Relative difference sets fixed by inversion
(ii)—character theoretical approach

Wei-Hung Liu\textsuperscript{a,1}, Yu Qing Chen\textsuperscript{b}, K.J. Horadam\textsuperscript{a}

\textsuperscript{a}School of Mathematical and Geospatial Sciences, RMIT-City Campus, GPO Box 2476V, Melbourne, VIC 3001, Australia

\textsuperscript{b}Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435-0001, USA

Received 12 August 2003
Available online 3 June 2005

Abstract

In this paper, we continue our investigation of relative difference sets fixed by inversion. We exclusively focus our attention on abelian groups. New necessary conditions are obtained and a new family of such relative difference sets with forbidden subgroup \( \mathbb{Z}/4\mathbb{Z} \) is constructed. The methods we use are character theory of abelian groups and Galois rings over \( \mathbb{Z}/4\mathbb{Z} \).

© 2004 Elsevier Inc. All rights reserved.

Keywords: Relative difference set; Reversible relative difference set; Forbidden subgroup \( \mathbb{Z}_4 \); Perfect quaternary array

1. Introduction

Let \( G \) be a finite group. A subset \( R \subseteq G \) is called a relative difference set relative to a subgroup \( N < G \) if there exists a constant \( \lambda \) such that

(i) for every element \( g \in G \setminus N \), there are exactly \( \lambda \) pairs of elements \( r_1, r_2 \in R \) such that \( g = r_1 r_2^{-1} \);

(ii) for every \( g \in N \setminus \{1\} \), there exist no elements \( r_1, r_2 \in R \) such that \( g = r_1 r_2^{-1} \).

E-mail addresses: weihung_liu@hotmail.com (W.-H. Liu), yuqing.chen@wright.edu (Y. Chen), horadam@rmit.edu.au (K.J. Horadam).

\textsuperscript{1}This work forms part of the first author’s Ph.D Thesis, taken under the supervision of the second two authors.
In the case where \( N = 1 \), \( R \) is simply called a difference set of \( G \). A relative difference set \( R \) is said to be fixed by inversion, or reversible when \( G \) is abelian, if \( R = R^{(-1)} := \{ r^{-1} \mid r \in R \} \). In the case where \( N \) has order \( n \), \( G \) has order \( mn \), and \( R \) has size \( k \), the relative difference set \( R \) is called an \((m, n, k, \lambda)\)-relative difference set; while if \( N = 1 \), then \( R \) is simply called an \((m, n, k, \lambda)\)-difference set. When \( N \neq 1 \), the subgroup \( N \) is called the forbidden subgroup. An \((m, n, k, \lambda)\)-relative difference set in a group \( G \) gives rise to a \((m, n, k, \lambda)\)-divisible design on which the group \( G \) acts regularly and transitively. The forbidden subgroup is the stabilizer of a point class of the design. When \( n = 1 \), the corresponding design is a symmetric design.

Relative difference sets fixed by inversion have been investigated by Arasu et al. [2], Leung and Ma [11] and Ma [12]. In the first paper of this sequence [5], we discovered a \((30, 2, 29, 14)\)-relative difference set fixed by inversion in the alternating group \( A_5 \) and established connections between relative difference sets fixed by inversion and distance regular graphs. In this paper, we continue our study of these relative difference sets in abelian groups.

Let \( G \) be a finite abelian group and \( \mathbb{Z}[G] \) the group ring of \( G \). For a subset \( S \subset G \), we identify it with the group ring element

\[
\sum_{g \in S} g \in \mathbb{Z}[G]
\]

and denote it again by \( S \). For an element

\[
A = \sum_{g \in G} a_g g \in \mathbb{Z}[G],
\]

we define

\[
A^{(t)} = \sum_{g \in G} a_g g^t \in \mathbb{Z}[G]
\]

for any integer \( t \). With these group ring notations, a subset \( R \) of \( G \) is an \((m, n, k, \lambda)\)-relative difference set in \( G \) relative to a subgroup \( N \) of \( G \) if and only if

\[
RR^{(-1)} = k + \lambda(G - N)
\]

in \( \mathbb{Z}[G] \) and \( R \) is reversible if and only if \( R = R^{(-1)} \).

A character \( \chi \) of an abelian group \( G \) is a homomorphism from \( G \) to the multiplicative group \( \mathbb{C}^* \) of all non-zero complex numbers. The trivial character which maps every element \( g \) in \( G \) to the complex number \( 1 \in \mathbb{C}^* \) is called the principal character. The set of all characters of \( G \) forms a group with the principal character as the identity. This group is called the dual of \( G \) and is denoted by \( \hat{G} \). Every character \( \chi \in \hat{G} \) can be extended to a ring homomorphism from \( \mathbb{Z}[G] \) to \( \mathbb{C} \). By the Fourier inversion formula, two elements \( X \) and \( Y \) in \( \mathbb{Z}[G] \) are equal if and only if \( \chi(X) = \chi(Y) \) for all \( \chi \in \hat{G} \). In terms of characters, relative difference sets in \( G \) relative to a subgroup \( N \) of \( G \) can be characterized as follows.
Lemma 1.1. A subset $R$ in an abelian group $G$ is an $(m, n, k, \lambda)$-relative difference set relative to subgroup $N$ of $G$ if and only if, for any character $\chi \in \hat{G}$,

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

The main results concerning reversible relative difference sets are contained in [2,12] and can be summarized as follows.

Proposition 1.2 (Arasu et al. [2], Ma [12]). Let $R$ be a non-trivial reversible $(m, n, k, \lambda)$-relative difference set in an abelian group $G$ relative to a subgroup $N$ of $G$. Then

(1) $m = k = n\lambda$ is a square, $\lambda$ is even and $n|\lambda$;
(2) $n$ is a power of 2;
(3) $N$ is a direct factor of $G$;
(4) $|R \cap gN| = 1$ for all $g \in G$;
(5) $R(t) = \chi$ for all $t$ relatively prime to $mn$;
(6) if $H$ is a proper subgroup of $N$ of order $h$ and $\rho : G \to G/H$ is the natural epimorphism, then $\rho(R)\chi$ is a non-trivial reversible $(m/n, h, k, \lambda h)$-relative difference set in $G/H$ relative to $N/H$.

