JOURNAL OF COMBINATORIAL THEORY, Series A **76**, 179–196 (1996)
ARTICLE NO. 0100

Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings II

Yu Qing Chen, D. K. Ray-Chaudhuri, and Qing Xiang*,[1]

Department of Mathematics, Ohio State University, Columbus, Ohio 43210;
**Department of Mathematics, California Institute of Technology, Pasadena, California 91125*

Communicated by the Managing Editors

Received June 20, 1995

In a previous paper, [*Des., Codes and Cryptogr.* **8** (1996), 215–227]; we used Galois rings to construct partial difference sets, relative difference sets and a difference set. In the present paper, we first generalize and improve the construction of partial difference sets in [*Des., Codes and Cryptogr.* **8** (1996), 215–227]; also we obtain a family of relative difference sets from these partial difference sets. Second, we construct a class of relative difference sets in $(Z_4)^{2m+1} \oplus (Z_4)^r \oplus (Z_2 \oplus Z_2)^s$, $r+s=m$, $r, s \geqslant 0$ with respect to a subgroup $(Z_2)^{2m+1}$. These constructions make use of character sums from Galois rings, and relate relative difference sets to Hadamard difference sets.

1. INTRODUCTION

Let G be a finite group of order v. A k-element subset D of G is called a (v, k, λ, μ)-*partial difference set* (PDS) in G if the differences $d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$, represent each nonidentity element in D exactly λ times and each nonidentity element not contained in D exactly μ times. D is called abelian if G is abelian. It is well known that a PDS D with $e \notin D$ and $\{d^{-1} : d \in D\} = D$ is equivalent to a strongly regular Cayley graph, such a PDS is called regular. The study of partial difference sets is closely related to partial geometries, Schur rings, strongly regular Cayley graphs and two-weight codes. The recent survey of Ma [5] contains very detailed descriptions of these connections.

Assume that $v = mn$ and that G contains a normal subgroup N of order n. A k-element subset R 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 differences $d_1 d_2^{-1}$, $d_1, d_2 \in R$, $d_1 \neq d_2$, represent each element in $G \backslash N$ exactly λ times and each nonidentity element in N zero time. If $G = H \times N$, where H is

[1] E-mail: dijen@math.ohio-state.edu; xiang@cco.caltech.edu.

0097-3165/96 $18.00

some subgroup of G, then R is called a splitting RDS. We will focus on (p^a, p^b, p^a, p^{a-b})-relative difference sets in this paper, these relative difference sets have been studied extensively, we refer the reader to the recent survey of Pott [8] for a summary.

In a previous paper [7], we used Galois rings to construct partial difference sets, relative difference sets and a difference set. The main idea is as follows. Given a subgroup of the unit group of a Galois ring, we may view the orbits of the multiplication action of that subgroup on the Galois ring as analogues of cyclotomic classes of finite fields, hence they may be used to construct partial difference sets, relative difference sets, and difference sets. Instead of calculating cyclotomic numbers, we use additive characters of the Galois ring to show that the candidate subsets we come up with have the required "difference" property. Galois rings have attracted a great deal of attention recently because of their applications in coding theory [3]. In this paper, we first generalize and improve the construction of partial difference sets in [7]; also we obtain a family of relative difference sets from these partial difference sets. Second, we construct a class of non-splitting relative difference sets in $(Z_4)^{2m+1} \oplus (Z_4)^r \oplus (Z_2 \oplus Z_2)^s$, $r+s=m$, $r, s \geqslant 0$ with respect to a subgroup $(Z_2)^{2m+1}$.

The following well-known character theoretic characterizations of abelian partial difference sets and relative difference sets will be used in our constructions.

LEMMA A. *Let G be an abelian group of order v and D be a subset of G with $\{d^{-1}: d \in D\} = D$. Then D is a (v, k, λ, μ)-partial difference set in G if and only if, for any character χ of G,*

$$\sum_{d \in D} \chi(d) = \begin{cases} k & \text{if } \chi \text{ is principal on } G, \\ \dfrac{\beta \pm \sqrt{\beta^2 + 4\gamma}}{2} & \text{if } \chi \text{ is nonprincipal on } G, \end{cases}$$

where $\beta = \lambda - \mu$; $\gamma = k - \lambda$ if $e \in D$, and $\gamma = k - \mu$ if $e \notin D$.

LEMMA B. *Let G be an abelian group of order mn with a subgroup N of order n, and R be a k-element subset of G. Then R is an (m, n, k, λ)-relative difference set in G relative to N if and only if, for any character χ of G,*

$$\left| \sum_{r \in R} \chi(r) \right| = \begin{cases} k & \text{if } \chi \text{ is principal on } G, \\ \sqrt{k - \lambda n} & \text{if } \chi \text{ is nonprincipal on } G \text{ but principal on } N, \\ \sqrt{k} & \text{if } \chi \text{ is nonprincipal on } N. \end{cases}$$

2. GALOIS RINGS OVER Z/p^2Z

For every integer $t \geqslant 1$, let F_{p^t} denote the finite field of order p^t, where p is a prime. Let $\mu_1: Z/p^2Z \to Z/pZ = F_p$ be the modulo p reduction map. We can extend μ_1 to $Z/p^2Z[x]$ in the natural way. Let $\bar{\phi}(x)$ be a primitive polynomial of degree t over F_p and let $\Phi(x)$ be a preimage of $\bar{\phi}(x)$ under the homomorphism μ_1. There is a unique monic $\Phi(x)$ whose root g satisfies $g^{p^t-1} = 1$.

The ring $Z/p^2Z[g]$ is an algebraic extension of Z/p^2Z; it is the Galois extension of Z/p^2Z of degree t. This extension $Z/p^2Z[g]$ is called a Galois ring and is denoted by $\mathrm{GR}(p^2, t)$.

$\mathrm{GR}(p^2, t)$ is a finite local ring, it has the unique maximal ideal $B = \{0, p, pg, ..., pg^{q-2}\}$, where $q = p^t$, the residue class field $\mathrm{GR}(p^2, t)/B = K = \{\bar{0}, \bar{1}, \bar{g}, ..., \bar{g}^{q-2}\}$ is isomorphic to F_q. We can take the Teichmuller system $\mathscr{T} = \{0, 1, g, ..., g^{q-2}\}$ as a set of representatives of $\mathrm{GR}(p^2, t)/B$. Therefore an arbitrary element α of $\mathrm{GR}(p^2, t)$ is uniquely represented as $\alpha = \alpha_0 + p\alpha_1$, $\alpha_0, \alpha_1 \in \mathscr{T}$. We denote the set of invertible elements of $\mathrm{GR}(p^2, t)$ by $\mathrm{GR}(p^2, t)^* = \mathrm{GR}(p^2, t) \setminus B$. Every element of $\mathrm{GR}(p^2, t)^*$ has a unique representation in the form $g^i(1 + p\alpha)$, $0 \leqslant i \leqslant q-2$, $\alpha \in \mathscr{T}$. $\mathrm{GR}(p^2, t)^*$ is a multiplicative group of order $(p^t - 1)p^t$ which is a direct product $H \times \mathscr{U}$, where H is the cyclic group of order $p^t - 1$ generated by g, and $\mathscr{U}$ is the group of principal units of $\mathrm{GR}(p^2, t)$, that is, elements of the form $1 + p\alpha$, $\alpha \in \mathscr{T}$. $\mathscr{U}$ has the structure of an elementary abelian group of order p^t and is isomorphic to the additive group of K via the map $1 + p\alpha \mapsto \bar{\alpha}$, $\alpha \in \mathscr{T}$.

For the proof of the above assertions on the structure of $\mathrm{GR}(p^2, t)^*$ and more detailed description of Galois rings, we refer the reader to MacDonald [6].

