AN EFFICIENT CONSTRUCTION OF SELF-DUAL CODES

JON-LARK KIM AND YOONJIN LEE

Abstract. Self-dual codes have been actively studied because of their connections with other mathematical areas including t-designs, invariant theory, group theory, lattices, and modular forms. We presented the building-up construction for self-dual codes over \( GF(q) \) with \( q \equiv 1 \pmod{4} \), and over other certain rings (see [19], [20]). Since then, the existence of the building-up construction for the open case over \( GF(q) \) with \( q = p^r \equiv 3 \pmod{4} \) with an odd prime \( p \) satisfying \( p \equiv 3 \pmod{4} \) with \( r \) odd has not been solved. In this paper, we answer it positively by presenting the building-up construction explicitly. As examples, we present new optimal self-dual \([16, 8, 7]\) codes over \( GF(7) \) and new self-dual codes over \( GF(7) \) with the best known parameters \([24, 12, 9]\).

1. Introduction

Since the development of Algebraic Coding Theory, self-dual codes have become one of the main research topics because of their connections with groups, combinatorial t-designs, lattices, and modular forms (see [26]). Some well known constructions of self-dual codes include the gluing vector technique ([23, 24]) and automorphism group method [15].

A recently developed and popular construction is to obtain self-dual codes from self-dual codes of smaller lengths. In [4, 6], the authors used shadow codes. Motivated by Harada’s work [12], the second author Kim [17] introduced the so-called building-up construction for binary self-dual codes. It shows that any binary self-dual code can be built from a self-dual code of a smaller length. Then later, the building-up construction for self-dual codes over finite fields \( GF(q) \) was developed when \( q \) is a power of 2 or \( q \equiv 1 \pmod{4} \) [19], and then over finite ring \( \mathbb{Z}_{p^m} \) with \( p \equiv 1 \pmod{4} \) [22], and over Galois rings \( GR(p^m, r) \).
with \( p \equiv 1 \pmod{4} \) with any \( r \) or \( p \equiv 3 \pmod{4} \) with \( r \) even [20], where \( m \) is any positive integer. The building-up construction is so powerful that one can find many (often new) self-dual codes of reasonable lengths (e.g. [9]).

In this paper, we complete the open cases of the building-up construction for self-dual codes over \( GF(q) \) with \( q = p^r \equiv 3 \pmod{4} \) with an odd prime \( p \) such that \( p \equiv 3 \pmod{4} \) with \( r \) odd. Since the length of the built codes from a given self-dual code increases by 4, it is more difficult to choose new four columns and two rows to be added to the generator matrix of a given self-dual code. Thus we have to change the proofs of the original papers [17], [19] dealing with the building-up construction for binary codes and codes over \( GF(q) \) with \( q \equiv 1 \pmod{4} \). Furthermore, as examples, we obtain 208 new optimal self-dual \([16,8,7]\) codes over \( GF(7) \) and 59 new self-dual codes over \( GF(7) \) with the best known parameters [24,12,9].

We remark that a preliminary result of this paper was announced in [21]. However, this full paper has never been published in a journal. The paper [21] claims that the building-up construction for the open case is possible but its proof is not given. Nevertheless, the authors [11] have already utilized the result of this full paper in order to study self-dual codes over \( F_2 + uF_2 \). Then recently Alfaro and Dhul-Qarnayn [3] and Han [10] have cited our paper as a main reference.

Therefore, we feel that it is worth publishing our full paper. This full paper contains detailed proofs of the main theorems and a new result on new optimal self-dual codes of lengths 16 and 24 over \( GF(7) \). All the codes in the paper are found by Magma [5] and are posted on [18].

2. Building-up construction for self-dual codes over \( GF(q) \) with \( q \equiv 3 \pmod{4} \)

In this section we provide the building-up construction for self-dual codes over \( GF(q) \) with \( q \equiv 3 \pmod{4} \), where \( q \) is a power of an odd prime. It is known [26, p. 193] that if \( q \equiv 3 \pmod{4} \) then a self-dual code of length \( n \) exists if and only if \( n \) is a multiple of 4. Our building-up construction needs the following known lemma [16, p. 281].

**Lemma 2.1.** Let \( q \) be a power of an odd prime with \( q \equiv 3 \pmod{4} \). Then there exist \( \alpha \) and \( \beta \) in \( GF(q)^* \) such that \( \alpha^2 + \beta^2 + 1 = 0 \) in \( GF(q) \), where \( GF(q)^* \) denotes the set of units of \( GF(q) \).

