 GGGGGGIIIIIKKKNNNNNNOOOOOO	
Mul= 24	Mul= 24
6 9FFGGHHJJJJLLLMMNNNNNNNNSS	
2 CGGGIIIIKKKKKKMMMNNNNNNOOO	
3 EEGGGGHHIIIKMMNNNNOOOOOOOO	
3 EEIIIIJJKKKKKKLLLLNNNNNNOO	
3 FFFFHHHHJJKKKKLLMMMMOOOOSS	
3 FFGGGGIIJJJJJJJJJMMNNOOQQSS	
3 FFGGIIJJJJKKKKLLMMMMNNNNQQ	
1 GGGGGGIIIIIKKKNNNNNNOOOOOO	
3 IIIIIIIIKKMMMMNNNNOOQQSSSS	

```
   32511    2064767 132121023 149130767 252024377 159132213 178974771
44411873   23762897 164938979 220848333 238424775  87254819  41219341
93117191 213392745 188963173 214328153 106613417  80688293  28792985
177817493 206682515 185478539 127052885 107826259  64565835         0
```

Mul= 24

```
2 BCEGHHIIIIIKKLMMMNNOPPPQQR
2 BEEGHHIIJKKKKKLMMNNNOOOPQR
2 BEEGHHJJJJJJLLLMMNNNNNNORY
2 CCDEIIJJJKKKKLLMMNNNNOOPQR
1 CCEGGHHIIIIKLLMMNNNNNNOQYY
1 DEGGHHHHHJKKKLLLMMOOOOOPQR
1 DHHIIIIJJKKKKLLLLLMMMMNOOR
2 EEFFHHHIIJJJJLLMNNNNOOPPQR
2 EFFFGHIIJJJJKLLLMMMNNOOQQY
1 FFHHIIJJJJKKKKKKLLNNNNOOPP
1 FGGGGHJJJJJKKLLLLLMMNOOOOOQ
1 FGGHHIIIIJJLLLLMMMMMMNNOPQ
2 FGGHHIIJJJKKKKLLMMMNNNOOOP
2 GGHHIIIIIJJJKLLLLMMNNOOOOP
1 GGHHJJLLLLMMNNNNOOOOPPQQRR
1 HHHHJJJJKKKKKKLLLLLLMMNNOO
1 HHIIIIIIIIIJJKKKKLLNNNNOOPP
1 IIJJJJKKKKMMMMNNOOOOPPQQQQ
1 JJJJKKLLLLMMMMMMMMNNPPPPRR
```

Mul= 4

```
6 CDGHHIJJJJJJKLLLLMMMNNQQQR
6 DGGGHIJJJKKKKLLLMMMMNNNOPQ
6 EFGGGHHIJJJJJKKKKLMPPQQQQR
6 EFGHHHIJJJJJJLLMMMMNNNOPQQ
3 FFFFLLLLNNNNNNNNOOOOOOQQQQ
```

Mul= 4

```
6 DEGGHHHHHJKKKLLLMMOOOOOPQR
6 DHHIIIIJJKKKKLLLLLMMMMNOOR
6 FGGGGHJJJJJKKLLLLMMNOOOOOQ
6 FGGHHIIIIJJLLLLMMMMMMNNOPQ
3 JJJJLLLLLLLLMMMMOOOOOOPPPP
```

Mul= 24

```
1 CDGHHIJJJJJJKLLLLMMMNNQQQR
1 CEEHHIIIIJJKKKLLLLNNPPQQQQ
1 DDGGGGHHIIKKLLNNNNNNNNNPPQQ
2 DFFGHHIJJJJKKKLMMMMMNPPPQQ
1 DGGGHIJJJKKKKLLLMMMMNNNOPQ
2 DGGHIIIIJJJJKKLMMMMNNNNPPR
2 DHHHIIIIJKKKKKLLLMMMNNNNOS
1 EFGGGHHIJJJJJKKKKLMPPQQQQR
1 EFGHHHIJJJJJJLLMMMMNNNOPQQ
2 EGGGGGIJJJKKKLLLLLMMNOPPQR
2 EGHHHIIIIJJKKKKLLLMMNNPQQR
2 EGHHIIIJJJKKKKKKKLLMNNPQQQ
2 FGGHHIIJJJJKKKKLLMMMMNOPPS
1 GGIIJJKKLLLLMMMMPPPPPPQQSS
2 GIIIIJJJJJJKKKKLLLLLMMNNPQ
1 HHIIIIJJJJKKKKLLLLMMNNNNNN
1 IIIIIIIIIJJKKKKLLLLLLLLOOPP
1 IIJJJJKKLLMMMMMMMMNNQQRRRR
1 IIKKKKKKLLLLMMMMMMPPPPQQQQ
```

Where • = 0, and A , • • •, Y = 10, • • • ,34, respectively.

References

1. H. Kimura. Hadamard matrices of order 28 with automorphism groups of order 2, J. Combin. Theory Ser. A 43(1986) 98-102

2. H.Kimura and H.Ohmori, Construction of Hadamard matrices of order 28, Graphs and Combin. 2(1986) 247-257

3. V. D. Tonchev. Hadamard matrices of order 28 with automorphisms of order 7, J. Combin. Theory Ser. A 40(1985) 62-81

4. H.Kimura and H. Ohmori, Hadamard matrices of order 28, Memoirs of the Faculty of Education Ehime University A,1987) (to appear)

ある種の平面分割の個数について

東大　理　　岡田　聡一

§1.

定義　plane partition（平面分割）とは，自然数a_{ij}を

$$\begin{array}{llll} a_{11} & a_{12} & a_{13} & \cdots\cdots \quad a_{1\lambda_1} \\ a_{21} & a_{22} & a_{23} & \cdots\cdots \quad a_{2\lambda_2} \\ \vdots & \vdots & & \\ a_{r1} & a_{r2} & \cdots\cdots & a_{r\lambda_r} \end{array}$$

のように並べたもので

(1)　$\lambda_1 \geqq \lambda_2 \geqq \cdots\cdots \geqq \lambda_r$

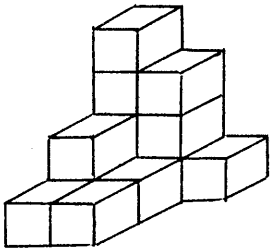
(2)　$a_{ij} \geqq a_{i,j+1}$

(3)　$a_{ij} \geqq a_{i+1,j}$

を満たすもののことをいう。（何も並べないものもplane partitionと考え，ϕで表す。）

Plane partition $\pi=(a_{ij})$は，数字a_{ij}の書かれている場所にa_{ij}個の立方体を積み重ねてできる立体としてとらえるのが便利である。例えば

$$\pi = \begin{matrix} 4 & 3 & 1 \\ 2 & 1 & \\ 1 & 1 & \end{matrix}$$ に対し



そこで，π に対して，π の diagram $D(\pi)$ を

$$D(\pi)=\{(i,j,k)\in\mathbb{N}^3;\ a_{ij} が定義され，\ 1\leqq k\leqq a_{ij}\}$$

とおいて定義する．すると，plane partition の定義の条件(1)．(2)．(3)は

(*) $(i,j,k),(i',j',k')\in\mathbb{N}^3$ に対して

$$i\geqq i',\ j\geqq j',\ k\geqq k',\ (i,j,k)\in D(\pi)\Rightarrow(i',j',k')\in D(\pi)$$

と言いかえることができる．

3次対称群 $\mathfrak{S}_3$ を座標の置換によって $\mathbb{N}^3$ に作用させる．このとき，plane partition π と $\omega\in\mathfrak{S}_3$ に対して $\omega\cdot D(\pi)$ がある plane partition の diagram となることが，(*)からわかる．

<u>定義</u>．plane partition π は

$$\omega\cdot D(\pi)=D(\pi)\quad(\forall\omega\in\mathfrak{S}_3)$$

を満たすとき，<u>totally symmetric</u> であるという．さらに，totally symmetric plane partition π に対して $D(\pi)$ の $\mathfrak{S}_3$-orbit の個数を，π の weight といい，$wt(\pi)$ で表すことにする．

例えば、$D(\pi)\subset[2]\times[2]\times[2]$ ($[2]=\{1,2\}$) となる totally symmetric plane partition は

π :	ϕ	1	21 1	22 21	22 22
$wt(\pi)$:	0	1	2	3	4

の5個である。今、

$$\mathcal{T}_n(d)=\{\pi : \text{totally symmetric plane partition},\ D(\pi)\subset[n]\times[n]\times[n],\ wt(\pi)=d\}$$

$$T_n(d)=\#\mathcal{T}_n(d)$$

($[n]=\{1,2,\cdots,n\}$) とおき、$T_n(d)$ の母関数

$$T_n=\sum_{d=0}^{\infty} T_n(d)q^d$$

($D(\pi)\subset[n]\times[n]\times[n]$ のとき $wt(\pi)\leqq n^3$ だから、T_n は q の多項式) を考える。この母関数について、次の予想がある。

予想 (G.E. Andrews, D.P. Robbins) ([1],[2]参照)

$$T_n=\prod_{1\leqq i\leqq j\leqq k\leqq n}\frac{1-q^{i+j+k-1}}{1-q^{i+j+k-2}}.$$

ここでは、上の予想が1つの行列式の計算に帰着されることを報告する。

§2.

まず，T_nがある行列の小行列式の和で表されることを見る．

定義　row-strict shifted plane partition とは，自然数a_{ij}を

$$\begin{array}{ccccccc} a_{11} & a_{12} & a_{13} & \cdots\cdots & & & a_{1,\mu_1} \\ & a_{22} & a_{23} & \cdots\cdots & & a_{2,\mu_2} & \\ & & a_{33} & \cdots\cdots & a_{3,\mu_3} & & \\ & & & \ddots & & & \\ & & & & a_{rr} & \cdots & a_{r,\mu_r} \end{array}$$

のように並べたもので

(1)　$\mu_1 \geqq \mu_2 \geqq \mu_3 \geqq \cdots \geqq \mu_r$

(2)　$a_{i,j} > a_{i,j+1}$

(3)　$a_{i,j} \geqq a_{i+1,j}$

を満たすもののことをいう．(何も並べないものもrow-strict shifted plane partitionと考え，Φで表す)

ここで

$$\mathcal{R}_n(d) = \{\sigma = (a_{ij}) : \text{row-strict shifted plane partition},\ a_{ij} \leqq n\ (\forall i,j),\ \sum_{i,j} a_{ij} = d\}$$

とおくと，次の命題が成り立つ．

命題1．$\pi = (a_{ij}) \in \mathcal{T}_n(d)$に対して，$b_{ij} = a_{ij} - j + 1$ ($i \leqq j$, $b_{ij} > 0$のときのみ定義する)とおくと，

$$\widetilde{\pi}=(b_{ij})\in\mathcal{R}_n(d)$$

であり，対応 $\pi\longmapsto\widetilde{\pi}$ は $\mathcal{T}_n(d)$ と $\mathcal{R}_n(d)$ の間の全単射を与える．

r 行から成る row-strict shifted plane partition $\sigma=(a_{ij})$ に対して，第 i 行に λ_i 個の自然数が書かれているとき，

$$sh(\sigma)=(\lambda_1,\lambda_2,\cdots,\lambda_r)\quad(\lambda_1>\lambda_2>\cdots>\lambda_r)$$

とおく．(σ の shape という)．自然数の減少列 $a_1>a_2>\cdots>a_r>0$，$\lambda_1>\lambda_2>\cdots>\lambda_r$ に対して

$$F(a_1,\cdots,a_r;\lambda_1,\cdots,\lambda_r;d)$$
$$=\#\{\sigma=(a_{ij})\in\mathcal{R}_n(d);a_{ii}=a_i(i=1,\cdots,r)$$
$$sh(\sigma)=(\lambda_1,\cdots,\lambda_r)\}$$

$$F(a_1,\cdots,a_r;\lambda_1,\cdots,\lambda_r)=\sum_{d=0}^{\infty}F(a_1,\cdots,a_r;\lambda_1,\cdots,\lambda_r;d)q^d$$

のように定義する．

<u>命題</u>2．$a_1>a_2>\cdots>a_r>0$，$\lambda_1>\lambda_2>\cdots>\lambda_r>0$ に対して

$$F(a_1,\cdots,a_r;\lambda_1,\cdots,\lambda_r)=\det\left(q^{a_i+\binom{\lambda_j}{2}}\begin{bmatrix}a_i-1\\ \lambda_j-1\end{bmatrix}\right)_{i,j=1,\cdots,r}$$

ここで，$\binom{a}{b}$ は2項係数であり，$\begin{bmatrix}a\\ b\end{bmatrix}$ は Gauss 多項式．

$$\begin{bmatrix}a\\ b\end{bmatrix}=\begin{cases}\dfrac{(1-q^a)(1-q^{a-1})\cdots(1-q^{a-b+1})}{(1-q)(1-q^2)\cdots(1-q^b)} & \begin{pmatrix}a\geqq 0\\ 0\leqq b\leqq a\end{pmatrix}\\ 0 & (\text{その他})\end{cases}$$

である．

ところが,

$$\sum_{d=0}^{\infty} \#\mathcal{R}_n(d)\, q^d = 1 + \sum F(a_1,\cdots,a_r;\lambda_1,\cdots,\lambda_r)$$

(和は $n \geqq a_1 > a_2 > \cdots > a_r > 0$, $n \geqq \lambda_1 > \lambda_2 > \cdots > \lambda_r > 0$ なる列 $a_1,\cdots a_r;\lambda_1,\cdots,\lambda_r$ 全て(rも動かす)にわたる) だから, 命題1,2により, T_nは次の行列A_nの小行列式全ての和(0次小行列式は1として加える)に等しいことがわかる.

$$A_n = \left(q^{i+\binom{j}{2}} \begin{bmatrix} i-1 \\ j-1 \end{bmatrix} \right)_{i,j=1,\cdots,n}$$

$$= \begin{pmatrix} q & 0 & 0 & \cdots & 0 \\ q^2\begin{bmatrix}1\\0\end{bmatrix} & q^3\begin{bmatrix}1\\1\end{bmatrix} & 0 & \cdots & 0 \\ q^3\begin{bmatrix}2\\0\end{bmatrix} & q^4\begin{bmatrix}2\\1\end{bmatrix} & q^6\begin{bmatrix}2\\2\end{bmatrix} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ q^n\begin{bmatrix}n-1\\0\end{bmatrix} & q^{n+1}\begin{bmatrix}n-1\\1\end{bmatrix} & q^{n+3}\begin{bmatrix}n-1\\2\end{bmatrix} & \cdots & q^{n+\binom{n}{2}}\begin{bmatrix}n-1\\n-1\end{bmatrix} \end{pmatrix}$$

§3.

この節では, より一般に, 変数z_{ij}を(i,j)成分とする$n\times m$行列$Z=(z_{ij})_{\substack{i=1,\cdots n\\ j=1,\cdots m}}$の小行列式の和を考える. $1 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_r \leqq n$, $1 \leqq b_1 \leqq b_2 \leqq \cdots \leqq b_r \leqq m$に対して

$$d(a_1,\cdots,a_r;b_1,\cdots,b_r) = \det\left(z_{a_i,b_j}\right)_{i,j=1,\cdots r}$$

とおき,

$$d(a_1,\cdots,a_r) = \sum_{1 \leqq b_1 < b_2 < \cdots < b_r \leqq m} d(a_1,\cdots,a_r;b_1,\cdots,b_r)$$

のように定義すると，$a_i = a_{i+1}$ となる i があるとき

$$d(a_1, \cdots, a_r) = 0.$$

であり，$1 \leqq a_1 < a_2 < \cdots < a_r \leqq n$ のとき $d(a_1, \cdots, a_r)$ は Z から $a_1, a_2, \cdots, a_r$ 行をとってできる $r \times m$ 行列 $(z_{a_i, j})_{\substack{i=1,\cdots r \\ j=1,\cdots m}}$ の r 次小行列式全ての和に等しい．このとき，次の recursive formula が成り立つ．

定理 1. $1 \leqq a_1 < a_2 < \cdots < a_r \leqq n$ とする．

(1) r が奇数のとき

$$d(a_1, \cdots, a_r) = \sum_{i=1}^{r} (-1)^{i-1} d(a_i)\, d(a_1, \cdots, a_{i-1}, a_{i+1}, \cdots, a_r)$$

(2) r が偶数のとき

$$d(a_1, \cdots a_r) = \sum_{i=2}^{r} (-1)^{i} d(a_1, a_i)\, d(a_2, \cdots, a_{i-1}, a_{i+1}, \cdots, a_r)$$

今，$2k$ 次交代行列 $X = (x_{ij})_{i,j=1,\cdots 2k}$ $(x_{ij} + x_{ji} = 0)$ の Pfaffian を $Pf(X)$ で表す．ただし，

$$J_k = \underbrace{\begin{pmatrix} 0 & 1 & & & & \\ -1 & 0 & & & \text{\Large 0} & \\ & & 0 & 1 & & \\ & & -1 & 0 & & \\ & & & & \ddots & \\ & \text{\Large 0} & & & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \end{pmatrix}}_{2k}$$

に対して，$Pf(J_k) = 1$ となるものをとる．すると，

$$Pf(X) = \sum_{i=2}^{2k} (-1)^{i} x_{1,i}\, Pf(X_{1,i})$$

(ここで，X_{ij} は X から i 行，j 行，i 列，j 列を除いて

得られる$2(k-1)$次交代行列である). これと定理1から

$d(a_1,\cdots,a_r)$は$d(a_i)=z_{a_i,1}+z_{a_i,2}+\cdots+z_{a_i,m}$, $d(a_i,a_j)$

$=\sum_{1\leq b<c\leq m}\det\begin{pmatrix} z_{a_i,b} & z_{a_i,c} \\ z_{a_j,b} & z_{a_j,c}\end{pmatrix}$ のみを用いて, 次のように

表される.

<u>系</u> $1\leq a_1<a_2<\cdots<a_r\leq n$ とする.

(1) rが奇数のとき

$$d(a_1,\cdots,a_r)=\mathrm{Pf}\begin{pmatrix} 0 & d(a_1) & d(a_2) & \cdots & d(a_r) \\ -d(a_1) & 0 & d(a_1,a_2) & \cdots & d(a_1,a_r) \\ -d(a_2) & -d(a_1,a_2) & 0 & \cdots & d(a_2,a_r) \\ -d(a_3) & -d(a_1,a_3) & -d(a_2,a_3) & \cdots & d(a_3,a_r) \\ \vdots & \vdots & \vdots & & \vdots \\ -d(a_r) & -d(a_1,a_r) & -d(a_2,a_r) & \cdots & 0 \end{pmatrix}$$

(2) rが偶数のとき

$$d(a_1,\cdots,a_r)=\mathrm{Pf}\begin{pmatrix} 0 & d(a_1,a_2) & d(a_1,a_3) & \cdots & d(a_1,a_r) \\ -d(a_1,a_2) & 0 & d(a_2,a_3) & \cdots & d(a_2,a_r) \\ -d(a_1,a_3) & -d(a_2,a_3) & 0 & \cdots & d(a_3,a_r) \\ -d(a_1,a_4) & -d(a_2,a_4) & -d(a_3,a_4) & \cdots & d(a_4,a_r) \\ \vdots & \vdots & \vdots & & \vdots \\ -d(a_1,a_r) & -d(a_2,a_r) & -d(a_3,a_r) & \cdots & 0 \end{pmatrix}$$

次に, 行列Zの小行列式全て(0次小行列式は1として含む)の和を$D(Z)$と表すことにすると

$$D(Z)=1+\sum d(a_1,\cdots,a_r)$$

(和は$1\leq a_1<a_2<\cdots<a_r\leq n$なる列$a_1,\cdots,a_r$全て($r$も動かす)に

わたる). このとき, $D(Z)$も$d(i)$, $d(i,j)$を用いて次のように表される.

定理2. (1) nが奇数のとき

$$D(Z)=\mathrm{Pf}\begin{pmatrix} 0 & d(1)+1 & d(2)-1 & d(3)+1 & \cdots & d(n)+1 \\ -d(1)-1 & 0 & d(1,2)+1 & d(1,3)-1 & \cdots & d(1,n)-1 \\ -d(2)+1 & -d(1,2)-1 & 0 & d(2,3)+1 & \cdots & d(2,n)+1 \\ -d(3)-1 & -d(1,3)+1 & -d(2,3)-1 & 0 & \cdots & d(3,n)-1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ -d(n)-1 & -d(1,n)+1 & -d(2,n)-1 & -d(3,n)+1 & \cdots & 0 \end{pmatrix}$$

(2) nが偶数のとき

$$D(Z)=\mathrm{Pf}\begin{pmatrix} 0 & d(1)+1 & d(2)-1 & \cdots & d(n)-1 & 1 \\ -d(1)-1 & 0 & d(1,2)+1 & \cdots & d(1,n)+1 & -1 \\ -d(2)+1 & -d(1,2)-1 & 0 & \cdots & d(2,n)-1 & 1 \\ -d(3)-1 & -d(1,3)+1 & -d(2,3)-1 & \cdots & d(3,n)+1 & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -d(n)+1 & -d(1,n)-1 & -d(2,n)+1 & \cdots & 0 & 1 \\ -1 & 1 & -1 & \cdots & -1 & 0 \end{pmatrix}$$

§4.

§2の最後で述べたように, totally symmetric plane partitionの母関数T_nは$A_n=\left(q^{i+\binom{j}{2}}\begin{bmatrix} i-1 \\ j-1 \end{bmatrix}\right)_{i,j=1,\cdots n}$の小行列式全ての和だったから, 定理2を適用することができる. そこで, §3において, $m=n$とし, $z_{i,j}=q^{i+\binom{j}{2}}\begin{bmatrix} i-1 \\ j-1 \end{bmatrix}$とおく. すると, $d(i)=\sum_{j=1}^{i} q^{i+\binom{j}{2}}\begin{bmatrix} i-1 \\ j-1 \end{bmatrix}$, $d(i,j)=\sum_{1\le k<l\le n}\det\begin{pmatrix} q^{i+\binom{k}{2}}\begin{bmatrix} i-1 \\ k-1 \end{bmatrix} & q^{i+\binom{l}{2}}\begin{bmatrix} i-1 \\ l-1 \end{bmatrix} \\ q^{j+\binom{k}{2}}\begin{bmatrix} j-1 \\ k-1 \end{bmatrix} & q^{j+\binom{l}{2}}\begin{bmatrix} j-1 \\ l-1 \end{bmatrix} \end{pmatrix}$に対して, 次

の命題が成り立つ.

