COMBINATORICA
Akadémiai Kiadó — Springer-Verlag

COMBINATORICA 8 (2) (1988) 207—216

# ON A RELATION BETWEEN A CYCLIC RELATIVE DIFFERENCE SET ASSOCIATED WITH THE QUADRATIC EXTENSIONS OF A FINITE FIELD AND THE SZEKERES DIFFERENCE SETS

MIEKO YAMADA

*Received 15 September 1985*
*Revised 9 May 1986*

Let $q \equiv 3 \pmod 4$ be a prime power and put $n=\frac{q-1}{2}$. We consider a cyclic relative difference set with parameters $q^2-1, q, 1, q-1$ associated with the quadratic extension $\mathrm{GF}(q^2)/\mathrm{GF}(q)$. The even part and the odd part of the cyclic relative difference set taken modulo $n$ are $2-\left\{n; \frac{n+1}{2}; \frac{n+1}{2}\right\}$ supplementary difference sets. Moreover it turns out that their complementary subsets are identical with the Szekeres difference sets. This result clarifies the true nature of the Szekeres difference sets. We prove these results by using the theory of the relative Gauss sums.

## 0. Notation

$q$: a power of a prime $p$
$F=\mathrm{GF}(q)$: a finite field with $q$ elements
$K=\mathrm{GF}(q^t)$: an extension of $F$ of degree $t \geqq 2$
$\xi$: a primitive element of $K$
$g$: a primitive element of $F$
$K^*$: the multiplicative group of $K$
$F^*$: the multiplicative group of $F$
$S_K$: trace from $K$
$S_F$: trace from $F$
$S_{K/F}$: relative trace from $K$ to $F$
$N_{K/F}$: relative norm from $K$ to $F$
$\mathbf{Z}$: the rational integer ring
$J_m(x)=1+x+x^2+\ldots+x^{m-1}$

## 1. Relative Gauss sums

We define Gauss sums and relative Gauss sums over a finite field.

**Definition 1.1.** Let $\chi$ be a character of $F$ and $\zeta_p=e^{2\pi i/p}$. Then the *Gauss sum* $\tau_F(\chi)$ is defined by:

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

AMS subject classification: 05 B 10

When $\chi=1$, the principal character, then $\tau_F(\chi)=-1$. If $\chi\neq 1$, then we have $\tau_F(\chi)\overline{\tau_F(\chi)}=q$.

If $\chi$ is a non-principal character of $K$, then the ratio

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

of the two Gauss sums is called the *relative Gauss sum associated with* $\chi$.

The following theorem gives important information on relative difference sets.

**Theorem 1.2.** (See [5]). *Let $\chi=\chi_K$ be a character of $K$ and let $\chi_F$ denote the character $\chi$ restricted to $F$. We take a system $L$ of representatives of the quotient group $K^*/F^*$ and we decompose $L$ in two parts as follows:*

$$L=L_0\cup L_1;\ L_0=\{\beta:\ S_{K/F}\beta=0\},\quad L_1=\{\beta:\ S_{K/F}\beta=1\}.$$

*Then we have:*

$$\sum_{\beta\in L_1}\chi(\beta)=\begin{cases}\vartheta_{K/F}(\chi) & \text{when}\quad \chi_F\neq 1,\\ -\dfrac{1}{q}\tau_K(\chi) & \text{when}\quad \chi_K\neq 1\quad\text{and}\quad \chi_F=1,\\ q^{t-1} & \text{when}\quad \chi_K=1.\end{cases}$$

**Proof.** An element $\alpha$ in $K^*$ is represented uniquely as $\alpha=a\beta$ for $a\in F^*$, $\beta\in L$.

$$\tau_K(\chi)=\sum_{a\in F^*}\sum_{\beta\in L}\chi(a\beta)\zeta_p^{S_F(a\beta)}=\sum_{\beta\in L}\chi(\beta)\sum_{a\in F^*}\chi(a)\zeta_p^{S_F(aS_{K/F}\beta)}.$$

We distinguish two cases.

(i) If $S_{K/F}\beta\neq 0$, then

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

(ii) If $S_{K/F}\beta=0$, then

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

Therefore:

(i) When $\chi_F\neq 1$, we get $\vartheta_{K/F}(\chi)=\dfrac{\tau_K(\chi)}{\tau_F(\chi)}=\sum_{\beta\in L_1}\bar{\chi}(S_{K/F}\beta)\chi(\beta)=\sum_{\beta\in L_1}\chi(\beta)$.

