UNIFIED COMBINATORIAL CONSTRUCTIONS OF OPTIMAL OPTICAL ORTHOGONAL CODES

CUILING FAN
School of Sciences
Nantong University
Nantong, 226007, P.R. China

KOJI MOMIHARA
Department of Mathematics, Faculty of Education
Kumamoto University
2-40-1 Kurokami, Kumamoto 860-8555, Japan

(Communicated by the associate editor name)

Abstract. We present unified constructions of optical orthogonal codes (OOCs) using other combinatorial objects such as cyclic linear codes and frequency hopping sequences. Some of obtained OOCs are optimal or asymptotically optimal with respect to the Johnson bound. Also, we are able to show the existence of new optimal frequency hopping sequences (FHSs) with respect to the Singleton bound from our observation on a relation between OOCs and FHSs. The last construction is based on residue rings of polynomials over finite fields, and which yields a new large class of asymptotically optimal \((q^{1}; k, k-2)\)-OOCs for any prime power \(q\) such that \(\gcd(q-1, k) = 1\). Some infinite families of optimal ones are included as a subclass.

1. Introduction. An optical orthogonal code is a kind of codes applied in code-division multiple-access (CDMA) systems in optical fiber networks. A \((v, k, \lambda_a, \lambda_c)\)-optical orthogonal code (OOC) is a family of binary sequences (codewords) of length \(v\) and constant Hamming weight \(k\) satisfying the following two conditions:

(i) (Auto-correlation property) For any codeword \(c = (c_0, c_1, \ldots, c_{v-1})\) and for any integer \(1 \leq t \leq n - 1\), it holds \(\sum_{i=0}^{v-1} c_i c_{i+t} \leq \lambda_a\),

(ii) (Cross-correlation property) For any two distinct codewords \(c, c'\) and for any integer \(0 \leq t \leq n - 1\), it holds \(\sum_{i=0}^{v-1} c_i c'_{i+t} \leq \lambda_c\),

where each subscript is reduced modulo \(v\). A \((v, k, \lambda_a, \lambda_c)\)-OOC with \((\lambda :=)\lambda_a = \lambda_c\) is denoted as \((v, k, \lambda)\)-OOC. An OOC with the maximum possible code size (denoted by \(M(v, k, \lambda_a, \lambda_c)\) or \(M(v, k, \lambda)\)) for fixed \(v, k, \lambda_a, \lambda_c\) is called maximal. In applications, maximal OOCs facilitate the largest possible number of asynchronous
users to transmit information efficiently and reliably. From the well known Johnson bound for constant weight codes, it follows that

$$M(v, k, \lambda) \leq (J(v, k, \lambda) :=) \left\lfloor \frac{v-1}{k-1} \left\lfloor \frac{v-2}{k-2} \cdots \left\lfloor \frac{v-\lambda}{k-\lambda} \right\rfloor \cdots \right\rfloor. \quad (1)$$

We say that an OOC with $J(v, k, \lambda)$ codewords is optimal. (An infinite family of maximal OOCs but not attain the Johnson bound was found in [4].)

As stated above, an application of OOCs is to optical CDMA communication systems where binary codewords with strong correlation properties are required (see [7, 10] for details). OOCs have been used for multimedia transmissions in networks using fiber-optics [18]. Moreover, OOCs have also been known as “cyclically permutable constant weight codes” in the construction of protocol sequences for multiuser collision channels without feedback [23]. We should remark that in a practical application to optical CDMA communications, a recent performance analysis by Mashhadi and Salehi [19] indicates that OOCs with $\lambda = 2, 3$ are more desirable than OOCs with $\lambda = 1$. However, it is quite difficult to construct optimal OOCs with $\lambda \geq 2$ and in fact, no optimal constructions appear in the literature for $\lambda > 2$ and $k > \lambda + 1$. Therefore, it is also of interest to consider a weaker problem to find infinite families of $(v, k, \lambda)$-OOCs $C$ satisfying

$$\lim_{v \to \infty} \frac{|C|}{J(v, k, \lambda)} = 1.$$ 

OOCs have been studied in their own right mathematically because of the equivalence between an OOC and a combinatorial configuration called a “strictly cyclic $t$-packing.” Assume that $K \subset \mathbb{N}$ and $v \geq k \geq t \geq 2$ are positive integers for any $k \in K$. A $t$-$(v, K)$ packing is a pair $(V, \mathcal{B})$, where $V$ is a $v$-set of points and $\mathcal{B}$ is a collection of subsets (called blocks) of $V$ satisfying all the block sizes are in $K$, such that every $t$-subset of $V$ occurs in at most one block of $\mathcal{B}$. For any block $B$ of a $t$-packing $(V, \mathcal{B})$ and a permutation $\sigma$ on $V$, define $B^{\sigma} = \{b^{\sigma} \mid b \in B\}$. If $B^{\sigma} \in \mathcal{B}$ for all $B \in \mathcal{B}$, then $\sigma$ is called an automorphism of the packing. The set of all such permutations forms a group under composition called the full automorphism group and any of its subgroups is called an automorphism group. In particular, a packing admitting a cyclic automorphism group is called cyclic. For a $t$-packing $(V, \mathcal{B})$ having $G$ as its automorphism group, the block orbit containing $B \in \mathcal{B}$ is defined to be the set $\{B^{\sigma} \mid \sigma \in G\}$ of distinct blocks. If $G$ is cyclic and the length of each block orbit is $v$, we say that the packing is strictly cyclic. When $K = \{k\}$, a $t$-$(v, \{k\})$ packing is often denoted as a $t$-$(v, k)$ packing.

In [14], Fuji-Hara and Miao showed that a strictly cyclic $t$-$(v, k)$ packing having maximum number of blocks for fixed $t, k, v$ is equivalent to a maximal $(v, k, t-1)$-OOC. In particular, there have been studied a lot of combinatorial constructions of optimal OOCs with $\lambda = 1$ in connection with cyclic difference families, see [9] and references therein for some recent progress. Furthermore, although only a few optimal or asymptotically optimal constructions of OOCs with $\lambda \geq 2$ had been known until quite recently, Alderson and Mellinger [1, 2, 3, 4, 5] made this situation changed and found many new classes of optimal or asymptotically optimal OOCs using some techniques in finite geometry in this 5 years. In Table 1, we list known optimal (maximal) or asymptotically optimal OOCs of general weight. (We avoid to list OOCs of small weight because of the large quantity.)

Our contribution of this paper is to unify some constructions of optimal or asymptotically optimal OOCs using other combinatorial objects such as “cyclic linear
Table 1. Optimal or asymptotically optimal OOCs with general weight. (In this table, \(p\) is a prime, \(q\) is a prime power, and \(\theta(k, q) = (q^{k+1} - 1)/(q - 1)\). The notations “o” and “a” mean respectively the OOCs to be optimal and asymptotically optimal, and “a/o” indicates the OOCs to be asymptotically optimal and includes an infinite family of optimal ones as a subclass.)