According to Proposition 1.2, the parameters of a reversible relative difference set must be of the form

$$(2^{2(s+t)}u^2, 2^t, 2^{2(s+t)}u^2, 2^{2s+t}u^2),$$

where $s \geq 0$, $t \geq 1$, and $u \geq 1$ are integers and $u$ is odd. We may further assume $G$ is of the form $H \times N$ for some abelian group $H$ of order $2^{2(s+t)}u^2$. When $t = 1$, these reversible relative difference sets are intimately related to the so-called Hadamard difference sets. In fact, a transversal $R$ of $N$ in $H \times N$, i.e., $R$ a subset of $H \times N$ which intersects with every coset of $1 \times N$ in $H \times N$ in exactly one element, for $|N| = 2$ and $|H| = 4n^2$ is a $(4n^2, 2, 4n^2, 2n^2)$-relative difference set if and only if $R \cap H$ is a $(4n^2, 2n^2 \pm n, n^2 \pm n)$-Hadamard difference set. For details about Hadamard difference sets and reversible Hadamard difference sets, see [4,10,3]. In this paper, we only consider cases with $t \geq 2$. Our main results are

Theorem 1.3. Let $s \geq 0$ and $t \geq 2$ be two integers. If there exists a reversible $(2^{2(s+t)}u^2, 2^t, 2^{2(s+t)}u^2, 2^{2s+t}u^2)$-relative difference set in a group $G$ relative to a subgroup $N$ of $G$, where $u = p_1^{k_1}p_2^{k_2} \cdots p_l^{k_l}$ is an odd integer and $p_1, p_2, \ldots, p_l$ are its prime divisors, then $2^t$ divides $(p_i^{k_i} - 1)/(p_i - 1)$ for all $i = 1, 2, \ldots, l$. In particular, $k_i$ is even for all $i = 1, 2, \ldots, l$ and $u$ is a perfect square. If we further assume that the exponent $\exp(N) \geq 4$, then $s + t \geq 3$.

Theorem 1.4. Let $m \geq 3$ be an integer. There is a reversible $(2^{2m}, 4, 2^{2m}, 2^{2m-2})$-relative difference set in $\mathbb{Z}_4^{m+1}$. 
Theorem 1.3 enables us to fill all but one missing entry of the table in Ma [12] with negative answers while Theorem 1.4 presents the first known family of reversible relative difference sets with the exponent of the forbidden subgroup exceeding 2.

The rest of the paper is organized as follows. In Section 2 we prove Theorem 1.3. In Section 3 we present a new version of Galois rings over \( \mathbb{Z}/p^2\mathbb{Z} \). Theorem 1.4 is proved in Section 4 while in Section 5, we discuss a connection between our newly constructed relative difference sets and quaternary arrays.

2. Proof of Theorem 1.3

We break the proof of Theorem 1.3 into several lemmas. The first part of the theorem is a strengthened version of a result of Ma [12, p. 430, and Theorem 3.2]. The main ingredients of our proof are from [12]. Let \( R \) be a reversible relative difference set in an abelian group \( G \) relative to a subgroup \( N \) of \( G \). Suppose that \( G = G_1 \times G_2 \) such that \( \gcd(|G_1|, |G_2|) = 1 \).

If the group \( G_2 = \{v_1, v_2, \ldots, v_{|G_2|}\} \), we can decompose \( R \) and get

\[
R = v_1 A_1 + v_2 A_2 + \cdots + v_{|G_2|} A_{|G_2|},
\]

where \( A_1, A_2, \ldots, A_{|G_2|} \) are subsets of \( G_1 \). Then we have

Lemma 2.1.

\[
A_i = A_i^{(t)}
\]

for every \( t \) relatively prime to \( |G_1| \) and all \( i = 1, 2, \ldots, |G_2| \).

Proof. For every character \( \chi \in \hat{G}_1 \), let \( \varphi_1, \varphi_2, \ldots, \varphi_{|G_2|} \) be all characters of \( G_2 \), and let \( \chi_i = \chi \varphi_i \), for every \( i = 1, 2, \ldots, |G_2| \), then

\[
\chi_i(R) = \sum_{i=1}^{|G_2|} \varphi_j(v_i) \chi(A_i) \in \mathbb{Z}.
\]

Let

\[
M = \begin{pmatrix}
\varphi_1(v_1) & \varphi_1(v_2) & \cdots & \varphi_1(v_{|G_2|}) \\
\varphi_2(v_1) & \varphi_2(v_2) & \cdots & \varphi_2(v_{|G_2|}) \\
\vdots & \vdots & \ddots & \vdots \\
\varphi_{|G_2|}(v_1) & \varphi_{|G_2|}(v_2) & \cdots & \varphi_{|G_2|}(v_{|G_2|})
\end{pmatrix}.
\]

Then

\[
M \begin{pmatrix}
\chi(A_1) \\
\chi(A_2) \\
\vdots \\
\chi(A_{|G_2|})
\end{pmatrix} = \begin{pmatrix}
\chi_1(R) \\
\chi_2(R) \\
\vdots \\
\chi_{|G_2|}(R)
\end{pmatrix}.
\]
Therefore
\[
\begin{pmatrix}
\chi(A_1) \\
\chi(A_2) \\
\vdots \\
\chi(A_{|G_2|})
\end{pmatrix} = \frac{1}{|G_2|} \overline{M}^\top \begin{pmatrix}
\chi_1(R) \\
\chi_2(R) \\
\vdots \\
\chi_{|G_2|}(R)
\end{pmatrix},
\tag{1}
\]
where \(\overline{M}\) consists of the complex conjugates of the entries of \(M\) and \(\overline{M}^\top\) is its transpose. Since the entries on the right of (1) are in \(\mathbb{Z}[\xi_{|G_1|}]\) while those on the left are in \(\mathbb{Z}[\xi_{|G_2|}]\), where \(\xi_{|G_1|}\) and \(\xi_{|G_2|}\) are primitive \(|G_1|\)-th and \(|G_2|\)-th complex roots of unity respectively, and \(\gcd(|G_1|, |G_2|) = 1\), we get
\[
\chi(A_i) \in \mathbb{Z}[\xi_{|G_1|}] \cap \mathbb{Z}[\xi_{|G_2|}] = \mathbb{Z}
\]
for all \(i = 1, 2, \ldots, |G_2|\). \(\square\)

We include the following lemma for the convenience of the reader.

