数理解析研究所講究録
第587巻 1986年 93-109

相対的Gaussの和とSzekeres差集合

東京女子大学・文理　山田美枝子 (Mieko Yamada)

1. 序

相対差集合の概念は1963年A.T. Butsonによって導入された[2]. 1966年には, Elliott-Butsonによって相対差集合に関するいくつかの結果が報告されている[3]. その後1975年にE. Spenceは有限体から作られる巡回的相対差集合を使って $p, q=p-2$ がともに素数中の場合で $p\equiv 1 \pmod 4$ のときに $4p$ 次Hadamard行列, $p\equiv 3 \pmod 4$ のときに $8p$ 次Hadamard行列を構成した。

一方 G. Szekeresは1969年に supplementary difference sets M, N で $x\in M$ ならば $-x\notin M$ をみたすものが $q\equiv 3 \pmod 4$ が素数中のとき存在することを示した[4,5]. これをここではSzekeres差集合と呼ぶことにする([5]におけるSzekeres差集合の定義と異なる). Szekeres差集合から $q+1$ 次 skew-Hadamard 行列が構成される.

本稿では有限体の2次拡大から作られるパラメータ $q^2-1, q, 1, q-1$ をもつ巡回的相対差集合を考える. 特に $q\equiv 3 \pmod 4$ の

とき、$n=\frac{q-1}{2}$ とおくとこの巡回的相対差集合の偶数部 $\mathcal{D}_0$ と奇数部 $\mathcal{D}_1$ は $2-\{n;\frac{n+1}{2};\frac{n+1}{2}\}$ supplementary difference sets を構成する。さらに $\mathcal{D}_0, \mathcal{D}_1$ の補集合は Szekeres 差集合に他ならない。このことを有限体の相対的 Gauss の和の理論を用いて証明する。

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 次拡大体，$t\geq 2$，Z：有理整数環、

ξ：K の乗法群 $K^\times$ の生成元、g：F の乗法群 $F^\times$ の生成元、

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、$N_{K/F}$：K から F へのノルム、

$J_m(x)=1+x+\cdots+x^{m-1}$。

2 相対的 Gauss の和

まず相対的 Gauss の和を定義する。

<u>定義</u>　χ を F の指標、$\zeta_p=e^{2\pi i/p}$ とする時 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 $\tau_F(\chi)=-1$，$\chi\neq 1$ ならば $\tau_F(\chi)\overline{\tau_F(\chi)}=q$ が成りたつ。$\chi\neq 1$ のとき、K の指標 χ に対する Gauss の和 $\tau_K(\chi)$ と χ を F に制限したときの F の Gauss の和 $\tau_F(\chi)$ との比

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

を χ の相対的 Gauss の和という.

次の相対的 Gauss の和に関する定理は相対差集合に対して重要な情報を与えている。

定理1 $\chi = \chi_K$ を K の指標、χ_F を χ を F に制限した指標とする。$K^\times/F^\times$ の代表系 $\mathcal{L}$ をとり次のように2つに分解する。

$$\mathcal{L} = \mathcal{L}_0 + \mathcal{L}_1, \quad \mathcal{L}_0 = \{\beta : S_{K/F}\beta = 0\}, \quad \mathcal{L}_1 = \{\beta : S_{K/F}\beta = 1\}$$

このとき

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

となる.

(証明) $K^\times$ の元 α は、$\alpha = a\beta$, $a\in F^\times$, $\beta\in\mathcal{L}$ と一意にかけるので

$$\begin{aligned}\tau_K(\chi) &= \sum_{a\in F^\times}\sum_{\beta\in\mathcal{L}} \chi(a\beta)\zeta_p^{S_K(a\beta)} \\ &= \sum_{\beta\in\mathcal{L}} \chi(\beta)\sum_{a\in F^\times}\chi(a)\zeta_p^{S_F(aS_{K/F}\beta)}\end{aligned}$$

となる。 2つの場合に分けて考える.

