COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 12 (4) (1992) 425–432

REVERSIBLE RELATIVE DIFFERENCE SETS

S. L. MA

Received October 24, 1989

We investigate nontrivial (m,n,k,λ)-relative difference sets fixed by the inverse. Examples and necessary conditions on the existence of relative difference sets of this type are studied.

1. Introduction

Let G be a finite group of order mn with a subgroup N of order n. A k-element subset D of G is called an (m,n,k,λ)-*relative difference set* (or, in short, an (m,n,k,λ)-RDS) in G relative to N if the expressions $d_1 d_2^{-1}$, for d_1 and d_2 in D with $d_1 \neq d_2$, represent each element in $G \setminus N$ exactly λ times and represent no nonidentity element in N. The concept of relative difference sets was introduced by Butson [3], [4] and Elliott and Butson [6] as a generalization of difference sets. (For detailed descriptions of difference sets, please consult [2], [8].)

For a subset S of G, we define $S^{(t)} = \{g^t | g \in S\}$. In this paper, we are going to study a particular type of relative difference sets which are fixed by the inverse, i.e. $D^{(-1)} = D$.

In the following, we assume that G is an abelian group of order mn and N is a subgroup in G of order n such that $m>1$ and $n>1$. For any subset S of G, S is called *reversible* if $S^{(-1)} = S$; and S is called *nontrivial* if $|S| \neq 0, 1, mn-1$ and mn.

Firstly, let us summarize the known results on reversible relative difference sets (see [1, Section 6]).

Proposition 1.1. *Let D be a nontrivial reversible (m,n,k,λ)-RDS in G relative to N. Then*

(i) $m = k = \lambda n$ *is a square and* λ *is even;*

(ii) $|D \cap gN| = 1$ *for all* $g \in G$*;*

(iii) $D^{(t)} = D$ *for all* t *relatively prime to the order of* G*;*

(iv) *if* H *is a proper subgroup in* N *of order* s *and* $\varrho : G \to G/N$ *is a natural epimorphism, then* ϱD *is a nontrivial reversible* $(\lambda n, n/s, \lambda n, \lambda s)$*-RDS in* G/H *relative to* N/H.

AMS subject classification code (1991): 05 B 10

By Proposition 1.1(ii), we learn that $|D \cap N| = 1$, say, $D \cap N = \{h\}$ for some $h \in N$. Since $D^{(-1)} = D$, we have $h^2 = 1$. Hence $D' = hD$ is a reversible relative difference set with $D' \cap N = \{1\}$. Let $E_1 = N \setminus \{1\}$, $E_2 = D' \setminus \{1\}$ and $E_3 = G \setminus (N \cup D')$. It is easy to verify that $\{1, E_1, E_2, E_3\}$ spans a Schur ring over G and hence can be used to construct an association scheme of class 3 (see [10]). This is one of the reasons why we are interested in reversible relative difference sets.

In Section 2, we shall see some examples of reversible relative difference sets. In Section 3, we shall show that there are some severe restrictions on the existence of nontrivial reversible relative difference sets. In particular, N must be a direct factor of G and n, the order of N, is a power of 2. Furthermore, if $n = 2$, every nontrivial reversible relative difference set is constructed by using a $(4u^2, 2u^2 \pm u, u^2 \pm u)$-difference set where $m = 4u^2$. Finally, in Section 4, some open problems are posed.

2. Examples

There are two known families of reversible relative difference sets.

Example 2.1. (Arasu, Jungnickel and Pott [1, Corollary 2.11]) If there exists a reversible $(4u^2, 2u^2 \pm u, u^2 \pm u)$-difference set C in a group K. Then

$$D = (\{0\} \times C) \cup (\{1\} \times (G \setminus C))$$

is a reversible $(4u^2, 2, 4u^2, 2u^2)$-RDS in $G = \mathbb{Z}_2 \times K$ relative to $\mathbb{Z}_2 \times \{1\}$.

With the constructions of reversible $(4u^2, 2u^2 \pm u, u^2 \pm u^2)$-difference sets given by Menon [12], Turyn [14], Dillon [5] and Leung and Ma [9], we have a large family of reversible $(4u^2, 2, 4u^2, 2u^2)$-RDS for $u = 2^s 3^t$ where s, t are nonnegative integers.