For $\alpha \in K = \{\bar{0}, \bar{1}, \bar{g}, ..., \bar{g}^{q-2}\}$, we define the trace function from K to F_p by $\mathrm{tr}_{t,1}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{t-1}}$. Let s be a positive divisor of t. Then there is a unique subfield F_{p^s} of K with p^s elements, we denote the trace maps from K to F_{p^s} and from F_{p^s} to F_p by $\mathrm{tr}_{t,s}$ and $\mathrm{tr}_{s,1}$ respectively. By transitivity of trace, we have $\mathrm{tr}_{t,1} = \mathrm{tr}_{s,1} \circ \mathrm{tr}_{t,s}$. The additive characters of K can be easily described by the trace function.

LEMMA C. *All additive characters χ_y of K are given by*

$$\chi_y(x) = \xi_p^{\mathrm{tr}_{t,1}(xy)}, \qquad x \in K$$

where ξ_p is a primitive pth root of unity.

The Frobenius map f from $\mathrm{GR}(p^2, t)$ to $\mathrm{GR}(p^2, t)$ is the ring automorphism $f: \alpha_0 + p\alpha_1 \mapsto \alpha_0^p + p\alpha_1^p$, α_0, $\alpha_1 \in \mathscr{T}$. The Galois group of

$GR(p^2, t)$ over Z/p^2Z is a cyclic group of order t which is generated by f. The set of elements of $GR(p^2, t)$ invariant under f is identical with Z/p^2Z.

For $\alpha \in GR(p^2, t)$, we define the trace function from $GR(p^2, t)$ to Z/p^2Z by $T_{t,1}(\alpha) = \alpha + \alpha^f + \cdots + \alpha^{f^{t-1}}$. Let s be a positive divisor of t. Then there is a unique subring $GR(p^2, s)$ of $GR(p^2, t)$ with p^{2s} elements (see [6]). Let us denote the relative traces from $GR(p^2, t)$ to $GR(p^2, s)$ and from $GR(p^2, s)$ to $GR(p^2, 1) = Z/p^2Z$ by $T_{t,s}$ and $T_{s,1}$ respectively. It is easy to check that $T_{t,1} = T_{t,s} \circ T_{s,1}$ and the diagram

$$\begin{array}{ccc} GR(p^2, t) & \xrightarrow{\mu_t} & K = F_{p^t} \\ \downarrow{\scriptstyle T_{t,s}} & & \downarrow{\scriptstyle \mathrm{tr}_{t,s}} \\ GR(p^2, s) & \xrightarrow{\mu_s} & F_{p^s} \\ \downarrow{\scriptstyle T_{s,1}} & & \downarrow{\scriptstyle \mathrm{tr}_{s,1}} \\ Z/p^2Z & \xrightarrow{\mu_1} & F_p \end{array}$$

is commutative, where μ_t and μ_s are the natural homomorphisms from the Galois rings $GR(p^2, t)$ and $GR(p^2, s)$ to their residue class fields respectively.

The additive characters of $GR(p^2, t)$ can also be described by the trace function.

LEMMA D. *All additive character λ_β of $GR(p^2, t)$ are given as follows*

$$\lambda_\beta(\alpha) = \xi_{p^2}^{T_{t,1}(\beta\alpha)}, \qquad \alpha \in GR(p^2, t)$$

where ξ_{p^2} is a primitive p^2th root of unity.

For the proofs of Lemma C and Lemma D, we refer the reader to Yamamoto and Yamada [9].

3. PARTIAL DIFFERENCE SETS

In this section, we generalize and improve the construction of partial difference sets in [7]. We will follow the notations used in Section 1 and 2. Considering the subgroup H of $GR(p^2, t)^*$, we enumerate the cosets of H in $GR(p^2, t)^*$ as, $E_{\bar{0}} = H$, $E_{\bar{1}} = (1+p)H$, $E_{\bar{g}} = (1+pg)H$, ..., $E_{\bar{g}^{q-2}} = (1+pg^{q-2})H$, where $q = p^t$. We note that $E_{\bar{0}}$, $E_{\bar{1}}$, $E_{\bar{g}}$, ..., $E_{\bar{g}^{q-2}}$, $B\backslash\{0\}$, $\{0\}$ are the orbits of the multiplication action of H on $GR(p^2, t)$, and $|E_{\bar{0}}| = |E_{\bar{1}}| = |E_{\bar{g}}| = \cdots = |E_{\bar{g}^{q-2}}| = q - 1$.

Let s be a positive divisor of t, $s<t$. There exists an element $\bar{0}\neq\bar{g}^a\in K$ such that $\mathrm{tr}_{t,s}(\bar{g}^a)=\bar{0}$. Let $V=\{\bar{x}\in K\colon \mathrm{tr}_{t,s}(\bar{g}^a\bar{x})=\bar{0}\}$. Then V is a $(t/s-1)$-dimensional F_{p^s}-subspace of K.

Let $V^\perp=\{\chi$ is an additive character of $K\colon \chi\mid_V=\chi_{\bar{0}}\}$. We claim that $V^\perp=\{\chi_{\bar{0}}\}\cup\{\chi_{\bar{h}}\colon \bar{h}=\bar{g}^a\bar{\alpha},\ \bar{\alpha}\in F_{p^s}^*\}$. To see this, one just needs to note that $\mathrm{tr}_{t,s}(\bar{\alpha}\bar{g}^a\bar{x})=\bar{\alpha}\,\mathrm{tr}_{t,s}(\bar{g}^a\bar{x})=\bar{0}$ for all $\bar{x}\in V$, $\bar{\alpha}\in F_{p^s}^*$, and $|V^\perp|=|K/V|=p^s$.

Define $D=\bigcup_{\bar{x}\in V}E_{\bar{x}}$. Then we have the following theorem.

THEOREM 3.1. *D is an $(n^2, r(n-1), n+r^2-3r, r^2-r)$-PDS in the additive group of $\mathrm{GR}(p^2,t)$ with $n=p^t$, $r=p^{t-s}$; $D\cup(B\backslash\{0\})$ is an $(n^2, r_1(n-1), n+r_1^2-3r_1, r_1^2-r_1)$-PDS in the additive group of $\mathrm{GR}(p^2,t)$ with $r_1=p^{t-s}+1$.*

Proof. Let λ be an arbitrary additive character of $\mathrm{GR}(p^2,t)$. By Lemma D, we consider the following three cases.

(1) λ is principal; i.e., $\lambda=\lambda_0$. In this case, $\lambda(D)=|D|=|V|(p^t-1)=p^{t-s}(p^t-1)$.

(2) $\lambda=\lambda_{pg^u}$, $0\leqslant u\leqslant(q-2)$. In this case, λ has order p. By the computation in the proof of Theorem 4.1 in [7], we know that $\lambda(E_{\bar{x}})=-1$. Hence $\lambda(D)=(-1)|V|=-p^{t-s}$.