(ii) When $\chi_F=1$, then since $\bar{\chi}(S_{K/F}\beta)\tau_F(\chi)=-1$ for $\beta\in L_1$, we have

$$\tau_K(\chi)=(q-1)\sum_{\beta\in L_0}\chi(\beta)-\sum_{\beta\in L_1}\chi(\beta)=-\sum_{\beta\in L}\chi(\beta)+q\sum_{\beta\in L_0}\chi(\beta).$$

For this case, if $\chi_K\neq 1$, then we have $\sum_{\beta\in L}\chi(\beta)=0$. Hence $\tau_K(\chi)=q\sum_{\beta\in L_0}\chi(\beta)=$ $=-q\sum_{\beta\in L_1}\chi(\beta)$.

When $\chi_K=1$, we have $\tau_K(\chi)=-\sum_{\beta\in L}\chi(\beta)+q\sum_{\beta\in L_0}\chi(\beta)=-\frac{q^t-1}{q-1}+q\sum_{\beta\in L_0}\chi(\beta)=$ $=-1$. Thus we get $\sum_{\beta\in L_0}\chi(\beta)=\frac{q^{t-1}-1}{q-1}$, and

$$\sum_{\beta\in L_1}\chi(\beta)=\sum_{\beta\in L}\chi(\beta)-\sum_{\beta\in L_0}\chi(\beta)=\frac{q^t-1}{q-1}-\frac{q^{t-1}-1}{q-1}=q^{t-1}. \quad \blacksquare$$

## 2. Relative difference sets

The concept of relative difference sets was introduced by A. T. Butson [2]. J. E. H. Elliott and A. T. Butson have shown several basic results [3]. We recall the definition of relative difference sets.

**Definition 2.1.** Let $G$ be an abelian group of order $v$ and $R$ be a subset of $G$ containing $k$ elements. Let $H$ be a subgroup of $G$ of order $h$. If for $d\neq 0$, $d\in G$, the number of pairs $(r, s)$ such that $d=r-s$, $r, s\in R$, has the fixed values

$$\begin{cases}\lambda & \text{when} \quad d\notin H,\\ 0 & \text{when} \quad d\in H,\end{cases}$$

then $R=R(v, k, \lambda, h)$ is called a *relative difference set.*

**Lemma 2.2.** *Assume that $G$ is a cyclic group. Let $f(x)$ denote the Hall polynomial of $R(v, k, \lambda, h)$, then we have*

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

The following is an example of cyclic relative difference sets.

**Theorem 2.3.** *Define the subset*

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

*of* $\mathbf{Z}/(q^t-1)\mathbf{Z}$. *Then $D_1$ is a relative difference set with parameters*

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

**Proof.** We prove the theorem by showing that

$$f(x)f(x^{-1})\equiv q^{t-1}+q^{t-2}\left(J_{q^t-1}(x)-J_{q-1}(x^{(q^t-1)/(q-1)})\right) \pmod{x^{q^t-1}-1},$$

where $f(x)$ denotes the Hall polynomial of $D_1$. If $\chi(\xi)=\zeta$ where $\chi$ is a character of $K$ and $\zeta$ is a $(q^t-1)^{\text{th}}$ root of unity, then we have $f(\zeta)=\sum_{m\in D_1}\zeta^m=\sum_{\beta\in L_1}\chi(\beta)$. Hence it sufficies to verify

$$\sum_{\beta\in L_1}\chi(\beta)\cdot\sum_{\beta\in L_1}\bar{\chi}(\beta)=q^{t-1}+q^{t-2}\left(J_{q^t-1}(\zeta)-J_{q-1}(\zeta^{(q^t-1)/(q-1)})\right) \tag{2.1}$$

for a $(q^t-1)^{\text{th}}$ root of unity $\zeta$. Now from Theorem 1.2, we have:

(i) when $\chi_F \neq 1$, then

$$\sum_{\beta\in L_1}\chi(\beta)\cdot\sum_{\beta\in L_1}\bar{\chi}(\beta)=\vartheta_{K/F}(\chi)\overline{\vartheta_{K/F}(\chi)}=\frac{\tau_K(\chi)\overline{\tau_K(\chi)}}{\tau_F(\chi)\overline{\tau_F(\chi)}}=q^{t-1};$$

(ii) when $\chi_F=1$ and $\chi_K\neq 1$, then

$$\sum_{\beta\in L_1}\chi(\beta)\cdot\sum_{\beta\in L_1}\bar{\chi}(\beta)=\frac{1}{q^2}\tau_K(\chi)\overline{\tau_K(\chi)}=q^{t-2};$$

(iii) when $\chi_K=1$, then

$$\sum_{\beta\in L_1}\chi(\beta)\cdot\sum_{\beta\in L_1}\bar{\chi}(\beta)=q^{2(t-1)}.$$

Combining these, we verify the formula (2.1). ∎

We shall call this the cyclic relative difference set associated with the extension $K/F$.

