

## 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  $-x \in M$  を満たすものが  $q \equiv 3 \pmod{4}$  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,  $t \geq 2$ ,  $\mathbb{Z}$ : 有理整数環。

$\xi$ :  $K$  の乗法群  $K^\times$  の生成元,  $\eta$ :  $F$  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。

定義  $\chi$  を  $F$  の指標,  $\zeta_p = e^{2\pi i/p}$  とする時 Gauss の和  $\zeta_F(\chi)$  は

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

で定義される。  $\chi = 1$  (単位指標) のとき  $\zeta_F(\chi) = -1$ ,  $\chi \neq 1$  ならば  $\zeta_F(\chi) \overline{\zeta_F(\chi)} = q$  が成り立つ。  $\chi \neq 1$  のとき、 $K$  の指標  $\chi$  に対する Gauss の和  $\zeta_K(\chi)$  と  $\chi$  を  $F$  に制限したときの  $F$  の Gauss の和  $\zeta_F(\chi)$  との比

$$\chi_{K/F}(x) = \frac{\chi_K(x)}{\chi_F(x)}$$

を  $\chi$  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、 $\chi_F$  を  $\chi$  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

$$\sum_{\beta \in \mathcal{L}_1} \chi(\beta) = \begin{cases} S_{K/F}(x) & \chi_F \neq 1 \text{ のとき,} \\ -\frac{1}{g} \chi_F(x) & \chi_F = 1, \chi_K \neq 1 \text{ のとき,} \\ g^{e-1} & \chi_K = 1 \text{ のとき.} \end{cases}$$

となる。

(証明)  $K^\times$  の元  $\alpha$  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

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

$$= \bar{\chi}(S_{\chi_F} \beta) \zeta_F(\chi).$$

(2)  $S_{\chi_F} \beta = 0$  の場合

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

以上から

(1)  $\chi_F \neq 1$  のとき

$$\vartheta_{\chi_F}(\chi) = \frac{\zeta_K(\chi)}{\zeta_F(\chi)} = \sum_{\beta \in \mathcal{L}_1} \bar{\chi}(S_{\chi_F} \beta) \chi(\beta) = \sum_{\beta \in \mathcal{L}_1} \chi(\beta).$$

(2)  $\chi_F = 1$  のとき  $\beta \in \mathcal{L}_1$  ならば  $\bar{\chi}(S_{\chi_F} \beta) \zeta_F(\chi) = -1$  になるので

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

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

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

を得る。 $\chi_K = 1$  のときは

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

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 Abelian 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,  
 $d = r - s, r, s \in R$  とはるペア  $(r, s)$  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  $f(x) = \sum_{r \in R} x^r$  とすると次が成り立つ。

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

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  $v, k, \lambda, h$  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  $\mathbb{Z}/(q^2-1)\mathbb{Z}$  の部分集合  $D_1$  を

$$D_1 = \{m : S_{q^2} \ni m = 1\}$$

で定義すると,  $D_1$  はパラメータ

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

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、

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

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

$$f(\zeta) = \sum_{m \in D_1} \zeta^m = \sum_{\beta \in K_1} \chi(\beta)$$

である。そこで任意の 1 の  $q^t-1$  乗根に対し

$$\sum_{\beta \in K_1} \chi(\beta) \cdot \sum_{\beta \in K_1} \bar{\chi}(\beta) = q^{t-1} + q^{t-2} (J_{q^{t-1}}(\zeta) - J_{q-1}(\zeta^{\frac{q^t-1}{q-1}}))$$

が成り立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)  $D_2 = \{m: S_{\kappa_f} \xi^m = 2\}$  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  $\{1, \xi, \dots, \xi^q\}$  にとると  $D_2 = \{k: \xi^k = \frac{2\xi^m}{S_{\kappa_f} \xi^m}, m=0, \dots, q, m \neq \frac{q+1}{2}\}$  と変形できる。

(III) さらに  $\xi^k$  の逆数をとって次のように変形できる。

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

$D = D_2$  は次のような性質をもつ。

定理 3  $D_0 = \{k \in D \pmod{q-1}, k: \text{偶数}\}, D_1 = \{k \in D \pmod{q-1}, k: \text{奇数}\}$

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  $-k \in D_1$ .

