On non-symmetric relative difference sets

Yutaka HIRAMINE
(Received February 5, 2007)

Abstract. Let $D$ be a $(m, u, k, \lambda)$-difference set in a group $G$ relative to a subgroup $U$ of $G$. We say $D$ is symmetric if $D^{(-1)}$ is also a $(m, u, k, \lambda)$-difference set. By a result of [7] $D$ is symmetric if $U$ is a normal subgroup of $G$. In general, $D$ is non-symmetric when $U$ is not normal in $G$. In this paper we study a condition under which $D$ is symmetric and show that if $D$ is semiregular then $D$ is symmetric if and only if the dual of dev($D$) is a divisible design. We also give a modification of Davis' product construction of relative difference sets and as an application we give a class of non-symmetric semiregular relative difference sets.

Key words: relative difference set, non-symmetric transversal designs.

1. Introduction

Let $G$ be a group of order $mu$ and $U$ a subgroup of $G$ of order $u$. A $k$-subset $D$ of $G$ is called a $(m, u, k, \lambda)$-difference set in $G$ with respect to $U$ if the list of quotients $d_1d_2^{-1}$ with $d_1, d_2 \in D$ ($d_1 \neq d_2$) contains each element in $G \setminus U$ exactly $\lambda$ times and no element in $U$. The definition yields the group ring equation

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

where we identify a subset $X$ of $G$ with a group ring element $\hat{X} = \sum_{x \in X} x \in \mathbb{C}[G]$ and set $X^{(-1)} = \sum_{x \in X} x^{-1}$. $D$ is also called a relative difference set relative to $U$ and $U$ is called a forbidden subgroup. By definition $m \geq k$ and $k^2 = k + \lambda(mu - u)$. We note that $D^{(-1)}$ is not always a relative difference set. For a $(m, u, k, \lambda)$-difference set $D$ in a group $G$ relative to $U$, dev($D$) (= $(\mathbb{P}, \mathbb{B})$) is an incidence structure with a set of points $\mathbb{P} = \{g \mid g \in G\}$ and a set of blocks $\mathbb{B} = \{Dg \mid g \in G\}$. Then dev($D$) is a $(m, u, k, \lambda)$-divisible design ([7]). If $m = k$ then $(m, u, k, \lambda) = (u\lambda, u, u\lambda, \lambda)$ and $D$ is said to be semiregular.

A $(m, u, k, \lambda)$-difference set $D$ is called symmetric if $D^{(-1)}$ is also a $(m, u, k, \lambda)$-difference set. In Section 2 we study a semiregular relative
difference set $D$ and show that $D$ is symmetric if and only if the dual of dev($D$) is a divisible design (Corollary 2.7).

In Sections 3 and 4 we give a construction for relative difference sets $D$ such that dev($D$) is non-symmetric. To construct such difference sets we present the following lemma on products of semiregular relative difference sets, which is a modification of Theorem 2.1 of [4] or Result 2.1 of [8].

**Lemma 3.1** Let $X = G \times H$ be a group, where $G$ is a group of order $u^2 \lambda$ and $H$ is a group of order $u \lambda'$. Let $D$ be a $(u \lambda, u, u \lambda, \lambda)$-difference set in $G$ relative to a subgroup $U$ of $G$ of order $u$ and let $C$ be a $(u \lambda', u, u \lambda', \lambda')$-difference set in $G' = U \times H$ relative to $U$. Then

(i) $CD$ is a $(u^2 \lambda \lambda', u, u^2 \lambda \lambda', u \lambda \lambda')$-difference set in $X$ relative to $U \times 1$.

(ii) $CD$ is symmetric if and only if $D$ is symmetric.

We note that $U$ is not assumed to be normal in $G$ in Lemma 3.1. Roughly speaking, Lemma 3.1(ii) implies that a non-symmetric and a splitting semiregular relative difference sets that share a forbidden subgroup give us another non-symmetric one. By a recursive construction applying Lemma 3.1 we obtain a class of non-symmetric semiregular relative difference sets (see Theorem 3.2 and Proposition 4.4).