命題3. (1) $d(1)=q$, $d(i)=q(1+q^{i-1})d(i-1)$

よって, $d(i)=q^i(1+q)(1+q^2)\cdots(1+q^{i-1})$

(2) $d(1,j)=q^{j+1}(1+q)(1+q^2)\cdots(1+q^{j-1})-q^{j+1}$

$d(i,j)=q(1+q^{i-1})d(i-1,j)-q^{2i+j-1}\begin{bmatrix} i+j-2 \\ i-1 \end{bmatrix}$

定理2と命題3を用いて計算すると, T_n^2 は次のような行列式で表されることがわかる.

定理3. B_n, C_n を次のような $n\times n$ 行列とする.

$$B_n=\begin{pmatrix} 1+q & & & & & \\ -1 & 1+q^2 & & & & \\ & -1 & 1+q^3 & & & \\ & & -1 & 1+q^4 & & \\ & & & \ddots & \ddots & \\ & & & & -1 & 1+q^n \end{pmatrix}$$

$$C_n=\left(q^{i+j-1}\begin{bmatrix} i+j-2 \\ i-1 \end{bmatrix}+q^{i+j}\begin{bmatrix} i+j-1 \\ i \end{bmatrix}\right)_{i,j=1,\cdots,n}$$

このとき,

$$T_n^{\,2}=\det(B_n+C_n).$$

従って, §1で述べた予想は定理3にある行列式 $\det(B_n+C_n)$ の計算に帰着された.

参考文献

[1] R. P. Stanley, A baker's dozen of conjectures concerning plane partitions, preprint.

[2] R. P. Stanley, Symmetries of plane partition, J. Combinatorial Theory (A). 43, (1986) p.p. 103-113

群が作用するblock designについて。

北大 理 荒川 則素
北大 理 吉田 知行

§1 概略

BIBDの性質を調べる上でincidence matrix N を考えるのは自然であり特に

$$\begin{cases} NN^t = mI + \lambda J \\ NN^t \text{の固有値は } rk, n, \cdots, n \text{ である。} \end{cases} \quad \cdots (1)$$

という事実からいくつかの有益な結果が得られる。以下において incidence matrix と(1)の関係を、R.M. Wilson および D.L. Kreher の方針に従って、t-design および自己同型群を持つ場合に拡張し、それに伴う古典的結果に対応する事実を述べる。

§2 定義及び使法、記号法.

以下で t-(v,k,λ) design を、点集合 P、ブロック集合 B、flag の集合 I の3つ組み (P,B,I) で表わす。標記の都合上、点とブロック間で、$\in$, $\subseteq$ 等の記号を使うが design が simple であることを仮定しているわけではない。(つまり $\beta,\gamma\in B$ で、$\{p\in P \mid p\in\beta\}=\{p\in P\mid p\in\gamma\}$ でも $\beta=\gamma$ とは限らない。) 自明な場合を避けるため $t\le k\le v-t$, $\lambda>0$ を仮定する。又、P の i 点集合 $\{I\in 2^P \mid |I|=i\}$ を $\binom{P}{i}$ で表わし、P 自身も $\binom{P}{v}$ で代用することがある。

今 (P,B,I) を t-$(v,k,1)$ design とする。

$i+j\le t$, $i,j\ge 0$ のとき、$I\in\binom{P}{i}$, $J\in\binom{P}{j}$ $I\cap J=\phi$ にとると、

$$b_i^j := \#\{\beta\in B \mid \beta\supseteq I,\ \beta\cap J=\phi\}$$

が、I,J の選び方によらずにきまり

$$\begin{cases} b_i^j = b_{i+1}^j + b_i^{j+1} \\ b_i^0 = \lambda\binom{v-i}{t-i} \Big/ \binom{k-i}{t-i} \end{cases}$$

で計算できる。

上の漸化式は

$$(b_{j+i}^0, b_{j+i-1}^0, \cdots, b_{j+i-u}^0, \cdots b_j^0) = (b_{j+i}^0, b_{j+i+1}^1, \cdots b_{j+i-u}^u \cdots b_j^i)\left(\binom{v}{u}\right)_{u,v=0}^{i} \quad \cdots (2)$$

とも書ける。$\binom{v}{u}$ は二項係数で $v<u$ なら0と定義する。

※群 $G \leq Sym(P) \times Sym(B)$ が (P, B, I) の自己同型であるとは、$I^g = I$ を満すことである。

ここで $I \ni (P, \beta)$, $g \in G$ について $(P, \beta)^g := (P^g, \beta^g)$ で定義する。

※ λ-(v, k, λ) design (P, B, I) において、$|B| = b_0^0 = \binom{v}{0}$ が成立するとき、right であると呼ぶのは、よく知られた術語である。以下の議論を簡単にするため、自己同型群 G をもち、$\binom{P}{\lambda}$ 上の G-orbit の数と、B 上の G-orbit の数が一致するとき G-right と呼ぶことにする。又、$\lambda = 1$ のとき、right は symmetric と読み換える。

※ M, N を有限集合とするとき、$M \times N$ から単位的可換環 R への写像全体を $Mat_R(M, N)$ とかき $M \times N$ 形行列と呼ぶ。 $A \in Mat_R(M, N)$, $B \in Mat_R(N, K)$ のとき

$A \cdot B \in Mat_R(M, K)$ を $A \cdot B[m, k] := \sum_{n \in N} A[m, n] B[n, m]$ で定義する。

λ-(v, k, λ) design (P, B, I) があるとき以下の行列は環 R に無関係に定義できる。

$N_i \in Mat\left(\binom{v}{i}, B\right)$

$$N_i[I, \beta] := \begin{cases} 0 & I \not\subset \beta \\ 1 & I \subset \beta \end{cases}$$ ($\lambda = 1$ なら普通の incidance matrix)

$W_{ij} \in Mat\left(\binom{v}{i}, \binom{v}{j}\right)$

$$W_{ij}[I,J] := \begin{cases} 0 & I \not\subseteq J \\ 1 & I \subseteq J \end{cases}$$

$M^{u}_{ij} \in Mat\left(\binom{v}{i}, \binom{v}{j}\right)$

$$M^{u}_{ij}[I,J] = \begin{cases} 0 & |I \cap J| \neq u \\ 1 & |I \cap J| = u \end{cases}$$

§3 t-design への拡張 (R.M. Wilson)

Th 1 $e+f \leq t$, $ef > 0$ とする。

$$N_e N_f^T = \sum_{u=0}^{\min(e,f)} b_{e+f-u} M^{u}_{ef} W_{ie}^T W_{uf} \qquad (3)$$

① 次の2式は定義より明らか。

$$\begin{cases} N_e N_f^T = \sum_{u=0}^{\min(e,f)} b_{e+f-u} M^{u}_{ef} \\ W_{ie}^T W_{if} = \sum_{u=0}^{\min(e,f)} \binom{u}{i} M^{u}_{ef} \end{cases}$$

2) を使えば 3) が得られる。 //

N_i の行で張られる $\mathbb{Q}^B$ の subspace を U_i とおく。

Cor (Petrenjuk-野田-坂内-Wilson-Chaudhuri)

$2s \leq t \Rightarrow N_s N_s^T$ は可逆. 特に $\dim_{\mathbb{Q}} U_s = \binom{v}{s}$

∵) $N_s N_s^T = \sum_{u=0}^{s} b_{2s-u} W_{us}^T W_{us}$ で, 右辺は正定値な2次形式. //

簡単な計算で, $U_0 \leq U_1 \leq \cdots \leq U_s$ が示せる。

$$\begin{cases} V_0 := U_0 \\ V_i := U_i \cap U_{i-1}^{\perp} \quad i=1,2,\cdots,s \end{cases} \quad \text{とおく。}$$

$\mathbb{Q}^B = V_0 \oplus V_1 \oplus \cdots \oplus V_s \oplus U_s^{\perp}$ である

Th 2 $N_s N_s^T$ の固有値は $\binom{b-i}{s-i} b_s^i$ $i=0,1,\cdots,s$ 及び 0 で対応する固有空間は、V_i $i=0,1,\cdots,s$ 及び $U_s^{\perp}$ である。

略証) $M_i := N_i^T N_i$ とおく。(3)より

$$M_e M_f = \sum_{u=0}^{\min\{e,f\}} \binom{b-u}{f-u}\binom{b-u}{e-u} b_{e+f-u}^{u} M_u \quad \cdots (4)$$

となることがわかる。このことより

$V_e M_s = \binom{b-e}{s-e} b_e^e V_e$ が計算できる。 //

Cor. $\det(N_s N_s^T) = \prod_{i=0}^{s} \left[\binom{b-i}{s-i} b_s^i\right]^{\binom{v}{i}-\binom{v}{i-1}}$

Cor. (P. Delsarte)

2-design において、$\#\{i \mid \lambda = |B\cap B_1|, B_1 \in \mathcal{B}\} = s+1$ なら、ブロック間に、i 点で交わるという関係で Association scheme が定義できる。

1) 4) より M_s 及び単位行列で張られる $s+2$ 次元可換 $\mathbb{Q}$ algebra が、求める Association scheme の Bose-Mesner algebra になることがわかる //

§4 自己同型群 G を持つ場合

R を単位的可換手環とする。

自己同型の定義より) N_s は RP から RB への

G-map を与えている。特に $\det(NN')$ が R の中で可逆であれば, RP は RB の R_G-直和因子となる。

以下 $R=\mathbb{C}$ とする。$\Omega = \Omega^P \cup B$ (以前の注意により, disjoint union である。)

$\tau : End_{\mathbb{C}G}(\mathbb{C}\Omega) \twoheadrightarrow End_{\mathbb{C}}(\mathbb{C}^{\Omega/G})$

なる自然な環準同形で, 転置を保つものがとれる。

これを使って Th 1, 2 を書き換えてみると,

Th 1' (D.L. Kreher)

$e+f \le 1 \Rightarrow \tau(N_e)\tau(N_f)^T = \sum_{\mu=0}^{\min(e,f)} b^{\mu}_{e+f-\mu}\tau(W_{\mu e})^T\tau(W_{\mu f})$

Th 2' (D.L. Kreher)

$2s \le 1 \Rightarrow \tau(N_s)^T\tau(N_s)$ の固有値は $\binom{k-i}{s-i} b_s^i$ $i=0,\cdots,s$ 及び 0 で, 対応する固有空間 V_i', $i=0,\cdots,s$, U_s^1 において

$\dim V_i' = |\binom{\Omega}{i}/G| - |\binom{\Omega}{i-1}/G|$, $U_s^1 = |B/G| - |\binom{\Omega}{s}/G|$

$\Omega/G = \{\Omega_1, \Omega_2, \cdots \Omega_{|\Omega/G|}\}$ を軌道分解とする。

$D \in Mat_{\mathbb{C}}(\Omega/G, \Omega/G)$ を

$D[\Omega_i, \Omega_j] := \delta_{ij}|\Omega_i|$ で定義する。

lemma (D.L. Kreher) $\forall A \in End_{\mathbb{C}G}(\mathbb{C}\Omega)$ について,

$\sqrt{D}^{-1}\tau(A)\sqrt{D} \in Mat_{\mathbb{Q}}(\Omega/G, \Omega/G)$.

が計算で示せる。 //

§5 応用

incidence matrix の線形代数的性質から直接得られる古典的諸定理は、同じ方法で拡張できる。例えば、

✻Th tight な design が、自己同型群 G をもてば、
G-tight である。

Fisher の不等式 より

✻Th (D.L. Kreher) 自己同型をもつ t-$(v,k,1)$ design において、$2s \leq t \Rightarrow |B/G| \geq |\binom{v}{s}/G|$

(Gが自明な場合は、Th 1 の Cor として、既に述べてある。)

以下では 2-$(v,k,1)$ design を考える。

$|B/G| = m$, $B/G = \{B_1, \cdots, B_m\}$

$|\binom{v}{s}/G| = n$ $\binom{v}{s}/G = \{S_1, \cdots, S_n\}$ とする。

Schutzenberger の定理 より

✻Th $\prod_{i=0}^{m} |B_i| \times \prod_{i=0}^{n} |S_i| \times \prod_{i=0}^{s} \left[\binom{k-i}{s-i} b_s^i\right]^{|\binom{v}{i}/G| - |\binom{v}{i-1}/G|}$ は
平方数

Bruck-Ryser-Chowla の定理 より

✻Th $Q = \sqrt{D'}^{-1} (N_s N_s^T) \sqrt{D'}^{-1}$ で表わされる
Q上の2次形式は、$\begin{pmatrix} |B_1| & & \\ & \ddots & \\ & & |B_m| \end{pmatrix}$ で表わされる2次形式を含まれる。ここで、$D' = \begin{pmatrix} |S_1| & & \\ & \ddots & \\ & & |S_n| \end{pmatrix}$.

特に $m \leq n+2$ なら Q の2次形式としての不等号に条件がつく。

注 今のところ行列式以外の不変量は計算できていないので実際に役に立つのは $m=n$ の場合（Schützenberger の定理）又は $(n,m)=(1,2),(1,3),(2,3),(2,4)$ の場合ぐらいであろう。

§6 今後の問題

残された問題は数多くある。

* 他にどんな定理が拡る表できるか。
* §4の前半の目地から見れば、$\mathrm{Th}1'$, $\mathrm{Th}2'$ は非常に限られた情報しか使っていない。他の情報は使えないか。

この方向では次のような結果がある。

2-$(v,k,1)$ design において、$r=b_0$, $m=b_1$ とする。

Th（吉田） R を $(n!)^{-1}$ を含むような単位的可換環、M を任意の RG-module とすると

$$Ext^m_{RP_0}(RP,M) \Big| Ext^m_{RG}(RB,M)$$

Cor. 特に $M=\mathbb{C}^*$ として、任意なる素数 l について、

$$\prod_{P\in P/G} (G_P/[G_P,G_P])_l \Big| \prod_{B\in B/G} (G_B/[G_B,G_B])_l .$$

Th (吉田)

$l \nmid nr \Rightarrow \sum_{p \in B/q} \#\{G_p \text{ の } l\text{-regular class}\}$

$\leq \sum_{p \in B/q} \#\{G_p \text{ の } l\text{-regular class}\}$

前の方の定理は比較的簡単なので、
一般のオへ拡張できるかもしれない。

* G-right な場合の B-R-C 定理をわかり易く述べる。
* Qの他の不変量の計算

§8 参考文献

ブロックデザイン一般については

・E.S.Lander (1983) Symmetric design ; London Math. Soc. Lecture Note series 74

二次形式については

・J.P.セール (1970) 数論講義 ; 岩波書店

主な結果は、

・R.M.Wilson Incidence Matrices of t-Designs ; LINEAR ALGEBRA AND ITS APPLICATONS 46:73-82 (1982)

・D. L. Kreher An Incidence Algebra for t-Designs With Automorphisms, JOURNAL of COMBINATORIAL THEORY, Series A 42: 251-261 (1986)

による。

巡回型ブロック・デザインの逐次構成
(グラフ・デザインの合成を中心として)

東京理科大学・理工　神保雅一
東京理科大学・理　　栗木進二

§1 Introduction.

Balanced incomplete block designs were generalized to balanced graph designs by Hell and Rosa[3]. They also studied the effect of products upon the decomposition of graphs into various subgraphs. Many authors considered these topics (see, for example, [1]-[6],[8] and [9]). In this paper, we consider a construction for cyclic graph designs by a product method.

Here, graphs are considered to be undirected unless otherwise stated. Edges are identified with pairs of endpoints but multiple edges and loops are allowed. V(G) denotes the vertex set of a graph G, and E(G) denotes the

Research supported in part by a Grant-in-Aid for Scientific Research of the Ministry of Education, Science and Culture under Contract Number 321-6009-61530017, and by Research Grant of Science University of Tokyo under Contract Number 86-1001.

multiset of edges of G. The number of vertices (*order* of G) and the number of edges are denoted by p(G) and e(G), respectively. The addition of two graphs G and H, $G \oplus H$, is defined by a graph with the vertex set $V(G \oplus H)=V(G) \cup V(H)$ and the edge set $E(G \oplus H)$ which is a collection of edges of G and H. λG denotes a graph such that a graph G is added λ times. Let H and G be graphs. If there is a family $\mathcal{G}=\{G_1, G_2, \ldots\}$ of subgraphs of H, which are isomorphic to a graph G, such that each edge of H is in precisely one member of $\mathcal{G}$, then $\mathcal{G}$ is said to be a *G-decomposition* of H. Then $H = G_1 \oplus G_2 \oplus \cdots$ holds.

The complete graph on v vertices, in which each vertex is joined precisely once to each other vertex, is denoted by K_v. A decomposition of λK_v into subgraphs isomorphic to a graph G of order k is called a *graph design* and denoted by a *(v, k, λ) G-design*. If G is a path, a circuit or a bipartite graph, then a G-design is called a *path design*, a *circuit design* or a *bipartite design*, respectively. If each vertex occurs in precisely the same number of subgraphs in the decomposition, then the G-design is said to be *balanced*. If there is a balanced (v,k,λ) G-design, then

$$\lambda v(v-1) = 2eb, \quad vr = bk, \quad \text{and} \quad \lambda(v-1) \equiv 0 \pmod{d},$$

hold, where e=e(G), b is the number of subgraphs of the G-decomposition, r is the number of subgraphs containing a given vertex of λK_v and d is the g.c.d. of the degrees of the vertices of G. We can easily verify that if G is a *regular* graph, which is defined to be a graph with the same

number of edges for each vertex, then a G-design is balanced. A K_k-decomposition of λK_v is simply a balanced incomplete block design.

A graph H is said to be *cyclic* if it has an automorphism of a single cycle of length v=p(H). If H is cyclic, then without loss of generality, we can assume that $V(H)=Z_v$, the residues of modulo v. And if {a,b} is an edge of H, then {a+c,b+c} (mod v) is also an edge of H. Let h_i be the number of edges {0,i}, in particular, h_0 is the number of loops {0,0}. Then obviously we have $h_i=h_{v-i}=h_{-i}$ for $i\in Z_v$. For a cyclic graph H, $H(x)=\sum_{i=0}^{v-1} h_i x^i$ is called a *characteristic polynomial* of H. While the following polynomial is called a *reciprocal characteristic polynomial* of H:

$$\overline{H}(x) = \begin{cases} \sum_{i=-(v-1)/2}^{(v-1)/2} h_i x^i & \text{if v is odd,} \\ \sum_{i=-v/2+1}^{v/2-1} h_i x^i + \frac{h_{v/2}}{2}(x^{v/2}+x^{-v/2}) & \text{if v is even.} \end{cases}$$

Let H and F be cyclic graphs of order $v_1=p(H)$ and $v_2=p(F)$ with a reciprocal characteristic polynomial $\overline{H}(x)$ and a characteristic polynomial F(y), respectively. A cyclic graph having a characteristic polynomial $\overline{H}(z)F(z^{v_1})$ with $z^{v_1 v_2}=1$ is called a *cyclic product* of H and F, denoted by H*F. Note that, in the case when v_1 is even, $h_{v_1/2}$ must be even in order that $\overline{H}(z)F(z^{v_1})$ is well-defined as a characteristic polynomial of a cyclic graph. Clearly, a cyclic product * is not commutative. Note that for cyclic

graphs H_1, H_2 and F, if $V(H_1)=V(H_2)$, then we have

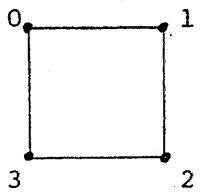
$$(H_1 \oplus H_2)*F = (H_1*F) \oplus (H_2*F),$$

and

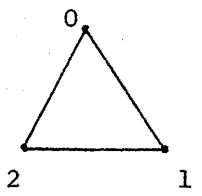
$$F*(H_1 \oplus H_2) = (F*H_1) \oplus (F*H_2).$$

Example 1. Let H and F be circuits of length 4 and 3, respectively. Then $\overline{H}(x)=x+x^{-1}$ and $F(y)=y+y^2$. Hence H*F is a cyclic graph of order 12 with a characteristic polynomial

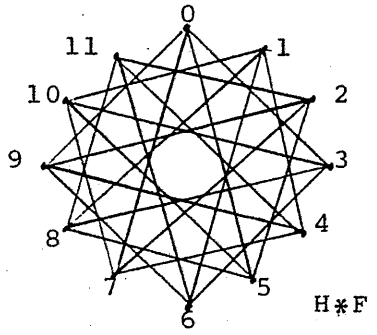
$$\overline{H}(z)F(z^4)=(z+z^{-1})(z^4+z^8)=z^3+z^5+z^7+z^9 \quad (z^{12}=1).$$



H



F



H*F

Lemma 1. Let $H=\lambda_1 K_{v_1}$ and $F=\lambda_2 K_{v_2}$, where λ_1 is even if v_1 is even. Then

$$\lambda_1\lambda_2 K_{v_1 v_2} = H*F \oplus \lambda_2 H*\mathbb{1}_{v_2} \oplus \lambda_1 \mathbb{1}_{v_1}*F \qquad (1)$$

holds, where $\mathbb{1}_{v_i}$ is a graph with v_i vertices and a loop for each vertex such that $V(\mathbb{1}_{v_1})=V(H)$ and $V(\mathbb{1}_{v_2})=V(F)$.