### 3. Cyclic relative difference sets associated with $K/F$ for the case $t=2$

In this paper, we treat the cyclic relative difference set above for the case $t=2$ in Theorem 2.3. From Theorem 2.3, the subset $D_1=\{m: S_{K/F}\xi^m=1\}$ of $\mathbf{Z}/(q^2-1)\mathbf{Z}$ is a cyclic relative difference set with parameters $v=q^2-1$, $k=q$, $\lambda=1$, $h=q-1$. Let $2=g^c$ for an integer $c\neq 0$, then $2=2S_{K/F}\xi^m=g^cS_{K/F}\xi^m=S_{K/F}\xi^{m+c(q+1)}$ for $m\in D_1$. Hence the subset $D_2=\{m: S_{K/F}\xi^m=2\}=\{m+c(q+1): S_{K/F}\xi^m=1\}=D_1+c(q+1)$ is a translate of $D_1$, and contains 0.

Next we take a system of the representatives $L'=\{1,\xi,\ldots,\xi^q\}$ of $K^*/F^*$. Then each element $\beta$ such that $S_{K/F}\beta=1$ is represented uniquely as $\beta=a^{-1}\alpha$ for $a=S_{K/F}\alpha\neq 0$. $\alpha\in L'$. Therefore we get

$$D_2=\left\{k: \xi^k=\frac{2\xi^m}{S_{K/F}\xi^m},\quad m=0,\ldots,q,\quad m\neq\frac{q+1}{2}\right\}.$$

The inverse element of $\xi^k$ is given by

$$\xi^{-k}=\frac{S_{K/F}\xi^m}{2\xi^m}=\frac{\xi^m+\xi^{mq}}{2\xi^m}=\frac{1}{2}(1+\xi^{m(q-1)})=\frac{1}{2}(\xi^{((q-1)/2)m}+\xi^{-((q-1)/2)m})\xi^{((q-1)/2)m}.$$

Thus we have

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

The subset $D=D_2$ has the following properties.

**Theorem 3.1.** *We define* $D_0=\{k\in D \pmod{q-1}, k \text{ even}\}$, and $D_1=\{k\in D \pmod{q-1}, k, \text{ odd}\}$, *so that* $D \pmod{q-1}=D_0\cup D_1$. *Then* $D \pmod{q-1}$ *has the following*

*properties:*

(1) *If $m$ is even (odd), then $k \pmod{q-1}$ is even (odd).*
(2) *$D \pmod{q-1}$ contains every $k \neq 0$ exactly twice.*
(3) *For the case $q \equiv 1 \pmod 4$, if $k \in D_0$ then $-k \in D_0$ and if $k \in D_1$ then $-k \notin D_1$. For the case $q \equiv 3 \pmod 4$, if $k \in D_0$ then $-k \notin D_0$ and if $k \in D_1$ then $-k \in D_1$.*

The following lemma is interesting and is essential in proving Theorem 3.1.

**Lemma 3.2.** *Put $\eta = \xi^{(q-1)/2}$ and let $\Lambda(x)$ denote the linear fractional transformation: $\Lambda(x) = \dfrac{x+1}{x-1}$. When $k$ is odd, there exists one and only one odd $k' \pmod{2q+2}$ satisfying $\Lambda(\eta^k) = \eta^{k'}$. When $k$ is even, there exists an even $k'$ satisfying $\Lambda(\eta^k) = \eta^{k'}$ if and only if $q \equiv 3 \pmod 4$ and $k \equiv \pm\dfrac{q+1}{2} \pmod{2q+2}$.*

**Proof.** First we suppose $k$ and $k'$ are even and $\Lambda(\eta^k) = \eta^{k'}$. Since $\eta^q = -\eta^{-1}$ and $\eta^{kq} = \eta^{-k}$, we have $\eta^{-k'} = \Lambda(\eta^k)^q = \Lambda(\eta^{kq}) = \Lambda(\eta^{-k}) = \dfrac{\eta^{-k}+1}{\eta^{-k}-1} = -\Lambda(\eta^k) = -\eta^{k'}$. Hence we have $\eta^{-k'} = -\eta^{k'}$ and $\eta^{k'} = \pm i$ where $i = \eta^{(q+1)/2}$ is a primitive fourth root of unity in $K$. Also $\eta^k = \pm i$. This means $k \equiv k' \equiv \pm\dfrac{q+1}{2} \pmod{2q+2}$.