2. Divisible designs and relative difference sets

Let $D$ be a relative difference set in a group $G$ relative to $U$. Then dev($D$) is a divisible design. However, the dual of dev($D$) is not always a divisible design. In this section we study a condition under which the dual of dev($D$) is a divisible design when $D$ is semiregular.

**Definition 2.1** An incidence structure $(P, B)$ is called a square $(m, u, k, \lambda)$-divisible design if the following conditions are satisfied.

(i) $|P| = |B| = mu$.

(ii) There exists a partition $P = P_1 \cup P_2 \cup \cdots \cup P_m$ of $P$ such that $|P_1| = \cdots = |P_m| = u$ and for any distinct points $p, q \in P$ the number of blocks $B \in B$ containing $p$ and $q$ is $0$ if $p, q \in P_i$ for some $i \in \{1, \ldots, m\}$ and $\lambda$ otherwise. (Each $P_i$ is called a point class of $(P, B)$.)

(iii) $|B| = k (\forall B \in B)$.

Counting all triples $(p, q, B)$ $(p, q \in B, p \neq q \in P, B \in B)$ in two ways we obtain the following fundamental equation.
429

\[ k(k - 1) = \lambda (mu - u) \]  \hspace{1cm} (2)

**Definition 2.2**  
(i) A square \((m, u, k, \lambda)\)-divisible design is said to be symmetric if its dual is also a square \((m, u, k, \lambda)\)-divisible design. In other words, there is a partition \(B = B_1 \cup \cdots \cup B_m\) of \(B\) such that for any two distinct blocks \(B, C\) \(\exists i \in \{1, \ldots, m\}\) such that \(B \cap C = \{0 \text{ if } B, C \in B_i \text{ for some } i \}, \lambda \text{ otherwise.}

(ii) A \((m, u, k, \lambda)\)-difference set \(D\) is said to be symmetric if \(D^{(-1)}\) is also a \((m, u, k, \lambda)\)-difference set.

**Remark 2.3**  
(i) In Theorem 6.2 of [3], W.S. Connor showed that \((P, B)\) is symmetric whenever \(k > u\lambda\) and \((k, \lambda) = 1\).

(ii) If a \((m, u, k, \lambda)\)-difference set \(D\) in a group \(G\) relative to \(U\) satisfies \(DD^{(-1)} = D^{(-1)}D\), then dev\((D)\) is symmetric.

(iii) By Jungnickel’s result in [7], \(DD^{(-1)} = D^{(-1)}D\) whenever \(G \supseteq U\). Hence, if \(G \supset U\), then \(D\) is symmetric.

**Definition 2.4** A square \((m, u, k, \lambda)\)-divisible design \((P, B)\) is called a transversal design and denoted by TD\(_{\lambda}\)\([k; u]\) if \(j\{\cdot\}\) for any \(B \in B\) and any point class \(P_i\) of \((P, B)\).

Hence, a square \((m, u, k, \lambda)\)-divisible design is a transversal design if and only if \(k = m\) \((= u\lambda)\).

**Lemma 2.5** Let \(D\) be a transversal design TD\(_{\lambda}\)\([u\lambda; u]\). If the dual of \(D\) is a \((m, n, k, \mu)\)-divisible design for some \(m, n, k, \mu \in \mathbb{N}\), then \((m, n, k, \mu) = (u\lambda, u, u\lambda, \lambda)\) and \(D\) is symmetric.

**Proof.** Clearly \(mn = u^2\lambda\), \(k = u\lambda\). By Theorem 3 of [2], \(k \geq n\mu\). Hence

\[ u\lambda \geq n\mu \]  \hspace{1cm} (3)

By (2), \(u\lambda(u\lambda - 1) = k(k - 1) = \mu(u^2\lambda - n) = u\lambda(u\mu) - \mu n\). From this \(\mu n \equiv 0 \pmod{u\lambda}\). Applying (3), we have \(u\lambda = n\mu\) and so \((n\mu)(n\mu - 1) = \mu(mn - n) = n\mu(m - 1)\). It follows that \(m = n\mu\). As \(n^2\mu = mn = u^2\lambda\), we have \(n = u\) and so \(\lambda = \mu\). Therefore the lemma holds.