We give the building-up construction below and prove that it holds for any self-dual code over \( GF(q) \) with \( q \equiv 3 \pmod{4} \).

**Proposition 2.2.** Let \( q \) be a power of an odd prime such that \( q \equiv 3 \pmod{4} \), and let \( n \) be even. Let \( \alpha \) and \( \beta \) be in \( GF(q)^* \) such that \( \alpha^2 + \beta^2 + 1 = 0 \) in \( GF(q) \). Let \( G_0 = (\mathbf{r}_i) \) be a generator matrix (not necessarily in standard form) of a self-dual code \( C_0 \) over \( GF(q) \) of length \( 2n \), where \( \mathbf{r}_i \) are the row vectors for \( 1 \leq i \leq n \). Let \( \mathbf{x}_1 \) and \( \mathbf{x}_2 \) be vectors in \( GF(q)^{2n} \) such that \( \mathbf{x}_1 \cdot \mathbf{x}_2 = 0 \) in
GF(q) and \( x_i \cdot x_i = -1 \) in GF(q) for each \( i = 1, 2 \). For each \( i, 1 \leq i \leq n \), let \( s_i := x_1 \cdot r_i, t_i := x_2 \cdot r_i \), and \( y_i := (-s_i, -t_i, -\alpha s_i - \beta t_i, -\beta s_i + \alpha t_i) \) be a vector of length 4. Then the following matrix

\[
G = \begin{bmatrix}
1 & 0 & 0 & 0 & x_1 \\
0 & 1 & 0 & 0 & x_2 \\
y_1 & \cdot & \cdot & \cdot & r_1 \\
\vdots & \cdot & \cdot & \cdot & \vdots \\
y_n & \cdot & \cdot & \cdot & r_n
\end{bmatrix}
\]

generates a self-dual code \( C \) over GF(q) of length \( 2n + 4 \).

Proof. We first show that any two rows of \( G \) are orthogonal to each other. Each of the first two rows of \( G \) is orthogonal to itself as the inner product of the \( i \)th row with itself equals \( 1 + x_i \cdot x_i = 0 \) in GF(q) for \( i = 1, 2 \). The first row of \( G \) is orthogonal to the second row of \( G \) as \( x_1 \cdot x_2 = 0 \) in GF(q). Furthermore, the first row of \( G \) is orthogonal to any \((i + 2)\)th row of \( G \) for \( 1 \leq i \leq n \) since the inner product of the first row of \( G \) with the \((i + 2)\)th row of \( G \) is

\[
(1, 0, 0, 0) \cdot y_i + x_1 \cdot r_i = -s_i + s_i = 0.
\]

Similarly, the second row of \( G \) is orthogonal to any \((i + 2)\)th row of \( G \) for \( 1 \leq i \leq n \). We note that \( r_i \cdot r_j = 0 \) for \( 1 \leq i, j \leq n \). Any \((i + 2)\)th row of \( G \) is orthogonal to any \((j + 2)\)th row for \( 1 \leq i, j \leq n \) because the inner product of the \((i + 2)\)th row of \( G \) with the \((j + 2)\)th row is equal to

\[
y_i \cdot y_j + r_i \cdot r_j = (1 + \alpha^2 + \beta^2)(s_i s_j + t_i t_j) = 0 \quad \text{in \( GF(q) \).}
\]

Therefore, \( C \) is self-orthogonal; so \( C \subseteq C^\perp \).

We claim that the code \( C \) is of dimension \( n + 2 \). It suffices to show that no nontrivial linear combination of the first two rows of \( G \) is in the span of the bottom \( n \) rows of \( G \). Assume such a combination exists. Denoting the first two rows of \( G \) by \( G_1 \) and \( G_2 \), we have \( c_1 G_1 + c_2 G_2 = \sum_{i=1}^{n} d_i (y_i, r_i) \) for some nonzero \( c_1 \) or \( c_2 \) in GF(q) and some \( d_i \) in GF(q) with \( i = 1, \ldots, n \). Then comparing the first four coordinates of the vectors in both sides, we get

\[
c_1 = -\sum_{i=1}^{n} d_i s_i, \quad c_2 = -\sum_{i=1}^{n} d_i t_i, \quad 0 = -\sum_{i=1}^{n} d_i (\alpha s_i + \beta t_i), \quad 0 = \sum_{i=1}^{n} d_i (-\beta s_i + \alpha t_i); \quad \text{thus} \quad 0 = -\sum_{i=1}^{n} d_i (\alpha s_i + \beta t_i) = \alpha (-\sum_{i=1}^{n} d_i s_i) + \beta (\sum_{i=1}^{n} d_i t_i) = \alpha c_1 + \beta c_2, \quad \text{that is, we have} \quad \alpha c_1 + \beta c_2 = 0.
\]

