Constructions of Hadamard Difference Sets

Richard M. Wilson and Qing Xiang*

Department of Mathematics, California Institute of Technology, Pasadena, California 91125

Communicated by the Managing Editors
Received May 3, 1996

Using a spread of $PG(3, p)$ and certain projective two-weight codes, we give a general construction of Hadamard difference sets in groups $H \times (Z_p)^4$, where $H$ is either the Klein 4-group or the cyclic group of order 4, and $p$ is an odd prime. In the case $p \equiv 3 \pmod{4}$, we use an ovoidal fibration of $PG(3, p)$ to construct Hadamard difference sets as a special case. In the case $p \equiv 1 \pmod{4}$, we construct new reversible Hadamard difference sets by explicitly constructing the two-weight codes needed in our general construction method. Using a well-known composition theorem, we conclude that there exist Hadamard difference sets with parameters $(4^m, 2^{2m^2}, 2^{m^2} \cdot 2^{m^2})$ with $a, b, c_1, c_2, c_3$ positive integers and where each $p_j$ is a prime congruent to 3 modulo 4, $1 \leq j \leq t$.  

1. INTRODUCTION

Let $G$ be a finite group of order $v$. A $k$-element subset $D$ of $G$ is called a $(v, k, \lambda)$ difference set in $G$ if the list of “differences” $d_1 d_2^{-1}, d_1, d_2 \in D, d_1 \neq d_2$, represents each nonidentity element in $G$ exactly $\lambda$ times. Using multiplicative notation for the group operation, $D$ is a $(v, k, \lambda)$ difference set in $G$ if and only if it satisfies the following equation in $Z[G]$,  

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

where $D = \sum_{d \in D} d, D^{(-1)} = \sum_{d \in D} d^{-1}$, and $1_G$ is the identity element of $G$. $D$ is called reversible if $D^{(-1)} = D$.

In the case $G$ is an abelian group, using the Fourier inversion formula, we have the following standard lemma in the theory of difference sets.

**Lemma A.** Let $G$ be an abelian group of order $v$. A $k$-subset $D$ is a $(v, k, \lambda)$ difference set in $G$ if and only if $|\chi(D)| = \sqrt{k - \lambda}$ for every nontrivial character $\chi$ of $G$. Furthermore, $D = D^{(-1)}$ if and only if $\chi(D) = \overline{\chi(D)}$ for every character $\chi$ of $G$.

* E-mail: rmw@cco.caltech.edu; xiang@cco.caltech.edu.

148

0097-3165/97 $25.00
Copyright 1997 by Academic Press
All rights of reproduction in any form reserved.
The difference sets considered in this paper have parameters

\[(v, k, \lambda) = (4m^2, 2m^2 - m, m^2 - m).\]

These difference sets are called Hadamard difference sets (HDS), since their \(\pm 1\) incidence matrices are Hadamard matrices. Alternative names used by other authors are Menon difference sets and H-sets.

The central problem in the study of HDS is for each integer \(m\), which groups of order \(4m^2\) contain a Hadamard difference set. This problem remains open, for abelian groups and non-abelian groups as well. However, considerable progress has been made on the construction of Hadamard difference sets in recent years. For example, in 1992, Xia [10] constructed Hadamard difference sets in groups \(H \times \mathbb{Z}_4 \times \mathbb{Z}_4 \times \cdots \times \mathbb{Z}_4\), where \(H\) is either the Klein 4-group or the cyclic group of order 4, and each \(p_j\) is a prime congruent to 3 modulo 4, \(1 \leq j \leq t\). Smith [8] constructed a non-abelian reversible Hadamard difference set in the group \((a, b, c | a^5 = b^5 = c^4 = [a, b] = cac^{-1}a^{-1}b^{-1} = 1)\). In October, 1995, Van Eupen and Tonchev [5] constructed a reversible Hadamard difference set in \(\mathbb{Z}_2 \times \mathbb{Z}_2 \times (\mathbb{Z}_5)^4\), which is the first example of an abelian Hadamard difference set with the order divisible by a prime congruent to 1 modulo 4.

In this paper, we first give a general construction method for Hadamard difference sets in groups \(H \times (\mathbb{Z}_p)^4\), where \(H\) is either group of order 4 and \(p\) is an odd prime, by assuming the existence of certain projective two-weight codes. This method applies to both cases that \(p \equiv 3 \pmod{4}\) and \(p \equiv 1 \pmod{4}\). In section 3, we explain Xia’s construction by using our general construction method. This was actually done by Xiang and Chen in [11]. We include this section here for the convenience of the reader. In section 4, we use an ovoidal fibration of \(PG(3, p)\) (see [1, 4, 6]) and spreads associated with it to construct Hadamard difference sets in \(H \times (\mathbb{Z}_5)^4\), where \(H\) is either group of order 4 and \(p\) is a prime congruent to 3 modulo 4. This construction includes Xia’s construction of Hadamard difference sets as a special case. In Section 5, we explicitly construct those projective two-weight codes needed in our general construction for HDS when \(p = 5, 13, 17\). Using a well-known composition theorem of Hadamard difference sets (for example, see [7, 9]), we conclude that there exist Hadamard difference sets with parameters \((4m^2, 2m^2 - m, m^2 - m)\), where \(m = 2^{3a}5^{2c}13^{2e}17^{2r}p_1^{c_1}p_2^{c_2} \cdots p_t^{c_t}\) with \(a, b, c_1, c_2, c_3\) positive integers and where each \(p_j\) is a prime congruent to 3 modulo 4, \(1 \leq j \leq t\).

