Further results on optimal optical orthogonal codes with weight 4

Yanxun Chang\textsuperscript{a}, Jianxing Yin\textsuperscript{b}

\textsuperscript{a}Department of Mathematics, Northern Jiaotong University, Beijing 100044, People’s Republic of China
\textsuperscript{b}Department of Mathematics, Suzhou University, Suzhou 215006, People’s Republic of China

Received 25 August 2002; received in revised form 6 December 2002; accepted 9 June 2003

Dedicated to Professor Lie Zhu on the occasion of his 60th birthday

Abstract

By a \((v,k,1)\)-OOC we mean an optical orthogonal code of length \(v\), weight \(k\), and correlation constraints 1. In this paper, we take advantage of the equivalence between such codes and cyclic packings of pairs to make further investigation regarding the existence of a \((v,4,1)\)-OOC. It is proved that an optimal \((v,4,1)\)-OOC exists whenever \(v = 3^u u\) with \(u\) a product of primes congruent to 1 modulo 4, or \(v = 2^u u\) with \(u\) a product of primes congruent to 1 modulo 6, where \(n\) is an arbitrary positive integer and \(n \neq 2\) in the case \(v = 2^u u\). A strong indication about the existence of an optimal \((2^u 4,1,1)\)-OOC with \(u\) a product of primes congruent to 1 modulo 6 has been given in (M. Buratti, Des. Codes Cryptogr. 26 (2002) 111–125). The results in this paper are obtained mainly by means of a great deal of direct constructions, including using Weil’s theorem with more than one independent variations.

\(\copyright\) 2003 Elsevier B.V. All rights reserved.

Keywords: Cyclic packings; Optical orthogonal codes; Optimal; Constructions

1. Introduction

Let \(v, k, \lambda_a\) and \(\lambda_c\) be positive integers. A \((0,1)\) sequence of length \(v\) and weight \(k\) is a sequence with exactly \(k\) 1’s and \(v - k\) 0’s. A \((v,k,\lambda_a,\lambda_c)\) optical orthogonal code(OOC), or a \((v,k,\lambda_a,\lambda_c)\)-OOC, \(\mathcal{C}\), is a family of \((0,1)\) sequences (called
codewords) of length \( v \) and weight \( k \) satisfying the following two properties:

1. **The auto-correlation property:**
   \[
   \sum_{0 \leq i \leq v-1} x_i x_{i+i} \leq \lambda_a \quad \text{for any } x = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C} \text{ and any integer } i \neq 0 \pmod{v};
   \]

2. **The cross-correlation property:**
   \[
   \sum_{0 \leq i \leq v-1} x_i y_{i+i} \leq \lambda_c \quad \text{for any } x = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}, \ y = (y_0, y_1, \ldots, y_{v-1}) \in \mathcal{C}
   \]
   with \( x \neq y \), and any integer \( i \).

**Example 1.1.** Here is a \((27, 4, 1)\)-OOC with two codewords:

\[
\begin{align*}
110010000010000000000000000 \\
101000010000000100000000000
\end{align*}
\]

OOCs have many applications in a code division multiple access (CDMA) communication using a fiber optical channel. For related details, the interested reader may refer to [11, 18–22]. Research on OOCs has mainly concentrated on the case \( \lambda_a = \lambda_c = 1 \), for which the notation is abbreviated to \((v, k, 1)\)-OOC.

A simple counting shows that the size \(|\mathcal{C}|\) of a \((v, k, 1)\)-OOC \( \mathcal{C} \) is upper bounded by \([(v-1)/k(k-1)]\) (see, for example, [11, 14, 23]). A \((v, k, 1)\)-OOC with \([(v-1)/k(k-1)]\) codewords is said to be optimal. The advantage of using an optimal optical orthogonal code is that it enables the largest number of asynchronous users to transmit information efficiently and reliably in such a CDMA communication system. The \((27, 4, 1)\)-OOC in Example 1.1 is in fact optimal.

It was shown [11] that an optimal \((v, 3, 1)\)-OOC exists if and only if \( v \neq 6t + 2 \) with \( t \equiv 2 \) or \( 3 \pmod{4} \). For \( k \geq 4 \), much work has been done on the existence problem (see, for example, [2, 6–8, 10, 12, 14–16, 23, 24]). However, even for \( k = 4 \), the problem is still far from settled. The only complete congruence classes of \( v \) for which the existence of an optimal \((v, 4, 1)\)-OOC was solved are, to our best knowledge, \( v \equiv 0, 6, 18 \pmod{24} \) (see [8, 16]). The purpose of this paper is to make further investigation regarding the existence of an optimal \((v, 4, 1)\)-OOC, taking advantage of the equivalence between such codes and cyclic packings of pairs.

Following [23], we use the notation \( CP(k, 1; v) \) to denote a cyclic pair packing with order \( v \), block size \( k \) and index \( \lambda = 1 \), each of its block orbits containing \( v \) blocks. A convenient way of viewing such a packing is from a difference family perspective. A \( CP(k, 1; v) \) can be thought of as a family \( \mathcal{B} = \{B_1, B_2, \ldots, B_t\} \) of \( t \) \( k \)-subsets (called base blocks, or starter blocks) of \( \mathbb{Z}_v \), where \( B_i = \{b_{i1}, b_{i2}, \ldots, b_{ik}\} \), \( 1 \leq i \leq t \), such that the differences in \( \mathcal{B} \), \( \Delta(\mathcal{B}) = \{b_{ij} - b_{is} : 1 \leq i \leq t, j \neq s, 1 \leq j, s \leq k\} \), cover each non-zero residue of integers modulo \( v \) at most once. The difference leave of \( \mathcal{B} \), denoted by \( DL(\mathcal{B}) \), is defined to be the set of all non-zero integers in \( \mathbb{Z}_v \) which are not covered by the differences generated by \( \mathcal{B} \), i.e., \( \Delta(\mathcal{B}) \). For some value of \( v \), the differences arising from the base blocks of such a cyclic packing may cover each non-zero residue of integers modulo \( v \) exactly once, in which case the cyclic packing is known as a cyclic balanced incomplete block design with parameters \( v, k, \lambda = 1 \), denoted by \( CB(k, 1; v) \). A \( CP(k, 1; v) \) is termed \( g \)-regular if the subset \( \mathbb{Z}_v \setminus \Delta(\mathcal{B}) \) forms an additive
subgroup of $\mathbb{Z}_v$ having order $g$. It is obvious that $t \leq \lfloor (v-1)/k(k-1) \rfloor$ in a $\text{CP}(k, 1; v)$. When $t = \lfloor (v-1)/k(k-1) \rfloor$, the $\text{CP}(k, 1; v)$ is called optimal. The following result is presented in [23].

Lemma 1.2 (Yin [23, Theorem 2.1]). An optimal $(v, k, 1)$-OOC is equivalent to an optimal $\text{CP}(k, 1; v)$.

In view of Lemma 1.2, results on optimal or $g$-regular $\text{CP}(k, 1; v)$’s can be used directly to create optimal $(v, k, 1)$-OOCs. As a matter of fact, most of the known constructions for optimal $(v, k, 1)$-OOCs are indeed design theoretic in nature (see, for example, [6,7,9,14,16,23]).

