Bounds and Constructions on \((v, 4, 3, 2)\)
Optical Orthogonal Codes

Lidong Wang\(^1,2\) and Yanxun Chang\(^1\)

\(^1\)Institute of Mathematics, Beijing Jiaotong University, Beijing 100044, P. R. China, E-mail: yxchang@bjtu.edu.cn
\(^2\)Department of Basic Courses, Chinese People’s Armed Police Force Academy, Langfang 065000, P. R. China

Received March 23, 2013; revised June 8, 2013

Published online in Wiley Online Library (wileyonlinelibrary.com).
DOI 10.1002/jcd.21362

Abstract: In this paper, we are concerned about optimal \((v, 4, 3, 2)\)-OOCs. A tight upper bound on the exact number of codewords of optimal \((v, 4, 3, 2)\)-OOCs and some direct and recursive constructions of optimal \((v, 4, 3, 2)\)-OOCs are given. As a result, the exact number of codewords of an optimal \((v, 4, 3, 2)\)-OOC is determined for some infinite series.

Keywords: optical orthogonal code; optimal; H design; semi-cyclic

1. INTRODUCTION

Let \(v\), \(k\), \(\lambda_a\), and \(\lambda_c\) be positive integers. A \((v, k, \lambda_a, \lambda_c)\) optical orthogonal code (briefly \((v, k, \lambda_a, \lambda_c)\)-OOC) is a family \(C\) of \((0, 1)\)-sequences (called codewords) of length \(v\) and Hamming weight \(k\) satisfying the following two properties:

1. (The auto-correlation property): \(\sum_{i=0}^{v-1} x_i x_{i+t} \leq \lambda_a\) for any \(X = (x_i) \in C\) and every integer \(t \not\equiv 0\) (mod \(v\));
2. (The cross-correlation property): \(\sum_{i=0}^{v-1} x_i y_{i+t} \leq \lambda_c\) for any \(X = (x_i), Y = (y_i) \in C\) with \(X \neq Y\) and every integer \(t\).

All subscripts here are reduced modulo \(v\) so that only periodic correlations are considered. The study of OOCs is motivated by their various applications in communications. Previous work has been done on using OOCs for multimedia transmission in fiber-optic...
local-area networks (LANs) and in multirate fiber-optic code-division multiple-access (CDMA) systems. For related details, the interested reader can refer to [27, 28, 32, 33].

Example 1.1. Here are \((v, 4, 3, 2)\)-OOCs for \(v = 5, 12\).

\[
\begin{align*}
v = 5 : & \quad 11110. \\
v = 12 : & \quad 111100000000, 101010100000, 100101000010, \\
& \quad 110010000100, 110001100000. \quad \Box
\end{align*}
\]

The number of codewords of a \((v, k, \lambda_a, \lambda_c)\)-OOC is called its size. For fixed \(v, k, \lambda_a, \lambda_c\), the largest size among all \((v, k, \lambda_a, \lambda_c)\)-OOCs is denoted by \(\Phi(v, k, \lambda_a, \lambda_c)\). A \((v, k, \lambda_a, \lambda_c)\)-OOC is said to be optimal if its size is equal to \(\Phi(v, k, \lambda_a, \lambda_c)\).

A \((v, k, \lambda_a, \lambda_c)\)-OOC in which \(\lambda_a = \lambda_c = \lambda\) is further briefly denoted by \((v, k, \lambda)\)-OOC. The first systematic investigation of OOCs appeared in 1989 [15]. For many years the research on OOCs concentrated mainly on optimal \((v, k, 1)\)-OOCs ([1, 5, 6, 8, 10–13, 19–21, 25, 26, 30, 34, 37]). Recently, many important results have also been obtained regarding optimal \((v, k, \lambda)\)-OOCs with \(\lambda = 2\) ([2, 14, 17]) and with \(\lambda > 2\) [3].

However, it does not mean that a \((v, k, \lambda_a, \lambda_c)\)-OOC with \(\lambda_a \neq \lambda_c\) is not of interest. Using arcs and Baer subspaces of finite projective spaces, Alderson and Mellinger [4] construct some infinite classes of OOCs with \(\lambda_a < \lambda_c\). When \(\lambda_a > \lambda_c\), an earlier investigation about them was made by Yang and Fuja [36]. Compared a \((v, w + m, \lambda + m, \lambda)\)-OOC with either a \((v, w + m, \lambda + m)\)-OOC or a \((v, w, \lambda)\)-OOC, they pointed out, from a practical point of view, the performance of a \((v, w + m, \lambda + m, \lambda)\)-OOC is at least as good as the other two codes. They also demonstrated that the size of the \((v, w + m, \lambda + m, \lambda)\)-OOC can actually exceed that of the other two codes. Thus more users can be provided even better performance. This motivates the study of such OOCs.

When \(v\) is even, optimal \((v, 3, 3, 1)\)-OOCs (also called conflict-avoiding codes) have been discussed thoroughly in [18, 23, 24, 29]. When \(\lambda_a = 2\) and \(\lambda_c = 1\), several direct and recursive constructions are given for optimal \((v, 4, 2, 1)\)-OOCs in [7, 31, 35]. Some preliminary results of optimal \((v, 5, 2, 1)\)-OOCs are also obtained in [9].

In this paper, we concentrate on optimal \((v, 4, 3, 2)\)-OOCs. In Section 2, some preliminaries and an equivalent description of \((v, 4, 3, 2)\)-OOCs using set notation are given. In Section 3, we get a tight upper bound on \(\Phi(v, 4, 3, 2)\). In Section 4, some auxiliary designs are introduced to establish recursive constructions for \((v, 4, 3, 2)\)-OOCs. As a consequence, the exact number of \(\Phi(v, 4, 3, 2)\) is determined for some infinite series. Finally, we give a conclusion in Section 5.

2. PRELIMINARIES

Throughout this paper, let \(Z_v\) be the residue ring of integers modulo \(v\). For integers \(a \leq b\), the set \([a, a + 1, a + 2, \cdots, b]\) is denoted by \([a, b]\). The notion of OOCs can be more conveniently reformulated by using set notation.

Suppose \(C\) is a \((v, k, \lambda_a, \lambda_c)\)-OOC. For each \((0, 1)\)-sequence \(C \in C\), its \(v\) positions are indexed by \(Z_v\). Construct a \(k\)-subset \(B_C\) of \(Z_v\) such that \(i \in B_C\) if and only if the \(i\)th position of \(C\) is not zero. Then, \(\{B_C : C \in C\}\) is a set-theoretic representation of a \((v, k, \lambda_a, \lambda_c)\)-OOC. Conversely, let \(\mathcal{F}\) be a family of \(k\)-subsets of \(Z_v\). \(\mathcal{F}\) constitutes a \((v, k, \lambda_a, \lambda_c)\)-OOC if satisfying the following conditions:
(1’) (The auto-correlation property): $|X \cap (X + t)| \leq \lambda_a$ for any $X \in \mathcal{F}$ and every $t \in Z_v \setminus \{0\}$;

(2’) (The cross-correlation property): $|X \cap (Y + t)| \leq \lambda_c$ for any $X, Y \in \mathcal{F}$ with $X \neq Y$ and every $t \in Z_v,$

where $X + t = \{x + t \pmod{v} : x \in X\}.$ For convenience, we still call $X$ a codeword for every $X \in \mathcal{F}$.

OOCs from Example 1.1 can be viewed in set notation.

- $v = 5 : \mathcal{F} = \{\{0, 1, 2, 3\}\}.$
- $v = 12 : \mathcal{F} = \{\{0, 1, 2, 3\}, \{0, 2, 4, 6\}, \{0, 3, 5, 10\}, \{0, 1, 4, 9\}, \{0, 1, 5, 6\}\}.$

Let $G$ be an abelian group. Let $X = \{a_i : 0 \leq i \leq k - 1\}$ be any $k$-subset of $G.$ Let $O(X) = \{\{a_i + g : 0 \leq i \leq k - 1\} : g \in G\},$ which is called the orbit of $X$ under $G.$ If the length of the orbit $|O(X)|$ is equal to the order of $G$, the orbit is full. Otherwise, short. Suppose $X = \{a, b, c\}$ is a 3-subset of $G.$ Obviously, $O(\{0, b - a, c - a\}) = O(\{0, a - b, c - b\}) = O(\{0, a - c, b - c\}).$ Let $G(a, b, c) = \{\{b - a, c - a\}, \{a - b, c - b\}, \{a - c, b - c\}\}.$ The following lemma from [16] is useful.

**Lemma 2.1.** [16] $O(\{a, b, c\}) = O(\{a', b', c'\})$ if and only if $G(a, b, c) = G(a', b', c').$

Lemma 2.1 shows that if $G(a, b, c) \neq G(a', b', c'),$ there is no common 3-subset between $O(\{a, b, c\})$ and $O(\{a', b', c'\}).$ This gives us a method to distinguish different orbits essentially.

It is readily checked that all 3-subsets of $Z_v$ can be partitioned into $M(v)$ distinct 3-subset orbits under $Z_v,$ where $M(v) = \frac{v(v - 3)}{6} + 1$ when $v \equiv 0 \pmod{3}$ and $M(v) = \frac{(v - 1)(v - 2)}{6}$ when $v \equiv 0 \pmod{3}.$ Clearly, $O(\{0, v/3, 2v/3\})$ is the only short 3-subset orbit under $Z_v$ when $v \equiv 0 \pmod{3}.$

For a given subset $X$ of $Z_v,$ we define the list of differences of $X$ by $\Delta X = \{j - i : i, j \in X, i \neq j\}$ as a multiset, and define the support of $\Delta X,$ denoted by $\text{supp}(\Delta X),$ as the set of underlying elements in $\Delta X.$ Let $\lambda(X)$ denote the maximum number among all the multiplicity of every difference in $\Delta X.$ Then we have

$$\lambda(X) = \max \left\{|X \cap (X + t)| : t \in Z_v \setminus \{0\}\right\}.$$ 

Hereinafter, we say that a 3-subset orbit appears in a codeword, if a representative of the 3-subset orbit appears in the codeword. From above correspondence, we give another equivalent description of a $(v, k, \lambda_a, 2)$-OOC, which is more convenient to check its correlation property.

Let $\mathcal{F}$ be a family of $k$-subsets of $Z_v.$ $\mathcal{F}$ constitutes a $(v, k, \lambda_a, 2)$-OOC if satisfying the following conditions:

(1’’) (The auto-correlation property): $\lambda_a = \max\{\lambda(X) : X \in \mathcal{F}\};$

(2’’) (The cross-correlation property): each 3-subset orbit appears at most in one codeword $X \in \mathcal{F}.$

Journal of Combinatorial Designs DOI 10.1002/jcd
3. UPPER BOUNDS OF \((v, 4, 3, 2)\)-OOCs

The determination of the exact value of \(\Phi(v, k, \lambda_a, \lambda_c)\) is of interest. However, since it is difficult to determine the exact value of \(\Phi(v, k, \lambda_a, \lambda_c)\) in general, upper bounds on \(\Phi(v, k, \lambda_a, \lambda_c)\) are also of interest. When \(\lambda_a \geq \lambda_c\), Yang and Fuja [36] pointed out that:

\[
\Phi(v, k, \lambda_a, \lambda_c) \leq \left\lfloor \frac{\lambda_a(v - 1)(v - 2) \cdots (v - \lambda_c)}{k(k - 1)(k - 2) \cdots (k - \lambda_c)} \right\rfloor.
\]

By above upper bound, it is easy to obtain \(\Phi(5, 4, 3, 2) \leq 1\) and \(\Phi(12, 4, 3, 2) \leq 13\). We will see this upper bound is far from being tight. In the remainder of this section, we shall give a tighter upper bound on \(\Phi(v, 4, 3, 2)\). The following result comes from [31].