Proof. Let $\overline{H}(x)$ be a reciprocal characteristic polynomial of H and let H(x) be a characteristic polynomial of H. Then we have $H(x)=\lambda_1(x+x^2+\cdots+x^{v_1-1})$. Similarly, the characteristic polynomial of F is $F(y)=\lambda_2(y+y^2+\cdots+y^{v_2-1})$. Hence that of $F \oplus \lambda_2 \mathbb{1}_{v_2}$ is $F'(y)=F(y)+\lambda_2=\lambda_2(1+y+y^2+\cdots+y^{v_2-1})$. Note that $z^{v_1}F'(z^{v_1})=F'(z^{v_1})$ and $z^{-i}=z^{v_1(v_2-1)+v_1-i}$ for

any integer $0 \le i \le v_1/2$, when $z^{v_1 v_2}=1$. Then we have $\overline{H}(z)F'(z^{v_1})=H(z)F'(z^{v_1})$ for $z^{v_1 v_2}=1$. And the characteristic polynomial of $\lambda_1 \mathbb{1}_{v_1} * F$ is $\lambda_1 F(z^{v_1})$. Thus the characteristic polynomial of the right hand side of (1) is

$$\overline{H}(z)F'(z^{v_1})+\lambda_1 F(z^{v_1}) = \{\overline{H}(z)+\lambda_1\}F'(z^{v_1})-\lambda_1\lambda_2$$

$$=\lambda_1\lambda_2(1+z+z^2+\cdots+z^{v_1-1})(1+z^{v_1}+z^{2v_1}+\cdots+z^{(v_2-1)v_1})-\lambda_1\lambda_2$$

$$=\lambda_1\lambda_2(z+z^2+\cdots+z^{v_1 v_2-1}),$$

which is the characteristic polynomial of $\lambda_1\lambda_2 K_{v_1 v_2}$. □

Let G be a subgraph of a cyclic graph H of order v. A graph G+i is defined by $V(G+i)=\{g+i \pmod v \mid g \in V(G)\}$ and $E(G+i)=\{\{a+i,b+i\} \pmod v \mid \{a,b\} \in E(G)\}$. The set of graphs $\{G+i \mid i=0,1,2,\ldots\}$ is called an *orbit* of G. An orbit can be represented by any one of its graphs, which will be called a *base graph*. The smallest positive integer i such that G+i=G is called the *length* of an orbit. If i=v then an orbit is said to be *full* otherwise it is said to be *short*. For an orbit of length i with base graph G, let

$$\langle G \rangle = G \oplus (G+1) \oplus (G+2) \oplus \cdots \oplus (G+i-1).$$

If a cyclic graph H of order v is represented as $H=\langle G_1 \rangle \oplus \cdots \oplus \langle G_\alpha \rangle$ for G_ℓ's isomorphic to a graph G, then H is said to have a *cyclic G-decomposition*. In this paper, we consider only the case when any orbits corresponding to G_ℓ's are full. For each graph G_ℓ, let

$$\Delta G_\ell(x) = \sum_{\{i,j\} \in E(G_\ell)} (x^{i-j} + x^{j-i}).$$

Then $\overline{H}(x)=\Delta G_1(x)+\cdots+\Delta G_\alpha(x)$ holds. A cyclic G-decomposition of λK_v is called a *cyclic (v,k,λ) G-design*, where k is the order of G. Note that a cyclic G-design is always balanced.

Lemma 2. For an even integer v, if there exists a cyclic (v,k,λ) G-design with no short orbit, then λ must be even.

Proof. Let $H=\langle G_1\rangle\oplus\cdots\oplus\langle G_\alpha\rangle$ be a cyclic G-decomposition of λK_v. If the edge $\{0,\frac{v}{2}\}$ is contained in a graph $G_\ell+j$ for a certain ℓ and j, then it is also contained in a graph $G_\ell+j+\frac{v}{2}$. Since the cyclic G-decomposition has no short orbit, $G_\ell+j$ and $G_\ell+j+\frac{v}{2}$ must be distict. Thus the set of all graphs having the edge $\{0,\frac{v}{2}\}$ can be partitioned into pairs of graphs $(G_\ell+j, G_\ell+j+\frac{v}{2})$'s. Hence λ must be even. □

§2 Difference arrays and Graph arrays.

Let F be a cyclic graph of order v with a characteristic polynomial $F(y)=\sum_{p=0}^{v-1} f_p y^p$, then $f=F(1)=\sum f_p$ is the degree of each vertex. Let G be a *simple* graph, which is defined to be a graph with no loops and no multiple edges, with vertex set $V(G)=\{0,1,\ldots,k-1\}$. A $k\times f$ array $D=(d_{ij})$ is called an *(F,G)-difference array* if $d_{ij}\in Z_v$ and every vertex p of F occurs exactly f_p times among the differences $\{d_{ij}-d_{i',j} \pmod v \mid j=1,2,\ldots,f\}$ for any two rows i and i′ such that $\{i,i'\}\in E(G)$, that is,

$$\sum_{j=0}^{f} y^{d_{ij}-d_{i'j}} = F(y) \qquad (y^v=1) \qquad (2)$$

holds for any $\{i,i'\}\in E(G)$.

Example 2. (i) Let F be a cyclic graph of order 5 with a characteristic polynomial $F(y)=1+y+y^4$ and G be a path of length 4. Then the following array is an (F,G)-difference array:

0 0 0
0 1 4
0 0 0
0 1 4

(ii) Let F be K_5 with a loop on each vertex and G be K_4, then the following array is an (F,G)-difference array:

0 0 0 0 0
0 1 2 3 4
0 2 4 1 3
0 3 1 4 2

In the case when a cyclic graph F is the complete graph K_v with a loop on each vertex, a $(\lambda F, K_k)$-difference array is called a *(v,k,λ) row difference scheme*, which is useful to construct cyclic BIB designs (see Jimbo and Kuriki[7]).

If there is a mapping ψ from V(G) onto a set of n colors such that $\psi(a)\neq\psi(b)$ for any $\{a,b\}\in E(G)$, then a graph G is said to be n-colorable.

Lemma 3. If G is 2-colorable then an (F,G)-difference array exists for any cyclic graph F.

Proof. We have the lemma by constructing an array such that the rows corresponding to the first color are all zero and

in the rows corresponding to the second color, every vertex p of F adjacent to the vertex 0 occurs f_p times, where $F(y)=\sum f_p y^p$ is a characteristic polynomial of F. □

Let G be a simple graph of order k=p(G) with e=e(G) edges. Let G^* be a directed graph obtained from G by replacing each edge by two arcs, one directed each way, between the same vertices. A k×2e matrix $A=(a_{ij})$ with elements from $V(G)=\{0,1,\ldots,k-1\}$ is called a *graph balanced array* for G, if every arc of G^* occurs exactly once in the set of ordered pairs $\{(a_{ij},a_{i'j})\,|\,j=1,2,\ldots,2e\}$, for any $\{i,i'\}\in E(G)$.

Lemma 4. A graph balanced array exists for any 2-colorable graph G.

An m×N matrix A with entries from a set of s(≥2) elements is called an orthogonal array of size N, m constraints, s levels, strength t and index λ, if any t×N submatrix of A contains all possible t×1 column vectors with the same frequency λ.

Lemma 5. If there exists an orthogonal array of size k^2, k+1 constraints, k levels, strength 2 and index 1, then a K_k-array exists.

Proof. Without loss of generality, we can assume that a $(k+1)\times k^2$ orthogonal array $A=(a_{ij})$ is standarized as follows:

$$a_{k+1,qk+r}=q \quad \text{for any } 0\le q\le k-1 \text{ and } 1\le r\le k,$$

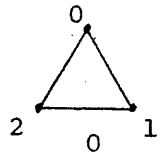
and

$$a_{i,k(k-1)+j}=j-1 \quad \text{for any } 1\le i\le k \text{ and } 1\le j\le k.$$

Then the submatrix $\tilde{A}=(a_{ij})$ $(i=1,\ldots,k; j=1,\ldots,k(k-1))$ is a K_k-array. □

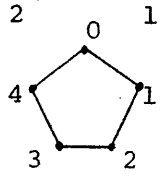
Example 3. The followings are graph balanced arrays for graph G's which are not 2-colorable and $k\leq 5$ except K_4 and K_5:

(i)



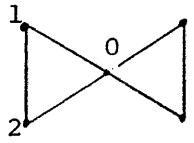
0	1	2	0	1	2
1	2	0	2	0	1
2	0	1	1	2	0

(ii)



0	1	2	3	4	0	1	2	3	4
1	2	3	4	0	4	0	1	2	3
2	3	4	0	1	3	4	0	1	2
3	4	0	1	2	2	3	4	0	1
4	0	1	2	3	1	2	3	4	0

(iii)



0	1	1	2	0	2	0	3	3	4	0	4
1	0	2	1	2	0	3	0	4	3	4	0
2	2	0	0	1	1	4	4	0	0	3	3
1	0	2	1	2	0	3	0	4	3	4	0
2	2	0	0	1	1	4	4	0	0	3	3

But the existence problem of graph balanced arrays is not solved, in general.

The following theorem shows a way to construct an (F,G)-difference array by using a graph balanced array.

Theorem 1. Let G be a simple graph with a graph balanced array. If a cyclic graph F has a cyclic G-decomposition with no short orbit, then there exists an (F,G)-difference array.

Proof. Let $F=\langle G_1\rangle\oplus\cdots\oplus\langle G_\alpha\rangle$ be a cyclic G-decomposition, where G_ℓ's are isomorphic to a graph G with k vertices and e edges. Then we have $\overline{F}(y)=\Delta G_1(y)+\cdots+\Delta G_\alpha(y)$. Let $\varphi_\ell: V(G)\to V(G_\ell)$ be isomorphisms. For a $k\times 2e$ G-array $A=(a_{ij})$, let $D_\ell=(\varphi_\ell(a_{ij}))$ for $\ell=1,2,\ldots,\alpha$. Then every arc of G_ℓ^* occurs exactly once in the set of ordered pairs

$\{(\varphi_\ell(a_{ij}),\varphi_\ell(a_{i',j}))\mid j=1,2,\ldots,2e\}$ for any $\{i,i'\}\in E(G)$, where G_ℓ^* is a directed graph corresponding to a graph G as before. Hence we have

$$\sum_{j=1}^{2e} y^{\varphi_\ell(a_{ij})-\varphi_\ell(a_{i',j})} = \Delta G_\ell(y).$$

Thus a $k\times 2e\alpha$ array $D=[\, D_1\ D_2\ \cdots\ D_\alpha\,]$ is an (F,G)-difference array. □

§3 A product theorem for cyclic decompositions.

In this section we consider a composition method (or a product method) of two cyclic G-decompositions.

The following lemma is ovbious:

Lemma 6. If cyclic graphs H and F with V(H)=V(F) have cyclic G-decompositions, then $H\oplus F$, λH and $1_v * H$ have cyclic G-decompositions, where the graph 1_v is a cyclic graph of order v with a loop for each vertex and no other edges.

Theorem 2. Let G be a simple graph. Let H and F be cyclic graphs. If

(i) H has a cyclic G-decomposition with no short orbit, and if

(ii) there is an (F,G)-difference array,

then the cyclic product H*F has a cyclic G-decomposition with no short orbit.

Proof. Let a $k\times f$ array $D=(d_{ij})$ be an (F,G)-difference array. Let $H=\langle G_1\rangle\oplus\cdots\oplus\langle G_\alpha\rangle$ be a cyclic G-decomposition, where G_ℓ's are isomorphic to G. Then we have

$\overline{H}(x)=\Delta G_1(x)+\cdots+\Delta G_\alpha(x)$. Let $\varphi_\ell: V(G)=\{0,1,\ldots,k-1\}\longrightarrow V(G_\ell)$ be an isomorphism. For each base graph G_ℓ of H, construct base graphs $G_{\ell j}$ $(j=1,2,\ldots,f)$ of H*F which have vertex sets

$$V(G_{\ell j})=\{\varphi_\ell(i)+v_1 d_{ij} \mid i \in V(G)\} \pmod{v_1 v_2}$$

and which is isomorphic to G, where v_1 and v_2 are the orders of H and F, respectively. Then we obtain by (2)

$$\begin{aligned}\sum_{j=1}^{f} \Delta G_{\ell j}(z) &= \sum_{j=1}^{f} \sum_{(i,i')\in E(G^*)} z^{\varphi_\ell(i)-\varphi_\ell(i')+v_1(d_{ij}-d_{i'j})} \\ &= \sum_{(i,i')\in E(G^*)} z^{\varphi_\ell(i)-\varphi_\ell(i')} \sum_{j=1}^{f} z^{v_1(d_{ij}-d_{i'j})} \\ &= \Delta G_\ell(z)\cdot F(z^{v_1}),\end{aligned}$$

where $z^{v_1 v_2}=1$. Hence

$$\begin{aligned}\overline{H}(z)\cdot F(z^{v_1}) &= \sum_{\ell=1}^{\alpha} \Delta G_\ell(z)\cdot F(z^{v_1}) \\ &= \sum_{\ell=1}^{\alpha} \sum_{j=1}^{f} \Delta G_{\ell j}(z),\end{aligned}$$

which implies that H*F can be decomposed cyclically by base graphs $G_{\ell j}$'s. Hence the theorem is proved. □

By combining Theorems 1 and 2, we obtain the following corollary:

Corollary 1. If cyclic graphs H and F have cyclic G-decompositions with no short orbit, and if there is a graph balanced array for G, then a cyclic G-decomposition of H*F exists.

The following corollary is the direct consequence of Theorem 2 and Lemma 3.

Corollary 2. Let a simple graph G be 2-colorable. If H has a cyclic G-decomposition with no short orbit, then for any cyclic graph F, H*F has a cyclic G-decomposition with no short orbit.

Corollary 3. Under the same assumption as Theorem 2 $H*(F\oplus\lambda\mathbb{1})$ has a cyclic G-decomposition with no short orbit, where $V(F)=V(\mathbb{1})$.

Proof. Note that $H*(F\oplus\lambda\mathbb{1})=(H*F)\oplus(\lambda H*\mathbb{1})$ and that $p(G)\times 1$ zerovector is an $(\mathbb{1},G)$-difference array. Hence $H*\mathbb{1}$ has a cyclic G-decomposition with no short orbit by Theorem 2. Thus the corollary is proved by Lemma 6. □

Theorem 3. Let G be an n-colorable simple graph of order k. If there are

(i) a cyclic (v_1,k,λ_1) G-design with no short orbit,

(ii) a cyclic $(v_2,k,\lambda_1\lambda_2)$ G-design with no short orbit and

(iii) a (v_2,n,λ_2) row difference scheme,

then there exists a cyclic $(v_1v_2,k,\lambda_1\lambda_2)$ G-design with no short orbit.

Proof. We have only to show that the graph $\lambda_1\lambda_2K_{v_1v_2}$ has a cyclic G-decomposition. Let $A_1,\ldots,A_n$ be n color classes of G. Let $D=(d_{ij})$ be a (v_2,n,λ_2) row difference scheme. Construct a $k\times\lambda_2v_2$ array $\tilde{D}$ as follows: Let every vertex of G correspond to a row of an array $\tilde{D}$ arbitrarily. And make copies of the i-th row of D to the rows which correspond to vertices of A_i for every i. Then it is easily shown that the array $\tilde{D}$ is a $(\lambda_2(K_{v_2}\oplus\mathbb{1}_{v_2}),G)$-difference array. From

the assumption (i), $\lambda_1 K_{v_1}$ has a cyclic G-decomposition with no short orbit. Hence by Theorem 2, the cyclic graph $\lambda_1 K_{v_1} * \lambda_2 (K_{v_2} \oplus 1_{v_2})$ has a cyclic G-decomposition with no short orbit. And $1_{v_1} * \lambda_1 \lambda_2 K_{v_2}$ has a cyclic G-decomposition with no short orbit by Lemma 6. Finally, by (1) of Lemma 1

$$\lambda_1 \lambda_2 K_{v_1 v_2} = \{ \lambda_1 K_{v_1} * \lambda_2 (K_{v_2} \oplus 1_{v_2}) \} \oplus (1_{v_1} * \lambda_1 \lambda_2 K_{v_2}),$$

we have the theorem. □

The following theorem can be shown from Corollary 1 by the similar argument to Theorem 3:

Theorem 4. Let G be a graph of order k with a graph balanced array. If there are

(i) a cyclic (v_1, k, λ_1) G-design with no short orbit and

(ii) a cyclic (v_2, k, λ_2) G-design with no short orbit,

then a cyclic $(v_1 v_2, k, \lambda_1 \lambda_2)$ G-design with no short orbit.

References.

[1] J.C. Bermond and D. Sotteau, Graph decompositions and G-designs, Proc. 5-th British Combinatorial Conf. (1975), 53-72.

[2] H. Enomoto and K. Ushio, C_k-factorizations of the complete bipartite graphs (in Japanese), Kyoto Univ. Inst. Math. Kokyuuroku 587 (1986), 52-57.

[3] P. Hell and A. Rosa, Graph decompositions, Handcuffed prisoners and balanced P-designs, Discrete Math. 2 (1972), 229-252.

[4] J.D. Horton, Resolvable path designs, J. Combi. Theory (A) 39 (1985), 117-131.

[5] C. Huang and A. Rosa, On the existence of Balanced bipartite designs, Utilitas Math. 4 (1973), 55-75.

[6] C. Huang, Resolvable balanced bipartite designs, Discrete Math. 14 (1976), 319-335.

[7] M. Jimbo and S. Kuriki, On a composition of cyclic 2-designs, Discrete Math. 46 (1983), 249-255.

[8] A. Rosa and C. Huang, Another class of balanced graph designs: Balanced circuit designs, Discrete Math. 12 (1975), 269-293.

[9] S. Yamamoto et al., On claw-decomposition of complete graphs and complete bigraphs, Hiroshima Math. J. 5 (1975), 33-42.

有限射影平面入門

中川 暢夫(近畿大・理工)

§1 Introduction

二つの結合構造 $\mathbb{P}=(\mathcal{P},\mathcal{L},I)$, $\mathbb{A}=(\mathcal{P}_1,\mathcal{L}_1,I_1)$ を定義する。$\mathcal{P}$ 及び $\mathcal{P}_1$ の元を点とよび大文字で, $\mathcal{L}$ 及び $\mathcal{L}_1$ の元を直線とよび小文字でかくことにする。また PIl (PI_1l) のとき点 P は直線 l 上にある, あるいは直線 l は点 P をとおるという。

$\mathbb{P}=(\mathcal{P},\mathcal{L},I)$ が projective plane

$\Leftrightarrow$ (P1) 二点 P,Q $(P\neq Q)$ をとおる直線は唯一つ存在する。

(P2) 二直線 l,m $(l\neq m)$ 上に唯一つの点が存在する。

(P3) 非退化な四点が存在する。
(四点 A,B,C,D でこのうちどの三点も同一直線上にないもの)

$\mathbb{A}=(\mathcal{P}_1,\mathcal{L}_1,I_1)$ が affine plane $\overset{\text{def}}{\Leftrightarrow}$

(A1) : (P1) と同じ
二直線 l と m が平行 $\overset{\text{def}}{\Leftrightarrow}$ $l=m$ または l,m 上に共通の点が存在しない. ($l\parallel m$ とかく)

(A2) $\forall l\in\mathcal{L}_1$, $\forall P\in\mathcal{P}_1$ に対し, $\exists!\, m\in\mathcal{L}_1$ s.t. $m\parallel l$, PIm.

(a3) 非退化な三点が存在する。

(a1), (a2) の下で "∥"（平行関係）は同値関係となる。直線の各平行類をpencilとよび，異なるすべてのpencilの集合を Π であらわす。

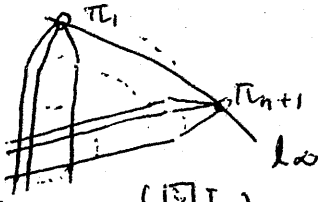
$\mathbb{P}$ に対して次のような自然数 n が定まる。

点Pをとおる直線の集合を (P)，直線 l をとおる点の集合を (l) とかくと，$|(P)| = |(l)| = n+1$ $(\text{for } {}^\forall P \in \mathcal{P}, {}^\forall l \in \mathcal{L})$，$|\mathcal{P}| = |\mathcal{L}| = n^2+n+1$。$n$ を $\mathbb{P}$ の位数という。

affine plane $\mathbb{A}$ から自然に projective plane $\mathbb{P}(\mathbb{A})$ が構成される。（図I参照）

$\mathbb{P}(\mathbb{A})$ の points : $\mathcal{P}_1 \cup \Pi$

$\mathbb{P}(\mathbb{A})$ の lines : $\mathcal{L}_1 \cup \{l_\infty\}$



（図I）

$\mathbb{P}(\mathbb{A})$ の結合関係 I_1^* は I_1 の拡張で，

${}^\forall \pi \in \Pi$, ${}^\forall l \in \mathcal{L}_1$ に対し $\pi \ni l \iff \pi I_1^* l$

$\pi I_1^* l_\infty$ $({}^\forall \pi \in \Pi)$　$P I_1^* l_\infty$ $({}^\forall P \in \mathcal{P}_1)$

$\mathbb{P}(\mathbb{A})$ の位数が n のとき，$\mathbb{A}$ の位数は n，という。$|\Pi| = |(A)| = n+1$ $({}^\forall A \in \mathcal{P}_1)$

$|(a)| = |\pi| = n$ $({}^\forall a \in \mathcal{L}_1, {}^\forall \pi \in \Pi)$

$|\mathcal{P}_1| = n^2$, $|\mathcal{L}_1| = n^2+n$

逆に projective plane $\mathbb{P}$ と $\mathbb{P}$ の各直線 l から，$\mathbb{P}$ の内部構造として affine plane $\mathbb{P}^l$ が構成される。

$\mathbb{P}^l$ の points : $\mathcal{P}\setminus(l)$, $\mathbb{P}^l$ の lines ; $\mathcal{L}\setminus\{l\}$

このように affine plane を考えることと，projective plane を考えることはほぼ同じとみてよい。projective plane の方が対称性に富んでいるが，affine plane を考える方がみやすい場合もある。

(例1) 有限体 $K=GF(q)$

points : $K\times K$, lines : $y=mx+t$ or $x=v$ ($m, t, v \in K$) 包含関係を relation として desarguesian affine plane $A(K)$ が得られる。

(例2) $k=GF(q)$, V : k 上3次元 vector space

points : V の1次元 subspaces

lines : V の2次元 subspaces

包含関係を relation として desarguesian projective plane $\mathbb{P}(K)$ が得られる。

(Def) 二つの projective plane $\mathbb{P}=(\mathcal{P}, \mathcal{L}, I)$, $\mathbb{P}'=(\mathcal{P}', \mathcal{L}', I')$ に対し，$\mathbb{P}$ から $\mathbb{P}'$ への (pts から pts ,

linesからlinesへの)bijection φが結合関係を保つとき，φを$\mathbb{P}$から$\mathbb{P}'$への同型写像という。($P I l \rightleftarrows \varphi(P) I' \varphi(l)$)