Similarly we also have \( -\beta c_1 + \alpha c_2 = 0 \). From both equations \( \alpha c_1 + \beta c_2 = 0, -\beta c_1 + \alpha c_2 = 0 \), it follows that \( c_1 = c_2 = 0 \), a contradiction.

As the code \( C \) is of dimension \( n + 2 \) and \( \dim C + \dim C^\perp = 2n + 4 \), \( C \) and \( C^\perp \) have the same dimension. Since \( C \subseteq C^\perp \), we have \( C = C^\perp \), that is, \( C \) is self-dual.

We give a more efficient algorithm to construct \( G \) in Proposition 2.2 as follows. The idea of this construction comes from the recursive algorithm in [1], [2].
Modified building-up construction

- **Step 1:**
  Under the same notations as above, we consider the following.
  For each \( i \), let \( s_i \) and \( t_i \) be in \( GF(q) \) and define \( y_i := (s_i, t_i, \alpha s_i + \beta t_i, \beta s_i - \alpha t_i) \) be a vector of length 4. Then
  \[
  G_1 = \begin{bmatrix}
  y_1 & r_1 \\
  \vdots & \vdots \\
  y_n & r_n
  \end{bmatrix}
  \]
generates a self-orthogonal code \( C_1 \).

- **Step 2:**
  Let \( C \) be the dual of \( C_1 \). Consider the quotient space \( C/C_1 \). Let \( U_1 \) be the set of all coset representatives of the form \( x'_1 = (1 \ 0 \ 0 \ 0 \ x_1) \) such that \( x'_1 \cdot x'_1 = 0 \) and \( U_2 \) the set of all coset representatives of the form \( x'_2 = (0 \ 1 \ 0 \ 0 \ x_2) \) such that \( x'_2 \cdot x'_2 = 0 \).

- **Step 3:**
  For any \( x'_1 \in U_1 \) and \( x'_2 \in U_2 \) such that \( x'_1 \cdot x'_2 = 0 \), the following matrix
  \[
  G = \begin{bmatrix}
  1 & 0 & 0 & 0 & x_1 \\
  0 & 1 & 0 & 0 & x_2 \\
  y_1 & r_1 \\
  \vdots & \vdots \\
  y_n & r_n
  \end{bmatrix}
  \]
generates a self-dual code \( C \) over \( GF(q) \) of length \( 2n + 4 \).

Then, we have the following immediately.

**Proposition 2.3.** Let \( SD_1 \) be the set of all self-dual codes obtained from Proposition 2.2 with all possible vectors of \( x_1 \) and \( x_2 \). Let \( SD_2 \) be the set of all self-dual codes obtained from the modified building-up construction with all possible values of \( s_i \) and \( t_i \) in \( GF(q) \) for \( 1 \leq i \leq n \). Then \( SD_1 = SD_2 \).

What follows is the converse of Proposition 2.2, that is, every self-dual code over \( GF(q) \) with \( q \equiv 3 \pmod{4} \) can be obtained by the building-up method in Proposition 2.2.

**Proposition 2.4.** Let \( q \) be a power of an odd prime such that \( q \equiv 3 \pmod{4} \). Any self-dual code \( C \) over \( GF(q) \) of length \( 2n \) with even \( n \geq 4 \) is obtained from some self-dual code \( C_0 \) over \( GF(q) \) of length \( 2n - 4 \) (up to permutation equivalence) by the construction method given in Proposition 2.2.

**Proof.** Let \( G \) be a generator matrix of \( C \). Let \( I_n \) denote the identity matrix of order \( n \). Without loss of generality we may assume that \( G = (I_n \ | \ A) = (e_i \ | \ a_i) \), where \( e_i \) and \( a_i \) are the row vectors of \( I_n \) and \( A \), respectively for \( 1 \leq i \leq n \). It is enough to show that there exist vectors \( x_1, x_2 \) in \( GF(q)^{2n-4} \).
and a self-dual code $C_0$ over $GF(q)$ of length $2n - 4$ whose extended code $C_1$
(constructed by the method in Proposition 2.2) is equivalent to $C$.

