5-SEEDS FROM THE LIFTED GOLAY CODE OF LENGTH 24 OVER $\mathbb{Z}_4$

JIANYING FANG
Institute of Computer Information Engineering
Jiangxi Normal University
Nanchang, Jiangxi 330022, China

(Communicated by Mario Osvin Pavcevic)

ABSTRACT. Spontaneous emission error designs (SEEDs) are combinatorial objects that can be used to construct quantum jump codes. The lifted Golay code $G_{24}$ of length 24 over $\mathbb{Z}_4$ is cyclic self-dual code. It is known that $G_{24}$ yields 5-designs. In this paper, by using the generator matrices of bordered double circulant codes, we obtain 22 mutually disjoint 5-(24, $k$, $\lambda$) designs with $(k, \lambda) = (8, 1), (10, 36), (12, 1584)$ and 5-(24, $k$; 22)-SEEDs for $k = 8, 10, 12, 13$ from $G_{24}$.

1. Introduction

Let $V$ be a set of $n$ elements and let $t, k$ be integers with $0 < t < k < n$. For a collection $\mathcal{B}$ of $k$-subsets (called blocks) of $V$, $(V, \mathcal{B})$ is called a $t$-(n, $k$, $\lambda$) design if $|\{B \in \mathcal{B} : T \subset B\}| = \lambda$ for all $t$-subsets $T$ of $V$. In particular, a $t$-(n, $k$, 1) design is called a Steiner system $S(t, k, n)$. A design with no repeated block is called simple. All designs studied in this paper are simple. Two $t$-(n, $k$, $\lambda$) designs defined over the same set are said to be disjoint if they have no blocks in common. Mutually disjoint simple $t$-designs can be used to construct $t$-spontaneous emission error designs ($t$-SEEDs) (see [1, 9, 10, 18]), and $t$-SEEDs are combinatorial objects having close connection with quantum jump codes (see [2, 11, 19]).

Let $n$, $k$, $t$, $m$ be integers with $0 < t < k < n$ and $V$ be a set of $n$ elements. A $t$-spontaneous emission error design, denoted by $t$-(n, $k$, $m$)-SEED, is a system $\mathcal{B}$ of $k$-subsets of $V$ with a partition $\mathcal{B}^{(1)}, \mathcal{B}^{(2)}, \ldots, \mathcal{B}^{(m)}$ of $\mathcal{B}$ satisfying that $|\{B \in \mathcal{B}^{(i)} : T \subset B\}|/|\mathcal{B}^{(i)}| = \lambda_T$ for any $1 \leq i \leq m$ and $T \subset V$ with $|T| \leq t$, where $\lambda_T$ is a constant depending only on $T$.

A quaternary code $C$ of length $n$ is a linear block code over $\mathbb{Z}_4$ (the ring of integers modulo 4), i.e., an additive subgroup of $\mathbb{Z}_4^n$. Elements of $\mathbb{Z}_4^n$ are termed “vectors” even though $\mathbb{Z}_4^n$ is not a vector space, and an element of $C$ is called a codeword. The Hamming weight of a codeword is the number of its non-zero components. The Euclidean weights of the elements 0, 1, 2 and 3 of $\mathbb{Z}_4$ are 0, 1, 4 and 1, respectively. The Euclidean weight of a codeword is just the rational sum of the Euclidean weights of its components.

2010 Mathematics Subject Classification: Primary: 58F15, 58F17; Secondary: 53C35.
Key words and phrases: Spontaneous emission error design (SEED), lifted Golay code, double circulant code, mutually disjoint $t$-design, cyclic code.

The author is supported by NSFC grant 11401271, 61462026, 61262015, 61462040.
The symmetrized weight enumerator (or s.w.e.) of a code \( C \) over \( \mathbb{Z}_4 \) is
\[
\text{swe}_C(W, X, Y) = \sum_{c \in C} W^{n_0(c)} \cdot X^{n_1(c)} \cdot Y^{n_2(c)},
\]
where \( n_0(c), n_1(c) \) and \( n_2(c) \) are the numbers of components of \( c \) equal to 0, \pm 1 and 2, respectively.

We say that two codes are equivalent if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. Codes differing by only a permutation of coordinates are called permutation-equivalent. Equivalent codes have the same s.w.e.