For the second example, we need a finite local ring. Let R be a finite local ring of characteristic 2 with its maximal ideal I generated by a prime element π. Suppose $R/I \cong \mathbb{F}_{2^d}$, a finite field of 2^d elements, and s is the smallest positive integer such that $I^s = (\pi^s) = (0)$.

Example 2.2. (Leung and Ma [9, Corollary 4.2]) Let $\{A_1, A_2, \ldots, A_{2^t}\}$ be a partition of R such that, for any coset $a + I^{s-1}$ in R and $i = 1, 2, \ldots, 2^t$, we have $|A_i \cap a + I^{s-1}| = 2^{d-t}$ where t is a positive integer less than or equal to d. Define $\varphi : R \to R$ be a mapping such that $\varphi(\pi^r u) = \pi^r u^{-1}$ for any $r = 0, 1, \ldots, s-1$ and unit u in R. Let $H = \{g_1, g_2, \ldots, g_{2^t}\}$ be an elementary 2-group with 2^t elements. Then

$$D = \bigcup_{i=1}^{2^t} (\{g_i\} \times \{(a, b) \in R \times R \mid \varphi(a)b \in A_i\})$$

is a reversible $(2^{2sd}, 2^t, 2^{2sd}, 2^{2sd-t})$-RDS in $H \times R \times R$ relative to $H \times \{0\} \times \{0\}$.*

Example 2.2 gives us a family of reversible relative difference sets with $n = 2^t$ for all t.

* For the case $s = 1$, we have to modify the construction: Use $R \cong F_{2^d}$, replace I^{s-1} by R and define $\varphi(a) = a^{-1}$ for all unit a and $\varphi(0) = 0$.

3. Necessary Conditions

In this section, we study the necessary conditions of the existence of relative difference sets. The readers are reminded that G is an abelian group of order $mn(=\lambda n^2)$ and N is a subgroup in G of order n where $n>1$.

Firstly, let us investigate the relation between G and N.

Theorem 3.1. *If a nontrivial reversible relative difference set exists in G relative to N, then N is a direct factor of G.*

Proof. Let p be any prime divisor of $|N|$ and P be the Sylow p-subgroup of G. It suffices to show that $P\cap N$ is a direct factor of P. By Proposition 1.1(iv), we can assume that $P\cap N=N$. Now, we are going to show that N is a pure subgroup of P and hence, by [7, Theorem 13.41], N is a direct factor of P.

Suppose g is any element in P with $g^{p^\alpha}\in N$ for an integer α. Let $gh\in D\cap gN$ where $h\in N$. Recall that $D^{(t)}=D$ for all t relatively prime to $|G|$. Let $|G|=p^s u$ where $p^s=|P|$ and $p\nmid u$. For $t\equiv p^\alpha+1 \pmod{p^s}$ and $t\equiv 1 \pmod{u}$, $D^{(t)}=D$ implies $g^{p^\alpha+1}h^{p^\alpha+1}\in D\cap gN$. By Proposition 1.1(ii), we have $gh=g^{p^\alpha+1}h^{p^\alpha+1}$. This implies $g^{p^\alpha}=h^{-p^\alpha}$. Hence N is a pure subgroup of P. ∎

In the following, we shall make use of the group ring $\mathcal{R}[G]$ where $\mathcal{R}=\mathbb{Z}$ or $\mathbb{C}$. For any subset S of G, we define $\overline{S}=\sum_{g\in G} g\in\mathcal{R}[G]$. For $y=\sum_{g\in G} a_g g\in\mathcal{R}[G]$, we define $y^{(t)}=\sum_{g\in G} a_g g^t$ where t is any integer. Also, for a group homomorphism $\sigma: G\to H$, we extend σ to a ring homomorphism from $\mathcal{R}[G]$ to $\mathcal{R}[H]$ such that $\sigma\left(\sum_{g\in G} a_g g\right)=\sum_{g\in G} a_g\sigma g$.

