Strong difference families with special patterns

Yanxun Chang\textsuperscript{a}, Simone Costa\textsuperscript{b}, Tao Feng\textsuperscript{a}, Xiaomiao Wang\textsuperscript{c}

\textsuperscript{a}Department of Mathematics, Beijing Jiaotong University, Beijing 100044, P. R. China
\textsuperscript{\textit{b}}Dipartimento DII, Università degli Studi di Brescia, Via Branze 38 - 25123 Brescia, Italy
\textsuperscript{\textit{c}}Department of Mathematics, Ningbo University, Ningbo 315211, P. R. China

yxchang@bjust.edu.cn, simone.costa@unibs.it, tfeng@bjust.edu.cn, wangxiaomiao@nbu.edu.cn

Abstract: Two kinds of patterns of strong difference families are introduced to produce new relative difference families from the point of view of both asymptotic existences and concrete examples. As applications, several classes of optimal optical orthogonal codes with weight 5, 6, 7, or 8 are obtained, and group divisible designs of type $30^w$ with block size 6 are discussed.

Keywords: relative difference family; strong difference family; cyclotomic class

1 Introduction

Throughout this paper, sets and multisets will be denoted by curly braces \{\} and square brackets [], respectively. Every union will be understood as multiset union with multiplicities of elements preserved. $A \cup A \cup \cdots \cup A$ ($h$ times) will be denoted by $hA$. Denote by $\mathbb{Z}_v$ the cyclic group of order $v$.

Definition 1. Let $\Sigma = [F_1, F_2, \ldots, F_s]$ be a family of multisets of size $k$ of a group $(G, +)$ of order $g$, where $F_i = \{f_{i,1}, f_{i,2}, \ldots, f_{i,k}\}$ for $1 \leq i \leq s$. $\Sigma$ is said to be a $(G, k, \mu)$ strong difference family, or a $(g, k, \mu)$-SDF over $G$, if the list

$$\Delta \Sigma := \bigcup_{i=1}^{s} \Delta F_i := \bigcup_{i=1}^{s} \{ f_{i,a} - f_{i,b} : 1 \leq a, b \leq k, a \neq b \} = \mu G,$$

i.e., every element of $G$ (0 included) appears exactly $\mu$ times in the multiset $\Delta \Sigma$. The members of $\Sigma$ are called base blocks.

The concept of strong difference families was introduced in \textsuperscript{5} to provide constructions of relative difference families (cf. also \textsuperscript{6} \textsuperscript{7} \textsuperscript{14}). A $(G, N, k, \lambda)$ relative difference family (DF), or $(g, n, k, \lambda)$-DF over a group $G$ of order $g$ relative to a subgroup $N$ of order $n$, is a family $\mathfrak{B} = [B_1, B_2, \ldots, B_r]$ of $k$-subsets of $G$, called base blocks, such that the list

$$\Delta \mathfrak{B} := \bigcup_{i=1}^{r} \Delta B_i := \bigcup_{i=1}^{r} \{ x - y : x, y \in B_i, x \neq y \} = \lambda (G \setminus N),$$

i.e., every element of $G \setminus N$ appears exactly $\lambda$ times in the multiset $\Delta \mathfrak{B}$ while it has no element of $N$. When $G$ is cyclic, we say that the $(g, n, k, \lambda)$-DF is cyclic (cf. \textsuperscript{14}).

This paper focuses on SDFs with special patterns. We will make use of cyclotomic conditions that generalize the procedure of \textsuperscript{10} \textsuperscript{11} to obtain new (asymptotic) existence results for DFs.

As usual we denote by $\mathbb{F}_q$ the finite field of order $q$ and by $\mathbb{F}_q^*$ its multiplicative group. If $q \equiv 1$ (mod $d$), then $C_0^{d,q}$ denotes the group of nonzero $d$th powers of $\mathbb{F}_q$ and once a primitive element $\omega$ of $\mathbb{F}_q$ has been fixed, we set $C_i^{d,q} = \omega^i \cdot C_0^{d,q}$ for $i = 0, 1, \ldots, d - 1$. Let

$$Q(d, m) = \frac{1}{4} \left( U + \sqrt{U^2 + 4d^{m-1}m} \right)^2, \text{ where } U = \sum_{h=1}^{m} \binom{m}{h} (d - 1)^h (h - 1),$$

for given positive integers $d$ and $m$. The following theorem ensures the existences of elements satisfying certain cyclotomic conditions in a finite field.

\footnote{Partially supported by Italian Ministry of Education under Grant PRIN 2015 D72F16000790001 (S. Costa). Supported by NSFC under Grant 11431003 (Y. Chang), NSFC under Grant 11871095 (T. Feng), NSFC under Grant 11771227, and Zhejiang Provincial Natural Science Foundation of China under Grant LY17A010008 (X. Wang).}
Theorem 1. [7,10] Let \( q \equiv 1 \pmod{d} \) be a prime power, let \( B = \{b_0, b_1, \ldots, b_{n-1}\} \) be an arbitrary \( m \)-subset of \( F_q \) and let \( \langle \beta_0, \beta_1, \ldots, \beta_{n-1} \rangle \) be an arbitrary element of \( \mathbb{Z}_q^m \). Set \( X = \{x \in F_q : x - b_i \in C_q^{2,q} \text{ for } i = 0, 1, \ldots, m - 1\} \). Then \( X \) is not empty for any prime power \( q \equiv 1 \pmod{d} \) and \( q > Q(d, m) \).

2 Pattern of length two

Definition 2. Let \((G, +)\) be an abelian group. A \((G, k, \mu)\)-SDF has a pattern of length two if it is the union of three families \( \Sigma_1, \Sigma_2 \) and \( \Sigma_3 \), each of which could be empty, where

1) if \( k \equiv 0 \pmod{2} \), then for any \( A \in \Sigma_1 \), \( A \) is of the form
   \[
   [x_1, \delta + x_1, x_2, \delta + x_2, \ldots, x_{[k/2]}, \delta + x_{[k/2]}]
   \]
   (resp. with a 0 at the beginning if \( k \equiv 1 \pmod{2} \)), where \( \delta \) is either an involution of \( G \) or zero, and \( \Delta[x_1, x_2, \ldots, x_{[k/2]}] \) does not contain involutions and zeros;

2) for any \( A \in \Sigma_2 \), each element of \( \Delta(A) \) is either an involution or zero;

3) for any \( A \in \Sigma_3 \), the multiplicity of \( A \) in \( \Sigma_3 \) is even and \( \Delta(A) \) does not contain involutions and zeros.

Example 1. The \((\mathbb{Z}_{10}, 5, 12)\)-SDF given below has a pattern of length two:

| \( \Sigma_1 \) | \( \Sigma_2 \) | \( \Sigma_3 \) |
|---|---|---|
| \([0, 3, 3, 7, 7]\) | \([0, 9, 6, 7, 8]\), \([0, 9, 6, 7, 8]\), \([0, 8, 4, 6, 7]\), \([0, 8, 4, 6, 7]\) |

Other examples of SDFs with a pattern of length two can be found in [5,10].

Lemma 1 (Paley SDFs [5]).

1) Let \( p \) be an odd prime power. Then the \((p, p, p - 1)\)-SDF over \( \mathbb{F}_p \) given by the single block \( \{0\} \cup 2C_q^{p,p} \), has a pattern of length two.