The dual code \( C^\perp \) of \( C \) is defined as \( C^\perp = \{ x \in \mathbb{Z}_4^n \mid x \cdot y = 0 \text{ for all } y \in C \} \), where \( x \cdot y = x_1y_1 + \cdots + x_ny_n \mod 4 \) for \( x = (x_1, \ldots, x_n) \) and \( y = (y_1, \ldots, y_n) \). \( C \) is self-dual if \( C = C^\perp \).

Any quaternary code is permutation-equivalent to a code with generator matrix of the form
\[
G = \begin{pmatrix}
I_{k_1} & A & B \\
0 & 2I_{k_2} & 2D
\end{pmatrix},
\]
where \( A \) and \( D \) are \( \mathbb{Z}_2 \)-matrices and \( B \) is a \( \mathbb{Z}_4 \)-matrix, and 0 is the \( k_2 \times k_1 \) zero matrix. A codeword has the form \( aG \), where \( a = (a_1, \ldots, a_{k_1}, a_{k_1+1}, \ldots, a_{k_1+k_2}) \), \( a_i \in \mathbb{Z}_4 \) if \( 1 \leq i \leq k_1 \); \( a_i \in \mathbb{Z}_2 \) if \( k_1 + 1 \leq i \leq k_1 + k_2 \). We say that a code with generator matrix (1) is of type \( 4^{k_1}k_2^2 \), containing \( 2^{2k_1+k_2} \) codewords (cf. [8]).

Equation (1) illustrates a difference in point of view between ring theory and coding theory. Quaternary codes are \( \mathbb{Z}_4 \)-modules. A quaternary code \( C \) is not in general a free module [17], and so need not have a basis. The code \( C \) is a free \( \mathbb{Z}_4 \)-modules if and only if \( k_2 = 0 \) [13]. In particular, if the code \( C \) is free, then the size of the basis is still termed dimension of \( C \).

If a quaternary code \( C \) has generator matrix (1), then the dual code \( C^\perp \) has generator matrix
\[
\begin{pmatrix}
-I_{k_1} & A^T & D^T \\
2A^T & I_{n-k_1-k_2}
\end{pmatrix},
\]
where 0 is the \( k_2 \times (n-k_1-k_2) \) zero matrix, and \( C^\perp \) is of type \( 4^{n-k_1-k_2}k_2^2 \). As with codes over finite fields, a generator matrix of \( C^\perp \) is called a parity check matrix of \( C \).

Recently a number of papers have studied self-dual codes over \( \mathbb{Z}_4 \) (see [3][4][8][12]). Type II codes over \( \mathbb{Z}_4 \), introduced by Bonnecaze et al. in [3], are self-dual \( \mathbb{Z}_4 \)-codes containing the all-ones vector with the property that all Euclidean weights are divisible by eight. This class of codes includes the Hensel lifted Golay code \( G_{24} \) of length 24. It is shown that codewords of certain weight in the lifted Golay code \( G_{24} \) form \( 5 \cdot (24, k, \lambda) \) designs with \( (k, \lambda) \in \{(8, 1), (10, 36), (12, 1584), (12, 48), (13, 936)\} \) [12] [14] [23].

For \( a \in \mathbb{Z}_4 \), let \( a \) denote a vector whose every entry is \( a \). A code with generator matrix of the form
\[
\begin{pmatrix}
I_{s+1} & A & 1^T \\
3 & 2
\end{pmatrix}
\]
is called a bordered double circulant code of length \( 2s+2 \), where \( I_{s+1} \) is the identity matrix of order \( s+1 \) and \( A \) is an \( s \times s \) circulant matrix.

In this paper, we shall use generator matrices of form (3) to construct \( 5 \cdot (24, k, 22) \)-SEEDs for \( k = 8, 10, 12, 13 \) from the lifted Golay code \( G_{24} \).
Throughout this paper, let $V_n$ be the set $\{1,2,\ldots,n\}$, permutations on a code $C$ of length $n$ are considered on coordinate positions $V_n$ of $C$. For any permutation $\pi$ acting on $C$, we denote the image by $\pi(C)$. However, permutations on $C$ can be considered as column permutations on matrix $M$ whose rows are all codewords in $C$. But $\pi(C)$ corresponds to a column permutation on a parity check matrix $H$ of $C$, that is, if $C = \{x \in \mathbb{Z}_4^n : Hx^T = 0\}$, then $\pi(C) = \{y \in \mathbb{Z}_4^n : \pi(H)y^T = 0\}$, the proof is analogous to the $\mathbb{F}_2$ case in [18].