(3) $\lambda=\lambda_\beta$, $\beta=(1+pb)g^u$, where $0\leqslant u\leqslant(q-2)$, and $b\in\mathscr{T}$. In this case, λ has order p^2, and

$$\begin{aligned}\lambda_\beta(D)&=\sum_{\bar{x}\in V}\sum_{i=0}^{q-2}\lambda_\beta((1+px)g^i)\\&=\sum_{\bar{x}\in V}\sum_{i=0}^{q-2}\xi_{p^2}^{T_{t,1}((1+px)g^i(1+pb)g^u)}\\&=\sum_{\bar{x}\in V}\sum_{i=0}^{q-2}\xi_{p^2}^{T_{t,1}((1+pb)g^i)}\xi_{p^2}^{T_{t,1}(pxg^i)}\\&=\sum_{i=0}^{q-2}\xi_{p^2}^{T_{t,1}((1+pb)g^i)}\chi_{\bar{g}^i}(V).\end{aligned}$$

By the claim proved before Theorem 3.1, we know that

$$\chi_{\bar{g}^i}(V)=\begin{cases}|V| & \text{if } \bar{g}^i=\bar{g}^a\bar{\alpha} \text{ for some } \bar{\alpha}\in F_{p^s}^*,\\ 0 & \text{otherwise.}\end{cases}$$

Hence,

$$\lambda_\beta(D) = |V| \sum_{\bar{\alpha} \in F_{p^s}^*} \xi_{p^2}^{T_{t,1}((1+pb)\, g^a \alpha)}$$
$$= |V| \sum_{\bar{\alpha} \in F_{p^s}^*} \xi_{p^2}^{T_{s,1}(T_{t,s}((1+pb)\, g^a)\alpha)}$$
$$= |V| \sum_{\bar{\alpha} \in F_{p^s}^*} \lambda_{T_{t,s}((1+pb)\, g^a)}(\alpha).$$

By the commutative diagram in Section 2, we have

$$\mu_s(T_{t,s}((1+pb)\, g^a)) = \mathrm{tr}_{t,s}(\mu_t((1+pb)\, g^a)) = \mathrm{tr}_{t,s}(\bar{g}^a) = \bar{0}.$$

This shows that $T_{t,s}((1+pb)g^a)$ is in the maximal ideal of $\mathrm{GR}(p^2, s)$, hence $\lambda_{T_{t,s}((1+pb)g^a)}$ is either the principal character or a character of order p of $\mathrm{GR}(p^2, s)$. Let $T_{t,s}(g^a) = pg^w \in \mathrm{GR}(p^2, s)$. By the surjectivity of $\mathrm{tr}_{t,s}$, there exists $\bar{b} \in K$ such that $\bar{g}^w + \mathrm{tr}_{t,s}(\bar{g}^a \bar{b}) = \bar{0}$; hence there exists $b \in \mathrm{GR}(p^2, t)$ such that $T_{t,s}((1+pb)g^a) = 0$, i.e., $\lambda_{T_{t,s}((1+pb)\, g^a)}$ is the principal character for some $b \in \mathrm{GR}(p^2, t)$. Therefore, we have

$$\lambda_\beta(D) = \begin{cases} p^{t-s}(p^s - 1) & \text{if } \lambda_{T_{t,s}((1+pb)\, g^a)} \text{ is the principal character,} \\ -p^{t-s} & \text{if } \lambda_{T_{t,s}((1+pb)\, g^a)} \text{ is a character of order } p. \end{cases}$$

Summing up all these calculations, we have shown that, for any nonprincipal additive character λ of $\mathrm{GR}(p^2, t)$, $\lambda(D) = p^{t-s}(p^s - 1)$ or $-p^{t-s}$. By Lemma A, D is an $(n^2, r(n-1), n + r^2 - 3r, r^2 - r)$-PDS in the additive group of $\mathrm{GR}(p^2, t)$ with $n = p^t$, $r = p^{t-s}$.

For the proof of the second part of the theorem, we note that for any nonprincipal additive character λ of $\mathrm{GR}(p^2, t)$,

$$\lambda(B \backslash \{0\}) = \begin{cases} -1 & \text{if } \lambda \text{ has order } p^2, \\ p^t - 1 & \text{if } \lambda \text{ has order } p. \end{cases}$$

Then by the above calculations of $\lambda(D)$ and Lemma A, we see that $D \cup (B \backslash \{0\})$ is an $(n^2, r_1(n-1), n + r_1^2 - 3r_1, r_1^2 - r_1)$-PDS in the additive group of $\mathrm{GR}(p^2, t)$ with $r_1 = p^{t-s} + 1$. This completes the proof of the theorem. ∎

Remark. In Theorem 3.1, if we let $s = 1$ and choose $\bar{g}^a = \bar{1}$ (hence $p \mid t$), we obtain Theorem 4.1 in [7]. S. L. Ma informed us that he and K. H. Leung also can get rid of the condition $p \mid t$ in our previous construction in [7] by using very different method. Here we could generalize our original construction to the case $t > s > 1$, $s \mid t$.

We continue to obtain more partial difference sets from the above construction.

Since $V=\{\bar{x}\in K\colon \mathrm{tr}_{t,s}(\bar{g}^a\bar{x})=\bar{0}\}$ is an F_{p^s}-subspace of K, $D=\bigcup_{\bar{x}\in V}E_{\bar{x}}$ is a subgroup of $\mathrm{GR}(p^2,t)^*$. Let $D_0=D$, $D_1=g_1D$, ..., $D_{p^s-1}=g_{p^s-1}D$ be the cosets of D in $\mathrm{GR}(p^2,t)^*$, where $g_i\in\mathscr{U}$, $1\leqslant i\leqslant p^s-1$. The character values of D_i can be easily calculated as

$$\lambda_0(D_i)=p^{t-s}(p^t-1),$$
$$\lambda_{pg^u}(D_i)=\lambda_{pg^ug_i}(D_0)=-p^{t-s},$$

and

$$\lambda_{(1+pb)g^u}(D_i)=\lambda_{(1+pb)g^ug_i}(D_0)$$
$$=\begin{cases}p^{t-s}(p^s-1)\\ \qquad \text{if} \quad \lambda_{T_{t,s}((1+pb)g^ag_i)} \text{ is the principal character,}\\ -p^{t-s}\\ \qquad \text{if} \quad \lambda_{T_{t,s}((1+pb)g^ag_i)} \text{ is a character of order } p,\end{cases}$$

for $i=1, 2, ..., p^s-1$.

Also for any fixed character $\lambda_{(1+pb)g^u}$, we have

$$\sum_{i=0}^{p^s-1}\lambda_{(1+pb)g^u}(D_i)=\lambda_{(1+pb)g^u}(\mathrm{GR}(p^2,t)\backslash B)=0.$$

Let $x=|\{i\mid 0\leqslant i\leqslant p^s-1,\ \lambda_{(1+pb)g^u}(D_i)=p^t-p^{t-s}\}|$. Then the above equation becomes $x(p^t-p^{t-s})-(p^s-x)p^{t-s}=0$; hence $x=1$. From this observation we have the following theorem.

THEOREM 3.2. *Let* $\{i_1, i_2, ..., i_l\}\subseteq\{0, 1, 2, ..., p^s-1\}$, $1\leqslant l\leqslant p^s$. $D_{i_1}\cup D_{i_2}\cup\cdots\cup D_{i_l}$ *is an* $(n^2, r_2(n-1), n+r_2^2-3r_2, r_2^2-r_2)$-PDS *in the additive group of* $\mathrm{GR}(p^2,t)$ *with* $n=p^t$, $r_2=lp^{t-s}$; $\bigcup_{j=1}^{l}D_{i_j}\cup(B\backslash\{0\})$ *is an* $(n^2, r_3(n-1), n+r_3^2-3r_3, r_3^2-r_3)$-*PDS in the additive group of* $\mathrm{GR}(p^2,t)$ *with* $r_3=lp^{t-s}+1$.

Proof. It suffices to check that the character values of $\bigcup_{j=1}^{l}D_{i_j}$ are as required by Lemma A. $\lambda_0(\bigcup_{j=1}^{l}D_{i_j})=lp^{t-s}(p^t-1)$. For any order p character λ_{pg^u}, $\lambda_{pg^u}(\bigcup_{j=1}^{l}D_{i_j})=-lp^{t-s}$. For any order p^2 character $\lambda_{(1+pb)g^u}$, by the observation made before Theorem 3.2, we know that there is at most one j, $1\leqslant j\leqslant l$, such that $\lambda_{(1+pb)g^u}(D_{i_j})=p^t-p^{t-s}$.

$$\lambda_{(1+pb)g^u}\left(\bigcup_{j=1}^{l}D_{i_j}\right)$$
$$=\begin{cases}p^t-lp^{t-s} & \text{if} \quad \lambda_{(1+pb)g^u}(D_{i_j})=p^t-p^{t-s} \text{ for some } j,\ 1\leqslant j\leqslant l,\\ -lp^{t-s} & \text{otherwise.}\end{cases}$$

This shows that $D_{i_1} \cup D_{i_2} \cup \cdots \cup D_{i_l}$ is an $(n^2, r_2(n-1), n+r_2^2-3r_2, r_2^2-r_2)$-PDS in the additive group of $\mathrm{GR}(p^2, t)$ with $n=p^t$, $r_2=lp^{t-s}$. The second part of the theorem can be similarly proved. This completes the proof. ∎

4. RELATIVE DIFFERENCE SETS

In this section, we give two constructions of relative difference sets. The first is a consequence of the construction of partial difference sets in Section 3. The second construction is for abelian 2-groups, in its general form (Theorem 4.6), the construction gives new relative difference sets in abelian 2-groups. We will maintain the notation in previous sections.