<table>
<thead>
<tr>
<th>No.</th>
<th>Parameters</th>
<th>Opt</th>
<th>Conditions</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>((q^k - 1)/(q - 1), q + 1, 1)</td>
<td>o</td>
<td>(k \geq 3)</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>((q^k - 1, q, 1))</td>
<td>o</td>
<td>(k \geq 2)</td>
<td>21</td>
</tr>
<tr>
<td>3</td>
<td>((p = k(k - 1)m + 1, k, 1))</td>
<td>o</td>
<td>sufficiently large (p)</td>
<td>27</td>
</tr>
<tr>
<td>4</td>
<td>(\left(\frac{q^2 - 1}{e}, \frac{q - (e - 1)}{e}, 1\right))</td>
<td>o</td>
<td>(e \mid q + 1, q \geq 3e^2 + e - 2)</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>(\left(\frac{q^2 - 1}{e}, \left\lceil \frac{q - (e - 1)/\sqrt{2}}{e}\right\rceil, 1\right))</td>
<td>o</td>
<td>(e \mid q^2 - 1, q \geq (4e^2 - e)/4) (\gcd(e, q + 1) = 1)</td>
<td>20</td>
</tr>
<tr>
<td>6</td>
<td>(\left(\frac{q^2 + 1}{e}, \left\lceil \frac{q + 1 - (e - 1)/\sqrt{2}}{e}\right\rceil, 1\right))</td>
<td>o</td>
<td>(e \mid q^2 + q + 1, q \geq 4(e^2 - 1)/2)</td>
<td>20</td>
</tr>
<tr>
<td>7</td>
<td>((q^k + 1, q + 1, 2))</td>
<td>o</td>
<td>(k \geq 2)</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>((q^k - 1, q + 1, 2))</td>
<td>o</td>
<td>(k \geq 2)</td>
<td>4, 11</td>
</tr>
<tr>
<td>9</td>
<td>(\theta(k, q), w + 1, w)</td>
<td>o</td>
<td>(\gcd(k + 1, i) = 1, 1 \leq i \leq w)</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>((pm, m, d))</td>
<td>a/o</td>
<td>(m \mid p - 1)</td>
<td>22</td>
</tr>
<tr>
<td>11</td>
<td>((q - 1)p, p - d, d)</td>
<td>a/o</td>
<td>(q = p^a)</td>
<td>22</td>
</tr>
<tr>
<td>12</td>
<td>((q^a - 1, q^a, q^{d-1}))</td>
<td>a/o</td>
<td>(a \geq d \geq 1)</td>
<td>24</td>
</tr>
<tr>
<td>13</td>
<td>((m(q + 1), m, 2d))</td>
<td>a</td>
<td>(m \mid q - 1, \gcd(m, q + 1) = 1)</td>
<td>22</td>
</tr>
<tr>
<td>14</td>
<td>(\theta(k, q), q + 1, d)</td>
<td>a</td>
<td>(k \geq d \geq 2, q \geq d)</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>(\left(\frac{q^2 - 1}{e}, \left\lceil \frac{q - 3(e - 1)/\sqrt{2}}{e}\right\rceil, 2\right))</td>
<td>a</td>
<td>none</td>
<td>20</td>
</tr>
<tr>
<td>16</td>
<td>(\theta(4, q^3), q - 1, 3)</td>
<td>a</td>
<td>none</td>
<td>2</td>
</tr>
<tr>
<td>17</td>
<td>(\theta(4, q), q, 3)</td>
<td>a</td>
<td>none</td>
<td>1</td>
</tr>
<tr>
<td>18</td>
<td>(\theta^2 - 1, q - 2, 3)</td>
<td>a</td>
<td>none</td>
<td>4</td>
</tr>
<tr>
<td>19</td>
<td>(\theta(2, q), q + 1, 4)</td>
<td>a</td>
<td>none</td>
<td>4</td>
</tr>
<tr>
<td>20</td>
<td>(\theta(5, q^5), q - 1, 4)</td>
<td>a</td>
<td>none</td>
<td>3</td>
</tr>
<tr>
<td>21</td>
<td>(\theta(d + 1, q^k), q - 1, d)</td>
<td>a</td>
<td>(d &gt; 1)</td>
<td>3</td>
</tr>
<tr>
<td>22</td>
<td>((q^k - 1, q - d + 3, q))</td>
<td>a</td>
<td>(k \geq d \geq 3, q \geq d)</td>
<td>2</td>
</tr>
<tr>
<td>23</td>
<td>(\theta(d - 2, q), q + 1, d)</td>
<td>a</td>
<td>(d \geq 4)</td>
<td>4</td>
</tr>
</tbody>
</table>

As codes and “frequency hopping sequences.” In Subsection 2.1, we give a construction of OOCs using cyclic linear codes, which yields as corollaries the 4th and 11th families of OOCs in Table 1. In Subsection 2.2, we see a close relation between special classes of OOCs and frequency hopping sequences (FHSs). (An FHS is also a kind of codes applied in spread spectrum communication systems and its formal definition will be given in Subsection 2.2.) Although new optimal OOCs are not found, we derive two new asymptotically optimal FHSs from the 10th and 13th families of OOCs in Table 1. Furthermore, we obtain a new large class of optimal ones by modifying the construction for one of the new families of FHSs. In Section 3, we present a general construction of OOCs from residue rings of polynomials over commutative rings and we consequently obtain an asymptotically optimal \((q - 1, k, k - 2)\)-OOCs with at least \(\left(\frac{q^k - 1}{k(q - 1)}\right) - \left(\frac{q^k - 1}{k - 2}\right)\)/(\((k - 1)(q - 1)\)) codewords for any prime.
power $q$ such that $\gcd(q - 1, k) = 1$, which includes some optimal families of OOCs in the cases where $k = 3$ and 4. In particular, the number of missing codewords the resultant OOC to be an optimal is at most $\binom{q - 1}{k - 2} / (q - 1)\left(\binom{q - 1}{k - 1}\right)$, that is, the number of base blocks of a “cyclic Steiner $(k - 2)$-design.” As far as the authors know, such good asymptotically optimal OOCs have not been ever known for general $\lambda$.

2. Unified construction of OOCs using other combinatorial configurations. In this section, we will unify known constructions of (optimal) OOCs using other combinatorial configurations such as cyclic linear codes and frequency hopping sequences. First, we provide a basic construction of packings.

**Lemma 2.1.** Let $G_1$ and $G_2$ be two (additively written) abelian groups of order $g_1$ and $g_2$, respectively. Let $S$ be a finite set of infinities and $\mathcal{F} = \{ f_i | i \in I \}$ a set of (not necessarily surjective) functions from $G_1$ to $G_2 \cup S$ satisfying the following conditions:

(i) For any $f \in \mathcal{F}$ and $(i, j) \in G_1 \times G_2$, there exists a unique $f' \in \mathcal{F}$ such that $f'(x + i) = y + j$ for all pairs $(x, y) \in G_1 \times G_2$ with $f(x) = y$;

(ii) The equation $f - g = 0$ has at most $\lambda$ roots in $G_1$ for any distinct $f, g \in \mathcal{F}$;

(iii) The number of elements in $f^{-1}(S)$ is at most $\ell$ for any $f \in \mathcal{F}$.