The paper is organized as follows. In Section 2, we recall background information on cyclic codes over $\mathbb{Z}_4$ and prove some lemmas for later use. In Section 3, we show the intersections among their images of Type II codes over $\mathbb{Z}_4$ with generator matrices of form [3] under some coordinate permutations. In Section 4, we give some constructions of 5-SEEDs from the lifted Golay code $G_{24}$.

2. SEVERAL LEMMAS

If $u = (u_0,u_1,\ldots,u_{n-1}) \in \mathbb{Z}_4^n$, define a function $f(u) = \sum_{i=0}^{n-1} u_i \in \mathbb{Z}$ with respect to $u$ (where $\mathbb{Z}$ is the set of integers). Suppose that $u = (u_0,u_1,\ldots,u_{n-1})$ and $v = (v_0,v_1,\ldots,v_{n-1})$ are quaternary vectors. Then it is easy to prove the following formula:

\begin{equation}
(4) \quad f(3u + v) \equiv 3f(u) + f(v) \pmod{4}.
\end{equation}

To generalize the concept of cyclic codes to codes over $\mathbb{Z}_4$, we need some algebra. Consider a polynomial $f(x)$ in $\mathbb{Z}_2[x]$ and write this as $f(x) = a(x^2) - xb(x^2)$. Define the map $\phi$ by

$$\phi(f)(x) = F(x) := \pm(a(x^2) - x(b(x^2))) \in \mathbb{Z}_4[x],$$

where the sign in $\pm$ is chosen in such a way that the coefficient of the highest power of $x$ is 1. The method of lifting (called, the Hensel lift) a polynomial in $\mathbb{Z}_2[x]$ to a polynomial in $\mathbb{Z}_4[x]$ is known as Graeffe’s method [24]. Clearly the inverse mapping is $f(x) \equiv F(x)(\pmod{2})$. Since both $\phi$ and its inverse do not change the degree of a polynomial nor the coefficient of the highest power of $x$, irreducible polynomials correspond to irreducible polynomials. $F(x)$ in $\mathbb{Z}_4[x]$ is called basic irreducible if $f(x)$ is irreducible in $\mathbb{Z}_2[x]$.

The polynomial ring $\mathbb{Z}_4[x]$ is not in general a unique factorization domain. But some special polynomials in $\mathbb{Z}_4[x]$ may have the unique factorization property. An example of such polynomials is $x^n - 1$ if $n$ is odd, and $x^n - 1$ can be factored into unique product of monic basic irreducible pairwise coprime polynomials in $\mathbb{Z}_4[x]$, i.e., $x^n - 1 = f_1f_2\cdots f_r$, where the $f_i$ are basic irreducible and pairwise coprime [16, Theorem 12.3.7].

As usual, a cyclic code $C$ of length $n$ over $\mathbb{Z}_4$ is a linear code with the property that if $(a_0,a_1,\ldots,a_{n-1}) \in C$, then $(a_{n-1},a_0,a_1,\ldots,a_{n-2}) \in C$. Let $R_n = \mathbb{Z}_4[x]/(x^n-1)$. Suppose that an element $c = (a_0,a_1,\ldots,a_{n-1}) \in C$ is identified with a polynomial $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ over $\mathbb{Z}_4$. Under this correspondence, a code is $\mathbb{Z}_4$ cyclic if and only if it is an ideal in the ring $R_n$. In [21] it was shown that any $\mathbb{Z}_4$ cyclic code $C$ of odd length $n$ has generators of the form $\langle f(x)h(x) \rangle \oplus \langle 2f(x)g(x) \rangle$ where $f(x)g(x)h(x) = x^{n-1}$ over $\mathbb{Z}_4$, $f(x), g(x)$, and $h(x)$ are unique, monic polynomials. Furthermore, $C$ has type $4^{\deg g(x)2^{\deg h(x)}}$. The proof is referred to Theorem 1 in [21] or Theorem 12.3.13 in [16]. In particular, if $h(x) = 1$, then $C = \langle f(x) \rangle$, and $C$ has type $4^{\deg f(x)}$ [16, Corollary 12.3.14].
In what follows we consider $C$ as a principal ideal of $R_n$ which is generated by an element $g(x)$ and $g(x)$ is a divisor of $x^n - 1$ for odd $n$. Moreover, we can easily write down a generator matrix $G$ for $C = \langle g(x) \rangle$, and the rows of $G$ correspond to $x^i g(x)$ for $0 \leq i \leq n - \deg g(x) - 1$. The following lemma is the same as [20] Theorem 49 except that the field is replaced by a ring, we state it here without proof.

