数理解析研究所講究録
第802巻 1992年 122-127


# ベア部分平面の分割と射影線型変換

(株) 東芝 システム・ソフトウェア技術研究所　上村 秀一* ( Shuichi Kamimura )
筑波大学 社会工学系　藤原 良　( Ryoh　Fuji-Hara )

## 1. 序

有限射影平面 $PG(2,q^2)$ の1つのベア部分平面[1]$\mathcal{P}$と排反なベア部分平面全体の集合$\boldsymbol{B}$は $q^4(q-1)^3(q+1)/3$ 個の要素からなる．$\boldsymbol{B}$を $q^3(q-1)^2(q+1)/3$ 個の $(q^2-q)$-部分集合[2]に分けたとき，任意の1つの $(q^2-q)$-部分集合に属する任意の異なる2つの要素（ベア部分平面）が排反になるように，$\boldsymbol{B}$を分けることを$\boldsymbol{B}$を $(q^2-q)$-部分集合に分解するという．$\boldsymbol{B}$を分解できることはまだ証明されていない．しかしながら，ベア部分平面$\mathcal{P}$上のサイクリック[3]な射影線型変換[4]全体の集合を使うと，ある仮定のもとで$\boldsymbol{B}$を $(q^2-q)$-部分集合に分解できることが証明できる．

サイクリックな射影線型変換全体の集合を共役[5]という同値関係で共役類と呼ばれる同値類に分けたとき，同じ仮定のもとで1つの共役類しか使わなくとも$\boldsymbol{B}$を分解できることを示す．それゆえ，1つの共役類に対してその仮定がいつでも成り立つことを示せば問題が肯定的に解決する．

点集合$\boldsymbol{V}$をベア部分平面$\mathcal{P}$に属さない $PG(2,q^2)$ の点全体の集合とする．そのとき，結合関係 $(\boldsymbol{V},\boldsymbol{B})$ から水準数が素数巾ではない直交配列[6]を構成できることがわかっている [8]．$\boldsymbol{B}$が $(q^2-q)$-部分集合に分解可能ならば，結合関係 $(\boldsymbol{V},\boldsymbol{B})$ から水準数が素数巾ではなくかつ分解可能[7]な直交配列を構成できる．

計算機実験によって，$q=2,3$ の場合，ベア部分平面と射影線型変換のすべての場合を尽くして，$\boldsymbol{B}$を分けられることを確認した．ここでは，第6節に $q=2$ の場合のみ分解と直交配列の例を載せる．

## 2. ベア部分平面

オーダー $r$の有限射影平面 $PG(2,r)$ の真の部分平面 $PG(2,q)$ が次の2条件を満たすならばベア部分平面である．

1. $PG(2,r)$ のすべての線は $PG(2,q)$ の少なくとも1点と結合している．

2. $PG(2,r)$ のすべての点は $PG(2,q)$ の少なくとも1線と結合している．

---

[1] Baer subplane
[2] 要素数が $q^2-q$ である部分集合．後に分割クラスと呼ぶ．
[3] cyclic
[4] projectivity
[5] conjugate
[6] orthogonal array
[7] resolvable

$PG(2,r)$ に部分平面 $PG(2,q)$ が存在するとき，$PG(2,q)$ がベア部分平面であることと $r=q^2$ は同値である [2] [5].

$\mathcal{P}$ を $PG(2,q^2)$ のベア部分平面とする．そのとき，$\mathcal{P}$ と排反なベア部分平面の数 $|\boldsymbol{B}|$ は

$$q^4(q-1)^3(q+1)/3$$

であることを Bose, Freeman, Glynn [1] が示した.

## 3. 射影線型変換

この節では Hirschfeld [3] [4] が示した結果を紹介する．Hirschfeld の結果は，平面だけでなく一般次元の射影幾何について述べていたが，ここでは射影平面しか扱わないので彼の結果を平面に限って述べる.