(1) $S_{K/F}\beta \neq 0$ の場合

$$\sum_{a\in F^\times}\chi(a)\zeta_p^{S_F(aS_{K/F}\beta)} = \sum_{a\in F^\times}\overline{\chi}(S_{K/F}\beta)\,\chi(aS_{K/F}\beta)\zeta_p^{S_F(aS_{K/F}\beta)}$$

$$= \overline{\chi}(S_{k/F}\beta)\tau_F(\chi).$$

(2) $S_{k/F}\beta = 0$ の場合

$$\sum_{a\in F^\times}\chi(a) = \begin{cases} 0 & \chi_F \neq 1 \text{ のとき.} \\ q-1 & \chi_F = 1 \text{ のとき。} \end{cases}$$

以上から

(1) $\chi_F \neq 1$ のとき

$$\vartheta_{k/F}(\chi) = \frac{\tau_k(\chi)}{\tau_F(\chi)} = \sum_{\beta\in\mathcal{L}_1}\overline{\chi}(S_{k/F}\beta)\chi(\beta) = \sum_{\beta\in\mathcal{L}_1}\chi(\beta).$$

(2) $\chi_F = 1$ のとき　$\beta\in\mathcal{L}_1$ ならば $\overline{\chi}(S_{k/F}\beta)\tau_F(\chi) = -1$ なので

$$\tau_k(\chi) = (q-1)\sum_{\beta\in\mathcal{L}_0}\chi(\beta) - \sum_{\beta\in\mathcal{L}_1}\chi(\beta) = -\sum_{\beta\in\mathcal{L}}\chi(\beta) + q\sum_{\beta\in\mathcal{L}_0}\chi(\beta)$$

となる。この場合で $\chi_k \neq 1$ ならば $\sum_{\beta\in\mathcal{L}}\chi(\beta) = 0$ である。

従って、$\chi_k \neq 1$ のとき

$$\tau_k(\chi) = q\sum_{\beta\in\mathcal{L}_0}\chi(\beta) = -q\sum_{\beta\in\mathcal{L}_1}\chi(\beta)$$

を得る。$\chi_k = 1$ のときは

$$\tau_k(\chi) = -\sum_{\beta\in\mathcal{L}}\chi(\beta) + q\sum_{\beta\in\mathcal{L}_0}\chi(\beta) = -\frac{q^t-1}{q-1} + q\sum_{\beta\in\mathcal{L}_0}\chi(\beta) = -1$$

から $\sum_{\beta\in\mathcal{L}_0}\chi(\beta) = \frac{q^{t-1}-1}{q-1}$ が求まり.

$$\sum_{\beta\in\mathcal{L}_1}\chi(\beta) = \sum_{\beta\in\mathcal{L}}\chi(\beta) - \sum_{\beta\in\mathcal{L}_0}\chi(\beta) = \frac{q^t-1}{q-1} - \frac{q^{t-1}-1}{q-1} = q^{t-1}$$

を得る。

3 相対差集合

相対差集合を定義する。

定義　Gを位数vのAbel群、Rをk個の元を持つGの部分集合、Hを位数hのGの部分群とする。$d\in G$, $d\neq 0$に対し、$d=r-s$, $r,s\in R$となるペア(r,s)の数が一定の値

$$\begin{cases} \lambda & d\notin H \text{ のとき}, \\ 0 & d\in H \text{ のとき}. \end{cases}$$

になるとき、Rを相対差集合といい$R(v,k,\lambda,h)$とかく。

補助定理1　Gが巡回群の時、$f(x)$を$R(v,k,\lambda,h)$の生成多項式、すなわち$f(x)=\sum_{r\in R} x^r$とすると次が成りたつ。

$$f(x)f(x^{-1}) \equiv k+\lambda\left(J_v(x)-J_h(x^{\frac{v}{h}})\right) \pmod{x^v-1}.$$

逆にRをk個の元をもつGの部分集合で上の合同式をみたすならば、Rはパラメータv,k,λ,hをもつ相対差集合である。

(証明)　略.

巡回的相対差集合の例として次のようなものがある。

定理2　$\mathbb{Z}/(g^t-1)\mathbb{Z}$の部分集合$D_1$を

$$D_1=\{m : S_{k/h}\xi^m=1\}$$

で定義すると、D_1はパラメータ

$$v = q^t - 1, \quad k = q^{t-1}, \quad \lambda = q^{t-2}, \quad n = q - 1$$

をもつ相対差集合である。

(証明) 補助定理1から D_1 の生成多項式 $f(x)$ に対し、

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

が成りたつことを示せばよい。χ を K の指標、ζ を 1 の q^{t-1} 乗根、$\chi(\zeta) = \zeta$ とすると

$$f(\zeta) = \sum_{m \in D_1} \zeta^m = \sum_{\beta \in \mathcal{R}_1} \chi(\beta)$$