In the remainder of this paper, we will show that an optimal $(v, 4, 1)$-OOC exists whenever $v = 3^nu$ with $u$ a product of primes congruent to 1 modulo 4, or $v = 2^nu$ with $u$ a product of primes congruent to 1 modulo 6, where $n$ is an arbitrary positive integer and $n \neq 2$ in the case $v = 2^nu$. To establish our results, we will employ both direct and recursive constructions.

It should be pointed out that a $g$-regular $(v, 4, 1)$-OOC is a special case of a relative difference family (it is in fact a $(v, g, 4, 1)$-RDF) and that it gives rise to a cyclic $(4, 1)$ group divisible design of type $g^{v^g}$. Also, in the case of $g = 1$, a $g$-regular $(v, 4, 1)$-OOC is an ordinary difference family and it generates a cyclic $(v, 4, 1)$ balanced incomplete block design (see [1,5]).

2. Direct constructions

In this section, we establish several new direct constructions, for optimal $\text{CP}(4, 1; v)$’s, or equivalently (by Lemma 1.2), optimal $(v, 4, 1)$-OOCs. For the application of Weil’s theorem, we will use a result proved by Buratti [6]. For an arbitrary prime $p \equiv 1 \pmod{n}$ and a primitive element $\omega \in \mathbb{Z}_p$, the notation $C^n_0$ will denote the multiplicative subgroup \( \{\omega^i : 0 \leq i \leq (p - 1)/n\} \) of the $n$th powers modulo $p$, while $C^n_j$ will denote the coset of $C^n_0$ in $\mathbb{Z}^*_p$ ($= C^1_0$) represented by $\omega^j$, i.e., $C^n_j = \omega^j \cdot C^n_0$. $C^2_0$, the set of quadratic residues modulo $p$, is usually denoted by $\mathbb{Z}_p^\square$, while $C^2_1$, the set of quadratic non-residues modulo $p$, is usually denoted by $\mathbb{Z}_p^\square$.

Lemma 2.1 (Buratti [6]). Let $p \equiv 1 \pmod{q}$ be a prime satisfying the inequality $p - (2q^3 - 3q^2 + 1)\sqrt{p} - 3q^2 > 0$. Then, for any triple $(j_1, j_2, j_3) \in \{0, 1, \ldots, q - 1\}^3$ and any given triple $(c_1, c_2, c_3)$ of pairwise distinct elements of $Z_p$, there exists an element $x \in Z_p$ such that $x + c_i \in C^q_{j_i}$ for each $i, i = 1, 2, 3$.

Now we describe our constructions.

Lemma 2.2. Let $p \equiv 1 \pmod{4}$ be a prime. Then a 27-regular $\text{CP}(4, 1; 27p)$ exists.

Proof. Let $p = 4m + 1$ and $\omega$ be a primitive element of $Z_p$. Then the desired 27-regular $\text{CP}(4, 1; 27p)$ can be constructed by taking the following 9$(p - 1)/4$ base blocks over
Lemma 2.3. Let \( p \equiv 7 (\text{mod } 12) \) be a prime. Then a 32-regular \( \text{CP}(4,1;32p) \) exists for \( p > 7 \).

**Proof.** Let \( \varepsilon \) be a cubic primitive root of unity (mod \( p \)). Take \( x \in Z_p \) such that \( \{ x - 1, x, x + 1 \} \subseteq Z_p \), which exists when \( p > 45 \) by Lemma 2.1. For \( p = 19, 31, 43 \), we may take \( x = 5, 8, 14 \), respectively. Consider the following subsets of \( Z_{32} \times Z_p \) being isomorphic to \( Z_{32p} \):

\[
\{(0,0),(0,\varepsilon),(0,\varepsilon^2),(16,0)\} \cdot (1,h),
\{(0,0),(10,\varepsilon),(1,-\varepsilon),(3,\varepsilon^2)\} \cdot (1,g),
\{(0,1+\varepsilon),(4,1),(14,0),(11,\varepsilon)\} \cdot (1,g),
\{(0,0),(8,\varepsilon),(12,-1),(17,-\varepsilon)\} \cdot (1,g),
\{(0,1),(6,x\varepsilon),(20,0),(5,\varepsilon)\} \cdot (1,g),
\{(0,1),(2,-\varepsilon),(26,x\varepsilon),(13,0)\} \cdot (1,g),
\]

where \( h \) runs over a complete system of representatives for the cosets of \( \langle -\varepsilon \rangle \) in \( Z_p^* \) and \( g \) runs over all elements of \( Z_p^* \).

Note that \( \varepsilon \in Z_p^*, -1 \in Z_p^* \) and \( \varepsilon^2 + \varepsilon + 1 = 0 \). It is appropriate to observe that the list of differences from the first initial base block may be written as \( \{0\} \times (\varepsilon - 1)(-\varepsilon) \cup \{16\} \times \langle -\varepsilon \rangle \), where \( \langle -\varepsilon \rangle \) is the group of 6th roots of unity mod \( p \). Also observe that the list of differences from the remaining initial base blocks may be written as \( \bigcup_{x \in Z_{32} \setminus \{0,16\}} \{x\} \times \{a_x, b_x\} \), where, for each \( x \), exactly one among \( a_x \) and \( b_x \) is a square. \( \square \)

**Remark 2.4.** Let \( p = 12n + 7 \). Using elementary number theory, one can find an explicit solution (or a constructive proof) of Lemma 2.3. For example, take \( x = 1/49 \), or \(-1/32\) depending on whether \( n \) is even or odd, respectively. It is readily checked that \( x - 1, x \) and \( x + 1 \) are three consecutive squares of \( Z_p \).
Lemma 2.5. Let \( p \equiv 7 \pmod{12} \) be a prime. If \( p \geq 223 \) and \( p \neq 271, 379 \), then there exists an ordered triple \((x, y, z) \in \mathbb{Z}_p^3 \) satisfying the following conditions:

1. \( \{x + 1, x - 1\} \subseteq C_5^6, x \in C_1^6; \)
2. \( y + 1 \in C_5^6, y \) and \(-(y + x)\) lie in difference cosets among \( C_0^6 \) and \( C_4^6; \)
3. \( z \in C_5^6, z - 1 \in C_2^6, z + x \in C_5^6. \)

Proof. By Lemma 2.1, an element \( x \) satisfying the first condition always exists in \( \mathbb{Z}_p \) for any prime \( p \equiv 7 \pmod{12} \) and \( p \geq 105841 \). Once the element \( x \in \mathbb{Z}_p \) has been determined, we can again apply Lemma 2.1 to obtain the required element \( y \), and then \( z \). For the remaining cases where \( p \equiv 7 \pmod{12} \), \( 223 \leq p < 105841 \) and \( p \neq 271, 379 \), a computer search shows that the desired triple \((x, y, z)\)'s all exist. For simplicity, we list our search results below only for \( p \leq 1000 \), where \( g \in \mathbb{Z}_p \) is a primitive element:

<table>
<thead>
<tr>
<th>((p, g, x, y, z))</th>
<th>((p, g, x, y, z))</th>
<th>((p, g, x, y, z))</th>
</tr>
</thead>
<tbody>
<tr>
<td>((223, 3, 21, 31, 19))</td>
<td>((283, 3, 187, 252, 23))</td>
<td>((307, 5, 22, 170, 60))</td>
</tr>
<tr>
<td>((331, 3, 41, 104, 203))</td>
<td>((367, 6, 70, 55, 195))</td>
<td>((439, 15, 173, 121, 40))</td>
</tr>
<tr>
<td>((463, 3, 295, 110, 30))</td>
<td>((487, 3, 47, 169, 278))</td>
<td>((499, 7, 86, 336, 120))</td>
</tr>
<tr>
<td>((523, 2, 198, 40, 118))</td>
<td>((547, 2, 430, 452, 51))</td>
<td>((571, 3, 297, 157, 220))</td>
</tr>
<tr>
<td>((607, 3, 431, 561, 91))</td>
<td>((619, 2, 11, 399, 177))</td>
<td>((631, 3, 274, 169, 17))</td>
</tr>
<tr>
<td>((643, 11, 165, 237, 88))</td>
<td>((691, 3, 12, 61, 449))</td>
<td>((727, 5, 77, 122, 174))</td>
</tr>
<tr>
<td>((739, 3, 118, 184, 96))</td>
<td>((751, 3, 313, 50, 77))</td>
<td>((787, 2, 13, 264, 76))</td>
</tr>
<tr>
<td>((811, 3, 326, 209, 172))</td>
<td>((823, 3, 260, 50, 110))</td>
<td>((859, 2, 83, 321, 25))</td>
</tr>
<tr>
<td>((883, 2, 104, 21, 16))</td>
<td>((907, 2, 102, 52, 41))</td>
<td>((919, 7, 497, 286, 46))</td>
</tr>
<tr>
<td>((967, 5, 47, 120, 276))</td>
<td>((991, 6, 147, 264, 31))</td>
<td>(\Box)</td>
</tr>
</tbody>
</table>

Lemma 2.6. Let \( p \equiv 7 \pmod{12} \) be a prime. If \( p \geq 223 \) and \( p \neq 271, 379 \), then a 16-regular CP(4, 1; 16p) exists.

Proof. Take an ordered triple \((x, y, z) \in \mathbb{Z}_p^3 \) satisfying conditions (1)–(3) of Lemma 2.5, and consider the following base blocks over \( \mathbb{Z}_{16} \times \mathbb{Z}_p \):

\[
\{(0,0), (2,1), (6,x), (5,x+1)\} \cdot (1,r),
\{(0,0), (2,x), (6,x^2), (5,x^2+x)\} \cdot (1,r),
\{(0,0), (2,x^2), (6,x^3), (5,x^3+x^2)\} \cdot (1,r),
\{(0,0), (2,-x), (10,x^2), (11,1)\} \cdot (1,r),
\{(0,0), (2,-x^2), (10,x^3), (11,x)\} \cdot (1,r),
\{(0,0), (2,-1), (6,-x), (3,y)\} \cdot (1,r),
\]
\[
\{(0, x), (0, x^2), (0, x^3), (7, 0)\} \cdot (1, r),
\]
\[
\{(0, z), (12, 0), (8, 1), (5, -x)\} \cdot (1, r),
\]
where \( r \) ranges over \( C_6^6 \).

It is enough to observe that the list of differences from the initial base blocks may be written as \( \bigcup_{x \in \mathbb{Z}_b} \{x\} \times S_x \) where, for each \( x \), \( S_x \) is a complete system of representatives for the cosets of \( C_0^6 \) in \( \mathbb{Z}_p^* \). \( \square \)

For the next construction, we need the concept of a skew starter, which we define now.

Let \((G, +)\) be an abelian group of order \( u > 1 \). A skew starter in \( G \) is a set of unordered pairs \( S = \{(x_i, y_i) : 1 \leq i \leq (u - 1)/2\} \) which satisfies the following three properties:

1. \( \{x_i : 1 \leq i \leq (u - 1)/2\} \cup \{y_i : 1 \leq i \leq (u - 1)/2\} = G \setminus \{0\}; \)
2. \( \{\pm(x_i - y_i) : 1 \leq i \leq (u - 1)/2\} = G \setminus \{0\}; \)
3. \( \{\pm(x_i + y_i) : 1 \leq i \leq (u - 1)/2\} = G \setminus \{0\}. \)

According to the definition, a skew starter in \( G \) can exist only if \( u \) is odd. Furthermore, if we write \( X = \{x_i : 1 \leq i \leq (u - 1)/2\} \) and \( Y = \{y_i : 1 \leq i \leq (u - 1)/2\}, \) then we may assume, without loss of generality, that \( X = -Y, \) and hence we have \( X \cup (-X) = Y \cup (-Y) = X \cup Y = G \setminus \{0\}. \)

Skew starters have been extensively studied. We summarize the existence results on skew starters over \( \mathbb{Z}_u \) in the following lemma.

**Lemma 2.7** (Chen et al. [10]). There exists a skew starter in \( \mathbb{Z}_u \) for each positive integer \( u \) such that \( \gcd(u, 150) = 1 \) or 25. There does not exist any skew starter in \( \mathbb{Z}_u \) if \( u \equiv 0 \pmod{3} \).

**Lemma 2.8.** Let \( p \equiv 7 \pmod{12} \) be a prime. Then a 64-regular \( \text{CP}(4, 1; 64p) \) exists for \( p > 7 \).

**Proof.** From Lemma 2.7, let \( S_p \) be a skew starter in \( \mathbb{Z}_p \). Then the desired 64-regular \( \text{CP}(4, 1; 64p) \) can be constructed by taking the following 16\((p - 1)/3\) base blocks based on \( \mathbb{Z}_{64} \times \mathbb{Z}_p \) being isomorphic to \( \mathbb{Z}_{64p} \). The first 4\((p - 1)\) base blocks are:

\[
\{(0, x), (0, y), (26, 0), (18, x + y)\},
\]
\[
\{(0, -x), (32, y), (52, x), (44, -y)\},
\]
\[
\{(0, \delta x), (4, -\delta x), (15, \delta y), (29, -\delta y)\},
\]
\[
\{(0, \delta x), (6, -\delta x), (28, \delta y), (37, -\delta y)\},
\]
\[
\{(0, \delta x), (7, -\delta x), (17, \delta y), (30, -\delta y)\},
\]
where \( \delta \in \{-1, +1\} \), and \( \{x, y\} \) runs over all pairs of the skew starter \( S_p \) in \( Z_p \). The remaining \( 4(p - 1)/3 \) base blocks are

\[
\{(0,1),(1,x),(2,x^2),(3,x^3)\} \cdot (1,r),
\{(0,x^2),(2,x^4),(5,x),(21,x^3)\} \cdot (1,r),
\{(0,0),(5,x^2),(21,1),(45,y)\} \cdot (1,r),
\{(0,x^5),(3,x^2),(19,x^4),(24,0)\} \cdot (1,r),
\]

where \( r \) ranges over \( C_0^3 \), \( x \) and \( y \) satisfy the properties that \( x \in C_1^3 \), \( x - 1 \in C_2^3 \), \( x + 1 \in C_0^3 \cup C_1^3 \), \( y \in C_1^3 \) and \( y - 1 \), \( y - x^2 \) are in different cosets among \( C_0^3 \) and \( C_1^3 \). By Lemma 2.1, an element \( x \) satisfying the first three conditions always exists in \( Z_p \) for any prime \( p \equiv 7 \pmod{12} \) and \( p \geq 838 \). Once the element \( x \in Z_p \) has been determined, we can again apply Lemma 2.1 to obtain the required element \( y \), when prime \( p \equiv 7 \pmod{12} \) and \( p \geq 838 \). For the remaining values of \( p \equiv 7 \pmod{12} \) and \( 7 < p < 838 \), the desired elements \( x \) and \( y \) are given in the following table, where \( g \in Z_p \) is a primitive element:

<table>
<thead>
<tr>
<th>( (p, g.x, y) )</th>
<th>( (p, g.x, y) )</th>
<th>( (p, g.x, y) )</th>
<th>( (p, g.x, y) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>(19, 2, 16, 17)</td>
<td>(31, 3, 6, 7)</td>
<td>(43, 3, 10, 6)</td>
<td>(67, 2, 13, 16)</td>
</tr>
<tr>
<td>(79, 3, 20, 2)</td>
<td>(103, 5, 7, 4)</td>
<td>(127, 3, 12, 3)</td>
<td>(139, 2, 19, 11)</td>
</tr>
<tr>
<td>(151, 6, 5, 2)</td>
<td>(163, 2, 12, 7)</td>
<td>(199, 3, 7, 2)</td>
<td>(211, 2, 7, 2)</td>
</tr>
<tr>
<td>(223, 3, 6, 42)</td>
<td>(271, 6, 6, 7)</td>
<td>(283, 3, 23, 24)</td>
<td>(307, 5, 15, 13)</td>
</tr>
<tr>
<td>(331, 3, 20, 17)</td>
<td>(367, 6, 13, 11)</td>
<td>(379, 2, 16, 10)</td>
<td>(439, 15, 30, 5)</td>
</tr>
<tr>
<td>(463, 3, 20, 3)</td>
<td>(487, 3, 10, 2)</td>
<td>(499, 7, 30, 14)</td>
<td>(523, 2, 5, 16)</td>
</tr>
<tr>
<td>(547, 2, 6, 7)</td>
<td>(571, 3, 3, 28)</td>
<td>(607, 3, 3, 38)</td>
<td>(619, 2, 5, 2)</td>
</tr>
<tr>
<td>(631, 3, 3, 4)</td>
<td>(643, 11, 22, 11)</td>
<td>(691, 3, 15, 6)</td>
<td>(727, 5, 14, 5)</td>
</tr>
<tr>
<td>(739, 3, 22, 15)</td>
<td>(751, 3, 3, 19)</td>
<td>(787, 2, 5, 16)</td>
<td>(811, 3, 6, 22)</td>
</tr>
<tr>
<td>(823, 3, 7, 3)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note that \( x(x + 1) \not\in C_0^3 \) which implies that \( x^2 + x \not\equiv -1 \pmod{p} \) as \( -1 \not\in C_0^3 \). Hence \( x^3 - 1 = (x - 1)(x^2 + x + 1) \not\equiv 0 \pmod{p} \). With this fact, it is enough to observe that the list of differences from the last 4 initial base blocks may be written as \( \bigcup_{x \in X} \{x\} \times S_t \), where \( X = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 16, \pm 19, \pm 21, \pm 24\} \) and each \( S_t \) is a complete system of representatives for the coset of \( C_0^3 \) in \( Z_p^* \). The other differences are covered in the first \( 4(p - 1) \) base blocks. This completes the proof. \( \square \)

3. Recursive constructions

Let \( (G, \cdot) \) be a finite group of order \( v \) and \( H \) a subgroup of order \( h \) in \( G \). An \( H \)-regular \( (v, k, \lambda) \) incomplete difference matrix over \( G \) is a \( k \times (v-h) \lambda \) matrix \( D=(d_{ij})_1^{i=k-1, j=\lambda(v-h)} \), with entries from \( G \), such that for any \( 0 \leq i < j \leq k-1 \),

\[
\sum_{i=0}^{j} d_{ij} = 0, \quad \text{for all } x \in G.
\]
the list
\[(d_{il} \cdot d_{jl}^{-1} : 1 \leq l \leq \lambda(v-h))\]
contains every element of \(G \setminus H\) exactly \(\lambda\) times. When \(G\) is an abelian group, typically additive notation is used, so that the differences \(d_{il} - d_{jl}\) are employed. In what follows, we assume that \(G = \mathbb{Z}_v\), and \(H\) is a subgroup of order \(h\) in \(\mathbb{Z}_v\). In this case, \(H = \{i \cdot v/h : 0 \leq i \leq h-1\}\). We usually denote an \(H\)-regular \((v;k;\lambda)\) incomplete difference matrix (IDM) over \(\mathbb{Z}_v\) by \(h\)-regular \((v;k;\lambda)\)-IDM if \(|H| = h\). An ordinary \((v,k,\lambda)\)-difference matrix is denoted by \((v,k,\lambda)\)-DM. Difference matrices have been investigated extensively, see, for example, [13] and the references therein. Here is one easy example.

**Lemma 3.1** (Colbourn and Colbourn [12]). Let \(v\) and \(k\) be positive integers such that \(\gcd(v, (k-1)!)=1\). Let \(d_{ij} \equiv ij \mod v\) for \(i = 0, 1, \ldots, k-1\) and \(j = 0, 1, \ldots, v-1\). Then \(D = (d_{ij})\) is a \((v,k,1)\)-DM over \(\mathbb{Z}_v\). In particular, if \(v\) is an odd prime number, then there exists a \((v,k,1)\)-DM over \(\mathbb{Z}_v\) for any integer \(k, 2 \leq k \leq v\).

Incomplete difference matrices over \(\mathbb{Z}_v\) have played an important role in the construction of \(g\)-regular \(C(4,1;\nu)\) (see [7,8]). We record the following two results for later use.

**Lemma 3.2** (Chang and Miao [7]). (1) There exists a \(2\)-regular \((2^n,4,1)\)-IDM over \(\mathbb{Z}_{2^n}\) for any positive integer \(n \geq 3\); (2) There exists a \((3^n,4,1)\)-DM over \(\mathbb{Z}_{3^n}\) for \(n = 3,4,5\).

**Lemma 3.3** (Chang and Miao [7]). Let \(v\) and \(m\) be two positive integers such that \(\gcd(m,v) = 1\). Suppose that there exist:

1. a \(g\)-regular \(C(k,1;\nu)\);
2. an \(h\)-regular \((m,k,1)\)-IDM over \(\mathbb{Z}_m\);
3. a \(gh\)-regular \(C(k,1;hv)\) (or a \(gh\)-regular \(C(k,1;gm)\), respectively).

Then there exists a \(gm\)-regular \(C(k,1;\nu m)\) (or an \(hv\)-regular \(C(k,1;\nu m)\), respectively).

The following known results are also useful to our recursion.