**Lemma 3.1.** [31] Let \(X\) be any 4-subset of \(Z_v\) containing 0. \(\lambda(X) = 3\) if and only if \(|\text{supp}(\Delta X)| = 4\) (\(X = \{0, v/5, 2v/5, 3v/5\}\), \(5\) (\(X = \{0, v/6, v/3, v/2\}\), or \(X = \{0, v/6, v/3, 2v/3\}\)), \(6\) (\(X = \{0, a, 2a, 3a\}\) or \(8\) (\(X = \{0, a, v/3, 2v/3\}\)).

The following lemma is useful in the determination of the number of 3-subset orbits contained in \(X\).

**Lemma 3.2.** Let \(X\) be any 4-subset of \(Z_v\) with \(\lambda(X) \leq 3\). \(X\) contains three distinct 3-subset orbits if and only if \(X\) is of form \(\{0, a, 2a, 3a\}\) for \(a \in Z_v\) and \(a \neq v/5, 2v/5\); \(X\) contains two distinct 3-subset orbits when \(X = \{0, a, 2a, 3a\}\) and \(a \in \{v/5, 2v/5\}\); \(X\) contains four distinct 3-subset orbits for other cases.

**Proof.** Since \(|X| = 4\), \(X\) contains at most four distinct 3-subset orbits. When \(\lambda(X) \leq 2\), \(X\) must contain four distinct 3-subset orbits. If not, there exists a \(t \in Z_v\) such that \(|X \cap (X + t)| = 3 \leq \lambda(X)\), a contradiction occurs. When \(\lambda(X) = 3\), by Lemmas 2.1 and 3.1, it is readily checked that the conclusion holds.

Let \(\mathcal{F}\) be a \((v, 4, 3, 2)\)-OOC. Then, for any codeword \(X \in \mathcal{F}\), \(\lambda(X) \leq 3\). Thus, by Lemma 3.2 we can partition \(\mathcal{F}\) into two parts \(\mathcal{F}_1\) and \(\mathcal{F}_2\), where \(\mathcal{F}_1\) consists of all codewords of the form \(\{0, a, 2a, 3a\}\). In order to get a tight upper bound on the size of an optimal \((v, 4, 3, 2)\)-OOC, we need to estimate the number of codewords \(X\) of the form \(\{0, a, 2a, 3a\}\).

Since two distinct codewords do not share a common 3-subset orbit when \(i = v/3\), and \(\lambda(X) = 4\) when \(i = v/4\). It is also easy to see that \(X\) and \(\{0, -i, -2i, -3i\}\) are in the same 4-subset orbit. Therefore, we can restrict that \(1 \leq i \leq \lfloor v/2 \rfloor - 1\), \(i \neq v/3\) and \(v/4\). Let \(\Omega_i = \{O(0, i, 2i), O(0, i, 3i), O(0, 2i, 3i)\}\). Suppose \(1 \leq j \leq \lfloor v/2 \rfloor - 1\), \(j \neq v/3\), \(v/4\) and \(j \neq i\). Let \(Y = \{0, j, 2j, 3j\}\) and \(\Omega_j = \{O(0, j, 2j), O(0, j, 3j), O(0, 2j, 3j)\}\).

By means of tedious calculations we have checked that:

**Lemma 3.3.** For \(i, j \in [1, \lfloor v/2 \rfloor - 1] \setminus \{v/3, v/4\}\) and \(i \neq j\), \(\Omega_i \cap \Omega_j \neq \emptyset\) if and only if \(i, j \in A_l\) for \(l \in \{1, 2, 3\}\), where \(A_1 = \{v/5, 2v/5\}\), \(A_2 = \{v/7, 2v/7, 3v/7\}\) and \(A_3 = \{v/8, 3v/8\}\).
Proof. The sufficiency is readily checked. We prove the necessity. If $\Omega_i \cap \Omega_j \neq \emptyset$, the following six situations may occur:

Case 1. $O(\{0, i, 2i\}) = O(\{0, j, 2j\})$;
Case 2. $O(\{0, i, 2i\}) = O(\{0, j, 3j\})$;
Case 3. $O(\{0, i, 2i\}) = O(\{0, 2j, 3j\})$;
Case 4. $O(\{0, i, 3i\}) = O(\{0, j, 3j\})$;
Case 5. $O(\{0, 2i, 3i\}) = O(\{0, 2j, 3j\})$.

Here, we only give a proof for Case 2. Since $G(0, i, 2i) = \{\{i, 2i\}, \{-i, i\}, \{-i, -2i\}\}$ and $G(0, j, 3j) = \{\{j, 3j\}, \{-j, 2j\}, \{-2j, -3j\}\}$, the discussion can be divided into three subcases by Lemma 2.1. The arithmetic is reduced modulo $v$. The proof can be divided into two situations. Here, we only discuss the case of $v \equiv 0(\text{mod } 5)$. Similar discussion can prove another situation.

We give some notations for later use. Define

$$\delta_0(v) = \begin{cases} 1 & \text{if } v \equiv 0(\text{mod } 3), \\ 0 & \text{otherwise,} \end{cases}$$
$$\delta_1(v) = \begin{cases} 2 & \text{if } v \equiv 0(\text{mod } 7), \\ 0 & \text{otherwise,} \end{cases}$$
$$\delta_2(v) = \begin{cases} 2 & \text{if } v \equiv 0(\text{mod } 8), \\ 1 & \text{if } v \equiv 4(\text{mod } 8), \\ 0 & \text{otherwise,} \end{cases}$$
$$\delta_3(v) = \begin{cases} 1 & \text{if } v \equiv 0(\text{mod } 5), \\ 0 & \text{otherwise.} \end{cases}$$

Let

$$U(v) = \left\lfloor \frac{M(v) + \lfloor v/2 \rfloor - 1 - \sum_{i=0}^{3} \delta_i(v)}{4} \right\rfloor.$$ 

Now, we are ready to give an upper bound on the size of an optimal $(v, 4, 3, 2)$-OOC.

**Theorem 3.4.** It holds that $\Phi(v, 4, 3, 2) \leq U(v)$.

Proof. According to whether $5$ is the factor of $v$, the proof can be divided into two situations. Here, we only discuss the case of $v \equiv 0(\text{mod } 5)$. Similar discussion can prove another situation.

Suppose $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$ is a $(v, 4, 3, 2)$-OOC, where $\mathcal{F}_1$ consists of all codewords of the form $\{0, i, 2i, 3i\}$. Let $|\mathcal{F}_1| = b_1$, $|\mathcal{F}_2| = b_2$. By Lemma 3.3, $i$ takes at most one element in each $A_l$ for $l = 1, 2, 3$. Thus, $b_1 \leq \Delta(v) = \lfloor v/2 \rfloor - 1 - \sum_{i=0}^{3} \delta_i(v)$.

As mentioned above, all $3$-subsets of $Z_v$ can be partitioned into $M(v)$ distinct $3$-subset orbits under $Z_v$. We divide the problem into two cases.
Case 1. \( \mathcal{F}_1 \) contains a codeword \( \{0, i, 2i, 3i\} \) for \( i = v/5 \) or \( 2v/5 \). In this case, \( \mathcal{F}_1 \) contains \( 3(b_1 - 1) + 2 \) distinct 3-subset orbits, and \( \mathcal{F}_2 \) contains \( 4b_2 \) distinct 3-subset orbits by Lemma 3.2. We have

\[
b_1 \leq \Delta(v),
\]

\[
3(b_1 - 1) + 2 + 4b_2 \leq M(v).
\]

So (1) + (2) shows

\[
4(b_1 + b_2) \leq M(v) + 1 + \Delta(v).
\]

Note that \( \delta_3(v) = 1 \). Since \( b_1 + b_2 \) is an integer, \( b_1 + b_2 \leq U(v) \).

Case 2. \( \mathcal{F}_1 \) does not contain any codewords \( \{0, i, 2i, 3i\} \) for \( i = v/5 \) and \( 2v/5 \). In this case, \( \mathcal{F}_1 \) contains \( 3b_1 \) distinct 3-subset orbits, and \( \mathcal{F}_2 \) contains \( 4b_2 \) distinct 3-subset orbits by Lemma 3.2. We have

\[
b_1 \leq \Delta(v) - 1,
\]

\[
3b_1 + 4b_2 \leq M(v).
\]

Similarly, (3)+(4) shows

\[
b_1 + b_2 \leq \lfloor (M(v) + \Delta(v) - 1)/4 \rfloor \leq U(v).
\]

Remark: Let \( Q(v) = A(v) \cap \mathbb{Z}^+ \), where \( A(v) = \{v/3, v/4, 2v/5, 2v/7, 3v/7, 3v/8\} \) and \( \mathbb{Z}^+ \) is the set of positive integers. Suppose \( \mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \) is an optimal \((v, 4, 3, 2)\)-OOC with \( U(v) \) codewords. If \( |\mathcal{F}_1| = \Delta(v) \), then \( \mathcal{F}_1 = \{0, i, 2i, 3i\} : i \in [1, [v/2] - 1] \setminus Q(v) \).

It is easy to see that \( U(5) = 1 \) and \( U(12) = 5 \). So, the \((v, 4, 3, 2)\)-OOCs given in Example 1.1 for \( v = 5, 12 \), are optimal. Hence, \( \Phi(5, 4, 3, 2) = 1 \) and \( \Phi(12, 4, 3, 2) = 5 \).

4. RECURSIVE CONSTRUCTIONS

Filling in holes is an effective method in the constructions of OOCs. To describe our recursive constructions, we introduce the so called \( g \)-regular \((v, 4, 3, 2)\)-OOC.

Let \( H \) be a subgroup of order \( g \) of \( \mathbb{Z}_v \). \( \mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \) is a collection of 4-subsets of \( \mathbb{Z}_v \). \( \mathcal{F} \) is called a \( g \)-regular \((v, 4, 3, 2)\)-OOC if each of the following are satisfied:

1. \( \lambda(X) \leq 3 \) for any codeword \( X \in \mathcal{F} \);
2. \( \mathcal{F}_1 = \{0, i, 2i, 3i\} : i \in [1, [v/2] - 1] \setminus Q(v), i \neq 0 \) (mod \( v/g \));
3. each 3-subset orbit appears in either \( H \) or exactly one codeword in \( \mathcal{F} \), but not both.