Next we suppose that $k$ and $k'$ are odd and $\Lambda(\eta^k) = \eta^{k'}$. Since $\eta^{kq} = -\eta^{-k}$, we have $\Lambda(\eta^k)^q = \Lambda(\eta^{kq}) = \Lambda(-\eta^{-k}) = \dfrac{-\eta^{-k}+1}{-\eta^{-k}-1} = -\Lambda(\eta^k)^{-1}$. Every $\Lambda(\eta^k)$ for odd $k$ satisfies the algebraic equation $x^{q+1}+1 = 0$ of degree $q+1$. On the other hand, the $q+1$ distinct elements $\eta^k$ for odd $k$ also satisfy the equation above, which means that $\eta^k$ are all the roots of the equation, i.e. there exists one and only one odd $k'$ such that $\Lambda(\eta^k) = \eta^{k'}$. ∎

**Proof of Theorem 3.1.** (1) Since $q-1$ is even, we see from $\xi^{-k} = \dfrac{S_{K/F}\xi^m}{2\xi^m}$ that if $m$ is even (odd), then $k$ is even (odd).

(2) If $k \in D$ then $kq \in D$. Since $kq \equiv k \pmod{q-1}$, we see that $D \pmod{q-1}$ contains $k \neq 0$ twice. Next we show that $D \pmod{q-1}$ contains $k \neq 0$ twice 'exactly'. Let $H$ be a group generated by $\xi^{q-1}$. This is characterized as the set of elements with relative norm 1. Put $\xi^{-k} = \dfrac{1}{2}(1+\xi^{(q-1)m})$ and $\xi^{-k'} = \dfrac{1}{2}(1+\xi^{(q-1)m'})$ and assume $k \equiv k' \pmod{q-1}$. This means $\xi^{-k} \equiv \xi^{-k'} \pmod{\times H}$, which is equivalent to

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

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

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

Putting $\alpha=\xi^{(q-1)m}$ and $\beta=\xi^{(q-1)m'}$, the equation above becomes $\alpha+\frac{1}{\alpha}=\beta+\frac{1}{\beta}$. Thus we have $\alpha=\beta$ or $\alpha=\frac{1}{\beta}$, that is $m\equiv\pm m' \pmod{q+1}$. This implies that there exists no $k$ such that $k\equiv k' \pmod{q-1}$ except $k=0$.

(3) Similarly let $\xi^{-k}$ and $\xi^{-k'}$ be as in the proof of (2) and assume $k\equiv -k' \pmod{q-1}$. From the proof of (1), we have $k\equiv k' \pmod 2$. The assumption $k+k'\equiv 0 \pmod{q-1}$ means $\xi^{k+k'}\in H$, or

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

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

Let $\eta$ and $i$ be as in Lemma 3.2. Since

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

$$=1-(\eta^{((q+1)/2)+m})^2=-\eta^{((q+1)/2)+m}(\eta^{((q+1)/2)+m}-\eta^{-((q+1)/2)-m}),$$

we have

$$N_{K/F}(\eta^{((q+1)/2)+m}\eta^{((q+1)/2)+m'}(\eta^{((q+1)/2)+m}-\eta^{-((q+1)/2)-m})\times \tag{3.1}$$

$$\times(\eta^{((q+1)/2)+m'}-\eta^{-((q+1)/2)-m'}))=4^2.$$

We observe

$$\left(\eta^k-\frac{1}{\eta^k}\right)^q=\eta^{kq}-\frac{1}{\eta^{kq}}=\left(-\frac{1}{\eta}\right)^k-(-\eta)^k=(-1)^k\left(\frac{1}{\eta^k}-\eta^k\right)=(-1)^{k-1}\left(\eta^k-\frac{1}{\eta^k}\right).$$