**Lemma 3.4.**

1. [4,9] There exists a \(1\)-regular \(C(4,1;p)\) for any prime \(p \equiv 1 \mod 12\);
2. [3] There exists a \(2\)-regular \(C(4,1;2p)\) for any prime \(p \equiv 1 \mod 6\);
3. [6] There exists a \(8\)-regular \(C(4,1;8p)\) for any prime \(p \equiv 1 \mod 6\);
4. [17] There exists a \(3\)-regular \(C(4,1;3p)\) for any prime \(p \equiv 1 \mod 4\);
5. [15] There exists a \(9\)-regular \(C(4,1;9p)\) for any prime \(p \equiv 1 \mod 4\) and \(p > 5\).
From Lemma 3.4, we have also

**Theorem 3.5.** There exists a $2^s$-regular CP$(4,1;2^sp)$ for any prime $p \equiv 1 \pmod{12}$ and $s = 4, 5, 6$.

**Proof.** By (1), (2) in Lemma 3.4 there are a 1-regular CP$(4,1;p)$ and a 2-regular CP$(4,1;2p)$ for prime $p \equiv 1 \pmod{12}$. Since there is a 2-regular $(2^s,4,1)$-IDM over $\mathbb{Z}_2$ from Lemma 3.2, applying Lemma 3.3 with $m = 2^s$ and $h = 2$ we get a $2^s$-regular CP$(4,1;2^sp)$.

4. Optimal or $g$-regular CP$(4,1;v)$’s for small order $v$

For convenience, we denote by $\mathcal{P}_m$ the set of integers which are products of primes congruent to 1 modulo $m$. In the present and next sections, we will establish the existence of an optimal CP$(4,1;3nu)$ for $u \in \mathcal{P}_4$ and an optimal CP$(4,1;2nu)$ for $u \in \mathcal{P}_6$. This section serves to construct several optimal or $g$-regular CP$(4,1;v)$’s with small order $v$.

**Lemma 4.1.** There exists an optimal CP$(4,1;v)$ for $v \in \{16,28,32,729\}$.

**Proof.** For $v = 16, 28, 32$, the base blocks of an optimal CP$(4,1;v)$ are listed below:

$v = 16$: $\{0,1,3,7\}$.
$v = 28$: $\{0,1,3,10\}$, $\{0,4,12,17\}$.
$v = 32$: $\{0,1,3,12\}$, $\{0,4,10,17\}$.

For $v = 729$, let $D = (d_{ij})$ be a $(27,4,1)$-DM over $\mathbb{Z}_{27}$ where $d_{ij} \in \mathbb{Z}_{27}$ for $0 \leq i \leq 3$ and $1 \leq j \leq 27$. Then the desired optimal CP$(4,1;729)$ can be constructed by taking the following 60 base blocks based on $\mathbb{Z}_{27}$. The first 54 base blocks are

$$\{27d_{0j}, 27d_{1j} + 2, 27d_{2j} + 7, 27d_{3j} + 15\},$$
$$\{27d_{0j}, 27d_{1j} + 1, 27d_{2j} + 4, 27d_{3j} + 10\},$$

where $j = 1, 2, \ldots, 27$, and the remaining 6 base blocks are

$$\{0,27,11,27 \times 2 + 11\},$$
$$\{0,27 \times 8,27 + 16,27 \times 4 + 16\},$$
$$\{0,27 \times 15,27 \times 2 + 16,27 \times 6 + 16\},$$
$$\{0,27 \times 9,27 \times 3 + 16,27 \times 16 + 16\},$$
$$\{0,27 \times 17,27 \times 4 + 11,27 \times 11 + 11\},$$
$$\{0,27 \times 5,27 \times 11,27 \times 18 + 11\}.$$

**Lemma 4.2.** There exist $g$-regular CP$(4,1;gu)$’s for $(g,u) = (9,9), (3,81), (27,9), (4,16), (1,49)$.
Proof. For \((g,u)=(9,9), (3,81), (27,9), (4,16),\) the desired \(g\)-regular \(CP(4,1;gu)\) can be found in [7]. The base blocks of 1-regular \(CP(4,1;49)\) is found in [1].

**Lemma 4.3** (Chang and Miao [7]). There exists a \(2^s\)-regular \(CP(4,1;2^{s+4})\) for any integer \(s \geq 3\).

Applying Lemma 4.3 repeatedly gives the following result.

**Lemma 4.4.** There exists a \(2^s\)-regular \(CP(4,1;2^{4n+s})\) for any integer \(n \geq 1\) and \(s = 3,4,5,6\).

The following three results are known.

**Lemma 4.5** (Yin [23, Theorem 2.6]). If \(1 \leq g \leq k(k-1)\), then a \(g\)-regular \(CP(k;1;v)\) is optimal.

**Lemma 4.6** (Yin [23, Construction 4.1]). Suppose that both a \(g\)-regular \(CP(k;1;v)\) and an optimal \(CP(k;1;g)\) exist. Then an optimal \(CP(k;1;v)\) also exists. Moreover, if the given \(CP(k;1;g)\) is \(r\)-regular, then so is the derived \(CP(k;1;v)\).

**Lemma 4.7** (Yin [23, Construction 4.2]). Suppose that both a \(g\)-regular \(CP(k;1;v)\) and a \((m;k;1)\)-DM over \(Z_m\) exist. Then so does a \(gm\)-regular \(CP(k;1;mv)\).

Now we apply Lemmas 4.5–4.7 to establish some more results.

**Lemma 4.8.** There exists a \(3\), or \(9\)-regular \(CP(4,1;9 \times 27^n)\) for any positive integer \(n \geq 1\).

Proof. Use induction on \(n\). The case \(n=1\) is settled in Lemma 4.2. Suppose that there is a \(3\), or \(9\)-regular \(CP(4,1;9 \times 27^n)\) for \(n \geq 1\). Since there is a \((27,4,1)\)-DM over \(Z_{27}\) from Lemma 3.2, by Lemma 4.7 we have a \(3 \times 27\)- or \(9 \times 27\)-regular \(CP(4,1;9 \times 27^{n+1})\). By Lemma 4.2 there are a \(9\)-regular \(CP(4,1;81)\) and a \(3\)-regular \(CP(4,1;243)\). By Lemma 4.6 there is a \(3\), or \(9\)-regular \(CP(4,1;9 \times 27^{n+1})\). The conclusion then follows. □

**Lemma 4.9.** There exists a \(27\)-regular \(CP(4,1;3^{2n+3})\) for any positive integer \(n \geq 1\).

Proof. Use induction on \(n\). The case \(n=1\) is settled in Lemma 4.2. Next we consider case \(n=2\) as follows. By Lemma 4.2 there exists a \(9\)-regular \(CP(4,1;81)\). Applying Lemma 4.7 with a \((27,4,1)\)-DM over \(Z_{27}\) from Lemma 3.2 gives a \(9 \times 27\)-regular \(CP(4,1;81 \times 27)\), i.e., a \(243\)-regular \(CP(4,1;3^{7})\). By Lemma 4.2 and Lemma 4.6 a \(27\)-regular \(CP(4,1;3^{7})\) exists.