We should remark here that a \( 1 \)-regular \((v, 4, 3, 2)\)-OOC is the optimal \((v, 4, 3, 2)\)-OOCs with \( U(v) \) codewords in which \( |\mathcal{F}_1| = \Delta(v) \).
We give some notations for later use. Define

\[
\begin{align*}
\gamma_0(g, n) &= \begin{cases} 
1 & \text{if } n \equiv 0 \pmod{3} \text{ and } g \not\equiv 0 \pmod{3}, \\
0 & \text{otherwise},
\end{cases} \\
\gamma_1(g, n) &= \begin{cases} 
2 & \text{if } n \equiv 0 \pmod{7} \text{ and } g \not\equiv 0 \pmod{7}, \\
0 & \text{otherwise},
\end{cases} \\
\gamma_2(g, n) &= \begin{cases} 
1 & \text{if } n \equiv 0 \pmod{5} \text{ and } g \not\equiv 0 \pmod{5}, \\
0 & \text{otherwise},
\end{cases} \\
\gamma_3(g, n) &= \begin{cases} 
2 & \text{if } n \equiv 0 \pmod{8} \text{ and } g \not\equiv 0 \pmod{4}, \\
1 & \text{if } n \equiv 0 \pmod{8} \text{ and } g \equiv 2 \pmod{4}, \\
1 & \text{if } n \equiv 4 \pmod{8} \text{ and } g \equiv 2 \pmod{4}, \\
0 & \text{otherwise},
\end{cases}
\end{align*}
\]

A necessary condition for the existence of a g-regular \((g, n, 4, 3, 2)\)-OOC is given as follows.

**Lemma 4.1.** A necessary condition for the existence of a g-regular \((g, n, 4, 3, 2)\)-OOC is

\[
M(gn) - M(g) - 3([gn/2] - [g/2] - \sum_{i=0}^{2} \gamma_i(g, n)) \equiv 0 \pmod{4}
\]

**Proof.** According to the value of \(\gamma_3(g, n)\), the proof can be divided into two situations.

We give a proof for the case of \(\gamma_3(g, n) = 1\). Note that \(n \equiv 0 \pmod{5}\) and \(g \not\equiv 0 \pmod{5}\) in this case. The proof for the remaining case is similar.

Let \(\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2\) be a g-regular \((g, n, 4, 3, 2)\)-OOC. In this case, \(Z_{gn}\) and the subgroup of order \(g\) contain \(M(gn)\) and \(M(g)\) distinct 3-subset orbits respectively. Thus, the number of distinct 3-subset orbits not contained in the subgroup of order \(g\) is \(M(gn) - M(g)\).

By the definition, \(\mathcal{F}_1\) contains a codeword \(\{0, i, 2i, 3i\}\) for \(i = gn/5\) or \(2gn/5\), and \(|\mathcal{F}_1| = \Gamma(g, n) = [gn/2] - [g/2] - \sum_{i=0}^{3} \gamma_i(g, n)\).

By Lemma 3.2, \(\mathcal{F}_1\) contains \(3(\Gamma(g, n) - 1) + 2\) distinct 3-subset orbits, and \(\mathcal{F}_2\) contains \(4|\mathcal{F}_2|\) distinct 3-subset orbits. We have

\[
3(\Gamma(g, n) - 1) + 2 + 4|\mathcal{F}_2| = M(gn) - M(g).
\]

So

\[
4|\mathcal{F}_2| = M(gn) - M(g) + 1 - 3\Gamma(g, n).
\]

That is

\[
M(gn) - M(g) - 3([gn/2] - [g/2] - \sum_{i=0}^{2} \gamma_i(g, n)) \equiv 0 \pmod{4}.
\]

We give some examples of g-regular \((v, 4, 3, 2)\)-OOCs.

**Lemma 4.2.** There exists a g-regular \((g, n, 4, 3, 2)\)-OOC for each \((g, n) \in \{(7, 2), (11, 2), (5, 5), (15, 2), (17, 2), (21, 2), (23, 2), (7, 7), (25, 2)\}\).
\textbf{Proof.} The required codes are constructed on $Z_{g,n}$. We only list the codewords of $F_2$ below.

\[(g, n) = (7, 2):\]
\[
\{0, 1, 4, 11\}, \{0, 1, 6, 7\}, \{0, 2, 5, 7\}.
\]

\[(g, n) = (11, 2):\]
\[
\{0, 1, 4, 5\}, \{0, 1, 6, 17\}, \{0, 1, 7, 16\}, \{0, 1, 9, 14\}, \{0, 1, 10, 11\}, \{0, 2, 5, 7\}, \{0, 2, 9, 11\}, \{0, 3, 7, 18\}, \{0, 3, 8, 11\}, \{0, 3, 10, 13\}.
\]

\[(g, n) = (5, 5):\]
\[
\{0, 2, 12, 15\}, \{0, 2, 14, 19\}, \{0, 1, 8, 18\}, \{0, 2, 5, 22\}, \{0, 2, 7, 20\}, \{0, 1, 4, 5\}, \{0, 2, 10, 16\}, \{0, 2, 11, 17\}, \{0, 3, 7, 10\}, \{0, 2, 8, 13\}, \{0, 4, 9, 20\}, \{0, 1, 6, 7\}, \{0, 3, 12, 16\}, \{0, 4, 10, 14\}, \{0, 1, 10, 11\}.
\]

\[(g, n) = (15, 2):\]
\[
\{0, 1, 10, 11\}, \{0, 1, 12, 13\}, \{0, 1, 14, 15\}, \{0, 3, 8, 15\}, \{0, 1, 4, 5\}, \{0, 1, 8, 9\}, \{0, 2, 11, 17\}, \{0, 2, 13, 23\}, \{0, 2, 15, 21\}, \{0, 3, 7, 10\}, \{0, 2, 5, 7\}, \{0, 2, 9, 19\}, \{0, 3, 13, 16\}, \{0, 3, 14, 19\}, \{0, 3, 18, 25\}, \{0, 4, 9, 25\}, \{0, 1, 6, 7\}, \{0, 4, 11, 15\}, \{0, 5, 11, 18\}, \{0, 5, 13, 22\}, \{0, 5, 17, 24\}.
\]

\[(g, n) = (17, 2):\]
\[
\{0, 1, 10, 11\}, \{0, 1, 13, 14\}, \{0, 1, 15, 20\}, \{0, 5, 12, 17\}, \{0, 2, 9, 19\}, \{0, 1, 8, 9\}, \{0, 1, 16, 17\}, \{0, 2, 11, 25\}, \{0, 2, 13, 15\}, \{0, 2, 17, 27\}, \{0, 3, 8, 11\}, \{0, 1, 6, 7\}, \{0, 3, 12, 25\}, \{0, 3, 13, 24\}, \{0, 3, 14, 17\}, \{0, 3, 15, 18\}, \{0, 3, 7, 10\}, \{0, 2, 5, 7\}, \{0, 3, 16, 21\}, \{0, 4, 11, 27\}, \{0, 4, 13, 17\}, \{0, 5, 11, 16\}, \{0, 4, 9, 29\}, \{0, 1, 4, 5\}, \{0, 6, 13, 19\}, \{0, 6, 15, 23\}, \{0, 6, 17, 25\}, \{0, 7, 15, 22\}.
\]

\[(g, n) = (21, 2):\]
\[
\{0, 1, 10, 11\}, \{0, 1, 12, 13\}, \{0, 1, 14, 15\}, \{0, 3, 28, 33\}, \{0, 6, 13, 21\}, \{0, 1, 8, 9\}, \{0, 1, 16, 17\}, \{0, 1, 18, 19\}, \{0, 1, 20, 21\}, \{0, 2, 13, 15\}, \{0, 7, 19, 26\}, \{0, 2, 5, 7\}, \{0, 2, 17, 27\}, \{0, 2, 19, 21\}, \{0, 3, 12, 17\}, \{0, 3, 13, 32\}, \{0, 9, 19, 30\}, \{0, 1, 6, 7\}, \{0, 3, 14, 27\}, \{0, 3, 18, 31\}, \{0, 3, 19, 24\}, \{0, 3, 20, 23\}, \{0, 3, 21, 26\}, \{0, 1, 4, 5\}, \{0, 4, 11, 35\}, \{0, 4, 13, 33\}, \{0, 4, 17, 21\}, \{0, 4, 31, 37\}, \{0, 5, 12, 25\}, \{0, 4, 9, 15\}, \{0, 5, 13, 18\}, \{0, 5, 16, 31\}, \{0, 5, 19, 28\}, \{0, 5, 20, 27\}, \{0, 5, 22, 35\}, \{0, 3, 8, 11\}, \{0, 6, 17, 31\}, \{0, 6, 19, 25\}, \{0, 6, 27, 35\}, \{0, 7, 16, 33\}, \{0, 7, 17, 24\}, \{0, 2, 9, 11\}, \{0, 8, 19, 27\}, \{0, 9, 21, 32\}, \{0, 3, 7, 10\}.
\]

\[(g, n) = (23, 2):\]
\[
\{0, 1, 10, 11\}, \{0, 1, 12, 13\}, \{0, 1, 14, 15\}, \{0, 3, 22, 25\}, \{0, 5, 20, 31\}, \{0, 1, 8, 9\}, \{0, 1, 17, 18\}, \{0, 1, 19, 20\}, \{0, 1, 21, 26\}, \{0, 1, 22, 23\}, \{0, 6, 17, 35\}, \{0, 1, 4, 5\}, \{0, 2, 13, 15\}, \{0, 2, 17, 19\}, \{0, 2, 21, 23\}, \{0, 3, 12, 15\}, \{0, 7, 23, 36\}, \{0, 1, 6, 7\}, \{0, 3, 13, 16\}, \{0, 3, 14, 17\}, \{0, 3, 18, 21\}, \{0, 3, 19, 30\}, \{0, 3, 20, 23\}, \{0, 2, 5, 7\}, \{0, 4, 11, 15\}, \{0, 4, 17, 23\}, \{0, 4, 19, 31\}, \{0, 4, 27, 33\}, \{0, 5, 11, 32\}, \{0, 4, 9, 13\}, \{0, 5, 12, 23\}, \{0, 5, 13, 18\}, \{0, 5, 14, 27\}, \{0, 5, 16, 21\}, \{0, 5, 19, 40\}, \{0, 3, 8, 11\}.
\]
{0, 5, 22, 29}, {0, 5, 24, 37}, {0, 5, 28, 39}, {0, 6, 13, 31}, {0, 6, 15, 37}, {0, 2, 9, 11}, {0, 6, 21, 39}, {0, 7, 15, 22}, {0, 7, 16, 37}, {0, 7, 17, 30}, {0, 7, 19, 26}, {0, 3, 7, 10}, {0, 8, 17, 31}, {0, 8, 21, 29}, {0, 8, 23, 37}, {0, 9, 19, 36}, {0, 9, 20, 29}, {0, 9, 21, 34}, {0, 10, 21, 31}.