Then there exists a $(\lambda + 1)$-$(g_1g_2, g_1 - \ell)$-packing with $|I|$ blocks having $G_1 \times G_2$ as its automorphism group.

**Proof:** Let $B_f = \{(x, y) \in G_1 \times G_2 | f(x) = y\}$ for $f \in \mathcal{F}$ and set $\mathcal{B} = \{ B_f | f \in \mathcal{F} \}$. Then, $\mathcal{B}$ forms a $(\lambda + 1)$-$(g_1g_2, \{ |B_f| | f \in \mathcal{F} \})$-packing having $G_1 \times G_2$ as its automorphism group and $k_f \geq g_1 - \ell$ holds for all $f \in \mathcal{F}$. In fact, for any $B_f$ and any $(i, j) \in G_1 \times G_2$, it follows that $B_{f'} + (i, j) = B_f$, for some $f' \in \mathcal{F}$ by the condition (i). Furthermore, for any distinct $B_f, B_g \in \mathcal{F}$ it follows that $|B_f \cap B_g| = |\{(x, y) \in G_1 \times G_2 | f(x) = y; g(x) = y\}| \leq |\{x \in G_1 | f(x) = g(x)\}| \leq \lambda$.

We can obviously obtain the desired packing by removing suitable $k_f - (g_1 - \ell)$ elements from each block of size $k_f$ in $\mathcal{B}$. □

**Remark 1.** Assume that $G_1$ and $G_2$ are cyclic and $\gcd(|G_1|, |G_2|) = 1$ in Lemma 2.1. If we discard all the functions $h(x)$ for which there exists $(i, j) \in G_1 \times G_2 \setminus \{(0, 0)\}$ such that $h(x + i) = h(x) + j$ for all $x \in G_1$, and denote the set of remaining functions as $\mathcal{F}'$, then the set $\{ B_f | f \in \mathcal{F}' \}$ forms a strictly cyclic $\lambda + 1$-$(g_1g_2, \{ |B_f| | f \in \mathcal{F}' \})$ packing. By taking representatives from block orbits and removing suitable $k_f - (g_1 - \ell)$ elements from each block of size $k_f$, we obtain a $(g_1g_2, g_1 - \ell, \lambda)$-OOC.

2.1. OOCs from cyclic linear codes. In this subsection, we apply Lemma 2.1 to cyclic linear codes. A $q$-ary $[n, k, d]$ linear code is a linear subspace $C$ of $\mathbb{F}_q^n$ with dimension $k$ such that the minimum Hamming distance between all pairs of distinct vectors (called codewords) in $C$ is $d$. We say that a code is cyclic if cyclic shifts of any codeword of $C$ are again codewords. In the rest of this subsection, we will assume that the reader is familiar with the coding theory. Our main references are [6, 17, 26].

Here is a construction of cyclic packings from cyclic linear codes.
Theorem 2.2. Let $q$ be a prime power and $\gcd(n,q-1) = 1$. If there exists a cyclic $q$-ary $[n,k,d]$ linear code, then there exists a cyclic $(n-d+1)-(n(q-1),d)$-packing with $q^k - 1$ blocks.

Proof: It is sufficient that there is a set of functions satisfying the conditions of Lemma 2.1. Let $\omega$ be a primitive root of $\mathbb{F}_q^*$ and $C \subseteq \mathbb{F}_q^n$ be the assumed linear code whose coordinates are labeled by the elements in $\mathbb{Z}_n$. For each non-all-zero codeword $x = (x_0,x_1,\ldots,x_{n-1}) \in C$, we define a function $f_x$ from $\mathbb{Z}_n$ to $\mathbb{Z}_{q-1} \cup \{\infty\}$ by

$$f_x(s) = \begin{cases} l & \text{if } x_s = \omega^l, \\ \infty & \text{if } x_s = 0. \end{cases}$$

Let $\mathcal{F} = \{f_x \mid x \in C, x \neq o\}$, where $o$ denotes the all-zero codeword. Then, $\mathcal{F}$ satisfies the conditions of Lemma 2.1 as $S = \{\infty\}$ and $(G_1,G_2,\lambda,\ell) = (\mathbb{Z}_n,\mathbb{Z}_{q-1},n-d,n-d)$. (i) For any $f_x \in \mathcal{F}$ and $(i,j) \in \mathbb{Z}_n \times \mathbb{Z}_{q-1}$, the function $f_{\omega^i \cdot \sigma^j(x)} = f_x(s)$ satisfies $f_{\omega^j \cdot \sigma^i(x)}(s+i) = f_x(s) + j$ for all $s \in \mathbb{Z}_n$, where $\sigma$ is a cyclic right shift of length $n$; (ii) For any distinct $x,y \in C, |\{s \mid f_x(s) = f_y(s)\}| = n - d(x,y) \leq n-d$, where $d(\cdot, \cdot)$ is the Hamming distance; (iii) For any $x \in C$ with $x \neq o$, $|\{s \mid f_x(s) = \infty\}| = n - d(x,o) \leq n-d$. Thus, the proof is completed.

Remark 2. By Remark 1, if we discard all the codewords $x$ for which there exists $(i,j) \in \mathbb{Z}_n \times \mathbb{Z}_{q-1} \setminus \{(0,0)\}$ satisfying $\omega^j \cdot \sigma^i(x) = x$, the resulting packing yields an $(n(q-1),d,n-d)$-OOC by taking representatives from block orbits. Especially, when the cyclic linear code is minimum distance separable (MDS), i.e., meeting the Singleton bound $d \leq n-k+1$ (cf. [17]), we obtain an $(n(q-1),n-k+1,k-1)$-OOC.

Hereafter, we apply Theorem 2.2 to two known classes of cyclic linear codes to obtain optimal OOCs. First, we use a special case of “generalized Reed-Solomon codes.” Let $\alpha = (\alpha_1,\alpha_2,\ldots,\alpha_n)$ where $\alpha_i$ are distinct elements of $\mathbb{F}_q$, and let $v = (v_1,v_2,\ldots,v_n)$ where $v_i$ are nonzero elements of $\mathbb{F}_q$. Then, the generalized Reed-Solomon code $\text{GRS}_k(\alpha,v)$ is a $q$-ary $[n,k,d]$ linear code consisting of all vectors

$$(v_1f(\alpha_1),v_2f(\alpha_2),\ldots,v_nf(\alpha_n))$$

with $f(x) \in \mathbb{F}_q[x]$ satisfying $\deg(f) \leq k-1$ for a fixed $k \leq n$. In particular, when $v = (1,1,\ldots,1)$ and $\alpha = (0,1,\ldots,p-1)$ for the characteristic $p$ of $\mathbb{F}_q$, it is clear that the code is cyclic and MDS.