Suppose that there is a \(27\)-regular \(CP(4,1;3^{2t+3})\) for \(1 \leq t \leq n\) where \(n \geq 2\). We will prove that a \(27\)-regular \(CP(4,1;3^{2(t+1)+3})\) exists. By the hypothesis there is a \(27\)-regular \(CP(4,1;3^{2(t-1)+3})\). By Lemma 3.2 there exists a \((81,4,1)\)-DM over \(Z_{81}\). Apply Lemma 4.7 again to get a \(27 \times 81\)-regular \(CP(4,1;3^{2(t-1)+3} \times 81)\), i.e., a \(3^{7}\)-regular
CP(4, 1; 3^{2(t+1)+3}). So, a 27-regular CP(4, 1; 3^{2(t+1)+3}) is produced by Lemma 4.6. This shows that a 27-regular CP(4, 1; 3^{2n+3}) exists for any integer n ≥ 1.

Lemma 4.10. There exists an optimal CP(4, 1; 3^n) for any positive integer n.

Proof. The cases n = 1, 2 are obvious. The case n = 3 is from Example 1.1. By Lemma 4.2 there exist a 9-regular CP(4, 1; 3^4) and a 3-regular CP(4, 1; 3^3). The cases n = 4, 5 then follow by Lemma 4.5. The case n = 6 is settled in Lemma 4.1.

Next we consider the case n ≥ 7. If n is odd, there exists a 27-regular CP(4, 1; 3^n) by Lemma 4.9. Since there is an optimal CP(4, 1; 27) in Example 1.1, we can get an optimal CP(4, 1; 3^n) for odd n ≥ 7 by Lemma 4.6. If n is even, then n ≥ 8. By Lemma 4.9 there exists a 27-regular CP(4, 1; 3^{n−3}) for even n ≥ 8. Applying Lemma 4.7 with a (27, 4, 1)-DM over Z_{27} gives a 27 × 27-regular CP(4, 1; 3^{n−3} × 27), i.e., a 729-regular CP(4, 1; 3^n), for even n ≥ 8. Since there is an optimal CP(4, 1; 729) from Lemma 4.1, we obtain an optimal CP(4, 1; 3^n) for even n ≥ 8 by Lemma 4.6. This completes the proof.

Lemma 4.11. There exists a 4-regular CP(4, 1; 64 · 7^{2s}) for any integer s ≥ 0.

Proof. The case s = 0 is settled by Lemma 4.2. By Lemma 4.2 there is a 1-regular CP(4, 1; 49). Since there is a (49, 4, 1)-DM over Z_{49} from Lemma 3.1, we apply Lemma 4.7 inductively with m = 49 to get 1-regular CP(4, 1; 72s) for s ≥ 1. Since there is a 2-regular CP(4, 1; 14) by Lemma 3.4, we then apply Lemma 4.7 iteratively with m = 7 to get a 2-regular CP(4, 1; 2 · 7^{2s}). By Lemma 3.2 there is a 2-regular (64, 4, 1)-IDM over Z_{64}. Applying Lemma 3.3 with m = 64 and h = 2 gives a 64-regular CP(4, 1; 64 · 7^{2s}). Since a 4-regular CP(4, 1; 64) exists by Lemma 4.2, we use Lemma 4.6 to get a 4-regular CP(4, 1; 64 · 7^{2s}).

Lemma 4.12. There exists an optimal CP(4, 1; 64 · 7^{a}) for any integer a ≥ 0.

Proof. The conclusion follows by Lemma 4.11 when a is even.

When a is odd, by Lemma 4.11 there is a 4-regular CP(4, 1; 64 · 7^{a−1}). Applying Lemma 4.7 with m = 7 gives a 28-regular CP(4, 1; 64 × 7^{a}). The conclusion follows immediately by Lemmas 4.1 and 4.6.

Lemma 4.13. There exists an optimal CP(4, 1; 9 · 5^{a}) for any integer a ≥ 1.

Proof. The result is shown in [15].

We have found a few more examples of g-regular CP(4, 1; v)’s with the aid of a computer.

Lemma 4.14. There exist g-regular CP(4, 1; gu)’s for (g, u) = (16, 7), (32, 7).
Proof. The base blocks of the desired $g$-regular $CP(4, 1; gu)$’s are listed below: 
\[(g, u) = (16, 7):\]
\[
\{0, 1, 3, 13\}, \{0, 4, 23, 59\}, \{0, 5, 32, 48\}, \{0, 6, 24, 46\},
\{0, 8, 34, 81\}, \{0, 9, 60, 101\}, \{0, 15, 45, 83\}, \{0, 17, 50, 75\}.
\]
\[(g, u) = (32, 7):\]
\[
\{0, 4, 15, 33\}, \{0, 16, 54, 102\}, \{0, 10, 166, 167\}, \{0, 5, 17, 39\},
\{0, 6, 82, 95\}, \{0, 2, 43, 52\}, \{0, 8, 87, 123\}, \{0, 19, 88, 149\},
\{0, 24, 64, 96\}, \{0, 27, 93, 144\}, \{0, 71, 74, 198\}, \{0, 59, 104, 151\},
\{0, 37, 81, 199\}, \{0, 31, 114, 134\}, \{0, 65, 111, 164\}, \{0, 23, 78, 108\}. \quad \square
\]

Lemma 4.15. There exist 16-regular $CP(4, 1; 16p)$’s for $p \in \{19, 31, 43, 67, 79, 103, 127, 139, 151, 163, 199, 211, 271, 379\}$.

Proof. Let $\varepsilon$ be a cubic primitive root of unity in $\mathbb{Z}_p$. Then the desired 16-regular $CP(4, 1; 16p)$ can be constructed by taking the following $4(p - 1)/3$ base blocks based on $\mathbb{Z}_{16} \times \mathbb{Z}_p$ being isomorphic to $\mathbb{Z}_{16p}$. The first $7(p - 1)/6$ base blocks are
\[
\{B \cdot (1, r) : B \in \mathcal{B}_p, r \in C_6^0\},
\]
where $C_6^0$ is in $\mathbb{Z}_p$ and $\mathcal{B}_p$ listed in the Appendix is a set of 7 initial base blocks whose list of differences is of the form $\bigcup_{x \in Z_{16} \setminus \{0, 8\}} \{x\} \times S_6$ where each $S_6$ is a complete system of representatives for the cosets of $C_6^0$ in $Z_p^6$. The remaining $(p - 1)/6$ base blocks are
\[
\{(0, 1), (0, \varepsilon), (0, \varepsilon^2), (8, 0)\} \cdot (1, h),
\]
where $h$ runs over a complete system of representatives for the cosets of $\langle -\varepsilon \rangle$ in $Z_p^6$. It is appropriate to observe that the list of differences from the last initial base block may be written as $(\{0\} \times (\varepsilon - 1)\langle -\varepsilon \rangle) \cup (\{8\} \times \langle -\varepsilon \rangle)$, being $\langle -\varepsilon \rangle$ the group of 6th roots of unity mod $p$. This completes the proof. \quad \square

Theorem 4.16. Given a prime $p \equiv 1 \pmod{6}$, there exists a $2^s$-regular $CP(4, 1; 2^s p)$ for $s = 3, 4, 5, 6$ but $(p, s) \neq (7, 6)$.