**Lemma 2.2** (Ma [12, Lemma 3.4]). Let \(a, b, c, r\) be non-negative integers with \(a = br + c\) and \(0 \leq c \leq r - 1\). If \(a_1, a_2, \ldots, a_r\) are \(r\) non-negative integers such that \(a_1 + a_2 + \cdots + a_r = a\), then
\[
a_1^2 + a_2^2 + \cdots + a_r^2 \geq b^2(r - c) + (b + 1)^2c,
\]
with equality if and only if \(|a_i : a_i = b + 1| = c\) and \(|a_i : a_i = b| = r - c\).

The next lemma improves Ma [12, p. 430, and Theorem 3.2] and the first part of Theorem 1.3 follows immediately.

**Lemma 2.3.** Suppose there exists a reversible \((2^{2(s+t)}u^2, 2^t, 2^{2(s+t)}u^2, 2^{2s+t}u^2)\)-relative difference set \(R\) in a group \(G = H \times N\) relative to \(N\), where \(s > 0\) and \(t \geq 2\) and \(u\) is odd. Let \(p\) be a prime divisor of \(u\). We can write \(u = pk^\top u_0\) with \(\gcd(p, u_0) = 1\). Then

(i) \((p^k - 1)/(p - 1) \equiv 0 \pmod{2^t}\);

(ii) if \(H_0\) is the subgroup in \(H\) of order \(2^{2(s+t)}u_0^2\), then \(R \cap (H_0 \times N)\) is a reversible \((2^{2(s+t)}u_0, 2^t, 2^{2(s+t)}u_0, 2^{2s+t}u_0)\)-relative difference set in \(H_0 \times N\) relative to \(N\).

**Proof.** Let \(H = H_0 \times P\), where \(P\) is the Sylow-\(p\) subgroup of \(H\). Suppose that \(H_0 \times N = \{v_1, v_2, \ldots, v_{|H_0|N}\}\), where \(|H_0N| = 2^{2s+3t}u_0^2\). Then \(R\) can be written as
\[
R = v_1A_1 + v_2A_2 + \cdots + v_{|H_0|N}A_{|H_0|N},
\]
where \(A_1, A_2, \ldots, A_{|H_0|N}\) are subsets of \(P\). Since
\[
RR^{-1} = 2^{2(s+t)}u^2 + 2^{2s+t}u^2(HN - N),
\]
we have
\[
\chi(R) = \chi(R)\chi(R^{-1}) = \chi(R)^2.
\]
Therefore, if \(\chi(R) = \chi(R)^2\), then \(\chi(R) = 0\) or \(\chi(R) = 1\).

We denote the conjugates of \(H\) and \(N\) by \(H^\prime\) and \(N^\prime\), respectively. Then
\[
\chi(R) \in \mathbb{Z}[\xi_{|H|}] \cap \mathbb{Z}[\xi_{|N|}] = \mathbb{Z}
\]
for all \(i = 1, 2, \ldots, |H_0|\). \(\square\)
if we let \( \rho : H \times N \to H_0 \times N \) be the natural projection, then we have

\[
\rho(R) = v_1|A_1| + v_2|A_2| + \cdots + v_{|H_0N|}|A_{H_0N}|, \\
\rho(R)\rho(R)^{(-1)} = 2^{(s+t)}u_0^2p^{2k} + 2^{s+t}u_0^2(p^{2k}H_0N - N).
\]

(2)

(3)

Since \( \chi(R) = 0 \) or \( \pm 2^{s+t}u_0p^k \) for every non-principal character \( \chi \) of \( G \) and \( \gcd(p, |H_0 \times N|) = 1 \), we infer, by the Fourier inversion formula, that \( p^k|A_i| \) for all \( i = 1, 2, \ldots, \ |H_0N| \). From (3), we have

\[
\left\{ \begin{array}{l}
\sum_{i=1}^{|H_0N|} |A_i|/p^k = 2^{(s+t)}u_0^2p^k, \\
\sum_{i=1}^{|H_0N|} (|A_i|/p^k)^2 = 2^{(s+t)}u_0^2 + 2^{s+t}u_0^2(p^{2k} - 1).
\end{array} \right.
\]

Let \( p^k = \alpha t + \beta \), where \( 1 \leq \beta \leq 2t - 1 \). By Lemma 2.2,

\[
\alpha^2(2^{2s+3t}u_0^2 - \beta 2^{(s+t)}u_0^2) + (\alpha + 1)^2 \beta 2^{(s+t)}u_0^2 \\
\leq 2^{(s+t)}u_0^2 + 2^{s+t}u_0^2((\alpha t + \beta)^2 - 1),
\]

(4)

which implies \( \beta^2 - \beta 2t + 2t - 1 \geq 0 \). The only possible solutions are \( \beta = 1 \) or \( \beta = 2t - 1 \). Both cases give us an equality of (4). Thus we conclude that \( |A_i| = \alpha p^k \) or \( (\alpha + 1)p^k \) for all \( i = 1, 2, \ldots, |H_0N| \). By Lemma 2.1, the size \( |A_i| \) is odd if and only if \( 1 \in A_i \). The number of sets of \( A_i \)’s with \( |A_i| \) odd is \( |H_0| = 2^{2(s+t)}u_0^2 \) because it is equal to \( |R \in (H_0 \times N) | \) and \( R \cap (H_0 \times N) \) is a transversal in \( H_0 \times N \) with respect to \( N \) since \( R \) is a transversal in \( H \times N \) with respect to \( N \). When \( |A_i| \) is even, we have \( (p - 1)| |A_i| \) because \( A_i^{(t)} = A_i \) for all \( \gcd(t, p) = 1 \).

If \( \beta = 2t - 1 \), then \( \rho(R) = \alpha p^k R_1 + (\alpha + 1)p^k R_2 \), where \( R_1 \) and \( R_2 \) form a partition of \( H_0 \times N \). Note that \( t \geq 2 \) and, by Lemma 2.2, \( |R_1| = |H_0| \), we have \( (p - 1)(\alpha + 1)p^k = (p^k + 1)p^k/2t \), which is impossible. Hence \( \beta = 1 \) and \( |R_2| = |H_0| \) and \( (p - 1)| \alpha p^k = (p^k - 1)p^k/2t \), or equivalently, \( 2^t(p^k - 1)/(p - 1) \). Also direct calculation shows that \( R_2 = R \cap (H_0 \times N) \) is a \( (2^{2(s+t)}u_0^2, 2t, 2^{2(s+t)}u_0^2, 2^{2s+t}u_0^2) \)-relative difference set in \( H_0 \times N \) relative to \( N \).