2) Let \( p \equiv 3 \pmod{4} \) be a prime power. Then the \((p, p + 1, p + 1)\)-SDF over \( \mathbb{F}_p \) given by the single block \( 2\{0\} \cup C_q^{2,p} \), has a pattern of length two.

We present the following example to explain how to apply SDFs with a pattern of length two to obtain DFs.

Example 2. Given any prime power \( q \equiv 1 \pmod{12} \) and \( q > Q(6, 4) \), there exists a \((\mathbb{Z}_{10} \times \mathbb{F}_q, \mathbb{Z}_{10} \times \{0, 5, 1\})\)-DF.

Proof. Take the \((\mathbb{Z}_{10}, 5, 12)\)-SDF, \( \Sigma = [A_1, A_2, \ldots, A_6] \), from Example 1, where \( A_1 = [0, 3, 3, 7, 7] \), \( A_2 = [0, 0, 5, 5] \), \( A_3 = A_4 = [0, 9, 6, 7, 8] \) and \( A_5 = A_6 = [0, 8, 4, 6, 7] \). Now, consider the family \( B = \{B_1, B_2, \ldots, B_6\} \) of base blocks whose first components come from \( \Sigma \), where

\[
B_1 = \{(0, 0), (3, y_1, 1),(3, -y_1, 1),(7, y_1, 2),(7, -y_1, 2)\};
\]
\[
B_2 = \{(0, y_2, 1), (0, y_2, 2), (0, y_2, 3), (5, y_2, 4), (5, y_2, 5)\};
\]
\[
B_3 = \{(0, y_3, 1), (9, y_3, 2), (6, y_3, 3), (7, y_3, 4), (8, y_3, 5)\};
\]
\[
B_4 = \{(0, y_4, 1), (8, y_4, 2), (4, y_4, 3), (6, y_4, 4), (7, y_4, 5)\};
\]
\[
B_5 = \{(0, y_5, 1), (8, y_5, 2), (4, y_5, 3), (6, y_5, 4), (7, y_5, 5)\};
\]

One can check that
\[
\Delta[B_1, B_2, \ldots, B_6] = \bigcup_{g \in \mathbb{Z}_{10}} \{g\} \times D_g,
\]
where \( D_g = \{1, -1\} \cdot L_g \), \( L_g = L_{-g} \) and

\[
L_0 = \{2y_1, 1, 2y_1, 2, y_2, 1 - y_2, 2, y_2, 1 - y_2, 3, y_2, 3 - y_2, 2, y_2, 4 - y_2, 5\};
\]
\[
L_1 = \{y_3, 2 - y_3, 3, y_3, 2 - y_3, 4, y_3, 4 - y_3, 3, y_3, 4 - y_3, 4, y_4, 4 - y_4, 5, y_4, 5 - y_4, 4\};
\]
\[
L_2 = \{y_5, 3 - y_5, 3, y_5, 3 - y_5, 4, y_5, 4 - y_5, 3, y_5, 4 - y_5, 4, y_5, 4 - y_5, 4\};
\]
\[
L_3 = \{y_1, 1 - y_1, 2, y_1, 2 - y_1, 3, y_1, 3 - y_1, 2, y_1, 4 - y_1, 3, y_1, 4 - y_1, 4, y_1, 4 - y_1, 3\};
\]
\[
L_4 = \{y_2, 1 - y_2, 1, y_2, 1 - y_2, 2, y_2, 4 - y_2, 2, y_2, 4 - y_2, 3, y_2, 3 - y_2, 4, y_2, 4 - y_2, 3\};
\]
\[
L_5 = \{y_2, 1 - y_2, 1, y_2, 1 - y_2, 2, y_2, 4 - y_2, 2, y_2, 4 - y_2, 3, y_2, 3 - y_2, 4, y_2, 4 - y_2, 3\}.
\]
By Theorem[1] for any prime power \( q \equiv 1 \pmod{12} \) and \( q > Q(6, 4) \), we can always require that every \( L_g \) is a system of representatives for \( C_0^{\mu/2} \) in \( F_q^* \). Therefore, given a transversal \( S \) for \( \{1, -1\} \) in \( C_0^{\mu/2} \), the family \( \{B \cdot (1, s) \mid s \in S, B \in \mathcal{B}\} \) is a \((\mathbb{Z}_{10} \times F_q, \mathbb{Z}_{10} \times \{0\}, 5, 1)\)-DF.

As a generalization of Example[2] we have the following theorem.

**Theorem 2.** If there exists a \((G, k, \mu)\)-SDF with a pattern of length two, then there exists a \((G \times F_q, G \times \{0\}, k, 1)\)-DF for any prime power \( q \equiv 1 \pmod{\mu} \) and \( q > Q(\mu/2, k - 1) \).

**Proof.** Let \( \Sigma = \{A_1, A_2, \ldots, A_n\} \) be a \((G, k, \mu)\)-SDF with a pattern of length two and \( \Sigma_3 = \{A_{t+1}, A_{t+2}, \ldots, A_n\} \), where \( A_{t+1} = A_{t+2}, \ldots, A_n - A_1 \). Note that \( \mu \) is necessarily even since the zero element of \( G \) clearly appears an even number of times in the list of differences of any multisubset of \( G \). Now, consider the family \( \mathcal{B} = \{B_1, B_2, \ldots, B_m\} \), where

- if \( k \) is even and \( A_i = [x_i, 1] \), then \( B_i = \{(x_{i, 1}, y_{i, 1}), (x_{i, 2}, y_{i, 2}), \ldots, (x_{i,k/2}, y_{i,k/2})\} \) (resp. with \( (0, 0) \) at the beginning if \( k \equiv 1 \pmod{2} \));
- if \( A_i = [x_i, 1] \), then \( B_i = \{(x_{i, 1}, y_{i, 1}), (x_{i, 2}, y_{i, 2}), \ldots, (x_{i,k}, y_{i,k})\} \);
- if \( A_i = A_{i+1} = [x_i, 1] \), then \( B_i = \{(x_{i, 1}, y_{i, 1}), (x_{i, 2}, y_{i, 2}), \ldots, (x_{i,k}, y_{i,k})\} \)

and \( B_{i+1} = (1, -1) \cdot B_i \).

Since \( \Sigma \) has a pattern of length two, one can check that

\[ \Delta[B_1, B_2, \ldots, B_m] = \bigcup_{g \in G} \{g\} \times D_g, \]

where \( D_g = \{1, -1\} \cdot L_g, L_g = L_{-g} \) and each element of \( L_g \) is of one of the forms: \( y_i, y_j, y_i, y_j, y_i, y_j \) and \( 2y_{i,j} \). By Theorem[1] for any prime power \( q \equiv 1 \pmod{\mu} \) and \( q > Q(\mu/2, k - 1) \), it can be required that every \( L_g \) is a system of representatives for \( C_0^{\mu/2} \) in \( F_q^* \). Therefore, given a transversal \( S \) for \( \{1, -1\} \) in \( C_0^{\mu/2} \), the family \( \{B \cdot (1, s) \mid s \in S, B \in \mathcal{B}\} \) is a \((G \times F_q, G \times \{0\}, k, 1)\)-DF.

**Remark 1.** Let \( k \) be odd and \( \Sigma \) be a \((G, k, \mu)\)-SDF with a pattern of length two. If \( \Sigma \) consists only of base blocks belonging to \( \Sigma_1 \), then the lower bound on \( q \) in Theorem[2] can be improved. That is to say, there exists a \((G \times F_q, G \times \{0\}, k, 1)\)-DF for any prime power \( q \equiv 1 \pmod{\mu} \) and \( q > Q(\mu/2, k - 2) \) (in this case every \( y_{i,j} \) contributes at most \( k - 2 \) cyclotomic conditions).