Let $G=(\mathrm{GR}(p^2, t), +)\oplus P$, where $(\mathrm{GR}(p^2, t), +)$ is the additive group of $\mathrm{GR}(p^2, t)$, and P is any abelian group of order p^s, where $s \mid t$, $1 \leqslant s < t$. Assume that $P=\{x_0, x_1, ..., x_{p^s-1}\}$. We define $R=(D_0, x_0)\cup (D_1, x_1)\cup \cdots \cup (D_{p^s-1}, x_{p^s-1})\cup (B, 0)$, where $D_0, D_1, ..., D_{p^s-1}$ were defined in Section 3. Then we have the following theorem.

THEOREM 4.1. *R is a $(p^{2t}, p^s, p^{2t}, p^{2t-s})$-relative difference set in G relative to P.*

Proof. Let ψ be an arbitrary character of G. Then $\psi=\lambda\otimes\chi$, where λ is an additive character of $\mathrm{GR}(p^2, t)$ and χ is a character of P. We consider two cases.

Case 1. χ is the principal character:

$$\psi(R)=\sum_{i=0}^{p^s-1}\lambda(D_i)+\lambda(B).$$

If λ is principal, then $\psi(R)=|R|=p^{2t}$.

If λ is not principal, then we distinguish two cases.

(1) $\lambda=\lambda_{pg^u}$. In this case, λ has order p, $\lambda(B)=|B|=p^t$, and $\lambda(D_i)=-p^{t-s}$, $0\leqslant i\leqslant p^s-1$. Hence $\psi(R)=(-p^{t-s})\,p^s+p^t=0$.

(2) $\lambda=\lambda_\beta$, $\beta=(1+pb)\,g^u$, where $0\leqslant u\leqslant (q-2)$, and $b\in\mathscr{T}$. In this case, λ has order p^2, $\lambda(B)=0$, and by the observation made before Theorem 3.2, we know that there is a unique j, $0\leqslant j\leqslant p^s-1$, such that $\lambda_{(1+pb)\,g^u}(D_j)=p^t-p^{t-s}$. Hence $\psi(R)=p^t-p^{t-s}+(p^s-1)(-p^{t-s})=0$.

Case 2. χ is nonprincipal on P:

$$\psi(R)=\sum_{i=0}^{p^s-1}\lambda(D_i)\,\chi(x_i)+\lambda(B);$$

we also distinguish three cases.

(1) λ is principal: $\psi(R) = |D_0| \sum_{i=0}^{p^s-1} \chi(x_i) + |B| = p^t$.

(2) λ has order p; i.e., $\lambda = \lambda_{pg^u}$. In this case, $\lambda(B) = |B| = p^t$ and $\lambda(D_i) = -p^{t-s}$, $0 \leqslant i \leqslant p^s - 1$. So $\psi(R) = -p^{t-s} \sum_{i=0}^{p^s-1} \chi(x_i) + p^t = p^t$.

(3) λ has order p^2; i.e., $\lambda = \lambda_\beta$, $\beta = (1+pb)\, g^u$. As in Case 1, there is a unique j, $0 \leqslant j \leqslant p^s - 1$, such that $\lambda_{(1+pb)\, g^u}(D_j) = p^t - p^{t-s}$. Hence, $\psi(R) = (p^t - p^{t-s})\, \chi(x_j) + \sum_{i \neq j} \chi(x_i)(-p^{t-s}) = p^t \chi(x_j)$. Therefore, $|\psi(R)| = p^t$.

So we have shown that

$$|\psi(R)| = \begin{cases} p^{2t} & \text{if } \psi \text{ is principal on } G. \\ 0 & \text{if } \psi \text{ is nonprincipal on } G \text{ but principal on } P. \\ p^t & \text{if } \psi \text{ is nonprincipal on } P. \end{cases}$$

By Lemma B, R is a $(p^{2t}, p^s, p^{2t}, p^{2t-s})$-relative difference set in G relative to P. This completes the proof. ∎

Remark. We remark that there are many constructions of (p^a, p^b, p^a, p^{a-b})-relative difference sets, see [8] for a summary. The good thing in Theorem 4.1 is that P is an arbitrary abelian p-group of order p^s.

The RDS in Theorem 4.1 is splitting. In the following, we construct a nonsplitting RDS in abelian 2-groups.

Let $A = \{\bar{x} \in K \mid \mathrm{tr}_{t,1}(\bar{x}) = \bar{0}\}$, $G = (\mathrm{GR}(4, t), +) \oplus (A, +)$, and $F_{\bar{a}} = E_{\bar{a}} \cup \{0\}$. Assume that $A = \{\overline{\alpha_1}, \overline{\alpha_2}, ..., \overline{\alpha_{2^{t-1}}}\}$, $\alpha_i \in \mathscr{T}$, $1 \leqslant i \leqslant 2^{t-1}$. Define $R = \bigcup_{i=1}^{2^{t-1}} (F_{\overline{\alpha_i}}, \overline{\alpha_i})$. We have the following theorem.

THEOREM 4.2. *If* $t = 2m+1$, $m \geqslant 1$, *then* R *is a* $(2^{4m+1}, 2^{2m+1}, 2^{4m+1}, 2^{2m})$*-relative difference set in* G *relative to* B, *where* B *is the unique maximal ideal of* $\mathrm{GR}(4, t)$.

Proof. Let ψ be an arbitrary character of G. Then $\psi = \lambda \otimes \chi$, where λ is an additive character of $\mathrm{GR}(4, t)$ and χ is a character of A.

If ψ is principal, then $\psi(R) = |R| = 2^{4m+1}$.

If λ is principal, χ is nonprincipal; then $\psi(R) = |F_{\overline{\alpha_1}}| \sum_{i=1}^{2^{t-1}} \chi(\overline{\alpha_i}) = 0$.

If λ has order 2, i.e., λ is principal on B but not principal on $\mathrm{GR}(4, t)$, then $\psi(R) = \sum_{i=1}^{2^{t-1}} (1 + \lambda(E_{\overline{\alpha_i}}))\, \chi(\overline{\alpha_i})$. Noting that $\lambda(E_{\overline{\alpha_i}}) = -1$, we have $\psi(R) = 0$.

If λ has order 4, we consider two cases.

Case 1. χ is principal:

$$\psi(R) = \sum_{i=1}^{2^{t-1}} (\lambda(E_{\overline{\alpha_i}}) + 1) = \sum_{i=1}^{2^{t-1}} \lambda(E_{\overline{\alpha_i}}) + 2^{t-1}.$$

By a result of Yamamoto and Yamada [9], we know that $\sum_{i=1}^{2^{t-1}} \lambda(E_{\overline{\alpha_i}}) = \pm 2^{t-1}\xi_4$, where $\xi_4 = \sqrt{-1}$. Hence $|\psi(R)| = \sqrt{2}\, 2^{t-1} = \sqrt{2^{2t-1}}$.