である。そこで任意の 1 の q^{t-1} 乗根に対し

$$\sum_{\beta \in \mathcal{R}_1} \chi(\beta) \cdot \sum_{\beta \in \mathcal{R}_1} \overline{\chi}(\beta) = q^{t-1} + q^{t-2}(J_{q^{t-1}}(\zeta) - J_{q-1}(\zeta^{\frac{q^{t-1}}{q-1}}))$$

が成りたつことを示すことに帰着するが、そのことは定理1の結果から容易に証明できる。

我々はこの定理から得られた相対差集合を有限体の拡大体 K/F に付随する巡回的相対差集合と呼ぶことにする。

4 有限体の2次拡大に付随する巡回的相対差集合

これから先は有限体の2次拡大に付随する巡回的相対差集合をとり扱う。定理2から

$$D_1 = \{ m : S_{K/F}\, \zeta^m = 1 \}$$

はパラメータ $q^2-1, q, 1, q-1$ をもつ巡回的相対差集合である。

D_1 を変形する。

(I) $D_2=\{m: S_{k,f}\xi^m=2\}$ は D_1 の translate、すなわち $D_2=D_1+c(q+1)$ である。ただし c は $q=\xi^{q+1}$ について $2=q^c$ となる整数である。

(II) 代表系を $\{1,\xi,\cdots,\xi^8\}$ にとると $D_2=\{k: \xi^k=\frac{2\xi^m}{S_{k,f}\xi^m}$, $m=0,\cdots,8, m\neq\frac{q+1}{2}\}$ と変形できる。

(III) さらに ξ^k の逆数をとって次のように変形できる。

$$D_2=\left\{k: \xi^k=\frac{1}{2}(\xi^{\frac{q-1}{2}m}+\xi^{-\frac{q-1}{2}m})\xi^{\frac{q-1}{2}m}=\frac{1}{2}(1+\xi^{(q-1)m}),\ m=0,\cdots,8, m\neq\frac{q+1}{2}\right\}.$$

$D=D_2$ は次のような性質をもつ。

<u>定理3</u> $D_0=\{k\in D \pmod{q-1}, k: 偶数\}$, $D_1=\{k\in D \pmod{q-1}, k: 奇数\}$ とおくと

$$D \pmod{q-1} = D_0 + D_1$$

で、次のような性質をもつ。

(1) m が偶数(奇数)ならば $k \pmod{q-1}$ も偶数(奇数)。

(2) $D \pmod{q-1}$ は $k=0$ を除いて丁度2個 k を含む。

(3) $q\equiv 1 \pmod 4$ のとき、$k\in D_0$ ならば $-k\in D_0$, $k\in D_1$ ならば $-k\notin D_1$.

$q\equiv 3 \pmod 4$ のとき、$k\in D_0$ ならば $-k\notin D_0$, $k\in D_1$ ならば $-k\in D_1$.

ただし $k\neq 0$.

この定理は次の興味深い補助定理を使って証明される。

<u>補助定理2</u> $\zeta=\xi^{\frac{q-1}{2}}$, $\Lambda(x)$ を

$$\Lambda(x)=\frac{x+1}{x-1}$$

なる一次分数変換とする。

(1) k が奇数のとき $\Lambda(\zeta^k)=\zeta^{k'}$ をみたす奇数の k' $(\mathrm{mod}\ 2g+2)$ が唯一つ存在する。

(2) k が偶数のとき $\Lambda(\zeta^k)=\zeta^{k'}$ をみたすのは $g\equiv 3\ (\mathrm{mod}\ 4)$ で $k\equiv k'\equiv \pm\frac{g+1}{2}$ $(\mathrm{mod}\ 2g+2)$ のときだけである。

(証明) k が偶数で $\Lambda(\zeta^k)=\zeta^{k'}$ であるとする。$\zeta^k=-\zeta^{-1}$ から $\zeta^{kg}=\zeta^{-k}$ で

$$\Lambda(\zeta^k)^g=\Lambda(\zeta^{kg})=\Lambda(\zeta^{-k})=\frac{\zeta^{-k}+1}{\zeta^{-k}-1}=-\Lambda(\zeta^k)=-\zeta^{k'}$$

