数理解析研究所講究録 1465 巻 2006 年 50-56

相対差集合に関するある予想について

熊本大学教育学部　平峰 豊 (Yutaka Hiramine)

1 Introduction

Definition 1.1 点集合$\mathbb{P}$とブロック集合$\mathbb{B}$からなる結合構造$(\mathbb{P},\mathbb{B})$が transversal design $TD_\lambda(u\lambda)$ $(u>1)$とは次がみたされることをいう.

(i) $|\mathbb{P}|=u^2\lambda$で$\mathbb{P}$がu元を含む$u\lambda$個の点クラス$\mathbb{P}_1,\mathbb{P}_2,\cdots,\mathbb{P}_{u\lambda}$に分割されて次をみたす.

$$\text{点 } p,q\,(p\neq q) \text{ を含むブロック数}=\begin{cases}0 & (p,q\in\mathbb{P}_i,\ \exists i)\\ \lambda & (\text{その他})\end{cases}$$

(ii) $|B\cap\mathbb{P}_i|=1\ \ (\forall B\in\mathbb{B},\forall i\in\{1,2,\cdots,u\lambda\})$.
(これより $|B|=u\lambda,\quad |\mathbb{B}|=u^2\lambda$.)

Example 1.2 $TD_2(4)$の例をあげる. 点集合$\mathbb{P}=\{1,2,\cdots,8\}$で$\mathbb{P}_1,\mathbb{P}_2,\mathbb{P}_3,\mathbb{P}_4$を point classes とする. $\mathbb{P}_1$〜$\mathbb{P}_4$と8ブロックは下の通りであるが, 各ブロックは各 point class の点をちょうど1点含む.

$$\begin{array}{l}\mathbb{P}_1=\{1,2\}\\ \mathbb{P}_2=\{3,4\}\\ \mathbb{P}_3=\{5,6\}\\ \mathbb{P}_4=\{7,8\}\end{array}\quad\left\{\begin{array}{l}1\\3\\5\\8\end{array}\right\}\left\{\begin{array}{l}2\\3\\5\\7\end{array}\right\}\left\{\begin{array}{l}1\\4\\5\\7\end{array}\right\}\left\{\begin{array}{l}1\\3\\6\\7\end{array}\right\}\left\{\begin{array}{l}2\\4\\6\\7\end{array}\right\}\left\{\begin{array}{l}1\\4\\6\\8\end{array}\right\}\left\{\begin{array}{l}2\\3\\6\\8\end{array}\right\}\left\{\begin{array}{l}2\\4\\5\\8\end{array}\right\}$$

Result 1.3 $(\mathbb{P},\mathbb{B})$が$TD_\lambda(u\lambda)$であり, Singer群 (i.e. 点正則な自己同型群) Gをもつとする. 点$p\in\mathbb{P}$とブロック$B\in\mathbb{B}$に対して$D=\{x\in G\mid p^x\in B\}$, $U=\{x\in G\mid p^x\in\mathbb{P}_1\}$ (ただし, $p\in\mathbb{P}_1$)とおけば次が成り立つ.

(i) Uは位数uのGの部分群である.

(ii) $DD^{(-1)}=u\lambda+\lambda(G-U)$.　すなわち,

$$\#\{Dx\mid a,b\in Dx,\ \ x\in G\}=\begin{cases}0 & (Ua=Ub)\\ \lambda & (Ua\neq Ub)\end{cases}\ (\forall a,b\in G,\ a\neq b).$$

(iii) DはG/Uの完全代表系である.　すなわち $G=UD$

(注) G の部分集合 S に対して上では次のような省略記号を用いている.

$$S^{(-1)} = \{x^{-1} \mid x \in S\}, \quad S \overset{\text{同一視}}{=} \widehat{S} \ (= \textstyle\sum_{x \in S} x \in \mathbb{C}[G])$$

Example 1.4 Example 1.2 の全自己同型群を X で表すとき X は正規部分群の列 $X \rhd A \rhd T \rhd K \rhd 1$ を持ち次が成り立つことが確かめられる.

$$\begin{aligned} K &= \langle (1,2)(3,4), (1,2)(5,6), (1,2)(7,8) \rangle \ (\simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2) \\ T &= \langle (1,3)(2,4)(5,7)(6,8), (1,5)(2,6)(3,7)(4,8) \rangle K \\ A &= \langle (1,3,5)(2,4,6) \rangle T \\ X &= \langle (1,3)(2,4) \rangle A \end{aligned}$$