$\mathbb{P}$から$\mathbb{P}'$への同型が在るとき $\mathbb{P} \cong \mathbb{P}'$ とかいて $\mathbb{P}$と$\mathbb{P}'$は同型であるという。

特に$\mathbb{P}=\mathbb{P}'$のとき，上のφを$\mathbb{P}$のcollineationとよぶ。affine plane $\mathbb{A}$, $\mathbb{A}'$に対しても，$\mathbb{A}$から$\mathbb{A}'$への同型写像及び$\mathbb{A}$のcollineationを上と同様に定義する。

- φが$\mathbb{A}$のcollineation $\rightleftarrows$ φが$\mathbb{P}(\mathbb{A})$のcollineationかつ$\varphi(l_\infty)=l_\infty$
- $K=GF(q)$のとき，$\mathbb{P}(\mathbb{A}(K)) \cong \mathbb{P}(K)$
  ($\mathbb{P}(K)$の任意の直線lに対して) $\mathbb{P}(K)^l \cong \mathbb{A}(K)$

§2 Translation plane

$\mathbb{A}$をaffine planeとする。$P+Q := (P$とQをとおる唯一つのline$)$ $(P \neq Q$のとき$)$

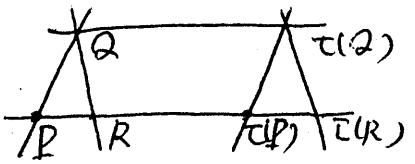
τが$\mathbb{A}$のcollineationで次の条件(i)，(ii)をみたすときτを$\mathbb{A}$のtranslationという。

(i) $P+Q \parallel \tau(P)+\tau(Q)$ $(\forall P, \forall Q \in \mathfrak{I}_1,\ P \neq Q)$

(i.e τは平行性を保つ)

(ii) $\tau(X) \neq X \quad (\forall X \in \mathcal{P}_1)$

○ translation τ は一点Pの像により一意的に決まる。(図II参照)



$P+\tau(P) \parallel Q+\tau(Q)$

$P+Q \parallel \tau(P)+\tau(Q)$

AをBに移すtranslationが存在すればこれをτ_{AB}とかく。

○ $\{P+\tau(P) \mid {}^{\forall}P \in \mathcal{P}_1\}$ はAの1つのpencil π となる。且つ $\tau(l)=l \rightleftarrows l \in \pi$。

π を τ の方向とよぶ。

{translations of A} を $\mathcal{T}$ とすると、$\mathcal{T}$ は写像の合成に関して群をなす。(Aのtranslation group)

各pencil π に対して

$\{\tau \in \mathcal{T} \mid \tau$ の方向が $\pi\}$ を $\mathcal{T}(\pi)$ とすると、

$\mathcal{T}(\pi) \lhd \mathcal{T}$ 且つ $\mathcal{T}(\pi_1) \cap \mathcal{T}(\pi_2) = \{1\}$ $(\text{if } \pi_1 \neq \pi_2)$

$(1=id_A$ も便宜上translationと考える。)

(Def) $\mathcal{T}$ がAの点集合 $\mathcal{P}_1$ 上可移に働くときAをtranslation planeという。

(i.e ${}^{\forall}A, {}^{\forall}B \in \mathcal{P}_1$ に対して $\exists! \tau_{AB} \in \mathcal{T}$)

またこのとき $\mathbb{P}(A)$ を、無限遠直線 l_∞ をtranslation

line とする projective translation plane
という。 T は l_∞ の各点を固定し, π をとおる
各直線を固定する。

○ $\mathbb{P}$: projective plane, $l \neq m$ で l, m が
$\mathbb{P}$ の translation line $\Rightarrow \mathbb{P} \cong \mathbb{P}(K)$ ($\exists K$ 有限体)
($\mathbb{P}$ desarguesian)

以下 translation plane $\mathcal{A}$ を考えることは
次のような対象 $(\mathcal{A})$ を考えることと同じであること
を説明する。

$(\mathcal{A})$ $K = GF(q)$, V は K 上 $2d$ 次元 vector space

$(\mathcal{A}1)$ $\mathcal{S} \subseteq \{V$ の d 次元 vector spaces$\}$ and
$|\mathcal{S}| \geq 3$

$(\mathcal{A}2)$ $V = \bigcup_{X \in \mathcal{S}} X$ and $X \cap Y = \{0\}$ if $X \neq Y$
$(X, Y \in \mathcal{S})$

$\mathcal{S}$ を V の spread とよぶ。 d を spread
$(V, \mathcal{S})$ または translation plane $\mathcal{A}(V, \mathcal{S})$
の Ostrom dimention という。

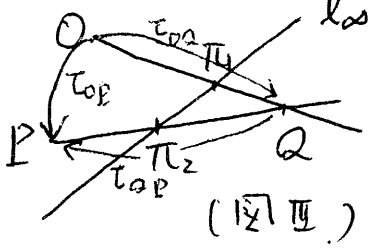
$\mathcal{A}$: translation plane とすると
(a3) より 非退化な三点 A, B, C がある。

$\tau_{AB} \neq 1$, $\tau_{BC} \neq 1$, $\tau_{CA} \neq 1$

$A+B \in \pi_1$, $B+C \in \pi_2$, $C+A \in \pi_3$ とすると

π_1, π_2, π_3 は互いに異なり, $T(\pi_1) \neq 1$
$T(\pi_2) \neq 1$. $T(\pi_3) \neq 1$. このことより
(イ) T : 可換群
(ロ) $\mathcal{S} := \{T(\pi) \mid \pi \in \Pi\}$ で $|\mathcal{S}| \geqq 3$
(ハ) $T = \bigcup_{\pi \in \Pi} T(\pi)$
(ニ) $T = T(\pi_1) \times T(\pi_2)$ if $\overset{\forall}{\pi_1} \neq \overset{\forall}{\pi_2}$ $(\pi_1, \pi_2 \in \Pi)$
が成立する。 (ニ)は成立のこと 次の図Ⅲ参照

$\left(\overset{\forall}{O}, \overset{\forall}{P} \in \Sigma_1 \right.$
$\left. \tau_{OP} = \tau_{QP} \cdot \tau_{OQ} \right)$



(図Ⅲ)

T と $\mathcal{S}$ より新しい translation plane $\mathbb{A}'$ が自然に構成される。T を加法群と考える。
$\mathbb{A}'$ の points ; T の各 elements
$\mathbb{A}'$ の lines ; $T(\pi) + a$ $(\overset{\forall}{\pi} \in \Pi, \overset{\forall}{a} \in T)$
結合関係として包含関係を考える。
$T(\pi_1) \cap T(\pi_2) = \{1\}$ $(\text{if } \pi_1 \neq \pi_2)$ に注意すれば
条件 (ロ), (ハ), (ニ) より $\mathbb{A}'$ は (a1), (a2), (a3) を満たす。
$\overset{\forall}{b} \in T$ に対して $\tau_b(x) = x + b$ $(\forall x \in T)$
$T' = \{\tau_b \mid b \in T\}$ とおくと T' は $\mathbb{A}'$ の translation group で T' は T 上可移に働き, $T \cong T$

(as group) が成り立つ。 O を $\mathbb{A}$ の一点とする。

$\mathbb{A} \xrightarrow{\varphi} \mathbb{A}'$, $\varphi(P) = \tau_{OP}$, $P \in l \in \Pi$ のとき $\varphi(l) = T(\pi) + \tau_{OP}$ と定義すると

$\varphi(l)$ は l 上の点 P によらずに一意的に定まり, φ は結合関係を保存する bijection となる。(i.e $\mathbb{A} \cong \mathbb{A}'$)

$\mathbb{A} \longrightarrow (T, \mathcal{S}) \longrightarrow \mathbb{A}(T, \mathcal{S}) \overset{\text{put}}{=} \mathbb{A}' \longrightarrow (T', \mathcal{S}')$

$(T', \mathcal{S}')$ は $(T, \mathcal{S})$ と同一視できる。

故に translation plane $\mathbb{A}$ を考えることと条件(I), (II), (III), (IV) をみたす $(T, \mathcal{S})$ を考えることは同じことである。

以下 $T = V$, $\mathcal{S} = \{X, Y, Z, \cdots\}$ とする。

$K(V, \mathcal{S}) = \{ f \in \mathrm{End}_{\mathbb{Z}}(V) \mid f(X) \subseteq X \ (\forall X \in \mathcal{S}) \}$

とおくと, $K(V, \mathcal{S})$ は条件 (II), (III), (IV) がきいて体をなす。 $K = K(V, \mathcal{S})$ とおく。

$f(a) = f \cdot a$ ($\forall f \in K$, $\forall a \in V$) で V は K-vector space をなし, X は K-subspace となる。($\forall X \in \mathcal{S}$) $\forall X, \forall Y \in \mathcal{S}$ に対して

$V = X \oplus Z = Y \oplus Z$ なる $Z \in \mathcal{S}$ が存在する。($\because |\mathcal{S}| \geq 3$) 故に $X \cong V/Z \cong Y$ (as K-vector space)

$\dim(X) = d$ とおく ($\forall X \in \mathcal{S}$)
このとき $\dim(V) = 2d$ となり 対象(☆)
が導かれる。

○ $d=1 \rightleftarrows A(V,\mathcal{S})$ が desarguesian plane

○ $\mathcal{S}$ は0をとおる直線の集合, $|K| = q$ とすると
$|\mathcal{S}| = q^d + 1$ となり, $A(V,\mathcal{S})$ の位数は
q^d (i.e translation plane の位数は常に
素数巾となる。)

$X, Y \in \mathcal{S}$, $(X \neq Y)$ に対して $V = X \oplus Y$
$X \underset{K}{\cong} Y$ より $V = X \oplus X$ (outer sum) として
よい。 $\mathcal{S}$ に $GL(V)$ の適当な変換を施す
ことにより, $V(0) = \{(x,0) \mid x \in X\}$, $V(\infty) = \{(0,x)$
$\mid x \in X\}$, $V(1) = \{(x,x) \mid x \in X\}$ が $\mathcal{S}$ の元として
よいことがわかる。 また $Z \in \mathcal{S}$, $Z \neq V(0)$
$Z \neq V(\infty) \Rightarrow \exists \sigma \in GL(X)$ s.t $Z = \{(x, x^\sigma)$
$\mid x \in X\}$

§3 Collineation group

$A = A(V,\mathcal{S})$; translation plane で
$V = X \oplus X$ とする。
次の定理が成り立つ。

○ σ が $\mathbb{A}$ の collineation, $\sigma(0)=0$
$\Rightarrow \sigma \in \Gamma L(V)$

○ σ が $\mathbb{A}$ の collineation, $\sigma(0)=0$
$\rightleftarrows$ $\sigma \in \Gamma L(V)$ and $\sigma(Y) \in \mathcal{S}$ for $^{\forall} Y \in \mathcal{S}$

$\mathbb{A}$ を non-desarguesian とすると 6P の注意より $Aut(\mathbb{A}) = Aut(\mathbb{P}(\mathbb{A})) \overset{put}{=} H$

上の定理より $H_0 \subseteq \Gamma L(V)$
(stabilizer of 0)

$C(\mathbb{A}) = H_0 \cap GL(V)$ を $\mathbb{A}$ の linear complement とよぶ。

$H/C(\mathbb{A})\cdot T \cong Aut(K)$ cyclic group ($\because H = H_0 \cdot T$)

$C(\mathbb{A})\cdot T/T \cong \mathbb{C}(\mathbb{A})$, T: elementary abelian p-group ($^{\exists}p$: 素数)

故に $C(\mathbb{A})$ の構造が わかれば $\mathbb{A}$ の full collineation group H の構造が わかる。 $\lambda \in K(V,\mathcal{S})^*$ に対して $d_\lambda(x,y) = (\lambda(x), \lambda(y))$ $(^{\forall}x, ^{\forall}y \in X)$ と定義すると d_λ は $\mathbb{A}(V,\mathcal{S})$ の collineation である。

$\Delta(0, l_\infty) \overset{put}{=} \{ d_\lambda \mid \lambda \in K(V,\mathcal{S})^* \} \cong K(V,\mathcal{S})^*$

(as group) $(d_\lambda \longleftrightarrow \lambda)$, $\Delta(0, l_\infty) \lhd C(\mathcal{A})$

§4 これからの課題

$C(\mathcal{A})$ が可解群の場合は Ostrom dimention d がいくらでも大きい例が知られている。(generalized André planes, semi-field planes) また主に $d=2$ に対して非常に多くの planes が構成されている。それ故 同型により plane を分類するのは絶望的に思われる。

$C(\mathcal{A})$ が非可解群の場合は少し見とおしがたつ。$C(\mathcal{A})$ の非可解極小正規部分群 G_T と, G_T に真に含まれる $C(\mathcal{A})$ の極大正規部分群 H を考える。H が $V\setminus\{0\}$ 上 正則に働くときは $H = Z(G_T)$ となり $G_T/Z(G_T)$ は同型な m 個の単純群の直積となる。$(\exists m \in \mathbb{N})$ G_T が V 上既約のとき $m \geq 2$ の例はない。以下 $m=1$ とする。G_T が V 上既約で d が奇数ならば $G_T/Z(G_T) \cong Su(2^{2r+1})$, A_7 or $PSL(2, p^n)$ また $d=2$ で p^{nt} $\mathrm{char}(K(V,\vartheta)) > 5$ ならば

$G/Z(G) \cong PSL(2,5)$, $PSL(2,9)$ or $PSL(2,p^n)$
Ostrom dimention d の 2-part が大きくなるとき $A(V,\mathcal{S})$ の扱いが難しくなる。

(課題1) $G/Z(G)$ が前述の単純群の一つと同型なとき, $A(V,\mathcal{S})$ を分類せよ。

(課題2) G が V 上既約のとき, $m \geq 2$ の plane の非存在を示すか, そのような例を作れ。

(課題3) d の 2-part が大きいときも, $G/Z(G)$ の可能性をしらべよ。

次に H が $V\setminus\{0\}$ 上非正則に働くときは, G は $C(A)$ の正規部分群 W を含み, W は elementary abelian w-群 または extra-special w-group に近い構造をもつ。
また W は $V\setminus\{0\}$ 上非正則に働き, 後者においては $Z(W)$ が $V\setminus\{0\}$ 上正則に働く。($\exists w$: 素数)

(課題4) W を手がかりに V の patial spread $\mathcal{S}_0$ をつくり, G-不変を保ちながら $\mathcal{S}_0$ を V の spread $\mathcal{S}$ にまで拡張せよ。(具体的群 G を与えて)。

$C(A)$ が非可解群で, G が V 上既約に働

くとき，$d=2$ に対しては分類できる望みがある。

$C(A)$ が非可解のとき，$d \geq 5$ の例は知られていない。

文献

(1) E. Artin ; Geometric Algebra , Interscience 1957

(2) H. Lüneburg ; Translation Planes , Springer-Verlag 1980

(3) G. Mason ; Orthogonal geometries over GF(2) and actions of extra-special 2-groups on translation planes , Eur. J. Comb. (1983) 4, 347－357

(4) G. Mason and T. G. Ostrom ; Some translation planes of order p^2 and of extra-special type , Geom. Ded 17, 307－322 (1985)

(5) T. G. Ostrom ; Lectures on finite translation planes . Univ. Bari , (1983)

可約非可解な自己同型群をもつ位数 p^2 の plane について.

大阪大学 教養部　平峰 豊

1. Introduction

p を素数, V を位数 p^{2r} の基本可換 p 群とする。V の位数 p^r の部分群 $W_1, \cdots, W_m$ $(m = p^r+1)$ からなる集合 $\mathcal{S}$ で次の条件をみたすものを V 上の spread という。

$$\mathcal{S} = \{W_1, \cdots, W_m\}, \quad |W_i| = p^r, \quad m = p^r+1$$

$$V^* (= V - \{0\}) = W_1^* \cup \cdots \cup W_m^* \quad (disj.)$$

spread が与えられると, V の元を点, すべての剰余類 $v + W_i$ $(v \in V, 1 \leqq i \leqq m)$ を直線, 結合関係を集合としての包含関係 とすることにより位数 p^r の affine plane が構成できる。([4] §1)

V を素体 $K = GF(p)$ 上のベクトル空間とみて $\overline{G} = GL(V)$ とおく。V 上の spread $\mathcal{S}'$ で $\mathcal{S}' = \mathcal{S}^g$, $g \in \overline{G}$ となるものは同型な affine plane を定めるので, 同値であるといい同一視する。$\mathcal{S}$ を全体として不変にする $\overline{G}$ の元全体 $C = C_{\mathcal{S}}$ $(= \{g \in \overline{G} \mid \mathcal{S}^g = \mathcal{S}\})$ は complement と呼ばれそれぞれの spread がもつ

"幾何的性質"が、ここによく反映される。$N = C^{(\infty)}$（Cの交換子群列の最終項），$\mathrm{sol}(N) = N$の最大可解正規部分群とおくとき，現在までに見つかっているspreadについては次のようになっている。

$N/\mathrm{sol}(N) \simeq 1$, $PSL(2,11)$, $Sz(2^{2r+1})$, $A_5 \times A_5$.

ここで (i) $N \simeq SL(2,5) \times SL(2,5)$, (ii) $\mathrm{sol}(N) \simeq$ 位数32の extra special 2-群 で $N/\mathrm{sol}(N) \simeq PSL(2,5)$ を除外すれば、$|\mathrm{sol}(N)| \leq 2$.

$N \neq 1$ である多くの実例では、V を射影空間とみて、spreadがこの中の"曲面"と関連して幾何的に意味をもつものが多い。spreadについて最もよく研究され、興味をもたれているのは次の問題である。

<問題> (抽象)群 G_0 を与えよ。このとき

$C_S \geq G \simeq G_0$ となる spread S を決定せよ。

知られているspreadのあるものは、この方法で特徴付けられている。([4] §31, §49, [5])

C_S の位数2の元の次の性質が、G_0 の可能性を強く制限する。

(Baer [4] 系4.6) C_S の位数の2の元 t は $t = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ (ただし $p>2$) または $|C_V(t)|^2 = |V|$,

ここで $C_V(t)=\{v\in V \mid vt=v\}$

$r=1$ (i.e. $|V|=p^2$) の時は spread の定義より spread は位数 p の部分群全体からなるものに限るが、対応する affine plane は位数 p のデザルグ平面である。$r=2$ の時 (i.e. $|V|=p^2$) は、$p\neq 2$ なら多くの同値でない spread があることが知られている。

$C_8\geq G$, $G^{(\infty)}=N$ とするとき次が示される。

<u>命題</u> $|V|=p^4$ で、V が G-可約ならば

(1) $N\simeq SL(2,p)$

(2) $5\mid p^2-1$ かつ $N\simeq SL(2,5)$ または

(3) $5\mid p^2-1$ かつ $N\simeq SL(2,5)\times SL(2,5)$

のいずれかが成りたつ。

(V が G-既約の時については [5] 参照)

(1)(2) についてはいずれも無限系列が知られているが、(3) については 14種の例が知られているだけである。([3]) 以下では、これらをすべて含む類を構成し、新しい spread 7種を追加する。

2. $\mathcal{L}$-collineation 群と $R*p$-plane

affine plane π の自己同型群で、任意の直線上

への global stabilizer が、この line 上 2重可移になっているものを <u>$\mathcal{L}$-collineation 群</u> という。$\mathcal{L}$-coll.群は translation 群を含むことが示されていて([2])従って π は前節でのべたようなベクトル空間 V上に実現されて、spread が対応する([4])。この $\mathcal{L}$-coll.群に関する最良の結果は Kallaher-Ostrom による[1]であると思う。また、Lüneburg は[3]において、$\mathcal{L}$-coll.群をもつ位数 p^2 の affine plane の特別なものとして次のように R*p-plane を定義した。

V, $\mathcal{S}$, C を前節と同じ記号とするとき、$\mathcal{S}$ が <u>R*p型の spread</u> であるとは次の条件がみたされることをいう。

(1) $|V| = p^4$ かつ $(C \leq) G$ が存在して
$\forall W \in \mathcal{S}$ に対して $\{g \in G \mid Wg = W\} \xrightarrow{\text{可移}} W^*$

(2) $G \geq {}^{\exists} X \times Y \quad X \simeq Y \simeq SL(2,5)$ s.t.
$C_V(X),\ C_V(Y) \in \mathcal{S}$

(3) G を $\mathcal{S}$ 上の置換群とみて $W^X = W^Y \quad \forall W \in \mathcal{S}$

R*p型の spread に対応する affine plane を <u>R*p-plane</u> という。

<u>定理</u> (Lüneburg [3])

R*p-plane は有限個で $p \in \{11, 19, 29, 59\}$ である。

3. $SL(2,5)\times SL(2,5)$ を admit する新しい plane

この節では $|V| = p^4$ $(p \geq 7)$, $\mathcal{S}$ を V 上の spread, $C_{\mathcal{S}} \geq G = X \times Y$, $X \simeq Y \simeq SL(2,5)$ とする。

G の中心は 3 個の位数 2 の元を含むが, これと Baer の定理を用いて次が示される。

補題 V は G-可約で, 適当な基底を選ぶことにより次のようにできる:

$$V = W \oplus W \qquad GL(W) \geq {}^{\exists}H \simeq SL(2,5)$$

$$X = \left\{ \begin{pmatrix} h_1 & 0 \\ 0 & e \end{pmatrix} \mid h_1 \in H \right\},\quad Y = \left\{ \begin{pmatrix} e & 0 \\ 0 & h_2 \end{pmatrix} \mid h_2 \in H \right\},\quad e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$\{(0,y) \in W \oplus W \mid y \in W\}$ $(= L(\infty)$ とおく$) \in \mathcal{S}$

$\{(x,0) \in W \oplus W \mid x \in W\}$ $(= L(0)$ とおく$) \in \mathcal{S}$

一方, $\mathcal{S}$ の $L(\infty)$, $L(0)$ 以外の元は適当な $m \in GL(W)$ を用いて $L(m) = \{(x, xm) \mid x \in W\}$ の形にかけることが spread の性質より分かる。([4] §2)

$\Sigma = \{m \in GL(W) \mid L(m) \in \mathcal{S}\} \cup \{0\}$ を spread set という。

補題 $L(m)^G = \bigcup_{h,h' \in H} L(hmh')$ $(= L(HmH)$ と書く$)$

とくに $|L(m)^G| = 120n$, $n = |H : H \cap H^{m^{-1}}| \in \{1, 5, 6, 10, 12, 20, 30, 60\}$ しかも $\Sigma - \{0\}$ は, 両側剰余類 HmH $(m \in GL(W))$ のいくつかの和集合である。

$R_n * p$ 型 spread の定義

$\mathcal{S}$ が $R_n * p$ 型であるとは次がみたされることをいう。

(*) $\exists L(m_0) \in \mathcal{S}$ $(m_0 \neq 0)$, $|L(m_0)^G| = 120n$

$L(m)^X = L(m)^Y$ $\forall L(m) \in \mathcal{S} - L(m_0)^G$

補題 $L(m)^X = L(m)^Y \iff Hm = mH$

このとき Hm は scalar 行列を含む.