**Lemma 1.** If $g(x)$ is a divisor of $x^n - 1$ for odd $n$ over $\mathbb{Z}_4$ and the degree of $g(x)$ is $n - k$, then $C = \langle g(x) \rangle$ has $4^k$ elements, i.e. the dimension of $C$ is $k$.

Let $C = \langle g(x) \rangle$ be a cyclic code over $\mathbb{Z}_4$ and $g(x)$ be a divisor of $x^n - 1$ for odd $n$. Let $h(x) = (x^n - 1)/g(x)$ and $h^\perp(x)$ denote its reciprocal polynomial, then $h^\perp(x)$ is a monic divisor of $x^n - 1$ as the constant term of $h(x)$ is $\pm 1$, and the dual code $C^\perp = \langle h^\perp(x) \rangle$. About these facts, we refer the reader to [16] Theorem 12.3.20. For a quaternary cyclic code, the following lemma is $Z_4$ analogous to Theorem 53 in [20].

**Lemma 2.** Let $C$ be a quaternary cyclic code of odd length $n$ with generator polynomial $x - 1$. Then $C$ has $4^{n-1}$ elements of $\mathbb{Z}_4^n$ consisting of all vectors $u$ with $f(u) \equiv 0 \pmod{4}$. Moreover, let $C' = \langle g(x) \rangle$ be a quaternary cyclic code, then $f(u) \equiv 0 \pmod{4}$ for any $u \in C'$ if $x - 1$ divides $g(x)$.

Proof. Noting that $C = \langle x - 1 \rangle$ and $x^n - 1 = (x - 1)(1 + x + \cdots + x^{n-1})$ over $\mathbb{Z}_4$, we have $C^\perp = \langle 1 + x + \cdots + x^{n-1} \rangle$ since $1 + x + \cdots + x^{n-1}$ is its own reciprocal polynomial. Then $C^\perp$ has 4 elements consisting of the vectors $a$ of length $n$ with $a \in \mathbb{Z}_4$. Hence, for any $u \in C$ we have $f(u) \equiv 0 \pmod{4}$ since $u$ and $a$ with $a \in \mathbb{Z}_4$ are orthogonal. Conversely, for any $u \in \mathbb{Z}_4^n$, if $f(u) \equiv 0 \pmod{4}$, then $u$ and $a$ with $a \in \mathbb{Z}_4$ are orthogonal. Hence $u \in C$.

Moreover, let $C' = \langle g(x) \rangle$ be a quaternary cyclic code, then $f(u) \equiv 0 \pmod{4}$ for any $u \in C'$ iff $u$ and $a$ with $a \in Z_4$ are orthogonal for any $u \in C'$ iff $C' \subseteq C$ if $x - 1$ divides $g(x)$.

The following lemma is analogous to Lemma 2.2 in [9] and is very useful for the proofs in the next sections.

**Lemma 3.** Let $A$ be a circulant matrix over $\mathbb{Z}_4$ with the first row $(c_0, c_1, \cdots, c_{n-1})$ corresponding to polynomial $c(x) = \sum_{i=0}^{n-1} c_i x^i$, where $n$ is odd. Let $g(x) = \gcd(x^n - 1, c(x))$. Then the degree of $g(x)$ is $n - k$ if and only if $\text{rank}(A) = k$.

Proof. Suppose that $C = \langle g(x) \rangle$. Then the dimension of $C$ is $k$ as the degree of $g(x)$ is $n - k$ by Lemma 1. Since $g(x)|c(x)$, the $i$-th row vector $x^i c(x)$ of $A$ is a codeword of $C$ for $0 \leq i \leq n - 1$. We next prove that the first $k$ rows of $A$, that is, the vectors $c(x), x c(x), \ldots, x^{k-1} c(x)$ are linearly independent. If they were not, then there would be $a_i \in \mathbb{Z}_4$, $0 \leq i \leq k - 1$, so that

$$a_0 c(x) + a_1 x c(x) + \cdots + a_{k-1} x^{k-1} c(x) = (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}) c(x) \equiv 0 \pmod{x^n - 1}.$$  

Because $\gcd(x^n - 1, c(x)) = g(x)$, we have the equality $a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} \equiv 0 \pmod{(x^n - 1)/g(x)}$. Note that $(x^n - 1)/g(x)$ is monic polynomial of degree $k$. We then have $a_i = 0$ for $0 \leq i \leq k - 1$. Hence, the first $k$ rows of $A$ are linearly independent. This means that the degree of $g(x)$ is $n - k$ if and only if $\text{rank}(A) = k$.