ここで, $\Omega = \{\mathbb{P}_1, \mathbb{P}_2, \mathbb{P}_3, \mathbb{P}_4\}$ とおくとき

$$G^\Omega \simeq Sym(4), \quad A^\Omega \simeq Alt(4), \quad T^\Omega \simeq \mathbb{Z}_2 \times \mathbb{Z}_2, \quad K^\Omega = 1$$

である. X は点集合 $\mathbb{P}$ 上に正則に作用する非同型な部分群を 4 種類持つ. Result 1.3 に従って $p = 1, B = \{1,3,5,8\}$ と選んで D を定めれば次のようになる.

(1) $G = \langle a, b \rangle$, $a = (1,3,5,7)(2,4,6,8)$, $b = (1,2)(3,4)(5,6)(7,8)$
$G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$, $D = \{1, a, a^2, a^3 b\}$, $U = \{e, b\}$.

(2) $G = \langle a, b \rangle$, $a = (1,3,5,7)(2,4,6,8), b = (1,2)(3,8)(4,7)(5,6)$
$G \simeq D_8$, $D = \{1, a, a^2, ab\}$, $U = \{1, b\}$.

(3) $G = \langle a, b, c \rangle$, $a = (1,3)(2,4)(5,7)(6,8)$, $b = (1,5)(2,6)(3,7)(4,8)$,
$c = (1,2)(3,4)(5,6)(7,8)$,
$G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $D = \{1, a, b, abc\}$, $U = \{1, c\}$.

(4) $G = \langle a, b \rangle$, $a = (1,3,2,4)(5,7,6,8), b = (1,5,2,6)(3,8,4,7)$
$G \simeq Q_8$, $D = \{1, a, b, ab\}$, $U = \{1, a^2 (= b^2)\}$

Result 1.5 群 G の部分群 $U(\neq 1)$ と部分集合 D が次をみたすとする.

$$DD^{(-1)} = k + \lambda(G - U) \text{ かつ } G = UD.$$

このとき $|U| = u$ とおけば次が成り立つ.

(i) $G = u^2\lambda$, $|D| = u\lambda$ $(= k)$.

(ii) $\mathbb{P} = G$, $\mathbb{B} = \{Dx \mid x \in G\}$ とおくと $(\mathbb{P}, \mathbb{B})$ は $TD_\lambda(u\lambda)$ である. また作用 $\mathbb{P} \ni x \mapsto xg \in \mathbb{P}$ $(\forall g \in G)$ は $(\mathbb{P}, \mathbb{B})$ の自己同型で, G は $(\mathbb{P}, \mathbb{B})$ の正則自己同型群である. さらに点クラスへの分割は $G = \bigcup_{d \in D} Ud$ で与えられる.

Definition 1.6 上の D を部分群 U に関する (u,λ)-差集合という.

Remark 1.7 上の Result 1.3 において, G は $\{\mathbb{P}_1,\cdots,\mathbb{P}_{u\lambda}\}$ の置換を誘導し, U は $\mathbb{P}_1$ を固定する. また U が任意の $\mathbb{P}_i$ を固定するための必要十分条件は $U \lhd G$ である. この場合, G/U は $\{\mathbb{P}_1,\cdots,\mathbb{P}_{u\lambda}\}$ 上に正則に作用する.

(u,λ)-差集合の研究は次を目的とする.

問題：可能な u,λ は何か. また, 群 G にはどのようなものが可能か.

(u,λ)-差集合が相対差集合の中でも最も詳しく研究されてきた理由の一つとして次がある.

Proposition 1.8 次の同値関係が成り立つ.
$(n,1)$-差集合が存在 $\Longleftrightarrow$ 軌道数 3 で *quasiregular* な位数 n^2 の自己同型群を持つ位数 n の射影平面の存在

以下では $\underline{\lambda \neq 1}$ のときだけを考える.

2 CASE $|G| = p^2q$

$u>2$ のときは G の位数 $u^2\lambda$ は素数べきであると予想されていた時期があったが, のちに反例が見つかった. $u^2\lambda$ の可能な素因数に関連して, u,λ がともに素数ならば (u,λ) の可能な組み合わせは何かということが考えられている. この節では $u=p$, $\lambda=q$ とおいて, p,q がともに素数のときについて考える.

Subcase $p=q$
$p=q$ のときは次の結果が知られている.