A \((m, u, k, \lambda)\)-difference set is called semiregular if \(m = k\) \((\text{or equivalently } m = k = u\lambda)\). Then, clearly \(|G| = u^2\lambda\). In this case dev\((D)\) is a
transversal design $\text{TD}_\lambda[u\lambda;u]$.

As an application of Lemma 2.5, we can show the following.

**Proposition 2.6** Let $D$ be a semiregular relative difference set in a group $G$ relative to a subgroup $U$ of $G$. Then the following conditions are equivalent.

(i) $\text{dev}(D)$ is symmetric.
(ii) $D^{(-1)}$ is a relative difference set in $G$ relative to a subgroup of $G$.
(iii) The dual of $\text{dev}(D)$ is a divisible design.

**Proof.** Set $(\mathbb{P}, \mathbb{B}) = \text{dev}(D)$ and assume (i). Then, there exists a partition $\mathbb{B} = \mathbb{B}_1 \cup \cdots \cup \mathbb{B}_{u\lambda}$ of $\mathbb{B}$ such that for any two distinct blocks $B, C \in \mathbb{B}$,

$$|B \cap C| = \begin{cases} 0 & \text{if } B, C \in \mathbb{B}_i \text{ for some } i \in \{1, \ldots, u\lambda\}, \\ \lambda & \text{otherwise}. \end{cases} \quad (4)$$

Set $\mathbb{B}_1 = \{Dg_1, Dg_2, \ldots, Dg_u\}$, where $g_1 = 1$. As $Dg_i \cap Dg_j = \emptyset$ for any distinct $i, j \in \{1, 2, \ldots, u\}$, for each $\mathbb{B}_k$ there is an element $g \in G$ so that $\mathbb{B}_k = \{Dg_1 g, Dg_2 g, \ldots, Dg_u g\}$.

We note that

$$Dg_i \cap Dg_j = \emptyset \iff \{(d_1, d_2) \mid d_1, d_2 \in D, d_1 g_i = d_2 g_j\} = \emptyset.$$ 

Hence

$$Dg_i \cap Dg_j = \emptyset \iff \{(d_1, d_2) \mid d_1, d_2 \in D, d_1^{-1} d_2 = g_i g_j^{-1}\} = \emptyset. \quad (5)$$

Set $V = \{g_1(=1), g_2, \ldots, g_u\}$. Let $g_i, g_j \in V$. Then, by (5), $Dg_i g_j^{-1} \cap D = \emptyset$. Hence $Dg_i g_j^{-1} \in \mathbb{B}_1$ and so $g_i g_j^{-1} \in V$. Thus $V$ is a subgroup of $G$ of order $u$. Assume $a \in G \setminus V$. Then $Da \notin \mathbb{B}_1$. As $D \in \mathbb{B}_1$, we have $|D \cap Da| = \lambda$ by (4). Then $|\{(d_1, d_2) \mid a = d_1^{-1} d_2\}| = \lambda$. Thus $D^{(-1)} D = u\lambda + \lambda(G - V)$. Therefore (ii) holds. Clearly (ii) implies (iii). By Lemma 2.5, (iii) implies (i). \hfill $\Box$

As a corollary of Proposition 2.6, we have

**Corollary 2.7** A semiregular relative difference set $D$ is symmetric if and only if the dual of $\text{dev}(D)$ is a divisible design.

Under the above assumption, $DD^{(-1)} \neq D^{(-1)} D$ in general. To our knowledge, transversal designs obtained from semiregular relative difference sets and previously known were symmetric. In Section 3 and 4 we
will give examples of semiregular relative difference sets $D$ with $\text{dev}(D)$ non-symmetric. Then they give us examples of non-symmetric semiregular relative difference sets.

Concerning the case $m > k$ we would like to ask the following.

**Question 2.8** Let $D$ be a $(m, u, k, \lambda)$-difference set in a group $G$ such that $m > k$. Is $D$ symmetric whenever the dual of $\text{dev}(D)$ is a divisible design?

### 3. Non-symmetric relative difference sets

In this section we construct non-symmetric relative difference sets. To do this we need the following lemma.