である。そこで k' の偶、奇によって $\zeta^{-k'}=-\zeta^{k'}$ か $\zeta^{-k'}=\zeta^{k'}$ となる。$\zeta^{k'}=\pm i=\pm\zeta^{\frac{g+1}{2}}$ か $\zeta^{k'}=-1$ で $\zeta^{k'}=-1$ は k' 奇数に反する。従って $\Lambda(\zeta^k)=\zeta^{k'}$ をみたすのは $g\equiv 3\ (\mathrm{mod}\ 4)$ で $k\equiv k'\equiv\pm\frac{g+1}{2}$ $(\mathrm{mod}\ 2g+2)$ のときだけである。

次に k を奇数とする。$\zeta^{kg}=-\zeta^{-k}$ から

$$\Lambda(\zeta^k)^g=\Lambda(\zeta^{kg})=\Lambda(-\zeta^{-k})=\frac{-\zeta^{-k}+1}{-\zeta^{-k}-1}=-\Lambda(\zeta^k)^{-1}$$

を得る。k が奇数である $\Lambda(\zeta^k)$ はすべて次の $g+1$ 次代数方程式

$$x^g=-\frac{1}{x}\ ,\ \text{i.e.}\quad x^{g+1}+1=0$$

をみたす。一方 $g+1$ 個の相異なるその奇数中もまた上の方程式をみたし、これらがこの方程式の根すべてである。従って $\Lambda(\zeta^k)=\zeta^{k'}$ となる奇数の k' が唯一つ存在する。

(定理3の証明) (1) $\xi^{-k}=\frac{S_{k/F}\xi^m}{2\xi^m}$ から m 偶数であれば k も偶数となり、$q-1$ は偶数なので(1)を得る。

(2) $k\in D$ ならば $kq\in D$ である。$kq\equiv k \pmod{q-1}$ から $D \pmod{q-1}$ は0以外の k を2個含む。次に'丁度'2個であることを示す。H を ξ^{q-1} で生成される群とする。この群は相対ノルムが1である元の集合として特徴づけられる。

$$\xi^{-k}=\frac{1}{2}(1+\xi^{(q-1)m}),\quad \xi^{-k'}=\frac{1}{2}(1+\xi^{(q-1)m'})$$

とおき、$k\equiv k' \pmod{q-1}$ と仮定する。このことは $\xi^{-k}\equiv\xi^{-k'} \pmod{\times H}$ を意味し、次と同値である。

$$N_{K/F}\left(\frac{1}{2}(1+\xi^{(q-1)m})\right)=N_{K/F}\left(\frac{1}{2}(1+\xi^{(q-1)m'})\right)$$

$$N_{K/F}(1+\xi^{(q-1)m})=N_{K/F}(1+\xi^{(q-1)m'})$$

$$\xi^{(q-1)m}+\xi^{-(q-1)m}=\xi^{(q-1)m'}+\xi^{-(q-1)m'}.$$

$\alpha=\xi^{(q-1)m}$, $\beta=\xi^{(q-1)m'}$ とおくと上の方程式は

$$\alpha+\frac{1}{\alpha}=\beta+\frac{1}{\beta}$$

であり、これが成りたつのは $\alpha=\beta$ か $\alpha=\frac{1}{\beta}$、$m\equiv\pm m' \pmod{q+1}$ である。従って $m\equiv 0 \pmod{q+1}$ すなわち $k=0$ を除いて $k\equiv k' \pmod{q-1}$ となる k, k' は存在しない。

(3) ξ^{-k}, $\xi^{-k'}$ を(2)と同じく定義する。$k\equiv k' \pmod{q-1}$ であると仮定する。(1)の証明から $k\equiv k' \pmod 2$ である。仮定から $\xi^{k+k'}\in H$ でこれは次と同値である。

$$N_{K/F}\left(\frac{1}{2}(1+\xi^{(q-1)m})\cdot\frac{1}{2}(1+\xi^{(q-1)m'})\right)=1$$

$$N_{k/\mathbb{Q}}((1+\xi^{(g-1)m})(1+\xi^{(g-1)m'})) = 4^2.$$

$\zeta = \xi^{\frac{g-1}{2}}$, $i = \xi^{\frac{g+1}{2}}$ とおくと

$$1+\xi^{(g-1)m} = 1-(i\zeta^m)^2 = 1-(\zeta^{\frac{g+1}{2}+m})^2 = -\zeta^{\frac{g+1}{2}+m}(\zeta^{\frac{g+1}{2}+m} - \zeta^{-\frac{g+1}{2}-m})$$