The following lemmas are useful for later use.
Lemma 4 (\[2\]). If there exist \(m\) mutually disjoint simple \((n, k, \lambda)\) designs, then there exists a \((n, k, m)\)-SEED.

Lemma 5. Let \((V, B^{(i)}), 1 \leq i \leq m\), be \(m\) simple \((n, k, \lambda)\) designs. If \(B^{(i)} \cap B^{(j)} = A\) for \(1 \leq i, j \leq m\) and \(i \neq j\), then there exists a \((n, k, m)\)-SEED.

Proof. Let \(B' = B^{(i)} \setminus A\) for \(1 \leq i \leq m\). By the definitions of a \((n, k, \lambda)\) design and a \((n, k, m)\)-SEED, we have that \(B'_i, 1 \leq i \leq m\), are mutually disjoint and they constitute a \((n, k, m)\)-SEED. \(\square\)

3. Intersections of Codes

In this section we let \(C\) (resp. \(C'\)) be a cyclic Type II code over \(\mathbb{Z}_4\) of length \(2s + 2\) for odd \(s\) with generator matrix \(G\) (resp. \(G'\)) of form (3) and \(A\) (resp. \(A'\)) be an \(s \times s\) circulant matrix in \(G\) (resp. \(G'\)), and suppose that \(a(x)\) (resp. \(a'(x)\)) denotes the polynomial corresponding to the first row of \(A\) (resp. \(A'\)). Let \(\delta = (s + 2, s + 3 \cdots 2s + 1)\) be the coordinate permutation acting on \(V_{2s+2} = \{1, 2, \ldots, 2s + 2\}\). We shall study the intersections of the images of \(C\) and \(C'\) under all permutations of the form \(\delta^i\). For any \(i, j \in \{0, 1, \ldots, s - 1\}\), define a polynomial depending on \(C\) and \(C'\) as follows:

\[
g_{ij}(C, C') = \gcd(3x^i a(x) + x^j a'(x), x^s - 1),
\]

Proposition 1. Let \(i, j \in \{0, 1, \ldots, s - 1\}\) and \(i \neq j\) if \(C = C'\). Then the dimension of \(\delta^i(C) \cap \delta^j(C')\) is \(d + 1\), where \(d\) is the degree of the polynomial \(g_{ij}(C, C')\).

Proof. Since \(C\) and \(C'\) are self-dual codes, we regard \(G\) and \(G'\) as their parity check matrices, respectively. Note that \(\pi(G) x^T = 0\) for any \(x \in \pi(C)\), where \(\pi\) is any coordinate permutation acting on \(V_{2s+2}\). Suppose that for any \(i, j \in \{0, 1, \ldots, s - 1\}\), \(x \in \delta^i(C) \cap \delta^j(C')\), then \(\delta^i(G) x^T = 0\) and \(\delta^j(G') x^T = 0\). So we get the homogeneous system of linear equations whose coefficient matrix is

\[
M = \begin{pmatrix}
\delta^i(G) \\
\delta^j(G')
\end{pmatrix} = \begin{pmatrix}
I_{s+1} & \delta^i(A) & 1^T \\
3 & 2 \\
I_{s+1} & \delta^j(A') & 1^T \\
3 & 2
\end{pmatrix}.
\]

For each \(l (1 \leq l \leq s + 1)\), we add 3 times of the \(l\)th row to the \((l + s + 1)\)th row in \(M\), getting

\[
\begin{pmatrix}
I_{s+1} & \delta^i(A) & 1^T \\
3 & 2 \\
0_{s+1} & 3\delta^i(A) + \delta^j(A') & 0^T \\
0 & 0
\end{pmatrix},
\]

where \(0_{s+1}\) is the zero matrix of order \(s + 1\).