Thus the equation (3.1) becomes

$$(\eta^{((q+1)/2)+m}-\eta^{-((q+1)/2)-m})(\eta^{((q+1)/2)+m'}-\eta^{-((q+1)/2)-m'})=\pm 4.$$

Replacing $m'$ by $q+1-m'$ if necessary, we may reduce to the case when $+$ sign is valid in the equation above. In this case,

$$\eta^{((q+1)/2)+m'}=\frac{\eta^{((q+1)/2)+m}+1}{\eta^{((q+1)/2)+m}-1}=A(\eta^{((q+1)/2)+m}),\ \eta^{((q+1)/2)+m'}=\frac{-\eta^{((q+1)/2)+m}+1}{\eta^{((q+1)/2)+m}+1}.$$

When we replace $\eta^{((q+1)/2)+m'}$ and $\eta^{((q+1)/2)+m}$ by $-\eta^{((q+1)/2)+m'}$ and $-\eta^{((q+1)/2)+m}$ respectively in the second equation, we get the first equation. If we put $k=\frac{q+1}{2}+m$ and $k'=\frac{q+1}{2}+m'$, then the assertion (3) follows by Lemma 3.2. ∎

In the rest of this section, we suppose $q\equiv 3 \pmod 4$. Put $n=\frac{q-1}{2}$, then $n$ is odd. Define the subset $D'=\{k \pmod n: \xi^{-k}=\frac{1}{2}(1+\xi^{(q-1)m}), m=0, 1, \ldots, n\}$,

and $D_0'=\{k\in D',\ m \text{ even}\}$ and $D_1'=\{k\in D',\ m \text{ odd}\}$. Then $D'=D_0'\cup D_1'$. From Theorem 3.1, $D_0'$ and $D_1'$ have the following properties:

(1) $D_0'$ has $\dfrac{n+1}{2}$ distinct elements (mod $n$) and the same is true for $D_1'$.
(2) If $k\in D_0'$ then $-k\notin D_0'$ and if $k\in D_1'$ then $-k\in D_1'$.
(3) Let $D_0'^*=\{-k\colon k\in D_0',\ k\neq 0\}$, then $D_0'\cup D_0'^*=\mathbf{Z}/n\mathbf{Z}$.

Now, we have

$$S_{K/F}\xi^{((q-1)/2)m}=\xi^{((q-1)/2)m}+\xi^{((q^2-q)/2)m}=\xi^{((q-1)/2)m}+\xi^{((q^2-1)/2)m-((q-1)/2)m}=$$

$$=\xi^{((q-1)/2)m}+(-1)^m\xi^{-((q-1)/2)m}$$

and

$$S_{K/F}\xi^{((q-1)/2)(((q+1)/2)+m)}=\xi^{((q-1)/2)(((q+1)/2)+m)}+(-1)^m\xi^{-((q-1)/2)(((q+1)/2)+m)}.$$

Thus we get

$$\xi^{-k}=-\xi^{((q-1)/2)m}\frac{S_{K/F}\xi^{((q-1)/2)m}}{2} \qquad \text{if } m \text{ is even,}$$

$$\xi^{-k}=\xi^{((q-1)/2)(((q+1)/2)+m)}\frac{S_{K/F}\xi^{((q-1)/2)(((q+1)/2)+m)}}{2} \qquad \text{if } m \text{ is odd.}$$

We define $r=r(m)$ by $g^r=g^{r(m)}=\dfrac{1}{2}S_{K/F}\xi^{((q-1/2)m}$, and define the subsets

$$\mathscr{D}_0=\left\{r(m)\colon g^{r(m)}=\frac{1}{2}S_{K/F}\xi^{((q-1)/2)m},\quad m=0,2,4,\ldots,\frac{q-3}{2}\right\},$$

$$\mathscr{D}_1=\left\{r(m)\colon g^{r(m)}=\frac{1}{2}S_{K/F}\xi^{((q-1)/2)m},\quad m=1,3,5,\ldots,\frac{q-1}{2}\right\},$$

of $\mathbf{Z}/n\mathbf{Z}$. Then we have $\mathscr{D}_0=-\dfrac{1}{2}D_0'$ and $\mathscr{D}_1=-\dfrac{1}{2}D_1'$. The subsets $\mathscr{D}_0$ and $\mathscr{D}_1$ have simpler structure than $D_0'$ and $D_1'$, and are convenient for computation.