から

$$N_{k/\mathbb{Q}}(\zeta^{\frac{g+1}{2}+m}\zeta^{\frac{g+1}{2}+m'}(\zeta^{\frac{g+1}{2}+m} - \zeta^{-\frac{g+1}{2}-m})(\zeta^{\frac{g+1}{2}+m'} - \zeta^{-\frac{g+1}{2}-m'})) = 4^2$$

を得る。ところで

$$(\zeta^k - \frac{1}{\zeta^k})^g = \zeta^{kg} - \frac{1}{\zeta^{kg}} = (-\frac{1}{\zeta})^k - (-\zeta)^k = (-1)^k(\frac{1}{\zeta^k} - \zeta^k) = (-1)^{k-1}(\zeta^k - \frac{1}{\zeta^k})$$

であるから上の相対ノルムは

$$(\zeta^{\frac{g+1}{2}+m} - \zeta^{-\frac{g+1}{2}-m})(\zeta^{\frac{g+1}{2}+m'} - \zeta^{-\frac{g+1}{2}-m'}) = \pm 4$$

となる。m' を $g+1-m'$ にかえると右辺の符号が変わるので＋符号の場合を証明すれば十分である。この場合に上の式から

$$\zeta^{\frac{g+1}{2}+m'} = \frac{\zeta^{\frac{g+1}{2}+m}+1}{\zeta^{\frac{g+1}{2}+m}-1} = \Lambda(\zeta^{\frac{g+1}{2}+m}),\quad \zeta^{\frac{g+1}{2}+m'} = \frac{-\zeta^{\frac{g+1}{2}+m}+1}{\zeta^{\frac{g+1}{2}+m}+1}$$

が求まる。第2式で $\zeta^{\frac{g+1}{2}+m'}$ を $-\zeta^{\frac{g+1}{2}+m'}$, $\zeta^{\frac{g+1}{2}+m}$ を $-\zeta^{\frac{g+1}{2}+m}$ におきかえると第一式になる。$k = \frac{g+1}{2}+m$, $k' = \frac{g+1}{2}+m'$ とおいて補助定理2から(3)が証明される。

これ以後 $g \equiv 3 \pmod 4$ であると仮定する。$n = \frac{g-1}{2}$ とおくとれは奇数である。次のように集合 D' を定義する。

$$D' = \{k \pmod n : \xi^{-k} = \frac{1}{2}(1+\xi^{(g-1)m}),\ m = 0, \cdots, n\}.$$

D' を偶数部 D_0', 奇数部 D_1' に分ける。すなわち

$D_0' = \{k \in D',\ m:\text{偶数}\}$, $D_1' = \{k \in D',\ m:\text{奇数}\}$, $D' = D_0' + D_1'$.

定理3から D_0', D_1' は次のような性質をもつことがわかる。

(1) D_0', D_1' は各々 $\frac{g+1}{2}$ 個の mod n で相異なる元を含む。

(2) $k \neq 0$, $k \in D_0'$ ならば $-k \notin D_0'$ で $k \in D_1'$ ならば $-k \in D_1'$.

(3) $D_0'^{*} = \{-k : k \in D_0',\ k \neq 0\}$ とすると $D_0' \cup D_0'^{*} = \mathbb{Z}/n\mathbb{Z}$ である。

ところで

$$S_{k/f}\,\xi^{\frac{g-1}{2}m} = \xi^{\frac{g-1}{2}m} + \xi^{\frac{g^2-g}{2}m} = \xi^{\frac{g-1}{2}m} + (-1)^m \xi^{-\frac{g-1}{2}m},$$

$$S_{k/f}\,\xi^{\frac{g-1}{2}(\frac{g+1}{2}+m)} = \xi^{\frac{g-1}{2}(\frac{g+1}{2}+m)} - (-1)^m \xi^{-\frac{g-1}{2}(\frac{g+1}{2}+m)},$$

であるので

$$\xi^{-k} = \xi^{\frac{g-1}{2}m} \cdot \frac{S_{k/f}\,\xi^{\frac{g-1}{2}m}}{2} \qquad m\text{が偶数のとき},$$

$$\xi^{-k} = \xi^{\frac{g-1}{2}(\frac{g+1}{2}+m)} \cdot \frac{S_{k/f}\,\xi^{\frac{g-1}{2}(\frac{g+1}{2}+m)}}{2} \qquad m\text{が奇数のとき}$$