We note that $a_i \cdot a_j = 0$ for $i \neq j$, $1 \leq i, j \leq n$ and $a_i \cdot a_i = -1$ for $1 \leq i \leq n$
since $C$ is self-dual. Let $\alpha$ and $\beta$ be in $GF(q)^*$ such that $\alpha^2 + \beta^2 + 1 = 0$
in $GF(q)$. We notice that $\mathcal{C}$ also has the following generator matrix

$$G' := \begin{bmatrix}
  e_1 + \alpha e_3 + \beta e_4 & a_1 + \alpha a_3 + \beta a_4 \\
  e_2 + \beta e_3 - \alpha e_4 & a_2 + \beta a_3 - \alpha a_4 \\
  e_3 & a_3 \\
  e_4 & a_4 \\
  \vdots & \vdots \\
  e_n & a_n
\end{bmatrix}.$$

Deleting the first four columns and the third and fourth rows of $G'$ produces the following $(n - 2) \times (2n - 4)$ matrix $G_0$:

$$G_0 := \begin{bmatrix}
  0 & \cdots & 0 & a_1 + \alpha a_3 + \beta a_4 \\
  0 & \cdots & 0 & a_2 + \beta a_3 - \alpha a_4 \\
  I_{n-4} & \vdots & & \vdots \\
  & & & a_n
\end{bmatrix}.$$

We claim that $G_0$ is a generator matrix of some self-dual code $C_0$ of length $2n - 4$. We first show that $G_0$ generates a self-orthogonal code $C_0$ as follows. The inner product of the first row of $G_0$ with itself is equal to

$$a_1 \cdot a_1 + \alpha^2 a_3 \cdot a_3 + \beta^2 a_4 \cdot a_4 = -(1 + \alpha^2 + \beta^2) = 0,$$

and similarly the second row is orthogonal to itself. For $3 \leq i \leq n - 2$, the inner product of the $i$th row of $G_0$ with itself equals $1 + a_{i+2} \cdot a_{i+2} = 0$. The inner product of the first row of $G_0$ with the second row is $\alpha \beta a_3 \cdot a_3 - \alpha \beta a_4 \cdot a_4 = 0$. Clearly, for $1 \leq i, j \leq n - 2$ with $i \neq j$, any $i$th row is orthogonal to any $j$th row.

Now we show that $|C_0| = q^{n-2}$, so $C_0$ is self-dual. First of all, we note that both vectors $v_1 := a_1 + \alpha a_3 + \beta a_4$ and $v_2 := a_2 + \beta a_3 - \alpha a_4$ in the first two rows of $G_0$ contain units. Otherwise, both vectors are zero vectors. Then $a_1 = -(\alpha a_3 + \beta a_4)$, then $-1 = a_1 \cdot a_1 = (\alpha a_3 + \beta a_4) \cdot (\alpha a_3 + \beta a_4) = -(\alpha^2 + \beta^2) = 1$, i.e., $-1 = 1$ in $GF(q)$, which is impossible since $q$ is odd. So, $v_1$ is a nonzero vector, and hence it contains a unit. Similarly, it is also true for $v_2$. We can also show that $v_1$ and $v_2$ are linearly independent. If not, $v_1 = cv_2$ for some $c$ in $GF(q)^*$. Then by taking inner products of both sides with $a_1$, we have $a_1 \cdot v_1 = c a_1 \cdot v_2$, so we get $-1 = 0$, a contradiction. Therefore it follows that $G_0$ is equivalent to a standard form of matrix $[I_{n-2} | * ]$, so that $|C_0| = q^{n-2}$, that is, $C_0$ is self-dual.