Proof. The conclusion follows by (3) of Lemmas 3.4, 2.6, 2.3, 2.8, 4.14 and 4.15 together with Theorem 3.5. \quad \square

5. Conclusions

Theorem 5.1. There exists an optimal $CP(4, 1; 2^n u)$ for any integer $n \geq 1$, $n \neq 2$ and $u \in \mathcal{P}_6$. 

Proof. When \( n = 1 \), let \( u = p_1^{n_1} p_2^{n_2} \cdots p_f^{n_f} \), where each \( p_i \equiv 1 \pmod{6} \) is a prime. Then applying Lemma 4.7 iteratively with (2) of Lemmas 3.4 and 3.1 gives a 2-regular \( CP(4, 1; 2u) \). The case \( n = 1 \) then follows by Lemma 4.5.

Next we consider the case \( n \geq 3 \). We can assume that \( n = 4t + s \) where \( t \geq 0 \) and \( s \in \{3, 4, 5, 6\} \). Let \( u = p_1^{n_1} p_2^{n_2} \cdots p_f^{n_f} \), where each \( p_i \equiv 1 \pmod{6} \) is a prime. By Lemma 4.4 there is a \( 2^s \)-regular \( CP(4, 1; 2^s) \). There is a \( (u, 4, 1) \)-DM over \( Z_u \) by Lemma 3.1. Applying Lemma 4.7 with \( m = u \) gives a \( 2^s \)-regular \( CP(4, 1; 2^s) \).

Case 1: \( s = 3, 4, 5, \) or \( s = 6 \) and \( \gcd(u, 7) = 1 \). By Theorem 4.16 there exists a \( 2^s \)-regular \( CP(4, 1; 2^s u_i) \) for \( 1 \leq i \leq f \). Then applying Lemma 4.7 iteratively with Lemma 3.1, we obtain a \( 2^s \)-regular \( CP(4, 1; 2^s u_i) \). Since there is a \( 2^s \)-regular \( CP(4, 1; 2^s u_i) \) as above mentioned, by Lemma 4.6 there is a \( 2^s \)-regular \( CP(4, 1; 2^s u_i) \). By Lemma 4.5 and Lemmas 4.1-4.2 an optimal \( CP(4, 1; 2^s) \) exists for \( s = 3, 4, 5, 6 \). Hence, an optimal \( CP(4, 1; 2^s u_i) \) exists by Lemma 4.6.

Case 2: \( s = 6 \) and \( 7 | u \). Let \( u = 7^a u' \) where \( \gcd(u', 7) = 1 \) and \( a \geq 1 \). By the proof of Case 1, there exists a \( 64 \)-regular \( CP(4, 1; 2^a u') \). Applying Lemma 4.7 with a \( (7^a, 4, 1) \)-DM over \( Z_{7^a} \), we get a \( 64 \times 7^a \)-regular \( CP(4, 1; 2^a u' \times 7^a) \), i.e., a \( 64 \times 7^a \)-regular \( CP(4, 1; 2^a u) \). By Lemma 4.12 and Lemma 4.6 there is an optimal \( CP(4, 1; 2^a u) \).

Theorem 5.2. There exists an optimal \( CP(4, 1; 3^s u) \) for any integer \( n \geq 1 \) and \( u \in \mathcal{P}_4 \).

Proof. For any integer \( n \geq 1 \), let \( n = 3t + s \) where \( t \geq 0 \) and \( s = 1, 2, 3 \). Let \( u = p_1^{n_1} p_2^{n_2} \cdots p_f^{n_f} \), where each \( p_i \equiv 1 \pmod{4} \) is a prime number.

Case 1: \( s = 1, 3 \), or \( 2 \) and \( \gcd(u, 5) = 1 \). Then applying Lemma 4.7 iteratively with (4), (5) of Lemmas 3.4, 2.2 and 3.1, we obtain a \( 3^s \)-regular \( CP(4, 1; 3^s u) \). By Lemma 4.7 inductively \( t \) times with a \( (27, 4, 1) \)-DM over \( Z_{27} \) from Lemma 3.2 there exists a \( 3^t \times 27^t \)-regular \( CP(4, 1; 3^t u \times 27^t) \), i.e., a \( 3^n \)-regular \( CP(4, 1; 3^n u) \). So, an optimal \( CP(4, 1; 3^n u) \) exists by Lemma 4.6 and Lemma 4.10.

Case 2: \( s = 2 \) and \( 5 | u \). Let \( u = 5^a u' \) where \( \gcd(u', 5) = 1 \) and \( a \geq 1 \). By the proof of Case 1, there exists a \( 3^s \)-regular \( CP(4, 1; 3^s u') \). Since \( n = 3t + 2 \), by Lemma 4.8 a 3-, or 9-regular \( CP(4, 1; 3^s u) \) exists. By Lemma 4.6 there exists a 3-, or 9-regular \( CP(4, 1; 3^s u) \). Applying Lemma 4.7 with a \( (5^a, 4, 1) \)-DM over \( Z_{5^a} \) we get a \( 3 \times 5^a \)-, or \( 9 \times 5^a \)-regular \( CP(4, 1; 3^s u' \times 5^a) \), i.e., a \( 3 \times 5^a \)-, or \( 9 \times 5^a \)-regular \( CP(4, 1; 3^s u) \). By the proof of Case 1 there exists a 3-regular \( CP(4, 1; 3 \times 5^a) \). By Lemma 4.13 an optimal \( CP(4, 1; 9 \times 5^a) \) exists. With those facts the conclusion then follows by Lemma 4.6.

In conjunction with Lemma 1.2, Theorems 5.1 and 5.2 can be rephrased as the following.

Theorem 5.3. There exists an optimal \( (2^n v, 4, 1) \)-OOC where \( n \geq 1 \), but \( n \neq 2 \) and \( v \) is a product of primes congruent to 1 modulo 6.

Theorem 5.4. There exists an optimal \( (3^n v, 4, 1) \)-OOC where \( n \geq 1 \) and \( v \) is a product of primes congruent to 1 modulo 4.
Note. If \( v \) is congruent to \( 2, 3, 4, 8, 9 \) (mod \( 12 \)), Theorems 5.3 and 5.4 then provide a partial solution for the existence of an optimal \((v, 4, 1)\)-OOC.

In the case of \( n = 2 \) of Theorem 5.3, a strong indication about the existence of an optimal \((4u, 4, 1)\)-OOC with \( u \) a product of primes congruent to \( 1 \) modulo \( 6 \) has been given in [6]. In particular, existence has been proved when any prime factor \( p \) of \( u \) satisfies the condition \( \gcd((p - 1)/6, 20!) \neq 1 \) (that is to say that \( (p - 1)/6 \) has at least one prime factor smaller than 20).

Acknowledgements

The authors wish to thank the anonymous referees for their careful reading and their useful comments. In particular, one referee suggests a constructive proof of Lemma 2.3 stated in Remark 2.4. The authors also would like to acknowledge the financial supports from TRAPOYT and NSFC grant No.10071002 (Y. Chang), and NSFC grant No.10071056 (J. Yin).