となる。そこで $r = r(m)$ を

$$\xi^{r(g+1)} = g^r = g^{r(m)} = \frac{1}{2} S_{k/f}\,\xi^{\frac{g-1}{2}m}$$

で定義し、あらたに集合 $\mathcal{Q}_0$, $\mathcal{Q}_1$ を次のように定義する。

$$\mathcal{Q}_0 = \left\{ r(m) : g^{r(m)} = \frac{1}{2} S_{k/f}\,\xi^{\frac{g-1}{2}m},\ m = 0, 2, \cdots, \frac{g-3}{2} \right\},$$

$$\mathcal{Q}_1 = \left\{ r(m) : g^{r(m)} = \frac{1}{2} S_{k/f}\,\xi^{\frac{g-1}{2}m},\ m = 1, 3, \cdots, \frac{g-1}{2} \right\}.$$

$\mathcal{Q}_0$, $\mathcal{Q}_1$ と D_0', D_1' の間には

$$\mathcal{Q}_0 \equiv -\frac{1}{2} D_0', \quad \mathcal{Q}_1 \equiv -\frac{1}{2} D_1' \pmod{n}$$

が成りたつ。集合 $\mathcal{Q}_0$, $\mathcal{Q}_1$ は D_0', D_1' より構造が簡単で計算がしやすい。

4 Szekeres 差集合

先に supplementary difference sets を定義する.

定義 $S_1, \cdots, S_n$ を mod v の相異なる剰余の集合で各々 $k_1, \cdots, k_n$ 個の元を持つ. $d \not\equiv 0 \pmod v$ に対して

$$\lambda_i(d) = \#\{(r, s) : d \equiv r - s \pmod v,\ r, s \in S_i\}$$

を定義する. $\lambda(d) = \lambda_1(d) + \cdots + \lambda_n(d)$ が $d \not\equiv 0 \pmod v$ によらず一定の値入になるとき、$S_1, \cdots, S_n$ を $n - \{v; k_1, \cdots, k_n; \lambda\}$ supplementary difference sets という. $k_1 = \cdots = k_n$ であるときは、$n - \{v; k_1; \lambda\}$ supplementary difference sets と略す.

$f_1(x), f_2(x), \cdots, f_n(x)$ を $S_1, \cdots, S_n$ の生成多項式とすると

$$\sum_{i=1}^{n} f_i(x) f_i(x^{-1}) \equiv \sum_{i=1}^{n} k_i - \lambda + \lambda J_v(x) \qquad (\bmod x^v - 1)$$

が成りたつ. 逆に mod v の相異なる剰余の集合 $S_1, \cdots, S_n$ が各々 $k_1, \cdots, k_n$ 個の元を持ち、それらの生成多項式が上の式をみたすならば $S_1, \cdots, S_n$ は $n - \{v; k_1, \cdots, k_n; \lambda\}$ supplementary difference sets である.

G. Szekeres は次のような supplementary difference sets の存在を示した.

定理4 (G. Szekeres [4, 5]) $q \equiv 3 \pmod 4$ を素数中. Q を F の平

方剰余の集合とする。集合M, Nを次のように定義する。

$$M=\{a: g^{2a}-1 \in Q\},\quad N=\{b: g^{2b}+1 \in Q\}.$$

M, Nは $2-\{\frac{g-1}{2};\frac{g-3}{4};\frac{g-7}{4}\}$ supplementary difference sets となる。

(証明) [4, 5] 参照。

このsupplementary difference setsをSzekeres差集合と呼ぶことにする。3で定義した$\mathfrak{D}_0, \mathfrak{D}_1$の補集合はこのSzekeres差集合に他ならないことを示す。

定理5　$\mathfrak{D}_0, \mathfrak{D}_1$を3で定義した集合、$n=\frac{g-1}{2}$とする。このとき次が成りたつ。

(1) $\mathfrak{D}_0, \mathfrak{D}_1$は $2-\{n;\frac{n+1}{2};\frac{n+1}{2}\}$ supplementary difference setsである。

(2) $\mathfrak{D}_0, \mathfrak{D}_1$の補集合$\mathfrak{D}_0^*, \mathfrak{D}_1^*$はSzekeres差集合である。