Using the language of the group ring, if D is a reversible $(\lambda n, n, \lambda n, \lambda)$-RDS in G relative to N, then

$$\overline{D}^2=\lambda\overline{G}-\lambda\overline{N}+\lambda n. \tag{3.1}$$

Theorem 3.2. *Suppose there exists a nontrivial reversible $(\lambda n, n, \lambda n, \lambda)$-RDS in G relative to N and p is a prime divisor of the order of G. Since λn is a square, we can write $n=p^r n_0$ and $\lambda=p^{2s-r}\lambda_0$ where $p\nmid\lambda_0$ and $p\nmid n_0$. Then*

(i) *$p^s\equiv\pm 1 \pmod{n_0}$;*

(ii) *if G_0 is the subgroup in G of order $\lambda_0 n_0^2$ and N_0 is the subgroup in N of order n_0, then there exists a reversible $(\lambda_0 n_0, n_0, \lambda_0 n_0, \lambda_0)$-RDS in G_0 relative to N_0.*

To prove Theorem 3.2, we need two lemmas.

Lemma 3.3. The Fourier Inversion Formula. (see [13, Section 6.2]) *Let $y=\sum_{g\in G} a_g g\in \mathbb{C}[G]$ and G^* be the group of characters of G. Then*

$$a_g=\frac{1}{|G|}\sum_{\chi\in G^*}\chi y\chi g^{-1}.$$

Lemma 3.4. *Let a,b,c,r be nonnegative integers with $a=br+c$ and $0\le c\le r-1$. Then the minimum value of $\sum_{i=1}^{r} X_i^2$, subject to the constraints that $\sum_{i=1}^{r} X_i = a$ and $X_1,\dots,X_r$ are nonnegative integers, is $b^2(r-c)+(b+1)^2c$ with $X_i=b$ or $b+1$ for all i. Note that $|\{X_i\,|\,X_i=b+1\}|=c$ and $|\{X_i\,|\,X_i=b\}|=r-c$.*

Proof. It suffices to show that the minimum occurs when $X_i=b$ or $b+1$ for all i. Suppose $X_j<b$ for some j. Since $\sum_{i=1}^{r} X_i = a = br+c$ with $0\le c\le r-1$, there exists some $X_k\ge b+1$. Define $X'_i=X_i$, for $i\ne j$, k, $X'_i=X_j+1$ and $X'_k=X_k-1$. Then $\sum_{i=1}^{r} X_i'^2=\sum_{i=1}^{r} X_i^2+2(X_j-X_k+1)<\sum_{i=1}^{r} X_i^2$ which shows that $\sum_{i=1}^{r} X_i^2$ is not the minimum.

On the other hand, if $X_i>b+1$ for some j, then we can find some $X_k\le b$. With $X''_i=X_i$, for $i\ne j$, k, $X''_j=X_j-1$ and $X''_k=X_k+1$, we can also get the inequality $\sum_{i=1}^{r} X_i''^2<\sum_{i=1}^{r} X_i^2$. ∎

Proof of Theorem 3.2. Let $\varrho: G\to G_0$ be the natural projection. By (3.1), we have

$$\varrho\overline{D}^2=p^{4s}\lambda_0\overline{G}_0-p^{2s}\lambda_0\overline{N}_0+p^{2s}\lambda_0 n_0. \tag{3.2}$$

For any character χ of G_0, $\chi(\varrho\overline{D})=\pm p^s\sqrt{\lambda_0 n_0}$, 0 or $p^{2s}\lambda_0 n_0$ and hence $\chi(\varrho\overline{D})\equiv 0 \pmod{p^s}$. By Lemma 3.3,we have $\varrho\overline{D}=p^s z$ for some $z\in\mathbb{Z}[G_0]$. By (3.2), we get

$$z^2=p^{2s}\lambda_0\overline{G}_0-\lambda_0\overline{N}_0+\lambda_0 n_0. \tag{3.3}$$

Let $z=\sum_{g\in G_0} a_g g$. It is obvious that

$$\begin{cases}\displaystyle\sum_{g\in G_0} a_g = p^s\lambda_0 n_0\\ \displaystyle\sum_{g\in G_0} a_g^2 = p^{2s}\lambda_0-\lambda_0+\lambda_0 n_0.\end{cases}$$