Since \(3\delta^i(A) + \delta^j(A')\) is also an \(s \times s\) circulant matrix and the polynomial corresponding to the first row of it is \(3x^i a(x) + x^j a'(x) \text{ (mod } x^s - 1)\). By Lemma 3 the rank of \(M\) is \(2s + 1\) and hence the dimension of \(\delta^i(C) \cap \delta^j(C')\) is \(d + 1\). \(\square\)

Let \(v = (0, \ldots, 0, 1, 3, \ldots, 3, 2)\) of weight \(s + 2\) denote the last row of \(G\) (resp. \(G'\)) (a codeword of \(C\) (resp. \(C'\))). Let \(W = \langle v, 1 \rangle\), i.e., \(W\) is a subspace generated by \(v\) and \(1\). Clearly, the distribution of non-zero codewords in \(W\) is \(2 \cdot 2^{s+1}, 4 \cdot (\pm 1)^{s+1} 2^s, 2 \cdot (\pm 1)^{s+1} 2^{s+2}, 1^{2s+2}, 2^{2s+2}, (-1)^{2s+2}\), where the shape \(2^{s+1}\) denotes that components of a codeword consist of \(s + 1\) 2's and \(s + 1\) 0’s, and the coefficient is the number of codewords corresponding to the shape; the
others are analogous. Moreover, the supports of two codewords of the shape $2^{s+1}$ are $B_1 = \{s + 1, s + 2, \ldots, 2s + 1\}$ and $B_2 = \{1, 2, \ldots, s, 2s + 2\}$. The supports of four codewords of the shape $(\pm 1)^{s+1}2$ are $B_3 = \{s + 1, s + 2, \ldots, 2s + 2\}$ and $B_4 = \{1, 2, \ldots, s + 1, 2s + 2\}$.

Note that $\delta(\mathbf{v}) = \mathbf{v}$ and $\delta(\mathbf{1}) = \mathbf{1}$ for any $0 \leq i \leq s - 1$. Then we have the following results.

**Fact 1.** Let $i, j \in \{0, 1, \ldots, s - 1\}$. Then $W \subseteq \delta_i(C) \cap \delta_j(C')$.

Suppose that $a(x)$ (resp. $a'(x)$) denotes the polynomial corresponding to the first row $u$ (resp. $u'$) of $A$ (resp. $A'$). Then we have the following result.

**Proposition 2.** Let $i, j \in \{0, 1, \ldots, s - 1\}$. Then $x - 1$ divides $g_{ij}(C, C')$. If $g_{ij}(C, C') = x - 1$ where $i \neq j$ if $C = C'$, then $W = \delta_i(C) \cap \delta_j(C')$.

**Proof.** For any $i, j \in \{0, 1, \ldots, s - 1\}$. Since $C$ (resp. $C'$) is self-dual and contains the all-ones vector. So we have $f(u) \equiv f(u') \equiv 2 \pmod{4}$. Note that the vector corresponding to $x^ia(x)$ is a cyclic shift of $u$. Similarly, the vector corresponding to $x^ia'(x)$ is a cyclic shift of $u'$. By formula (4), for the vector $u_1$ corresponding to $(3x^ia(x) + x^ja'(x)) \pmod{x^s - 1}$, $f(u_1) \equiv 0 \pmod{4}$. Then by Lemma 2, $x - 1$ divides $(3x^ia(x) + x^ja'(x)) \pmod{x^s - 1}$. So $x - 1$ divides $g_{ij}(C, C')$ since $x - 1$ is a factor of $x^s - 1$ over $\mathbb{Z}_4$. If $g_{ij}(C, C') = x - 1$, by Proposition 1 the dimension of $\delta_i(C) \cap \delta_j(C')$ is 2. By Fact 1, $W = \delta_i(C) \cap \delta_j(C')$.  

4. 5-SEEDs from lifted Golay code $G_{24}$

The lifted Golay code $G_{24}$ over $\mathbb{Z}_4$ is defined in [1] as the extended Hensel lifted quadratic residue code of length 24. $G_{24}$ is a Type II code constructed from the cyclic code with generator polynomial

$$x^{11} + 2x^{10} + 3x^9 + 3x^7 + 3x^6 + 3x^5 + 2x^4 + x + 3,$$

by appending 3 to the last coordinate of the generator vectors. The s.w.e. of $G_{24}$ is given in [12]. It is shown that $G_{24}$ is equivalent to double circular Type II code $C_{1,11}$ in $[12]$ with the generator matrix of form $[3]$, where $A$ is an $11 \times 11$ circulant matrix with the first row $e=(2, 3, 1, 2, 1, 1, 0, 1, 0, 0)$, where we call this Type II code $C_1$. Moreover, let $C_2$ with the generator matrix of form $[3]$ be equivalent to $C_1$, where the first row of $A$ is $(0, 0, 1, 0, 1, 1, 2, 1, 3, 3, 2)$ obtained in inverse order from $e$.