Let $x_1 = (0, \ldots, 0 \mid a_1)$ and $x_2 = (0, \ldots, 0 \mid a_2)$ be row vectors of length $2n - 4$. Then for $i = 1, 2$, $x_i \cdot x_i = a_i \cdot a_i = -1$ in $GF(q)$ and $x_1 \cdot x_2 = \ldots$
\( a_1 \cdot a_2 = 0 \) in \( GF(q) \). Using the vectors \( x_1, x_2 \) and the self-dual code \( C_0 \), we can construct a self-dual code \( C_1 \) with the following \( n \times 2n \) generator matrix \( G_1 \) by Proposition 2.2:

\[
G_1 := \begin{bmatrix}
1 & 0 & 0 & 0 & \ldots & 0 & a_1 \\
0 & 1 & 0 & 0 & \ldots & 0 & a_2 \\
1 & 0 & \alpha & \beta & 0 & \ldots & 0 & a_1 + a_3 + \beta a_4 \\
0 & 1 & \beta & -\alpha & 0 & \ldots & 0 & a_2 + \beta a_3 - \alpha a_4 \\
0 & 0 & 0 & 0 & \ldots & 0 & a_5 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \ldots & 0 & a_n \\
\end{bmatrix}.
\]

Clearly \( G_1 \) is row equivalent to \( G \). Hence the given code \( C \) is the same as the code \( C_1 \) that is obtained from the code \( C_0 \) by the building-up construction in Proposition 2.2. This completes the proof. \( \square \)

Remark 2.5. Note that in the statement of Proposition 2.4 we do not have any condition on the minimum distance of \( C \). In the middle part of the proof of Proposition 2.4 we have shown that \( G_0 \) has size \((n - 2) \times (2n - 4)\) and has dimension \( n - 2 \) without using the minimum distance of \( C \).

2.1. Self-dual codes over \( GF(7) \)

Next we consider self-dual codes over \( GF(7) \). The classification of self-dual codes over \( GF(7) \) was known up to lengths 12 (see [7, 8, 14, 25]). The papers [7, 8] used the monomial equivalence and monomial automorphism groups of self-dual codes over \( GF(7) \). Hence we also use the monomial equivalence and monomial automorphism groups. On the other hand, the \((1, -1, 0)\)-monomial equivalence was used in [25, Theorem 1] to give a mass formula:

\[
\sum_j \frac{2^n n!}{|\text{Aut}(C_j)|} = N(n) = 2 \prod_{i=1}^{(n-2)/2} (7^i + 1),
\]

where \( N(n) \) denotes the total number of distinct self-dual codes over \( GF(7) \). In particular, when \( n = 16 \), there are at least 785086 > \( N(16)/2^{16}16! \) inequivalent self-dual \([16, 8]\) codes over \( GF(7) \) under the \((1, -1, 0)\)-monomial equivalence. It will be very difficult to classify all self-dual \([16, 8]\) codes. In what follows, we focus on self-dual codes with the highest minimum distance.

For length \( n = 16 \), only ten optimal self-dual \([16, 8, 7]\) codes over \( GF(7) \) were known [8]. These have (monomial) automorphism group orders 96 or 192. We construct at least 214 self-dual \([16, 8, 7]\) codes over \( GF(7) \) by applying the building-up construction to the bordered circulant code with \( \alpha = 0, \beta = 2 = \gamma \) and the row \((2, 5, 5, 2, 0)\), denoted by \( C_{1,1} \) in [7]. We check that the 207 codes of the 214 codes have automorphism group orders 6, 12, 24, 48, 72, and hence they are new. On the other hand, the remaining seven codes have group orders 96 or 192, and we have checked that six of them are equivalent to the first four.
codes and the last two codes in [8, Table 7], and that the remaining one code is new. We list 20 of our 214 codes in Table 1, where \( x_1 \) and \( x_2 \) are given in the second and third columns respectively, and \( A_7 \) and \( A_8 \) are given in the last column so that the Hamming weight enumerator of the corresponding code can be derived from the appendix of [8].