Result 2.1 (i) $\mathbb{Z}_{p^2}\times\mathbb{Z}_p$ (Ma-Pott [4] により完全分類)

(ii) $\mathbb{Z}_p\times\mathbb{Z}_p\times\mathbb{Z}_p$, $M(p)$, $M_3(p)$ (存在, 未分類)

(iii) D_8, Q_8 (存在, Example 1.4 参照)

(iv) $\mathbb{Z}_{p^3}$ (非存在, J. A. Davis 1992 [1])

Subcase $p \neq q$

$p \neq q$ のときは次の結果が知られている.

Result 2.2 (i) $(\mathbb{Z}_7 \rtimes \mathbb{Z}_3) \times \mathbb{Z}_3$ (秋山-末竹)

(ii) $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$ $(p < q)$ (非存在, S. L. Ma 1996 [5])

(iii) $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$ $(p > q)$ (未決定)

(iv) 位数 p^2q の非可換群 (未決定)

(v) $p = 3$, $q \equiv 2 \pmod 3$ (非存在, 平峰)

また, $u = p$ (素数) のときには次が成り立つことが分かる.

Proposition 2.3 位数 p^2m の群 G が位数 p の部分群 U に関する (mp, p) 差集合をもち, 指数 p の正規部分群 N で $N \not\supset U$ となるものが存在すれば m の square free part m^* の任意の素因子 $p_1(\neq p)$ は $\mathrm{Ord}_p(p_1) \equiv 1 \pmod 2$ をみたす.

Corollary 2.4 上の Proposition において $p = 3$ ならば m^* の任意の素因子 $p_1(\neq 3)$ は $p_1 \equiv 1 \pmod 3$ であり, さらに合同式 $x^2 + 3 \equiv 0 \pmod 3$ は整数解 x を持つ.

3 CASE $|G| = p^2qr$

$u = p$(素数) で $\lambda = qr$ (q, r は素数) のときを考える.

Subcase $p \neq q$ または $p \neq r$

次の例と事実が知られている.

(i) $(p, qr) = (2, 6)$: $G = SL(2, 3)$, Q_{24}, $Q_8 \times \mathbb{Z}_3$

(ii) $(p, qr) = (3, 4)$: $G = Q_{12} \times \mathbb{Z}_3, A_4 \times \mathbb{Z}_3, \mathbb{Z}_6 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ (Berkesch et al. 2002)

(iii) $p = 3 < q \leq r$ で $q \equiv 2 \pmod 3$ または $r \equiv 2 \pmod 3$ なら非存在

上記以外は未決定.

Subcase $p=q=r$

$p=q=r$ のとき (つまり $u=p$, $\lambda=p^2$, 従って $|G|=p^4$ のとき) は
次の結果が知られている.

- 非アーベル群では 3 種が未決定, 他はすべて存在:

(1) $M_4(p)=\langle a,b \mid a^{p^3}=b^p=1,\ b^{-1}ab=a^{p^2+1}\rangle$

(2) metacyclic 群 $MC_{p^4}=\langle a,b \mid a^{p^3}=b^{p^2}=1,\ b^{-1}ab=a^{p+1}\rangle$

(3) order 81 の群 $P_{81}=\langle a,b,c \mid a^9=b^3=c^9=1,$
$a^3=c^3, a^c=ab, b^c=a^3b, ab=ba\rangle$

- アーベル群では次のようになっている:

(1) $Z_p\times\mathbb{Z}_p\times\mathbb{Z}_p\times\mathbb{Z}_p$ ($p>2$ では存在, しかし未分類)

(2) $Z_{p^2}\times\mathbb{Z}_p\times\mathbb{Z}_p$ (存在, しかし未分類)

(3) $G=\mathbb{Z}_{p^4}$ (非存在)

(4) $Z_{p^3}\times\mathbb{Z}_p$ (非存在)

(5) $\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}$ (未決定)

Remark 3.1 上の (5) はもっと一般の未決定な場合の最小の時に相当する.
すなわち, 次の (I)(II) の (p,p^n) 差集合が存在するかどうか未解決である.

(I) $G\simeq\mathbb{Z}_{p^{n+1}}\times\mathbb{Z}_{p^{n+1}}$, $U=\{0\}\times\mathbb{Z}_p$ ($n=0$ では存在)

(II) $G\simeq\mathbb{Z}_{p^{n+1}}\times\mathbb{Z}_{p^n}\times\mathbb{Z}_p$, $U=\{0\}\times\{0\}\times\mathbb{Z}_p$ ($n=0,1$ では存在)

上に述べた $\mathbb{Z}_{p^2}\times\mathbb{Z}_{p^2}$ について最近得られた結果を次の節で紹介したい.