For the second part of Theorem 1.3, it suffices to prove the case \( t = 2 \). Let \( n = 2^{s+1}u \) and \( N = \langle x \rangle \cong \mathbb{Z}_4 \). Then a \( (4n^2, 4, 4n^2, n^2) \)-relative difference set \( R \) in \( G = H \times N \) relative to \( N \) can be written as

\[
R = R_0 + R_1x + R_2x^2 + R_3x^3,
\]

where \( R_0, R_1, R_2 \) and \( R_3 \) are subsets of \( H \) which form a partition of \( H \). The next lemma computes the character values of \( R_0, R_1, R_2 \) and \( R_3 \) when \( N \cong \mathbb{Z}_4 \) and the second part of Theorem 1.3 is a direct consequence of this lemma.

Lemma 2.4. The set \( R \) is a reversible \( (4n^2, 4, 4n^2, n^2) \)-relative difference set in \( G = H \times N \) relative to \( N \cong \mathbb{Z}_4 \) if and only if

(i) \( R_0 = R_0^{(-1)}, R_2 = R_2^{(-1)} \) and \( R_1 = R_1^{(-1)} \).
(ii) \( |R_0|, |R_2| = \{ n^2 \mp 3n/2, n^2 \pm n/2 \} \) and \( |R_1| = |R_3| = n^2 \mp n/2 \), and
(iii) \( R_1 + R_2 \) and \( R_1 + R_3 \) are Hadamard difference sets and \( \chi(R_1 + R_2) = \pm n \) or \( \pm n\sqrt{-1} \) for every non-principal character \( \chi \in \hat{H} \).

**Proof.** If \( R \) is a reversible relative difference set, then statement (i) is obvious while statement (ii) can be obtained from the 4 characters which are principal on \( H \), since \( R_0 + R_2 \) and \( R_1 + R_3 \) are reversible Hadamard difference sets and \( R_0 + R_1 + R_2 + R_3 = H \). For (iii), since \( R\hat{R}(\hat{R})^{-1} = R^2 = 4n^2 + n^2(G - N) = 4n^2 + n^2(H - 1)N \), we have

\[
R_0^2 + R_2^2 + 2R_1R_3 = 4n^2 + n^2(H - 1),
\]
\[
2R_0R_1 + 2R_2R_3 = n^2(H - 1),
\]
\[
2R_0R_2 + R_1^2 + R_3^2 = n^2(H - 1),
\]
\[
2R_0R_3 + 2R_1R_2 = n^2(H - 1).
\]

From (5)–(7) and (6)–(8), we get

\[
(R_0 - R_2)^2 = 4n^2 + (R_1 - R_3)^2,
\]
\[
(R_0 - R_2)(R_1 - R_3) = 0.
\]

Let \( \chi \in \hat{H} \) be a non-principal character. Then either \( \chi(R_0 - R_2) = 0 \) and \( \chi(R_1 - R_3) = \pm 2n\sqrt{-1} \), or \( \chi(R_0 - R_2) = \pm 2n \) and \( \chi(R_1 - R_3) = 0 \). Statement (iii) follows from the fact that \( \chi(R_0 + R_2) = \pm n \) and \( \chi(R_1 + R_3) = \mp n \). The converse follows from straightforward character computations. \( \square \)

Since \( \chi^2R \) is also a reversible \((4n^2, 4, 4n^2, n^2)\)-relative difference set in \( G = H \times N \) relative \( N \) whenever \( R \) is, we can, without loss of generality, assume that \( |R_1| = |R_2| = |R_3| \).

**Corollary 2.5.** If \( R = R_0 + R_1x + R_2x^2 + R_3x^3 \) is a reversible \((4n^2, 4, 4n^2, n^2)\)-relative difference set in \( G = H \times N \) relative to \( N \), where \( N = \langle x \rangle \cong \mathbb{Z}_4 \), and \( |R_1| = |R_2| = |R_3| \), then

\[
(R_1 + R_2)^2 = 3(n^2 + (n^2 \pm n)H)/2 - 2R_1R_3
\]

and \( n \) must be a multiple of 4.

**Proof.** The character values of \( R_0, R_1, R_2 \) and \( R_3 \) can be explicitly obtained from the Proof of Lemma 2.4 and (11) can be easily verified with these character values. Suppose \( n = 4k + 2 \), by (11), we have

\[
R_1^{(2)} + R_2^{(2)} \equiv (R_1 + R_2)^2 \equiv H \pmod{2}
\]

which is impossible because the map \( x \to x^2 \) from \( H \) to itself is not surjective as \( |H| \) is even. Hence \( n \) is a multiple of 4. \( \square \)
3. Galois rings over $\mathbb{Z}/p^2\mathbb{Z}$

In this section, we provide background material on Galois rings over $\mathbb{Z}/p^2\mathbb{Z}$ which will be used in the next section to construct reversible relative difference sets. We will use Cartesian coordinates instead of $p$-adic notations to represent elements in these Galois rings. The advantage of our presentation is that the arithmetic operations in the Galois rings can be made explicit, which in turn makes computation more transparent. The equivalence of our notation and the $p$-adic ones in [13,16] is left to the reader to fill in.