Case 2. χ is nonprincipal. We assume that $\lambda = \lambda_{(1+2b)g^u}$, and $\chi = \chi_{\bar{g}^v}$, where $g^u \in H$, $\bar{g}^v \in K$, $v \neq 0$, then

$$\begin{aligned}
\psi(R) &= \sum_{i=1}^{2^{t-1}} (\lambda(E_{\overline{\alpha_i}}) + 1)\, \chi(\overline{\alpha_i}) \\
&= \sum_{i=1}^{2^{t-1}} \sum_{j=0}^{2^t-2} (\xi_4^{T_{t,1}((1+2\alpha_i)g^j(1+2b)g^u)} + 1)(-1)^{\mathrm{tr}_{t,1}(\bar{g}^v\overline{\alpha_i})} \\
&= \sum_{i=1}^{2^{t-1}} \sum_{j=0}^{2^t-2} \xi_4^{T_{t,1}((1+2b+2\alpha_i)g^j)}(-1)^{\mathrm{tr}_{t,1}(\bar{g}^v\overline{\alpha_i})} \\
&= \sum_{j=0}^{2^t-2} \xi_4^{T_{t,1}((1+2b)g^j)} \sum_{i=1}^{2^{t-1}} (-1)^{\mathrm{tr}_{t,1}((\bar{g}^j+\bar{g}^v)\overline{\alpha_i})} \\
&= \sum_{j=0}^{2^t-2} \xi_4^{T_{t,1}((1+2b)g^j)} \chi_{\bar{g}^j+\bar{g}^v}(A)
\end{aligned}$$

Since A is the trace zero hyperplane in K, if an additive character χ is neither $\chi_{\bar{0}}$ nor $\chi_{\bar{1}}$, then $\chi(A) = 0$. Let $\bar{g}^j + \bar{g}^v = \bar{0}$. Then $\bar{g}^j = \bar{g}^v$. If we set $\bar{g}^j + \bar{g}^v = \bar{1}$, then $\bar{g}^j = \bar{1} - \bar{g}^v = \bar{g}^w$ (say). Hence

$$\begin{aligned}
\psi(R) &= \xi_4^{T_{t,1}((1+2b)g^v)} 2^{t-1} + \xi_4^{T_{t,1}((1+2b)g^w)} 2^{t-1} \\
&= 2^{t-1}((-1)^{\mathrm{tr}_{t,1}(\bar{g}^v\bar{b})}\xi_4^{T_{t,1}(g^v)} + (-1)^{\mathrm{tr}_{t,1}(\bar{g}^w\bar{b})}\, \xi_4^{T_{t,1}(g^w)}).
\end{aligned}$$

By the commutative diagram in Section 2, we have $\mu_1(T_{t,1}(g^v)) = \mathrm{tr}_{t,1}(\bar{g}^v)$, and $\mu_1(T_{t,1}(g^w)) = \mathrm{tr}_{t,1}(\bar{1} - \bar{g}^v) = t + \mathrm{tr}_{t,1}(\bar{g}^v)$. So if t is odd, then $\mu_1(T_{t,1}(g^v))$ and $\mu_1(T_{t,1}(g^w))$ have opposite parity. Therefore $|\psi(R)| = 2^{t-1}\,|\pm 1 \pm \xi_4| = \sqrt{2}\, 2^{t-1} = \sqrt{2^{2t-1}}$.

Summing up all these calculations, we have shown that

$$|\psi(R)| = \begin{cases} 2^{2t-1} & \text{if } \psi \text{ is principal on } G. \\ 0 & \text{if } \psi \text{ is nonprincipal on } G \text{ but principal on } B. \\ \sqrt{2^{2t-1}} & \text{if } \psi \text{ is nonprincipal on } B. \end{cases}$$

By Lemma B, we conclude that R is a $(2^{4m+1}, 2^{2m+1}, 2^{4m+1}, 2^{2m})$-relative difference set in G relative to B. This completes the proof. ∎

Remark. Jungnickel [4] has given a construction of $(2^a, 2^b, 2^a, 2^{a-b})$-RDS in $(Z_4)^b \oplus (Z_2)^{a-b}$. Our method of construction here is quite different from Jungnickel's method. Also the construction in Theorem 4.2 gives Hadamard difference sets in $(A, +)$ as we will show below, these

Hadamard difference sets in turn allow us to generalize the construction in Theorem 4.2 to more general groups.

Let A and $F_{\bar{a}}$ be the same as before, and λ be any order 4 character of GR(4, t). We assume that $\lambda = \lambda_{\gamma_1 + 2\gamma_2}$ for some $\gamma_1, \gamma_2 \in \mathscr{T}$, $\gamma_1 \neq 0$, also we will denote the trace map $T_{t,1}$ from GR(4, t) to Z_4 simply by T, then we have the following lemma.

LEMMA 4.1. $\sum_{x \in \mathscr{T}} \lambda(x) = (\sum_{x \in \mathscr{T}} \xi_4^{T(x)})\, \xi_4^{-T(\gamma_2/\gamma_1)}$.

Proof (Calderbank). From Section E of [3], we know that $\sigma: x \mapsto (ax+b)^{2^m}$, $a, b \in \mathscr{T}$, $a \neq 0$ induces a permutation on $\mathscr{T}$. Hence

$$\begin{aligned}
\sum_{x \in \mathscr{T}} \lambda(x) &= \sum_{x \in \mathscr{T}} \xi_4^{T((\gamma_1 + 2\gamma_2)x)} \\
&= \sum_{x \in \mathscr{T}} \xi_4^{T((\gamma_1 + 2\gamma_2)(ax+b)^{2^m})} \\
&= \sum_{x \in \mathscr{T}} \xi_4^{T((\gamma_1 + 2\gamma_2)(ax + b + 2(abx)^{2^{m-1}}))} \\
&= \sum_{x \in \mathscr{T}} \xi_4^{T(a\gamma_1 x + 2a\gamma_2 x + \gamma_1 b + 2\gamma_2 b + 2\gamma_1 (abx)^{2^{m-1}})}.
\end{aligned}$$

Noting that $T(2y) = T(2y^2)$ for $y \in \mathscr{T}$, and letting $a = 1/\gamma_1$, $b = \gamma_2/\gamma_1^2$, we have

$$\begin{aligned}
\sum_{x \in \mathscr{T}} \lambda(x) &= \sum_{x \in \mathscr{T}} \xi_4^{T(x - (\gamma_2/\gamma_1))} \\
&= \left(\sum_{x \in \mathscr{T}} \xi_4^{T(x)} \right) \xi_4^{-T(\gamma_2/\gamma_1)}.
\end{aligned}$$

This completes the proof. ∎

Assume that $A = \{\overline{\alpha_1}, \overline{\alpha_2}, \ldots, \overline{\alpha_{2^{t-1}}}\}$, $\overline{\alpha_1} = \bar{0}$, $\alpha_i \in \mathscr{T}$; then $F_{\bar{0}} = \mathscr{T}$ and for each i, $2 \leqslant i \leqslant 2^{t-1}$, $F_{\overline{\alpha_i}} = (1 + 2\alpha_i)\mathscr{T}$. Given any order 4 character $\lambda_{(1+2\gamma)g^u}$, $\gamma \in \mathscr{T}$, $0 \leqslant u \leqslant 2^t - 2$, one has

$$\begin{aligned}
\lambda_{(1+2\gamma)g^u}(F_{\overline{\alpha_i}}) &= \sum_{j=0}^{2^t-2} \xi_4^{T((1+2\gamma)g^u(1+2\alpha_i)g^j)} + 1 \\
&= \sum_{j=0}^{2^t-2} \xi_4^{T((1+2\gamma)(1+2\alpha_i)g^j)} + 1 \\
&= \lambda_{1+2\gamma}(F_{\overline{\alpha_i}}),
\end{aligned}$$

so we may concentrate on characters of the form $\lambda_{1+2\gamma}$, $\gamma \in \mathscr{T}$.