2. THE CONSTRUCTION

We begin with the definition of a projective \((n, k, h_1, h_2)\) set in \(PG(k - 1, q)\), where \(q\) is a power of a prime \(p\).
Definition. A projective \((n, k, h_1, h_2)\) set \(\mathcal{C}\) is a proper, nonempty set of \(n\) points of the projective space \(PG(k-1, q)\) with the property that every hyperplane meets \(\mathcal{C}\) in \(h_1\) points or \(h_2\) points.

Let \(\mathcal{C} = \{\langle y_1 \rangle, \langle y_2 \rangle, \ldots, \langle y_n \rangle\}\) be a set of \(n\) points in \(PG(k-1, q)\). Associated with \(PG(k-1, q)\) is the \(k\)-dimensional vector space \(W = V_k(q)\). Let \(\mathcal{W} = \{ v \in W | \langle v \rangle \in \mathcal{C} \}\) be the set of vectors in \(W\) corresponding to \(\mathcal{C}\). For \(w \in GF(q)^k\), define an additive character of \(GF(q)^k\) as

\[
\chi_w : x \mapsto \xi^{Tr(w \cdot x)}, \quad x \in GF(q)^k,
\]

where \(\xi\) is a primitive \(p\)th root of unity and \(Tr\) is the trace from \(GF(q)\) to \(GF(p)\). It is easy to see that \(\chi_w, w \in GF(q)^k\), are all the additive characters of \(GF(q)^k\).

For any nontrivial additive character \(\chi_w\) of \(GF(q)^k\), we have

\[
\chi_w(\mathcal{W}) = (q-1)|w^+ \cap \{ y_1, y_2, \ldots, y_n \}| + (-1)(n - |w^+ \cap \{ y_1, y_2, \ldots, y_n \}|)
\]

\[
= q|w^+ \cap \{ y_1, y_2, \ldots, y_n \}| - n,
\]

where \(w^+ = \{ y \in GF(q)^k | y \cdot w = 0 \}\), and \(y \cdot w\) is the usual dot product.

Hence we have the following lemma.

Lemma 2.1. \(\mathcal{C}\) is a projective \((n, k, h_1, h_2)\) set if and only if \(\chi_w(\mathcal{W}) = qh_1 - n\) or \(qh_2 - n\), for every nontrivial additive character \(\chi_w, w \in GF(q)^k\).

Also we mention that projective \((n, k, h_1, h_2)\) sets are equivalent to projective two-weight codes and certain strongly regular Cayley graphs.

We refer the reader to the survey papers \([3, 7]\) for more detailed discussion of these three objects.

Let \(\Sigma = PG(3, p)\) denote projective 3-space over \(GF(p)\), where \(p\) is an odd prime. A spread of \(\Sigma\) is any collection of \(p^2 + 1\) pairwise disjoint lines of \(\Sigma\), necessarily partitioning the points of \(\Sigma\). A partial spread in \(\Sigma\) is a set of lines no two of which intersect. Also, for convenience, we will call a subset \(C\) of \(\Sigma\) a type \(Q\) set if \(C\) is a projective \(((p^2 - 1)/4(p-1), 4, (p-1)^2/4, (p+1)^2/4)\) set.

Theorem 2.2. Assume that \(S = \{ L_1, L_2, \ldots, L_{p^2+1}\}\) is a spread of \(\Sigma\). If there exist two subsets \(C_0, C_1\) of type \(Q\) in \(\Sigma\) such that \(|C_0 \cap L_i| = (p+1)/2, 1 \leq i \leq s\), and \(|C_1 \cap L_i| = (p+1)/2, (s+1) \leq j \leq 2s\), where \(s = (p^2 + 1)/2\), then there exists a Hadamard difference set in \(H \times (Z_p)^4\), where \(H\) is either the Klein 4-group or the cyclic group of order \(4\); in the first case, the Hadamard difference set obtained is reversible.

Proof. Let \(C_2 = (L_1 \cup L_2 \cup \cdots \cup L_s) \setminus C_0\), \(C_3 = (L_{s+1} \cup L_{s+2} \cup \cdots \cup L_{2s}) \setminus C_1\). We first prove that \(C_2, C_3\) are also two subsets of type \(Q\) in \(\Sigma\).
Associated with $\Sigma_3$ is the four-dimensional vector space $W = V_d(p)$ over $\mathbb{F}_p$. Let $\mathcal{C}_0 = \{w \in W \mid \langle w \rangle \in C_0\}$, $\mathcal{C}_2 = \{w \in W \mid \langle w \rangle \in C_2\}$.

Since $C_0$ is a set of type $Q$ in $\Sigma_3$, by Lemma 2.1 we have $\chi(\mathcal{C}_0) = (p^2 - 1)/4 - p^2$ or $(p^2 - 1)/4$, for every nontrivial additive character $\chi$ of $W$.

We will use $W^*$ to denote the additive character group of $W$, and define $U = \{\chi \in W^* \mid \chi(\mathcal{C}_0) = (p^2 - 1)/4 - p^2\}$, $V = \{\chi \in W^* \mid \chi(\mathcal{C}_0) = (p^2 - 1)/4\}$.

Let $\mathcal{L}_2 = \{w \in W \mid \langle w \rangle \in \bigcup_{i=1}^s L_i\}$. Since $\{L_1, L_2, ..., L_s\}$ is a partial spread, we have

$$\chi(\mathcal{L}_2) = \begin{cases} -\frac{p^2 + 1}{2}, & \text{if } \chi \in N_1; \\ -\frac{p^2 - 1}{2}, & \text{if } \chi \in T_1, \end{cases}$$

where $N_1 = \{\chi \in W^* \setminus \{\mathcal{C}_0\} \mid \chi$ is nontrivial on every $L_i$, $1 \leq i \leq s\}$ and $T_1 = \{\chi \in W^* \setminus \{\mathcal{C}_0\} \mid \chi$ is trivial on exactly one $L_i$, for some $i$, $1 \leq i \leq s\}$.