It is shown the supports of codewords of Hamming weight 8, 10, 12, 13 corresponding to the shape $2^8$, $(\pm 1)^82^2$, $(\pm 1)^82^4$, $(2)^{12}$, $(\pm 1)^{12}2$ in turn form 5-($24, k, \lambda$) designs with $(k, \lambda) \in \{(8, 1), (10, 36), (12, 1584), (12, 48), (13, 936)\}$ [12, 14, 23].

For the $G_{24}$, we have that $s = 11$ and $\delta = (13 14 \cdots 23)$ is the coordinate permutation acting on $V_{24}$. The notations $\mathbf{v}$, $W$, and $B_i$, $i = 1, 2, 3, 4$ are defined as above section. We then have the following lemma.

**Lemma 6.** $W = \delta_i(C_e) \cap \delta_j(C_f)$ for any $e, f \in \{1, 2\}$, $i, j \in \{0, 1, \ldots, 10\}$ and $(i, e) \neq (j, f)$.

**Proof.** By the Hensel lift, $x^{11} - 1 = (x - 1) \sum_{i=0}^{10} x^i$ over $\mathbb{Z}_4$, where $x - 1$ and $\sum_{i=0}^{10} x^i$ are basic irreducible polynomials. For any $i, j \in \{0, 1, \ldots, 10\}$, $C, C' \in \{C_e : e = 1, 2\}$ and $i \neq j$ if $C = C'$, by Magma [6] it is verified that $g_{ij}(C, C') = x - 1$. By Proposition 3 the conclusion follows. 

[1] Advances in Mathematics of Communications, Volume 11, No. 3 (2017), 259–266.
Note that there is no codeword of weight \( k \) in \( W \), where \( k = 8, 10 \) and weight 12 of shape \((\pm 1)^{824}\). Hence, we get 22 mutually disjoint \(5-(24,k,\lambda)\) designs with \((k, \lambda) = (8, 1), (10, 36), (12, 1584)\) from \(\delta^i(C_e)\) \((i = 0, 1, \ldots, 10, e = 1, 2)\).

Moreover, \(B_1 = \{12, 13, \ldots, 23\}\) and \(B_2 = \{1, 2, \ldots, 11, 24\}\) are the only two common support sets of codewords of weight 12 corresponding to the shape \(2^{12}\) in \(\delta^i(C_e)\) \((i = 0, 1, \ldots, 10, e = 1, 2)\). For every one of \(5-(24, 12, 48)\) designs in \(\delta^i(C_e)\) \((i = 0, 1, \ldots, 10, e = 1, 2)\), by deleting these two blocks, we then obtain a \(5-(24, 12; 22)\)-SEED by Lemma 3. So by Lemma 4 there are two methods to construct a \(5-(24, 12; 22)\)-SEED since there exist 22 mutually disjoint \(5-(24, 12, 1584)\) designs.

Similarly, \(B_3 = \{12, 13, \ldots, 24\}\) and \(B_4 = \{1, 2, \ldots, 12, 24\}\) are the only two common support sets of codewords of weight 13 in \(\delta^i(C_e)\) \((i = 0, 1, \ldots, 10, e = 1, 2)\). For every one of \(5-(24, 13, 936)\) designs in \(\delta^i(C_e)\) \((i = 0, 1, \ldots, 10, e = 1, 2)\), by deleting these two blocks, we then obtain a \(5-(24, 13; 22)\)-SEED by Lemma 5. Combining Lemma 4 and the arguments, we summarize the results as follows.

**Theorem 1.** There exist 22 mutually disjoint \(5-(24,k,\lambda)\) designs with \((k, \lambda) = (8, 1), (10, 36), (12, 1584)\) and \(5-(24,k;22)\)-SEEDs for \(k = 8, 10, 12, 13\).