Let $p^s=\alpha n_0+\beta$ where $1\le\beta\le n_0-1$. By Lemma 3.4, the minimum value of $\sum X_g^2$ with $\sum X_g=p^s\lambda_0 n_0$ is equal to $\alpha^2(\lambda_0 n_0^2-\beta\lambda_0 n_0)+(\alpha+1)^2\beta\lambda_0 n_0$ with $X_g=\alpha$ or $\alpha+1$ for all $g\in G_0$. Hence

$$\alpha^2(\lambda_0 n_0^2-\beta\lambda_0 n_0)+(\alpha+1)^2\beta\lambda_0 n_0\le(\alpha n_0+\beta)^2\lambda_0-\lambda_0+\lambda_0 n_0 \tag{3.4}$$

which implies $\beta^2-\beta n_0+n_0-1\ge 0$. The only possible solutions are $\beta=1$ or $\beta=n_0-1$. But both cases give us an equality of (3.4). Thus we conclude that $a_g=\alpha$ or $\alpha+1$ for all $g\in G_0$. Let us write $z=\alpha\overline{D}_0+(\alpha+1)\overline{D}_1$ where $\{D_0,D_1\}$ is a partition of G_0. Note that $|D_0|=\lambda_0 n_0^2-\beta\lambda_0 n_0$, $|D_1|=\beta\lambda_0 n_0$ and $\overline{D}_0+\overline{D}_1=\overline{G}_0$.

If $\beta=1$, by substituting $z=\alpha\overline{G}_0+\overline{D}_1$ to (3.3), we obtain

$$(\alpha^2|G_0|+2\alpha|D_1|)\overline{G}_0+\overline{D}_1^2=p^{2s}\lambda_0\overline{G}_0-\lambda_0\overline{N}_0+\lambda_0 n_0.$$

With $\alpha=(p^{2s}-1)/n_0$, $|G_0|=\lambda_0 n_0^2$ and $|D_1|=\lambda_0 n_0$, we have

$$\overline{D}_1^2 = \lambda_0\overline{G}_0 - \lambda_0\overline{N}_0 + \lambda_0 n_0.$$

Hence D_1 is a reversible $(\lambda_0 n_0, n_0, \lambda_0 n_0, \lambda_0)$-RDS.

If $\beta=n_0-1$, by substituting $z=(\alpha+1)\overline{G}_0-\overline{D}_0$ to (3.3), we obtain

$$[(\alpha+1)^2|G_0| - 2(\alpha+1)|D_0|]\overline{G}_0 + \overline{D}_0^2 = p^{2s}\lambda_0\overline{G}_0 - \lambda_0\overline{N}_0 + \lambda_0 n_0.$$

With $\alpha+1=(p^{2s}+1)/n_0$, $|G_0|=\lambda_0 n_0^2$ and $|D_0|=\lambda_0 n_0$, we have

$$\overline{D}_0^2 = \lambda_0\overline{G}_0 - \lambda_0\overline{N}_0 + \lambda_0 n_0.$$

Hence D_0 is a reversible $(\lambda_0 n_0, n_0, \lambda_0 n_0, \lambda_0)$-RDS. ∎

Corollary 3.5. *If a nontrivial reversible $(\lambda n, n, \lambda n, \lambda)$-RDS exists in an abelian group, then n is a power of 2.*

Proof. Suppose n is not a power of 2. By applying Theorem 3.2 with $p=2$, we obtain a nontrivial reversible $(\lambda_0 n_0, n_0, \lambda_0 n_0, \lambda_0)$-RDS where both λ_0 and n_0 are odd. But this contradicts Proposition 1.1(i). ∎

The next theorem gives us another constraint on the parameters.

Theorem 3.6. *If a $(\lambda n, n, \lambda n, \lambda)$-RDS exists in an abelian group, then $n\,|\,\lambda$.*