We contend that $T_1 \cap U = \emptyset$.

For each $L_j$, $1 \leq j \leq 2s$, which is now viewed as a two-dimensional subspace of $W$, let $L_j^0 = \{\chi \in W^* \mid \chi$ is trivial on $L_j\}$. Then $|L_j^0| = |W/L_j| = p^2$.

For $1 \leq j \leq s$, we define $\alpha_j = |(L_j^0 \setminus \{\mathcal{C}_0\}) \cap U|$, $\beta_j = |(L_j^0 \setminus \{\mathcal{C}_0\}) \cap V|$. Then $\alpha_j + \beta_j = p^2 - 1$.

For every $\chi \in L_j^0$, we have $\chi(\mathcal{C}_0) = \chi(\mathcal{C}_0 \setminus (\mathcal{C}_0 \cap L_j)) + |\mathcal{C}_0 \cap L_j|$. Therefore,

$$\sum_{\chi \in L_j^0} \chi(\mathcal{C}_0) = \sum_{w \in \mathcal{C}_0 \setminus (\mathcal{C}_0 \cap L_j)} \sum_{\chi \in L_j^0} \chi(w) + p^2 |\mathcal{C}_0 \cap L_j|.$$ 

Noting that $\sum_{\chi \in L_j^0} \chi(w) = 0$ if there is a $\chi \in L_j^0$ such that $\chi(w) \neq 1$, we have

$$\sum_{\chi \in L_j^0} \chi(\mathcal{C}_0) = p^2 |\mathcal{C}_0 \cap L_j|.$$ 

That is, $(p^2 - 1)/4 + \alpha_j((p^2 - 1)/4 - p^2) + \beta_j(p^2 - 1)/4 = p^2 |\mathcal{C}_0 \cap L_j|$. Simplifying this we get

$$\frac{1 - p^2}{2} + \beta_j = |\mathcal{C}_0 \cap L_j|.$$ 

Since $|\mathcal{C}_0 \cap L_j| = (p^2 - 1)/2$ for every $j$, $1 \leq j \leq s$, we have $\beta_j = p^2 - 1$, $\alpha_j = 0$, $1 \leq j \leq s$. Hence, $T_1 \cap U = \emptyset$.

For any nontrivial $\chi \in W^*$, $\chi(\mathcal{C}_2) = \chi(\mathcal{L}_2) - \chi(\mathcal{C}_0)$. Since $T_1 \cap U = \emptyset$, we have

$$\chi(\mathcal{C}_2) = \begin{cases} \frac{p^2 - 1}{4} - p^2, & \text{if } \chi \in N_1 \cup V; \\ \frac{p^2 - 1}{4}, & \text{if } \chi \in (N_1 \cup U) \cup (T_1 \cup V). \end{cases}$$

This shows that $C_2$ is a set of type $Q$ in $\Sigma_3$. 


Similarly, define \( C_1 = \{ w \in W \mid \langle w \rangle \in C_1 \} \), \( C_3 = \{ w \in W \mid \langle w \rangle \in C_3 \} \). Let \( \mathcal{L}_2 = \{ w \in W \mid \langle w \rangle \in \bigcup_{j=1}^{2s+1} L_j \} \). Since \( C_1 \) is a set of type \( Q \) in \( \mathcal{L}_1 \) and \( \{ L_{s+1}, L_{s+2}, \ldots, L_{2s} \} \) is a partial spread, we have

\[
\chi(C_1) = \begin{cases} 
\frac{p^2 - 1}{4} - p^2, & \text{if } \chi \in X, \\
\frac{p^2 - 1}{4}, & \text{if } \chi \in Y,
\end{cases}
\]

and

\[
\chi(C_3) = \begin{cases} 
\frac{-p^2 + 1}{2}, & \text{if } \chi \in N_3, \\
\frac{p^2 - 1}{2}, & \text{if } \chi \in T_3,
\end{cases}
\]

where \( N_3 = T_1 \) and \( T_3 = N_1 \).

By the same argument as above, we can show that \( T_2 \cap X = \emptyset \); hence,

\[
\chi(C_3) = \begin{cases} 
\frac{p^2 - 1}{4} - p^2, & \text{if } \chi \in N_2 \cap Y; \\
\frac{p^2 - 1}{4}, & \text{if } \chi \in (N_2 \cap X) \cup (T_2 \cap Y).
\end{cases}
\]

Assume that \( A \) is the union of any \( (p^2 - 1)/4 \) lines from \( L_{s+1}, L_{s+2}, \ldots, L_{2s} \), \( B \) is the union of any \( (p^2 - 1)/4 \) lines from \( L_1, L_2, \ldots, L_s \), and we view \( A, B \) as subsets in the vector space \( W \) (we make the convention that \( A, B \) when viewed as subsets in \( W \), do not contain the zero vector). Define

\[
D_0 = C_0 \cup A, \quad D_1 = C_1 \cup B, \\
D_2 = C_2 \cup A, \quad D_3 = C_3 \cup B.
\]

For any nontrivial \( \chi \in W^* \), we distinguish two cases:

1. \( \operatorname{Ker} \chi = L_j \), for some \( j, 1 \leq j \leq s \). In this case, \( \chi \in N_2 = T_1 \). Since \( T_1 \cap U = \emptyset \), we have \( \chi \in V \). Therefore, \( \chi(D_0) = (p^2 - 1)/4 + (- (p^2 - 1)/4) = 0 \), and \( \chi(D_2) = (p^2 - 1)/4 + (- (p^2 - 1)/4) = 0 \),

\[
\chi(B) = \begin{cases} 
p^2 - \frac{p^2 - 1}{4}, & \text{if } L_j \in B; \\
p^2 - \frac{p^2 - 1}{4}, & \text{if } L_j \notin B.
\end{cases}
\]
Hence

\[ \chi(D_1) = \begin{cases} 0, & \text{if } \chi \in Y; L_j \notin B \text{ or } \chi \in X; L_j \in B; \\ \pm p^2, & \text{if } \chi \in Y; L_j \in B \text{ or } \chi \in X; L_j \notin B; \end{cases} \]

and

\[ \chi(D_3) = \begin{cases} 0, & \text{if } \chi \in Y; L_j \notin B \text{ or } \chi \in X; L_j \notin B; \\ \pm p^2, & \text{if } \chi \in Y; L_j \in B \text{ or } \chi \in X; L_j \in B. \end{cases} \]

This shows that \( \chi(D_0) = \chi(D_2) = 0 \), and only one of \( \chi(D_1) \), \( \chi(D_3) \) vanishes, the other is \( \pm p^2 \).

(2) \( \text{Ker } \chi \supset L_j \), for some \( j \), \( (s+1) \leq j \leq 2x \). In this case, \( \chi \in N_1 = T_2 \).

Since \( T_2 \cap X = \emptyset \), we have \( \chi \notin Y \). In a manner similar to that of case (1), we can show that \( \chi(D_1) = \chi(D_2) = 0 \) and only one of \( \chi(D_0) \), \( \chi(D_3) \) vanishes; the other is \( \pm p^2 \).

We first construct an HDS in the group \( Z_2 \times Z_2 \times (W, +) \). Let us denote the elements of \( Z_2 \times Z_2 \) by \( \{1, a, b, ab\} \). Define \( D = D_0 \cup aD_1 \cup bD_2 \cup ab(W \setminus D_3) \). We contend that \( D \) is a reversible Hadamard difference set in \( Z_2 \times Z_2 \times (W, +) \).

Let \( \phi \otimes \chi \) be an arbitrary nontrivial character of \( Z_2 \times Z_2 \times W \).

If \( \chi \) is trivial, \( \phi \) is nontrivial, then

\[ |\phi \otimes \chi(D)| = |D_0| + |\phi(a)|D_1| + |\phi(b)|D_2| + |\phi(ab)|W \setminus D_3| = p^3|\phi(ab)|, \]

so \( |\phi \otimes \chi(D)| = p^2 \).

If \( \chi \) is nontrivial, by the discussion in the two cases above, we have

\[ |\phi \otimes \chi(D)| = \pm p^2; \]

hence \( |\phi \otimes \chi(D)| = p^2 \).

By Lemma A, \( D \) is a Hadamard difference set. Since \( \phi(D) = \overline{\phi(D)} \) for every nontrivial character \( \phi \) of \( Z_2 \times Z_2 \times W \), \( D \) is reversible. In the case the group is \( Z_4 \times (Z_2)^4 \), let the elements of \( Z_4 \) be \( \{1, c, c^2, c^3\} \), and \( D = D_0 \cup cD_1 \cup c^2D_2 \cup c^3(W \setminus D_3) \). Then it is easy to show that \( D \) is a Hadamard difference set in \( Z_4 \times (W, +) \). This completes the proof of the theorem.

3. ON XIA’S CONSTRUCTION

In 1992, Xia [10] constructed Hadamard difference sets in groups \( H \times Z_p^4 \times Z_p^4 \times \cdots \times Z_p^4 \), where \( H \) is either group of order 4 and each \( p_j \) is a prime congruent to 3 modulo 4, \( 1 \leq j \leq t \). Xia’s construction depends on
very complicated calculations involving cyclotomic classes of high order. Xiang and Chen [11] have given a simpler proof for Xia’s construction by using additive characters of finite fields.

In view of Theorem 2.2, in order to construct Hadamard difference sets in \( H \times \mathbb{Z}_p^3 \), where \( H \) is either group of order 4 and \( p \) is a prime congruent to 3 modulo 4, all we need are a spread in \( \Sigma_3 \), and sets \( C_0, C_1 \) of type Q in \( \Sigma_3 \) satisfying the conditions in Theorem 2.2.

Let \( p \) be a prime congruent to 3 modulo 4 and let \( \beta \) be a primitive element of \( \mathbb{F}_p^4 \). We model \( \mathbb{F}_p^4 \) by viewing \( \mathbb{F}_p^4 \) as four-dimensional vector space over \( \mathbb{F}_p \). Thus the points of \( \Sigma_3 \) are represented by \( \langle 1 \rangle, \langle \beta \rangle, \ldots, \langle \beta^{p^2+1} \rangle \). Let \( L_i = \{ \langle \beta^i \rangle, \langle \beta^{p^2+1+i} \rangle, \ldots, \langle \beta^{p^2+1}(p^2+1+i) \rangle \}, \ 0 \leq i \leq p^2 \). Then it is easy to see that \( S = \{ L_0, L_1, \ldots, L_{p^2} \} \) is a spread in \( \Sigma_3 \).