4 $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ における (p, p^2)-差集合

Ma-Schmidt は奇素数 p に対して次を予想した ([6]).

予想 $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ に (p, p^2)-差集合は存在しない.

この予想に関して次が知られている.

Result 4.1 (C. Remling, et. al. 1996) $\mathbb{Z}_9 \times \mathbb{Z}_9$ に $(3, 9)$-差集合は存在しない.

S. L. Ma と B. Schmidt により次が示されていた.

Theorem 4.2 (Ma-Schmidt [6]) 奇素数 p に対して群 $G = \langle a \rangle \times \langle b \rangle \simeq \mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$ の (p, p^2)-差集合 D は次の形に同値である.

$$D = \sum_{0 \le i,j \le p-1} a^i b^j \sum_{x \in \mathbb{Z}_p} (a^p)^x (b^p)^{u_{ij}x^2 + v_{ij}x + w_{ij}}$$
$$(\exists u_{ij}, v_{ij}, w_{ij} \in \mathbb{Z}_p,\ u_{ij} \neq 0)$$

C. Remling 達の結果は上記の定理から得られる関数を用いた同値条件を計算機でチェックすることで得られたものと想像するが, Ma-Schmidt [6] の論文中に引用があるだけで公表されていないようである. 河本健二はこれを計算機の使用を最小限にして次の論文で再証明した.

Theorem 4.3 (河本健二 [3]) $\mathbb{Z}_9 \times \mathbb{Z}_9$ は $(3, 9)$-差集合を持たない.

この Ma-Schmidt による予想に関して最近次の結果を得た.

Theorem 4.4 ([2]) Ma-Schmidt の予想は正しい.

証明の方針は G の任意の線形指標 χ で $U \not\subset \mathrm{Ker}(\chi)$ となるものをとり, 群環の方程式 $DD^{(-1)} = p^3 + p^2(G - U)$ 両辺の像をとれば $\chi(D)\overline{\chi(D)} = p^3$ が成り立つことを用いる. この性質が Theorem 4.2 における定数 u_{ij}, v_{ij}, w_{ij} に与える制限を詳しく調べていくことにより最終的に矛盾を得る.

最後にこの方面に関連する今後の課題についてまとめておきたい.

- $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$ における (p, p^2)-差集合を分類すること.
- $\mathbb{M}(p), \mathbb{M}_3(p)$ における (p, p^2)-差集合を分類すること.

- $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_q$ $(p > q)$ における (p, q)-差集合が存在するか否かを決定すること.
- 位数 $9q$ $(q \equiv 1 \pmod 3)$ の非可換群における $(3, q)$-差集合が存在するか否かを決定すること.
- $p = 3 < q \leq r$ で $q \equiv r \equiv 1 \pmod 3$ のとき $(3, qr)$-差集合が存在するか否かを決定すること.
- $M_4(p), MC_{p^4}, P_{81}$ における (p, p^2)-差集合が存在するか否かを決定すること.
- $a > 1$ のとき $\mathbb{Z}_{p^{a+1}} \times \mathbb{Z}_{p^{a+1}}$ $(p > 2)$ に (p, p^{2a})-差集合が存在するか否かを決定すること.

References

[1] An Exponent bound of Relative Difference Sets in p-groups, *Ars. Combin.* **34** (1992), 318-320.

[2] Y. Hiramine, A conjecture on semiregular relative difference sets in $\mathbb{Z}_{p^2} \times \mathbb{Z}_{p^2}$, submitted.

[3] Kenji Kawamoto, On relative difference sets in finite groups, Master thesis, Kumamoto University, 2005.

[4] S.L. Ma and A. Pott, Relative difference sets, planar function and generalized Hadamard matrices, *J. Algebra* **175** (1995), 505-525.

[5] S.L. Ma, Planar functions, relative difference sets, and character theory, *JCTA* **185** (1996), 342-356.

[6] S.L. Ma and B. Schmidt, Relative (p^a, p^b, p^a, p^{a-b})-Difference Sets : A unified exponent bound and local ring construction, *Finite Fields and Their Applications* **6** (2000), 1-22.