この補題より Lüneburg の定義した $R * p$ 型 spread は, $R_1 * p$ 型 spread であることが分かる。また上記の2つの補題と spread set の基本的性質

$\Sigma \ni m, m', m \neq m' \Rightarrow \det(m - m') \neq 0$ ([4] §2)

を用いて, 次が証明される.

定理 $R_n * p$ 型 spread は $p \leqq 89$ であり従って有限個存在し, $R * p$ 型 spread 14個をすべて含む。

$R_n * p$ 型 spread を具体的に書きあげるためにパソコンを用いた。この結果, いままでに知られていない7種の spread が新たにみつかった。p の値は実際には $p \leqq 59$ であることも分かった。

(新しいものは $(p, n) = (31, 5)$ のとき4種 $(59, 5)$, $(59, 6)$, $(59, 12)$ のとき各1種)

今後の課題として次のことが残った。

(1) $R_n * p$ 型 spread 21個の $PG(3,p)$ でのそれぞれの幾何的意味は何か？

(2) $SL(2,5) \times SL(2,5)$ を admit する spread の無限系列はあるか？

(3) $SL(2,5) \times SL(2,5)$ を admit する V 上の spread の一般的性質を調べる。

文献

[1] M.J. Kallaher and T. G. Ostrom: Collineation groups irreducible on the components of a translation plane, Geom. Dedicata 9 (1980) 153–194.

[2] H. Lüneburg: Affine Ebenen, in denen der Stabilisator jeder Geraden zweifach transitiv ist, Arch. Math. 24 (1973), 663–669.

[3] H. Lüneburg: Über einige merkwürdige Translationsebenen, Geom. Dedicata 3 (1974), 263–288.

[4] H. Lüneburg: Translation Planes, Springer-Verlag, Berlin-Heidelberg-New York, 1980.

[5] T. G. Ostrom: Lectures on finite translation planes, Confer. Sem. Mat. Univ. Bari No. 191 (1983), 1–29.

表現次数が T 度 p^s で割り切れるような G_n の既約指標の個数を表す母関数について

東大・理　中村博昭

§1. 諸定義

素数 p を一つ固定し，ν_p を整数環 $\mathbb{Z}$ の p 進指数付値（即ち，整数 n に対し，$\nu_p(n)$ で n が p で割りきれる回数の最大値 (≥ 0) を表す）とする。

Def. (Mckay number)

有限群 G の複素既約指標の全体を $\mathrm{Irr}(G)$ で表し，k を 0 を含めた自然数とする時，Mckay-number $m_p(k,G)$ を次のように定義する。

$$m_p(k,G) := \#\{\chi \in \mathrm{Irr}(G) \mid \nu_p(\chi(1)) = k\}$$

目標は $G = G_n$ (n 次対称群) の時に $m_p(k, G_n)$ を k と n に関する 2 重数列として母関数の形に記述することである。$G = A_n$ (交代群), $W(B_n), W(C_n)$ (古典 Weyl 群) の時も同様な母関数が得られたが，ここでは主に対称群の場合を扱うことにする。

Def. (Macdonald number)

有限群 G の共役類全体の集合を $\mathrm{Class}(G)$ で表し，

ℓ, ν_p を上と同様とする時,

$$\mu_p(\ell, G) := \#\{C \in Class(G) \mid \nu_p(|C|) = \ell\}$$

なる数をここでは Macdonald number と呼ぶことにする。

§2. 動機

この問題を考えるようになったきっかけは大学のセミナーの折に Macdonald の本 [1] の中の次のような命題にさしかかったことである。

命題1. $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_m p^m$ $(0 \leq a_i < p)$ を自然数 n の p 進展開とする時, 次の等式が成立する。

$$\mu_p(0, G_n) = P(a_0) \cdot (a_1+1)(a_2+1)\cdots(a_m+1)$$

ここで $P(a_0)$ は a_0 の分割数をあらわす。特に $p=2$ の時は, $\mu_2(0, G_n)$ は 2 の中乗の形をしている。

これに関連して岩堀長慶教授は同じことを character degree でやったらどうなるかという問題を出された。私は計算機を用いて幾つかの実例にあたり $p=2$ の場合に $m_2(0, G_n)$ の公式を得たが有木進氏は一般の p で次のような公式を出された。

命題2. $n = a_0 + a_1 p + \cdots + a_m p^m$ $(0 \leq a_i < p)$ を自

然数 n の p 進展開とする時，次の等式が成り立つ。

$$m_p(0, G_n) = C(1, a_0) \cdot C(p, a_1) \cdot C(p^2, a_2) \cdots\cdots C(p^m, a_m)$$

但し $C(p^k, a)$ は次の無限積の展開係数として定まる数とする；$\sum_{n=0}^{\infty} C(p^k, n) x^n = \prod_{n=1}^{\infty} (1-x^n)^{-p^k}$.

この命題は実はMacdonald自身が1971年の論文[3]の中で得ているのであるが，その当時は知る由もなかった。こうして p と互いに素な場合は完全に解決されたが，指導教官はさらに p で何回か割れる場合，すなわち $m_p(k, G_n)$ はうまく記述されるだろうかという問題を出された。

§3. ヤング図形の Affine type, Projective type

よく知られているように $\mathrm{Irr}(G_n)$ は，n 個の箱からなるヤング図形で parameterize されていて，ヤング図形 λ に対応する G_n の既約指標を χ_λ とかくことにすれば，その表現次数 $\chi_\lambda(1)$ は次の hook-formula で与えられる。(文献[5]参照)

命題3. $\chi_\lambda \in \mathrm{Irr}(G_n)$ に対して，

$$\chi_\lambda(1) = \frac{n!}{h_\lambda}$$

但し h_λ はヤング図形 λ の各箱の hook の長さの積.

(例1) $\lambda = (3,3,2)$, $\chi_\lambda \in \mathrm{Irr}(G_8)$

λ の各箱に hook の長さを書き込むと

右図のようになる

5	4	2
4	3	1
2	1	

$$\therefore \chi_\lambda(1) = \frac{8!}{5\cdot4\cdot2\cdot4\cdot3\cdot1\cdot2\cdot1} = 42$$

この hook-formula を出発点とすれば, $\chi_\lambda(1)$ が素数 p で何回割れるかを調べる為には, $\nu_p(h_\lambda)$ を調べることになる。ヤング図形 λ の形から組合せ論的に $\nu_p(h_\lambda)$ についての情報を得るため次の定義をする。

Def. (Affine type of λ)

素数 p とヤング図形 λ が与えられたとき, 各項が p の巾乗の形をした自然数の有限非増加列 $A(p,\lambda) = (p^{e_1}, p^{e_2}, \cdots, p^{e_m})$ を次のように定め. λ の p に関する Affine type と呼ぶ。

(i) λ の沿岸道路で長さが p の巾乗であるもののうち最大のものの長さを p^{e_1} とし, その沿岸道路を取りはずす。

(ii) p^{e_i} まで定ま, たとし, 残, たヤング図形から p^{e_i} を越えない p の巾乗の長さの沿岸道路のうち最大の

ものの長さを $p^{e_{i+1}}$ とし，その沿岸道路をとりはずす。

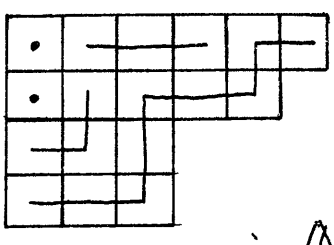
(iii) 以上の操作をヤング図形が空になるまで続ける。

Remark. λ の Affine type 中に p^k が a_k 回重複してあらわれるとき，$A(p,\lambda) = \langle a_0 + a_1 p + a_2 p^2 + \cdots + a_e p^e \rangle$ と形式的に書くことにする。ヤング図形の Core, Quotients の理論（文献 [6] 2.7 節）によれば a_k は λ の p^{k+1}-Core の p^k-weight と一致しているので，$A(p,\lambda)$ は沿岸道路の取りはずしが一意でなくても一意に定まる。

Def. (Projective type of λ)

素数 p とヤング図形 λ が与えられると Affine type $A(p,\lambda)$ が定まるが，$A(p,\lambda)$ の各項 p^e を $(p^e-1)/p-1$ で置きかえたものを λ の p に関する Projective type と呼び $P(p,\lambda)$ とかくことにする。

(例1) $p=3$. $n=17$. $\lambda=(6,5,3,3)$ の場合

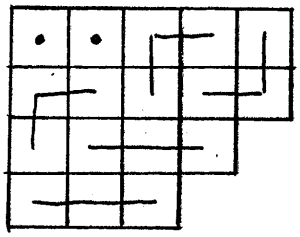


長さ9の沿岸道路1本 → とりはずす
長さ3の沿岸道路2本 → とりはずす
長さ1の沿岸道路2本 → とりはずす → 空

$\therefore A(3,\lambda) = (9,3,3,1,1) = \langle 2\cdot 1 + 2\cdot 3 + 1\cdot 3^2 \rangle$

$P(3,\lambda) = (4,1,1,0,0)$

(例2) $p=3$, $n=17$. $\lambda=(5,5,4,3)$ の場合



長さ9の沿岸道路はとれない.
長さ3の沿岸道路5本 → とりはずす
長さ1の沿岸道路2本 → とりはずす → 空

$\therefore A(3,\lambda)=(3,3,3,3,3,1,1,)=\langle 2\cdot 1+5\cdot 3\rangle$

$P(3,\lambda)=(1,1,1,1,1,0,0)$

命題4. ヤング図形λのhook-lengthsの積をh_λとすると, $\nu_p(h_\lambda)$は $P(p,\lambda)$ の成分の和に等しい。

§4. $m_p(k,G_n)$ の記述

前§の命題4より $\nu_p(h_\lambda)$ はヤング図形λのAffine type $A(p,\lambda)$ から決まることがわかったので, 次に考えることは, 同じAffine typeをもつヤング図形がどれだけあるかということである。

命題5. Affine typeが $\langle b_0+b_1p+b_2p^2+\cdots+b_\ell p^\ell\rangle$ となるようなヤング図形の個数は,

$$\tilde{C}(1,b_0)\cdot\tilde{C}(p,b_1)\cdot\tilde{C}(p^2,b_2)\cdots\cdots\tilde{C}(p^\ell,b_\ell)$$

と等しい。但し $\tilde{C}(p^k,a)$ は次の無限積の展開係数として定まる数とする; $\sum_{n=0}^{\infty}\tilde{C}(p^k,n)x^n=\prod_{n=1}^{\infty}(1-x^{np})^{p^{k+1}}(1-x^n)^{-p^k}$.

従って以上までで $m_p(k, G_n)$ は和が n となるようなすべての Affine type のうち、その Projective type の和が $\nu_p(n!)-k$ となるようなものについて命題5のような積を合計すれば得られることになる。このことは実は、J. B. Olsson が 1976 年の論文の中で実質的に述べていることなのであったが、やはりそのことはずっと後になるまで知らないでいた。そして今年の夏、セミナーの先輩方がアメリカに行かれ、Macdonald 先生や Olsson 先生と会って話し合われた結果、私の考えたことの大部分はすでに過去の論文に出ているということが判明したのである。しかしながら次に述べる $m_p(k, G_n)$ の母関数についてはまだ残っているようなので、それを発表するのが今回の目的である。

定理

$$\sum_{k=0}^{\infty}\sum_{n=0}^{\infty} m_p(k, G_n)\, x^{\nu_p(n!)-k} y^n = \prod_{k=0}^{\infty}\prod_{n=1}^{\infty}\left(\frac{1-\left(x^{p+p^2+\cdots+p^{k-1}} y^{p^k}\right)^n}{1-\left(x^{1+p+\cdots+p^{k-1}} y^{p^k}\right)^n}\right)^{p^k}$$

但し $m_p(k, G_0) = \begin{cases} 1 & k=0 \\ 0 & k>0 \end{cases}$

$x^{p+p^2+\cdots+p^{k-1}} = 0 \quad (k=0)$; $1+p+\cdots+p^{k-1} = 0 \quad (k=0)$

$\phantom{x^{p+p^2+\cdots+p^{k-1}}} = 1 \quad (k=1)$

§5. $\mu_p(k, G_n)$ の母関数

character degree の方ばかり考えていて共役類の方はすっかり忘れていたのであるが、松山に来てから考えてみるとこちらの方は母関数だけなら意外と簡単であることがわかったのでついでに書いておく。

定理

$$\sum_{k=0}^{\infty}\sum_{n=0}^{\infty} M_p(k, G_n)\, x^{\nu_p(n!)-k} y^n = \prod_{k=0}^{\infty}\prod_{n=1}^{\infty} \frac{1-x^{p+p^2+\cdots+p^k+\nu_p(n)p^{k+1}} y^{np^{k+1}}}{1-x^{1+p+\cdots+p^{k-1}+\nu_p(n)p^k} y^{np^k}}$$

どちらの定理も $x=1$ とすると普通の分割関数 $\prod_{n=1}^{\infty}(1-y^n)^{-1}$ に戻ってしまう所を注目されたい。

[文献]

[1] I.G. Macdonald "Symmetric Functions and Hall Polynomials" Oxford 1979

[2] J. Mckay "Irreducible Representations of Odd Degree" J. of Algebra 20, 416-418 (1972)

[3] I.G. Macdonald "On the degrees of the Irreducible Representations of Symmetric Groups" Bull. London. Math. Soc. 3 (1971) 189-192

[4] J.B. Olsson "Mckay Numbers and Heights of Characters"

MATH. SCAND. 38 (1976), 25-42

[5] 岩堀長慶『対称群と一般線形群の表現論』岩波書店

[6] G. James, A Kerber "The Representation Theory of the Symmetric Group" Addison-Wesley 1981

Distance-Regular Digraphs. II

東大 理 情報科学　榎本彦衛

岡山大学における「代数的組み合せ論」の研究集会（1983年）以後の '距離正則有向グラフで内周 4 のものの存在' に関する研究の進展について報告する。

以下、有向グラフのみを考えるので、有向グラフのことをたんにグラフということにする。最初に、記法と [2] における主要結果を復習しておく。

グラフ G の2頂点 x,y に対し、

$d_G(x,y)$:= x から y 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。（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、

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

特に、

$$\Gamma(x) := \Gamma_1(x) = \{y \in V(G) \mid x \text{ と } y \text{ は隣接している}\}$$

とおく。

定義1. $|\Gamma_i(x) \cap \Gamma(y)|$ 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。

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 s_{ij} と書くことにする。

定理2. (1) d(G) = g(G) または d(G) = g(G) − 1

(2) 0 < t < g(G) のとき、d(x,y) = t ならば、 d(y,x) = g(G) − t となる。

(3) d(G) = g(G) − 1 のとき、任意の集合 M に対し (|M| ≧ 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。

(4) d(H) = g(H) の距離正則グラフ H はすべて (3) の方法により構成される。

以下、d(G) = g(G) − 1 とし、g := g(G)、$0^* := 0$、$t^* := g - t$ (0 < t < g) とおく。定理2 (2)より $d(x,y)^* = d(y,x)$ となることが

わかる。 $d(x,y) = k$ のときの

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

を p^i_{jk} とおき、

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

を intersection matrix と呼ぶ。 Γ_iに関する隣接行列を A_i とおくと、

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

が成り立つ。特に、

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

より

$$A_1 A_i = \sum_{j=0}^{i+1} s_{i^*j^*} A_j \quad (0 \leqq i \leqq d-1)$$

となる。

以下、$g=4$ の場合を考える。A_1 の固有値を θ_1、θ_2、$\overline{\theta_1}$、その重複度を m_1、m_2、m_1、

$$B_1 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & a & e & 0 \\ 0 & f & d & b \\ k & a & c & a \end{bmatrix}$$

とすると、2つのパラメータβと q を使って

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

$$a = 2\beta q - \beta - q$$

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

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

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

$$e = \beta q$$

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

$$\theta_1 + \overline{\theta_1} = a$$

$$\theta_1\overline{\theta_1} = qb$$

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

$$m_1 = \frac{(n-1)\beta - k}{2\beta + a}$$

$$m_2 = \frac{(n-1)a + 2k}{2\beta + a}$$

と表わせることはわかっていたが、２種類の 1-パラメータ系列以外には可能性がないことが次のようにしてわかる（[3]）。

$\beta = 1$ とすると、$k = 2q - 1, a = q - 1$ となる。これは、$\Gamma(x)$が regular tournament であるということを意味する。$k \geqq 3$ とすると内周が 3 になってしまうので、$k = 1$、すなわち、G は４角形である。

以下、$\beta \geqq 2$ の場合を考える。 βと q の最大公約数を d とお

き、$\gamma := \beta/d$、$\lambda := q/d$、$\delta := 2\beta + a$ とおくと、m_1 の整数性より

$$6\beta^4 + 3\beta^3 - 3\beta^2 - \frac{\beta^4 - \beta^3}{q} \equiv 0 \pmod{\delta}$$

となり、

$$2d(2\lambda - \gamma) \equiv 0 \pmod{2d\gamma\lambda + \gamma - \lambda} \qquad (*)$$

となることがわかる。

Case 1 $2\lambda = \gamma$

$(\lambda, \gamma) = 1$ より $\lambda = 1$, $\gamma = 2$ のみ可能。すなわち、$\beta = 2q$ となる。

Case 2 $2\lambda > \gamma$

$\lambda = 1$, $\gamma = 1$ しか可能性がないことを示す。

（＊）より

$$2d(2\lambda - \gamma) \geqq 2d\gamma\lambda + \gamma - \lambda$$

すなわち

$$2d(\gamma - 2)(\lambda + 1) + 4d + \gamma - \lambda \leqq 0$$

となることがわかる。

$\gamma \geqq 3$ とすると、

$$\text{左辺} \geqq 2d(\lambda + 1) + 4d + \gamma - \lambda > 0$$

となり矛盾。

また、$\gamma = 2$ とすると、$\lambda \geqq 4d + 2$ となるが、$(\lambda, \gamma) = 1$ より λ

$> 4d + 2$ となることがわかる。そこで（＊）に戻って考えると、

$$2d(2\lambda - 2) \equiv \lambda - 4d - 2 \equiv 0 \pmod{4d\lambda + 2 - \lambda}$$

となり、

$$\lambda - 4d - 2 \geqq 4d\lambda + 2 - \lambda$$

すなわち、

$$4d\lambda + 4d - 2\lambda + 4 = (2d - 1)(2\lambda + 2) + 6 \leqq 0$$

となるが、これは矛盾。

従って、$\gamma = 1$ としてよい。再び（＊）より

$$2d(2\lambda - 1) \equiv 2\lambda - 2d - 2 \equiv 0 \pmod{2d\lambda + 1 - \lambda}$$

となる。$\lambda > d + 1$ とすると

$$2\lambda - 2d - 2 \geqq 2d\lambda + 1 - \lambda$$

より $d = 1$ となるが、$\beta \geqq 2$ に反する。$\lambda = d + 1$ とすると、$\beta = d$、$q = d(d + 1)$ となるが、$q \mid \beta^4 - \beta^3$ より $d = 1$、すなわち $\beta = 1$ となる。$\lambda < d + 1$ の場合は

$$2d + 2 - 2\lambda \geqq 2d\lambda + 1 - \lambda$$

より

$$(2d + 1)(\lambda - 1) \leqq 0$$

となり、$\lambda = 1$ となることがわかった。

Case 3 $2\lambda < \gamma$

（＊）より

$$2d\gamma\lambda + \gamma - \lambda \leqq 2d(\gamma - 2\lambda)$$

となる。ところが

$$\text{左辺} > 2d\gamma\lambda \geqq 2d\gamma > \text{右辺}$$

なので、この場合は起こらない。

$\beta = 2q$ となる例は知られていない。（$\beta = 2, q = 1$ の場合は存在しないことが証明されている。）$\beta = q = 1$ ならば4角形になる。$\beta = q = 2$ の例が [3] で構成されたが、もっと一般に $\beta = q = 2^t$ の例が [4] で構成された。その構成法を以下に示す。

$$m := 2t + 1$$

$$F := GF(2^m)$$

とおき、

$$F^* = <\zeta>$$

とする。ζ の最小多項式を $g(X)$ とすると、Z_4 上の多項式 $f(X)$ で

$$f(X) \equiv g(X) \pmod 2$$

$$f(X) \mid X^{2^m-1} - 1$$

を満たすものが存在する。そこで、$f(X) = 0$ の根 ξ を Z_4 に添加してできる環を R とおく：

$$R := Z_4[\xi] = Z_4[X]/(f(X))$$

R から F への自然な準同型写像を ^ とすると、任意の多項式 $\varphi(X)$ に

対し

$$\hat{}(\varphi(\xi)) \equiv \varphi(\xi) \pmod 2$$

が成り立つ。

$$E := 2R = \{\alpha \in R \mid 2\alpha = 0\}$$

$$U := R - E = \{\alpha \in R \mid \alpha \text{は可逆元}\}$$

$$S := \{\alpha^2 \mid \alpha \in U\}$$

$$= \{\xi^i \mid 0 \leqq i \leqq 2^m - 2\}$$

$$T := 1 + E = \{\alpha \mid \alpha^2 = 1\}$$

とおくと、

$$U = ST, \quad S \cap T = \{1\}$$

が成り立つ。そこで

$$[\hat{}(\alpha)] := (1 + 2\alpha)S \quad (\alpha \in R)$$

$$[e] := E - \{0\}$$

$$[\infty] := \{0\}$$

$$\tilde{F} := F \cup \{e, \infty\}$$

とおくと、

$$\{[x] \mid x \in \tilde{F}\}$$

は、R の S-軌道への分解を与える。従って、$\gamma \in [z]$ のとき

$$n(x,y;z) := \#\{(\alpha,\beta) \in [x] \times [y] \mid \alpha + \beta = \gamma\}$$