Corollary 1. Let $p$ be a prime and put $q = p^a$. Then there exists a $(p(q-1),p-k+1,k-1)$-OOC of size $M = p^{a-1}(q^{k-1}-1)/(q-1)$, which is asymptotically optimal (when $p \to \infty$ and $k$ is fixed). In particular, it is optimal provided that $a = 1$ and $k = 2$.

Proof: We apply Theorem 2.2 to $\text{GRS}_k(\alpha,v)$ as $v = (1,1,\ldots,1)$ and $\alpha = (0,1,\ldots,p-1)$. Then, by Theorem 2.2, we have a cyclic $k$-$(p(q-1),p-k+1)$ packing with $q^k - 1$ blocks. Furthermore, since only the codewords $x_s = (s,s,\ldots,s)$, $s \in \mathbb{F}_p$, satisfy $\omega^i \cdot \sigma^j(x) = x$ for some $(i,j) \in \mathbb{Z}_p \times \mathbb{Z}_{q-1} \setminus \{(0,0)\}$, by removing such codewords, we obtain the desired OOC. The optimality is directly checked by (1).

Next, we apply Theorem 2.2 to “irreducible cyclic codes.” Let $q$ be a prime power and let $f$ and $n$ be positive integers such that $q^k = fn+1$. Let $C = \{c(\alpha) \mid \alpha \in \mathbb{F}_q^n\}$
be the set of vectors
\[ c(\alpha) := (\text{Tr}_{q^k/q}(\alpha), \text{Tr}_{q^k/q}(\alpha \gamma^{f_1}), \text{Tr}_{q^k/q}(\alpha \gamma^{f_2}), \ldots, \text{Tr}_{q^k/q}(\alpha \gamma^{-(n-1)f})), \]
where \( \text{Tr}_{q^k/q} \) denotes the relative trace from \( \mathbb{F}_{q^k} \) to \( \mathbb{F}_q \) and \( \gamma \) is a primitive root of \( \mathbb{F}_{q^k} \). It is known that \( C \) forms a cyclic \( q \)-ary \([n,k,d]\) linear code, called an irreducible cyclic code, where its weight distribution is computed in terms of “Gauss sums” \([6]\) as follows.

The canonical additive character \( \psi \) of \( \mathbb{F}_{q^k} \) is defined by \( \psi : \mathbb{F}_{q^k} \to \mathbb{C}^* \) with \( \psi(x) = \zeta_p^{\text{Tr}_{q^k/q}(x)} \), where \( \zeta_p = \exp(\frac{2\pi i}{p}) \). For a multiplicative character \( \chi \) of \( \mathbb{F}_{q^k} \), we define the Gauss sum
\[ G_{q^k}(\chi) = \sum_{x \in \mathbb{F}_{q^k}} \chi(x) \psi(x). \]
Let \( \chi_f \) denote a multiplicative character of order \( f \) of \( \mathbb{F}_{q^k} \). As a natural generalization of Theorem 11.7.2 of \([6]\), the weight distribution of an irreducible cyclic code is computed as
\[
\begin{align*}
\omega(c(\alpha)) &= n - |\{i | \text{Tr}_{q^k/q}(\alpha \gamma^{f_i}) = 0; 0 \leq i \leq n - 1\}| \\
&= n - \frac{1}{q} \sum_{x \in \alpha(\gamma_f)} \sum_{y \in \mathbb{F}_q} \psi(y) \\
&= n - \frac{n}{q} - \frac{1}{q} \sum_{x \in \alpha(\gamma_f)} \sum_{y \in \mathbb{F}_q} \psi(xy) \\
&= n - \frac{n}{q} - \frac{1}{q^f} \sum_{x \in \mathbb{F}_{q^k}} \sum_{y \in \mathbb{F}_q} \chi_f^{-\ell}(\alpha) \chi_{\psi}^f(x) \psi(xy) \\
&= n - \frac{n}{q} + \frac{1}{q f} \sum_{\alpha \in \mathbb{F}_{q^k}} \sum_{y \in \mathbb{F}_q} \chi_f^{-\ell}(\alpha) G_{q^k}(\chi_{\psi}^f) \left( \sum_{y \in \mathbb{F}_q} \chi_f^{-\ell}(y) \right) \\
&= \frac{(q-1)q^k}{qf} - \frac{q-1}{q f} \sum_{\ell=1}^{c} \chi_f^{-\ell}(\alpha) G_{q^k}(\chi_{\psi}^f), \quad (2)
\end{align*}
\]
where \( e = \gcd(f, (q^k - 1)/(q - 1)) \), since the restriction of \( \chi_f \) to \( \mathbb{F}_q \) is of order \( f/e \).

**Corollary 2.** Let \( q \) be a prime power and \( k \) any positive integer. Let \( f \) be a divisor of \( q^k - 1 \) satisfying \( q - 1 \mid f \), say \( f = (q - 1)s \), and put \( n = (q^k - 1)/f \). Then, if \( \gcd(n,q-1) = 1 \), there exists an \( (n(q-1),d,n-d) \)-OOC with \( s \) codewords, where
\[
d = \frac{(q-1)q^k}{qf} - \frac{q-1}{q f} \max \left\{ \sum_{\ell=1}^{c} \chi_f^{-\ell}(\alpha) G_{q^k}(\chi_{\psi}^f) : \alpha \in \mathbb{F}_{q^k} \right\}.
\]
In particular, when \( k = 2 \), we obtain a \((q^2-1)/s, (q-s+1)/s, 1)\)-OOC with \( s \) codewords, which is optimal provided that \( q \geq 3s^2 + s - 2 \).

**Proof:** Note that \( e = \gcd(f, (q^k - 1)/(q - 1)) \) is \( s \) by the assumption that \( \gcd(n,q-1) = 1 \). Since only the all-zero codeword satisfies \( \omega_j \cdot \sigma^j(x) = x \) for some \((i,j) \in \mathbb{Z}_n \times \mathbb{Z}_{q-1} \setminus \{(0,0)\}\) for such an irreducible cyclic code, by Theorem 2.2 and the weight distribution (2), we obtain an \((n(q-1),d,n-d)\)-OOC with \( \frac{q^k-1}{n(q-1)} = s \)
codewords. In particular, when $k = 2$, by using $|G_{q^f}(x_s^f)| = q^{k/2}$ (cf. [16, P.193]), we have

$$d \geq \left(\frac{q-1}{q^f}\right)^2 - \frac{q-1}{q^f} \cdot (s-1)q = \frac{q+1-s}{s},$$

i.e., $n - d \leq 1$. The optimality is directly checked by (1).

In general, the explicit evaluation of Gauss sums is a very difficult problem. There are only a few cases where the Gauss sums have been completely evaluated. The authors refer the readers to [6] for the general theory and known evaluations of Gauss sums. Although it is possible to compute the exact value of $d$ of Corollary 2 using such known evaluations of Gauss sums, we are not able to obtain further optimal OOCs unfortunately.