## 4. Szekeres difference sets

First we define supplementary difference sets.

**Definition 4.1.** (See [4], *p.* 281). Let $S_1,\ldots,S_n$ be sets of distinct residues modulo $v$ containing $k_1,\ldots,k_n$ elements respectively. For the residue $d\not\equiv 0 \pmod v$, we define the number $\lambda_i(d)=\#\{(r,s)\colon d\equiv r-s \pmod v,\ r,s\in S_i\}$, and let $\lambda(d)=\lambda_1(d)+\lambda_2(d)+\ldots+\lambda_n(d)$. If $\lambda(d)$ has a constant value $\lambda$ for any residue $d\not\equiv 0 \pmod v$, then $S_1,\ldots,S_n$ are called $n-\{v;k_1,\ldots,k_n;\lambda\}$ *supplementary difference sets.* If $k_1=\ldots=k_n$, we write $n-\{v;k_1;\lambda\}$. Let $f_1(x),f_2(x),\ldots,f_n(x)$ be the

Hall polynomials of $S_1, S_2, \ldots, S_n$ respectively, then we have

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

This equation characterizes the supplementary difference sets.

G. Szekeres has shown the existence of the following supplementary difference sets.

**Theorem 4.2.** (Szekeres, [4]). *Let* $q \equiv 3 \pmod 4$ *be a prime power and let* $Q$ *be the set of the quadratic residues in* $F$. *We define the sets* $M = \{a: g^{2a} - 1 \in Q\}$, *and* $N = \{b: g^{2b} + 1 \in Q\}$. *Then* $M$ *and* $N$ *are* $2 - \left\{\frac{q-1}{2}; \frac{q-3}{4}; \frac{q-7}{4}\right\}$ *supplementary difference sets.*

We may call this the *Szekeres difference sets*. It is known that the Szekeres difference sets are important for construction of Hadamard matrices. Here we show that the complementary subsets of $\mathcal{D}_0$ and $\mathcal{D}_1$ as in Section 3 are the Szekeres difference sets. This gives an explanation to the origin of the somewhat isolated Szekeres difference sets, showing that their complementary sets are more natural, and are derived from a cyclic relative difference set associated with the extension of a finite field.

**Theorem 4.3.** *Let* $\mathcal{D}_0, \mathcal{D}_1$ *and* $n$ *be as in Section 3. Then*

(1) $\mathcal{D}_0$ *and* $\mathcal{D}_1$ *are* $2 - \left\{n; \frac{n+1}{2}; \frac{n+1}{2}\right\}$ *supplementary difference sets,*

(2) *the complementary sets of* $\mathcal{D}_0$ *and* $\mathcal{D}_1$ *are the Szekeres difference sets.*

**Proof.** (1) Since $\mathcal{D}_0 = -\frac{1}{2}D_0'$ and $\mathcal{D}_1 = -\frac{1}{2}D_1'$, it sufficies to show that $D_0'$ and $D_1'$ are $2 - \left\{n; \frac{n+1}{2}; \frac{n+1}{2}\right\}$ supplementary difference sets. Let $\theta(x)$, $\theta_0(x)$, and $\theta_1(x)$ be the Hall polynomials of $D$, $D_0'$ and $D_1'$ respectively. From the results in Section 3, we have

$$\begin{cases} \theta(x) \equiv -1 + 2\theta_0(x) + 2\theta_1(x) & (\mathrm{mod}\ x^n - 1), \\ \theta_0(x) + \theta_0(x^{-1}) \equiv 1 + J_n(x) & (\mathrm{mod}\ x^n - 1), \\ \theta_1(x) \equiv \theta_1(x^{-1}) & (\mathrm{mod}\ x^n - 1). \end{cases}$$

And from Theorem 2.3, we have $\theta(x)\theta(x^{-1}) \equiv q + J_{q^2-1}(x) - J_{q-1}(x^{q+1}) \pmod{x^{q^2-1} - 1}$. Since