Let \( C_0 = \{ \langle 1 \rangle, \langle \beta^i \rangle, \langle \beta^{p^2} \rangle, \ldots, \langle \beta^{p^2+1}(p^2+1) \rangle \}, \ C_1 = \{ \langle \beta^i \rangle, \langle \beta^{p^2} \rangle, \langle \beta^{p^2+1}(p^2+1) \rangle \}. \) Since \( p \equiv 3 \) (mod 4), by uniform cyclotomy (see [2, 7]), \( C_0, C_1 \) are two sets of type Q in \( \Sigma_3 \). Also it is easy to see that \( |C_0 \cap L_{2i}| = \frac{(p+1)}{2}, \ 0 \leq i \leq (p^2-1)/2, \) and \( |C_1 \cap L_{2i+1}| = \frac{(p+1)}{2}, \ 0 \leq i \leq (p^2-1)/2. \) Therefore by Theorem 2.2, we have

**Corollary 3.1.** There exists a Hadamard difference set in \( H \times (\mathbb{Z}_p^4)^t \), where \( p \) is a prime congruent to 3 modulo 4 and \( H \) is either the Klein 4-group or the cyclic group of order 4. In the first case, the Hadamard difference set constructed by Theorem 2.2 is reversible.

Using a composition theorem of Turyn [9], it is routine to construct Hadamard difference sets in \( H \times \mathbb{Z}_p^1 \times \mathbb{Z}_p^2 \times \cdots \times \mathbb{Z}_p^t \), where \( H \) is either group of order 4, and each \( p_j \) is a prime congruent to 3 modulo 4, \( 1 \leq j \leq t. \)

### 4. General Construction in the Case \( p \equiv 3 \) (mod 4)

In this section, we give a general construction of Hadamard difference sets in \( H \times (\mathbb{Z}_p^4)^t \), where \( H \) is either group of order 4, and \( p \) is a prime congruent to 3 modulo 4, by using an ovoidal fibration of \( PG(3, p) \) in [1, 4, and 6, page 253]. We introduce the following notation as in [1, 4].

Let \( p \) be a prime congruent to 3 modulo 4. We view \( GF(p^4) \) as a four-dimensional vector space over \( GF(p) \), and, hence, the one-dimensional subspaces of this vector space can be thought of as the projective points of \( \Sigma_3 = PG(3, p) \). Similarly, we identify the lines of \( \Sigma_3 \) with the two-dimensional vector subspaces of \( GF(p^4) \) over \( GF(p) \). We also let \( \langle A \rangle \) denote the vector subspace generated by the set \( A \) over \( GF(p) \).

If \( \beta \) is a primitive element of \( GF(p^4) \), then \( \alpha(\beta) = p^4 - 1 = (p+1)(p-1)(p^2+1) \) and hence \( \beta^{p+1}(p^2+1) \) is a primitive element of
GF(p). We therefore identify the points of \( \Sigma_3 \) with \( \{ \langle \beta^t \rangle \mid t = 0, 1, 2, \ldots, (p + 1)(p^2 + 1) - 1 \} \). If we now let \( \Omega_i = \{ \langle \beta^t \rangle \mid t \equiv i \pmod{p + 1} \} \), each \( \Omega_i \) is an ovoid (Theorem 3 of [4]) and the points of \( \Sigma_3 \) are thus partitioned into \( p + 1 \) disjoint ovoids:

\[
\Sigma_3 = \Omega_0 \cup \Omega_1 \cup \cdots \cup \Omega_{p}.
\]

Moreover, each line of \( \Sigma_3 \) is tangent to precisely 0 or 2 of these ovoids (Lemma 1 and Theorem 4 of [4]). Lines of the former type will be called “secant-type” and those of the latter “tangent-type”. If \( L_s = \langle \beta^0, \beta^{s(p+1)} \rangle \) denotes the line of \( \Sigma_3 \) joining the points \( \langle \beta^0 \rangle \) and \( \langle \beta^{s(p+1)} \rangle \) of \( \Omega_0 \) for any integer \( s \) with \( 1 \leq s \leq p^2 \), then \( L_s \) is a secant-type line if and only if \( s \) is odd (Theorem 4 of [4]).

We quote the following theorem and corollary from [1].

**Theorem B.** Using the above notation, let \( s \) be an odd integer with \( 1 \leq s \leq p^2 \). Consider the secant-type line \( L_s = \langle \beta^0, \beta^{s(p+1)} \rangle \), necessarily secant to \((p + 1)/2\) ovoids in the fibration \((\ast)\). Then there exists a positive integer \( d \) such that \( L_s^d \) is a secant-type line meeting the \((p + 1)/2\) ovoids of \((\ast)\) missed by \( L_s \). Moreover, if \( s \neq (p^2 + 1)/2 \), \( d \) is unique modulo \( p + 1 \).

**Corollary C.** \( L_s \cup (L_s)^d \) is a spread of \( \Sigma_3 \). This spread is regular precisely when \( s = (p^2 + 1)/2 \).

Now we use the spread in Corollary C to construct Hadamard difference sets. By Theorem 2.2, we need to come up with two sets \( C_0, C_1 \) in \( \Sigma_3 \) of type \( Q \) satisfying the conditions in Theorem 2.2.

Let \( L_s \) and \( (L_s)^d \) be the secant-type lines in Theorem B. We assume that \( L_s \) is secant to \( \Omega_{t_1}, \Omega_{t_2}, \ldots, \Omega_{t_r} \), and \( (L_s)^d \) is secant to \( \Omega_{t_1}, \Omega_{t_2}, \ldots, \Omega_{t_r} \), where \( r = (p + 1)/2 \). By Theorem B, \( \{t_1, t_2, \ldots, t_r\} = \{0, 1, 2, \ldots, p\} \). Since \( p \equiv 3 \pmod{4} \), \( r \) is even. Let \( C_0 \) be the union of any \( r/2 \) ovoids from \( \{\Omega_{t_1}, \Omega_{t_2}, \ldots, \Omega_{t_r}\} \), and let \( C_1 \) be the union of any \( r/2 \) ovoids from \( \{\Omega_{t_r'}, \Omega_{t_r'}, \ldots, \Omega_{t_r'}\} \), then we have the following lemma.