**Remark 2.** Start from the Paley SDFs from Lemma[4] and then use Remark[1] and Theorem[2]. We can obtain the following DFs:

1. there exists an \((\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p, 1)\)-DF for any odd prime powers \( p, q \) with \( q \equiv 1 \pmod{p-1} \) and \( q > Q((p-1)/2, p-2) \);
2. there exists an \((\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, p+1, 1)\)-DF for any prime powers \( p, q \) with \( p \equiv 3 \pmod{4} \), \( q \equiv 1 \pmod{p+1} \) and \( q > Q((p+1)/2, p) \).

These DFs can also be found in Theorems 3.11 and 3.12 of [10].

Using SDFs with a pattern of length two listed in Example[1] and Appendix, and applying Theorem[2] and Remark[1] we get the DFs of Theorem[3]. For the values of \( q \) smaller than the lower bounds, we found, by computer search, all the DFs that satisfy the required conditions of the proof except for the cases of \( (h, q, k, \lambda) \in \{(10, 13, 5, 1), (30, 7, 6, 1), (5, 13, 6, 1), (5, 37, 6, 1), (15, 13, 6, 1), (25, 7, 6, 1), (35, 7, 6, 1), (45, 7, 6, 1), (21, 13, 7, 1), (35, 7, 7, 1), (49, 7, 7, 1)\) \). The interested reader may get a copy of these data from the authors.

For \( (h, q, k, \lambda) = (10, 13, 5, 1) \), we give an explicit construction of a \((\mathbb{Z}_{10} \times \mathbb{F}_{13}, \mathbb{Z}_{10} \times \{0\}, 5, 1)\)-DF:
\((0, 0), (3, 1), (3, 12), (7, 3), (7, 10)\),
\((0, 0), (0, 1), (0, 4), (5, 3), (5, 8)\),
\((1, x) \cdot \{(0, 0), (9, 4), (6, 10), (7, 5), (8, 6)\},
\((1, x) \cdot \{(0, 0), (8, 2), (4, 7), (6, 12), (7, 9)\}.

where \(x\) runs over \(C_0^{6,13}\).

For \((h, q, k, \lambda) = (5, 13, 6, 1)\), an exhaustive search shows that no \((\mathbb{Z}_5 \times \mathbb{F}_{13}, \mathbb{Z}_6 \times \{0\}, 6, 1)\)-DF exists.

For \((h, q, k, \lambda) \in \{(30, 7, 6, 1), (5, 37, 6, 1), (15, 13, 6, 1), (35, 7, 6, 1), (45, 7, 6, 1), (21, 13, 7, 1)\}\), we give an explicit construction of a \((\mathbb{Z}_h \times \mathbb{F}_q, \mathbb{Z}_k \times \{0\}, k, 1)\)-DF as follows:

\[
\begin{array}{|c|c|}
\hline
\text{(30 \times 7, 30, 6, 1)-DF} & \{0, 11, 30, 111, 131, 171\}, \{0, 12, 27, 73, 148, 165\}, \\
\text{(5 \times 37, 5, 6, 1)-DF} & \{0, 1, 3, 25, 34, 128\} \times 29^i, \{0, 5, 37, 43, 53, 139\} \times 29^i, \text{where } i = 0, 1. \\
\text{(15 \times 13, 15, 6, 1)-DF} & \{0, 1, 3, 11, 42, 123\} \times 26^i, \{0, 5, 19, 77, 145, 169\} \times 26^i, \text{where } i = 0, 1. \\
\text{(35 \times 7, 35, 6, 1)-DF} & \{0, 10, 30, 85, 130, 195\}, \{0, 1, 3, 54, 158, 167\} \times 116^i, \\
\text{(45 \times 7, 45, 6, 1)-DF} & \{0, 1, 3, 11, 61, 244\} \times 16^i, \{0, 4, 29, 135, 171, 278\} \times 16^i, \\
\text{(21 \times 13, 21, 7, 1)-DF} & \{0, 1, 3, 9, 88, 116, 135\} \times 16^i, \{0, 4, 37, 86, 127, 204, 211\} \times 16^i, \text{where } i = 0, 1, 2. \\
\hline
\end{array}
\]

Theorem 3. Let \(q\) be a prime. Then there exists a \((\mathbb{Z}_h \times \mathbb{F}_q, \mathbb{Z}_k \times \{0\}, k, 1)\)-DF in the following cases:

\[
\begin{array}{|c|c|}
\hline
\text{(hq, h, k, \lambda)} & \text{possible exceptions / definite ones} \\
\hline
(2q, 2, 5, 1): q \equiv 1 \pmod{20} & \text{} \\
(10q, 10, 5, 1): q \equiv 1 \pmod{12} & \text{} \\
(12q, 12, 5, 1): q \equiv 1 \pmod{20} & \text{} \\
\hline
\text{(hq, h, 6, 1): h \in \{25, 30, 35, 45\}, q \equiv 1 \pmod{6}} & (25 \times 7, 25, 6, 1) \\
\hline
\text{(hq, h, 6, 1): h \in \{5, 15\}, q \equiv 1 \pmod{12}} & (5 \times 13, 5, 6, 1) \\
\hline
\text{(hq, h, 7, 1): h \in \{35, 49\}, q \equiv 1 \pmod{6}} & (35 \times 7, 35, 7, 1), (49 \times 7, 49, 7, 1) \\
\text{(21q, 21, 7, 1): q \equiv 1 \pmod{12}} & \text{} \\
\hline
\end{array}
\]

3 Pattern of length four

Definition 3. Let \((G, +)\) be an abelian group of odd order. A \((G, k, \mu)\)-SDF has a pattern of length four if \(k \equiv 0, 1 \pmod{4}\) and it is the union of two families \(\Sigma_1\) and \(\Sigma_2\) (\(\Sigma_2\) could be empty), where:

1) if \(k \equiv 0 \pmod{4}\), then \(\Sigma_1\) consists of only one base block (called the distinguished base block) of the form

\[\{x, x_1, x_1, x_1, \ldots, x_1, x_{k/4}, -x_{k/4}, -x_{k/4}, -x_{k/4}\}\]

(resp. with a 0 at the beginning if \(k \equiv 1 \pmod{4}\)) and \(\Delta[x, x_1, x_2, x_2, \ldots, x_{k/4}, -x_{k/4}]\) does not contain zeros;

2) for any \(A \in \Sigma_2\), the multiplicity of \(A\) in \(\Sigma_2\) is doubly even and \(\Delta(A)\) does not contain zeros.

Remark 3. According to the definition of a \((G, k, \mu)\)-SDF, \(\Sigma\), with a pattern of length four, the zero element of \(G\) must appear \([k/4] \times 4\) times in \(\Delta \Sigma\), so \(\mu = 4[k/4]\).

Example 3. The \((\mathbb{Z}_{45}, 5, 4)\) given below has a pattern of length four:

\[
\begin{array}{|c|c|}
\hline
\Sigma_1 & \Sigma_2 \\
\hline
[0, 1, 1, -1, -1] & [0, 3, 7, 13, 30], [0, 3, 7, 13, 30], [0, 3, 7, 13, 30], [0, 5, 14, 26, 34], [0, 5, 14, 26, 34], [0, 5, 14, 26, 34], [0, 5, 14, 26, 34] \\
\hline
\end{array}
\]

4
Other examples of SDFs with a pattern of length four can be found in [5, 10].

**Lemma 2.** [5] Let \( p \equiv 1 \pmod{4} \) be an odd prime power. Then the \((p, p, p − 1)\)-SDF over \( \mathbb{F}_p \) given by the single block \( \{0\} \cup \mathbb{Z}^2_0 \), has a pattern of length four.