Let $q = p^n$, where $p$ is a prime. Let $\mathbb{F}_q$ be the finite field of order $q$. The Frobenius automorphism is denoted by $\sigma$, that is $\sigma(x) = x^p$ for all $x \in \mathbb{F}_q$. The inverse automorphism of $\sigma$ is denoted by $\frac{1}{p\sqrt{-1}}$. We define

$$\psi_p(x, y) = ((x + y)^p - x^p - y^p)/p.$$  

Note that $\psi_p(x, y)$ is a polynomial with integer coefficients. The Galois ring over $\mathbb{Z}/p^2\mathbb{Z}$ with residue field $\mathbb{F}_q$, denoted by $\text{GR}(\mathbb{F}_q)$, is defined to be $\mathbb{F}_q \times \mathbb{F}_q$ equipped with the following addition and multiplication,

$$(a, b) + (c, d) = (a + c, b + d - \frac{\sqrt{\psi_p(a, c)}}{p}),$$

$$(a, b)(c, d) = (ac, ad + bc), a, b, c, d \in \mathbb{F}_q.$$  

For instance, if $p = 2$ then $\psi_2(x, y) = xy$ and the addition in $\text{GR}(\mathbb{F}_q)$ is given by

$$(a, b) + (c, d) = (a + c, b + d - \sqrt{ac}) = (a + c, b + d + \sqrt{ac}).$$

From [7, Section 4.1], the additive group $(\text{GR}(\mathbb{F}_q), +)$ is isomorphic to $(\mathbb{Z}/p^2\mathbb{Z})^n$. If we let

$$M = \{(0, x) \mid x \in \mathbb{F}_q\} \quad \text{and} \quad T = \{(x, 0) \mid x \in \mathbb{F}_q\},$$

then $M$ is the unique maximal ideal of $\text{GR}(\mathbb{F}_q)$ and $\text{GR}(\mathbb{F}_q)/M \cong \mathbb{F}_q$, and $T$ is the Teichmuller system of $\text{GR}(\mathbb{F}_q)$, i.e. $T$ is a set of representatives of cosets in $\text{GR}(\mathbb{F}_q)/M$ and $T^* = T \setminus \{(0, 0)\}$ forms a multiplicative subgroup which is isomorphic to the multiplicative group of the residue field $\mathbb{F}_q^* = \mathbb{F}_q^\times \setminus \{0\}$. When $n = 1$, there is a unique ring isomorphism between $\text{GR}(\mathbb{F}_p)$ and $\mathbb{Z}/p^2\mathbb{Z}$ which takes the identity $(1, 0)$ to $1$. Using this isomorphism, we can calculate, for a fixed complex primitive $p^2$th root of unity $\xi_{p^2}$, the value of $\zeta_{p^2}^{(x,y)}$ for every $(x, y) \in \text{GR}(\mathbb{F}_p)$. Also note that $p(1, 0) = (0, 1)$, hence we have

$$\zeta_{p^2}^{(x,y)} = \zeta_{p^2}^{(x,0) + (0,y)} = \zeta_{p^2}^{(x,0)} \zeta_{p^2}^{y},$$

where $\zeta_{p^2} = \xi_{p^2}^p$ is a primitive $p$th root of unity.

Let $n' | n$ and $q' = p^{n'}$. Then $\mathbb{F}_q$ is a Galois extension of $\mathbb{F}_{q'}$ and there is a trace map $\text{tr}_{q'/q'} : \mathbb{F}_q \rightarrow \mathbb{F}_{q'}$ defined by

$$\text{tr}_{q'/q'}(x) = \sum_{i=1}^{n/n'} x^{q'^i}.$$
for every \( x \in \mathbb{F}_q \). Similarly, \( GR(\mathbb{F}_q) \) is a Galois extension of \( GR(\mathbb{F}_{q'}) \) and the trace map \( \text{Tr}_{q/q'} : GR(\mathbb{F}_q) \to GR(\mathbb{F}_{q'}) \) is defined by

\[
\text{Tr}_{q/q'}((x, y)) = \sum_{i=1}^{n/n'} (x^{q^i}, y^{q^i})
\]

for every \((x, y) \in \mathbb{GR}(\mathbb{F}_q)\). When \( n' = 1 \), the trace maps \( tr_{q/p} \) and \( \text{Tr}_{q/p} \) are called absolute trace maps and denoted by \( tr \) and \( \text{Tr} \), respectively.

We end this section with a description of characters of additive groups of \( \mathbb{F}_q \) and \( GR(\mathbb{F}_q) \) which can be found in [16].

**Lemma 3.1** (Yamamoto and Yamada [16]). All additive characters \( \chi_y \) of \( \mathbb{F}_q \), \( y \in \mathbb{F}_q \), are given by

\[
\chi_y(x) = \xi_{p}^{\text{tr}(xy)}, \quad x \in \mathbb{F}_q,
\]

where \( \xi_{p} \) is a primitive \( p \)th root of unity.

All additive characters \( \chi_{\beta} \) of \( GR(\mathbb{F}_q) \), \( \beta \in GR(\mathbb{F}_q) \), are given by

\[
\chi_{\beta}(x) = \xi_{p^2}^{\text{Tr}(\beta x)}, \quad x \in GR(\mathbb{F}_q),
\]

where \( \xi_{p^2} \) is a primitive \( p^2 \)th root of unity.

4. Proof of Theorem 1.4

This section is devoted to prove Theorem 1.4. We use Lemma 2.4 together with the Galois rings to explicitly construct reversible \((2^{2m}, 4, 2^{2m}, 2^{2m}-2)\)-relative difference sets in \( (\mathbb{Z}/4\mathbb{Z})^{m+1} \) for all \( m \geq 3 \). We begin with the following rather trivial lemma.

**Lemma 4.1.** Let \( \mathbb{F} \) be a finite field of characteristic \( 2 \) with \( |\mathbb{F}| \geq 8 \). Then there exist three distinct non-zero elements \( a, b_1 \) and \( b_2 \) in \( \mathbb{F} \) such that \( \text{tr}(b_1) = 1 \), \( \text{tr}(a) = \text{tr}(b_2) = \text{tr}(a(b_1 + b_2)) = 0 \).

