数理解析研究所講究録
第1593巻 2008年 219-224

因子団と相対差集合の構成について

熊本大学教育学部　平峰 豊 (Yutaka Hiramine)
Department of Mathematics, Faculty of Education,
Kumamoto University

1 Factor Sets

以下では Q を位数 m のアーベル群，U を位数 u のアーベル群とする．

Definition 1.1. $\psi : Q \times Q \longrightarrow U$ が**因子団** (factor set) であるとは次をみたすことをいう．

$$\psi(\sigma,\tau)\psi(\sigma\tau,\rho) = \psi(\sigma,\tau\rho)\psi(\tau,\rho) \tag{1}$$

$$\psi(\sigma,1) = \psi(1,\tau) = 1 \quad (\forall \sigma,\tau,\rho \in Q) \tag{2}$$

このとき，群 Q による群 U の中心拡大 $G_\psi = U \times Q$ が次の演算で定義される．

$$(a,\sigma)(b,\tau) = (ab\psi(\sigma,\tau),\sigma\tau)$$

• 半正則相対差集合から得られる直交因子団

Definition 1.2. 位数 mu の群 G と G の位数 u の部分群 U が次の条件をみたすとする．

$(\star)$　　$U \leq Z(G)$ かつ G/U はアーベル群

また，$Q = G/U(= \{Ug \mid g \in G\})$ とおくとき，G/U の完全代表系 $T(\ni 1)$ に対して，写像 $f : Q \longrightarrow T$ を $\{f(\sigma)\} = \sigma \cap T$ により定める．このとき因子団 $\psi_T : Q \times Q \longrightarrow U$ が次で得られる．

$$\psi_T(\sigma,\tau) = f(\sigma)f(\tau)f(\sigma\tau)^{-1} \in U$$

$$(\text{i.e. } f(\sigma)f(\tau) = \psi(\sigma,\tau)f(\sigma\tau))$$

Definition 1.3. 群 G の部分集合 R が部分群 U に関する $(m,u,m,m/u)$-差集合 (半正則相対差集合) とは $|G| = mu$, $|U| = u$, $|R| = m$ でかつ $d_1 d_2^{-1} (d_1, d_2 \in R, d_1 \neq d_2)$ 達が $G \setminus U$ の各元をちょうど $\lambda(= m/u)$ 回重複して表し U の元を表さないことをいう．

半正則相対差集合 R の translate $Rg(g \in G)$ も半正則相対差集合であるから，R は単位元を含むと仮定できる．以下では常に $1 \in R$ とする (正規化された相対差集合)．定義より R は G/U の完全代表系であるから，$1 \in R$ の仮定とあわせると，対応する因子団 ψ_R は因子団の条件 (1)(2) をみたす．

半正則相対差集合から上のようにして得られる因子団は次の性質を持つ．

Result 1.4. (J. C. Galati[2], Perera-Horadam [3]) 群 G と部分群 U は条件 $(\star)$ をみたすとする．R を G の正規化された $(m,u,m,m/u)$-差集合 (relative to U) として，$Q=G/U$ とおくとき因子団 ψ_R は次の性質を持つ．

$$(*)\ \sum_{\tau\in Q}\psi_R(\sigma,\tau)=\lambda\hat{U}\ in\ \mathbb{Z}[U]\ \ (\forall\sigma\neq 1)$$

この性質に対して直交因子団を次のように定義する．

Definition 1.5. Q,U をアーベル群とする．因子団 $\psi(\sigma,\tau):Q\times Q\longrightarrow U$ が**重複度 λ の直交因子団** (orthogonal factor set) であるとは次が成り立つことをいう．

$(*)\ \sum_{\tau\in Q}\psi(\sigma,\tau)=\lambda U\ \ (\forall\sigma\neq 1)$

重要なことは次に述べるように Result 1.4 の逆も成り立つことである．

- 直交因子団による相対差集合の構成

Result 1.6. (J. C. Galati [2], Perera-Horadam [3]) Q,U をアーベル群とする．因子団 $\psi(\sigma,\tau):Q\times Q\longrightarrow U$ が重複度 λ の直交因子団ならば $\{1\}\times Q$ は G_ψ における $(m,u,m,m/u)$-差集合で，$m=u\lambda$ が成り立つ．