We present the following example to explain how to apply SDFs with a pattern of length four to obtain DFs.

**Example 4.** Given any prime power \( q \equiv 1 \pmod{4} \), there exists a \((\mathbb{Z}_{45} \times \mathbb{F}_q, \mathbb{Z}_{45} \times \{0\})\)-DF.

**Proof.** Take the \((\mathbb{Z}_{45}, 5, 4)\)-SDF, \( \Sigma = [A_1, A_2, \ldots, A_9] \), from Example [3] where \( A_1 = [0, 1, 1, -1, -1], A_2 = A_3 = A_4 = A_5 = [0, 3, 7, 13, 30] \) and \( A_6 = A_7 = A_8 = A_9 = [0, 5, 14, 26, 34] \). Let \( \xi \) be a primitive 4th root of unity in \( \mathbb{F}_q \). Now, consider the family \( \mathcal{B} = \{B_1, B_2, \ldots, B_9\} \) of base blocks whose first components come from \( \Sigma \), where

\[
B_1 = \{0, 0\}, \quad B_2 = \{(0, y_2, 1), (3, y_2, 2), (7, y_2, 3), (13, y_2, 4), (30, y_2, 5)\},
\]

\[
B_3 = \{1, \xi\} \cdot B_2; \quad B_4 = \{1, -1\} \cdot B_3; \quad B_5 = \{1, -\xi\} \cdot B_2;
\]

\[
B_6 = \{(0, y_6, 1), (5, y_6, 2), (14, y_6, 3), (26, y_6, 4), (34, y_6, 5)\},
\]

\[
B_7 = \{1, \xi\} \cdot B_6; \quad B_8 = \{1, -1\} \cdot B_7; \quad B_9 = \{1, -\xi\} \cdot B_6.
\]

One can check that

\[
\Delta[B_1, B_2, \ldots, B_9] = \bigcup_{g \in \mathbb{Z}_{45}} \{g\} \times D_g,
\]

where \( D_g = \{1, -1, \xi, -\xi\} \cdot L_g \) and \( |L_g| = 1 \) for any \( g \in \mathbb{Z}_{45} \). For any prime power \( q \equiv 1 \pmod{4} \), we can always require that each \( L_g \) does not contain zero. Therefore, given a transversal \( S \) for \( \{1, -1, \xi, -\xi\} \) in \( F_q \), the family \( \{B \cdot (1, s) \mid s \in S, B \in \mathcal{B}\} \) is a \((\mathbb{Z}_{45} \times \mathbb{F}_q, \mathbb{Z}_{45} \times \{0\})\)-DF.

Before stating a theorem similar to Theorem [2] we prove a technical lemma. A **spanning subgraph** of a graph \( G \) is a subgraph obtained by edge deletions only, in other words, a subgraph whose vertex set is the entire vertex set of \( G \). If \( E \) is the set of deleted edges, this subgraph of \( G \) is denoted by \( G \setminus E \). A subgraph obtained by vertex deletions only is called an **induced subgraph**. If \( U \) is the set of vertices deleted, the resulting subgraph is denoted by \( G \setminus U \).

**Lemma 3.** Given \( r \geq 5 \), for any \( a \in \mathbb{Z}_r \) and any set of ordered pairs \( P \) from \( \mathbb{Z}_r \) satisfying

1. \( x \neq y \) for any \( (x, y) \in P \),
2. the multisets \( \{x \mid (x, y) \in P\} \) and \( \{y \mid (x, y) \in P\} \) are simple sets,

there exists a bijection \( \pi : \mathbb{Z}_r \to \mathbb{Z}_r \) such that \( \pi(x) \neq \pi(y) - a \pmod{r} \) for any \( (x, y) \in P \).

**Proof.** When \( a = 0 \), any bijection \( \pi : \mathbb{Z}_r \to \mathbb{Z}_r \) can lead to the desired conclusion. Assume that \( a \neq 0 \).

We first give an equivalent description of this lemma in the language of graphs. We define a directed graph \( \overrightarrow{H} \), whose vertices are taken from \( \mathbb{Z}_r \). For any two vertices \( x, y \), \((x, y)\) is a directed edge of \( \overrightarrow{H} \) if and only if \( (x, y) \in P \). Since the indegree and outdegree of each vertex of \( \overrightarrow{H} \) are at most 1 and \( \overrightarrow{H} \) contains no loop, we can add directed edges into \( \overrightarrow{H} \) to form a directed graph \( \overrightarrow{H}' \) such that the indegree and outdegree of each vertex of \( \overrightarrow{H}' \) are both 1 and \( \overrightarrow{H}' \) contains no loop. It follows that \( \overrightarrow{H}' \) is the union of disjoint directed cycles of lengths \( l_1, l_2, \ldots, l_s \), where each \( l_i \geq 2 \) and \( \sum_{i=1}^{s} l_i \leq r \). Now regard the mapping \( \pi \) as an embedding of \( \overrightarrow{H}' \) in the complete directed graph \( \overrightarrow{K}_r \) defined on \( \mathbb{Z}_r \). Consider the directed graph \( \overrightarrow{C} \) whose edge set is given by the pairs \( \{(x, x+ a) \mid x \in \mathbb{Z}_r\} \). \( \overrightarrow{C} \) is the union of directed cycles whose length \( l \) is the order of \( a \) in \( \mathbb{Z}_r \). Now we prove that for any \( r \geq 5 \), \( \overrightarrow{H}' \) can be embedded in \( \overrightarrow{K}_r \setminus E(\overrightarrow{C}) \).

Case 1 \( l = 2 \): Here \( r \) must be even, so \( r \geq 6 \). Given any embedding of \( \overrightarrow{H}' \) in \( \overrightarrow{K}_r \), it suffices to show that there is a 1-factor in the undirected graph \( K_r \setminus E(\overrightarrow{H}') \). This 1-factor can be used as \( \overrightarrow{C} \). A necessary and sufficient condition for the existence of a 1-factor in a graph is given by the Tutte’s theorem (see Theorem 16.13 in [2]) that says:
A graph $G$ has a 1-factor if and only if $o(G - U) \leq |U|$ for all $U \subseteq V(G)$, where $o(G - U)$ is the number of connected components with an odd number of vertices in $G - U$.

Let $U \subseteq V(K_r)$. If $U = \emptyset$, then since $r \geq 6$ and $r$ is even, $(K_r \setminus E(H')) \setminus U$ is a connected graph with an even number of vertices, which yields $o((K_r \setminus E(H')) \setminus U) = 0 = |U|$. If $|U| \in \{r - 1, r\}$, then since $r \geq 6$, $o((K_r \setminus E(H')) \setminus U) \leq |U|$. If $U \neq \emptyset$ and $(K_r \setminus E(H')) \setminus U$ is a connected graph, then $o((K_r \setminus E(H')) \setminus U) \leq 1 \leq |U|$. In what follows assume that $1 \leq |U| \leq r - 2$ and $(K_r \setminus E(H')) \setminus U$ is a disconnected graph.