**Lemma 3.1** Let $X = G \times H$ be a group, where $G$ is a group of order $u^2\lambda$ and $H$ is a group of order $u\lambda'$. Let $D$ be a $(u\lambda, u, u\lambda, \lambda)$-difference set in $G$ relative to a subgroup $U$ of $G$ of order $u$ and let $C$ be a $(u\lambda', u, u\lambda', \lambda')$-difference set in $G' = U \times H$ relative to $U$. Then

(i) $CD$ is a $(u^2\lambda\lambda', u, u^2\lambda\lambda', u\lambda\lambda')$-difference set in $X$ relative to $U$.

(ii) $CD$ is symmetric if and only if $D$ is symmetric.

**Proof.** Let $c_1, c_2 \in C$ and $d_1, d_2 \in D$ and assume $c_1d_1 = c_2d_2$. Then $c_1^{-1}c_2 = d_1d_2^{-1} \in UH \cap G = U$. Thus $d_1 = d_2$ and so $c_1 = c_2$. Therefore $CD$ is a subset of $X$.

Let $S$ and $T$ be subsets of $G$ and $H$, respectively. We identify $S$ and $T$ with $S \times \{1\} \subset X$ and $\{1\} \times T \subset X$, respectively. Then, by assumption, the following hold.

\[
DD^{(-1)} = u\lambda + \lambda(G - U) \quad (6)
\]
\[
CC^{(-1)} = u\lambda' + \lambda'(UH - U) \quad (7)
\]
\[
G = UD, \quad UC = UH \quad (8)
\]

Hence, substituting (6) and (7) we have

\[
(CD)(CD)^{(-1)} = C(DD^{(-1)})C^{(-1)}
\]
\[
= C(u\lambda + \lambda(G - U))C^{(-1)}
\]
\[
= u\lambda CC^{(-1)} + \lambda CGC^{(-1)} - \lambda CUC^{(-1)}.
\]

As $C, U \subset UH$ and $U < UH$, we have $CU = UC$. Similarly $GC = CG$. It
follows that
\[
(CD)(CD)^{-1} = u\lambda(u' + \lambda' (UH - U)) + \lambda G C^{-1} - \lambda U C^{-1}
\]
\[
= u^2\lambda' + u\lambda'UH - u\lambda'U
\]
\[
+ \lambda G(u' + \lambda'UH - \lambda'U) - \lambda U(u' + \lambda'UH - \lambda'U)
\]
\[
= u^2\lambda' + u\lambda'X - u\lambda'G.
\]
Thus we have (i).

Since $UH \triangleright U$, we obtain $C^{-1}C = CC^{-1} = u\lambda' + \lambda' UH - \lambda' U$. Hence
\[
(CD)^{-1}CD = D^{-1}(CC^{-1})D = D^{-1}(u\lambda' + \lambda' UH - \lambda' U)D.
\]
By (8), we have
\[
(CD)^{-1}CD = u\lambda' D^{-1}D + u\lambda'X - u\lambda'G.
\]
(9)
Assume $CD$ is symmetric. Then
\[
(CD)^{-1}CD = u^2\lambda' + u\lambda'X - V
\]
for a subgroup $V$ of $X$ of order $u$. By (9), $u\lambda' D^{-1}D - u\lambda'X = u^2\lambda' - u\lambda'X$. Thus $D^{-1}D = u\lambda + \lambda(G - V)$. In particular, $V$ is a subgroup of $G$ of order $u$ and so $D$ is symmetric. Conversely, assume $D$ is symmetric. Then $D^{-1}D = u\lambda + \lambda(G - V)$ for a subgroup $V$ of $G$ of order $u$. Then, by (9), $CD^{-1}CD = u\lambda'(u\lambda + \lambda(G - V)) + u\lambda'X - u\lambda'G = u^2\lambda' + u\lambda'X - V$. Therefore $CD$ is symmetric. Thus we have (ii).

We note that Lemma 3.1(i) is a modification of Result 2.4 of [8], where $N$ is assumed to be normal in $G$.

We now prove the following theorem on a recursive construction of non-symmetric semiregular relative difference sets.