Jimbo and Shiromoto [13] give 22 mutually disjoint Steiner systems \(S(5,8,24)\) from the binary extended Golay \([24,12,8]\) code. In [12], 5 mutually disjoint \(5-(24,10,36)\) designs are given. The existence of 22 mutually disjoint \(5-(24,12,1584)\) designs is a new result.

**Acknowledgments**

The author would like to thank Junling Zhou for helpful discussions and the editor and two anonymous referees for their helpful comments.

**References**

[1] M. Araya, M. Harada, V. D. Tonchev and A. Wassermann, Mutually disjoint designs and new 5-designs derived from groups and codes, *J. Combin. Des.*, 18 (2010), 305–317.

[2] T. Beth, C. Charnes, M. Grassl, G. Alber, A. Delgado and M. Mussinger, A new class of designs which protect against quantum jumps, *Des. Codes Crypt.*, 29 (2003), 51–70.

[3] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over \(\mathbb{Z}_4\), *IEEE Trans. Inform. Theory*, 43 (1997), 969–976.

[4] A. Bonnecaze, P. Solé and A. R. Calderbank, Quaternary quadratic residue codes and unimodular lattices *IEEE Trans. Inform. Theory*, 41 (1995), 366–377.

[5] A. R. Calderbank and N. J. A. Sloane, Modular and \(p\)-adic cyclic codes, *Des. Codes Crypt.*, 6 (1995), 21–35.

[6] J. Cannon and W. Bosma, *Handbook of Magma functions*, Version 2.12, Univ. Sydney, 2005.

[7] C. Charnes and T. Beth, Combinatorial aspects of jump codes, *Discrete Math.*, 294 (2005), 43–51.

[8] J. H. Conway and N. J. A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory Ser. A*, 62 (1993), 30–45.

[9] J. Fang and Y. Chang, Mutually disjoint \(t\)-designs and \(t\)-SEEDs from extremal doubly-even self-dual codes *Des. Codes Crypt.*, 73 (2014), 769–780.

[10] J. Fang and Y. Chang, Mutually disjoint \(5\)-designs and \(5\)-spontaneous emission error designs from extremal ternary self-dual codes *J. Combin. Des.*, 23 (2015), 78–89.

[11] J. Fang, J. Zhou and Y. Chang, Non-existence of some quantum jump codes with specified parameters, *Des. Codes Crypt.*, 73 (2014), 223–235.

[12] T. A. Gulliver and M. Harada, Extremal double circulant Type II codes over \(\mathbb{Z}_4\) and \(5-(24,10,36)\) designs *Descrete Math.*, 194 (1999), 129–137.

[13] A. R. Hammons, Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The \(\mathbb{Z}_4^+\)-linearity of Kerdock, Preparata, Goethals, and related codes *IEEE Trans. Inform. Theory*, 40 (1994), 301–319.
[14] M. Harada, New 5-designs constructed from the lifted Golay code over $\mathbb{Z}_4$, J. Combin. Des., 6 (1999), 225–229.
[15] W. C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields Appl., 11 (2005), 451–490.
[16] W. C. Huffman and V. Pless, Fundamentals of Error Correcting Codes, Cambridge Univ. Press, Cambridge, 2003.
[17] T. W. Hungerford, Algebra, Springer-Verlag, New York, 1974.
[18] M. Jimbo and K. Shiromoto, A construction of mutually disjoint Steiner systems from isomorphic Golay codes, J. Combin. Theory Ser. A, 116 (2009), 1245–1251.
[19] M. Jimbo and K. Shiromoto, Quantum jump codes and related combinatorial designs, Inf. Sec. Coding Theory Rel. Combin., 29 (2011), 285–311.
[20] V. Pless, Introduction to the Theory of Error-Correcting Codes, 3rd edition, Wiley, New York (1998).
[21] V. Pless and Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory, 42 (1996), 1594–1600.
[22] V. Pless, P. Solé and Z. Qian, Cyclic self-dual $\mathbb{Z}_4$-codes, Finite Fields Appl., 3 (1997), 48–69.
[23] K. Tanabe, An Assmus-Mattson theorem for $\mathbb{Z}_4$-codes, IEEE Trans. Inform. Theory, 46 (2000), 48–53.
[24] J. V. Uspensky, Theory of Equations, McGraw-Hill, New York, 1948.

Received for publication November 2015.
E-mail address: fangjianying@163.com