Note that the OOCs of Corollaries 1 and 2 are not new, which are respectively found in [22, Theorem 2] and [20, Remark 3.3 (i)] (the 11th and 4th families of Table 1). However, we could unify such two different optimal classes in terms of cyclic linear codes.

### 2.2. OOCs and frequency hopping sequences

In this subsection, we observe a nice relation between an OOC and a combinatorial configuration, called “frequency hopping sequences”. A frequency hopping (FH) sequence is also a kind of codes applied in spread spectrum communication systems such as FH-CDMA systems. Here is the definition of FH sequences: Let $A = \{a_0, a_1, \ldots, a_{v-1}\}$ be a set of symbols (e.g., available frequencies in a communication system such as FH-CDMA).

A frequency hopping (FH) sequence of length $n$ is a $n$-dimensional vector $x = (x_0, x_1, \ldots, x_{n-1})$ with $x_i \in A$ for $0 \leq i \leq n-1$. Let $x$ and $y$ be two FH sequences. The Hamming correlation between $x$ and $y$ is

$$H_{x,y}(\tau) = \sum_{j=0}^{n-1} h[x_j, y_{j+\tau}]$$

for $0 \leq \tau \leq n-1$, where $h[x, y] = 1$ if $x = y$, and 0 otherwise, and all indices are reduced modulo $n$. Let $S$ be a set of FH sequences of length $n$. For $x, y \in S$, let

$$H(x) = \max_{0 \leq \tau < n} \{H_{x,x}(\tau)\},$$

$$H(x, y) = \max_{0 \leq \tau < n} \{H_{x,y}(\tau)\},$$

$$M(S) = \max \left\{ \max_{x \in S} H(x), \max_{x,y \in S, x \neq y} H(x, y) \right\}.$$

We denote by $\text{FHS}(n, N, \lambda; v)$ a set $S$ of $N$ FH sequences with length $n$, $|A| = v$, and $M(S) = \lambda$. Several bounds on the parameters $n, N, \lambda, v$ of FHSs have been found in [12, 15, 25]. In particular, the following bound was obtained in [12] from the Singleton bound on error correcting codes.

**Lemma 2.3.** Let $S$ be an $\text{FHS}(n, N, \lambda; v)$, where $n > \lambda$ and $v > 1$. Then

$$N \leq (S(n, \lambda; v) := \left\lfloor \frac{v^{\lambda+1}}{n} \right\rfloor. \quad (3)$$

In this paper, we say that $S$ is optimal if the Singleton bound is met. If $\lim_{n \to \infty} \frac{N}{\text{FHS}(n, N, \lambda; v)} = 1$, we call that $S$ is asymptotically optimal. There have been known a lot of combinatorial constructions of optimal or asymptotically optimal FH sequences. For example, we refer to [12, 13, 25, 28] and the references therein for recent progress on constructions of FHSs.
The following theorem shows that special classes of OOCs and FHSs are equivalent.

**Theorem 2.4.** Assume that $\gcd(n,v) = 1$ and $\lambda < n$. The following are equivalent:

(A) The existence of an FHS $(n,N,\lambda;v)$ $S$ satisfying that $x + \ell \cdot 1$ for $\ell \in \mathbb{Z}_v$ and $x \in S$ are distinct FH sequences in $S$, where we assume that $A = \mathbb{Z}_v$;

(B) The existence of an $(nv,n,\lambda)$-OOC $B$ with $N/v$ codewords (over $\mathbb{Z}_n \times \mathbb{Z}_v$) satisfying

$$\Delta B \cap \{(0) \times \mathbb{Z}_v\} = \emptyset$$

where $\Delta B$ is the list of differences of $B$, i.e., $\Delta B = \{a-b \mid a,b \in B, a \neq b\}$. In particular, the FHS is asymptotically optimal if and only if the OOC is asymptotically optimal (as $n \to \infty$). Here, the notation 1 indicates the all one vector of length $n$.

**Proof:** (A)→(B): It is sufficient that there is a set of functions satisfying the conditions of Lemma 2.1. Let $S' = \{\sigma^i(x) : x \in S, i \in \mathbb{Z}_n\}$, where $\sigma$ is a cyclic right shift of length $n$. For each sequence $x = (x_0,x_1,\ldots,x_{n-1}) \in S'$, we define a function $f_x$ from $\mathbb{Z}_n$ to $\mathbb{Z}_v$ by $f_x(s) = x_s$ for all $s \in \mathbb{Z}_n$ and set $F = \{f_x : x \in S'\}$.

Then, we show that $F$ satisfies the conditions of Lemma 2.1 as $S = \emptyset$ and

$$(G_1,G_2,\lambda,\ell) = (\mathbb{Z}_n,\mathbb{Z}_v,\lambda,0).$$

(i) For any $f_x \in F$ and $(i,j) \in \mathbb{Z}_n \times \mathbb{Z}_v$, the function $f_{j \cdot 1 + \sigma^i(x)} \in F$ satisfies $f_{j \cdot 1 + \sigma^i(x)}(s+i) = f_x(s+j)$ for all $s \in \mathbb{Z}_n$; (ii) For any distinct $x,y \in S'$, there are $x = \sigma^i(x_0)$, $y = \sigma^j(y_0)$ for some $x_0,y_0 \in S$ and $i,j \in \mathbb{Z}_n$. Then $\{|s : f_x(s) = f_y(s)| = H_{x_0,y_0}(i-j) \leq \lambda\}$; (iii) The number of elements in $f^{-1}(S)$ is obviously 0. Finally, we see that $\sigma^i(x + j \cdot 1) \neq x$ for any $(i,j) \neq (0,0)$ and any $x \in S$, which shows that the resultant packing forms an OOC by Remark 1. If $j = 0$, $H_{x,x}(i) \leq \lambda < n$ for all $i \neq 0$ implies that $\sigma^i(x) \neq x$. If $j \neq 0$, by our assumption that $x + j \cdot 1 \in S$ with $x + j \cdot 1 \neq x$ and by $H_{x,x+j}(i) \leq \lambda < n$ for all $i$, we have $\sigma^i(x + j \cdot 1) \neq x$.

(B)→(A): Let $B = \{B_i : 1 \leq i \leq \frac{N}{v}\}$ be the assumed OOC. Since $\Delta B \cap \{(0) \times \mathbb{Z}_v\} = \emptyset$, we can assume that $B_i = \{(s,x_i,s) : 0 \leq s \leq n-1\}$. Let $x_i = (x_{i,s})_s$ for $1 \leq i \leq \frac{N}{v}$ and $x_i + \ell \cdot 1$ for $\ell \in \mathbb{Z}_v$. Then $S = \{x_i + \ell \cdot 1 : 1 \leq i \leq \frac{N}{v}, \ell \in \mathbb{Z}_v\}$ is the desired FHS$(n,N,\lambda;v)$. In fact,

$$H_{x_i,x_i}(\ell) = |B_i \cap (B_j + (-\ell,\ell))| \leq \lambda$$

for any $\delta(i,j,\ell) = t \leq n$, where $\delta(i,j,\ell) = 1$ if $i = j$, $\ell = 0$, and 0 otherwise.