**Theorem 3.2** Let $D$ be a $(u\lambda_0, u, \lambda_0, u\lambda)$-difference set in a group $G$ relative to a subgroup $U$ of $G$. Let $H_i$ be a group of order $u\lambda_i$ and assume the existence of a splitting $(u\lambda_i, u, u\lambda_i, \lambda_i)$-difference set, say $D_i$, in $U \times H_i$ relative to $U \times 1$ for each $i \in \{1, 2, \ldots, n-1\}$. Set $\lambda = \lambda_0 \lambda_1 \lambda_2 \cdots \lambda_{n-1}$. Then,

(i) $D_1D_2 \cdots D_{n-1}D$ is a $(u^n\lambda, u, u^n\lambda, u^{n-1}\lambda)$-difference set in $G \times H_{n-1} \times H_{n-2} \times \cdots \times H_1$ relative to $U \times 1 \times \cdots \times 1$.

(ii) $D_1D_2 \cdots D_{n-1}D$ is non-symmetric if and only if $D$ is non-symmetric.

**Proof.** Set $X = G \times H_{n-1}$. Since $U \times H_{n-1}$ contains a $(u\lambda_{n-1}, u, u\lambda_{n-1}, \lambda_{n-1})$-difference set $D_{n-1}$ relative to $U \times 1$, applying Lemma 3.1 we have that $D_{n-1}D$ is a $(u^2\lambda, u, u^2\lambda, \lambda_{n-1})$-difference set in $X$ relative to $U \times 1$. 

Set $X' = (G \times H_{n-1}) \times H_{n-2}$ and let $\psi$ be the natural projection from $U \times H_{n-2}$ to $X'$. Then we can regard $D_{n-2}$ as a $(u\lambda_{n-2}, u, u\lambda_{n-2}, \lambda_{n-2})$-difference set relative to $(U \times 1) \times 1$. Applying Lemma 3.1 again, we obtain a $(u^3\lambda\lambda_{n-1}\lambda_{n-2}, u, u^2\lambda\lambda_{n-1}\lambda_{n-2})$-difference set $C_{n-2}C_{n-1}D$ in $X'$ relative to $U \times 1 \times 1$. Repeating the procedure we have the theorem. 

4. Examples of non-symmetric relative difference sets

We denote by $m^*$ the square free part of a positive integer $m$.

Proposition 4.1 Assume the existence of a splitting $(3\lambda, 3, 3\lambda, \lambda)$-difference set. Then

(i) $p \equiv 1 \pmod{3}$ for each prime divisor $p \neq 3$ of $\lambda^*$.

(ii) The congruence $x^2 \equiv -12 \pmod{4\lambda^*}$ has a solution in integers.

Proof. Let $D$ be a $(3\lambda, 3, 3\lambda, \lambda)$-difference set in a group $G = H \times U$ relative to $U \simeq \mathbb{Z}_3$. Let $\chi$ be a linear character of $G$ such that $\chi|_H$ is principal, while $\chi|_U$ is not. Then, as $U \simeq \mathbb{Z}_3$, $\chi(D) = a + b\omega + c\omega^2$, $a + b + c = |D| = 3\lambda$ for non-negative integers $a, b, c$. Hence $\chi(D)\overline{\chi(D)} = a^2 + b^2 + c^2 - ab - bc - ca$. On the other hand, $\chi(D)\overline{\chi(D)} = 3\lambda$ by (1). From this, $(2a + b - 3\lambda)^2 + 3(b - \lambda)^2 = 4\lambda$. Thus an equation $x^2 + 3y^2 = 4\lambda$ has an integral solution $(x, y) = (2a + b - 3\lambda, b - \lambda)$. In particular, $2 \nmid \lambda^*$. By Theorem 7 in Section 7.6 of Chapter 2 in [1], the congruence $x^2 \equiv -12 \pmod{4\lambda^*}$ is solvable.

Let $p \neq 3$ be an odd prime dividing $\lambda^*$. Assume $p \equiv 2 \pmod{3}$. Then, by Theorem 2 in Section 2.2 of Chapter 5 in [1], $(p)$ is a prime ideal in the ring of algebraic integers in $\mathbb{Q}(\omega)$. This is contrary to the fact that $\chi(D)\overline{\chi(D)} = 3\lambda$. Thus $p \equiv 1 \pmod{3}$. Therefore the proposition holds.