次の節ではこれを利用して既知の半正則相対差集合を一般化する．

2 Feng の相対差集合の一般化

$$M(x_1,\cdots,x_{n-1}):=\begin{bmatrix}1 & x_1 & \cdots & x_{n-3} & x_{n-2} & x_{n-1}\\ & 1 & \ddots & \ddots & x_{n-3} & x_{n-2}\\ & & 1 & \ddots & \ddots & x_{n-3}\\ & & & \ddots & \ddots & \vdots\\ & & & & \ddots & x_1\\ & & & & & 1\end{bmatrix}\ \text{とおく．}$$

以下では $M(x_1,\cdots,x_{n-1})$ を単に $(x_1,\cdots,x_{n-1})$ で表す．

$$G_{n,F}=\{(x_1,\cdots,x_{n-1})\mid x_1,\cdots,x_{n-1}\in F=GF(q)\}$$

とおけば $G = G_{n,F}$ は位数 q^{n-1} の可換 p-群で演算は次で定められる.

$$\begin{aligned}&(x_1, \cdots, x_{n-1})(y_1, \cdots, y_{n-1})\\ &= (x_1 + y_1, x_2 + y_2 + x_1y_1, \cdots, x_k + y_k + \sum_{i=1}^{k-1} x_iy_{k-i},\\ &\qquad \cdots, x_{n-1} + y_{n-1} + \sum_{i=1}^{n-2} x_iy_{n-1-i})\end{aligned}$$

T. Feng はこの群の中に次の相対差集合を構成した.

Result 2.1. (T. Feng [1]) $f(x) = ax^2 + bx + c$ $(a, b, c \in F)$ とおくとき

$$R = \{(x_1, \cdots, x_{n-2}, f(x_1) \mid x_1, \cdots, x_{n-2} \in F\}$$

は $G_{n,F}$ における $(q^{n-2}, q, q^{n-2}, q^{n-3})$-差集合 (rel. to $U = 0 \times \cdots \times 0 \times F$) である. ただし $(n, 2a) \neq (3, 1)$.

直交因子団を用いてこれは次のように一般化される.

Theorem 2.2. 元 $a \in F = GF(p^e)$ と F から F への任意の homomorphism 達 $\theta_1, \cdots, \theta_{n-2}$ に対して

$f(x_1, \cdots, x_{n-2}) = ax_1^2 + x_1^{\theta_1} + x_2^{\theta_2} + \cdots + x_{n-2}^{\theta_{n-2}}$ とおくとき

$$R = \{(x_1, \cdots, x_{n-2}, f(x_1, \cdots, x_{n-2})) \mid x_1, \cdots, x_{n-2} \in F\}$$

は $G_{n,F}$ における $(q^{n-2}, q, q^{n-2}, q^{n-3})$-差集合 (rel. to $U = 0 \times \cdots \times 0 \times F$) である. ただし $(n, 2a) \neq (3, 1)$.

(定理の証明)

$Q = G_{n-1,F} = \{(x_1, \cdots, x_{n-2}) \mid x_1, \cdots, x_{n-2} \in F\}$ として $x = (x_1, \cdots, x_{n-2}) \in Q$ に対して $\tilde{x} = (x, f(x))$ とおく. さらに $x, y \in Q$ に対して $\tilde{x}\tilde{y}(\widetilde{xy})^{-1} = (0, \cdots, 0, \psi(x, y))$ とおけば

$$\begin{aligned}\psi(x, y) &= f(x) + f(y) - f(xy) + \sum_{1 \leq k \leq n-2} x_k y_{n-1-k}\\ &= -2ax_1y_1 - (x_1y_1)^{\theta_2} - (x_1y_2 + x_2y_1)^{\theta_3} - \cdots\\ &\quad -(x_1y_{n-3} + \cdots + x_{n-3}y_1)^{\theta_{n-2}} + x_1y_{n-2} + x_2y_{n-3} + \cdots + x_{n-2}y_1\end{aligned}$$

$x = (x_1, \cdots, x_{n-2}) \neq (0, \cdots, 0)$ を固定したとき, 任意の $s \in F$ に対して次を示す.

$(\star)$ $\psi(x, y) = s$ をみたす解 $y = (y_1, \cdots, y_{n-2})$ が q^{n-3} 通りある.

$n = 3$ ならば $\psi(x, y) = -2ax_1y_1 + x_1y_1 = (1 - 2a)x_1y_1$ であるから $1 - 2a \neq 0$ が条件である. 従って $n \geq 4$ を仮定してよい.