Finally, we observe that

$$\lim_{n \to \infty} \frac{N}{S(n,\lambda;v)} = \lim_{n \to \infty} \frac{v \cdot J(nv,n,\lambda)}{\frac{v^{\frac{n+1}{n}}}{n}} \cdot \frac{N/v}{J(nv,n,\lambda)} = 1,$$

i.e., the FHS of (A) is asymptotically optimal if the OOC of (B) is asymptotically optimal. The converse is also true. \qed

Unfortunately, we can not obtain new OOCs, but instead we have a chance to apply Theorem 2.4 in order to obtain new families of FHSs. To utilize Theorem 2.4, we need the following results given in [22].
Proposition 1. (1) ([22, Theorem 1]) Let \( p \) be a prime, \( m \) a divisor of \( p - 1 \), and \( t \) an integer such that \( 1 \leq t \leq m - 1 \). Then, there exists an asymptotically optimal (as \( m \to \infty \)) \((pm,m,t)-OOC\) of
\[
(M_1 :=) \frac{1}{pm} \sum_{d \mid p-1} (p^{\lceil(t+1)/d\rceil} - 1)\mu(d) \quad (4)
\]
codewords, where \( \mu \) is the Moebius function defined by
\[
\mu(d) = \begin{cases} 
1 & \text{if } d = 1, \\
(-1)^s & \text{if } d \text{ is the product of } s \text{ distinct prime numbers}, \\
0 & \text{if } d \text{ contains a repeated prime factor.}
\end{cases}
\]

(2) ([22, Theorem 3], [8, Proposition 3.3]) Let \( q = p^s \), where \( s \geq 1 \), \( p \) a prime, \( m \) a divisor of \( q - 1 \) such that \( \gcd(m,q+1) = 1 \), and \( t \) an integer such that \( 1 \leq t < m/2 \). Then there exists an asymptotically optimal (as \( m \to \infty \)) \((q+1)m,m,2t)-OOC\) of
\[
(M_2 :=) \frac{1}{(q+1)m} \sum_{d \mid q-1} (q^{\lceil t/d \rceil} - q)\mu(d) \quad (5)
\]
codewords.

Each of the OOCs \( B \) above satisfies \( \Delta B \cap (\{0\} \times \mathbb{Z}_v) = \emptyset \) for any \( B \in \mathcal{B} \), where \( v = p \) or \( q+1 \) respectively.

Now, by applying Theorem 2.4 to the OOCs of Proposition 1, we obtain the following two families of FHSs immediately.

Corollary 3. (1) Let \( p \) be a prime, \( m \) a divisor of \( p - 1 \), and \( t \) an integer such that \( 1 \leq t \leq m - 1 \). Then there exists an asymptotically optimal FHS\((m,pm_1,t;p)\), where \( M_1 \) is defined by (4).

(2) Let \( q = p^s \), where \( s \geq 1 \), \( p \) a prime, \( m \) a divisor of \( q - 1 \) such that \( \gcd(m,q+1) = 1 \), and \( t \) an integer such that \( 1 \leq t < m/2 \). Then there exists an asymptotically optimal FHS\((m,(q+1)m_2,2t;q+1)\), where \( M_2 \) is defined by (5).

In the case where \( m = p - 1 \) and \( t = 1 \) in Corollary 3 (1), since \( M_1 = 1 \), the missing number of FH sequences to be optimal is \( S(p - 1,1;p) - p = 1 \), i.e., the obtained FHS is almost optimal. On the other hand, in [12, 13], it was shown that there exists an optimal FHS\((q - 1,(q^{t+1} - 1)/(q - 1),t;q)\) for a prime power \( q \) under a certain condition. Hence, this FHS has one more sequence than our FHS of Corollary 3 when \( q \) is a prime and \( t = 1 \). However, our situation is not completely included in that of [12, 13]. We close this section giving a common improvement of our and their results, which gives a new large optimal class of FHSs. A proof will be given in the Appendix.

Theorem 2.5. Let \( q \) be a prime power, \( m \) a divisor of \( q - 1 \), and \( t \) an integer such that \( 1 \leq t \leq m - 1 \). Then there exists an FHS\((m,M,t;q)\), where
\[
M = \frac{1}{m} \sum_{d \mid m} (q^{\lceil(t+1)/d\rceil} - 1)\mu(d).
\]

In particular, the resultant FHS is optimal provided that \( m \) is a prime.
3. Construction of OOCs using residue rings of polynomials. In this section, we give a new construction of (asymptotically) optimal OOCs using residue rings of polynomials.

Let \( R \) be a commutative ring with an additive group \( G \) and a unit group \( H \) having unity \( 1 := 1_R \). For a positive integer \( t \), consider the residue ring \( R[x]/(x^t) \) of polynomials. We denote the unit group of \( R[x]/(x^t) \) by \((R[x]/(x^t))^*\), which consists of all polynomials in \( R[x]/(x^t) \) with constants of \( H \). Since \( H \) is naturally embedded in \((R[x]/(x^t))^*\) as a subgroup, we are able to consider the quotient group \((R[x]/(x^t))^*/H\).

**Theorem 3.1.** Let \( k \geq t + 1 \) and let \( \mathcal{F}_k \) be the set of all \( k \)-subsets of \( H \). Define the map \( \tau \) from \( \mathcal{F}_k \) to \((R[x]/(x^t))^*/H\) by

\[
\tau : B \in \mathcal{F}_k \mapsto \prod_{a \in B} (x - a) \in (R[x]/(x^t))^*/H,
\]

where \( \overline{f(x)} \) means the reduction of \( f(x) \in (R[x]/(x^t))^* \) modulo \( H \). Then, \( \text{Ker} \tau \subseteq \mathcal{F}_k \) forms a \((k - t + 1)\cdot(|H|, k)\) packing having \( H \) as its automorphism group.

**Proof:** The coefficient of \( x^{k-\gamma} \) in \( \prod_{a \in B} (x - a) \) is

\[
\sum_{\{\alpha_{11}, \ldots, \alpha_{is}\} \subseteq B} (-1)^s \alpha_{i1} \cdots \alpha_{is}.
\]

On the other hand, the coefficient of \( x^{k-\gamma} \) in \( \prod_{\alpha \in a \cdot B} (x - a) \) is

\[
a^s \sum_{\{\alpha_{i1}, \ldots, \alpha_{is}\} \subseteq B} (-1)^s \alpha_{i1} \cdots \alpha_{is}.
\]

This shows that \( a \cdot B \in \text{Ker} \tau \) for any \( a \in H \) if \( B \in \text{Ker} \tau \).