**Proof.** Let \( 0 \neq a \in \mathbb{F} \) such that \( \text{tr}(a) = 0 \). Let \( H_0 = \{ x \in \mathbb{F} | \text{tr}(x) = 0 \} \) and \( H = \{ x \in \mathbb{F} | \text{tr}(ax) = 0 \} \). The intersection of \( H \) with the complement of \( H_0 \) is not empty as long as \( |\mathbb{F}| > 2 \). Choose an element \( c \) in the intersection. Then \( \text{tr}(c) = 1 \) and \( \text{tr}(ac) = 0 \). Since \( |\mathbb{F}| \geq 8 \), the size \( |H_0| \geq 4 \). Therefore we can find an element \( b_2 \in H_0 \) such that \( b_2 \neq 0 \) and \( b_2 \neq a \). Let \( b_1 = c + b_2 \). Clearly, \( a, b_1 \) and \( b_2 \) are the required elements in \( \mathbb{F} \). \( \square \)

Let \( \mathbb{F}, a, b_1 \) and \( b_2 \) be as in Lemma 4.1. We define

\[
H = \{ x \in \mathbb{F} | \text{tr}(ax) = 0 \},
\]

\[
K_1 = \{ x \in \mathbb{F} | \text{tr}(ax) = \text{tr}(b_1x) = 0 \},
\]

\[
K_2 = \{ x \in \mathbb{F} | \text{tr}(ax) = \text{tr}(b_2x) = 0 \}.
\]
From our choices of $a$, $b_1$ and $b_2$, it is clear that $1 \in K_2 \subset H$ and $K_1 \subset H$ but $1 \notin K_1$. For any $\omega \notin H$, we can use $H$, $K_1$ and $K_2$ to partition the Galois ring $GR(\mathbb{F})$ by letting

$$R_1 = \{(g, gx) \in GR(\mathbb{F}) | g \in \mathbb{F}^*, x \in K_1\},$$
$$R_2 = \{(g, gx) \in GR(\mathbb{F}) | g \in \mathbb{F}^*, x \in K_2 + \omega\},$$
$$R_3 = \{(g, gx) \in GR(\mathbb{F}) | g \in \mathbb{F}^*, x \in K_1 + 1\}
$$

and

$$R_0 = GR(\mathbb{F}) - R_1 - R_2 - R_3,$$

where $\mathbb{F}^* = \mathbb{F}\setminus\{0\}$. It can be easily checked that $|R_1| = |R_2| = |R_3| = (|F|^2 - |\mathbb{F}|)/4$, $|R_0| = (|\mathbb{F}|^2 + 3|\mathbb{F}|)/4$, $R_2(-1) = R_2$, $R_0(-1) = R_0$ and $R_1(-1) = R_3$. The next several lemmas show that $R_0$, $R_1$, $R_2$ and $R_3$ satisfy Lemma 2.4 (iii) and, therefore, there is a reversible $(2^m, 4, 2^m, 2^{2m-2})$-relative difference set in $GR(\mathbb{F}) \times \mathbb{Z}/4\mathbb{Z}$.

We first prove that $R_1 + R_2$ is an Hadamard difference set in $GR(\mathbb{F})$ and has the correct character values as specified in Lemma 2.4 (iii). We then show that $R_1 + R_3$ is a reversible Hadamard difference set in $GR(\mathbb{F})$.

**Lemma 4.2.** The set $R_1 + R_2$ is an Hadamard difference set in $GR(\mathbb{F})$ and for every non-principal character $\chi$ of $GR(\mathbb{F})$, $\chi(R_1 + R_2) = \pm \frac{|\mathbb{F}|}{2}$ or $\pm \frac{|\mathbb{F}|}{2} \sqrt{-1}$.

**Proof.** For every $(g_1, g_2) \in GR(\mathbb{F})$, we have

$$Z_{(g_1,g_2)}(R_1 + R_2) = \sum_{g \in \mathbb{F}^*, x \in K_1} \sqrt{-1} \text{tr}((g_1, g_2)(g, gx)) + \sum_{g \in \mathbb{F}^*, x \in K_2} \sqrt{-1} \text{tr}((g_1, g_2)(g, g(x + \omega)))$$

$$= \sum_{g \in \mathbb{F}^*, x \in K_1} \sqrt{-1} \text{tr}((g_1, g)x + g_2)) + \sum_{g \in \mathbb{F}^*, x \in K_2} \sqrt{-1} \text{tr}((g_1, g)(g, x + g_1 \omega + g_2)).$$

If $g_1 = g_2 = 0$, then $Z_{(0,0)}$ is the principal character of $GR(\mathbb{F})$ and

$$Z_{(0,0)}(R_1 + R_2) = |R_1| + |R_2| = (|\mathbb{F}|^2 - |\mathbb{F}|)/2.$$

If $g_1 = 0$ and $g_2 \neq 0$, then

$$Z_{(0,g_2)}(R_1 + R_2) = \sum_{g \in \mathbb{F}^*, x \in K_1} \sqrt{-1} \text{tr}((0, g_2g)) + \sum_{g \in \mathbb{F}^*, x \in K_2} \sqrt{-1} \text{tr}((0, g_2g))$$

$$= \sum_{g \in \mathbb{F}^*, x \in K_1} (-1)^{\text{tr}(g_2)} + \sum_{g \in \mathbb{F}^*, x \in K_2} (-1)^{\text{tr}(g_2)}$$

$$= \sum_{g \in \mathbb{F}^*, x \in K_1} (-1)^{\text{tr}(g)} + \sum_{g \in \mathbb{F}^*, x \in K_2} (-1)^{\text{tr}(g)}$$

$$= -|K_1| - |K_2|$$

$$= -|\mathbb{F}|/2.$$
If $g_1 \neq 0$, note that $|K_1| = |K_2| = |\mathbb{F}|/4$ and $(-1)^{tr(a\omega)} = -1$, then

$$
\chi_{(g_1, g_2)}(R_1 + R_2) = \sum_{g \in \mathbb{F}^*, x \in K_1} \sqrt{-1}^\text{Tr}((gg_1, 0) + (0, g(g_1x + g_2)) \\
+ \sum_{g \in \mathbb{F}^*, x \in K_2} \sqrt{-1}^\text{Tr}((gg_1, 0) + (0, g(g_1x + g_1\omega + g_2))

= \sum_{g \in \mathbb{F}^*, x \in K_1} \sqrt{-1}^\text{Tr}((gg_1, 0) (-1) \text{tr}(g(g_1x + g_2)) \\
+ \sum_{g \in \mathbb{F}^*, x \in K_2} \sqrt{-1}^\text{Tr}((gg_1, 0) (-1) \text{tr}(g(g_1x + g_1\omega + g_2))

= \sum_{g \in \mathbb{F}^*, x \in K_1} \sqrt{-1}^\text{Tr}((g, 0)) (-1) \text{tr}(g(x + g_1^{-1}g_2)) \\
+ \sum_{g \in \mathbb{F}^*, x \in K_2} \sqrt{-1}^\text{Tr}((g, 0)) (-1) \text{tr}(g(x + \omega + g_1^{-1}g_2))