CASE $x_1 \neq 0$ のとき

y_{n-2} を含む項は $x_1 y_{n-2}$ だけである．したがって $x_1 \neq 0$ のときは $(\star)$ は正しい．

$c_1 = \cdots = c_{k-1} = 0$ かつ $c_k \neq 0 (2 \leq k \leq n-2)$ とする．このとき $\psi(c,y) = (c_k y_1)^{\theta_{k+1}} + (c_k y_2 + c_{k+1} y_1)^{\theta_{k+2}} + \cdots + (c_k y_{n-k-2} + c_{k+1} y_{n-k-3} + \cdots + c_{n-3} y_1)^{\theta_{n-2}} + c_k y_{n-k-1} + c_{k+1} y_{n-k-2} + \cdots + c_{n-2} y_1$ であることが容易にチェックできる．このとき $\psi(c,y)$ における y_{n-k-1} の係数は c_k, $(\star)$ であるから c_k 以外の c_i を任意に与えるとき c_k がただ 1 つに決まることから $(\star)$ が成り立つことが分かる．

3 因子団から得られる $(q,q,q,1)$-差集合

素数 p に対して $F(+,\cdot)$ が位数 $q = p^e$ の pre-semifield であるとは次の条件をみたすことをいう．

(i) $F(+)$ は 0 を単位元とする elementary abelian p-群である．
(ii) $ab = 0$ ならば $a = 0$ または $b = 0$ が成り立つ．
(iii) 両側の分配律をみたす：$a(b+c) = ab + ac, (a+b)c = ac + bc$

F を位数 $q = p^e$ の pre-semifield とする．また，θ を $F(+)$ から $F(+)$ への任意の homomorphism とする．このとき，位数 p^{2e} の群 G を次で定める．

$$G = F \times F, \quad (a,b)(c,d) = (a+c, b+d+ac^\theta) \quad \forall (a,b),(c,d) \in G$$

また $U = 0 \times F$ とおくと $U \leq Z(G)$ かつ $G/U \simeq (F,+)$．θ が零写像ならば G は $F(+)$ と $F(+)$ の通常の直積である．

Lemma 3.1. 次が成り立つ．

(i) $(a,b)^{-1} = (-a, -b + aa^\theta)$
(ii) $(a,b)(c,d)^{-1} = (a-c, b-d-(a-c)c^\theta)$
(iii) $(a,b)^i = (-ia, -ib + \frac{i(i-1)}{2} aa^\theta)$
(iii) $\mathrm{C}_G(a,b) = \{(x,y) \mid ax^\theta = xa^\theta\}$

f を F から F への関数として $R = R_f = \{(x, f(x)) \mid x \in F\}$ とおくと R は G/U の完全代表系．R に対応する因子団を $\psi = \psi_R$ おけば次が成り立つ．

$$\psi(a,b) = f(a) + f(b) - f(a+b) + ab^\theta \tag{3}$$

(証明) $(a,f(a))(b,f(b))(a+b,f(a+b))^{-1} = (a+b, f(a)+f(b)+ab^\theta)(-(a+b), -f(a+b)+(a+b)(a+b)^\theta) = (0, f(a)+f(b)+ab^\theta - f(a+b) + (a+b)(a+b)^\theta + (a+b)(-(a+b))^\theta) = (0, f(a)+f(b)-f(a+b)+ab^\theta)$.

上の結果 (3) と Result 1.6 より任意の $a \in F \setminus \{0\}$ に対して関数

$(\star)$ $f(a)+f(x)-f(a+x)+ax^\theta$

が 1:1 であれば R_f は G における $(q,q,q,1)$ 差集合 (rel. to U) である.

Theorem 3.2. $F=GF(p^e), F^*=\langle\omega\rangle, x^\theta=x^{p^m}, \Gamma=\langle\omega\rangle\setminus\langle\omega^{p^m-1}\rangle$ とおく. $f(x)=ix^2+cx+jx^{1+\theta}$ に対して次の (i) または (ii) が成り立てば R_f は G の $(p^e,p^e,p^e,1)$-差集合 (rel. to U) である.

(i) $j=1$ かつ $-2i\in\Gamma\cup\{0\}$.
(ii) $j\neq 1$ かつ $\{\frac{2i+j\omega^{(p^m-1)k}}{1-j} \mid 0\le k<p^e-1\}\subset\Gamma\cup\{0\}$.