For any fixed $\lambda_{1+2\gamma}$, $\gamma \in \mathscr{T}$, we have

$$\lambda_{1+2\gamma}(F_{\overline{\alpha_i}}) = \sum_{x \in \mathscr{T}} \xi_4^{T((1+2\gamma)(1+2\alpha_i)x)}$$
$$= \sum_{x \in \mathscr{T}} \xi_4^{T((1+2\gamma+2\alpha_i)x)}.$$

Assuming that $\gamma + \alpha_i = \beta_i + 2\theta_i$, β_i, $\theta_i \in \mathscr{T}$, by Lemma 4.1, we have

$$\lambda_{1+2\gamma}(F_{\overline{\alpha_i}}) = \sum_{x \in \mathscr{T}} \xi_4^{T((1+2\beta_i)x)}$$
$$= \lambda_1(F_{\bar{0}})\, \xi_4^{-T(\beta_i)}.$$

On the other hand,

$$\lambda_{1+2\gamma}(F_{\bar{0}}) = \sum_{x \in \mathscr{T}} \xi_4^{T((1+2\gamma)x)}$$
$$= \lambda_1(F_{\bar{0}})\, \xi_4^{-T(\gamma)};$$

noting that $\gamma^2 + 2\gamma\alpha_i + \alpha_i^2 = \beta_i^2$, we have

$$\frac{\lambda_{1+2\gamma}(F_{\overline{\alpha_i}})}{\lambda_{1+2\gamma}(F_{\bar{0}})} = \xi_4^{-T(\beta_i - \gamma)}$$
$$= \xi_4^{-T(\beta_i^2 - \gamma^2)}$$
$$= \xi_4^{-T((1+2\gamma)\alpha_i)}.$$

Since $\mathrm{tr}_{t,1}(\overline{\alpha_i}) = \bar{0}$, $T((1+2\gamma)\alpha_i) = T(\alpha_i) + 2T(\gamma\alpha_i) \in \{0, 2\}$.

Define $\omega_\gamma : A \to \{\pm 1\}$ via $\omega_\gamma(\overline{\alpha_i}) = \lambda_{1+2\gamma}(F_{\overline{\alpha_i}})/\lambda_{1+2\gamma}(F_{\bar{0}}) = \xi_4^{T((1+2\gamma)\alpha_i)}$. We have the following theorem.

THEOREM 4.3. *If $t = 2m+1$, $m \geqslant 1$, then $\omega_\gamma^{-1}[1]$ is a $(2^{2m}, 2^{2m-1} \pm 2^{m-1}, 2^{2m-2} \pm 2^{m-1})$-difference set in $(A, +)$ for all $\gamma \in \mathscr{T}$.*

Proof. First we note that

$$\sum_{i=1}^{2^{t-1}} \lambda_{1+2\gamma}(F_{\overline{\alpha_i}}) = \sum_{i=1}^{2^{t-1}} \lambda_{1+2\gamma}(E_{\overline{\alpha_i}}) + 2^{t-1} = 2^{2m} \pm 2^{2m}\xi_4,$$

where $\sum_{i=1}^{2^{t-1}} \lambda_{1+2\gamma}(E_{\overline{\alpha_i}}) = \pm 2^{2m}\xi_4$ follows from Yamamoto and Yamada [9]. Hence

$$|\omega_\gamma^{-1}[1]|\, \lambda_{1+2\gamma}(F_{\bar{0}}) - (2^{t-1} - |\omega_\gamma^{-1}[1]|)\, \lambda_{1+2\gamma}(F_{\bar{0}}) = 2^{2m} \pm 2^{2m}\xi_4.$$

Also by a result of Boztas, Hammons, and Kumar in [1], we know that $\lambda_{1+2\gamma}(F_{\overline{\alpha_i}}) = \pm 2^m \pm 2^m \xi_4$. It follows that $|\omega_\gamma^{-1}[1]| = 2^{2m-1} \pm 2^{m-1}$. From the proof of Theorem 4.2, Case 2, χ is nonprincipal; therefore we have

$$\begin{aligned}\psi(D) &= \sum_{i=1}^{2^{t-1}} \lambda_{1+2\gamma}(F_{\overline{\alpha_i}})\,\chi(\overline{\alpha_i}) \\ &= \lambda_{1+2\gamma}(F_{\bar{0}})\,\chi(\omega_\gamma^{-1}[1]) - \lambda_{1+2\gamma}(F_{\bar{0}})\,\chi(A\backslash\omega_\gamma^{-1}[1]) \\ &= 2\lambda_{1+2\gamma}(F_{\bar{0}})\,\chi(\omega_\gamma^{-1}[1]),\end{aligned}$$

where ψ, χ, and D are the same as those in the proof of Theorem 4.2. By Theorem 4.2, $|\psi(D)| = \sqrt{2}\,2^{2m}$; also $|\lambda_{1+2\gamma}(F_{\bar{0}})| = \sqrt{2}\,2^m$. We have $|\chi(\omega_\gamma^{-1}[1])| = 2^{m-1}$, for every nonprincipal character χ of A. Hence $\omega_\gamma^{-1}[1]$ is a Hadamard difference set in A. This completes the proof. ∎

From the above theorem, we see that each $\gamma \in \mathscr{T}$ gives rise to a Hadamard difference set $\omega_\gamma^{-1}[1]$ in $(A, +)$; the relationship between these $\omega_\gamma^{-1}[1]$, $\gamma \in \mathscr{T}$, is given in the following proposition.

PROPOSITION 4.4. (1) *If* $\gamma \in \mathscr{T}$, $\bar{\gamma} \in A$, *then* $\omega_\gamma^{-1}[1] = \omega_0^{-1}[1] + \bar{\gamma}$ *if* $T(\gamma) = 0$, $A\backslash\omega_\gamma^{-1}[1] = \omega_0^{-1}[1] + \bar{\gamma}$ *if* $T(\gamma) = 2$.

(2) *If* $\gamma \in \mathscr{T}$, $\bar{\gamma} \notin A$, *assuming that* $\bar{\gamma} = \bar{1} + \overline{\alpha_i}$ *for some* $\overline{\alpha_i} \in A$, *then* $\omega_\gamma^{-1}[1] = \omega_1^{-1}[1] + \overline{\alpha_i}$ *if* $T(\gamma - 1) = 0$; $A\backslash\omega_\gamma^{-1}[1] = \omega_1^{-1}[1] + \overline{\alpha_i}$ *if* $T(\gamma - 1) = 2$. *Also* $\omega_1^{-1}[1] = \omega_0^{-1}[1]$.

Proof. We prove the proposition for the case $\gamma \in \mathscr{T}$, $\bar{\gamma} \in A$, $T(\gamma) = 0$. The rest of the proposition can be similarly proved.

If $\bar{x} \in \omega_0^{-1}[1]$, $x \in \mathscr{T}$, then $T(x) = 0$. We claim that $\bar{x} + \bar{\gamma} \in \omega_\gamma^{-1}[1]$, so $\omega_0^{-1}[1] + \bar{\gamma} \subseteq \omega_\gamma^{-1}[1]$. Let $\bar{x} + \bar{\gamma} = \bar{y}$, $y \in \mathscr{T}$. Assume that $x + \gamma = y + 2z$, $z \in \mathscr{T}$, then $\gamma - y = 2z - x$, so $\gamma^2 - 2y\gamma + y^2 = x^2$.

$$\begin{aligned}T(y(1+2\gamma)) &= T(y^2) - 2T(y\gamma) \\ &= T(x^2) - T(\gamma^2) \\ &= -T(\gamma) = 0.\end{aligned}$$

Hence $\bar{y} = \bar{x} + \bar{\gamma} \in \omega_\gamma^{-1}[1]$. This proves the claim.

Conversely, for any $\bar{x} \in \omega_\gamma^{-1}[1]$, $x \in \mathscr{T}$, we can similarly prove that $\bar{x} - \bar{\gamma} \in \omega_0^{-1}[1]$; hence $\bar{x} \in \omega_0^{-1}[1] + \bar{\gamma}$.