Appendix

\[
\begin{array}{c|c|c}
& B_{19}: & B_{31}: \\
\{(0, 0), (1, 1), (2, 3), (3, 2)\}, & \{(0, 0), (2, 4), (4, 1), (5, 5)\}, & \{(0, 0), (2, 3), (4, 1), (5, 6)\}, \\
\{(0, 0), (3, 4), (7, 1), (9, 9)\}, & \{(0, 0), (4, 2), (9, 1), (10, 11)\}, & \{(0, 0), (4, 5), (9, 1), (10, 16)\}, \\
\{(0, 0), (5, 1), (7, 16), (10, 5)\}, & \{(0, 0), (6, 10), (9, 15), (12, 11)\}, & \{(0, 0), (6, 1), (9, 6), (12, 4)\}, \\
\{(0, 0), (7, 2), (11, 6), (12, 4)\}. & & \{(0, 0), (7, 11), (11, 5), (12, 18)\}. \\
\end{array}
\]

\[
\begin{array}{c|c|c}
& B_{33}: & B_{57}: \\
\{(0, 0), (1, 1), (2, 3), (3, 8)\}, & \{(0, 0), (2, 9), (4, 6), (5, 15)\}, & \{(0, 0), (2, 6), (4, 2), (5, 35)\}, \\
\{(0, 0), (3, 1), (7, 2), (9, 3)\}, & \{(0, 0), (4, 3), (9, 29), (10, 12)\}, & \{(0, 0), (4, 6), (9, 11), (10, 17)\}, \\
\{(0, 0), (5, 1), (7, 3), (10, 6)\}, & \{(0, 0), (6, 7), (9, 14), (12, 28)\}, & \{(0, 0), (6, 4), (9, 57), (12, 21)\}, \\
\{(0, 0), (7, 1), (11, 3), (12, 9)\}. & & \{(0, 0), (7, 1), (11, 4), (12, 11)\}. \\
\end{array}
\]
\{(0, 0), (1, 1), (2, 3), (3, 2)\}, \{(0, 0), (2, 6), (4, 5), (5, 33)\},
\{(0, 0), (3, 1), (7, 2), (9, 4)\}, \{(0, 0), (4, 2), (9, 36), (10, 29)\},
\{(0, 0), (5, 1), (7, 5), (10, 3)\}, \{(0, 0), (6, 1), (9, 8), (12, 40)\},
\{(0, 0), (7, 1), (11, 4), (12, 10)\}.

\{(0, 0), (1, 1), (2, 3), (3, 2)\}, \{(0, 0), (2, 4), (4, 2), (5, 19)\},
\{(0, 0), (3, 1), (7, 2), (9, 4)\}, \{(0, 0), (4, 4), (9, 47), (10, 18)\},
\{(0, 0), (5, 1), (7, 6), (10, 4)\}, \{(0, 0), (6, 2), (9, 1), (12, 52)\},
\{(0, 0), (7, 1), (11, 4), (12, 16)\}.

\{(0, 0), (1, 1), (2, 4), (3, 13)\}, \{(0, 0), (2, 13), (4, 42), (5, 24)\},
\{(0, 0), (3, 1), (7, 2), (9, 7)\}, \{(0, 0), (4, 5), (9, 34), (10, 9)\},
\{(0, 0), (5, 1), (7, 10), (10, 6)\}, \{(0, 0), (6, 5), (9, 58), (12, 23)\},
\{(0, 0), (7, 3), (11, 6), (12, 21)\}.

\{(0, 0), (1, 1), (2, 3), (3, 2)\}, \{(0, 0), (2, 8), (4, 17), (5, 22)\},
\{(0, 0), (3, 1), (7, 2), (9, 4)\}, \{(0, 0), (4, 4), (9, 12), (10, 29)\},
\{(0, 0), (5, 1), (7, 5), (10, 3)\}, \{(0, 0), (6, 1), (9, 100), (12, 63)\},
\{(0, 0), (7, 1), (11, 3), (12, 12)\}.

\{(0, 0), (1, 1), (2, 3), (3, 2)\}, \{(0, 0), (2, 4), (4, 16), (5, 3)\},
\{(0, 0), (3, 1), (7, 2), (9, 4)\}, \{(0, 0), (4, 4), (9, 19), (10, 49)\},
\{(0, 0), (5, 1), (7, 7), (10, 3)\}, \{(0, 0), (6, 4), (9, 46), (12, 139)\},
\{(0, 0), (7, 1), (11, 4), (12, 11)\}.

\{(0, 0), (1, 1), (2, 3), (3, 2)\}, \{(0, 0), (2, 5), (4, 3), (5, 18)\},
\{(0, 0), (3, 1), (7, 2), (9, 4)\}, \{(0, 0), (4, 4), (9, 2), (10, 12)\},
\{(0, 0), (5, 1), (7, 5), (10, 3)\}, \{(0, 0), (6, 1), (9, 19), (12, 107)\},
\{(0, 0), (7, 1), (11, 3), (12, 6)\}.

\{(0, 0), (1, 1), (2, 3), (3, 2)\}, \{(0, 0), (2, 6), (4, 17), (5, 20)\},
\{(0, 0), (3, 1), (7, 2), (9, 4)\}, \{(0, 0), (4, 4), (9, 25), (10, 57)\},
\{(0, 0), (5, 1), (7, 5), (10, 3)\}, \{(0, 0), (6, 1), (9, 39), (12, 94)\},
\{(0, 0), (7, 3), (11, 1), (12, 22)\}. 
\[
\begin{align*}
\mathcal{B}_{211} : & \quad \{ (0,0), (1,1), (2,3), (3,2) \}, \quad \{ (0,0), (2,16), (4,12), (5,28) \}, \\
& \quad \{ (0,0), (3,1), (7,2), (9,6) \}, \quad \{ (0,0), (4,4), (9,33), (10,13) \}, \\
& \quad \{ (0,0), (5,1), (7,9), (10,3) \}, \quad \{ (0,0), (6,2), (9,71), (12,170) \}, \\
& \quad \{ (0,0), (7,1), (11,3), (12,7) \}. \\
\mathcal{B}_{271} : & \quad \{ (0,0), (1,1), (2,3), (3,2) \}, \quad \{ (0,0), (2,6), (4,2), (5,23) \}, \\
& \quad \{ (0,0), (3,1), (7,2), (9,4) \}, \quad \{ (0,0), (4,4), (9,2), (10,53) \}, \\
& \quad \{ (0,0), (5,1), (7,5), (10,3) \}, \quad \{ (0,0), (6,2), (9,1), (12,77) \}, \\
& \quad \{ (0,0), (7,1), (11,4), (12,18) \}. \\
\mathcal{B}_{379} : & \quad \{ (0,0), (1,1), (2,3), (3,2) \}, \quad \{ (0,0), (2,8), (4,27), (5,16) \}, \\
& \quad \{ (0,0), (3,1), (7,2), (9,4) \}, \quad \{ (0,0), (4,3), (9,23), (10,5) \}, \\
& \quad \{ (0,0), (5,1), (7,5), (10,3) \}, \quad \{ (0,0), (6,1), (9,72), (12,291) \}, \\
& \quad \{ (0,0), (7,4), (11,1), (12,19) \}.
\end{align*}
\]

References