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

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。

補助定理 2  $z = \xi^{\frac{q-1}{2}}$ ,  $\Lambda(x)$  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  $\Lambda(\eta^k) = \eta^{k'}$  をみたす奇数の  $k' \pmod{2g+2}$  が唯一存在する。

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

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

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

である。そこで  $k'$  の偶、奇によらず  $\eta^{-k'} = -\eta^{k'}$  か  $\eta^{-k'} = \eta^{k'}$  とする。

$\eta^{k'} = \pm i = \pm \eta^{\frac{g+1}{2}}$  か  $\eta^{k'} = -1$  で  $\eta^{k'} = -1$  は  $k'$  が奇数に反する。従って  $\Lambda(\eta^k) = \eta^{k'}$  をみたすのは  $g \equiv 3 \pmod{4}$  で  $k \equiv k' \equiv \pm \frac{g+1}{2} \pmod{2g+2}$  のときだけである。

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

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

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

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

をみたす。一方  $g+1$  個の相異なる  $\eta$  の奇数中に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  $\Lambda(\eta^k) = \eta^{k'}$  とする奇数の  $k'$  が唯一存在する。

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

(2)  $k \in D$  ならば  $kg \in D$  である。  $kg \equiv k \pmod{g-1}$  から  $D \pmod{g-1}$  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  $\xi^{g-1}$  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。

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

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

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

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

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

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

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

であり、これが成り立つのは  $\alpha = \beta$  か  $\alpha = \frac{1}{\beta}$ 、 $m \equiv \pm m' \pmod{g+1}$  である。従って  $m \equiv 0 \pmod{g+1}$  とならば  $k=0$  を除いて  $k \equiv k' \pmod{g-1}$  となる  $k, k'$  は存在しない。

(3)  $\xi^{-k}, \xi^{-k'}$  を (2) と同じく定義する。  $k \equiv k' \pmod{g-1}$  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  $\xi^{k+k'} \in H$  でありこれは  $\xi$  と同値である。

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

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

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

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

から

$$N_{K/F}(\eta^{\frac{g+1}{2}+m} \eta^{\frac{g+1}{2}+m'} (\eta^{\frac{g+1}{2}+m} - \eta^{-\frac{g+1}{2}-m}) (\eta^{\frac{g+1}{2}+m'} - \eta^{-\frac{g+1}{2}-m'})) = 4^2$$

を得る。ところで

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

であるから上の相対ノルムは

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

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

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

が求まる。又2式で  $\eta^{\frac{g+1}{2}+m'}$  を  $-\eta^{\frac{g+1}{2}+m'}$ ,  $\eta^{\frac{g+1}{2}+m}$  を  $-\eta^{\frac{g+1}{2}+m}$  におきか

えると1式になる。  $k = \frac{g+1}{2} + m$ ,  $k' = \frac{g+1}{2} + m'$  において補助定

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  $n$  は奇数である。次のように集合  $D'$  を定義する。

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

$D'$  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  $\text{mod } n$  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

$$\begin{aligned} S_{k \neq} \xi^{\frac{g-1}{2}m} &= \xi^{\frac{g-1}{2}m} + \xi^{\frac{g^2-8}{2}m} = \xi^{\frac{g-1}{2}m} + (-1)^m \xi^{-\frac{g-1}{2}m}, \\ S_{k \neq} \xi^{\frac{g-1}{2}(\frac{g+1}{2}+m)} &= \xi^{\frac{g-1}{2}(\frac{g+1}{2}+m)} - (-1)^m \xi^{-\frac{g-1}{2}(\frac{g+1}{2}+m)} \end{aligned}$$

であるので

$$\begin{aligned} \xi^{-k} &= \xi^{\frac{g-1}{2}m} \cdot \frac{S_{k \neq} \xi^{\frac{g-1}{2}m}}{2} && m \text{ が偶数のとき} \\ \xi^{-k} &= \xi^{\frac{g-1}{2}(\frac{g+1}{2}+m)} \cdot \frac{S_{k \neq} \xi^{\frac{g-1}{2}(\frac{g+1}{2}+m)}}{2} && m \text{ が奇数のとき} \end{aligned}$$

となる。そこで  $r = r(m)$  と

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

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

$$\mathcal{D}_0 = \{r(m): g^{r(m)} = \frac{1}{2} S_{k \neq} \xi^{\frac{g-1}{2}m}, m=0, 2, \dots, \frac{g-3}{2}\},$$

$$\mathcal{D}_1 = \{r(m): g^{r(m)} = \frac{1}{2} S_{k \neq} \xi^{\frac{g-1}{2}m}, m=1, 3, \dots, \frac{g-1}{2}\}.$$

$\mathcal{D}_0, \mathcal{D}_1$  と  $D'_0, D'_1$  の間には

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

が成り立つ。集合  $\mathcal{D}_0, \mathcal{D}_1$  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  $S_1, \dots, S_n$  を  $\text{mod } v$  の相異なる剰余の集合で 各々  $k_1, \dots, k_n$  個の元を持つ。  $d \not\equiv 0 \pmod{v}$  に対し