\((g, n) = (7, 7)\):

{0, 1, 10, 11}, {0, 1, 12, 13}, {0, 1, 14, 15}, {0, 1, 30, 32}, {0, 1, 31, 34}, {0, 1, 4, 5}, {0, 1, 16, 19}, {0, 1, 18, 20}, {0, 1, 21, 22}, {0, 1, 23, 27}, {0, 1, 14, 19}, {0, 1, 8, 9}, {0, 2, 12, 14}, {0, 2, 13, 15}, {0, 2, 16, 18}, {0, 3, 12, 15}, {0, 6, 14, 41}, {0, 1, 6, 7}, {0, 2, 21, 23}, {0, 2, 22, 29}, {0, 2, 24, 26}, {0, 3, 27, 31}, {0, 6, 22, 28}, {0, 2, 5, 7}, {0, 3, 13, 16}, {0, 3, 14, 17}, {0, 3, 20, 24}, {0, 3, 21, 25}, {0, 3, 22, 30}, {0, 3, 7, 10}, {0, 3, 28, 32}, {0, 4, 10, 14}, {0, 4, 11, 15}, {0, 4, 16, 20}, {0, 4, 17, 23}, {0, 4, 9, 13}, {0, 4, 18, 35}, {0, 4, 30, 36}, {0, 5, 11, 16}, {0, 5, 12, 17}, {0, 5, 13, 20}, {0, 2, 9, 11}, {0, 5, 21, 33}, {0, 5, 23, 28}, {0, 5, 24, 29}, {0, 5, 34, 41}, {0, 6, 13, 29}, {0, 2, 8, 10}, {0, 6, 15, 31}, {0, 6, 16, 30}, {0, 6, 17, 38}, {0, 6, 20, 35}, {0, 6, 21, 34}, {0, 3, 8, 11}, {0, 6, 24, 40}, {0, 6, 25, 39}, {0, 6, 26, 42}, {0, 7, 16, 39}, {0, 7, 17, 40}, {0, 7, 18, 25}, {0, 7, 19, 26}, {0, 7, 22, 34}, {0, 7, 24, 32}, {0, 8, 17, 36}, {0, 8, 18, 29}, {0, 8, 20, 37}, {0, 8, 21, 40}, {0, 8, 23, 31}, {0, 8, 28, 39}, {0, 9, 19, 37}, {0, 9, 21, 39}, {0, 9, 22, 36}, {0, 9, 23, 35}, {0, 9, 24, 34}, {0, 10, 22, 32}, {0, 11, 23, 34}, {0, 11, 24, 35}.

\((g, n) = (25, 2)\):

{0, 1, 10, 11}, {0, 1, 12, 13}, {0, 1, 14, 15}, {0, 1, 26, 29}, {0, 5, 17, 30}, {0, 1, 8, 9}, {0, 1, 16, 19}, {0, 1, 18, 21}, {0, 1, 20, 23}, {0, 1, 22, 25}, {0, 1, 24, 27}, {0, 1, 4, 5}, {0, 1, 28, 31}, {0, 2, 13, 15}, {0, 5, 25, 38}, {0, 1, 6, 7}, {0, 2, 17, 19}, {0, 2, 21, 31}, {0, 2, 23, 25}, {0, 3, 12, 15}, {0, 7, 15, 32}, {0, 2, 5, 7}, {0, 3, 13, 16}, {0, 3, 14, 17}, {0, 4, 11, 15}, {0, 4, 17, 23}, {0, 4, 9, 13}, {0, 4, 29, 35}, {0, 5, 11, 16}, {0, 5, 12, 33}, {0, 5, 13, 18}, {0, 5, 14, 41}, {0, 2, 9, 11}, {0, 5, 19, 36}, {0, 5, 21, 34}, {0, 5, 22, 43}, {0, 5, 23, 28}, {0, 5, 24, 29}, {0, 3, 8, 11}, {0, 6, 13, 43}, {0, 6, 15, 39}, {0, 6, 17, 41}, {0, 6, 19, 37}, {0, 6, 23, 29}, {0, 3, 7, 10}, {0, 7, 16, 41}, {0, 7, 17, 24}, {0, 7, 18, 39}, {0, 7, 22, 31}, {0, 7, 23, 30}, {0, 10, 23, 37}, {0, 7, 26, 35}, {0, 8, 17, 27}, {0, 8, 19, 35}, {0, 8, 23, 39}, {0, 9, 21, 39}, {0, 10, 25, 39}, {0, 9, 21, 30}, {0, 9, 22, 37}, {0, 7, 25, 42}, {0, 9, 20, 39}, {0, 11, 23, 38}, {0, 10, 21, 35}.

\(\square\)

The following construction is simple but very useful.

**Construction 4.3.** Suppose there exists a \(g\)-regular \((gn, 4, 3, 2)\)-OOC. If there exists a \((g, 4, 3, 2)\)-OOC with \(U(g)\) codewords, then there exists a \((gn, 4, 3, 2)\)-OOC with \(U(gn)\) codewords.

**Proof.** Let \(\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2\) be a \(g\)-regular \((gn, 4, 3, 2)\)-OOC, where \(\mathcal{F}_1\) consists of all codewords of the form \(\{0, i, 2i, 3i\} \).

*Journal of Combinatorial Designs* DOI 10.1002/jcd
Let \( E \) be a \((g, 4, 3, 2)\)-OOC with \( U(g) \) codewords. If \( B = \{b_1, b_2, b_3, b_4\} \in \mathcal{E} \), we take

\[
 nB = \{nb_1, nb_2, nb_3, nb_4\} \pmod{gn}.
\]

Since \( \mathcal{F} \) and \( \{nB : B \in \mathcal{E}\} \) contain no common 3-subset orbits, then \( \mathcal{F} \cup \{nB : B \in \mathcal{E}\} \) forms the desired \((gn, 4, 3, 2)\)-OOC. For checking optimality of the required code, it suffices to show that

\[
|\mathcal{F}| + |\mathcal{E}| = U(gn).
\]

According to the value of \( \gamma_3(g, n) \), the proof can be divided into two situations. We give a proof for the case of \( \gamma_3(g, n) = 1 \). Note that \( n \equiv 0 \pmod{5} \) and \( g \not\equiv 0 \pmod{5} \) in this case. The proof for the remaining case is similar.

By Lemma 3.2, \( \mathcal{F}_1 \) contains \( 3(|\mathcal{F}_1| - 1) + 2 \) distinct 3-subset orbits, and \( \mathcal{F}_2 \) contains \( 4|\mathcal{F}_2| \) distinct 3-subset orbits. Thus,

\[
3(|\mathcal{F}_1| - 1) + 2 + 4|\mathcal{F}_2| = M(gn) - M(g).
\]

We have

\[
|\mathcal{F}_1| + |\mathcal{F}_2| = (M(gn) - M(g) + 1 + |\mathcal{F}_1|)/4.
\]

Note that

\[
|\mathcal{F}_1| = \left\lceil gn/2 \right\rceil - \left\lceil g/2 \right\rceil - \sum_{i=0}^{3} \gamma_i(g, n)
\]

\[
= \left\lceil gn/2 \right\rceil - \left\lceil g/2 \right\rceil - \sum_{i=0}^{2} \gamma_i(g, n),
\]

\[
|\mathcal{E}| = \left( M(g) + \left\lceil g/2 \right\rceil - 1 - \sum_{i=0}^{2} \delta_i(g) \right)/4.
\]

It is readily checked that \( \delta_i(gn) = \delta_i(g) + \gamma_i(g, n) \) for each \( 0 \leq i \leq 2 \). So

\[
|\mathcal{F}_1| + |\mathcal{F}_2| + |\mathcal{E}|
\]

\[
= \left( M(gn) - M(g) + 1 + |\mathcal{F}_1|)/4 + (M(g) + \left\lceil g/2 \right\rceil - 1 - \sum_{i=0}^{2} \delta_i(g))/4 \right)
\]

\[
= U(gn). \quad \square
\]

Construction 4.3 shows that for the purpose of constructing \((v, 4, 3, 2)\)-OOCs, it is useful to find some \(g\)-regular \((v, 4, 3, 2)\)-OOCs. We introduce some auxiliary designs that will be used in the construction of \(g\)-regular \((v, 4, 3, 2)\)-OOCs.

Let \( n, g, k, t \) be positive integers. An \( H \) design is a triple \((X, G, B)\), where \( G \) is a partition of a set of points \( X \) into \( n \) subsets (called groups), each of size \( g \), and \( B \) is a collection of subsets of \( X \) (called blocks), each of size \( k \), such that each block intersects any given group in at most one point, and each \( t \)-subset of \( X \) from \( t \) distinct groups is contained in a unique block. Such a design is denoted by \( H(n, g, k, t) \).
An automorphism group of an $H$ design $(X, \mathcal{G}, \mathcal{B})$ is a permutation group on $X$ leaving $\mathcal{G}, \mathcal{B}$ invariant, respectively. If an $H$ design $(X, \mathcal{G}, \mathcal{B})$ of type $g^n$ admits an automorphism consisting of $n$ cycles of length $g$, then it is said to be semi-cyclic. We can always identify $X$ with $I_n \times \mathbb{Z}_g$ and $\mathcal{G} = \{(i) \times \mathbb{Z}_g : i \in I_n\}$, where $I_n = \{0, 1, \ldots, n-1\}$. In this case the automorphism can be taken as $(i, x) \mapsto (i, x + 1) (\mod (-, g)), i \in I_n$ and $x \in \mathbb{Z}_g$.

A $t$-($v, k, 1$) packing is a pair $(X, \mathcal{B})$, where $X$ is a set of points and $\mathcal{B}$ is a set of $k$-subsets of $X$ (called blocks) such that every $t$-subset of $X$ occurs in at most one block.

An automorphism group of a $t$-($v, k, 1$) packing $(X, \mathcal{B})$ is a permutation group on $X$ leaving $\mathcal{B}$ invariant. A $t$-($v, k, l$) packing is said to be cyclic if it admits an automorphism consisting of a cycle of length $v$. Without loss of generality identify $X$ with $\mathbb{Z}_v$ and the automorphism can be taken as $x \mapsto x + 1 (\mod v), x \in \mathbb{Z}_v$.

Let $p \equiv 1 (\mod 4)$ be a prime number. Suppose $3$ is a primitive root mod $p$. Suppose also $l$ is a positive integer. A CPQS$^*$(p$^{l+1}$) $(\mathbb{Z}_{p^{l+1}}, \mathcal{B})$ is a cyclic 3-($p^{l+1}$, 4, 1) packing satisfying that each of the following distinct 3-subset orbits appears in one block, while others do not appear in any block.

1. $O((0, r + xp^i, s + yp^i)), \quad$ where $(r, s) \in \{(1, 2), (1, 3), (2, 3)\}, sx - ry \not\equiv 0 (\mod p)$, and $0 \leq x, y \leq p - 1$.
2. $O((0, xp^i, s + yp^i)), \quad$ where $s = \pm 1, \pm 3, x \equiv 3^2i (\mod p)$ for $1 \leq i \leq \frac{p-1}{4}$, and $0 \leq y \leq p - 1$.

When $l \geq 2$ for $p = 5$ and when $l \geq 1$ for $p > 5$, it is not difficult to check above 3-subset orbits are mutually different by Lemma 2.1. One obtains immediately that the total number of base blocks of a CPQS$^*$(p$^{l+1}$) is $p(p - 1)$.

We give two examples of such designs for $p \in \{5, 17\}$. The required designs are constructed on $\mathbb{Z}_{p^{l+1}}$. For each $a \in \mathbb{Z}_{p^{l+1}}$, we use $(r, x)$ to denote $a$ if $a = r + xp^i$, where $0 \leq r \leq p^l - 1$ and $0 \leq x \leq p - 1$. Let $a \equiv 3p^{l-1}(p-1)(\mod p^{l+1})$.