Now we show that the size \( \lambda \) of the intersection of any two distinct blocks from \( \text{Ker} \tau \) is at most \( k - t \). Let \( B_1, B_2 \in \text{Ker} \tau \) with \( B_1 \neq B_2 \). Then, \( \tau(B_1) = \tau(B_2) = \overline{\tau} \in (R[x]/(x^t))^*/H \), and this implies that there exists \( \ell \in H \) s.t.

\[
\prod_{a \in B_1} (x - a) - \ell \prod_{\beta \in B_2} (x - \beta) = 0 \mod(x^t).
\]

For the greatest common divisor \( g(x) = \prod_{\gamma \in U} (x - \gamma) \) of \( \prod_{\alpha \in B_1} (x - \alpha) \) and \( \prod_{\beta \in B_2} (x - \beta) \), it holds that

\[
\frac{\prod_{\alpha \in B_1} (x - \alpha) - \ell \prod_{\beta \in B_2} (x - \beta)}{g(x)} \equiv 0 \mod(x^t)
\]

since \( g(x) \not\equiv 0 \mod(x) \). By noting that \( |U| = \lambda \) and \( B_1 \neq B_2 \), we have

\[
\frac{\prod_{\alpha \in B_1} (x - \alpha) - \ell \prod_{\beta \in B_2} (x - \beta)}{g(x)} \neq 0
\]

in \( R[x] \) and hence \( k - |U| \geq t \), i.e., \( \lambda \leq k - t \).

The following proposition provides a lower bound on the number of blocks of packings of Theorem 3.1 for the case when \( t = 2 \) and \( R = \mathbb{F}_q \), where \( q = p^n \) is a prime power.

**Proposition 2.** The packing of Theorem 3.1 contains at least \((q^{-1})/k - (q^{-1})/(k - 1)\) blocks if \( R = \mathbb{F}_q \) and \( t = 2 \).
Proof: Let $I_k := \{1, 2, \ldots, k\}$. If $t = 2$, the $|\text{Ker}(\tau)|$ is equal to the number of unordered $k$-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ of distinct elements in $\mathbb{F}_q^*$ satisfying

$$
\sum_{i \in I_k} \prod_{j \in I_k \setminus \{i\}} \alpha_j = \left(\prod_{j \in I_k} \alpha_j\right) \cdot \left(\sum_{i \in I_k} \alpha_j^{-1}\right) = 0,
$$

i.e.,

$$
\sum_{i \in I_k} \alpha_i = 0.
$$

We denote the set of ordered $k$-tuples $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ of distinct elements in $\mathbb{F}_q^*$ satisfying

$$
i \cdot \alpha_h + \sum_{j \in I_k \setminus \{h\}} \alpha_j = 0
$$

by $S_{k,i,h}$ for $i \in \mathbb{Z}$. Obviously, $|S_{k,i,h}| = |S_{k,i,h'}|$ for any $h, h' \in I_k$, and $S_{k,i,h} \cap S_{k,i,h'} = \emptyset$ for any distinct $h, h' \in I_k$ if $i \neq 1$. Now set $N_{k,i} := |S_{k,i,h}|$.

For $i = 0$, it is clear that $N_{k,0} = (|\mathbb{F}_q^*| - (k - 1))N_{k-1,1}$. Next, we consider the case when $i \neq 0$. Eq. (7) implies that

$$
- \sum_{j \in I_k \setminus \{h\}} \alpha_j \neq 0
$$

and then $\alpha_h$ is determined by the other $\alpha_j$’s. If $\alpha_h = \alpha_\ell$ for some $\ell \in I_k \setminus \{h\}$, Eq. (7) is equivalent to

$$
\sum_{i \in I_k \setminus \{h, \ell\}} \alpha_j + (i + 1)\alpha_\ell = 0.
$$

Therefore, $N_{k,i} = A_k - N_{k-1,1} - (k - 1)N_{k-1,i+1}$ follows, where $A_k = (q^{-1}) \cdot (k-1)!$. Thus, we obtain the inductive formula

$$
N_{k,i} = \begin{cases} 
(q-k)N_{k-1,1} & \text{if } i = 0, \\
A_k - N_{k-1,1} - (k - 1)N_{k-1,i+1} & \text{if } i \neq 0,
\end{cases}
$$

with

$$
N_{2,i} = \begin{cases} 
q - 1 & \text{if } i, i + 1 \neq 0, \\
0 & \text{otherwise}.
\end{cases}
$$

Hence, it holds that

$$
|\text{Ker}(\tau)| = \frac{N_{k,1}}{k!} = \frac{A_k - N_{k-1,1} - (k - 1)N_{k-1,2}}{k!} \geq \frac{A_k - kA_{k-1}}{k!} = \frac{(q-1)}{k-1} \cdot \frac{k}{k} - \frac{(q-1)}{k-2} / (k-1),
$$

which shows the assertion. □

Remark 3. Note that any $t$-$(q - 1, k)$ packing of Theorem 3.1 has no short block orbit if $\gcd(k, q - 1) = 1$. Then, by Proposition 2, we can claim that there exists an asymptotically optimal $(q - 1, k, k - 2)$-OOC with $(\frac{q-1}{k-1})/(k(q-1)) - (\frac{q-1}{k-2})/(k-1)/(q-1)$ codewords under the assumption that $\gcd(k, q - 1) = 1$. In fact,

$$
J(q - 1, k, k - 2) \leq \frac{(q-1)}{k(q-1)}.
and
\[ \lim_{q \to \infty} \frac{(q-1)}{(k-1)(q-1)} \cdot \frac{k(q-1)}{(q-1)^2} = 0. \]

In particular, the number of missing codewords the resultant OOC to be optimal (a cyclic Steiner \((k-1)\)-design) is at most \( \frac{(q-1)}{(k-1)(q-1)} \), that is, the number of base blocks of a cyclic Steiner \((k-2)\)-design. As far as the authors know, such good asymptotically optimal OOCs have never been known for general \( \lambda \).

In the following examples, we compute the exact number of codewords of OOCs obtained in Theorem 3.1 in the case where \( k = 3 \) and \( 4 \). We will find some infinite families of optimal OOCs in these cases.

**Example 1.** If \((k,t) = (3,2)\), by the induction formula of Proposition 2, we have a cyclic \(2-(q-1,3)\) packing with \( |\text{Ker}(\tau)| \) blocks, where

\[ |\text{Ker}(\tau)| = \frac{N_{3,1}}{6} = \frac{A_{3} - N_{2,1} - 2N_{2,2}}{6} = \begin{cases} \frac{(q-1)(q-5)}{6} & \text{if } p \neq 2, 3, \\ \frac{(q-1)(q-2)}{6} & \text{if } p = 2, \\ \frac{(q-1)(q-3)}{6} & \text{if } p = 3. \end{cases} \]

It is clear that a triple \( B \subseteq \mathbb{F}_q^* \) containing 1 is in a short block orbit under the action of \( \mathbb{F}_q^* \) if and only if \( 3 | q - 1 \) and \( B = \{1, \gamma^{\frac{q-1}{2}}, \gamma^{\frac{2(q-1)}{3}}\} \), where \( \gamma \) is a primitive root of \( \mathbb{F}_q \). Note that \((x-1)(x-\gamma^{\frac{q-1}{2}})(x-\gamma^{\frac{2(q-1)}{3}}) \equiv -1 \pmod{x^2} \), i.e., \( B \in \text{Ker}(\tau) \).