= \sum_{g \in \mathbb{F}^*} \sqrt{-1}^\text{Tr}((g, 0)) (-1) \text{tr}(gg_1^{-1}g_2) \left( \sum_{x \in K_1} (-1)^{tr(gx)} \right) \\
+ \sum_{g \in \mathbb{F}^*} \sqrt{-1}^\text{Tr}((g, 0)) (-1) \text{tr}(g(\omega + g_1^{-1}g_2)) \left( \sum_{x \in K_2} (-1)^{tr(gx)} \right)

= \sum_{g \in \{a, b_1, a+b_1\}} \sqrt{-1}^\text{Tr}((g, 0)) (-1) \text{tr}(gg_1^{-1}g_2) |K_1| \\
+ \sum_{g \in \{a, b_2, a+b_2\}} \sqrt{-1}^\text{Tr}((g, 0)) (-1) \text{tr}(g_1^{-1}g_2) (-1)^{tr(\omega)} |K_2|

= \sum_{g \in \{b_1, a+b_1\}} \sqrt{-1}^\text{Tr}((g, 0)) (-1) \text{tr}(gg_1^{-1}g_2) \left| \mathbb{F} \right|/4 \\
+ \sum_{g \in \{b_2, a+b_2\}} \sqrt{-1}^\text{Tr}((g, 0)) (-1) \text{tr}(g_1^{-1}g_2) (-1)^{tr(\omega)} \left| \mathbb{F} \right|/4.

On the other hand, by setting $g^* = g_1^{-1}g_2$, one has

$$
\sum_{g \in \{b_1, a+b_1\}} \sqrt{-1}^\text{Tr}((g, 0)) (-1)^{tr(g_1^{-1}g_2)) \\
= \sqrt{-1}^\text{Tr}((b_1, 0)) (-1)^{tr(b_1g^*)} + \sqrt{-1}^\text{Tr}((a+b_1, 0)) (-1)^{tr((a+b_1)g^*)}

= \sqrt{-1}^\text{Tr}((b_1, 0)) (-1)^{tr(b_1g^*)} (1 + \sqrt{-1}^\text{Tr}((a+b_1, 0) - (b_1, 0)) (-1)^{tr(\omega g^*)})

= \sqrt{-1}^\text{Tr}((b_1, 0)) (-1)^{tr(b_1g^*)} (1 + \sqrt{-1}^\text{Tr}((a, b_1 + \sqrt{(a+b_1)b_1})) (-1)^{tr(\omega g^*)}).

\[ \text{Proof.} \]

For every \( \sum \) and \( g \)

\[ \text{Then} \quad \sqrt{-1}^{\text{Tr}((b_1, 0))} (-1)^{\text{tr}(b_1 g^* + \omega (g_1^{-1} g_2 + \omega))} \]

\[ = \sqrt{-1}^{\text{Tr}((b_1, 0))} (-1)^{\text{tr}(b_1 g^*)} (1 + \sqrt{-1}^{\text{Tr}((a, 0) + (g_1^{-1} g_2 + \omega))} (-1)^{\text{tr}(g^*)}) \]

\[ = \sqrt{-1}^{\text{Tr}((b_1, 0))} (-1)^{\text{tr}(b_1 g^*)} (1 + \sqrt{-1}^{\text{Tr}((a, 0))} (-1)^{\text{tr}(ab_1)} (-1)^{\text{tr}(g^*)}) \]

and

\[ \sum_{g \in \{b_2, a + b_2\}} \sqrt{-1}^{\text{Tr}((g, 0))} (-1)^{\text{tr}(g(g_1^{-1} g_2 + \omega))} \]

\[ = \sqrt{-1}^{\text{Tr}((b_2, 0))} (-1)^{\text{tr}(b_2 (g^* + \omega))} + \sqrt{-1}^{\text{Tr}((a + b_2, 0))} (-1)^{\text{tr}((a + b_2, 0))} (-1)^{\text{tr}(g^*)} \]

\[ = \sqrt{-1}^{\text{Tr}((b_2, 0))} (-1)^{\text{tr}(b_2 (g^* + \omega))} (1 - \sqrt{-1}^{\text{Tr}((a + b_2, 0))} (-1)^{\text{tr}(g^*)}) \]

\[ = \sqrt{-1}^{\text{Tr}((b_2, 0))} (-1)^{\text{tr}(b_2 (g^* + \omega))} (1 - \sqrt{-1}^{\text{Tr}((b_2, 0))} (-1)^{\text{tr}(g^*)}) \]

\[ = \sqrt{-1}^{\text{Tr}((b_2, 0))} (-1)^{\text{tr}(b_2 (g^* + \omega))} (1 - \sqrt{-1}^{\text{Tr}((a, 0))} (-1)^{\text{tr}(ab_2)} (-1)^{\text{tr}(g^*)}) \]

Since \( \text{tr}(a (b_1 + b_2)) = 0 \), we have \( (-1)^{\text{tr}(ab_1)} = (-1)^{\text{tr}(ab_2)} \). Let

\[ \varepsilon = \sqrt{-1}^{\text{Tr}((a, 0))} (-1)^{\text{tr}(ab_1)} (-1)^{\text{tr}(g^*)} = \sqrt{-1}^{\text{Tr}((a, 0))} (-1)^{\text{tr}(ab_2)} (-1)^{\text{tr}(g^*)}. \]

Then \( \varepsilon^2 = (-1)^{\text{tr}(a)} = 1 \) and hence \( \varepsilon = \pm 1 \). Therefore

\[ \chi_{(g_1, g_2)}(R_1 + R_2) = \begin{cases} \sqrt{-1}^{\text{Tr}((b_1, 0))} (-1)^{\text{tr}(b_1 g^*)}|F|/2 & \text{if } \varepsilon = 1, \\ \sqrt{-1}^{\text{Tr}((b_2, 0))} (-1)^{\text{tr}(b_2 (g^* + \omega))}|F|/2 & \text{if } \varepsilon = -1. \end{cases} \]