射影線型変換は結合関係を保存する $PG(2,q)$ からそれ自身への全単射であり，行列で表せる写像である．射影線型変換 $\mathcal{A}$ が $PG(2,q)$ のすべての点を 1 サイクルで巡るとき，その射影線型変換[8]はサイクリックであると言う．そのとき，$\mathcal{A}^i=I$ となる最小の正整数 $i$ は $PG(2,q)$ の点の数 $(q^2+q+1)$ である.

$PG(2,q)$ のサイクリックな射影線型変換の数は，

$$q^3(q-1)^2(q+1)\phi(q^2+q+1)/3$$

であることを Hirschfeld [3] [4] が示した．ただし，$\phi$ はオイラー関数である.

いくつかの互いに排反なベア部分平面が有限射影平面 $PG(2,q^2)$ を覆っているとき，そのベア部分平面の集合をタイリング[9]と呼ぶ．1 つのタイリングは $q^2-q+1$ 個[10]のベア部分平面を持つ.

Hirschfeld [3] [4] が次の定理を示した.

**定理**

有限射影平面 $PG(2,q^2)$ の射影線型変換 $\mathcal{A}$ がベア部分平面 $PG(2,q)$ 上でサイクリックならば，

1. $PG(2,q^2)$ 上のサイクリックな射影線型変換 $\mathcal{T}$ のうち $\mathcal{T}^{q^2-q+1}=\mathcal{A}$ であるようなものが存在する.

2. $\mathcal{A}$ の軌道[11]はそれぞれ $PG(2,q^2)$ のベア部分平面である.

3. $\mathcal{A}$ の軌道全体の集合はタイリングである． □

[8] 恒等変換を $I$ で表わす.
[9] tiling
[10] $|PG(2,q^2)|/|PG(2,q)|=(q^4+q^2+1)/(q^2+q+1)=q^2-q+1$
[11] orbit

## 4. ベア部分平面による分割クラスへの分解

前節の Hirschfeld の定理から，$PG(2,q^2)$ の 1 つのベア部分平面 $\mathcal{P}$ を固定したとき，$\mathcal{P}$ 上のサイクリックな射影線型変換に対応する数だけ，タイリングが同じものを含めて存在する．$\mathcal{P}$ は $PG(2,q)$ であるから，つまり延べ $q^3(q-1)^2(q+1)\phi(q^2+q+1)/3$ 個のタイリングが存在し，それらはすべて固定したベア部分平面 $\mathcal{P}$ を含んでいる．

延べ $q^3(q-1)^2(q+1)\phi(q^2+q+1)/3$ 個のタイリングのうち同一のものが $\phi(q^2+q+1)$ 個ずつある．なぜなら，2 つのサイクリックな射影線型変換 $\mathcal{A},\mathcal{B}$ に対して $\mathcal{B}=\mathcal{A}^i$ となる整数 $i$ が存在するならば，$\mathcal{A}$ と $\mathcal{B}$ の軌道は同一であり，$\mathcal{A}$ と $\mathcal{B}$ が作るタイリングは同じである．$\mathcal{B}$ がサイクリックなので $i$ は $q^2+q+1$ と互いに素である．よって固定したベア部分平面を $\mathcal{P}$ を含むタイリングの数は

$$R = q^3(q-1)^2(q+1)/3 = \frac{q^3(q-1)^2(q+1)\phi(q^2+q+1)/3}{\phi(q^2+q+1)}$$

である．

$PG(2,q^2)$ の点集合の部分集合 $\boldsymbol{V}$ を，固定したベア部分平面 $\mathcal{P}$ に属さない点全体[12] とする．ベア部分平面の集合 $\boldsymbol{B}$ を $\mathcal{P}$ と排反なベア部分平面全体とする．$q^2-q$ 個の $\boldsymbol{B}$ のベア部分平面が $\boldsymbol{V}$ を覆う[13] とき，この $q^2-q$ 個のベア部分平面を $\boldsymbol{V}$ の分割という．$\boldsymbol{B}$ を $\boldsymbol{V}$ の分割に分解できるとき，その分割を分割クラスと呼ぶ．