Proof. By Theorem 3.1, N is a direct factor of G. Thus, there exists a natural projection $\varrho: G\to N$. Let $n=2^r$. By (3.1),

$$\varrho\overline{D}^2 = (2^r\lambda^2 - \lambda)\overline{N} + 2^r\lambda$$

For $\chi\in N^*$, we have $\chi(\varrho\overline{D}) = \pm\sqrt{2^r\lambda}$ if χ is nonprincipal and $\chi(\varrho\overline{D}) = 2^r\lambda$ if χ is principal. By Lemma 3.3,

$$\text{the coefficient of the identity in } \varrho\overline{D} = \frac{1}{|N|}\sum_{\chi\in N^*}\chi(\varrho\overline{D})$$
$$= \frac{1}{2^r}(2^r\lambda + \sqrt{2^r\lambda}\sum_{\substack{\chi\in N^*\\ \chi\overline{N}=0}}\varepsilon_\chi)$$

where $\varepsilon_\chi=\chi(\varrho\overline{D})/\sqrt{2^r\lambda}=\pm1$. Since there are 2^r-1 nonprincipal characters, $\sum\varepsilon_\chi$ must be odd. Hence, $2^r\,|\,\sqrt{2^r\lambda}$ and $2^r\,|\,\lambda$. ∎

If λ is a power of 2, then we have a necessary and sufficient condition on the parameters.

Corollary 3.7. *There exists nontrivial reversible $(2^{2s}, 2^r, 2^{2s}, 2^{2s-r})$-RDS in some abelian 2-group if and only if $s\geq r$.*

Proof. The sufficient part follows by Example 2.2 and the necessary part is a particular case of Theorem 3.6. ∎

Finally, we characterize the structure of a nontrivial reversible relative difference set if $n=2$. By Theorem 3.1, we can write $G=H\times N$ where H is a subgroup of G.

Theorem 3.8. *Let D be a nontrivial reversible relative difference set in $G=H\times N$ relative to N. If $|N|=2$, say $N=\{1,g\}$, then $D=A\cup g(H\backslash A)$ where A is a reversible $(4u^2, 2u^2\pm u, u^2\pm u)$-difference set in H for some integer u.*

Proof. Put $D=A\cup gB$ where A, $B\subset H$. By (3.1), we have

$$(\overline{A}+g\overline{B})^2=\lambda(\overline{H}+g\overline{H})-\lambda(1+g)+2\lambda$$

which implies $\overline{A}^2+\overline{B}^2=\lambda\overline{H}+\lambda$ and $2\overline{A}\overline{B}=\lambda\overline{H}-\lambda$. For any nonprincipal character χ of H,

$$\begin{cases} \chi\overline{A}^2+\chi\overline{B}^2=\lambda \\ 2\chi\overline{A}\chi\overline{B}=-\lambda. \end{cases}$$

Hence $\chi\overline{A}=-\chi\overline{B}=\pm\frac{\sqrt{2\lambda}}{2}=\pm\sqrt{\frac{|H|}{4}}$. By Lemma 3.3, we have $\overline{B}=\mu\overline{H}-\overline{A}$ and $\overline{A}\overline{A}^{(-1)}=\overline{A}^2=\mu'\overline{H}+\frac{|H|}{4}$ for some integers μ and μ'. Since the coefficients of $\overline{B}$ are 0 and 1, it is obvious that $\mu=1$ and hence $B=H\backslash A$. Also, by [12], we learn that A must be a reversible $(4u^2, 2u^2\pm u, u^2\pm u)$-difference set in H. ∎

By Proposition 1.1(iv) and a nonexistence theorem of reversible $(4u^2, 2u^2\pm u, u^2\pm u)$-difference set by McFarland [11, Theorem 3.4], we have the following corollary.

Corollary 3.9. *If there exists a nontrivial reversible $(\lambda n, n, \lambda n, \lambda)$-RDS in an abelian group, then $\lambda n=4u^2$ where the square free part of u is equal to 2^s3^t for some nonnegative integers s and t.*

4. Open Problems

Summarizing the results in Section 3, every nontrivial reversible relative difference set in an abelian group has the parameters

$$(m,n,k,\lambda)=(2^{2s}u_0^2, 2^r, 2^{2s}u_0^2, 2^{2s-r}u_0^2)$$

where r, s are positive integers and u_0 is an odd integer such that

(i) $r\leq s$;

(ii) if p is a prime divisor of u_0 and $p^t\|u_0$, then $p^t\equiv\pm1 \pmod{2^r}$; and

(iii) the square free part of u_0 is equal to 3^w for some nonnegative integer w.