**Lemma 4.1.** \( C_0 \) meets every line in \([L_s]\) in \((p + 1)/2\) points, and \( C_1 \) meets every line in \((L_s)^d \) in \((p + 1)/2\) points. \( C_0, C_1 \) are two sets of type \( Q \) in \( \Sigma_3 \).
Proof. The first assertion is clear by the definition of \( C_0 \) and \( C_1 \). For the proof of the second part, we observe that every plane of \( \Sigma_3 \) must meet each of the \( p+1 \) ovoids in (\*) in a point or an oval. A simple counting argument then shows that each plane of \( \Sigma_3 \) is tangent to 1 of the ovoids in (\*) and meets the other \( p \) ovoids in disjoint ovals. Let \( \pi \) be an arbitrary plane of \( \Sigma_3 \). Then \( |\pi \cap C_0| = 1 + (r^2 - 1)(p + 1) = (p - 1)^2/4 \) if \( C_0 \) contains some \( \Omega_i \) such that \( |\pi \cap \Omega_i| = 1 \), \( 1 \leq j \leq r \), and \( |\pi \cap C_0| = (r/2)(p + 1) = (p + 1)^2/4 \) if \( |\pi \cap \Omega_i| = p + 1 \) for every \( \Omega_i \) contained in \( C_0 \). This shows that \( C_0 \) is a set of type \( Q \) in \( \Sigma_3 \). Similarly, we can show that \( C_1 \) is also a set of type \( Q \) in \( \Sigma_3 \). This completes the proof of the lemma.

**Corollary 4.2.** Let \( [L_s] \cup [(L_s)^{p^2}] \), \( C_0 \), \( C_1 \) be defined as above. Then there exists a Hadamard difference set in \( H \times (Z_p)^4 \), where \( H \) is either group of order 4, and \( p \) is a prime congruent to 3 modulo 4, by using the spread \( [L_s] \cup [(L_s)^{p^2}] \) and the sets \( C_0 \) and \( C_1 \) of type \( Q \) in \( \Sigma_3 \).

**Proof.** This is clear from Lemma 4.1 and Theorem 2.2.

**Remarks.** (1) If we let \( s = (p^2 + 1)/2 \), then \( L_s = GF(p^2) \), \( L_s^p = L_s \), and \( [L_s] \cup [\beta L_s] \) is the regular spread in Section 3. Also we note that \( L_s \) meets the ovoids \( \Omega_0, \Omega_2, \Omega_4, ..., \Omega_{p-1} \) (Lemma 1 of [4]), and \( \beta L_s \) meets the ovoids \( \Omega_1, \Omega_3, \Omega_5, ..., \Omega_p \). If we choose the union of \( \Omega_0, \Omega_4, \Omega_8, ..., \Omega_{p-3} \) as \( C_0 \) and the union of \( \Omega_1, \Omega_5, \Omega_9, ..., \Omega_{p-2} \) as \( C_1 \), then the construction in this section will give rise to Xia’s construction.

(2) Let \( G = K_4 \times P \), where \( K_4 \) is the Klein 4-group and \( P = Z_{p^2}^* \), \( p \) is a prime congruent to 3 modulo 4. Two difference sets \( D \) and \( D' \) in \( G \) are said to be equivalent if \( D' = gD \) for some automorphism \( g \) of \( G \) and some element \( g \) of \( G \). Since \( K_4 \) and \( P \) have relatively prime orders, they must be invariant under every automorphism of \( G \). Therefore the automorphism group of \( G \) has size \( |GL(2,2)| \cdot |GL(4,p)| = 6p^6(p^4-1)(p^3-1)(p^2-1) \) \((p-1)\). From Theorem 2.2 and the construction in this section, we see that there are at least

\[
\frac{4!}{2} \frac{(p^2+1)^2}{(p+1)^2} \frac{(p^2+1)^2}{(p+1)^2} \frac{(p^2-1)^2}{(p+1)^2} = \frac{4!}{2} \frac{(p^2+1)^2}{(p+1)^2} \frac{(p^2+1)^2}{(p+1)^2} \frac{(p^2-1)^2}{(p+1)^2} \frac{(p^2-1)^2}{(p+1)^2} \frac{(p^2-1)^2}{(p+1)^2}
\]

pairwise inequivalent Hadamard difference sets in \( G \).
5. THE CASE \( p \equiv 1 \pmod{4} \)

In this section, we construct sets of type Q in \( \Sigma_3 = PG(3, p) \) with \( p \equiv 1 \pmod{4} \). Again let \( W \) be the four-dimensional vector space over \( GF(p) \). We may consider \( W \) as a direct product \( GF(p^2) \times GF(p^2) \).

Let \( g \) be a primitive element of \( GF(p^2) \). \( L_0 \) will denote the line \( \{0\} \times GF(p^2) \), and for any \( d \) in \( GF(p^2) \), \( L_d \) will denote the line \( \{(x, dx^p) \mid x \in GF(p^2)\} \). It is easy to verify that \( S = \{L_d \mid d \in GF(p^2)\} \cup \{L_0\} \) is a spread in \( \Sigma_3 \).

We now consider the action of

\[
T = \begin{pmatrix}
g^2 & 0 \\
0 & g^{-2}
\end{pmatrix}
\]

on the points of \( \Sigma_3 \), which are now viewed as one-dimensional subspaces over \( GF(p) \) of the four-dimensional vector space \( GF(p^2) \times GF(p^2) \) over \( GF(p) \).