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

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

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

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

が成り立つ。逆に  $\text{mod } v$  の相異なる剰余の集合  $S_1, \dots, S_n$  が各々  $k_1, \dots, k_n$  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  $S_1, \dots, S_n$  は  $n - \{v; k_1, \dots, k_n; \lambda\}$  supplementary difference sets である。

G. Szekeres はこのような 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 とする。

(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  $D_0, D_1$  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  $D_0, D_1$  を 3 で定義した集合。  $n = \frac{g-1}{2}$  とする。このとき次が成り立つ。

(1)  $D_0, D_1$  は  $2 - \{n; \frac{n+1}{2}; \frac{n+1}{2}\}$  supplementary difference sets である。

(2)  $D_0, D_1$  の補集合  $D_0^*, D_1^*$  は Szekeres 差集合である。

(証明) (1)  $D_0 \equiv -\frac{1}{2} D_0', D_1 \equiv -\frac{1}{2} D_1' \pmod{n}$  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

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

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

$$\theta_1(x^{-1}) \equiv \theta_1(x). \pmod{x^n - 1}.$$

定理 2 から

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

∴

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

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

から

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

を得る。一方

$$\begin{aligned} \theta(x)\theta(x^{-1}) &\equiv (-1+2\theta_0(x)+2\theta_1(x))(-1+2\theta_0(x^{-1})+2\theta_1(x^{-1})) \\ &\equiv 1-2(\theta_0(x)+\theta_0(x^{-1})+\theta_1(x)+\theta_1(x^{-1}))+4(\theta_0(x)\theta_0(x^{-1})+\theta_1(x)\theta_1(x^{-1})) \\ &\quad +4(\theta_0(x)\theta_1(x^{-1})+\theta_0(x^{-1})\theta_1(x)) \\ &\equiv -1+2n J_n(x)+4(\theta_0(x)\theta_0(x^{-1})+\theta_1(x)\theta_1(x^{-1})) \pmod{x^n-1} \end{aligned}$$

∴ 比較することにより次が求まる。

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

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

$$\#D'_0 = \#D'_1 = \frac{n+1}{2} \quad \text{から } D'_0, D'_1 \text{ は } 2-\{n; \frac{n+1}{2}; \frac{n+1}{2}\} \text{ supplementary}$$

difference sets となる。

(2)  $\gamma \in D_0$  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

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

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  $r \in \mathcal{Q}_1$  とする。

$$g^r = \frac{1}{2} S_{\frac{n}{2}} \xi^{\frac{n-1}{2}m} = \frac{1}{2} S_{\frac{n}{2}} \eta^m = \frac{1}{2}(\eta^m - \eta^{-m}),$$

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

同じようにして

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

から

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

を得る。以上から  $r \in \mathcal{Q}_0$  ならば  $r \in M^*$ ,  $r \in \mathcal{Q}_1$  ならば  $r \in N^*$ ,

$M^*, N^*$  は  $M, N$  の補集合である。しかし  $\#\mathcal{Q}_0 = \#\mathcal{Q}_1 = \frac{n+1}{2}$ ,

$$\#M^* = \#N^* = n - \frac{n-1}{2} = \frac{n+1}{2}. \text{ 従って}$$

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

である。

## 5 あとがき

我々は  $\mathcal{Q}_0, \mathcal{Q}_1$  の方が Szehered 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られている。

$q=19$ 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)  $\mathcal{D}_0 = \{r(m) : g^{\frac{r(m)}{2}} = \frac{1}{2} S_{\frac{r(m)}{2}} \xi^{9m}, m=0, 2, \dots, 8\}, \mathcal{D}_1 = \{r(m) : g^{\frac{r(m)}{2}} = \frac{1}{2} S_{\frac{r(m)}{2}} \xi^{9m}, m=1, 3, \dots, 9\}$

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

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

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

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

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

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

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

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

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

$$\begin{aligned} a=0 : 1-1=0 & \quad \bullet a=5 : 5-1=4 \\ \bullet a=1 : 6-1=5 & \quad a=6 : 11-1=10 \\ \bullet a=2 : 17-1=16 & \quad a=7 : 9-1=8 \\ \bullet a=3 : 7-1=6 & \quad a=8 : 16-1=15 \\ a=4 : 4-1=3 & \end{aligned}$$

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

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

$$\begin{aligned} b=0 : 1+1=2 & \quad \bullet b=5 : 5+1=6 \\ \bullet b=1 : 6+1=7 & \quad b=6 : 11+1=12 \\ b=2 : 17+1=18 & \quad b=7 : 9+1=10 \\ b=3 : 7+1=8 & \quad \bullet b=8 : 16+1=17 \\ \bullet b=4 : 4+1=5 & \end{aligned}$$

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

## 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, Enseignement 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.