For any two vertices $x$ and $y$ in $K_r - U$, $x$ and $y$ are not connected in $(K_r \setminus E(H')) \setminus U$ if and only if $x$ and $y$ are adjacent in a cycle $(x, y, v_3, \ldots, v_i)$ of $H'$ for some $1 \leq i \leq s$, and

1. $V(K_r) \setminus U = \{x, y\}$ when $l_i = 2$,
2. $V(K_r) \setminus U \subseteq \{x, y, v_3\}$ when $l_i = 3$,
3. $V(K_r) \setminus U \subseteq \{x, y, v_3, v_i\}$ when $l_i = 4$,
4. $V(K_r) \setminus U \subseteq \{x, y, v_i\}$ or $\{x, y, v_i\}$ when $l_i \geq 5$.

Since $r \geq 6$, when $l_i \in \{2, 3\}$ we have that $o((K_r \setminus E(H')) \setminus U) \leq 3 \leq |U|$; in case $l_i \geq 4$, instead, it holds that $o((K_r \setminus E(H')) \setminus U) \leq 2 \leq |U|$.

Case 2 $l \neq 2$: Assume, up to isomorphism, that $\overrightarrow{C}$ is the union of the clockwise oriented cycles $(l - 1, l - 2, \ldots, 0), (2l - 1, 2l - 2, \ldots, l), \ldots, (r - 1, r - 2, \ldots, r - l)$. If every $l_i \neq 2$ for $1 \leq i \leq s$, then we can embed $\overrightarrow{H}$ in $K_r^2 \setminus E(\overrightarrow{C})$ as the union of the clockwise oriented cycles

$$(0, 1, \ldots, l_1 - 1), (l_1, l_1 + 1, \ldots, l_1 + l_2 - 1), \ldots, (\sum_{i=1}^{k-1} l_i, \sum_{i=1}^{k-1} l_i + 1, \ldots, \sum_{i=1}^{k} l_i - 1).$$

Assume that $l_1 \leq l_2 = \cdots = l_{s'} = 2$ and $l_i \neq 2$ for $i > s'$. We first embed the union $\overrightarrow{H}_1$ of $s'$ cycles of length 2 in $K_r^2 \setminus \overrightarrow{C}$; for $s' \geq 3$, this embedding can be provided as in Case 1 considering only the first 2$s'$ vertices; for $s' \in \{1, 2\}$, this embedding can be checked by hand since $r \geq 5$. Then denote by $v_1, v_2, \ldots, v_{r-2s'}$ the vertices of $V(K_r^2) \setminus V(\overrightarrow{H}_1)$ such that $v_1 < v_2 < \cdots < v_{r-2s'}$. Now we can embed $\overrightarrow{H}_2 = \overrightarrow{H} \setminus \overrightarrow{H}_1$ as the union of the clockwise oriented cycles

$$(v_1, \ldots, v_{l_1-1}), (v_{l_1-1}, \ldots, v_{l_1+i_1}), \ldots, (v_{l_{s'+1}+i_{s'+2}+1}, \ldots, v_{l_{s'+1}+i_{s'+2}+i_{s'+3}}), \ldots.$$ 

This completes the proof.

**Theorem 4.** If there exists a $(G, k, \mu)$-SDF with a pattern of length four, whose distinguished base block is denoted by $A$, then for any prime power $q \equiv 1 \pmod{\mu}$ and $q > Q(\mu, k - 1)$, there exists a $(G \times \mathbb{F}_q, G \times \{0, k\})$-DF in the following cases

1. $k \equiv 0 \pmod{4}$;
2. $k = 5$;
3. $k \in \{9, 13, 17\}$ and $x_1 \neq \pm 2x_2$ for any nonzero $x_1, x_2 \in A$ ($x_1$ could be $x_2$);
4. $k \equiv 1 \pmod{4}, k \geq 21$ and $3x \neq 0$ for any nonzero $x \in A$.

**Proof.** Let $\Sigma = \{A_1, A_2, \ldots, A_n\}$ be the given $(G, k, \mu)$-SDF with a pattern of length four, where $A_1 = A, A_2 = A_3 = A_4 = A_5, \ldots, A_{n-3} = A_{n-2} = A_{n-1} = A_n$. By Remark 3, $\mu = 4|k|/4$. Let $\xi$ be a primitive 4th root of unity in $\mathbb{F}_q^*$. Consider the family $\mathcal{B} = \{B_1, B_2, \ldots, B_n\}$, where

- if $k \equiv 0 \pmod{4}$ and $A_1 = [x_1, x_1 - x_1, -x_1, x_1, \ldots, x_1, (k/4), -x_1, (k/4), -x_1]$, then

  $$B_1 = \{(x_1, y_1), (x_1, y_1, -y_1, x_1, (k/4), -y_1, (k/4), x_1, (k/4)), \ldots, (x_1, (k/4), y_1, (k/4), x_1, (k/4), y_1, (k/4)), \ldots\}$$

  (resp. with a $(0, 0)$ at the beginning if $k \equiv 1 \pmod{4}$);
- If \( A_i = A_{i+1} = A_{i+2} = A_{i+3} = [x_{i,1}, x_{i,2}, \ldots, x_{i,k}] \) for \( i \equiv 2 \pmod{4} \), then

\[
B_i = \{(x_{i,1}, y_{i,1}), (x_{i,2}, y_{i,2}), \ldots, (x_{i,k}, y_{i,k})\},
\]

and

\[ B_{i+1} = (1, \xi) \cdot B_i, \quad B_{i+2} = (1, -1) \cdot B_i, \quad B_{i+3} = (1, -\xi) \cdot B_i. \]

One can check that

\[
\Delta[B_1, B_2, \ldots, B_n] = \bigcup_{g \in G} \{g \times D_g, \}
\]

where \( D_g = \{1, -1, \xi, -\xi\} \cdot L_g, \quad L_g = L_{-g} \) and each element of \( L_g \) is one of the following forms:

\[
y_{1,j_1}, 2y_{1,j_1} (1 - \xi)y_{1,j_1}, y_{1,j_2} \pm \xi y_{1,j_2}, y_{1,j_3} \pm y_{1,j_2}, y_{1,j_1} - y_{1,j_2}, \text{ and } y_{1,j_1} - y_{1,j_3} \text{ for } i \geq 2. \]

Note that if \( 2y_{1,j_1} \in L_{0}, (1 - \xi)y_{1,j_1} \in L_{\pm 2x_{i,j_1}}, \text{ and when } k \equiv 1 \pmod{4}, y_{1,j_1} \in L_{\pm x_{i,j_1}}. \text{ If } \quad \quad \text{If every } L_g, g \in G, \text{ is a system of representatives for } C^0_{4/4} \text{ in } \mathbb{F}_4^*, \text{ then given a transversal } S \text{ for } \{1, -1, \xi, -\xi\} \text{ in } C^0_{4/4}, \text{ the family } \{B \cdot (1, s) \mid s \in S, B \in B\} \text{ forms a } (G \times \mathbb{F}_q, G \times \{0\}, k)-1-\text{DF. By Theorem 1 this can be done for any prime power } q \equiv 1 \pmod{4} \text{ and } q > Q(\mu/4, k - 1) \text{ if no } L_g \text{ contains a 2-subset of the form } \{y_{1,j_1}, (1 - \xi)y_{1,j_1}\}. \]