**Example 4.4.** There exists a CPQS$^*$(5$^{l+1}$) for any positive integer $l \geq 2$.

**Proof.** The total 20 base blocks can be obtained by multiplying each of the following 4 base blocks by $a^i, 0 \leq i \leq 4$.

\[
\begin{align*}
&\{(0, 0), (1, 0), (2, 4), (3, 4)\}, \quad \{(0, 0), (1, 3), (2, 3), (3, 1)\}, \\
&\{(0, 0), (0, 1), (1, 0), (3, 1)\}, \quad \{(0, 0), (2, 3), (3, 3), (3, 4)\}. \\
\end{align*}
\]

**Example 4.5.** There exists a CPQS$^*$(17$^{l+1}$) for any positive integer $l$.

**Proof.** The total 272 base blocks can be obtained by multiplying each of the following 16 base blocks by $a^i, 0 \leq i \leq 16$.

\[
\begin{align*}
&\{(0, 0), (1, 0), (2, 8), (3, 3)\}, \quad \{(0, 0), (1, 0), (2, 5), (3, 4)\}, \\
&\{(0, 0), (2, 4), (3, 4), (3, 12)\}, \quad \{(0, 0), (0, 2), (1, 0), (3, 2)\}, \\
&\{(0, 0), (0, 8), (1, 0), (3, 10)\}, \quad \{(0, 0), (0, 1), (1, 0), (3, 1)\}, \\
&\{(0, 0), (0, 4), (1, 0), (3, 14)\}, \quad \{(0, 0), (1, 15), (2, 15), (3, 1)\}, \\
&\{(0, 0), (1, 16), (2, 8), (3, 8)\}, \quad \{(0, 0), (1, 0), (2, 16), (3, 16)\}, \\
&\{(0, 0), (1, 16), (2, 12), (3, 12)\}, \quad \{(0, 0), (1, 11), (2, 11), (3, 7)\}, \\
\end{align*}
\]
We give a recursive construction for $g$-regular $(gn, 4, 3, 2)$-OOCs.

**Construction 4.6.** Let $p \equiv 1 (\text{mod } 4)$ be a prime number. Suppose $l$ is a nonnegative integer. Suppose also that $3$ is a primitive root of the group of units $U(Z_{p^{l+1}})$. If there exist a $p^l$-regular $(p^{l+1}, 4, 3, 2)$-OOC and a CPQS$(p^{l+2})$, then there exists a $p^{l+1}$-regular $(p^{l+2}, 4, 3, 2)$-OOC.

**Proof.** Let $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2$ be a $p^l$-regular $(p^{l+1}, 4, 3, 2)$-OOC on $Z_{p^{l+1}}$, where $\mathcal{F}_1 = \{(0, i, 2i, 3i) : 1 \leq i \leq (p^{l+1} - 1)/2, i \not\equiv 0 (\text{mod } p)\}$. It is readily checked that $|\mathcal{F}_1| = p^l(p - 1)/2$ and $|\mathcal{F}_2| = |\mathcal{F}| - |\mathcal{F}_1| = (p^{2l}(p^2 - 1) - 12p^l(p - 1))/24$.

We shall construct the required $p^{l+1}$-regular $(p^{l+2}, 4, 3, 2)$-OOC on $Z_{p^{l+2}}$.

(i) For every codeword $B = \{x_i : 1 \leq i \leq 4\} \in \mathcal{F}_2$ where $0 \leq x_i < p^{l+1} - 1$ for $1 \leq i \leq 4$, construct a semi-cyclic H(4, $p$, 4, 3) on $B \times Z_p$ with groups $\{\{x_i \times Z_p : x \in B\}$. Such a design exists by Corollary 3.5 in [17]. Denote the family of base blocks of this design by $\mathcal{A}_B$. For each $A = \{(x_i, y_i) : 1 \leq i \leq 4\} \in \mathcal{A}_B$, let $A' = \{x_i + y_i, p^{l+1} : 1 \leq i \leq 4\}$. Denote $\mathcal{C}_B = \{A' : A \in \mathcal{A}_B\}$ and $\mathcal{C}_1 = \bigcup_{B \in \mathcal{F}_2} \mathcal{C}_B$.

(ii) Let $(Z_{p^{l+2}}, \mathcal{B})$ be a CPQS$(p^{l+2})$. Let $\mathcal{C}_2 = \{3'B : 0 \leq i \leq 2(p - 1)/2 - 1, B \in \mathcal{B}\}$ where $3'B = \{3x (\text{mod } p^{l+2}) : x \in B\}$.

(iii) Let $\mathcal{C}_3 = \{(0, i, 2i, 3i) : 1 \leq i \leq (p^{l+2} - 1)/2, i \not\equiv 0 (\text{mod } p)\}$.

Let $\mathcal{F}' = \mathcal{F}_1 \cup \mathcal{F}_2$, where $\mathcal{F}_1 = \mathcal{C}_3$, $\mathcal{F}_2' = \mathcal{C}_1 \cup \mathcal{C}_2$. We obtain that $|\mathcal{F}'_1'| = p^{l+1}(p - 1)/2$ and $|\mathcal{F}'_2| = p^2|\mathcal{F}_2| + p^l(p - 1)/2|\mathcal{B}| = (p^{2l+1}(p^2 - 1) - 12p^l(p - 1))/24$. Since the size of $\mathcal{F}'$ is the right number of codewords in a $p^{l+1}$-regular $(p^{l+2}, 4, 3, 2)$-OOC, in the following, it suffices to show that each 3-subset orbit not contained in the subgroup of order $p^{l+1}$ appears in exactly one codeword of $\mathcal{F}'$.

Let $T = O((a, b, c))$ be such a 3-subset orbit of $Z_{p^{l+2}}$. Let $a = r + xp^{l+1}$ and $b = s + yp^{l+1}$, where $0 \leq r, s \leq p^{l+1} - 1$ and $0 \leq x, y \leq p - 1$. Clearly, $r$ and $s$ cannot be divisible by $p$ at the same time.

**Case 1.** $O((0, r, s))$ is contained in a codeword $B \in \mathcal{F}_2$, that is, there exists an integer $0 \leq \tau \leq p^{l+1} - 1$ such that $\{0, r, s\} + \tau = \{r, r', s'\} \subseteq B$, where $r' = r + \tau - [(r + \tau)/p^{l+1}]p^{l+1}$ and $s' = s + \tau - [(s + \tau)/p^{l+1}]p^{l+1}$. Thus, there exists an integer $0 \leq c \leq p - 1$ such that $\{(r, c), (r', c + x + [(r + \tau)/p^{l+1}]), (s, c + y + [(s + \tau)/p^{l+1}])\}$ appears in one block $A$ of $\mathcal{A}_B$. It is easy to see that $\{\tau + cp^{l+1}, a + \tau + cp^{l+1}, b + \tau + cp^{l+1}\} = \{\tau + cp^{l+1}, r' + (c + x + [(r + \tau)/p^{l+1}])p^{l+1}, s' + (c + y + [(s + \tau)/p^{l+1}])p^{l+1}\}$ appears in $A'$ of $\mathcal{C}_1$, and hence $T$ appears in a codeword of $\mathcal{C}_1$.

**Case 2.** $O((0, r, s))$ is contained in a codeword $B \in \mathcal{F}_1$. Without loss of generality, we can assume that $\{0, r, s\} \in \{(0, i, 2i), (0, i, 3i), (0, 2i, 3i)\}$ for some $1 \leq i \leq (p^{l+1} - 1)/2$ and $i \not\equiv 0 (\text{mod } p)$.

**Subcase 1.** $2r \equiv s (\text{mod } p^{l+1})$. If $|2r/p^{l+1}| + 2x \equiv y (\text{mod } p)$, we have $2a \equiv b (\text{mod } p^{l+2})$. In this case $T$ appears in a codeword of $\mathcal{C}_3$.

Otherwise, there is an integer $c$, where $0 \leq t \leq p^l(p - 1)/2 - 1$, such that $c \equiv (1)^{t}c' (\text{mod } p^{l+1})$ with $t \in [0, 1]$. Let $x' = \sum_{c}(x - [(c'/p^{l+1}]) (\text{mod } p)$, $y' = \sum_{c}(y - [(c'/p^{l+1}]) (\text{mod } p)$. Then $\{a, b, c\} = 3'(0, (1)^{t}x + x' p^{l+1}, 2(1)^{t}y + y' p^{l+1})$. Since $2r/p^{l+1} + 2x \equiv y (\text{mod } p)$, it is readily checked that $2x' \not\equiv y'(\text{mod } p)$.
$O(0, (-1)^c + x'p^{l+1}, 2(-1)^c + y'p^{l+1})$ appears in a block $B$ of $C$. Thus, $T$ appears in the codeword $3'B$ of $C_2$. Note that $O((0, -1 + x'p^{l+1}, -2 + y'p^{l+1}) = O((0, 1 + (x' - y')p^{l+1}, 2 - y'p^{l+1})) and $2(x' - y') \neq -y'(mod \ p)$.

**Subcase 2.** $3r \equiv s (mod \ p^{l+1})$. If $(3r/p^{l+1}) + 3x \equiv y (mod \ p)$, we have $3a \equiv b \equiv b$ (mod $p^{l+2}$). In this case $T$ appears in a codeword of $C_3$.

Otherwise, there is an integer $t$, where $0 \leq t \leq p'(p - 1)/2 - 1$, such that $r \equiv (-1)^c 3t^t (mod \ p^{l+1})$ with $e \in [0, 1]$. Let $x' = 3^{-t}(x - \lfloor (-(1)^c 3t^t/p^{l+1}) \rfloor (mod \ p))$, $y' = 3^{-t}(y - \lfloor (-(1)^c 3t^t/p^{l+1}) \rfloor (mod \ p))$. Then $\{0, a, b\} = 3'(0, (-1)^c + x'p^{l+1}, 3(-1)^c + y'p^{l+1})$. Since $(3r/p^{l+1}) + 3x \not\equiv y (mod \ p)$, it is readily checked that $3x' \not\equiv y'(mod \ p)$. Then, $O((0, (-1)^c + x'p^{l+1}, 3(-1)^c + y'p^{l+1})) is contained in a block $B$ of $C$. So $T$ appears in the codeword $3'B$ of $C_2$. Note that $O((0, -1 + x'p^{l+1}, -3 + y'p^{l+1})) = O((0, 2 + (x' - y')p^{l+1}, 3 - y'p^{l+1})) and 3(x' - y') \neq -2y'(mod \ p)$.

**Subcase 3.** $3r \equiv 2s (mod \ p^{l+1})$. If $(3r/p^{l+1}) + 3x \equiv 2s/p^{l+1} + 2y (mod \ p)$, we have $3a \equiv 2b (mod \ p^{l+2}) and b \equiv 3w (mod \ p^{l+2})$. Thus $T$ appears in $\{0, w, 2w, 3w\}$ of $C_3$.