Together with the examples in Section 2, we have a list of parameters (m,n,k,λ) for the existence of nontrivial reversible relative difference sets with $4\leq k\leq 2500$:

m	n	k	λ	u_0	
4	2	4	2	1	Examples 2.1 and 2.2
16	2	16	8	1	Examples 2.1 and 2.2
16	4	16	4	1	Example 2.2
36	2	36	18	3	Example 2.1
64	2	64	32	1	Examples 2.1 and 2.2
64	4	64	16	1	Examples 2.1 and 2.2
64	8	64	8	1	Example 2.2
144	2	144	72	3	Example 2.1
144	4	144	36	3	unknown
256	2	256	128	1	Examples 2.1 and 2.2
256	4	256	64	1	Example 2.2
256	8	256	32	1	Example 2.2
256	16	256	16	1	Example 2.2
324	2	324	162	9	Example 2.1
576	2	576	288	3	Example 2.1
576	4	576	144	3	unknown
1024	2	1024	512	1	Examples 2.1 and 2.2
1024	4	1024	256	1	Example 2.2
1024	8	1024	128	1	Example 2.2
1024	16	1024	64	1	Example 2.2
1024	32	1024	32	1	Example 2.2
1296	2	1296	648	9	Example 2.1
1296	4	1296	324	9	unknown
2304	2	2304	1152	3	Example 2.1
2304	4	2304	576	3	unknown
2500	2	2500	1250	25	unknown

In order to answer the undecided cases in the list, we pose the following questions.

Question 4.1. If $u_0 \neq 1$, i.e. the group is not a 2-group, then is it possible to have $n > 2$?

Question 4.2. Is it possible to have a prime divisor p of u_0 with $p > 3$? In particular, is there any reversible $(4u^2, 2u^2 \pm u, u^2 \pm u)$-difference set when $u \neq 2^s 3^t$?

Finally, if one looks into the group structure, then he will find that, in all the known examples, N is an elementary 2-group. Thus, we want to ask the following.

Question 4.3. Must N be an elementary 2-group? In particular, is it possible to have N being a cyclic group of order 4?

References

[1] K. T. Arasu, D. Jungnickel and A. Pott: Divisible Difference Sets with Multiplier −1, *J. Algebra* **133** (1990), 35–62.

[2] T. Beth, D. Jungnickel and H. Lenz: *Design Theory*, Cambridge University Press, Cambridge, 1986.

[3] A. T. BUTSON: Generalized Hadamard Matrices, *Proc. Amer. Math. Soc.* **13** (1962), 894–898.

[4] A. T. BUTSON: Relations Among Generalized Hadamard Matrices, Relative Difference Sets, and Maximal Length Linear Recurring Sequences, *Can. J. Math.* **15** (1963), 42–48.

[5] J. F. DILLON: Difference Sets in 2-groups, *Proc. NSA Math. Sc. Meeting* (1987), 165–172.

[6] J. E. H. ELLIOTT and A. T. BUTSON: Relative Difference Sets, *Illinois J. Math.* **10** (1966), 517–531.

[7] M. HALL. JR.: *The Theory of Groups*, Chelsea Publishing Company, New York, 1976.

[8] E. S. LANDER: *Symmetric Designs: An Algebraic Approach*, Cambridge University Press, Cambridge 1983.

[9] K. H. LEUNG and S. L. MA: Constructions of Partial Difference Sets and Relative Difference Sets on p-groups, *Bull. London Math. Soc.* **22** (1990), 533–539.

[10] S. L. MA: On Association Schemes, Schur Rings, Strongly Regular Graphs and Partial Difference Sets, *Ars Combinatoria* **27** (1989), 211–220.

[11] R. L. MCFARLAND: Sub-Difference Sets of Hadamard Difference Sets, *J. Combin. Th. Ser. A.* **54** (1990), 112–122.

[12] P. K. MENON: On Difference Sets whose Parameters Satisfy a Certain Relation, *Proc. Amer. Math. Soc.* **13** (1962), 739–745.

[13] J-P. SERRE: *Linear Representations of Finite Groups*, Springer, New York, 1978.

[14] R. J. TURYN: A Special Class of Williamson Matrices and Difference Sets, *J. Combin. Th. Ser. A* **36** (1984), 111–115.

S. L. Ma

Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 0511
matmasl@nusvm.bitnet