The orbits of the action of \( T \) on the points of \( \Sigma_3 \) are

1. Four “short” orbits, each of length \( (p+1)/2 \). We choose \((0, 1)\), \((0, g)\), \((1, 0)\), and \((g, 0)\) as the representatives of these four orbits.

2. \( 4(p+1) \) “long” orbits, each of length \( (p^2-1)/4 \). The representatives of these \( 4(p+1) \) orbits can be chosen as

\[
(1, 1), (1, g), (1, g^3), \ldots, (1, g^{p^2+1}),
\]

\[
(g, 1), (g, g), (g, g^3), \ldots, (g, g^{p^2+1}).
\]

It is clear that each short orbit consists of \( (p+1)/2 \) points of \( L_0 \) or \( L_{\infty} \).

Next we show that each long orbit consists of \( (p+1)/2 \) points of \( L_0 \) or \( L_{\infty} \). Each column in the above diagram consists of \( (p+1)/2 \) points of some line \( L_d \), \( d \neq 0 \), \( d \in GF(p^2) \); hence the orbit represented by \((1, g^i)\) consists of \( (p+1)/2 \) points of \( (p-1)/2 \) lines from the
set of lines $L_d$, $d \neq 0$, $d \in GF(p^2)$. This argument applies to any orbit represented by $(g, g^i)$, $0 \leq i \leq 2p + 1$.

For $p = 5$ let $g$ be a root of $x^2 + x + 2 \in GF(5)[x]$. With the help of a computer (we will give more details about the computer search at the end of this section), we found that the union of the following orbits

$$(1, g), (1, g^3), (1, g^6), (1, g^{13}), (g, 1), (g, g^8), (1, 0)$$

forms a set of type Q in $PG(3, 5)$, which we will call $C_0$, also the union of the following orbits

$$(1, g^9), (1, g^{10}), (1, g^{13}), (g, g^2), (g, g^8), (g, g^{10}), (0, 1)$$

forms another set of type Q in $PG(3, 5)$, which we denote by $C_1$. Let $S = \{ L_d \mid d \in GF(5^2) \} \cup \{ L_{-d} \}$. We have seen that each orbit of $T$ intersects the lines in $S$ in 0 or 3 points, also no two orbits of $T$ in $C_0$, $C_1$ intersect the same line, hence $C_0$, $C_1$ satisfy the conditions of Theorem 2.2. Therefore there exists a Hadamard difference set in $H \times (Z_5)^4$, where $H$ is either group of order 4. We state this as a corollary.

**Corollary 5.1.** There exists a Hadamard difference set in $H \times (Z_5)^4$, where $H$ is either the Klein 4-group or the cyclic group of order 4; in the first case, the Hadamard difference set is reversible.

**Remark.** Van Eupen and Tonchev ([5]) were the first to construct a reversible Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$. We remark that the structure of the Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$ constructed in Corollary 5.1 is different from that of Van Eupen and Tonchev's Hadamard difference set. For example, in Theorem 2.2 (hence in Corollary 5.1), we choose $A$, $B$ both as union of lines from a spread in $\Sigma_3$, while in Van Eupen and Tonchev's example, one projective $(36, 4, 6, 11)$ set in $PG(3, 5)$ comes from the union of six lines, the other does not.

In the case $p = 13$, let $g$ be a root of $x^2 + x + 2 \in GF(13)[x]$. With the help of a computer, we found the following two sets of type Q in $PG(3, 13)$.

The union of the orbits

$$(1, g^5), (1, g^6), (1, g^8), (1, g^{13}), (1, g^{15}), (1, g^{17}), (1, g^{24}), (g, g^8), (g, g^9), (g, g^{10}), (g, g^{16}), (g, g^{23}), (1, 0)$$

forms a set of type Q in $PG(3, 13)$, which we will denote by $C_0$. And the union of the orbits

$$(1, 1), (1, g^2), (1, g^4), (1, g^7), (1, g^8), (1, g^{12}), (1, g^{25}), (g, g), (g, g^8), (g, g^9), (g, g^{11}), (g, g^{13}), (g, g^{24}), (g, g^{27}), (0, 1)$$

forms another set of type Q in $PG(3, 13)$, which we denote by $C_1$. Let $S = \{ L_d \mid d \in GF(13^2) \} \cup \{ L_{-d} \}$. We have seen that each orbit of $T$ intersects the lines in $S$ in 0 or 3 points, also no two orbits of $T$ in $C_0$, $C_1$ intersect the same line, hence $C_0$, $C_1$ satisfy the conditions of Theorem 2.2. Therefore there exists a Hadamard difference set in $H \times (Z_5)^4$, where $H$ is either group of order 4. We state this as a corollary.

**Corollary 5.1.** There exists a Hadamard difference set in $H \times (Z_5)^4$, where $H$ is either the Klein 4-group or the cyclic group of order 4; in the first case, the Hadamard difference set is reversible.

**Remark.** Van Eupen and Tonchev ([5]) were the first to construct a reversible Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$. We remark that the structure of the Hadamard difference set in $Z_2 \times Z_2 \times (Z_5)^4$ constructed in Corollary 5.1 is different from that of Van Eupen and Tonchev's Hadamard difference set. For example, in Theorem 2.2 (hence in Corollary 5.1), we choose $A$, $B$ both as union of lines from a spread in $\Sigma_3$, while in Van Eupen and Tonchev's example, one projective $(36, 4, 6, 11)$ set in $PG(3, 5)$ comes from the union of six lines, the other does not.