Otherwise, there is another integer $j$ such that $r \equiv 2j (mod \ p^{l+1}) and s \equiv 3j (mod \ p^{l+1})$. Let $j \equiv (-1)^c 3j (mod \ p^{l+1})$, where $e \in [0, 1]$ and $0 \leq t \leq p'(p - 1)/2 - 1$. Let $x' = 3^{-t}(x - \lfloor (-(1)^c 3j/p^{l+1}) \rfloor (mod \ p))$, $y' = 3^{-t}(y - \lfloor (-(1)^c 3j/p^{l+1}) \rfloor (mod \ p))$. Then $\{0, a, b\} = 3'(0, 2(-1)^c + x'p^{l+1}, 3(-1)^c + y'p^{l+1})$. Since $(3r/p^{l+1}) + 3x \not\equiv \lfloor 2s/p^{l+1} \rfloor + 2y (mod \ p)$, it is readily checked that $3x' \not\equiv y' (mod \ p)$. (In fact, let $2j = r + n_1p^{l+1}$, $3j = s + n_2p^{l+1}$. We obtain $3r - 2s = (2n_2 - 3n_1)p^{l+1}$. Thus, $[3r/p^{l+1}] - [2s/p^{l+1}] = 2n_2 - 3n_1$. If $3x' \equiv 2y (mod \ p)$, we have $3(x - \lfloor 2j/p^{l+1} \rfloor) \equiv 2(y - \lfloor 3j/p^{l+1} \rfloor) (mod \ p)$. So $3(x - n_1) \equiv 2(y - n_2) (mod \ p)$.) That is $3r/p^{l+1} + 3x \equiv \lfloor 2s/p^{l+1} \rfloor + 2y (mod \ p)$, a contradiction occurs.) Then, $O((0, 2(-1)^c + x'p^{l+1}, 3(-1)^c + y'p^{l+1})) appears in a block $B of C$. So $T$ appears in the codeword $3'B$ of $C_2$. Note that $O((0, -2 + x'p^{l+1}, -3 + y'p^{l+1})) = O((0, 1 + (x' - y')p^{l+1}, 3 - y'p^{l+1})) and 3(x' - y') \not\equiv -2y'(mod \ p)$.

**Case 3.** $s \not\equiv r = 0$. For $T$ cannot appear in the subgroup of order $p^{l+1}$, we have $s \not\equiv 0 (mod \ p)$. Without loss of generality, suppose $x \equiv 3^0 (mod \ p)$, $0 \leq k \leq (p - 1)/2 - 1$. Let $3^{\lfloor -t \rfloor} \equiv (-1)^c 3' (mod \ p^{l+1})$ where $0 \leq t \leq p'(p - 1)/2 - 1$ and $e \in [0, 1]$. Rewrite $t = q(p - 1)/2 - 2r + n$ for integers $1 \leq q \leq p'$, $1 \leq r \leq (p - 1)/4 and $n \in [0, 1]$. Note that $3^{(p-1)/2} \equiv 1 (mod \ p)$. Let $z \equiv (-1)^c 3^n (mod \ p^{l+1})$. We have $s \equiv \lfloor 3^{\lfloor -t \rfloor + n} \rfloor (mod \ p^{l+1})$.

**Subcase 1.** $t - n + k \leq p'(p - 1)/2 - 1$. If $q \equiv 0 (mod \ 2)$, let $x' \equiv 3^{2^r} (mod \ p)$, $y' \equiv 3^{\lfloor -t \rfloor + n} (y - \lfloor 3^{\lfloor -t \rfloor + n} / p^{l+1} \rfloor) (mod \ p)$. Then $\{0, a, b\} = 3^{\lfloor -t \rfloor + n} \lfloor 0, x'p^{l+1}, z + y'p^{l+1} \rfloor$. Since $O((0, x'p^{l+1}, z + y'p^{l+1})) is contained in a block $B \in B$, $T$ appears in the codeword $3^{\lfloor -t \rfloor + n} B of C_2$.

Otherwise, let $x' \equiv 3^{2^r} (mod \ p)$, $y' \equiv 3^{\lfloor -t \rfloor + n} (y - \lfloor 3^{\lfloor -t \rfloor + n} / p^{l+1} \rfloor) (mod \ p)$. Then $\{0, a, b\} = 3^{\lfloor -t \rfloor + n} \lfloor 0, x'p^{l+1}, z + y'p^{l+1} \rfloor$. Note that $O((0, a, b)) = O((0, -a, b - a))$. Since $O((0, x'p^{l+1}, z + y'p^{l+1})) is contained in a block $B \in B$, $T$ appears in the codeword $3^{\lfloor -t \rfloor + n} B of C_2$.

**Subcase 2.** $t - n + k \geq p'(p - 1)/2$. Let $e = t - n + k - p'(p - 1)/2$. If $q \equiv 1 (mod \ 2)$, let $x' \equiv 3^{2^r} (mod \ p)$, $y' \equiv 3^{\lfloor -t \rfloor + n} (y - \lfloor 3^{\lfloor -t \rfloor + n} / p^{l+1} \rfloor) (mod \ p)$. Then $\{0, a, b\} = 3^{\lfloor -t \rfloor + n} \lfloor 0, x'p^{l+1}, z + y'p^{l+1} \rfloor$. Since $O((0, x'p^{l+1}, z + y'p^{l+1})) is contained in a block $B \in B$, $T$ appears in the codeword $3^{\lfloor -t \rfloor + n} B of C_2$.

Otherwise, let $x' \equiv 3^{2^r} (mod \ p)$, $y' \equiv 3^{\lfloor -t \rfloor + n} (y - \lfloor 3^{\lfloor -t \rfloor + n} / p^{l+1} \rfloor) (mod \ p)$. Thus, $\{0, -a, b - a\} = 3^0 \lfloor 0, x'p^{l+1}, z + y'p^{l+1} \rfloor$. Note that $O((0, a, b)) = O((0, -a, b - a))$. Thus, $T$ appears in the codeword $3^{\lfloor -t \rfloor + n} B of C_2$.
Since $O(\{0, x'p^{l+1}, -z + y'p^{l+1}\})$ is contained in a block $B \in \mathcal{B}$, $T$ appears in the codeword $3^rB$ of $C_2$.

Lemma 4.7. [22] If $p$ is an odd prime and $l \in \mathbb{Z}^+$, then the group of units $U(\mathbb{Z}_p^l)$ is cyclic. Further, if $g \in \mathbb{Z}$ is a primitive root mod $p$ and $g^{p-1} \not\equiv 1 \pmod{p^2}$, then $g$ is a primitive root mod $p^l$.

Corollary 4.8. For $p \in \{5, 17\}$ and any $l \in \mathbb{Z}^+$, $3$ is a primitive root of $U(\mathbb{Z}_p^l)$.

Proof. Since $3$ is a primitive root of $U(\mathbb{Z}_p)$ and $3^{p-1} \not\equiv 1 \pmod{p^2}$ for $p \in \{5, 17\}$, the conclusion then follows by Lemma 4.7.

Lemma 4.9. There exists a $p^l$-regular $(p^{l+1}, 4, 3, 2)$-OOC for $l \in \mathbb{Z}^+$ and $p \in \{5, 17\}$.

Proof. (1) $p = 5$. For $l = 1$, the result comes from Example 4.2. For $l \geq 2$, start with a $5$-regular $(25, 4, 3, 2)$-OOC. Applying Construction 4.6 inductively give the desired codes. The needed CPQS$^\star(5^{l+2})$ with $l \geq 1$ comes from Example 4.4.

(2) $p = 17$. Start with a $1$-regular $(17, 4, 3, 2)$-OOC from Appendix. Applying Construction 4.6 inductively give the desired codes. The needed CPQS$^\star(17^{l+2})$ with $l \geq 0$ comes from Example 4.5.

Theorem 4.10. There exists an optimal $(p^l, 4, 3, 2)$-OOC with $U(p^l)$ codewords for any positive integer $l$ and $p \in \{5, 17\}$.

Proof. For $l = 1$, the results come from Example 1.1 and Appendix, respectively. For $l \geq 2$, applying Construction 4.3 with a $(p^{l-1}, 4, 3, 2)$-OOC with $U(p^{l-1})$ codewords and a $p^{l-1}$-regular $(p^l, 4, 3, 2)$-OOC inductively, we can obtain the required codes. Here, the needed $p^{l-1}$-regular $(p^l, 4, 3, 2)$-OOC comes from Lemma 4.9.

5. CONCLUSION

In this paper, we make a preliminary study on the size of optimal $(v, 4, 3, 2)$-OOCs. A recursive construction and some direct constructions are given. With these results, we construct an optimal $(v, 4, 3, 2)$-OOC with $U(v)$ codewords for some infinite series. For small values of $v$, we have the following result.

Theorem 5.1. There exists an optimal $(v, 4, 3, 2)$-OOC with $U(v)$ codewords for each $5 \leq v \leq 50$ and $v \not\in \{8, 10, 13, 16, 18, 19, 20, 24, 32, 40, 48\}$.

Proof. For each $v \in \{14, 22, 25, 30, 34, 42, 46, 49, 50\}$, applying Construction 4.3 with a proper $g$-regular $(v, 4, 3, 2)$-OOC from Lemma 4.2 and an optimal $(g, 4, 3, 2)$-OOC with $U(g)$ codewords, we obtain the desired code. The needed $(g, 4, 3, 2)$-OOCs come from Example 1.1 and Appendix, respectively. For each other value $v$, the optimal $(v, 4, 3, 2)$-OOC with $U(v)$ codewords can be found in Appendix.

Thus, we tend to conjecture that $\Phi(v, 4, 3, 2) = U(v)$, if $v$ sufficiently large.

Journal of Combinatorial Designs DOI 10.1002/jcd
REFERENCES


[17] T. Feng, Y. Chang, and L. Ji, Constructions for strictly cyclic 3-designs and applications to optimal OOCs with $\lambda = 2$, J Combin Theory A 115 (2008), 1527–1551.


[29] M. Mishima, H. L. Fu, and S. Uruno, Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3, Des Codes Cryptogr 52 (2009), 275–291.

APPENDIX

For shortening the list of codewords for optimal $(v, 4, 3, 2)$-OOCs with $U(v)$ codewords, all codewords are divided into two parts. The first part consists of $\{0, i, 2i, 3i\}$, $i \in [1, \lfloor v/2 \rfloor - 1] \setminus Q(v)$. The second part is displayed below. For $v \in \{6, 7, 9, 11\}$, the second part is the empty set.

$v = 15$: 
$\{0, 1, 4, 5\}, \{0, 1, 6, 10\}, \{0, 2, 5, 12\}, \{0, 2, 7, 9\}$.

$v = 17$: 
$\{0, 1, 4, 5\}, \{0, 1, 7, 11\}, \{0, 2, 5, 14\}, \{0, 2, 8, 10\}$.

$v = 21$: 
$\{0, 2, 9, 11\}, \{0, 3, 7, 13\}, \{0, 3, 10, 14\}, \{0, 1, 8, 9\}, \{0, 2, 5, 7\}, \{0, 2, 8, 10\}, \{0, 4, 9, 16\}, \{0, 3, 11, 17\}, \{0, 1, 4, 5\}, \{0, 1, 6, 7\}$.