(証明) (1) $\mathfrak{D}_0 \equiv -\frac{1}{2}D_0'$, $\mathfrak{D}_1 \equiv -\frac{1}{2}D_1'$ (mod n) から D_0', D_1'が $2-\{n;\frac{n+1}{2};\frac{n+1}{2}\}$ supplementary difference setsであることを示せば十分である。集合D, D_0', D_1'の生成多項式を$\theta(x), \theta_0(x), \theta_1(x)$とする。3の結果から

$$\theta(x) \equiv -1+2\theta_0(x)+2\theta_1(x) \quad (\mathrm{mod}\ x^n-1),$$

$$\theta_0(x)+\theta_0(x^{-1}) \equiv 1+J_n(x) \quad (\mathrm{mod}\ x^n-1),$$

$$\theta_1(x^{-1}) \equiv \theta_1(x). \quad (\mathrm{mod}\ x^n-1).$$

定理2から

$$\theta(x)\theta(x^{-1}) \equiv g + J_{g^2-1}(x) - J_{g-1}(x^{g+1}) \pmod{x^{g^2-1}-1}$$

で

$$J_{g^2-1}(x) = J_{\frac{g-1}{2}}(x) J_{2g+2}(x^{\frac{g-1}{2}}) \equiv (2g+2) J_n(x) \pmod{x^n-1},$$

$$J_{g-1}(x^{g+1}) = J_{\frac{g-1}{2}}(x^{g+1}) J_2(x^{\frac{g^2-1}{2}}) \equiv 2 J_n(x) \pmod{x^n-1},$$

から

$$\theta(x)\theta(x^{-1}) \equiv g + 2g J_n(x) \pmod{x^n-1}$$

を得る。 一方

$$\theta(x)\theta(x^{-1}) \equiv (-1+2\theta_0(x)+2\theta_1(x))(-1+2\theta_0(x^{-1})+2\theta_1(x^{-1}))$$

$$\equiv 1-2(\theta_0(x)+\theta_0(x^{-1})+\theta_1(x)+\theta_1(x^{-1})) + 4(\theta_0(x)\theta_0(x^{-1})+\theta_1(x)\theta_1(x^{-1}))$$

$$+ 4(\theta_0(x)\theta_1(x^{-1}) + \theta_0(x^{-1})\theta_1(x))$$

$$\equiv -1 + 2n J_n(x) + 4(\theta_0(x)\theta_0(x^{-1}) + \theta_1(x)\theta_1(x^{-1})) \pmod{x^n-1}$$

で、比較することにより次が求まる。

$$4(\theta_0(x)\theta_0(x^{-1}) + \theta_1(x)\theta_1(x^{-1})) \equiv 2n+2+(2n+2) J_n(x)$$

$$\theta_0(x)\theta_0(x^{-1}) + \theta_1(x)\theta_1(x^{-1}) \equiv \frac{n+1}{2} + \frac{n+1}{2} J_n(x) \pmod{x^n-1}.$$

$\#D_0' = \#D_1' = \frac{n+1}{2}$ から D_0', D_1' は $2-\{n; \frac{n+1}{2}; \frac{n+1}{2}\}$ supplementary difference sets となる。

(2) $\gamma \in \mathcal{D}_0$ と仮定する。

$$g^r = \frac{1}{2} S_{k/f} \xi^{\frac{g-1}{2}m} = \frac{1}{2} S_{k/f} \eta^m = \frac{1}{2}(\eta^m + \eta^{-m}),$$

$$g^{2r} - 1 = \left(\frac{1}{2}(\eta^m + \eta^{-m})\right)^2 - 1 = \left(\frac{1}{2}(\eta^m - \eta^{-m})\right)^2.$$

一方

$$\left(\frac{1}{2}(\eta^m - \eta^{-m})\right)^g = -\frac{1}{2}(\eta^m - \eta^{-m})$$

から

$$\frac{1}{2}(\zeta^m - \zeta^{-m}) \notin F, \quad \left(\frac{1}{2}(\zeta^m - \zeta^{-m})\right)^2 \in F$$

であることがわかる。これは

$$g^{2r} - 1 \notin Q$$

であることを意味する。

次に $r \in \mathcal{D}_1$ とする。

$$g^r = \frac{1}{2} S_{k/F}\, \xi^{\frac{g-1}{2}m} = \frac{1}{2} S_{k/F}\, \zeta^m = \frac{1}{2}(\zeta^m - \zeta^{-m}),$$

$$g^{2r} + 1 = \left(\frac{1}{2}(\zeta^m - \zeta^{-m})\right)^2 + 1 = \left(\frac{1}{2}(\zeta^m + \zeta^{-m})\right)^2.$$