When \( k \equiv 0 \pmod{4}, y_{1,j_1} \text{ cannot occur in any } L_{g}, \text{ so no } L_g \text{ contains a 2-subset of the form } \{y_{1,j_1}, (1 - \xi)y_{1,j_1}\}. \]

When \( k = 5, \quad L_g = 1 \text{ for any } g \in G, \text{ so no } L_g \text{ contains a 2-subset of the form } \{y_{1,j_1}, (1 - \xi)y_{1,j_1}\}. \]

When \( k \equiv 1 \pmod{4}, k \geq 9 \text{ and some } L_q \text{ contains a 2-subset of the form } \{y_{1,j_1}, (1 - \xi)y_{1,j_1}\}, \text{ since } y_{1,j_1} \in L_{\pm x_{i,j_1}} \text{ and } (1 - \xi)y_{1,j_1} \in L_{\pm 2x_{i,j_1}}. \text{ We have } g = \pm x_{1,j_1} = \pm 2x_{1,j_2}. \text{ Thus if } x_{1,j_1} \neq \pm 2x_{1,j_2} \text{ for any nonzero } x_{1,j_1}, x_{1,j_2} \in A_1 (j_1 \text{ could be } j_2), \text{ then no } L_g \text{ contains a 2-subset of the form } \{y_{1,j_1}, (1 - \xi)y_{1,j_1}\}. \]

Assume that \( k \equiv 1 \pmod{4} \text{ and } k \geq 21. \text{ We shall show that even if some } L_q \text{ contains a 2-subset of the form } \{y_{1,j_1}, (1 - \xi)y_{1,j_1}\}, \text{ we can still require every } L_g, g \in G, \text{ is a system of representatives for } C^0_{4/4} \text{ in } \mathbb{F}_4^*, \text{ provided for any nonzero } x \in A, 3x \neq 0. \]

Let \( P \) be the set of pairs \((y_{1,j_1}, y_{1,j_2})\) for all possible \( j_1 \text{ and } j_2 \text{ such that } (y_{1,j_1}, (1 - \xi)y_{1,j_2}) \text{ is a 2-subset of some } L_g. \text{ If } \{y_{1,j_1}, y_{1,j_2}\} \text{ and } (y_{1,j_1}, y_{1,j_1}) \in P, \text{ then } x_{1,j_1} = \pm 2x_{1,j_1} = \pm 2x_{1,j_2} \text{ and hence } 2(x_{1,j_2} \pm x_{1,j_1}) = 0 \text{ but, since } \Delta[x_{1,j_1} - x_{1,j_1}, \ldots, x_{1,k/4}, -x_{1,k/4}] \text{ does not contain involutions } \text{ (} G \text{ is of odd order) and zeros this is possible only if } x_{1,j_2} = j_3. \text{ If } (y_{1,j_2}, y_{1,j_1}) \text{ and } (y_{1,j_1}, y_{1,j_1}) \in P, \text{ then } x_{1,j_1} = \pm 2x_{1,j_1} = \pm 2x_{1,j_2} \text{ but this is possible only if } j_2 = j_3. \text{ It follows that the multiset } \{y_{1,j_1} \mid (y_{1,j_1}, y_{1,j_2}) \in P\} \text{ and } \{y_{1,j_2} \mid (y_{1,j_1}, y_{1,j_2}) \in P\} \text{ are simple sets. Moreover, if } (y_{1,j_1}, y_{1,j_2}) \in P \text{ and } j_1 = j_2, \text{ then } x_{1,j_1} = \pm 2x_{1,j_1} \text{ and hence } 3x_{1,j_1} = 0. \text{ It is impossible since for any nonzero } x \in A, 3x \neq 0. \]

Let \( r = \mu/4 = [k/4] \geq 5. \text{ Let } 1 - \xi \in C^r_{\sigma - n}. \text{ Since } L_0 = \{2y_{1,1}, 2y_{1,2}, \ldots, 2y_{r,1}\}, \text{ which is a system of representatives for } C^r_{\sigma} \text{ in } \mathbb{F}_4^*, \text{ we can regard the pairs of } P \text{ as pairs of element of } \mathbb{Z}_r. \text{ By Lemma 3 there exists a bijection } \pi : \{y_{1,1}, y_{1,2}, \ldots, y_{1,r}\} \rightarrow \mathbb{Z}_r \text{ such that } \pi(y_{1,j}) \neq \pi(y_{1,j}) + \alpha \text{ (mod } r\text{) for any } (y_{1,j_1}, y_{1,j_2}) \in P. \text{ Thus we can assign to each } y_{1,j} \text{ the cyclotomic class given by the map } \pi. \]

**Remark 4.** Let \( \Sigma \) be a \((G, k, \mu)-\text{SDF with a pattern of length four. If } \Sigma = \Sigma_1, i.e., \Sigma \text{ consists only of the distinguished base block, then every cyclotomic contribution at most } k - 3 \text{ cyclotomic conditions when } k \equiv 0 \pmod{4} \text{ (resp. } k - 4 \text{ when } k \equiv 1 \pmod{4}. \text{ Therefore, the lower bound on } q \text{ in Theorem 3 can be improved, that is to say, } q > Q(\mu/4, k - 3) \text{ when } k \equiv 0 \pmod{4} \text{ and } q > Q(\mu/4, k - 4) \text{ when } k \equiv 1 \pmod{4}). \]

**Remark 5.** Start from the Paley SDF from Lemma 2. By using Theorem 3 and Remark 4, we have that there exists an \((\mathbb{F}_p \times \mathbb{F}_q, \mathbb{F}_p \times \{0\}, 1)-\text{DF for any prime power } p \text{ and } q \text{ with } p \equiv 1, 5 \pmod{12}, p \notin \{13, 17\}, q \equiv 1 \pmod{p - 1} \text{ and } q > Q((p - 1)/4, p - 4) \text{ (see also Theorem 3.8(1) of [10]).} \]

Using SDFs with a pattern of length four listed in Example 3 and Appendix, and applying Theorem 4 we can get the following DFs in Theorem 5. For the values of } q \text{ smaller than the lower bounds, we found, by computer search, all the DFs that satisfy the required conditions of the proof except for the cases of } (h, q, k, \lambda) \in \{(63, 17, 8, 1), (63, 41, 8, 1), (81, 17, 9, 1), (81, 41, 9, 1)\}. \text{ The interested reader may get a copy of these data from the authors. For } (h, q, k, \lambda) = (63, 41, 8, 1), \text{ we give here an explicit construction for a } (\mathbb{Z}_{63} \times \mathbb{F}_{41}, \mathbb{Z}_{63} \times \{0\}, 8, 1)-\text{DF:}
(1, x) · \{(20, 0), (20, 1), (−20, 7), (−20, 35), (29, 5), (29, 37), (−29, 18), (−29, 24)\};
(1, y) · \{(0, 0), (1, 1), (3, 7), (7, 4), (19, 2), (34, 3), (42, 6), (53, 27)\};
(1, y) · \{(0, 0), (1, 3), (4, 2), (6, 1), (26, 8), (36, 29), (43, 36), (51, 15)\},

where \(x\) runs over \(C_0^{8,41}\) and \(y\) runs over \(C_0^{2,41}\).