とおき、[x] に関する隣接行列を A_x とすると、

$$A_xA_y = \sum_z n(x,y;z)A_z$$

と書ける。n(x,y;z) の具体的な値は次のようになる。

$$n(\infty,y;z) = \begin{cases} 0 & y \neq z \\ 1 & y = z \end{cases}$$

$$n(e,e;z) = \begin{cases} 2^m - 1 & z = \infty \\ 2^m - 2 & z = e \\ 0 & z \neq e, \infty \end{cases}$$

以下、$y \in F$ とする。

$$n(e,y;z) = \begin{cases} 0 & z = y, e, \infty \\ 1 & z \in F - \{y\} \end{cases}$$

以下、$x, y \in F$ とする。

$$n(x,y;\infty) = \begin{cases} 2^m - 1 & y = x + 1 \\ 0 & y \neq x + 1 \end{cases}$$

$$n(x,y;e) = \begin{cases} 0 & y = x + 1 \\ 1 & y \neq x + 1 \end{cases}$$

以下、$x, z \in F$ とする。

$$n(x,x;z) = \begin{cases} 0 & z = x \\ 2 & z \neq x, \mathrm{tr}\, z = \mathrm{tr}\, x \\ 1 & \text{それ以外} \end{cases}$$

$$n(x,x+1;z) = \begin{cases} 0 & z = x, x + 1 \\ 1 & z \neq x, x + 1 \end{cases}$$

以下、$x, y, z \in F, y \neq x, x + 1$ とする。

$$n(x,y;z) = \begin{cases} 1 & z = x, y \\ 2 & z \neq x, y, \mathrm{tr}\,(x+z)(y+z) = 0 \\ 0 & \text{それ以外} \end{cases}$$

次に、F を GF(2) 上のベクトル空間と考え、a, b∈F に対し、

$$\langle a,b \rangle := \mathrm{tr}\ ab$$

と定義すると、〈,〉は nondegenerate な内積になる。H をこの内積に関する maximal totally isotropic subspace とし、

$$A_1 := \sum_{a \in H} A_a$$

とおくと、

$$A_1{}^T = \sum_{a \in H} A_{1+a}$$

となる。さらに

$$A_2 := \sum_{\substack{a \in F \\ a \notin H \\ a+1 \notin H}} A_a$$

とおくと、

$$A_1{}^2 = 2^{t+1}(2^t - 1)A_1 + 2^{2t}A_2$$

$$A_1 A_1{}^T = 2^t(2^{2t+1} - 1)I + 2^{t+1}(2^t - 1)(A_1 + A_1{}^T) + 2^t(2^t - 1)A_2$$

が成り立つことから、A_1 が内周４の距離正則グラフの隣接行列になっていることがわかる。

文献

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

[2] 榎本彦衛, Distance-regular digraphs, 「代数的組み合せ論の研究」(岡山大学 1983年) 報告集, 9-16

[3] H.Enomoto-R.A.Mena, Distance-regular digraphs of girth 4, J. Combinatorial Theory (B), to appear

[4] R.A.Liebler-R.A.Mena, Certain distance-regular digraphs and related rings of characteristic 4, to appear

次数４の距離正則グラフについて

東京医科歯科大学 教養部　野村和正

[１] 距離正則グラフの定義と基本的事項

G を連結な有限単純無向グラフ，V を G の点集合とする．　V の２点 u と v に対して，u と v を結ぶ最短通路の長さを $\partial(u,v)$ と表すと ∂ は距離空間の公理系をみたし V は距離空間となる．　点 u を中心とする半径 r の球面を

$$\Gamma_r(u) = \{ x \in V \mid \partial(u,x) = r \}$$

とし，さらに２つの球面の交わりを

$$D_s^r(u,v) = \Gamma_r(u) \cap \Gamma_s(v)$$

と書く．　ここで r, s は整数とし，r, s が負のときはこれらは空集合と考える．　$D_s^r(u,v)$ の要素の個数 $|D_s^r(u,v)|$ が r, s と $\partial(u,v)$ だけで決まり個々の u, v のとりかたによらないとき，すなわち任意の整数 r, s と任意の V の点 u, v, u', v' に対して

$$\partial(u,v) = \partial(u',v') \text{ ならば } |D_s^r(u,v)| = |D_s^r(u',v')|$$

が成立しているときグラフ G は 距離正則 であるという．　文献 [1] に距離正則グラフに関する詳しい記述がある．

以後 G は距離正則であるとする．　点 u と隣接している点の個数 $k = |\Gamma_1(u)|$ は点のとりかたによらず一定になる．　k を G の 次数 という．　G の２点間の最大距離

$$d(G) = max \{ \partial(u,v) \mid u, v \in V \}$$

を G の 直径 という． また G のサイクルで長さが最小のものの長さを G の 内周 という． 以下 G の次数を k，直径を d，内周を g とする．

G の任意の点 u をとり，さらに任意の整数 r（$0 \leqq r \leqq d$）に対して $\Gamma_r(u)$ の任意の点 x をとる． x と隣接している点は $\Gamma_{r-1}(u)$, $\Gamma_r(u)$, $\Gamma_{r+1}(u)$ のいずれかに属する． それらの点の個数をそれぞれ c_r, a_r, b_r とおく． すなわち

$$c_r = |\Gamma_1(x) \cap \Gamma_{r-1}(u)|$$
$$a_r = |\Gamma_1(x) \cap \Gamma_r(u)|$$
$$b_r = |\Gamma_1(x) \cap \Gamma_{r+1}(u)|$$

これらの数 a_r, b_r, c_r は u と x のとりかたによらないことがわかる． これを G の 交叉数 という．

$$a_r + b_r + c_r = k$$

であり，また $c_0 = 0$, $a_0 = 0$, $b_0 = k$, $c_1 = 1$, $b_d = 0$ となることが定義からすぐわかる． さらに交叉数には次のような単調性があることが知られている．

$$0 = c_0 \leqq c_1 \leqq c_2 \leqq \cdots\cdots \leqq c_d$$
$$k = b_0 \geqq b_1 \geqq b_2 \geqq \cdots\cdots \geqq b_d = 0$$

これらの交叉数を次のように並べたものを G の 交叉配列 という．

$$\begin{Bmatrix} c_0 & c_1 & c_2 & \cdots\cdots & c_d \\ a_0 & a_1 & a_2 & \cdots\cdots & a_d \\ b_0 & b_1 & b_2 & \cdots\cdots & b_d \end{Bmatrix}$$

［２］ 距離正則グラフの分類問題

距離正則グラフをすべて分類することは殆ど不可能である． 例えば直径をわずか３にして交叉配列をつぎの形に限定しても，そのような距離正則グラフの分類はできていない．

$$\left\{\begin{array}{cccc} 0 & 1 & 1 & k \\ 0 & 0 & 0 & 0 \\ k & k-1 & k-1 & 0 \end{array}\right\}$$

（実はこの形の距離正則グラフを考えることは位数 $k-1$ の射影平面を考えることと同じことになる）． そこで分類問題を考えるにはある程度範囲を限る必要があるが，そのような条件として Q-polinomiality といわれるものを導入して，すべての Q-polinomial な距離正則グラフを分類しようというのが文献 [1] の主題である． 急速な進展を見せているがまだ完成はしていない．

一方，最近になって Biggs, Boshier, Shawe-Taylor により次数３の距離正則グラフが分類された（文献 [4]）． このきっかけとなったのが次の Ivanov の定理である．

［定理］(Ivanov，文献 [12]) 次数 k，内周 g ($g > 3$) の距離正則グラフの直径は k と g のある関数でおさえられる．

この定理であたえられる直径 d の上界はかなり大きいので，すぐには実用にならないが， Ivanov が用いた証明方法は非常に有用で，

Biggs 等は Ivanov の方法の延長線上に，新たにサイクルパターン法という新しい方法を開発して次数３の分類に成功した．　これらの証明方法は純組合せ論的であり，今まで用いられてきた固有値による代数的方法と著しい対照をなしている．

これらの証明は非常に興味あるものであるが，相当に複雑であり論理のチェックだけでも相当労力を要する．　そこで以前から用いていた交叉図式なるものを用いてこれらの証明を書きなおしてみると，その証明が短くなるだけでなく目に見える形になった．（交叉図式を用いた証明については文献［3］を参照）．　交叉図式はもともとは文献［9］の研究の際に考え付いたものである．　こうして交叉図式が距離正則グラフの研究にかなり有用であることがわかり，その後文献［6］，［13］の結果を交叉図式を用いることにより得た．

さて次数３が終わったので，次にやるべ仕事は当然次数４の分類ということになる．　交叉図式によって次の結果を得た．

［定理］次数が４で内周が３の距離正則グラフは次のものに限る．

1) 完全グラフ K_5

2) 正８面体

3) 次のグラフの線グラフ

　a) Petersen グラフ

　b) 完全２部グラフ $K_{3,3}$

　c) Heawood グラフ

　d) Tutte's 8-cage

　e) 12-cage

ここでグラフ G の線グラフ $L(G)$ とは G の辺集合を点集合とし，2辺が1端点を共有しているときに隣接しているとしてできるグラフのこと．　3) に現れている a) から e) の5個のグラフはいずれも次数3の距離正則グラフである．　次数3の距離正則グラフは全部で13個あるが，　ここに現れているのは　Moore　グラフと　generalized polygon　といわれるものである．

Moore グラフ

a) d = 2 Petersen グラフ

generalized polygon

b) d = 2 $K_{3,3}$

c) d = 3 Heawood グラフ

d) d = 4 8-cage

e) d = 6 12-cage

Moore グラフというのは

$$c_1 = c_2 = \cdots = c_d = 1$$

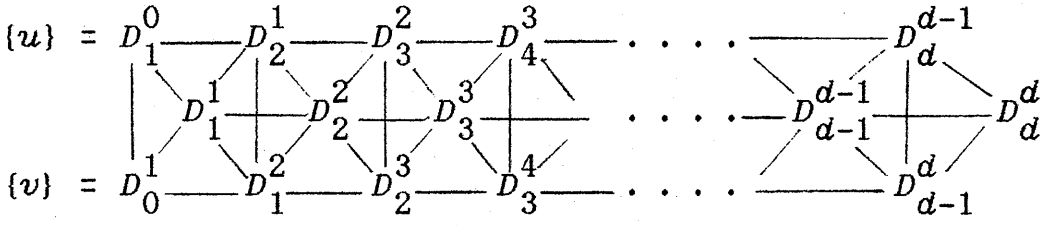
となっているグラフであり，坂内，伊藤，Damerell 等により分類されている（文献 [2], [7]）．　また generalized polygon というのは

$$c_1 = c_2 = \cdots = c_{d-1} = 1\ ,\ c_d = k$$

なるもののこと（文献 [8] 参照）．

［３］ 交叉図式

G の隣接している２点 u, v を１組固定して，$D_s^r(u,v)$ を簡単に D_s^r と表すことにする． $\partial(u,v)=1$ であることから，$|r-s| \geqq 2$ ならば $D_s^r=\varnothing$ となっている． さて次のような図式を書く．



ここで D_s^r 達の間にひいてある線はそれらの間を結ぶ辺が存在する可能性をあらわしている． すなわち線でむすばれていないところには辺がない． この図式を u, v に関する交叉図式と呼ぶ． （ここでは $\partial(u,v)=1$ と仮定しているが，一般には任意の２点に関する交叉図式を書くことができる）．

さて D_s^r の点 x をとり，x からの辺の出方を見る． x から $D_{s'}^{r'}$ に向かって出ている辺の本数を

$$e_{s'-s}^{r'-r}(x) = |\Gamma_1(x) \cap D_{s'}^{r'}|$$

と表すことにする． $|r-r'| \geqq 2$ または $|s-s'| \geqq 2$ のときは D_s^r と $D_{s'}^{r'}$ の間には辺がないので，

$e_{+1}^{+1}(x), e_0^{+1}(x), e_{-1}^{+1}(x), e_{+1}^{0}(x), e_0^{0}(x), e_{-1}^{0}(x), e_{+1}^{-1}(x), e_0^{-1}(x), e_{-1}^{-1}(x)$

だけを考えればよい． つぎの補題は u からの距離と v からの距離を考えることにより容易に得られる．

［補題１］ $x \in D_r^{r+1}$ ならば次の等式が成立する．

$$e_{-1}^{0}(x) = e_{-1}^{+1}(x) = e_{0}^{+1}(x) = 0$$

$$e_{+1}^{+1}(x) = b_{r+1}$$

$$e_{+1}^{+1}(x) + e_{+1}^{0}(x) + e_{+1}^{-1}(x) = b_r$$

$$e_{-1}^{-1}(x) = c_r$$

$$e_{+1}^{-1}(x) + e_{0}^{-1}(x) + e_{-1}^{-1}(x) = c_{r+1}$$

$$e_{+1}^{0}(x) + e_{0}^{0}(x) = a_{r+1}$$

$$e_{0}^{0}(x) + e_{0}^{-1}(x) = a_r$$

$x \in D_{r+1}^{r}$ についても同様のことがいえる．

［補題２］ $x \in D_r^r$ ならば

$$e_{+1}^{0}(x) + e_{+1}^{+1}(x) = e_{0}^{+1}(x) + e_{+1}^{+1}(x) = b_r$$

$$e_{0}^{-1}(x) + e_{-1}^{-1}(x) = e_{-1}^{0}(x) + e_{-1}^{-1}(x) = c_r$$

$$e_{0}^{+1}(x) + e_{0}^{0}(x) + e_{0}^{+1}(x) = e_{+1}^{0}(x) + e_{0}^{0}(x) + e_{-1}^{0}(x) = a_r$$

補題１から交叉数の単調性が導かれることに注意．　さらに $b_r = b_{r+1}$ ならば

$$e_{+1}^{0}(x) = e_{+1}^{-1}(x) = 0$$

であり，またもし $c_r = c_{r+1}$ ならば

$$e_{+1}^{-1}(x) = e_{0}^{-1}(x) = 0$$

となることも明らか．　また補題２から $x \in D_r^r$ にたいしては

$$e_{+1}^{0}(x) = e_{0}^{+1}(x), \quad e_{0}^{-1}(x) = e_{-1}^{0}(x)$$

が成り立つこともわかる.

一般には D_s^r の点からの辺の出方は点のとりかたにより異なるが, 交叉配列の形によっては, 上の補題により辺の出方が一意に決定されることがある. そういう場合には交叉図式が特に威力を発揮することになる.

[4] 定理の証明の概略

G を次数4, 内周3の距離正則グラフとする. G の直径を d, 交叉数を c_r, a_r, b_r $(0 \leqq r \leqq d)$ とする. 内周が3であることから $a_1 \geqq 1$ となっているが, $a_1 = 3$ のときは, G は K_5 と同型となり, また $a_1 = 2$ のときは G は正8面体となることが直接確かめられるので, 以下 $a_1 = 1$ と仮定する. このときは G の任意の辺に対して, その辺を含む3角形が唯一つある. $a_r + b_r + c_r = 4$ と b_r および c_r の単調性などを考えることにより, G の交叉配列は

$$\left\{ \begin{array}{cccccccccccccccc} 0 & 1 & \cdots & 1 & 1 & \cdots & 1 & 2 & \cdots & 2 & 2 & \cdots & 2 & 3 & \cdots & 3 & c_d \\ 0 & 1 & \cdots & 1 & 2 & \cdots & 2 & 0 & \cdots & 0 & 1 & \cdots & 1 & 0 & \cdots & 0 & a_d \\ 4 & 2 & \cdots & 2 & 1 & \cdots & 1 & 2 & \cdots & 2 & 1 & \cdots & 1 & 1 & \cdots & 1 & 0 \end{array} \right\}$$

の形になる. ここで (1,2,1) 型と (2,0,2) 型はどちらか片方しかない. 実際は (2,0,2) 型は現れないことが, つぎの定理からわかる.

[定理] (文献 [13])

(i)　$0 < a_r < b_r$ ならば $a_{r+1} > 0$

(ii)　$0 < a_r < c_r$ ならば $a_{r-1} > 0$

また

$$|\Gamma_r(u)| = \frac{b_0 b_1 \cdots\cdots b_{r-1}}{c_1 c_2 \cdots\cdots c_r}$$

より，(3,0,1) 型はないことがわかる．　従って交叉配列は次の形になる．

$$\left\{\begin{array}{cccccccccccc} 0 & 1 & \cdots & 1 & 1 & \cdots & 1 & 2 & \cdots & 2 & c_d \\ 0 & 1 & \cdots & 1 & 2 & \cdots & 2 & 1 & \cdots & 1 & a_d \\ 4 & 2 & \cdots & 2 & 1 & \cdots & 1 & 1 & \cdots & 1 & 0 \end{array}\right\}$$

(1,1,2)，(1,2,1)，(2,1,1) 型の欄の個数をそれぞれ α，β，γ とする．G の隣接した2点 u，v をとり，$D_s^r = D_s^r(u,v)$ とおく．

(Case 1)　$\beta > 0$ のとき

まず $\beta \geqq 2$ と仮定してみる．　$\Gamma_{\alpha+1}(u)$ の点 x をとる．　x から $\Gamma_\alpha(u)$ に出ている辺を (x,y)，$\Gamma_{\alpha+2}(u)$ に出ている辺を (x,z) とする．　それらを含む3角形をそれぞれ (x,y,p)，(x,z,q) とする．x から $\Gamma_{\alpha+1}(u)$ へは辺が2本出ているはずだから，p，$q \in \Gamma_{\alpha+1}(u)$ となっている．　すると z から $\Gamma_{\alpha+1}(u)$ に向かって2本の辺 (z,x)，(z,q) が出ているから $c_{\alpha+2} \geqq 2$ となり，仮定に反する．　従って $\beta = 1$ である．

つぎに $\gamma > 0$ と仮定してみる． $|D_1^1| = \alpha_1 = 1$ であるから，$D_1^1 = \{w\}$ とおく． 前節の補題をくりかえし用いることにより，辺の出方を決定すると次のようになる．

$e_{-1}^0(w) = e_0^{-1}(w) = 1$, $e_{+1}^{+1}(w) = 2$

x が D_r^{r+1} $(1 \leqq r \leqq \alpha-1)$, D_{r+1}^r $(1 \leqq r \leqq \alpha-1)$ または D_r^r $(2 \leqq r \leqq \alpha)$ の点ならば $e_{-1}^{-1}(x) = 1$, $e_0^0(x) = 1$, $e_{+1}^{+1}(x) = 2$

$x \in D_\alpha^{\alpha+1}$ ならば $e_{-1}^{-1}(x) = 1$, $e_0^0(x) = 1$, $e_{+1}^0(x) = 1$, $e_{+1}^{+1}(x) = 1$

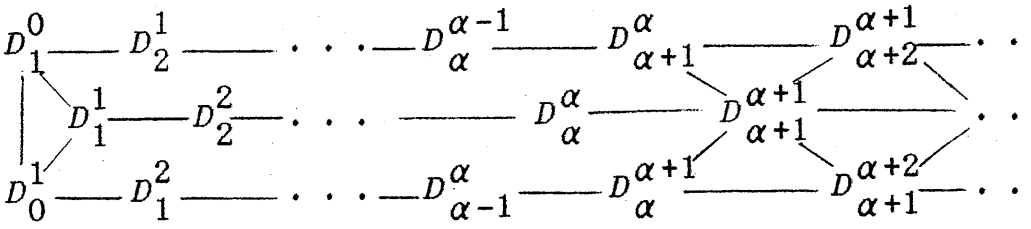
$x \in D_{\alpha+1}^{\alpha+2}$ ならば $e_{-1}^{-1}(x) = 1$, $e_0^{-1}(x) = 1$, $e_0^0(x) = 1$, $e_{+1}^{+1}(x) = 1$

$x \in D_{\alpha+1}^{\alpha+1}$ のときは次のいずれかが成立

(i) $e_0^{-1}(x) = 1$, $e_{-1}^0(x) = 1$, $e_{+1}^0(x) = 1$, $e_0^{+1}(x) = 1$

(ii) $e_{-1}^{-1}(x) = 1$, $e_0^0(x) = 2$, $e_{+1}^{+1}(x) = 1$

このことから G の交叉図式は次の様に書ける．



これらのことから

D_1^0, D_0^1, D_1^2, . . . $D_\alpha^{\alpha+1}$, $D_{\alpha+1}^{\alpha+1}$, $D_{\alpha+1}^{\alpha}$, . . . D_2^1, D_1^0

を順次通るような長さ $2\alpha+3$ のサイクルがあることがわかる． 実はもっと強く，長さ $\alpha+1$ の任意の通路を含むような，長さ $2\alpha+3$ のサイクルがあることがいえる． さて w から D_2^2 にむかって出ている辺 (w,p_2) をとる． 次に p_2 から D_3^3 に出ている辺 (p_2,p_3) を

とる．　この操作をくりかえして，w と $D_{\alpha+1}^{\alpha+1}$ の点 $p_{\alpha+1}$ をむすぶ長さ α の通路ができる．　この通路に v を付け加えて長さ $\alpha+1$ の通路をつくる．　この通路を含む長さ $2\alpha+3$ のサイクル

$p_0=v, p_1=w, p_2, \cdots, p_\alpha, p_{\alpha+1}, p_{\alpha+2}, \cdots, p_{2\alpha+2}, p_{2\alpha+3}=v$

がある．　$p_{\alpha+1}$ からの辺の出方をみることにより，$p_{\alpha+2} \in D_{\alpha+1}^{\alpha+1}$ でなければならない．　$p_{\alpha+2}$ からの辺の出方と $\partial(v,p_{\alpha+3}) \leqq \alpha$ より $p_{\alpha+3} \in D_\alpha^\alpha$ となる．　同様にして $p_{\alpha+3+r} \in D_{\alpha-r}^{\alpha-r}$ $(r=1,2,\ldots,\alpha-1)$ がいえる．　とくに $p_{2\alpha+2} \in D_1^1$ となる．　従って $p_1=w=p_{2\alpha+2}$ となり不合理．　よって $\gamma=0$ でなければならない．　したがって $d=d(G)=\alpha+2$.