**Lemma 4.3.** The set \( R_1 + R_3 \) is an Hadamard difference set in \( \text{GR}(F) \).

**Proof.** For every \( (g_1, g_2) \in \text{GR}(F) \), we have

\[ \chi_{(g_1, g_2)}(R_1 + R_3) = \sum_{g \in F^*, x \in K_1} \sqrt{-1}^{\text{Tr}((g_1, g_2)(g, gx))} \]

\[ + \sum_{g \in F^*, x \in K_1} \sqrt{-1}^{\text{Tr}((g_1, g_2)(g, g(x + 1)))} \]

\[ = \sum_{g \in F^*, x \in H} \sqrt{-1}^{\text{Tr}(gg_1 g_1 x + g_2)} . \]

If \( g_1 = g_2 = 0 \), then

\[ \chi_{(g_1, g_2)}(R_1 + R_3) = |R_1| + |R_3| = (|F|^2 - |F|)/2. \]

If \( g_1 = 0 \) and \( g_2 \neq 0 \), then

\[ \chi_{(g_1, g_2)}(R_1 + R_3) = \sum_{g \in F^*, x \in H} \sqrt{-1}^{\text{Tr}((0, gg_2))} . \]
\[
\sum_{g \in F^*, x \in H} (-1)^{tr(gg^*)} = \sum_{g \in F^*, x \in H} (-1)^{tr(g)} = -|H| = -|F|/2.
\]

If \( g_1 \neq 0 \), let \( g^* = g_1^{-1} g_2 \), then
\[
\chi_{(g_1, g_2)}(R_1 + R_3) = \sum_{g \in F^*, x \in H} \sqrt{-1}^{tr((g.g(x+g^*)))} = \sum_{g \in F^*, x \in H} \sqrt{-1}^{tr((g.0)) + tr((0,gx+gg^*)))}
\]
\[
= \sum_{g \in F^*, x \in H} \sqrt{-1}^{tr((g.0))} (-1)^{tr(gg^*)} (-1)^{tr(gx)} = \sum_{g \in F^*, x \in H} \sqrt{-1}^{tr((a,0))} (-1)^{tr(\overline{ag^*})} |H|
\]
\[
= \sqrt{-1}^{tr((a,0))} (-1)^{tr(\overline{ag^*})} |F|/2.
\]

5. Construction of perfect quaternary arrays from RDS in \( H \times N \) with forbidden subgroup \( N = \mathbb{Z}_4 \)

Perfect quaternary arrays (PQA) can be used for sequence design for 4-phase digital signals with good correlation. We refer the reader to [1,8] for more detail.

Definition 5.1. Let \( H \cong \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_n} \), and let \( N = \{\pm 1, \pm \sqrt{-1}\} \subset \mathbb{C} \), so \( N \cong \mathbb{Z}_4 \). A set map \( \phi : H \to N \) is a perfect quaternary array (PQA) if \( 1 \neq g \in H \) implies
\[
\sum_{h \in H} \phi(h) \overline{\phi(hg)} = 0.
\]

If \( n = 1 \) then \( \phi \) is a perfect quaternary sequence. The PQA is flat if the list \( \phi(h) \overline{\phi(hg)} \), \( h \in H \), contains each of the four elements \( \pm 1, \pm \sqrt{-1} \) an equal number of times.

Not many examples of PQA are known. Perfect quaternary sequences exist for \( s_1 = 4, 8, 16 \) and it is conjectured that these are the only values possible. Some non-flat examples of PQA with \( n = 2 \) are given in [1].

A PQA corresponds to a complex Hadamard matrix [1], while a flat PQA corresponds to a generalized Hadamard matrix with entries in \( N \) and also to an ordinary Hadamard matrix.
of twice the size [8]. A PQA which is flat is equivalent to a semiregular RDS with respect to a forbidden subgroup isomorphic to $\mathbb{Z}_4$.

**Lemma 5.2.** Let $|H| = m$ and let $\phi : H \rightarrow N$ be a set map. Then $\phi$ is a flat PQA if and only if $R = \{(h, \phi(h)) : h \in H\}$ is a $(m, 4, m/4)$-RDS in $H \times N$ relative to $\{1\} \times N$. In this case, $\phi(h^{-1}) = \phi(h)^{-1}$, $h \in H$ if and only if $R$ is reversible.

**Proof.**

$$R R^{(-1)} = \sum_{h \in H} \left( \sum_{k \in H} (hk^{-1}, \phi(h)\phi(k)) \right)$$

$$= m(1, 1) + \sum_{1 \neq g \in H} \left( \sum_{h \in H} (g^{-1}, \phi(h)\phi(gh)) \right)$$

and $\sum_{h \in H} (g^{-1}, \phi(h)\phi(gh))$ equals $(m/4)((g^{-1}, 1) + (g^{-1}, -1) + (g^{-1}, \sqrt{-1}) + (g^{-1}, -\sqrt{-1}))$ for each $g \neq 1$ and only if $\phi$ is a flat PQA. Finally, with $R_0 = \{h, 1 \in R\}$, $R_1 = \{(h, \sqrt{-1}) \in R\}$, $R_2 = \{(h, -1) \in R\}$ and $R_3 = \{(h, -\sqrt{-1}) \in R\}$, $R^{-1} = R$ if and only if $\phi(h^{-1}) = \phi(h)^{-1}$, $h \in H$. $\square$

This means the $(2^{2t}, 4, 2^{2t} - 2)$-RDS in $\mathbb{Z}_4^{t+1}$ relative to $\mathbb{Z}_4$ obtained by projection from the RDS constructed in [6, Theorem 4.1] are equivalent to flat PQA. The examples of reversible RDS with forbidden subgroup $\mathbb{Z}_4$ obtained in Theorem 1.4 give a new infinite family of flat PQA satisfying an additional balance property.

**Corollary 5.3.** With $F$ and $R$ as in Lemma 4.1, define $\phi : GR(F) \rightarrow N$ by $\phi(h) = 1$, $h \in R_0$, $\phi(h) = \sqrt{-1}$, $h \in R_1$, $\phi(h) = -1$, $h \in R_2$ and $\phi(h) = -\sqrt{-1}$, $h \in R_3$. Then $\phi$ is a flat PQA with the additional property that $\phi(-h) = \phi(h)^{-1}$, $h \in GR(F)$.

**References**


**Further reading**