$\mathcal{P}$ を含むタイリングの 1 つが $\{\mathcal{P},\mathcal{P}_1,\mathcal{P}_2,\ldots,\mathcal{P}_{q^2-q}\}$ であるとき，このタイリングから固定したベア部分平面 $\mathcal{P}$ を除いた $\{\mathcal{P}_1,\mathcal{P}_2,\ldots,\mathcal{P}_{q^2-q}\}$ は $\boldsymbol{V}$ の分割になる．$\mathcal{P}$ を含むタイリングの数，$R$ 個だけ，$\boldsymbol{B}$ の分割が見つかる．

$$\begin{array}{lll} \text{分割 } 1 & \boldsymbol{R}_1 & = \{\mathcal{P}_1^1,\mathcal{P}_2^1,\ldots,\mathcal{P}_{q^2-q}^1\} \\ \text{分割 } 2 & \boldsymbol{R}_2 & = \{\mathcal{P}_1^2,\mathcal{P}_2^2,\ldots,\mathcal{P}_{q^2-q}^2\} \\ \vdots & \vdots & \vdots \\ \text{分割 } R & \boldsymbol{R}_R & = \{\mathcal{P}_1^R,\mathcal{P}_2^R,\ldots,\mathcal{P}_{q^2-q}^R\} \end{array}$$

$R$ 個の分割に $\boldsymbol{B}$ のベア部分平面が延べ $\sum_i^R |\boldsymbol{R}_i|$ 個現れている．

$$\sum_i^R |\boldsymbol{R}_i| = R\cdot(q^2-q) = q^4(q-1)^3(q+1)/3$$

この数はちょうど $\boldsymbol{B}$ の要素数と一致している．任意の分割 $\boldsymbol{R}_i$ は $\boldsymbol{B}$ の部分集合であるので，「$R$ 個の分割のうちどの異なる 2 つも互いに排反である」と仮定すれば，$R$ 個の分割に $\boldsymbol{B}$ のすべてのベア部分平面が現れている．すると，$\boldsymbol{B}=\boldsymbol{R}_1\cup\boldsymbol{R}_2\cup\ldots\cup\boldsymbol{R}_R$ であり，$\boldsymbol{B}$ は分割クラスに分解される．しかしながら，「$R$ 個の分割のうちどの異なる 2 つも互いに排反である」かどうかは未証明のままである．

## 5. 射影線型変換の共役類

射影線型変換 $\mathcal{A},\mathcal{B}$ に対して，$\mathcal{A}=\mathcal{H}^{-1}\mathcal{B}\mathcal{H}$ となる射影線型変換 $\mathcal{H}$ が存在するならば，$\mathcal{A},\mathcal{B}$ は共役であるという．共役は同値関係であるので，同値類に分けられる．この同値類を共役類と呼ぶ．

[12] $|V| = (q^4+q^2+1)-(q^2+q+1) = q^4-q$

[13] $|V|/(q^2-q) = q^2+q+1 =$ [1 つのベア部分平面の大きさ]

共役な射影線型変換$\mathcal{A}, \mathcal{B}$を表わす行列が$\mathbf{A}, \mathbf{B}$であるとき，$\mathbf{A} = \mathbf{H}^{-1}\mathbf{B}\mathbf{H}$であるような行列$\mathbf{H}$が存在する．行列$\mathbf{A}, \mathbf{B}$の特性多項式は同じである．Hircshfeld [4] と Room, Kirkpatrick [7] が示した事実を用いると，2つのサイクリックな射影線型変換を表わす行列の特性多項式が一致するならば，それらの射影線型変換は共役であることがわかる．