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

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

we have

$$\theta(x)\theta(x^{-1}) \equiv q + 2qJ_n(x) \pmod{x^n - 1}. \tag{4.1}$$

On the other hand,

$$\begin{aligned}(4.2)\qquad \theta(x)\theta(x^{-1}) &\equiv (-1+2\theta_0(x)+2\theta_1(x))(-1+2\theta_0(x^{-1})+2\theta_1(x^{-1}))\\ &\equiv 1-2(\theta_0(x)+\theta_0(x^{-1})+\theta_1(x)+\theta_1(x^{-1}))+4(\theta_0(x)\theta_1(x^{-1})\\ &\quad+\theta_0(x^{-1})\theta_1(x))+4(\theta_0(x)\theta_0(x^{-1})+\theta_1(x)\theta_1(x^{-1}))\\ &\equiv 1-2(J_n(x)+1+2\theta_1(x))+4(J_n(x)+1)\theta_1(x)\\ &\quad+4(\theta_0(x)\theta_0(x^{-1})+\theta_1(x)\theta_1(x^{-1}))\\ &\equiv -1+2nJ_n(x)+4(\theta_0(x)\theta_0(x^{-1})+\theta_1(x)\theta_1(x^{-1}))\\ &\qquad\qquad (\mathrm{mod}\ x^n-1).\end{aligned}$$

Comparing (4.1) with (4.2), we get

$$\begin{aligned}4(\theta_0(x)\theta_0(x^{-1})+\theta_1(x)\theta_1(x^{-1})) &\equiv q+1+2qJ_n(x)-2nJ_n(x)\\ &\equiv 2n+2+(2n+2)J_n(x) \pmod{x^n-1}.\end{aligned}$$

Namely

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

Since $\#D_0'=\#D_1'=\dfrac{n+1}{2}$, we see that $D_0'$ and $D_1'$ are $2-\left\{n;\dfrac{n+1}{2};\dfrac{n+1}{2}\right\}$ supplementary difference sets.

(2) Assume $r\in\mathscr{D}_0$, then

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

and

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

Since $\dfrac{1}{2}(\eta^m-\eta^{-m})^q=-\dfrac{1}{2}(\eta^m-\eta^{-m})$ we have $\dfrac{1}{2}(\eta^m-\eta^{-m})\notin F$, $\left(\dfrac{1}{2}(\eta^m-\eta^{-m})\right)^2\in F$. Thus we obtain $g^{2r}-1\notin Q$.

Next we assume $r\in\mathscr{D}_1$, then

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

and

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

Similarly we have $\dfrac{1}{2}(\eta^m+\eta^{-m})\notin F$, $\left(\dfrac{1}{2}(\eta^m+\eta^{-m})\right)^2\in F$, that is $g^{2r}+1\notin Q$. Consequently if $r\in\mathscr{D}_0$, then $r\in M^*$ and if $r\in\mathscr{D}_1$, then $r\in N^*$ where $M^*$ and $N^*$ are

the complementary sets of $M$ and $N$ respectively. But we know that $\#D_0 = \#D_1 = \frac{n+1}{2}$ and $\#M^* = \#N^* = n - \frac{n-1}{2} = \frac{n+1}{2}$. Hence we have that $\mathscr{D}_0 = M^*$, $\mathscr{D}_1 = N^*$. ∎

**Example.** $q=19$, $n=9$, $g=14$.

(1)

| $m$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $r(m)$ | 0 | 11 | 16 | 12 | 4 | 16 | 17 | 6 | 6 | 9 |
| $r(m) \pmod 9$ | 0 | 2 | 7 | 3 | 4 | 7 | 8 | 6 | 6 | 0 |

$$\mathscr{D}_0 = \{0, 7, 4, 8, 6\}, \quad \mathscr{D}_1 = \{2, 3, 7, 6, 0\},$$
$$\mathscr{D}_0^* = \{1, 2, 3, 5\}, \quad \mathscr{D}_1^* = \{1, 4, 5, 8\}.$$

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

| $m$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| $g^{2m}-1$ | 0 | $5 \in Q$ | $16 \in Q$ | $6 \in Q$ | 3 | $4 \in Q$ | 10 | 8 | 15 |
| $g^{2m}+1$ | 2 | $7 \in Q$ | 18 | 8 | $5 \in Q$ | $6 \in Q$ | 12 | 10 | $17 \in Q$ |

$$M = \{1, 2, 3, 5\}, \quad N = \{1, 4, 5, 8\}.$$

## References


[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] 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.

[5] K. YAMAMOTO, On congruences arising from relative Gauss sums, in: *Number Theory and Combinatorics Japan 1984, World Scientific Publ.*, 1985, 423—446.



Mieko Yamada

*Department of Mathematics*
*Tokyo Woman's Christian University*
*Zempukuji 2-6-1, Suginami-ku*
*Tokyo, 167 Japan*