(証明) $\psi(a,x)=f(a)+f(x)-f(a+x)+ax^\theta=-(2ia+ja^\theta)x+(1-j)ax^\theta$ が確かめられる. これが任意の $a\neq 0$ に対して 1 : 1 の関数であるための条件をみる.
$r=2ia+ja^\theta, s=(1-j)a$ とおくと, $\psi(a,x)=k-rx+sx^\theta$ で, さらに次が成り立つ.
$\psi(a,x)=\psi(a,y)(\exists x\neq\exists y)\iff r(x-y)=s(x-y)^\theta(\exists x\neq\exists y)\iff r=sz^{p^m-1}(\exists z\neq 0)$.
上のことから $r\neq sz^{p^m-1}(\forall z\neq 0)$ が条件.
CASE I : $j=1$
このときは. $r=2ia+a^\theta$, $s=0$ より $r\neq 0$, つまり $i=0$ または $-2i\in\langle\omega\rangle\setminus\langle\omega^{p^m-1}\rangle$ が条件. よって (i) が成り立つ.
CASE II : $j\neq 1$
このときは $r\neq 0$ となる $a\neq 0$ に対して $\frac{r}{s}\in\Gamma$ であればよい. つまり $2i+ja^{p^m-1}\neq 0$ なる $a\neq 0$ に対して $\frac{2i+ja^{p^m-1}}{1-j}\in\Gamma$ であればよい. 従って, (ii) が成り立つ.

上の定理よりただちに次が分かる.

Corollary 3.3. $f(x)$ が次のいずれかをみたせば R_f は G の $(p^e,p^e,p^e,1)$-差集合 (rel. to U) である.

(i) $f(x)=ix^2+cx+x^{1+\theta}$ $(-2i\in\Gamma\cup\{0\})$
(ii) $f(x)=cx+jx^{1+\theta}$ $(\frac{j}{1-j}\in\Gamma)$
(iii) $f(x)=ix^2+cx$ $(2i\in\Gamma\cup\{0\})$

GAP を用いて次の例を得る.

Example 3.4. 次のとき R_f は G の $(p^e,p^e,p^e,1)$-差集合 (rel. to U) である. ただし ω は $GF(p^e)$ の原始元とする. (GAP に従って, $\omega^{p^{e-1}+\cdots+p+1}$ は $GF(p)$ の"最小の"原始元となるように選ばれている)

(i) $p=5,\ e=2,\ m=1,\ i=1,\ j=\omega$.
(ii) $p=7,\ e=2,\ m=1,\ i=1,\ j=\omega^4$.
(iii) $p=3,\ e=4,\ m=2,\ i=\omega^{10},\ j=\omega^{10}$.

(iv) $p=5,\ e=4,\ m=2,\ i=1,\ j=3.$
(v) $p=7,\ e=4,\ m=2,\ i=1,\ j=2.$
(vi) $p=3,\ e=6,\ m=3,\ i=\omega^{91},\ j=\omega^{28}.$
(vii) $p=5,\ e=6,\ m=3,\ i=1,\ j=\omega^{651}.$
(viii) $p=3,\ e=8,\ i=\omega^{820},\ j=2.$

◇ Albert's twisted pre-semifield
$F=GF(p^n),\ F^*=\langle\omega\rangle$
$x\circ y=xy^q-cx^qy.$ ここで, $q=p^m(\leq p^n)$ かつ $c\notin\langle\omega^{q-1}\rangle.$

Example 3.5. $n=2m,\ x^\theta=x^q$ とする. また $f(x)=kx^2$ とおく. このとき, $f(a)+f(x)-f(a+y)+a\circ x^\theta=ka^2+kx^2-k(a^2+x^2+2ax)+a(x^\theta)^q-ca^qx^\theta=-2k(ax)-(ax)-c(ax)^q=-(2k+1)(ax)-c(ax)^q$. これは linear map なので $2k+1=0$ または $\frac{-(2k+1)}{c}\notin\langle\omega^{q-1}\rangle$ が条件. 後者は例えば $k=-\frac{c^2+1}{2}$ とすればよい.

参考文献

[1] T. Feng, Relative (p^a,p^b,p^a,p^{a-b}) Difference Sets in Subgroups of $SL(n,K)$, preprint

[2] J.C. Galati, A Group Extensions Approach to Relative Difference Sets, *J. Combin. Designs* Vol.12 (2004), pp. 279-298.

[3] A.A.I. Perera and K.J. Horadam, Cocyclic generalized Hadamard matrices and central relatice difference sets, *Designs, Codes and Cryptography* Vol. 15 (1998) pp. 187-200