$\mathcal{A}$をサイクリックな射影線型変換とする．そのとき，$\mathcal{A}^q$もサイクリックな射影線型変換である．$\mathcal{A}$を表わす行列が$\mathbf{A}$であるとき，$\mathcal{A}^q$を表わす行列は$\mathbf{A}^q$である．$q$は有限体の標数なので，行列$\mathbf{A}$と$\mathbf{A}^q$は同じ固有値を持ち，特性多項式が一致する．つまり，$\mathcal{A}, \mathcal{A}^q, \mathcal{A}^{q^2}$は同じ共役類にある．しかも，$\mathcal{A}$の巾乗に関してはこれらしか同じ共役類にない[14]．

任意の軌道に対してそれを決定するサイクリックな射影線型変換は$\mathcal{A}^i$（$i$は$q^2+q+1$と互いに素）であり，$\phi(q^2+q+1)$個ずつあるので，$\phi(q^2+q+1)$個ずつ同じ分割クラスが出てくる．サイクリックな射影線型変換を表わす行列の性質から，$\phi(q^2+q+1)$個の射影線型変換$\mathcal{A}^i$の3つずつ[15]が同一の共役類に属しており，共役類の数は$\phi(q^2+q+1)/3$個である．

例えば，$q=3$，$\mathcal{A}$を$\mathcal{P}$上のサイクリックな射影線型変換とする．そのとき，$\mathcal{A}^2, \mathcal{A}^3, \mathcal{A}^4, \mathcal{A}^5, \mathcal{A}^6, \mathcal{A}^7, \mathcal{A}^8, \mathcal{A}^9, \mathcal{A}^{10}, \mathcal{A}^{11}, \mathcal{A}^{12}$もサイクリックな射影線型変換であり，次のように共役類に属している．

$$
\begin{aligned}
&\text{共役類}1 \ni \mathcal{A}, \mathcal{A}^3, \mathcal{A}^9 \\
&\text{共役類}2 \ni \mathcal{A}^2, \mathcal{A}^6, \mathcal{A}^5 \\
&\text{共役類}3 \ni \mathcal{A}^4, \mathcal{A}^{12}, \mathcal{A}^{10} \\
&\text{共役類}4 \ni \mathcal{A}^7, \mathcal{A}^8, \mathcal{A}^{11}
\end{aligned}
$$

前節で$\boldsymbol{B}$を分割クラスに分解するとき，ベア部分平面$\mathcal{P}$上のサイクリックな射影線型変換全体を使い，それらの軌道から分割クラスを得ていた．任意の軌道に対して，それを決定する$\phi(q^2+q+1)$個のサイクリックな射影線型変換はすべての共役類にまんべんなく散らばっているので，$\boldsymbol{B}$の分割クラスを得るために$\mathcal{P}$上のサイクリックな射影線型変換全体を使わなくとも，1つの共役類で十分である．共役類の大きさはサイクリックな射影線型変換の集合より小さく（$3/\phi(q^2+q+1)$）扱いやすいと考えられる．また，共役類は，特性多項式が同一であるという条件の付いた射影線型変換の集合でもある．これらの理由から，共役類の上に限って考えると，未証明のままである仮定を見通しよく証明できるようになると考える．

## 6. $\mathbf{q=2}$の場合

点集合$\boldsymbol{V}$をベア部分平面$\mathcal{P}$に属さない$PG(2,q^2)$の点全体の集合，ベア部分平面の集合$\boldsymbol{B}$を$\mathcal{P}$と排反なベア部分平面全体の集合とする．そのとき，結合関係$(\boldsymbol{V}, \boldsymbol{B})$から水準数が素数巾ではない直交配列[16]を構成できることが示されている [8]．ベア部分平面の集合$\boldsymbol{B}$を分割クラスへ分解できるならば，結合関係$(\boldsymbol{V}, \boldsymbol{B})$から水準数が素数巾ではなくかつ分解可能な直交配列を構成できる．