<table>
<thead>
<tr>
<th>#</th>
<th>( x_1 = (0 \ldots 0x_1 \ldots x_{12}) )</th>
<th>( x_2 = (0 \ldots 0x_5 \ldots x_{12}) )</th>
<th>Aut</th>
<th>( A_7, A_8 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2 1 2 6 1 1 6 1 0</td>
<td>1 2 1 1 6 5 1 0</td>
<td>24</td>
<td>696, 3432</td>
</tr>
<tr>
<td>2</td>
<td>1 2 2 6 1 6 1 0</td>
<td>4 5 6 4 4 6 1 0</td>
<td>24</td>
<td>720, 3360</td>
</tr>
<tr>
<td>3</td>
<td>5 1 5 6 1 6 1 0</td>
<td>4 5 1 3 6 1 3 0</td>
<td>12</td>
<td>636, 3780</td>
</tr>
<tr>
<td>4</td>
<td>5 1 5 1 1 6 1 0</td>
<td>6 3 3 6 1 2 3 0</td>
<td>6</td>
<td>564, 3996</td>
</tr>
<tr>
<td>5</td>
<td>6 5 5 1 1 6 1 0</td>
<td>3 4 1 2 4 1 1 0</td>
<td>12</td>
<td>540, 4068</td>
</tr>
<tr>
<td>6</td>
<td>5 2 1 1 1 6 1 0</td>
<td>2 1 2 1 5 2 3 0</td>
<td>12</td>
<td>588, 3924</td>
</tr>
<tr>
<td>7</td>
<td>1 6 2 2 1 6 1 0</td>
<td>3 2 1 5 1 2 2 0</td>
<td>6</td>
<td>612, 3804</td>
</tr>
<tr>
<td>8</td>
<td>4 2 3 3 1 6 1 0</td>
<td>3 3 5 3 3 5 2 0</td>
<td>12</td>
<td>576, 3936</td>
</tr>
<tr>
<td>9</td>
<td>5 3 3 3 1 6 1 0</td>
<td>4 1 4 5 1 3 1 0</td>
<td>12</td>
<td>588, 3876</td>
</tr>
<tr>
<td>10</td>
<td>3 2 4 3 1 6 1 0</td>
<td>5 5 2 4 1 5 1 0</td>
<td>12</td>
<td>552, 4104</td>
</tr>
<tr>
<td>11</td>
<td>2 3 4 3 1 6 1 0</td>
<td>4 4 5 4 2 2 0</td>
<td>12</td>
<td>624, 3744</td>
</tr>
<tr>
<td>12</td>
<td>5 4 4 3 1 6 1 0</td>
<td>6 2 6 3 1 3 0</td>
<td>12</td>
<td>612, 3852</td>
</tr>
<tr>
<td>13</td>
<td>5 3 4 4 1 6 1 0</td>
<td>5 5 3 5 1 1 0</td>
<td>48</td>
<td>576, 3936</td>
</tr>
<tr>
<td>14</td>
<td>1 5 1 5 1 6 1 0</td>
<td>3 1 2 4 3 1 0</td>
<td>24</td>
<td>480, 4320</td>
</tr>
<tr>
<td>15</td>
<td>2 6 1 5 1 6 1 0</td>
<td>5 3 1 1 3 3 0</td>
<td>24</td>
<td>672, 3552</td>
</tr>
<tr>
<td>16</td>
<td>3 4 4 5 1 6 1 0</td>
<td>5 2 5 3 6 2 1 0</td>
<td>48</td>
<td>528, 4128</td>
</tr>
<tr>
<td>17</td>
<td>2 1 6 5 1 6 1 0</td>
<td>6 2 5 2 3 2 1 0</td>
<td>12</td>
<td>672, 3552</td>
</tr>
<tr>
<td>18</td>
<td>5 2 3 5 2 6 1 0</td>
<td>1 4 4 5 1 4 1 0</td>
<td>12</td>
<td>660, 3708</td>
</tr>
<tr>
<td>19</td>
<td>2 2 4 5 2 6 1 0</td>
<td>2 1 2 1 2 5 3 0</td>
<td>6</td>
<td>564, 4092</td>
</tr>
<tr>
<td>20</td>
<td>6 6 6 5 2 6 1 0</td>
<td>1 3 1 4 6 2 3 0</td>
<td>6</td>
<td>600, 3912</td>
</tr>
</tbody>
</table>

**Theorem 2.6.** There exist at least 218 self-dual \([16, 8, 7]\) codes over \( GF(7) \).

For length 20 only one optimal self-dual \([20, 10, 9]\) code over \( GF(7) \) is known ([7], [8]). It is an open question to determine whether this code is unique.