Summing up, we have shown that $\omega_\gamma^{-1}[1] = \omega_0^{-1}[1] + \bar{\gamma}$ if $T(\gamma) = 0$. This completes the proof of the proposition. ∎

We remark that ω_γ can also be defined by $\omega_\gamma(\overline{\alpha_i}) = \xi_4^{T((1+2\gamma^2)\alpha_i^2)}$, $\alpha_i \in \mathscr{T}$, since $T((1+2\gamma)\alpha_i) = T((1+2\gamma^2)\alpha_i^2)$. In general, we have $\omega_\gamma(\bar{x}) = \xi_4^{T((1+2\gamma^2)x^2)}$, where we do not require $x \in \mathscr{T}$. This definition is more convenient to use.

We note that $\omega_\gamma: A \to \{\pm 1\}$ defines a function $b_\gamma: A \to \{0, 1\}$ via $\omega_\gamma(\bar{x}) = (-1)^{b_\gamma(\bar{x})}$ for all $\gamma \in \mathscr{T}$. By the relationship between Hadamard difference sets and bent functions (see [2]), we have the following corollary.

COROLLARY 4.5. *b_γ is a bent function on $A \cong F_2^{2m}$ for every $\gamma \in \mathscr{T}$.*

We continue to study the bent functions b_γ, $\gamma \in \mathscr{T}$.

LEMMA 4.2 *For each $\gamma \in \mathscr{T}$, b_γ is a quadratic form on $A \cong F_2^{2m}$.*

Proof. It suffices to prove that $b_\gamma(\bar{x}+\bar{y}) - b_\gamma(\bar{x}) - b_\gamma(\bar{y})$ is a bilinear form on A. From the definition of b_γ, we see that

$$\begin{aligned}(-1)^{(b_\gamma(\bar{x}+\bar{y}) - b_\gamma(\bar{x}) - b_\gamma(\bar{y}))} &= \xi_4^{T((1+2\gamma^2)(x+y)^2) - T((1+2\gamma^2)x^2) - T((1+2\gamma^2)y^2)} \\ &= \xi_4^{T(2xy)} \\ &= (-1)^{\mathrm{tr}_{t,1}(\overline{xy})}.\end{aligned}$$

So $b_\gamma(\bar{x}+\bar{y}) - b_\gamma(\bar{x}) - b_\gamma(\bar{y}) = \mathrm{tr}_{t,1}(\overline{xy})$ is a bilinear form on A. This completes the proof. ∎

From Remark 6.3.1 of [2], we know that b_γ, $\gamma \in \mathscr{T}$ (up to complementation), belong to family Q (see [2]), and it has the form

$$b_\gamma(X, Y) = X_1 Y_1 + X_2 Y_2 + \cdots + X_m Y_m$$

with respect to a suitable basis $x_1, x_2, ..., x_m, y_1, y_2, ..., y_m$ of A over F_2. Hence the difference set $\omega_\gamma^{-1}[1]$ (up to complementation) is the Menon composition (which corresponds to the Kronecker product of the corresponding Hadamard matrices, see [2]) of singleton difference sets in $Z_2 x_i + Z_2 y_i$, $i = 1, 2, ..., m$.

Let $W = (Z_4)^r \oplus (Z_2 \oplus Z_2)^s$, $r+s=m$. We define a bijection $f_\gamma: A \to W$ by setting $f_\gamma = f^{(1)} \times f^{(2)} \times \cdots \times f^{(m)}$, where $f^{(i)}: Z_2 x_i + Z_2 y_i \to Z_4$ or $(Z_2 \oplus Z_2)$ is an arbitrary bijection. We note that the definition of f_γ depends on the basis $x_1, x_2, ..., x_m, y_1, y_2, ..., y_m$ of A over F_2. We need the following lemma.

LEMMA 4.3. *$f_\gamma(\omega_\gamma^{-1}[1] + z)$ are Hadamard difference sets for all $\gamma \in \mathscr{T}$ and $z \in A$.*

Proof. We prove the lemma in the case $m = 2$. The rest follows by induction on m.

If $m=2$, let $G_i=Z_2x_i+Z_2y_i$ and let D_i be trivial difference sets in G_i, $i=1, 2$ (by trivial difference sets we mean that D_i is either a singleton difference set or the complement of a singleton difference set). From the discussion above we see that $\omega_\gamma^{-1}[1]=[D_1\times(G_2\backslash D_2)]\cup[(G_1\backslash D_1)\times D_2]$.

Let $z=(z_1, z_2)$, $z_i\in G_i$, $i=1, 2$. Then

$$\begin{aligned}\omega_\gamma^{-1}[1]+z&=[(D_1+z_1)\times((G_2\backslash D_2)+z_2)]\cup[((G_1\backslash D_1)+z_1)\times(D_2+z_2)]\\&=[(D_1+z_1)\times(G_2\backslash(D_2+z_2))]\cup[(G_1\backslash(D_1+z_1))\times(D_2+z_2)];\\f_\gamma(\omega_\gamma^{-1}[1]+z)&=[f^{(1)}(D_1+z_1)\times(f^{(2)}(G_2)\backslash f^{(2)}(D_2+z_2))]\\&\quad\cup[(f^{(1)}(G_1)\backslash f^{(1)}(D_1+z_1))\times f^{(2)}(D_2+z_2)].\end{aligned}$$

Since D_1 and D_2 are trivial difference sets in G_1 and G_2, $f^{(1)}(D_1+z_1)$ and $f^{(2)}(D_2+z_2)$ are trivial difference sets in G_1 and G_2, respectively. Hence $f_\gamma(\omega_\gamma{}^{-1}[1]+z)$ is a Hadamard difference set in $f^{(1)}(G_1)\times f^{(2)}(G_2)$. The proof is complete. ∎

With the above preparation, we can now generalize Theorem 4.2 as follows.

Let $G=(\mathrm{GR}(4, t), +)\oplus W$, where $t=2m+1$, $m\geqslant 1$, $W=(Z_4)^r\oplus(Z_2\oplus Z_2)^s$, $r+s=m$, $r, s\geqslant 0$, and let f_0 be the bijection from A to W defined before Lemma 4.3. We define $R=\bigcup_{i=1}^{2^{t-1}}(F_{\overline{\alpha}_i}, f_0(\overline{\alpha}_i))$, where $A=\{\overline{\alpha}_1, \overline{\alpha}_2, ..., \overline{\alpha}_{2^{t-1}}\}$, $\overline{\alpha}_1=\bar{0}$, $\alpha_i\in\mathscr{T}$ is the trace zero hyperplane of $K=\mathrm{GR}(4, t)/B$. We have the following theorem.

THEOREM 4.6 *R is a $(2^{4m+1}, 2^{2m+1}, 2^{4m+1}, 2^{2m})$-relative difference set in G relative to B, where B is the unique maximal ideal of* $\mathrm{GR}(4, t)$.

Proof. Let ψ be an arbitrary character of G. Then $\psi=\lambda\otimes\chi$, where λ is an additive character of $\mathrm{GR}(4, t)$ and χ is a character of W.

If ψ is principal, then $\psi(R)=|R|=2^{4m+1}$.

If λ is principal, χ is nonprincipal, then $\psi(R)=|F_{\overline{\alpha}_1}|\sum_{i=1}^{2^{t-1}}\chi(f_0(\overline{\alpha}_i))=0$.

If λ has order 2, i.e., λ is principal on B but not principal on $\mathrm{GR}(4, t)$, then $\psi(R)=\sum_{i=1}^{2^{t-1}}(1+\lambda(E_{\overline{\alpha}_i}))\chi(f_0(\overline{\alpha}_i))$. Noting that $\lambda(E_{\overline{\alpha}_i})=-1$, we have $\psi(R)=0$.

If λ has order 4, we consider two cases:

Case 1. χ is principal:

$$\begin{aligned}\psi(R)&=\sum_{i=1}^{2^{t-1}}(\lambda(E_{\overline{\alpha}_i})+1)\\&=2^{t-1}\pm 2^{t-1}\xi_4.\end{aligned}$$

Hence $|\psi(R)|=\sqrt{2}\,2^{t-1}=\sqrt{2^{2t-1}}$.