Theorem 5. Let \(q\) be a prime. Then there exists a \((\mathbb{Z}_h \times \mathbb{F}_q, \mathbb{Z}_h \times \{0\}, k, \lambda)\)-DF in the following cases:

\[
\begin{array}{|c|c|}
\hline
(hq, h, k, \lambda) & \text{possible exceptions} \\
\hline
(45q, 45, 1)-DF: q \equiv 1 \pmod{4} & \ \\
(63q, 63, 8, 1)-DF: q \equiv 1 \pmod{8} & (63 \times 17, 63, 8, 1) \\
(81q, 81, 9, 1)-DF: q \equiv 1 \pmod{8} & (81 \times 17, 81, 9, 1), (81 \times 41, 81, 9, 1) \\
\hline
\end{array}
\]

4 Concluding remarks

Group divisible designs are closely related to difference families. Let \(K\) be a set of positive integers. A group divisible design (GDD) \((X, G, A)\) satisfying the following properties:

(1) \(G\) is a partition of a finite set \(X\) into subsets (called groups);
(2) \(A\) is a set of subsets of \(X\) (called blocks), whose cardinalities are from \(K\), such that every 2-subset of \(X\) is either contained in exactly one block or in exactly one group, but not in both. If \(G\) contains \(u_i\) groups of size \(g_i\), for \(1 \leq i \leq r\), then \(g_1^{u_1}g_2^{u_2} \cdots g_r^{u_r}\) is called the type of the GDD. The notation \(k\)-GDD is used when \(K = \{k\}\). If each group of a \(k\)-GDD consists of one element and \(|X| = v\), then the \(k\)-GDD is referred to as a balanced incomplete block design, denoted by a \((v, k, 1)\)-BIBD.

By Theorem 3 there exists a \((\mathbb{Z}_m \times \mathbb{F}_q, \mathbb{Z}_m \times \{0\}, 6, 1)\)-DF for any prime \(q \equiv 1 \pmod{6}\). Developing its base blocks under \(\mathbb{Z}_m \times \mathbb{F}_q\), we obtain a 6-GDD of type \(30^6\). In Table 3.18 in [2], it is reported that when \(u < 100\), a 6-GDD of type \(30^u\) exists for \(u \in \{6, 16, 21, 26, 31, 36, 41, 51, 61, 66, 71, 76, 78, 81, 86, 90, 91, 96\}\).

Lemma 4. There exists a 6-GDD of type \(30^u\) for \(u \in \{42, 48, 84, 85\}\).

Proof. It is well known that there exists a 7-GDD of type \(g_7^u\) for \(g \in \{7, 13\}\), which is equivalent to 5 mutually orthogonal Latin squares of order \(g\) (see Table 3.87 in [1]). Therefore there exist \{6, 7\}-GDDs of type \(6^7\), of type \(7^66^1\), of type \(13^66^1\) and of type \(13^67^1\). Apply Wilson’s Fundamental Construction (see Theorem 2.5 in [12]) with 6-GDDs of type \(30^6\) and of type \(30^7\), where a \(k\)-GDD of type \(30^6\) is equivalent to 4 mutually orthogonal Latin squares of order 30, and a 6-GDD of type \(30^7\) exists by Theorem 3. Then we obtain 6-GDDs of type \(180^7\), of type \(210^6180^1\), of type \(390^6180^3\) and of type \(390^6210^7\). Filling in the groups with 6-GDDs of type \(30^6\), of type \(30^7\) and of type \(30^{13}\), we get a 6-GDD of type \(30^u\) for \(u \in \{42, 48, 84, 85\}\), where the needed 6-GDD of type \(30^{13}\) is from Theorem 3.

For \(u \in \{25, 49\}\), since \(u\) is a prime power, we constructed a \((\mathbb{Z}_{30} \times \mathbb{F}_u, \mathbb{Z}_{30} \times \{0\}, k, \lambda)\)-DF such that it satisfies the required cyclotomic conditions of the proof of Theorem 2. The interested reader may get a copy of these data from the authors. To summarize, we have the following theorem.

Theorem 6. There exists a 6-GDD of type \(30^u\) for \(u \in \{6, 16, 21, 25, 26, 36, 41, 42, 48, 49, 51, 66, 71, 76, 78, 81, 84, 85, 86, 90, 91, 96\}\) \(\cup \{q : q \equiv 1 \pmod{6}\}\) is a prime).

Remark 6. There is only one \((31, 6, 1)\)-BIBD up to isomorphism (see Table 6.5 in [14]), which is a projective plane of order 5. Check its full automorphism group and one can see that it admits an automorphism consisting of one fixed point and \(k\) cycles of length \(30/k\) for each \(k \in \{6, 10\}\). Such a BIBD is called \(k\)-rotational (see Section 9.2.4 in [13]). Up to rename the elements, we can obtain a \(k\)-rotational \((31, 6, 1)\)-BIBD on \(\mathbb{Z}_{30} \cup \{\infty\}\) for \(k \in \{6, 10\}\) such that the map \(x \mapsto x + k\) is an automorphism. For any prime \(q \equiv 1 \pmod{6}\), since our 6-GDDs of type \(30^u\) admits \(\mathbb{Z}_{30} \times \mathbb{F}_q\) as its automorphism group whose action is the translation, filling each group with the above \(k\)-rotational \((31, 6, 1)\)-BIBD for \(k \in \{6, 10\}\), we obtain a \(k\)-rotational \((30q + 1, 6, 1)\)-BIBD.
Finally we apply Theorems 5 and 6 to obtain optimal optical orthogonal codes. A \((v, k, 1)\)-optical orthogonal code (OOC) is defined as a set of \(k\)-subsets (called codewords) of \(\mathbb{Z}_v\) whose list of differences does not contain repeated elements. It is optimal if the size of the set of missing differences is less than or equal to \(k(k - 1)\). Clearly a cyclic \((gv, g, k, 1)\)-DF can be seen as a \((gv, k, 1)\)-OOC whose set of missing differences is \(\{0, v, 2v, \ldots, (g - 1)v\}\). Furthermore, one can construct a \((g, k, 1)\)-OOC on the set of missing differences to produce a new \((gv, k, 1)\)-OOC (cf. Construction 4.1 in [15]).

Therefore via cyclic DFs from Theorems 5 and 6 we have the following theorem, where the needed \((35, 6, 1)\)-OOC and \((45, 6, 1)\)-OOC contain only one codeword, taken as \(\{0, 1, 3, 7, 12, 20\}\), the needed \((49, 7, 1)\)-OOC is \(\{0, 1, 3, 7, 27, 35, 40\}\), the needed \((45, 5, 1)\)-OOC consists of two codewords \(\{0, 1, 3, 7, 19\}\) and \(\{0, 5, 14, 22, 35\}\) and the needed \((63, 8, 1)\)-OOC is \(\{0, 1, 3, 7, 15, 20, 31, 41\}\). Note that there is no \((81, 9, 1)\)-OOC with one codeword by exhaustive search.

**Theorem 7.**

1. There exist an optimal \((2q, 5, 1)\)-OOC and an optimal \((12q, 5, 1)\)-OOC for any prime \(q \equiv 1 \pmod{12}\).
2. There exists an optimal \((gq, k, 1)\)-OOC where \((g, k) \in \{(10, 5), (5, 6), (15, 6), (21, 7)\}\) for any prime \(q \equiv 1 \pmod{12}\) except for \((g, q, k) = (5, 13, 6)\).
3. There exists an optimal \((gq, k, 1)\)-OOC where \((g, k) \in \{(25, 6), (30, 6), (35, 6), (45, 6), (35, 7), (49, 7)\}\) for any prime \(q \equiv 1 \pmod{6}\) except for \((g, q, k) \in \{(25, 7, 6), (35, 7, 7), (49, 7, 7)\}\).
4. There exists an optimal \((45q, 5, 1)\)-OOC for any prime \(q \equiv 1 \pmod{4}\) and \(q > 5\).
5. There exists an optimal \((63q, 8, 1)\)-OOC for any prime \(q \equiv 1 \pmod{8}\) and \(q > 17\).