For length 24 there are 488 best known self-dual \([24, 12, 9]\) codes over \( GF(7) \) ([8]). It has been confirmed [13] that the 488 codes in [8] (only 40 codes are shown in [8]) have non-trivial automorphism groups. On the other hand, we have found at least 59 self-dual \([24, 12, 9]\) codes over \( GF(7) \), each of which has a trivial automorphism group. To do this, we have used the bordered circulant code over \( GF(7) \) with \( \alpha = 2, \beta = 1 = \gamma \) and the row \((4, 6, 3, 6, 6, 1, 4, 3, 0)\), denoted by \( C_{20,1} \) [7]. We list 10 of our 59 codes in Table 2, where \( x_1 \) and \( x_2 \) are given in the second and third columns respectively, and \( A_9, \ldots, A_{12} \) are given in the last column so that the Hamming weight enumerator of the
Table 2. New [24,12,9] self-dual codes over GF(7) using $C_{20,1}$ in [7] with trivial automorphism groups

<table>
<thead>
<tr>
<th>#</th>
<th>$x_1 = (0, \ldots, 0x_9, \ldots, x_{20})$</th>
<th>$x_2 = (0, \ldots, 0x_9, \ldots, x_{20})$</th>
<th>$A_9, A_{10}, A_{11}, A_{12}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2 6 2 3 2 1 6 1 6 1 0 0</td>
<td>4 4 3 5 3 2 1 1 6 1 0 0</td>
<td>948, 8496, 65520, 425484</td>
</tr>
<tr>
<td>2</td>
<td>2 2 5 1 3 1 6 1 6 1 0 0</td>
<td>3 5 4 6 4 2 1 6 1 0 0</td>
<td>894, 8802, 64572, 427704</td>
</tr>
<tr>
<td>3</td>
<td>6 4 4 1 4 1 6 1 6 1 0 0</td>
<td>3 6 2 6 1 2 2 1 6 1 0 0</td>
<td>936, 8436, 65580, 427704</td>
</tr>
<tr>
<td>4</td>
<td>2 6 2 3 5 1 6 1 6 1 0 0</td>
<td>5 3 3 4 4 2 1 1 6 1 0 0</td>
<td>882, 8592, 65444, 427086</td>
</tr>
<tr>
<td>5</td>
<td>5 6 5 4 5 1 6 1 6 1 0 0</td>
<td>2 1 3 5 1 5 1 1 6 1 0 0</td>
<td>774, 8706, 66204, 428204</td>
</tr>
<tr>
<td>6</td>
<td>1 4 2 2 1 2 6 1 6 1 0 0</td>
<td>3 3 5 6 3 4 2 1 6 1 0 0</td>
<td>948, 8466, 65520, 426306</td>
</tr>
<tr>
<td>7</td>
<td>4 5 3 4 2 6 1 6 1 0 0</td>
<td>1 3 5 1 2 1 2 1 6 1 0 0</td>
<td>936, 8982, 63516, 426750</td>
</tr>
<tr>
<td>8</td>
<td>1 6 4 6 4 3 6 1 6 1 0 0</td>
<td>2 1 6 3 2 6 2 1 6 1 0 0</td>
<td>966, 8502, 65148, 426792</td>
</tr>
<tr>
<td>9</td>
<td>1 3 1 1 3 6 1 6 1 0 0</td>
<td>5 2 3 2 4 2 1 6 1 0 0</td>
<td>966, 8700, 64500, 425730</td>
</tr>
<tr>
<td>10</td>
<td>4 6 1 6 3 4 6 1 6 1 0 0</td>
<td>5 1 6 3 6 2 2 1 6 1 0 0</td>
<td>846, 8796, 65448, 424134</td>
</tr>
</tbody>
</table>

The corresponding code can be derived from the appendix of [8]. We therefore obtain the following theorem.

**Theorem 2.7.** There exist at least 547 self-dual [24,12,9] codes over GF(7).

3. Conclusion

We have completed the open cases of the building-up construction for self-dual codes over GF(q) with $q \equiv 3 \pmod{4}$ with $p \equiv 3 \pmod{4}$.

We have seen that the building-up construction is a very efficient way of finding many self-dual codes of reasonable lengths. In particular, we obtain new optimal self-dual [16,8,7] codes over GF(7) and new self-dual codes over GF(7) with the best known parameters [24,12,9].

References


JON-LARK KIM
DEPARTMENT OF MATHEMATICS
SO GANG UNIVERSITY
SEOUL 121-742, KOREA
E-mail address: jlkim@sogang.ac.kr

YOON JIN LEE
DEPARTMENT OF MATHEMATICS
EWH A WOMANS UNIVERSITY
SEOUL 120-750, KOREA
E-mail address: yoonjinl@ewha.ac.kr