Case 2. χ is nonprincipal. We assume that $\lambda = \lambda_{(1+2\gamma)g^u}$, $\gamma \in \mathscr{T}$. Noting that $\lambda_{(1+2\gamma)g^u}(F_{\overline{\alpha_i}}) = \lambda_{1+2\gamma}(F_{\overline{\alpha_i}})$, we have

$$\psi(R) = \sum_{i=1}^{2^{t-1}} \lambda_{1+2\gamma}(F_{\overline{\alpha_i}})\, \chi(f_0(\overline{\alpha_i})).$$

If $\gamma = 0$, then

$$\begin{aligned}\psi(R) &= \lambda_1(F_{\bar{0}})\, \chi(f_0(\omega_0^{-1}[1])) - \lambda_1(F_{\bar{0}})\, \chi(W \backslash f_0(\omega_0^{-1}[1])) \\ &= 2\lambda_1(F_{\bar{0}})\, \chi(f_0(\omega_0^{-1}[1])).\end{aligned}$$

By Lemma 4.3, we know that $|\chi(f_0(\omega_0^{-1}[1]))| = 2^{m-1}$, so $|\psi(R)| = 2\sqrt{2}\, 2^m 2^{m-1} = \sqrt{2}\, 2^{2m}$.

If $\gamma \neq 0$, $\bar{\gamma} \in A$, then

$$\psi(R) = \sum_{\bar{x} \in A} \lambda_1(F_{\bar{x}+\bar{\gamma}})\, \chi(f_0(\bar{x})).$$

Let $\bar{x} + \bar{\gamma} = \bar{y}$. Then

$$\begin{aligned}\psi(R) &= \sum_{\bar{y} \in A + \bar{\gamma}} \lambda_1(F_{\bar{y}})\, \chi(f_0(\bar{y} - \bar{\gamma})) \\ &= \sum_{\bar{y} \in A} \lambda_1(F_{\bar{y}})\, \chi(f_0(\bar{y} - \bar{\gamma})) \\ &= \lambda_1(F_{\bar{0}})\, \chi(f_0(\omega_0^{-1}[1] - \bar{\gamma})) - \lambda_1(F_{\bar{0}})\, \chi(W \backslash f_0(\omega_0^{-1}[1] - \bar{\gamma})) \\ &= 2\lambda_1(F_{\bar{0}})\, \chi(f_0(\omega_0^{-1}[1] - \bar{\gamma})).\end{aligned}$$

By Lemma 4.3, we know that $|\chi(f_0(\omega_0^{-1}[1] - \bar{\gamma}))| = 2^{m-1}$, so $|\psi(R)| = 2\sqrt{2}\, 2^m 2^{m-1} = \sqrt{2}\, 2^{2m}$.

If $\gamma = 1$, then

$$\begin{aligned}\psi(R) &= \sum_{i=1}^{2^{t-1}} \lambda_3(F_{\overline{\alpha_i}})\, \chi(f_0(\overline{\alpha_i})) \\ &= \sum_{i=1}^{2^{t-1}} \overline{\lambda_1(F_{\overline{\alpha_i}})}\, \chi(f_0(\overline{\alpha_i})) \\ &= 2\overline{\lambda_1(F_{\bar{0}})}\, \chi(f_0(\omega_0^{-1}[1])).\end{aligned}$$

Hence $|\psi(R)| = 2\sqrt{2}\, 2^m 2^{m-1} = \sqrt{2}\, 2^{2m}$.

If $\bar{\gamma} \notin A$, $\gamma \neq 1$, we can write $\bar{\gamma} = \bar{1} + \bar{\beta}$ with $\bar{\beta} \in A$; then $\lambda_{1+2\bar{\gamma}}(F_{\overline{\alpha_i}}) = \lambda_3(F_{\bar{\beta}+\overline{\alpha_i}}) = \overline{\lambda_1(F_{\bar{\beta}+\overline{\alpha_i}})}$, so

$$\begin{aligned}
\psi(R) &= \sum_{\bar{x} \in A} \overline{\lambda_1(F_{\bar{x}+\bar{\beta}})}\, \chi(f_0(\bar{x})) \\
&= \sum_{\bar{y} \in A+\bar{\beta}} \overline{\lambda_1(F_{\bar{y}})}\, \chi(f_0(\bar{y}-\bar{\beta})) \\
&= \sum_{\bar{y} \in A} \overline{\lambda_1(F_{\bar{y}})}\, \chi(f_0(\bar{y}-\bar{\beta})) \\
&= \overline{\lambda_1(F_{\bar{0}})}\, \chi(f_0(\omega_0^{-1}[1]-\bar{\beta})) - \overline{\lambda_1(F_{\bar{0}})}\, \chi(W \backslash f_0(\omega_0^{-1}[1]-\bar{\beta})) \\
&= 2\overline{\lambda_1(F_{\bar{0}})}\, \chi(f_0(\omega_0^{-1}[1]-\bar{\beta})).
\end{aligned}$$

Hence by Lemma 4.3 $|\psi(R)| = 2\sqrt{2}\, 2^m 2^{m-1} = \sqrt{2}\, 2^{2m}$.

In summary, we have shown that

$$|\psi(R)| = \begin{cases} 2^{2t-1} & \text{if } \psi \text{ is principal on } G, \\ 0 & \text{if } \psi \text{ is nonprincipal on } G \text{ but principal on } B, \\ \sqrt{2^{2t-1}} & \text{if } \psi \text{ is nonprincipal on } B. \end{cases}$$

Therefore R is a $(2^{4m+1}, 2^{2m+1}, 2^{4m+1}, 2^{2m})$-relative difference set in G relative to B, where B is the unique maximal ideal of GR(4, t).

Remark. If we replace the group W in Theorem 4.6 by any abelian 2-group L, and if there is a bijection $\rho: A \to L$ which maps every translate of $\omega_0^{-1}[1]$ to a difference set in L, then the construction in Theorem 4.6 still works for the group $(\mathrm{GR}(4, t), +) \oplus L$, but it seems difficult to construct such a bijection ρ except in the case $W = (Z_4)^r \oplus (Z_2 \oplus Z_2)^s$, $r + s = m$, $r, s \geqslant 0$.

ACKNOWLEDGMENTS

The authors thank Dr. A. R. Calderbank for his generous help, in particular, the third author thanks Dr. A. R. Calderbank for kindly showing him the proof of Lemma 4.1 which is very important in understanding the Hadamard difference sets $\omega_\gamma^{-1}[1]$. Finally, the first author thanks Professor Henry Glover for his guidance and encouragement.

REFERENCES

1. S. Boztas, R. Hammons, and P. V. Kummar, 4-phase sequences with near-optimum correlation properties, *IEEE Trans. Inform. Theory* **38**, No. 3 (1992), 1101–1113.
2. J. F. Dillon, "Elementary Hadamard Difference Sets," Ph.D. thesis, University of Maryland, 1974.

3. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Sole, The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Trans. Inform. Theory* **40**, No. 2 (1994), 301–319.
4. D. Jungnickel, On automorphism groups of divisible designs, *Canad. J. Math.* **24** (1982), 257–297.
5. S. L. Ma, A survey of partial difference sets, *Designs, Codes and Cryptogr.* **4** (1994), 221–261.
6. B. R. MacDonald, "Finite Rings with Identity," New York, Marcel Dekker, 1974.
7. D. K. Ray-Chaudhuri and Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings, *Designs, Codes and Cryptography* **8** (1996), 215–227.
8. A. Pott, A survey on relative difference sets, *in* "Proceedings, Difference Set Conference," to appear.
9. K. Yamamoto and M. Yamada, Hadamard difference sets over an extension of $Z/4Z$, *Utilitas Math.* **34** (1988), 169–178.