**Acknowledgments**

The authors thank Professor Marco Buratti of Università di Perugia for his many valuable comments. Research of this paper was partially carried out while the second author was visiting Beijing Jiaotong University. He expresses his sincere thanks to the 111 Project of China (grant number B16002) for financial support and to the Department of Mathematics of Beijing Jiaotong University for their kind hospitality.

**References**

[1] R.J.R. Abel, C.J. Colbourn, and J.H. Dinitz, Mutually orthogonal Latin squares, in: CRC Handbook of Combinatorial Designs (C.J. Colbourn and J.H. Dinitz, 2nd ed.), CRC Press 2007, 160–193.

[2] R.J.R. Abel and M. Greig, BIBDs with small block size, in: CRC Handbook of Combinatorial Designs (C.J. Colbourn and J.H. Dinitz, eds), CRC Press, Boca Raton, (2007), 72–79.

[3] J.A. Bondy and U.S.R. Murty, Graph Theory, Springer, New York, 2008.

[4] M. Buratti, Recursive constructions for difference matrices and relative difference families, J. Combin. Des., 6 (1998), 165–182.

[5] M. Buratti, Old and new designs via difference multisets and strong difference families, J. Combin. Des., 7 (1999), 406–425.

[6] M. Buratti, N. Finizio, Existence results for 1-rotational resolvable Steiner 2-designs with block size 6 or 8, Bull. Institute Combin., 50 (2007), 29–44.

[7] M. Buratti and A. Pasotti, Combinatorial designs and the theorem of Weil on multiplicative character sums, Finite Fields Appl., 15 (2009), 332–344.

[8] M. Buratti and F. Zuanni, G-invariantly resolvable Steiner 2-designs arising from 1-rotational difference families, Bull. Belg. Math. Soc., 5 (1998), 221–235.
Appendix

SDFs with a pattern of length two:

| SDF              | $\Sigma_2$                                                                 |
|------------------|----------------------------------------------------------------------------|
| $(\mathbb{Z}_2, 5, 20)$-SDF | $\begin{bmatrix} 0, 0, 0, 1, 1 \end{bmatrix}, \begin{bmatrix} 0, 0, 0, 1 \end{bmatrix}$ |
| $(\mathbb{Z}_{12}, 5, 20)$-SDF | $\begin{bmatrix} 0, 0, 0, 6, 6 \end{bmatrix}, \begin{bmatrix} 0, 0, 0, 6 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 2, 3, 4 \end{bmatrix}, \begin{bmatrix} 0, 1, 2, 4, 5 \end{bmatrix}, \begin{bmatrix} 0, 1, 3, 5, 8 \end{bmatrix}, \begin{bmatrix} 0, 1, 4, 5, 8 \end{bmatrix}, \begin{bmatrix} 0, 2, 4, 7, 9 \end{bmatrix}$ |
| $(\mathbb{Z}_{25}, 6, 6)$-SDF | $\begin{bmatrix} 0, 0, 5, 5, 14, 14 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 2, 3, 6, 18 \end{bmatrix}, \begin{bmatrix} 0, 2, 8, 12, 15, 19 \end{bmatrix}$ |
| $(\mathbb{Z}_{30}, 6, 6)$-SDF | $\begin{bmatrix} 0, 0, 6, 6, 16, 16 \end{bmatrix}, \begin{bmatrix} 0, 15, 3, 18, 7, 22 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 2, 3, 8, 21 \end{bmatrix}, \begin{bmatrix} 0, 2, 5, 9, 13, 18 \end{bmatrix}$ |
| $(\mathbb{Z}_{45}, 6, 6)$-SDF | $\begin{bmatrix} 0, 0, 8, 8, 18, 18 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 2, 3, 5, 15 \end{bmatrix}, \begin{bmatrix} 0, 2, 8, 12, 15, 19 \end{bmatrix}$ |
| $(\mathbb{Z}_{45}, 6, 6)$-SDF | $\begin{bmatrix} 0, 0, 10, 10, 26, 26 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 3, 11, 17, 31 \end{bmatrix}, \begin{bmatrix} 0, 4, 9, 22, 30, 37 \end{bmatrix}, \begin{bmatrix} 0, 1, 3, 7, 12, 25 \end{bmatrix}, \begin{bmatrix} 0, 1, 3, 7, 12, 25 \end{bmatrix}$ |
| $(\mathbb{Z}_{5}, 6, 12)$-SDF | $\begin{bmatrix} 0, 0, 1, 1, 2, 2 \end{bmatrix}, \begin{bmatrix} 0, 0, 2, 2, 4, 4 \end{bmatrix}$ |
| $(\mathbb{Z}_{15}, 6, 12)$-SDF | $\begin{bmatrix} 0, 0, 3, 3, 8, 8 \end{bmatrix}, \begin{bmatrix} 0, 0, 4, 4, 9, 9 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 2, 3, 4, 7 \end{bmatrix}, \begin{bmatrix} 0, 1, 2, 4, 8, 10 \end{bmatrix}$ |
| $(\mathbb{Z}_{35}, 7, 6)$-SDF | $\begin{bmatrix} 0, 7, 7, 17, 17, 30, 30 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 3, 3, 5, 5, 21, 29 \end{bmatrix}, \begin{bmatrix} 0, 3, 9, 13, 17, 24, 29 \end{bmatrix}$ |
| $(\mathbb{Z}_{49}, 7, 6)$-SDF | $\begin{bmatrix} 0, 4, 4, 16, 16, 36, 36 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 3, 20, 28, 38, 43 \end{bmatrix}, \begin{bmatrix} 0, 1, 3, 27, 31, 36, 42 \end{bmatrix}, \begin{bmatrix} 0, 1, 3, 27, 31, 36, 42 \end{bmatrix}$ |
| $(\mathbb{Z}_{21}, 7, 12)$-SDF | $\begin{bmatrix} 0, 5, 5, 10, 10, 17, 17 \end{bmatrix}$, $\Sigma_3 = 2 \begin{bmatrix} 0, 1, 3, 7, 11, 13, 16 \end{bmatrix}$ |

SDFs with a pattern of length four:

| SDF              | $\Sigma_1$                                                                 |
|------------------|----------------------------------------------------------------------------|
| $(\mathbb{Z}_{63}, 8, 8)$-SDF | $\begin{bmatrix} 20, 20, 20, 20, 20, 29, 29, 29, 29, 29 \end{bmatrix}$, $\Sigma_2 = 4 \begin{bmatrix} 0, 1, 3, 7, 19, 34, 42, 53 \end{bmatrix}, \begin{bmatrix} 0, 1, 4, 6, 26, 36, 43, 51 \end{bmatrix}$ |
| $(\mathbb{Z}_{81}, 9, 8)$-SDF | $\begin{bmatrix} 0, 4, 4, 4, 2, 4, 37, 37, 37, 37 \end{bmatrix}$, $\Sigma_2 = 4 \begin{bmatrix} 0, 1, 4, 6, 17, 18, 38, 63, 72 \end{bmatrix}, \begin{bmatrix} 0, 2, 7, 27, 30, 38, 53, 59, 69 \end{bmatrix}$ |