同じようにして

$$\frac{1}{2}(\zeta^m + \zeta^{-m}) \notin F, \quad \left(\frac{1}{2}(\zeta^m + \zeta^{-m})\right)^2 \in F$$

から

$$g^{2r} + 1 \notin Q$$

を得る。以上から $r \in \mathcal{D}_0$ ならば $r \in M^*$, $r \in \mathcal{D}_1$ ならば $r \in N^*$, M^*, N^* は M, N の補集合である。しかし $\#\mathcal{D}_0 = \#\mathcal{D}_1 = \frac{n+1}{2}$, $\#M^* = \#N^* = n - \frac{n-1}{2} = \frac{n+1}{2}$. 従って

$$\mathcal{D}_0^* = M, \quad \mathcal{D}_1^* = N$$

である。

5 あとがき

我々は $\mathcal{D}_0, \mathcal{D}_1$ の方が Szekeres 差集合と比べて、集合をパラメータを使って具体的に与えている。相対差集合との関係が明

確である点等から、より本質的であり発展性があると考えている。

$q=19$の場合について、$\mathcal{D}_0, \mathcal{D}_1$, Szekeres差集合の例をあげる。

例 $q=19$, $g=14$, $n=\frac{q-1}{2}=9$

(1) $\mathcal{D}_0=\{r(m): g^{r(m)}\equiv\frac{1}{2}S_{14}\xi^{9m}, m=0,2,\cdots,8\}$, $\mathcal{D}_1=\{r(m): g^{r(m)}\equiv\frac{1}{2}S_{14}\xi^{9m}, m=1,3,\cdots,9\}$

m	0	2	4	6	8
$r(m)$	0	16	4	17	6
$r(m)\pmod 9$	0	7	4	8	6

m	1	3	5	7	9
$r(m)$	11	12	16	6	9
$r(m)\pmod 9$	2	3	7	6	0

$\mathcal{D}_0=\{0,7,4,8,6\}$ $\mathcal{D}_1=\{2,3,7,6,0\}$

$\mathcal{D}_0^*=\{1,2,3,5\}$ $\mathcal{D}_1^*=\{1,4,5,8\}$

difference d	$(r,s), \pm d\equiv r-s\pmod 9, r,s\in\mathcal{D}_0$	$(r,s), \pm d\equiv r-s\pmod 9, r,s\in\mathcal{D}_1$	$\lambda(d)=\lambda$
±1	(0,8) (6,7) (7,8)	(2,3) (6,7)	5
±2	(0,7) (4,6) (6,8)	(0,2) (0,7)	5
±3	(0,6) (4,7)	(0,3) (0,6) (3,6)	5
±4	(0,4) (4,8)	(2,6) (2,7) (3,7)	5

(2) $Q=\{1,6,17,7,4,5,11,9,16\}$

$M=\{a: g^{2a}-1\in Q\}$

$a=0: 1-1=0$
- $a=1: 6-1=5$
- $a=2: 17-1=16$
- $a=3: 7-1=6$

$a=4: 4-1=3$
- $a=5: 5-1=4$

$a=6: 11-1=10$

$a=7: 9-1=8$

$a=8: 16-1=15$

$M=\{1,2,3,5\}$

$N=\{b: g^{2b}+1\in Q\}$

$b=0: 1+1=2$
- $b=1: 6+1=7$

$b=2: 17+1=18$

$b=3: 7+1=8$
- $b=4: 4+1=5$
- $b=5: 5+1=6$

$b=6: 11+1=12$

$b=7: 9+1=10$
- $b=8: 16+1=17$

$N=\{1,4,5,8\}$

参考文献

[1] L.D.Baumert, Cyclic Difference Sets, Springer-Verlag, Berlin-Heidelberg-New York, 1971.

[2] A.T.Butson, Relations among generalized Hadamard matrices, relative difference sets, and maximal length linear recurring sequences, Canad. J. Math. 15 (1963),42-48.

[3] J.E.H.Elliott and A.T.Butson, Relative difference sets, Illinois J. Math. 10 (1966),517-531.

[4] G.Szekeres, Tournaments and Hadamard matrices, Enseigment Math. 15 (1969),269-278.

[5] W.D.Wallis, A.P.Street and J.S.Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Springer-Verlag, Berlin-Heidelberg-New York, 1972.

[6] M.Yamada, On a relation of a cyclic relative difference set associated with the quadratic extension of a finite field and the Szekeres difference sets, submitted to Combinatorica.

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