$x \in D_{\alpha+1}^{\alpha+1}$ で $e_{-1}^{-1}(x)=1$ なるものをとる．　もし $e_0^{+1}(x)=0$ ならば，上と同様にして矛盾が生じるから $e_0^{+1}(x)=e_{+1}^0=1$ でなければならない．　これから $e_0^0(x)=1$ もわかる．　x から D_α^α に出ている辺を (x,y) とし，この辺を含む3角形を (x,y,z) とすると，$z \in D_{\alpha+1}^{\alpha+1}$ となる．　また x から $D_{\alpha+2}^{\alpha+1}$ に向かう辺を (x,p) とし，これを含む3角形を (x,p,q) とすると，$q \in D_{\alpha+1}^{\alpha+2}$ となる．　次に p から $D_{\alpha+1}^\alpha$ に出る辺を (p,f) とし，これを含む3角形を (p,f,h) とする．　f からの辺の出方を見ることにより，$h \in D_{\alpha+1}^{\alpha+1}$ であることがわかる．　p からは $\Gamma_{\alpha+1}(v)$ にむかって4本の辺 (p,f), (p,h), (p,x), (p,q) がでているので，$c_d=4$ であることもわかる．従って G の交叉配列は次の様になる．

$$\left\{\begin{array}{cccccc} 0 & 1 & \cdots & 1 & 1 & 4 \\ 0 & 1 & \cdots & 1 & 2 & 0 \\ 4 & 2 & \cdots & 2 & 1 & 0 \end{array}\right\}$$

さてここで，G の3角形の作るグラフを G とする．　すなわち，$\bar{G}$ は G の互いに隣接した3点 x_1, x_2, x_3 の集合 $\{x_1, x_2, x_3\}$ を点とし，2つの3点集合は，それらの共通部分が空でないときに隣接していると定義してできるグラフである．　いまの場合，$\bar{G}$ は次数3の距離正則グラフになることが証明できる（証明略）．　さらに，$\overline{G}$ の交叉配列は

$$\left\{\begin{array}{ccccc} 0 & 1 & \cdots\cdots & 1 & 1 \\ 0 & 0 & \cdots\cdots & 0 & 2 \\ 3 & 2 & \cdots\cdots & 2 & 0 \end{array}\right\}$$

の形になることもいえる．　ここで (1,0,2) 型の欄は α 個．　よって $\bar{G}$ は Moore グラフになり，坂内，伊藤，Damerell による Moore グラフの分類定理により，$d = 2$ であることがわかり，$\bar{G}$ は Petersen グラフになる．　G が $\bar{G}$ の線グラフになることは容易にわかる．

(Case 2)　$\beta = 0$ のとき

詳しく述べると長くなるので，方針を示すにとどめる．

まず $\gamma > 0$ の場合を考える．　このときは $D_{\alpha}^{\alpha+1}$ の点からの

辺のでかたは2種類の可能性があるが，$D^{\alpha}_{\alpha+1}$ へむかう辺がある場合は，その辺を含む3角形があることから矛盾がでる．　すると，$D^{\alpha+1}_{\alpha}$ の各点から D^{α}_{α} に向かって辺がでていることになる．　いっぽう D^{α}_{α} の点からは $D^{\alpha+1}_{\alpha}$ にむかって，高々1本しか辺が出ていないことがいえる．　ところが，$2\,|D^{\alpha}_{\alpha}| = |D^{\alpha+1}_{\alpha}|$ であるので矛盾．　従って $\gamma = 0$.

$|\Gamma_{\alpha}|$ が3で割れないことから $c_d \neq 3$ がいえる．　多少複雑な推論により，$c_d \neq 1$ であることもいえるので，G の交叉配列は

$$\left\{\begin{array}{ccccccc} 0 & 1 & \cdots\cdots & 1 & 2 \\ 0 & 1 & \cdots\cdots & 1 & 2 \\ 4 & 2 & \cdots\cdots & 2 & 0 \end{array}\right\}$$

という形になる．　ここでさらに D^{d}_{d-1} や D^{d}_{d} の点からの辺の出方を詳しく調べることにより，G の3角形の作るグラフが距離正則になることがいえる．　そして，その交叉配列は

$$\left\{\begin{array}{ccccccc} 0 & 1 & \cdots\cdots & 1 & 3 \\ 0 & 0 & \cdots\cdots & 0 & 0 \\ 3 & 2 & \cdots\cdots & 2 & 0 \end{array}\right\}$$

となることがわかる．　これは generalized polygon であるから，Feit, Higman の定理により，$d = 2, 3, 4$ または 6 となる．　これらの線グラフが G となる．

参照文献

1. E. BANNAI AND T. ITO, "Algebraic Combinatorics I," Benjamin, California, 1984.
2. E. BANNAI AND T. ITO, On finite Moore graphs, *J. Fac. Sci. Univ. Tokyo*, Sect IA **20** (1973), 191-208.
3. E. BANNAI AND T. ITO, Current researches on algebraic combinatorics, to appear in *Graphs and Combinatorics*.
4. N.L. BIGGS, A.G. BOSHIER AND J. SHAWE-TAYLOR, Cubic distance-regular graphs, to appear.
5. N. L. BIGGS AND D. H. SMITH, On trivalent graphs, *Bull. London Math. Soc.* **2** (1970), 155-158.
6. A. BOSHIER AND K. NOMURA, A remark on the intersection array of a distance-regular graph, to appear in *J. Combin. Thory Ser.B*.
7. R. M. DAMERELL, On Moore graphs, *Proc. Cambridge Philos. Soc.* **74** (1973), 227-236.
8. W. FEIT AND G. HIGMAN, The nonexistence of certain generalized polygons, *J. Algebra* **1** (1964), 114-131.
9. A. D. GARDINER, An elementary classification of distance-transitive graphs of valency four, to appear.
10. T. HILANO AND K. NOMURA, Distance degree regular graphs, *J. Combin. Theory Ser.B* **37** (1984), 96-100.

11. T. ITO, Bipartite distance-regular graphs of valency three, *Linear algebra and its application*, **46** (1982), 195-213.

12. A.A. Ivanov, Bounding the diameter of a distance-regular graphs, *Soviet Math. Dokl* **28** (1983), 149-152.

13. K. NOMURA, An inequality between intersection numbers of a distance-regular graph, to appear in *J. Combin. Theory Ser.B.*

14. D. H. SMITH, On tetravalent graphs, *J. London Math. Soc.* (2), **6** (1973), 659-662.

15. D. H. SMITH, Distance-transitive graphs of valency four, *J. London Math. Soc.* (2), **8** (1974), 377-384.

16. D. H. SMITH, On bipartite tetravalent graphs, *Discrete Math.* **10** (1974), 167-172.

Large Cliques in the Graphs of Quadratic Forms

東理大・理　江川　嘉美

q を奇素数べきとし，V を $GF(q)$ 上の n 次元ベクトル空間とする．(本稿で述べることは，適当に修正すれば q が2べきの場合にも成立するが，ここでは簡単のため奇素数べきの場合に限ることにする．) V 上の2次形式の全体を Q とおく．$x \in Q$ に対し，B を x に付随する対称双1次形式として，

$$\mathrm{Rad}\, x = \mathrm{Rad}\, B$$
$$= \{u \in V \mid \text{すべての } v \in V \text{ に対して } B(u,v) = 0\},$$
$$\mathrm{rk}\, x = \mathrm{rk}\, B = n - \dim(\mathrm{Rad}\, x)$$

とおく．Q 上のグラフを

$$x \text{ と } y \text{ が adjacent} \iff \mathrm{rk}(x-y) = 1 \text{ or } 2 \qquad (x, y \in Q)$$

により定義すると，Q は距離正則グラフになる([1])．ここでは，Q の極大 clique について調べる．

$x_0 \in Q$ に対し，

$$C(x_0) = \{x \in Q \mid \mathrm{rk}(x - x_0) \leq 1\}$$

とおくと，$n \geq 3$ であれば，$C(x_0)$ は位数 q^n の極大

cliqueになる．我々はこれをtype 1のcliqueと呼ぶ．
つぎに，Vの$(n-1)$次元部分空間Wと$x_0 \in Q$に対し，

$$\mathcal{C}(W, x_0) = \{x \in Q \mid x|_W = x_0|_W\}$$

とおくと，$\mathcal{C}(W, x_0)$も，$n \geq 3$であれば，位数q^nの極大cliqueになる．（ここで，$x|_W$はxのWへの制限を表す．）これをtype 2と呼ぶ．さらに，Vの$(n-2)$次元部分空間Wと$x_0 \in Q$に対し，

$$\mathcal{C}(x_0, W) = \{x \in Q \mid \mathrm{Rad}(x - x_0) \supseteq W\}$$

とおくと，$n \geq 3$であれば，$\mathcal{C}(x_0, W)$は位数q^3の極大cliqueになる．これをtype 3と呼ぶ．

J. Hemmeter ([2])は，$\mathcal{C}$をQの極大cliqueとすると，$|\mathcal{C}| \leq q^3((q^3-1)/(q-1))$であるか，または，$\mathcal{C}$はtype 1または2であることを示した．本稿の目的は，この結果がつぎのように精密化されることを注意することにある．

Main Theorem. Let $\mathcal{C}$ be a maximal clique of Q. Then $|\mathcal{C}| \leq q^2+q+2$, or $\mathcal{C}$ is of type 1, 2, or 3.

以下証明の方針を述べる．

Lemma 1. Let x, y be rank 2 quadratic forms on a 2-dimensional space V, $x \neq y$. Then

(i) There are at most two rank 1 forms z such that $x, y \in \mathcal{C}(z)$.

(ii) If there is a 1-dimensional subspace U such that $x, y \in \mathcal{C}(U, 0)$, then there is at most one rank 1 form z such that $x, y \in \mathcal{C}(z)$.

(iii) There are at most two 1-dimensional subspaces U such that $x, y \in \mathcal{C}(U, 0)$, and if there do exist two such subspaces then there is no rank 1 form z such that $x, y \in \mathcal{C}(z)$.

証明は容易である

以下 $n \geq 3$ とする.

Lemma 2. Let $\mathcal{C}_1, \mathcal{C}_2$ be distinct cliques of type 1 or 2. Then $|\mathcal{C}_1 \cap \mathcal{C}_2| \leq q+1$.

証明は, $\mathcal{C}_1, \mathcal{C}_2$ がともに type 1 の時が最も面倒だが, 結局は, $GF(q)$ において, $\alpha x^2 + \beta y^2 = \gamma$ という形の, x, y に関する方程式 (但し, $\alpha\beta\gamma \neq 0$) の解の個数は, $q+1$ 個または $q-1$ 個であるという, 古典的な結果に帰着される.

Lemma 3. Let X_1, X_2 be rank 2 forms such that $\dim(\mathrm{Rad}\, X_1 \cap \mathrm{Rad}\, X_2) = n-3$ and $\mathrm{rk}(X_1 - X_2) = 2$. Then one of the following holds:

(i) There exists a rank 1 form x_0 such that $x_1, x_2 \in \mathcal{C}(x_0)$. (Further, the form x_0 is uniquely determined.)

(ii) There exists an $(n-1)$-dimensional subspace U such that $x_1, x_2 \in \mathcal{C}(U, 0)$. (The subspace U is uniquely determined.)

証明は3次の対称行列に関する計算に帰着される

Lemma 4. Let W be a 1-dimensional subspace of a 3-dimensional space V. Let $\mathfrak{X}$ be a set of rank 2 forms having W as their radical. Let v be a rank 2 form with $\mathrm{Rad}\, v \neq W$ such that $\mathrm{rk}(x - v) = 2$ for all $x \in \mathfrak{X}$. Then one of the following holds:

(I) There exists a rank 1 form z such that $v \in \mathcal{C}(z)$ and $\mathfrak{X} \subseteq \mathcal{C}(z)$.

(II) There exists a 2-dimensional subspace U such that $v \in \mathcal{C}(U, 0)$ and $\mathfrak{X} \subseteq \mathcal{C}(U, 0)$.

Proof. Set $U = W + \mathrm{Rad}\, v$. Fix $y \in \mathfrak{X}$. Note that if v and y are as in (i) of Lemma 3 then $v(U) \neq 0$, and if they are as in (ii) then $v(U) = 0$. Thus in the latter case, v and x are related as in Lemma 3 (ii) for every $x \in \mathfrak{X}$. That is, (II) holds. Suppose then that v and y are related as

in Lemma 3(i). Let T denote the 2-dimensional subspace orthogonal to U with respect to v. Let z be the form defined by

$$\mathrm{Rad}\ z = U, \qquad v|_T = z|_T.$$

Then z is of rank 1, and $x, y \in \mathcal{C}(z)$. The definition of z, however, did not depend on y. Hence (I) holds.

Lemma 5. Let X_1, X_2 and X_3 be pairwise adjacent rank 2 quadratic forms, with associated bilinear forms B_1, B_2 and B_3. If there is no $(n-3)$-dimensional subspace contained in the radicals of all three X_i, then one of the following holds:

(i) There exists a rank 1 form X_0 such that $X_i \in \mathcal{C}(X_0)$ for $i = 1, 2, 3$.

(ii) There exists an $(n-1)$-dimensional subspace W such that $X_i \in \mathcal{C}(W, 0)$ for $i = 1, 2, 3$.

Proof. Case 1: X_1 and X_2 are as in Lemma 3(i).

Let X_0 be also as in Lemma 3(i), and let B_0 be its associated bilinear form. By way of contradiction, suppose $\mathrm{rk}(B_3 - B_0) \geq 2$. Then $\mathrm{Rad}(B_3 - B_0) = \mathrm{Rad}\ B_3 \cap \mathrm{Rad}\ B_0$. From $\mathrm{rk}((B_3 - B_0) - (B_1 - B_0)) = 2$ and $\mathrm{rk}((B_3 - B_0) - (B_2 - B_0)) = 2$, we obtain also $\mathrm{Rad}(B_3 - B_0) \subseteq \mathrm{Rad}(B_1 - B_0) \cap \mathrm{Rad}(B_2 - B_0)$. So

$$\begin{aligned}\mathrm{Rad}(B_3 - B_0) &\subseteq \mathrm{Rad}(B_1 - B_0) \cap \mathrm{Rad}(B_2 - B_0) \cap \mathrm{Rad}\ B_0 \\ &= \mathrm{Rad}\ B_1 \cap \mathrm{Rad}\ B_2.\end{aligned}$$

Since $\mathrm{rk}(B_3 - B_0) \leq 3$, $\mathrm{Rad}(B_3 - B_0) = \mathrm{Rad}\, B_1 \cap \mathrm{Rad}\, B_2$. But then we have an $(n-3)$-dimensional, namely $\mathrm{Rad}\, B_1 \cap \mathrm{Rad}\, B_2$, contained in the radical of each of x_1, x_2 and x_3, a contradiction. Hence $\mathrm{rk}(B_3 - B_0) = 1$ and we have (i).

Case 2: x_1 and x_2 are related as in Lemma 3 (ii).

There exists an $(n-1)$-dimensional subspace W such that $B_1|_W = B_2|_W = 0$. Suppose $B_3|_W \neq 0$. If either x_1 and x_3 or x_2 and x_3 were related as in Lemma 3(i), we would end up in Case 1. So we may assume that there exist $(n-1)$-dimensional subspaces W_1, W_2 with $W_1 \neq W \neq W_2$ such that $B_1|_{W_1} = B_3|_{W_1} = 0$ and $B_2|_{W_2} = B_3|_{W_2} = 0$. If $W_1 = W_2$, then $\mathrm{Rad}\, B_1 = W_1 \cap W = W_2 \cap W = \mathrm{Rad}\, B_2$, a contradiction. If $W_1 \neq W_2$, then $\mathrm{Rad}\, B_3 = W_1 \cap W_2 \supseteq \mathrm{Rad}\, B_1 \cap \mathrm{Rad}\, B_2$, another contradiction. Thus $B_3|_W = 0$ after all.

Proof of the Main Theorem. We may assume $0 \in \mathcal{C}$.

Case 1: $\mathcal{C}$ has no rank 2 forms. Then $\mathcal{C}$ must be $\mathcal{C}(0)$.

Case 2: There exist rank 2 forms x_1, x_2 and $x_3 \in \mathcal{C}$ whose radicals do not all contain any $(n-3)$-dimensional subspace. In this case, we easily get the desired conclusion from Lemma 5.

Case 3: $\mathcal{C}$ has at least one rank 2 form, but the

radical of each rank 2 form contains some $(n-3)$-dimensional subspace. In this case, we may assume $\dim V = 3$. Also assume $\mathcal{C}$ is not of type 3. For each 1-dimensional subspace W, let $\mathcal{C}_W$ denote the set of the forms belonging to $\mathcal{C}$ whose radical is W. Assume first that $\mathcal{C}$ contains no rank 1 form. Then as $q^2 + q + 2 = (q^3 - 1)/(q - 1) + 1$, we may assume that there exists a 1-dimensional subspace, say W_0, such that $|\mathcal{C}_{W_0}| \geq 2$. Pick $0 \neq v \in \mathcal{C} - \mathcal{C}_{W_0}$. Then by Lemma 4, one of the following holds:

(i) There exists a rank 1 form z such that $v \in \mathcal{C}(z)$ and $\mathcal{C}_{W_0} \subseteq \mathcal{C}(z)$.

(ii) There exists a 2-dimensional subspace U such that $v \in \mathcal{C}(U, 0)$ and $\mathcal{C}_{W_0} \subseteq \mathcal{C}(U, 0)$.

If there exists a rank 1 form z such that (i) holds for all $0 \neq v \in \mathcal{C} - \mathcal{C}_{W_0}$, then $\mathcal{C} = \mathcal{C}(z)$. In fact, under our assumption that $\mathcal{C}$ contains no rank 1 form, this is impossible. Likewise, there can be no 2-dimensional subspace U such that (ii) holds for all $0 \neq v \in \mathcal{C} - \mathcal{C}_{W_0}$, lest $\mathcal{C}$ be $\mathcal{C}(U, 0)$.

Thus we have $|\mathcal{C}_{W_0}| \leq q$ by Lemma 2. Further, we see from Lemma 1 that one of the follwing holds:

(iii) There exist two distinct rank 1 forms z_1, z_2 such that for each $0 \neq v \in \mathcal{C} - \mathcal{C}_{W_0}$, one of z_1 or z_2 satisfies (i).

(vi) There exist a rank 1 form z_1 and a 2-dimensional subspace U_2 such that for each $0 \neq v \in \mathcal{C} - \mathcal{C}_{W_0}$, either z_1 satisfies (i), or U_2 satisfies (ii).

(v) There exist two distinct 2-dimensional subspaces U_1, U_2 such that for each $0 \neq v \in \mathcal{C} - \mathcal{C}_{W_0}$, one of U_1 or U_2 satisfies (ii).

If (iii) or (iv) occurs, then set $U_i = \mathrm{Rad}\, z_i$. Then in any case, each 1-dimensional subspace W with $\mathcal{C}_W \neq \phi$ is contained in U_1 or U_2. Set

$$\mathcal{W}_i = \{W \subseteq U_i \mid \dim W = 1,\ \mathcal{C}_W \neq \phi,\ W \neq W_0\}, \qquad i = 1, 2.$$

Clearly $|\mathcal{W}_i| \leq q$. Also the above argument shows that $|\mathcal{C}_W| \leq q$ for all $W \in \mathcal{W}_1 \cup \mathcal{W}_2$. If $|\mathcal{C}_W| = 1$ for all $W \in \mathcal{W}_1 \cup \mathcal{W}_2$, then $|\mathcal{C}| \leq 2q + q + 1$. Therefore we may assume, by symmetry, that there exists $W_1 \in \mathcal{W}_1$ such that $|\mathcal{C}_{W_1}| \geq 2$. Pick $W_2 \in \mathcal{W}_2$. Arguing as above with W_1 in place of W_0, we see that each 1-dimensional subspace W with $\mathcal{C}_W \neq \phi$ is contained in $W_1 + W_2$ or U_1. This means $\mathcal{W}_2 = \{W_2\}$. If $|\mathcal{C}_{W_2}| \geq 2$, then a similar argument yields $\mathcal{W}_1 = \{W_1\}$, which implies $|\mathcal{C}| \leq 3q + 1$. On the other hand, if $|\mathcal{C}_{W_2}| = 1$, then we have $|\mathcal{C}| \leq q(q + 1) + 1 + 1$.

Now assume that $\mathcal{C}$ contains some rank 1 form, say b. If $\mathcal{C}$ contains another rank 1 form x with $\mathrm{Rad}\, x \neq \mathrm{Rad}\, b$, then $\mathcal{C}$ must be of type 1 or 3. So we may assume that all rank 1 forms belonging to $\mathcal{C}$ have the same radical as b. Note that

$$\mathrm{Rad}\, v \subseteq \mathrm{Rad}\, b \quad \text{for all rank 2 forms } v \in \mathcal{C}. \tag{*}$$

Thus we may again assume that there exists a 1-dimensional subspace W_0 such that $|\mathcal{C}_{W_0}| \geq 2$. Pick a rank 2 form $v \in \mathcal{C} - \mathcal{C}_{W_0}$. Then again (i) or (ii) holds. But (*) implies that if (i) occurs then $\mathrm{Rad}\, z$ must coincide with $\mathrm{Rad}\, b$ and so $x(\mathrm{Rad}\, b) \neq 0$ for all $x \in \mathcal{C}_{W_0}$, and that if (ii) occurs then U must coincide with $\mathrm{Rad}\, b$ and so $x(\mathrm{Rad}\, b) = 0$ for all $x \in \mathcal{C}_{W_0}$. Now the observation made immediately after the statement of (i), (ii) together with the argument used in the proof of Lemma 4 yields that $\mathcal{C}$ is of type 1 or 2.

---

1. Y. Egawa, Association schemes of quadratic forms, J. Combin. Theory Ser. A 38 (1985), 1-14.

2. J. Hemmeter, The large cliques in the graph of quadratic forms, preprint.

群とグラフに関する幾つかの結果

城西大・理　芳沢光雄

(I) ある種の sharply t-transitive sets について.