In the case $p = 13$, let $g$ be a root of $x^2 + x + 2 \in GF(13)[x]$. With the help of a computer, we found the following two sets of type Q in $PG(3, 13)$.

The union of the orbits

$$(1, g^5), (1, g^6), (1, g^8), (1, g^{13}), (1, g^{15}), (1, g^{17}), (1, g^{24}), (g, g^8), (g, g^9), (g, g^{10}), (g, g^{16}), (g, g^{23}), (1, 0)$$

forms a set of type Q in $PG(3, 13)$, which we will denote by $C_0$. And the union of the orbits

$$(1, 1), (1, g^2), (1, g^4), (1, g^7), (1, g^8), (1, g^{12}), (1, g^{25}), (g, g), (g, g^8), (g, g^9), (g, g^{11}), (g, g^{13}), (g, g^{24}), (g, g^{27}), (0, 1)$$

forms another set of type Q in $PG(3, 13)$, which we denote by $C_1$. Let $S = \{ L_d \mid d \in GF(13^2) \} \cup \{ L_{-d} \}$. We have seen that each orbit of $T$ intersects the lines in $S$ in 0 or 3 points, also no two orbits of $T$ in $C_0$, $C_1$ intersect the same line, hence $C_0$, $C_1$ satisfy the conditions of Theorem 2.2. Therefore there exists a Hadamard difference set in $H \times (Z_5)^4$, where $H$ is either group of order 4. We state this as a corollary.
forms another set of type $Q$, which we will denote by $C_1$. Let $S = \{ L_d \mid d \in GF(13^2) \} \cup \{ L_\infty \}$. It is easy to see that $S$, $C_0$, $C_1$ satisfy the conditions in Theorem 2.2.

By Theorem 2.2, we have

**Corollary 5.2.** There exists a Hadamard difference set in $H \times (Z_{13})^4$, where $H$ is either the Klein 4-group or the cyclic group of order 4; in the first case the Hadamard difference set is reversible.

When $p = 17$, let $g$ be a root of $x^2 + x + 3 \in GF(17)[x]$. With the help of a computer, we found the following two sets of type $Q$ in $PG(3, 17)$. The union of the orbits

\[
(1, g^3), (g, g), (1, g^7), (g, g^6), (1, g^{12}), (g, g^{11}), (1, g^{15}),
\]
\[
(g, g^{14}), (1, g^8), (g, g^9), (1, g^{26}), (g, g^{25}), (1, g^{35}), (g, g^{31}), (1, g^{34}),
\]
\[
(g, g^{33}), (1, g^{21}), (1, g^{22}), (1, 0)
\]
forms a set of type $Q$ in $PG(3, 17)$, which we will denote by $C_0$. And the union of the following orbits

\[
(1, g^5), (g, g^4), (1, g^6), (g, g^5), (1, g^9), (g, g^8), (1, g^{10}),
\]
\[
(g, g^9), (1, g^{11}), (g, g^8), (1, g^{17}), (g, g^{16}), (g, g^{17}), (1, g^{31}),
\]
\[
(g, g^{30}), (1, g^4), (g, g^{20}), (0, 1)
\]
forms another set of type $Q$ in $PG(3, 17)$, which will be denoted by $C_1$. Let $S = \{ L_d \mid d \in GF(17^2) \} \cup \{ L_\infty \}$. Then it is easy to check that $S$, $C_0$, $C_1$ satisfy the conditions in Theorem 2.2.

By Theorem 2.2, we have

**Corollary 5.3.** There exists a Hadamard difference set in $H \times (Z_{17})^4$, where $H$ is either the Klein 4-group or the cyclic group of order 4; in the first case, the Hadamard difference set is reversible.

**Remark.** We give more details about our computer search in what follows. In order to search for sets of type $Q$ in $\mathbb{Z}_3$ by computer, we first noted that $T$ also permutes the planes in four “short” orbits and $4(p + 1)$ “long” orbits. We formed a square nonnegative integral matrix $M$ whose rows were indexed by the orbits of $T$ on the points, whose columns were indexed by the orbits of $T$ on the planes, and where the entry in row $i$ and column $j$ was the the cardinality of the intersection of a (any) plane in plane-orbit $j$ with the $i$th orbit of points. A union of point-orbits is a set of type $Q$ if and only if the sum of the corresponding rows of $M$ has entries $(p + 1)^2/4$ only.
For example, when $p = 17$, the matrix $M$ is square of order 76. The sum of all rows was a constant vector of 307s. We searched for 19 rows (one row corresponding to a short orbit and the others to long orbits) so that the sum of the 19 rows had entries 64 and 81 only. Our search was not exhaustive but simply moved from one set of 19 rows to another set by deleting one row—with a large entry in a column where the sum exceeded 81—and randomly adding another one. This was done with Mathematica on a PC. Finally, using a composition theorem of Turyn [9], it is routine to construct $(4m^2, 2m^2-m, m^2-m)$ Hadamard difference sets with $m = 2^{3+5^2+13^{2+1}} 17^{2+1} p_1^{c_1} p_2^{c_2} \cdots p_t^{c_t}$, where $a$, $b$, $c_1$, $c_2$, $c_t$ are positive integers and each $p_j$ is a prime congruent to 3 modulo 4, $1 \leq j \leq t$.

ACKNOWLEDGMENTS

We thank G. Ebert, W. Kantor, and V. Tonchev for their helpful discussions.

REFERENCES

5. M. van Eupen and V. D. Tonchev, The existence of a reversible Hadamard difference set in $Z_2 \times Z_2 \times (Z_2^5)$ and an infinite class of Williamson matrices, preprint, Oct. 1995.