Then, \( \text{Ker}(\tau) \) contains a short block orbit if and only if \( 3 | q - 1 \). Thus, there exists a \((q-1,3,1)\)-OOC with \( m \) codewords, where

\[ m = \begin{cases} \frac{q-5}{6} & \text{if } p \neq 2, 3 \text{ and } 3 | q - 1, \\ \frac{q-7}{6} & \text{if } p \neq 2, 3 \text{ and } 3 | q - 1, \\ \frac{q-9}{6} & \text{if } p = 2 \text{ and } 3 | q - 1, \\ \frac{q-3}{2} & \text{if } p = 3. \end{cases} \]

By the Johnson bound (1), the obtained \((q-1,3,1)\)-OOCs are ALL optimal.

**Example 2.** If \((k,t) = (4,2)\), by the induction formula of Proposition 2, we have a cyclic \(3-(q-1,4)\) packing with \( |\text{Ker}(\tau)| \) blocks, where

\[ |\text{Ker}(\tau)| = \frac{N_{4,1}}{24} = \frac{A_{4} - N_{3,1} - 3N_{3,2}}{24} = \begin{cases} \frac{(q-1)(q^2 - 9q + 26)}{24} & \text{if } p \neq 2, 3, \\ \frac{(q-1)(q-2)(q-4)}{24} & \text{if } p = 2, \\ \frac{(q-1)(q-3)(q-6)}{24} & \text{if } p = 3. \end{cases} \]

A quadruple \( B \subseteq \mathbb{F}_q^* \) containing 1 is in a short block orbit under the action of \( \mathbb{F}_q^* \) if and only if \( 2 | q - 1 \) and \( B = \{1, a, \gamma^{\frac{q-1}{2}}, a\gamma^{\frac{q+1}{2}}\} \) for some \( a \in \mathbb{F}_q^* \setminus \{1, -1\} \) or \( 4 | q - 1 \) and \( B = \{1, \gamma^{\frac{q-1}{2}}, \gamma^{\frac{q+1}{4}}, \gamma^{\frac{2(q+1)}{3}}\} \). Note that \((x-1)(x-a)(x-\gamma^{\frac{q-1}{2}})(x-a\gamma^{\frac{q+1}{2}}) \equiv a^2 \pmod{x^2} \), i.e., \( B \in \text{Ker}(\tau) \).

Then, \( \text{Ker}(\tau) \) has \( [(q-3)/4] \) short block orbits of length \((q-1)/2\) if and only if \( 2 | q - 1 \), and one short block orbit of length \((q-1)/4\) if and only if \( 4 | q - 1 \). From this, the total number of blocks in short block orbits is
(q - 1)(q - 3)/8 if \( p \neq 2 \). Thus, there exists a \((q - 1, 4, 2)\)-OOC with \( m \) codewords, where

\[
m = \begin{cases} 
\frac{(q-5)(q-7)}{24} & \text{if } p \neq 2, 3, \\
\frac{(q-2)(q-4)}{24} & \text{if } p = 2, \\
\frac{(q-3)(q-9)}{24} & \text{if } p = 3.
\end{cases}
\]

By the Johnson bound (1), the obtained OOCs for \( p = 2 \) are optimal.

REFERENCES

By noting that \( g \) and define \( \omega := \alpha^{q-1} \). Let
\[
\mathcal{E} = \{ g(x) \mid g(x) \neq g(x^j) \text{ for all } 0 \leq j \leq m-1 \} \subseteq \mathbb{F}_q[x]_t
\]
and define
\[
S' = \{ x_g := (g(1), g(\omega), \ldots, g(\omega^{m-1})) \mid g(x) \in \mathcal{E} \}.
\]
We say that two sequences are equivalent if one is a cyclic shift of the another. The sequences of \( S' \) are now classified into equivalent classes and each class contains exactly \( m \) sequences by the definition of \( \mathcal{E} \). Pick up one and only one sequence from each equivalent class and put them together, denoted by \( S \). Then, \( S \) forms the desired FHS. In fact, for \( x_g, x_h \in S \),
\[
H_{x_g, x_h}(\tau) = |\{ s \mid g(\omega^s) = h(\omega^{\tau+s}) \}| \leq |\{ x \in \mathbb{F}_q^* \mid g(x) = h(\omega^\tau x) \}| \leq t
\]
for \( 1 \leq \tau < m \) if \( g = h \) or for \( 0 \leq \tau < m \) otherwise. Therefore, it is sufficient to see that
\[
|\mathcal{E}| = \sum_{d \mid m} (q^{|(t+1)/d|} - 1)\mu(d).
\] (8)

To show this, we first observe that \( g(x) = g(x^j) \) for some \( j \) if and only if \( \gcd(\Delta_g, m) \neq 1 \), where \( \Delta_g = \gcd\{ i \mid a_i \neq 0 \} \) for \( g(x) = \sum_{i=1}^{t+1} a_i x^i \in \mathbb{F}_q[x]_t \). In fact, \( g(x^j) = \sum_{i=1}^{t+1} a_i \omega^{ji} x^i = \sum_{i=1}^{t+1} a_i x^i \) implies that \( \omega^{ji} = 1 \) for all \( i \in \{ i \mid a_i \neq 0 \} \). So the order of \( \omega^j \) divides \( \Delta_g \), which deduce \( \gcd(\Delta_g, m) \neq 1 \). Conversely, if \( \gcd(\Delta_g, m) \neq 1 \), the element \( y := \omega^{m/\gcd(\Delta_g, m)} \) satisfies \( g(x) = g(xy) \).

Let
\[
\mathcal{E}_d := \{ g(x) \in \mathbb{F}_q[x]_t \mid d \text{ divides } \Delta_g \}
\]
and then, by the aid of the Moebius function, we have
\[
|\mathcal{E}| = \sum_{d \mid m} \mu(d)|\mathcal{E}_d|.
\]
By noting that \( g(x) = g_1(x^d) \) with \( \deg(g_1) \leq \lfloor (t+1)/d \rfloor \) for \( g(x) \in \mathcal{E}_d \), we have
\[
|\mathcal{E}_d| = |\mathcal{E}_{\lfloor (t+1)/d \rfloor}| = q^{|(t+1)/d|} - 1,
\]
which shows (8). In particular, if \( m \) is a prime, we have \( |S| = |\mathcal{E}|/m = (q^{t+1} - 1)/m \), which attains the Singleton bound \( S(m, t; q) = [q^{t+1}/m] \).
E-mail address: clfan@yahoo.cn
E-mail address: momihara@educ.kumamoto-u.ac.jp