Ω: finite set, $t(\geq 2)$: integer に対し、
S^Ω の subset G が t-transitive set
$\overset{\text{def.}}{\Leftrightarrow}$ $\forall \alpha_1, \overset{\neq}{\cdots}, \alpha_t$, $\forall \beta_1, \overset{\neq}{\cdots}, \beta_t \in \Omega$ に対し
$|\{g \in G \mid g(\alpha_i) = \beta_i,\ i=1,\cdots,t\}| = c$ (const).
とくに $c=1$ のとき、G を sharply t-trans set という。

G に次のように距離を入れる。
$G \ni \forall g, g'$ に対し $\partial(g,g') := |\Omega| - (g^{-1}g' \text{ の固定点数})$.

この距離により G が association scheme をなすとき、G を schematic という。以下 schem sharply t-trans set について考えることにする。

最初に例であるが、$t=2$ については全て o.k.
又、A_5 $(t=3)$ が例になることも易しく分かる。

さらに $PSL(2,8)$ $(t=3)$ も例になる。これについては、$PFL(2,8)$ 内で共役類を考えれば、ほとんどの事については check できるが、一部計算機を使って check した。一般の $PSL(2,2^n)$ $(t\geq 3)$ も全て例になると予想できるが、M_{10} $(t=3)$, M_{11} $(t=4)$ について計算機で調べたところ、これらは schematic にはならなかった。

一般的な結果として、次の Th. を得た。

Th. Ω 上の sharply t-trans set G が schem
$\Rightarrow$ $2t-1 \leq k := |\Omega|$.

証明の概略: $k \leq 2t-2$ として矛盾を出す。

最初に G の元 g に対し、g から距離 $k-i$ $(i=0,\cdots,t)$ にある G の元の個数は

$$\sum_{s=i}^{t-1} \binom{s}{i}\binom{k}{s}\{(k-s)(k-s-1)\cdots(k-t+1)-1\}(-1)^{s+i}$$

になることを示す。これから G には次のような3元 g_1, g_2, g_3 があることを得る。ただし $n=k-t$ とおく。

$$\partial(g_1,g_2)=2n+2,\quad \partial(g_1,g_3)=\partial(g_2,g_3)=n+1.$$

今、g_1, g_2 を fix し、g_1, g_2 から共に距離 $n+1$ にある元

の個数を調べると、それは次の式になる。

$$\frac{\binom{t-1}{n+1}n\binom{t+n}{n+1}n}{\sum_{i=t-n-2}^{t-1}\binom{i}{t-n-2}\binom{t+n}{i}\{(t+n-i)(t+n-i-1)\cdots(n+1)-1\}(-1)^{i+t-n-2}}$$

上の式の値は整数になることから、予想を得る。

(II) 群を表わすグラフについて。

Frucht (1948) は任意の有限群Gに対し、$\mathrm{Aut}\Gamma\cong G$ となる connected 3-regular graph Γ の存在を示し、Sabidussi (1957) は任意の有限群Gと任意の自然数 $n\geq 3$ に対し、$\mathrm{Aut}\Gamma\cong G$ となる conn. n-reg. graph Γ の存在を示した。最近 Vogler (1984) は $|V\Delta|\geq 3$ をみたす孤立点を含む任意の constant link Δ と任意の有限群Gに対し、$\mathrm{Aut}\Gamma\cong G$, Δ は Γ の const link, となる conn. graph Γ の存在を示した。尚、Δ が Γ の const link になるとは次のときにいう：$V\Gamma\ni\forall\alpha$ に対し $N(\alpha)-\{\alpha\}$ (α から距離1にある点全体に制限した subgraph) $\cong\Delta$ (グラフ)。

nK_1 は $K_{n,n}$ の const link になるので Vogler の結果は Sabidussi の結果の拡張になっている。

さて群を無限群に目を向けると、Sabidussi が 1960 年に、任意の無限群を自己同型群にもつ conn graph の存在を示している。Vogler の結果を拡張して次の結果を得た。

Th. Δ:(有限グラフの) const link, $|V\Delta| \geq 3$, Δ は孤立点をもつ。

$\Rightarrow$ 任意の countable group G に対し、$\mathrm{Aut}\Gamma \cong G$, Δ は Γ の const link, となる conn graph Γ が存在。

証明の方針： $i=3,4,5$ に対し、$\mathrm{Aut}(\Gamma_i) \cong G$ となる conn. i-reg graph Γ_i の存在を示す。

次に Sabidussi の graph multiplication の方法により、i を 3 以上の任意の自然数に拡張する。

最後に Vogler の方法により、自己同型群が変わらないように、Γ_i の各頂点に const link Δ を技工的につける。

(III) subdivided $K_{3,3}$ をもたないグラフで表わされる群について.

平面グラフの自己同型群として表わされる群は、本質的にはトポロジーから決定されるそうです。さて、平面グラフは subdivided $K_{3,3}$ も subdivided K_5 も持たないグラフと同じである (Kuratowski の定理)。
subdivided $K_{3,3}$ を持たないグラフで表わされる群について、次の(実験的な)結果を得た。(勿論、目標としては、subdivided $K_{3,3}$ を持たないグラフで表わされる群の分類にあります。)

Prop.1 Γ: subdivided $K_{3,3}$ をもたない conn graph (必ずしも regular graph でなくてもよい), $G \leq Aut\Gamma$, $G \curvearrowright V\Gamma$ semiregular, $P \in Syl_p(G)$.

$\Rightarrow$
- p: odd のとき P は cyclic,
- $p=2$ のとき、P の任意の可換部分群 Q (order 2^t) をとると、$Q = Z_{2^t}$, $Z_{2^{t-1}} \times Z_2$ or $Z_2 \times Z_2 \times Z_2$.

証明の概略: G の $V\Gamma$ 上の orbit 分解を $\Delta_1, \Delta_2, \cdots, \Delta_s$ とする。

$\exists w_i \in \Delta_i$ $(i=1,\cdots,s)$ s.t. $\Delta = [\{w_1,\cdots,w_s\}]$ (induced subgraph) は connected, ということが分かる。

$|V\Gamma| = \sum_{g\in G} g(V\Delta)$ である。次のグラフ $\overline{\Gamma}$ を定める。

$\overline{\Gamma}$: $\begin{cases} V\overline{\Gamma} = \{g(V\Delta) : g\in G\}, \\ E\overline{\Gamma} = \{\{g(V\Delta), g'(V\Delta)\} : g(V\Delta) と g'(V\Delta) を結ぶ \Gamma \\ \qquad\qquad\qquad\qquad の辺がある。\} \end{cases}$.

$G \le Aut(\overline{\Gamma})$ で, $G \curvearrowright V\overline{\Gamma}$: regular となる。

従って、 $\overline{\Gamma}$ = Cayley graph $\overline{\Gamma}(G,H)$ となる。

又、別に調べることにより、$\overline{\Gamma}$ も subdivided $K_{3,3}$ を持たないことが分かる。

以上のことは $G = P$ (or Q) としても成り立つことなので、そのような条件のもとで調べて、結論を得る。

Prop1を使って、次のPropを得た。

Prop.2 Γ: connected graph, $|V\Gamma|$: odd とする。このとき、

Γ: C_n (circuit graph) $\Longleftrightarrow$ $\begin{cases} Aut\Gamma \curvearrowright V\Gamma$: Frobenius gp. \\ subdivided $K_{3,3}$ をもたない。 \end{cases}$

Spanning trees fixed by automorphisms of a graph

Mikio Kano 加納幹雄 Akashi Technological College
Akio Sakamoto 坂本明雄 The University of Tokushima

1. Introduction

We consider a finite graph G which has no loops and no multiple edges. We denote by V(G) and E(G) the vertex set and the edge set of G, respectively. An edge joining two vertices v and w is denoted by vw or wv. An automorphism α of G is a permutation on V(G) that preserves adjacency, that is, if e=vw is an edge of G, then $\alpha(e)=\alpha(v)\alpha(w)$ is also an edge of G. The set of automorphisms of G forms the automorphism group Aut(G). Let $\alpha\in Aut(G)$ and A be a subgroup of Aut(G). For a subset X of E(G), we write $\alpha(X)=\{\alpha(e)\in E(G) \mid e\in X\}$, and say that X is A-invariant if $\alpha(X)=X$ for all $\alpha\in A$. We write F(A) for the set of vertices of G fixed by A, that is, $F(A)=\{v\in V(G) \mid \alpha(v)=v \text{ for all } \alpha\in A\}$. We denote by G[F(A)] the subgraph of G induced by F(A). For a subset S of V(G), define the subgroup A_S of A by $A_S=\{\alpha\in A \mid \alpha(x)=x \text{ for all } x\in S\}$. If S={x}, we write A_x for A_S. Other notation and defintions not defined in this paper can be found in [1].

We consider the following problem. Let P be a property

of graphs and A be a subgroup of Aut(G). When does the graph G have an A-invariant subgraph that possesses the property P? In this paper we prove the following theorem.

Theorem Let G be a connected graph, and A be a subgroup of Aut(G). Then G has an A-invariant spanning tree if and only if one of the following conditions holds.

(i) $F(A)\neq\phi$ and the induced subgraph $G[F(A_x)]$ is connected for every vertex x of G.

(ii) $F(A)=\phi$ and A fixes an edge uw such that $F(A_x)$ contains u and w for all $x\in V(G)$. Moreover, for every vertex x of G, the induced subgraph $G[F(A_x)]$ is connected.

We now give examples. Let A be a subgroup of $Aut(K_m)$, where K_m denotes the complete graph on m vertices. Then it is easily shown by the theorem that K_{2n+1} contanis an A-invariant spanning tree if and only if A fixes at least one vertex. Furthermore, it also follows immediately from the theorem that K_{2n} contains an A-invariant spanning tree if and only if (a) A fixes at least one vertex, or (b) A fixes an edge uw such that $F(A_x)\supseteq\{u,w\}$ for all vertices x of K_{2n} (i.e. each cycle, in the cycle decomposition of every $\alpha\in A$ acting on V(G) with $\alpha(u)=w$, has even length).

2. Proof of Theorem

Proof of necessity Let T be an A-invariant spanning tree of G, where we regard T as a subset of E(G). Let B be any subgroup of A with $F(B)\neq\phi$. Let x and y be any two distinct vertices of F(B), and let P(x,y) denote the unique path in T from x to y. Then B fixes P(x,y), and so B fixes all the vertices in P(x,y). Hence G[F(B)] is connected. In particular, if $F(A)\neq\phi$, then the condition (i) holds.

We now assume $F(A)=\phi$. Since the center of T, which is clearly A-invariant, is K_1 or K_2, we obtain that the center of T is K_2 and that A fies the edge uw contained in the center of T. Let B be any subgroup of A with $F(B)\neq\phi$. Suppose u is not contained in F(B). Then $w\notin F(B)$. Take $x\in F(B)$, and choose $\beta\in B$ so that $\beta(u)=w$. Then a subset $P(x,u)\cup P(x,w)\cup uw$ of T contains a cycle, where P(x,u) is the path in T from x to u and $\beta(P(x,u))=P(x,w)$. Then we have a contradiction. Hence F(B) contains both u and w. Consequently, if $F(A)=\phi$, then the condition (ii) follows.

Proof of the sufficienly of (i) For a subgroup B of A, we denote the order of B by $|B|$.

We assume that the condition (i) holds. Put $X_0=F(A)$, and let $X_1, X_2, \ldots, X_m$ be the orbits of the permutation

group A acting on $V(G)\backslash X_0$. We construct a digraph D with vertex set $V(D)=\{X_0,X_1, \ldots ,X_m\}$ from G as follows. For any two vertices X and Y of D, (X,Y) is an arc of D if and only if there exists an edge xy of G such that $x\in X$, $y\in Y$ and $A_x\supseteq A_y$ (i.e. A_y fixes x). We shall show that D is connected and has a rooted spanning tree T* possessing the property that for every vertex X, $X\neq X_0$, there exists a path $X_0,X_a,X_b, \ldots ,X_d,X$ in T* such that (X_0,X_a), (X_a,X_b), ... , (X_d,X) are arcs of T*. In order to prove the connectivity of D and the existence of T*, it suffices to show that the following two statements hold.

(1) For each vertex $X\neq X_0$ of D, the in-degree of X is positive.

(2) For each strongly connected component C of D with $X_0\notin V(C)$, there exist vertices $X\in V(C)$ and $X'\notin V(C)$ such that (X',X) is an arc of D.

We first prove (1). Let $x\in X$. Since the induced subgraph $G[F(A_x)]$ is connected, there exists a path x,a,..., d,p,...,r,s in $G[F(A_x)]$ such that xa,...,dp,...,rs are edges, $\{x,a,\ldots,d\}\subseteq X$, $p\in X'\neq X$ and $s\in X_0$. Since A_x is included in A_a, ... , A_s and $|A_x|=|A_a|= \ldots =|A_d|$ (as X is an orbit), we obtain $A_x=A_d=A_{\{x,a,\ldots,d\}}$. Hence (X',X) is an arc of D, and so (1) is proved.

It is immediate that if (X_i,X_j) is an arc of D, then for for any vertices $a\in X_i$ and $b\in X_j$, we have $|A_a|\geq|A_b|$. Thus, if X_i and X_j are vertices of a strongly connected component of D, then for all vertices $a\in X_i$ and $b\in X_j$, we have $|A_a|=|A_b|$. We now prove (2). Take a vertex $x\in X$, $X\in V(C)$, and put $V(C)=\{X_1, X_2, \ldots, X_n\}$. Then there exists a path $x,a,\ldots,c,p,\ldots,r,s$ in $G[F(A_x)]$ such that $xa,\ldots,rs$ are edges of G, $\{x,a,\ldots,c\}\subseteq X_1\cup\ldots\cup X_n$, $c\in X_k$, $X_k\in V(C)$, $p\in X'$, $X'\notin V(C)$ and $s\in X_0$. We can similarly show that (X',X_k) is an arc of D as $A_c=A_x\subseteq A_p$. Hence (2) holds.

Let T* be a spanning tree of D given above. For each arc (X,Y) of T*, we take exactly one edge e=xy of G such that $x\in X$, $y\in Y$ and $A_x\supseteq A_y$, and let $\{e_1,\ldots,e_m\}$ be the set of such edges. Set

$$T=(\text{a spanning tree of } G[X_0])\cup\{\alpha(e_i)\mid 1\leq i\leq m,\ \alpha\in A\}.$$

Then it is obvious that T is an A-invariant connected spanning subgraph of G. Suppose T contains a cycle. Then there exists an edge $e=xy\in\{e_1,\ldots,e_m\}$ such that $\alpha(x)\neq\alpha(x)$ and $\tau(y)=\tau(y)$ for some $\alpha,\tau\in A$. Then $\tau^{-1}\alpha(x)\neq x$ and $\tau^{-1}\alpha(y)=y$, which contradicts $A_x\supseteq A_y$. Therefore, T contains no cycles, and we can conclude that T is a desired A-invariant spanning spanning tree of G.

Proof of the sufficiency of (ii) We construct a new

graph G' from G be inserting a new vertex v of degree 2 into the edge uw. Then $V(G')=V(G)\cup\{v\}$ and $E(G')=(E(G)\setminus uw)\cup\{uv,vw\}$. For every $\alpha\in A$, define the permutation α' acting on $V(G')$ by $\alpha'(x)=\alpha(x)$ for all $x\in V(G)$ and $\alpha'(v)=v$. Then α' is an automorphism of G'. The condition (ii) guarantees that G' and $A'=\{\alpha'\in Aut(G') \mid \alpha\in A\}$ satisfy the condition (i). Hence G' has an A'-invariant spanning tree T'. It is clear that T' contains edges uv and vw. Consequently, G has an A-invariant spanning tree $T=(T'\setminus\{uv,vw\})\cup\{uw\}$.

Acknowledgment One of the authors is gratefut to Professor Hiroshi Kawakami for suggesting the original version of the problem considered herein and his continuous encouragement.

References

[1] M. Behzad, G. Chartrand and L. Lesniak-Foster, Graphs & Digraphs, Prindle,Weber and Schmidt,Boston 1979.

ここで述べた定理に関連する問題としては次のようなものがある.

(a) $A\subseteq Aut(G)$ のとき GにA-不変な1-因子が存在するための必要十分条件 or 十分条件を求めよ.

(b) $A\subseteq Aut(G)$ のとき GにA-不変な odd-degree spanning subgraph (even-degree) が存在するための条件を求めよ. (各点の次数が odd (even))

グラフの連結性について

太田　克弘　　東大・理・情報

５点以上の任意の３連結グラフには、 contract しても３連結性を保存する辺（これを 3-contractibleな辺と呼ぶ）が、存在した。しかし、contract して、４連結性を保存する辺を一つも持たない４連結グラフが無数に存在することが分かっている。そこで、４連結性を保存するような、グラフの変形操作を考える。

xyz を４連結グラフ G の長さ２の path とする。このとき、

$$\Gamma_G(y) - \{x, z\} = A \cup B \qquad \text{(partition)}$$

に対し、 G から y を取り去って、 x と A の点及び、 z と B の点をつなぎ、さらに x と z をつないで出来るグラフを、 G' とおく。($A = \emptyset$ のとき、この操作は辺 yz の contraction である。) G' が４連結のとき、G から G' を作るこの操作を、xyz における P_3-reduction と呼ぶことにする。 xyzにおいて P_3-reduction が出来るためには、 $G - \{x, y, z\}$ ：２連結でなければならない。

<u>補題１</u>．　６点以上の４連結グラフ G の任意の点 y に対して、 $G - \{x, y, z\}$ ：２連結となる x, z が存在する。

<u>補題２</u>．　６点以上の４連結グラフ G の長さ２のパス xyz が、 $G - \{x, y, z\}$ ：２連結 を満たすとき、

（I）　$xz \in E(G)$ ならば、xyzにおいて P_3-reduction が存在する。

（II）　xyz において P_3-reduction が存在しないならば、xyw 及び wyz において P_3-reduction が存在するような $w \in \Gamma_G(y) - \{x, z\}$ が存在す

る。

すなわち、補題1・2より、次の定理が得られたわけである。

定理3． 6点以上の4連結グラフ G の任意の点 y の回りに P_3-reduction が存在する。

一方、補題1は、K_5 を除く任意の4連結グラフの任意の点に対して、その点及びその点の適当な2点近傍を取り除いてできるグラフが2連結となるようにできることを意味している。一般に n連結グラフから m点を取り除くと、$n-m$連結は保証されるが、上の場合さらにもう1連結を保証しているわけである。ここでは、1点とその近傍という形の m点で、取り除いたとき連結度を1だけかせぐものについて考える。ある m についてこの様な点集合があったとすれば、もう1点付け加えて $m+1$点にしても連結度を1だけかせぐことができる。したがって、次の定義に意味がある。すなわち、

定義1． $n+2$点以上の任意の n連結グラフ G の任意の点 y に対して、$\Gamma_G(y)$ の適当な r点部分集合 S を選ぶと、$G-(\{y\}\cup S)$ が $n-r$連結グラフとできるような最小の r を $r(n)$ と書くことにする。

一般に、$K_{n+2}-\{\ \left\lfloor\frac{n+1}{2}\right\rfloor$-independent edges $\}$ を考えたときに、$r=\left\lfloor\frac{n}{2}\right\rfloor-1$ とすると、任意の点とその近傍の任意の n点に対し、これらの $r+1$点全てと隣接する次数 n の点が存在するので、$r(n)\geqq\left\lceil\frac{n}{2}\right\rceil$ が分かる。このことと補題1を用いると、$r(4)=2$ を得る。

また、$r(n+1)\leqq r(n)+1$ が成り立つので $r(5)=3$ である。容易に $r(1)=r(2)=1$, $r(3)=2$ も示されるので、上の下限で等号が成立すると思われる。

予想4. $r(n) = \left\lceil \frac{n}{2} \right\rceil$。

この予想は、次の Slater の予想を含んでいる。

予想5. [Slater, 1977] $2k > n$ に対し、K_{n+1} が唯一の (n,k)-グラフである。

但し、(n,k)-グラフ G とは、任意の k 点以下の点集合 S に対し、$G - S$ の連結度が $n - |S|$ になるグラフのことである。

予想4の肯定的な結論として、次の定理を得た。

定理6. $r(6) = 3$.

定理6から $r(n)$ の上限として、次の系を得る。

系7. $n \geqq 5$ ならば、$r(n) \leqq n-3$. 特に、$r(7) = 3$.

定義1において、「任意の点」を「ある点」に変えるとどうなるであろうか。

定義2. $n+2$点以上の任意の n連結グラフ G に対して、ある点 y が存在して、$\Gamma_G(y)$ の適当な r点部分集合をとると、$G - (\{y\} \cup S)$ が $n-r$連結になるような最小の r を $r'(n)$ と書く。

$r'(n)$ については、次のことが分かる。

☆ $\left\lfloor \frac{n}{2} \right\rfloor \leqq r'(n) \leqq r(n)$.

従って、具体的な n で、自明に分かるものは以下のものである。

☆ $r'(1) = 0$.

☆ $r'(2) = r'(3) = 1$.

☆ $r'(4) = 2$.

☆ $r'(6) = 3$.

予想8．　$r'(n) = \left\lfloor \frac{n}{2} \right\rfloor$.

この予想も、Slaterの予想（予想5）を含んでいる。

$n = 5$ については、少し強い形で肯定的に解決された。得られた結果は、

定理9．7点以上の5連結グラフ G の次数5の任意の点 y に対して、$\Gamma_G(y)$ の適当な2点 x, z を選ぶと、$G - \{x,y,z\}$ が3連結になるようにできる。

これは、3連結グラフに関する次の定理のアナロジーになっている。

定理10．[Ando, Enomoto & Saito]　5点以上の3連結グラフの次数3の任意の点には、3-contractibleな辺が接続している。

任意の奇数連結グラフに対して、このタイプの命題が成り立つと思われる。

予想11．　$2k+3$点以上の $2k+1$連結グラフ G の次数 $2k+1$ の任意の点 y に対して、$\Gamma_G(y)$ の適当な k点部分集合 S を選ぶと、$G - (\{y\} \cup S)$ が $k+1$連結になる。

最後に、これよりさらに強い予想として、以下を挙げておく。

予想12．　$2k+3$点以上の $2k+1$連結グラフ G の任意の $2k+2$点部分集合 W に対し、W のちょうど $k+1$点を含み、残りの $k+1$点と交わらない $k+1$連結部分グラフが存在する。