$v = 23$: 
$\{0, 1, 4, 5\}, \{0, 1, 9, 15\}, \{0, 1, 10, 14\}, \{0, 4, 10, 17\}, \{0, 2, 7, 18\}, \{0, 1, 6, 7\}, \{0, 2, 8, 10\}, \{0, 2, 11, 13\}, \{0, 3, 11, 14\}, \{0, 3, 7, 19\}, \{0, 2, 5, 20\}$.

Journal of Combinatorial Designs DOI 10.1002/jcd
\[ v = 26: \]
\[ \{0, 5, 11, 20\}, \{0, 1, 10, 11\}, \{0, 2, 7, 20\}, \{0, 1, 8, 19\}, \{0, 1, 4, 5\}, \{0, 2, 9, 19\}, \{0, 3, 12, 16\}, \{0, 1, 12, 13\}, \{0, 2, 5, 23\}, \{0, 2, 8, 21\}, \{0, 1, 6, 7\}, \{0, 2, 11, 13\}, \{0, 3, 13, 17\}, \{0, 3, 11, 14\}, \{0, 4, 9, 21\}, \{0, 3, 7, 10\}. \]

\[ v = 27: \]
\[ \{0, 1, 10, 11\}, \{0, 1, 12, 16\}, \{0, 5, 12, 20\}, \{0, 4, 9, 22\}, \{0, 1, 8, 9\}, \{0, 2, 5, 7\}, \{0, 2, 10, 19\}, \{0, 2, 11, 13\}, \{0, 2, 12, 14\}, \{0, 3, 7, 23\}, \{0, 1, 6, 7\}, \{0, 2, 9, 20\}, \{0, 3, 13, 16\}, \{0, 4, 10, 21\}, \{0, 4, 13, 17\}, \{0, 3, 8, 22\}, \{0, 1, 4, 5\}, \{0, 2, 8, 21\}. \]

\[ v = 28: \]
\[ \{0, 1, 11, 18\}, \{0, 1, 12, 17\}, \{0, 1, 6, 14\}, \{0, 3, 11, 14\}, \{0, 2, 7, 23\}, \{0, 1, 8, 9\}, \{0, 1, 13, 16\}, \{0, 1, 15, 23\}, \{0, 2, 5, 25\}, \{0, 3, 12, 19\}, \{0, 2, 8, 21\}, \{0, 1, 4, 5\}, \{0, 2, 11, 19\}, \{0, 2, 12, 14\}, \{0, 3, 7, 24\}, \{0, 3, 10, 13\}, \{0, 1, 7, 22\}, \{0, 2, 9, 22\}, \{0, 4, 10, 14\}, \{0, 4, 13, 17\}, \{0, 4, 9, 23\}. \]

\[ v = 29: \]
\[ \{0, 1, 11, 12\}, \{0, 1, 13, 17\}, \{0, 2, 16, 22\}, \{0, 2, 9, 15\}, \{0, 1, 8, 9\}, \{0, 1, 4, 5\}, \{0, 2, 12, 19\}, \{0, 2, 13, 18\}, \{0, 2, 14, 17\}, \{0, 2, 8, 10\}, \{0, 3, 8, 14\}, \{0, 2, 5, 7\}, \{0, 3, 11, 21\}, \{0, 3, 12, 20\}, \{0, 3, 18, 24\}, \{0, 4, 9, 24\}, \{0, 3, 7, 10\}, \{0, 1, 6, 7\}, \{0, 4, 10, 23\}, \{0, 4, 13, 20\}, \{0, 4, 14, 18\}. \]

\[ v = 31: \]
\[ \{0, 1, 10, 13\}, \{0, 1, 12, 20\}, \{0, 1, 14, 18\}, \{0, 6, 13, 24\}, \{0, 4, 9, 21\}, \{0, 2, 7, 9\}, \{0, 1, 19, 22\}, \{0, 2, 10, 23\}, \{0, 2, 12, 14\}, \{0, 6, 15, 22\}, \{0, 2, 5, 20\}, \{0, 1, 8, 9\}, \{0, 2, 13, 28\}, \{0, 2, 15, 17\}, \{0, 3, 15, 19\}, \{0, 5, 14, 22\}, \{0, 3, 8, 11\}, \{0, 1, 6, 7\}, \{0, 4, 10, 25\}, \{0, 4, 11, 15\}, \{0, 4, 14, 26\}, \{0, 5, 11, 25\}, \{0, 3, 7, 10\}, \{0, 1, 4, 5\}, \{0, 2, 8, 25\}. \]

\[ v = 33: \]
\[ \{0, 1, 10, 11\}, \{0, 1, 12, 13\}, \{0, 1, 14, 15\}, \{0, 4, 15, 22\}, \{0, 4, 9, 16\}, \{0, 2, 5, 7\}, \{0, 2, 12, 14\}, \{0, 2, 13, 18\}, \{0, 2, 15, 19\}, \{0, 7, 15, 25\}, \{0, 2, 8, 10\}, \{0, 1, 4, 5\}, \{0, 2, 16, 20\}, \{0, 2, 17, 22\}, \{0, 3, 14, 22\}, \{0, 3, 16, 19\}, \{0, 3, 7, 10\}, \{0, 1, 6, 7\}, \{0, 4, 10, 26\}, \{0, 4, 11, 27\}, \{0, 4, 13, 24\}, \{0, 4, 14, 23\}, \{0, 2, 9, 11\}, \{0, 1, 8, 9\}, \{0, 4, 21, 28\}, \{0, 5, 11, 21\}, \{0, 5, 13, 25\}, \{0, 5, 17, 27\}, \{0, 6, 14, 20\}, \{0, 3, 8, 11\}. \]

\[ v = 35: \]
\[ \{0, 1, 10, 11\}, \{0, 1, 13, 14\}, \{0, 1, 15, 16\}, \{0, 3, 10, 26\}, \{0, 2, 9, 15\}, \{0, 1, 6, 7\}, \{0, 2, 11, 18\}, \{0, 2, 12, 20\}, \{0, 2, 14, 16\}, \{0, 3, 21, 27\}, \{0, 2, 8, 10\}, \{0, 1, 8, 9\}, \{0, 2, 17, 25\}, \{0, 2, 19, 26\}, \{0, 2, 22, 28\}, \{0, 5, 14, 19\}, \{0, 3, 8, 15\}, \{0, 1, 4, 5\}, \{0, 3, 11, 17\}, \{0, 3, 12, 28\}, \{0, 3, 13, 20\}, \{0, 3, 14, 24\}, \{0, 3, 18, 25\}, \{0, 2, 5, 7\}, \{0, 3, 23, 30\}, \{0, 4, 10, 23\}, \{0, 4, 14, 20\}, \{0, 4, 15, 24\}, \{0, 4, 16, 29\}, \{0, 4, 9, 21\}, \{0, 4, 17, 22\}, \{0, 4, 18, 30\}, \{0, 4, 19, 25\}, \{0, 5, 11, 16\}, \{0, 5, 13, 27\}, \{0, 3, 7, 31\}. \]
v = 36:
{0, 1, 10, 11}, {0, 1, 12, 13}, {0, 1, 14, 15}, {0, 5, 11, 16}, {0, 4, 9, 13}, {0, 1, 6, 7},
{0, 1, 16, 21}, {0, 1, 17, 18}, {0, 2, 12, 14}, {0, 6, 20, 29}, {0, 2, 9, 11}, {0, 2, 5, 7},
{0, 2, 13, 15}, {0, 2, 16, 18}, {0, 3, 11, 20}, {0, 3, 12, 22}, {0, 3, 7, 10}, {0, 1, 8, 9},
{0, 3, 15, 24}, {0, 3, 16, 23}, {0, 3, 17, 27}, {0, 3, 18, 31}, {0, 3, 19, 28}, {0, 1, 4, 5},
{0, 4, 10, 29}, {0, 4, 11, 30}, {0, 4, 14, 18}, {0, 4, 15, 19}, {0, 4, 17, 23}, {0, 3, 8, 21},
{0, 5, 12, 29}, {0, 5, 13, 24}, {0, 5, 14, 19}, {0, 5, 17, 28}, {0, 6, 13, 22}, {0, 2, 8, 10},
{0, 7, 15, 25}, {0, 7, 18, 28}.

v = 37:
{0, 1, 10, 11}, {0, 1, 12, 15}, {0, 1, 14, 16}, {0, 4, 10, 24}, {0, 4, 9, 13}, {0, 1, 8, 9},
{0, 1, 17, 21}, {0, 1, 22, 24}, {0, 1, 23, 26}, {0, 7, 16, 28}, {0, 2, 8, 10}, {0, 1, 4, 5},
{0, 2, 12, 14}, {0, 2, 17, 19}, {0, 2, 18, 21}, {0, 3, 10, 16}, {0, 3, 7, 33}, {0, 1, 6, 7},
{0, 3, 12, 27}, {0, 3, 13, 28}, {0, 3, 18, 22}, {0, 3, 24, 30}, {0, 5, 12, 29}, {0, 2, 5, 7},
{0, 4, 14, 25}, {0, 4, 16, 27}, {0, 4, 17, 31}, {0, 4, 18, 23}, {0, 5, 11, 31}, {0, 3, 8, 11},
{0, 5, 13, 30}, {0, 5, 17, 22}, {0, 5, 18, 24}, {0, 6, 14, 29}, {0, 6, 15, 21}, {0, 2, 9, 11},
{0, 7, 18, 25}, {0, 8, 17, 28}, {0, 8, 18, 26}.

v = 38:
{0, 1, 10, 17}, {0, 1, 14, 16}, {0, 1, 27, 30}, {0, 1, 23, 25}, {0, 1, 7, 11}, {0, 1, 4, 5},
{0, 1, 15, 19}, {0, 1, 18, 21}, {0, 1, 20, 24}, {0, 1, 22, 29}, {0, 1, 9, 12}, {0, 1, 6, 8},
{0, 1, 28, 32}, {0, 1, 31, 33}, {0, 2, 10, 35}, {0, 2, 12, 21}, {0, 2, 5, 30}, {0, 2, 9, 11},
{0, 2, 13, 23}, {0, 2, 17, 27}, {0, 2, 19, 28}, {0, 3, 15, 26}, {0, 3, 7, 10}, {0, 3, 8, 14},
{0, 3, 16, 23}, {0, 3, 17, 22}, {0, 3, 18, 25}, {0, 3, 19, 24}, {0, 3, 27, 33}, {0, 4, 9, 22},
{0, 4, 13, 27}, {0, 4, 15, 29}, {0, 4, 16, 26}, {0, 4, 20, 33}, {0, 5, 12, 17}, {0, 5, 14, 20},
{0, 5, 23, 29}, {0, 6, 13, 19}, {0, 6, 17, 23}, {0, 7, 18, 26}, {0, 7, 19, 27}, {0, 8, 17, 25}.