[14]行列$\mathbf{A}$の特性多項式の根の数が3だから

[15]$\mathcal{A}^i$, $\mathcal{A}^{iq}$, $\mathcal{A}^{iq^2}$

[16]orthogonal array

$PG(2,2^2)$の点集合を$\{0,1,2,\ldots,20\}$とする．ベア部分平面$PG(2,2)$を$\mathcal{P}=\{0,3,6,9,12,15,18\}$とする．そのとき，$PG(2,2)$と排反なベア部分平面の数は16個である．これらは次のように8つの分割クラスに分解される．

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 分割クラス1 | 1 | 4 | 7 | 10 | 13 | 16 | 19 | 2 | 5 | 8 | 11 | 14 | 17 | 20 |
| 分割クラス2 | 1 | 7 | 10 | 13 | 11 | 5 | 2 | 8 | 14 | 17 | 20 | 4 | 19 | 16 |
| 分割クラス3 | 4 | 10 | 13 | 16 | 14 | 8 | 5 | 11 | 17 | 20 | 2 | 7 | 1 | 19 |
| 分割クラス4 | 7 | 13 | 16 | 19 | 17 | 11 | 8 | 14 | 20 | 2 | 5 | 10 | 4 | 1 |
| 分割クラス5 | 10 | 16 | 19 | 1 | 20 | 14 | 11 | 17 | 2 | 5 | 8 | 13 | 7 | 4 |
| 分割クラス6 | 13 | 19 | 1 | 4 | 2 | 17 | 14 | 20 | 5 | 8 | 11 | 16 | 10 | 7 |
| 分割クラス7 | 16 | 1 | 4 | 7 | 5 | 20 | 17 | 2 | 8 | 11 | 14 | 19 | 13 | 10 |
| 分割クラス8 | 19 | 4 | 7 | 10 | 8 | 2 | 20 | 5 | 11 | 14 | 17 | 1 | 16 | 13 |

次の直交配列は$OA[16,7,2,2;4]$[17]である．これは上の$\mathcal{P}$と排反な16個のベア部分平面と$\mathcal{P}$に属さない14個の点の結合関係によって構成される．この例では16個のベア部分平面が8つの分割クラスに分解されているので，直交配列も分解できている．

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 分割クラス1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 分割クラス2 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 分割クラス3 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 |
| 分割クラス4 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 分割クラス5 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| 分割クラス6 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 分割クラス7 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
| 分割クラス8 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |

$q=3$の場合も計算機実験によって分解可能であることを確かめた．ベア部分平面の数が多いため割愛する．このとき，分解可能な水準数が素数巾ではない直交配列$OA[864,13,6,2;24]$が得られる．

## 参考文献


[1] R. C. Bose, J. W. Freeman and D. G. Glynn: On the intersection of two Baer subplanes in a finite projective plane, *Utilitas Math.* **17**, 1980, 65-77.

[2] J. Cofman: Baer subplanes in finite projective and affine planes, *Can. J. Math.* **24**, 1972, 90-97.

[3] J. W. P. Hirschfeld: Cyclic projectivities in $PG(n,q)$, *Teorie Combinatorie (Rome, 1973)* **1**, Accad. Naz. dei Lincei, 1976, 201-211.


[17]パラメーターは順にサイズ，制約数，水準数，強さ，インデックスと呼ばれる．

[4] J. W. P. HIRSCHFELD: *Projective Geometries over Finite Fields*, Oxford University Press, New York, 1979.

[5] D. R. HUGHES AND F. C. PIPER: *Projective Planes*, Springer-Verlag, New York, 1973.

[6] 永尾汎: 群とデザイン, 岩波書店, 東京, 1974.

[7] T. G. ROOM AND P. B. KIRKPATRICK: *Miniquaternion Geometry*, Cambridge University Press, London , 1971.

[8] 上村秀一: A construction of orthogonal arrays from Baer subplanes, 筑波大学社会工学研究科修士論文, 1991.