Example 4.2 By Proposition 4.1, there are no splitting $(3\lambda, 3, 3\lambda, \lambda)$-difference sets for $\lambda = 2, 5, 6, 8, 10, 11$. On the other hand, here exist splitting a $(3\lambda, 3, 3\lambda, \lambda)$-difference set for $\lambda = 1, 3, 4, 7, 9$ (for $\lambda = 7$, see [9]). Also there exists a splitting $(3 \cdot 2^{2s}3^t, 3, 3 \cdot 2^{2s}3^t, 2^{2s}3^t)$-difference set for any $s, t \geq 0$ by Corollary 4.4 of [5].

We now show that a relative difference set in $G = S_3 \times \mathbb{Z}_6$ constructed in [6] is non-symmetric.
Example 4.3 Let $G = \langle a, b, c \mid a^3 = b^2 = e^6 = 1, b^{-1}ab = a^{-1}, ac = ca, bc = cb \rangle$ and set $D = \{1, c, c^2, c^3, a, ac, ab, a^2bc^5, abc, a^2bc, bc^4, abc\}$. Then $D$ is a $(12, 3, 12, 4)$-difference set relative to $U = \langle ac^2 \rangle \simeq Z_3$. We can easily check that $DD^{(-1)} = 12 + 4(G - U)$, while $D^{(-1)}D = 12 + 4a + 4a^2 + 4b + 4ab + 4a^2b + 4c + 3ac + 5a^2c + 3bc + 5abc + 4a^2bc + 4c^2 + 2ac^2 + 2a^2c^3 + 4bc^2 + 4abc^2 + 4a^2bc^2 + 4c^3 + 4ac^3 + 4a^2c^3 + 6bc^3 + 2abc^3 + 4a^2bc^3 + 4c^4 + 2ac^4 + 2a^2c^4 + 4bc^3 + 4ab^2c^4 + 4c^5 + 5ac^5 + 3a^2c^5 + 3bc^5 + 5abc^5 + 4a^2bc^5$. Thus $D^{(-1)}$ is not a relative difference set. Thus $D$ is a non-symmetric relative difference set.

By Theorem 3.2 and Examples 4.2 and 4.3 we have the following.

Proposition 4.4 There exists a non-symmetric $(2^{2m+1})$, $(3, 2^{2m-1})$, $(2^{2m} \lambda)$-difference set $D$ for any $\lambda = 2^{2m}3^{m1}7^{m2}$, $m \geq m_1 + m_2$ and $s, t \ (m_1, m_2, s, t \in \mathbb{N} \cup \{0\})$. Under this condition, $\text{dev}(D)$ is a non-symmetric $TD_{2^{2m} \lambda}[2^{2m+1} \lambda; 3]$.  

Example 4.5 Let $G = \langle a, b \rangle \times \langle c \rangle \simeq S_3 \times Z_6$, where $a^3 = b^2 = 1$, $bab = a^{-1}$ and let $H = \langle d \rangle \times \langle e \rangle \simeq Z_2 \times Z_6$. Set $X = G \times H$. Then one can verify that $C = \{1, c, c^2, c^3, ac^2e^4, ac^2e^5, a^2c^4d, de, ac^2de^2, a^2c^4de^3, ac^2de^4, de^5\}$ is a $(12, 3, 12, 4)$-difference set in $(a^2c^4d) \times \langle e \rangle \simeq Z_2 \times Z_6$ relative to $(ac^2) \simeq Z_3$. By Example 4.3, $D = \{1, c, c^2, c^3, a, ac, b, a^2bc^5, abc, a^2bc, bc^4, abc\}$ is a non-symmetric $(12, 3, 12, 4)$-difference set in $G$ relative to $(ac^2) \simeq Z_3$. Applying Lemma 3.1, $CD$ is a non-symmetric $(144, 3, 144, 48)$-difference set.

References


[9] Akiyama K. and Suetake C., On \(STD_{k/3}[k;3]\)'s. preprint.

Department of Mathematics
Faculty of Education
Kumamoto University
Kurokami, Kumamoto, Japan
E-mail: hiramine@gpo.kumamoto-u.ac.jp