v = 39:
{0, 1, 10, 11}, {0, 1, 12, 13}, {0, 1, 14, 15}, {0, 4, 18, 23}, {0, 4, 9, 28}, {0, 1, 8, 9},
{0, 1, 16, 17}, {0, 1, 18, 22}, {0, 2, 12, 14}, {0, 7, 17, 29}, {0, 2, 8, 10}, {0, 1, 4, 5},
{0, 2, 13, 15}, {0, 2, 16, 18}, {0, 2, 17, 24}, {0, 2, 19, 21}, {0, 5, 14, 30}, {0, 2, 5, 7},
{0, 3, 12, 16}, {0, 3, 13, 19}, {0, 3, 17, 20}, {0, 3, 23, 29}, {0, 3, 26, 30}, {0, 1, 6, 7},
{0, 4, 10, 26}, {0, 4, 11, 19}, {0, 4, 14, 29}, {0, 4, 15, 34}, {0, 4, 17, 33}, {0, 2, 9, 11},
{0, 4, 20, 25}, {0, 4, 24, 32}, {0, 5, 11, 26}, {0, 5, 12, 31}, {0, 5, 13, 32}, {0, 3, 7, 10},
{0, 5, 16, 28}, {0, 5, 18, 33}, {0, 6, 13, 25}, {0, 6, 14, 31}, {0, 6, 20, 32}, {0, 3, 8, 11},
{0, 7, 18, 28}, {0, 8, 17, 30}, {0, 8, 18, 26}.

v = 41:
{0, 1, 10, 11}, {0, 1, 12, 13}, {0, 1, 15, 16}, {0, 5, 14, 26}, {0, 1, 6, 7}, {0, 1, 8, 9},
{0, 1, 17, 18}, {0, 1, 19, 23}, {0, 2, 12, 14}, {0, 6, 15, 32}, {0, 8, 18, 31}, {0, 2, 5, 7},
{0, 2, 13, 16}, {0, 2, 17, 19}, {0, 2, 18, 25}, {0, 2, 20, 22}, {0, 2, 27, 30}, {0, 1, 4, 5},
{0, 3, 12, 15}, {0, 3, 13, 17}, {0, 3, 18, 26}, {0, 3, 20, 23}, {0, 3, 27, 31}, {0, 3, 8, 11}.
{0, 4, 10, 24}, {0, 4, 11, 34}, {0, 4, 16, 27}, {0, 4, 18, 29}, {0, 4, 19, 25}, {0, 4, 9, 13}, {0, 4, 20, 26}, {0, 4, 21, 35}, {0, 5, 11, 16}, {0, 5, 12, 34}, {0, 5, 13, 25}, {0, 3, 7, 10}, {0, 5, 19, 24}, {0, 5, 20, 32}, {0, 5, 21, 33}, {0, 6, 13, 34}, {0, 6, 14, 33}, {0, 2, 8, 10}, {0, 6, 16, 31}, {0, 6, 17, 23}, {0, 6, 19, 28}, {0, 7, 15, 22}, {0, 8, 17, 28}, {0, 2, 9, 11}, {0, 8, 21, 32}, {0, 9, 19, 31}.

\(v = 43:\)
{0, 1, 10, 11}, {0, 1, 12, 13}, {0, 1, 14, 17}, {0, 4, 22, 34}, {0, 4, 9, 38}, {0, 1, 8, 9}, {0, 1, 16, 18}, {0, 1, 19, 20}, {0, 1, 26, 28}, {0, 1, 27, 30}, {0, 3, 7, 10}, {0, 1, 4, 5}, {0, 2, 12, 14}, {0, 2, 13, 19}, {0, 2, 16, 20}, {0, 2, 21, 23}, {0, 2, 25, 29}, {0, 1, 6, 7}, {0, 2, 26, 32}, {0, 3, 12, 15}, {0, 3, 13, 22}, {0, 3, 14, 27}, {0, 5, 20, 26}, {0, 2, 5, 7}, {0, 3, 18, 21}, {0, 3, 19, 32}, {0, 3, 24, 33}, {0, 4, 10, 14}, {0, 4, 11, 28}, {0, 2, 8, 10}, {0, 4, 13, 25}, {0, 4, 15, 23}, {0, 4, 16, 26}, {0, 4, 19, 36}, {0, 4, 21, 31}, {0, 2, 9, 11}, {0, 4, 24, 32}, {0, 5, 11, 25}, {0, 5, 12, 27}, {0, 5, 13, 18}, {0, 5, 17, 31}, {0, 3, 8, 11}, {0, 5, 21, 36}, {0, 5, 22, 28}, {0, 5, 23, 37}, {0, 6, 13, 36}, {0, 6, 14, 24}, {0, 6, 15, 34}, {0, 6, 16, 22}, {0, 6, 25, 35}, {0, 7, 15, 33}, {0, 7, 16, 23}, {0, 7, 17, 35}, {0, 8, 20, 31}, {0, 8, 21, 29}, {0, 9, 20, 29}.

\(v = 44:\)
{0, 1, 10, 11}, {0, 1, 12, 13}, {0, 1, 14, 17}, {0, 1, 28, 31}, {0, 4, 21, 25}, {0, 1, 8, 9}, {0, 1, 16, 18}, {0, 1, 19, 20}, {0, 1, 21, 22}, {0, 1, 27, 29}, {0, 5, 17, 22}, {0, 1, 4, 5}, {0, 2, 12, 14}, {0, 2, 13, 15}, {0, 2, 19, 22}, {0, 2, 20, 26}, {0, 6, 15, 21}, {0, 1, 6, 7}, {0, 2, 24, 27}, {0, 3, 12, 15}, {0, 3, 13, 24}, {0, 3, 14, 18}, {0, 7, 18, 33}, {0, 2, 5, 7}, {0, 3, 19, 26}, {0, 3, 21, 28}, {0, 3, 23, 34}, {0, 3, 29, 33}, {0, 4, 10, 31}, {0, 4, 9, 29}, {0, 4, 11, 35}, {0, 4, 13, 37}, {0, 4, 14, 26}, {0, 4, 17, 38}, {0, 4, 19, 39}, {0, 2, 9, 11}, {0, 4, 22, 34}, {0, 5, 11, 16}, {0, 5, 12, 29}, {0, 5, 13, 35}, {0, 5, 14, 36}, {0, 3, 8, 11}, {0, 5, 19, 30}, {0, 5, 20, 37}, {0, 5, 21, 26}, {0, 6, 13, 28}, {0, 6, 14, 20}, {0, 2, 8, 10}, {0, 6, 16, 34}, {0, 6, 17, 33}, {0, 6, 22, 37}, {0, 7, 15, 36}, {0, 7, 16, 35}, {0, 3, 7, 10}, {0, 7, 19, 32}, {0, 8, 17, 31}, {0, 8, 19, 27}, {0, 8, 21, 35}, {0, 9, 19, 34}, {0, 9, 21, 32}.

\(v = 45:\)
{0, 1, 10, 14}, {0, 1, 13, 15}, {0, 1, 28, 30}, {0, 2, 25, 31}, {0, 4, 22, 29}, {0, 1, 6, 8}, {0, 1, 16, 18}, {0, 1, 17, 20}, {0, 1, 19, 21}, {0, 1, 25, 27}, {0, 1, 26, 29}, {0, 1, 4, 5}, {0, 1, 31, 33}, {0, 1, 32, 36}, {0, 1, 34, 37}, {0, 1, 35, 39}, {0, 1, 38, 40}, {0, 2, 5, 9}, {0, 2, 10, 12}, {0, 2, 11, 13}, {0, 2, 16, 22}, {0, 2, 19, 23}, {0, 2, 24, 28}, {0, 1, 9, 12}, {0, 2, 38, 42}, {0, 3, 10, 13}, {0, 3, 15, 18}, {0, 3, 22, 25}, {0, 3, 34, 40}, {0, 3, 8, 14}, {0, 4, 15, 19}, {0, 4, 16, 31}, {0, 4, 17, 25}, {0, 4, 18, 33}, {0, 4, 20, 27}, {0, 1, 7, 11}, {0, 4, 24, 32}, {0, 5, 12, 17}, {0, 5, 13, 28}, {0, 5, 14, 36}, {0, 5, 16, 34}, {0, 5, 18, 32}, {0, 5, 19, 27}, {0, 5, 21, 26}, {0, 5, 22, 37}, {0, 5, 23, 31}, {0, 6, 13, 24}, {0, 6, 15, 26}, {0, 6, 16, 28}, {0, 6, 21, 30}, {0, 6, 23, 35}, {0, 6, 25, 36}, {0, 6, 27, 38}, {0, 7, 15, 22}, {0, 7, 16, 36}, {0, 7, 17, 24}, {0, 7, 20, 32}, {0, 8, 17, 36}, {0, 8, 18, 35}, {0, 8, 19, 33}, {0, 8, 20, 34}, {0, 9, 19, 35}, {0, 9, 22, 32}, {0, 10, 21, 31}.

Journal of Combinatorial Designs DOI 10.1002/jcd
\( v = 47: \)
\[
\{0, 1, 10, 11\}, \{0, 1, 12, 13\}, \{0, 1, 14, 15\}, \{0, 2, 20, 22\}, \{0, 3, 8, 11\}, \{0, 2, 5, 7\}, \\
\{0, 1, 17, 18\}, \{0, 1, 19, 20\}, \{0, 1, 21, 22\}, \{0, 2, 23, 25\}, \{0, 2, 8, 10\}, \{0, 1, 4, 5\}, \\
\{0, 2, 12, 14\}, \{0, 2, 13, 15\}, \{0, 2, 16, 18\}, \{0, 2, 19, 21\}, \{0, 2, 9, 11\}, \{0, 1, 6, 7\}, \\
\{0, 3, 12, 15\}, \{0, 3, 13, 16\}, \{0, 3, 14, 17\}, \{0, 3, 18, 21\}, \{0, 3, 7, 10\}, \{0, 1, 8, 9\}, \\
\{0, 3, 19, 23\}, \{0, 3, 20, 24\}, \{0, 3, 26, 30\}, \{0, 3, 27, 31\}, \{0, 4, 10, 14\}, \{0, 4, 9, 13\}, \\
\{0, 4, 11, 15\}, \{0, 4, 16, 25\}, \{0, 4, 18, 33\}, \{0, 4, 19, 29\}, \{0, 4, 22, 32\}, \{0, 4, 26, 35\}, \\
\{0, 5, 11, 16\}, \{0, 5, 12, 17\}, \{0, 5, 13, 38\}, \{0, 5, 14, 39\}, \{0, 5, 18, 34\}, \{0, 5, 20, 25\}, \\
\{0, 5, 22, 28\}, \{0, 5, 23, 29\}, \{0, 5, 24, 30\}, \{0, 6, 13, 32\}, \{0, 6, 14, 26\}, \{0, 6, 15, 38\}, \\
\{0, 6, 16, 37\}, \{0, 6, 17, 33\}, \{0, 6, 19, 31\}, \{0, 6, 20, 36\}, \{0, 6, 21, 40\}, \{0, 6, 22, 34\}, \\
\{0, 6, 27, 39\}, \{0, 7, 15, 35\}, \{0, 7, 16, 23\}, \{0, 7, 17, 29\}, \{0, 7, 19, 39\}, \{0, 7, 22, 30\}, \\
\{0, 7, 24, 32\}, \{0, 7, 25, 37\}, \{0, 8, 17, 38\}, \{0, 8, 18, 26\}, \{0, 8, 19, 36\}, \{0, 9, 20, 33\}, \\
\{0, 9, 23, 36\}, \{0, 10, 21, 36\}, \{0, 10, 23, 33\}.