Bull. Korean Math. Soc. **52** (2015), No. 3, pp. 915–923
http://dx.doi.org/10.4134/BKMS.2015.52.3.915

# 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 $GR(p^m, r)$

Received April 23, 2014; Revised October 29, 2014.

2010 *Mathematics Subject Classification.* Primary 94B05.

*Key words and phrases.* building-up construction, linear codes, self-dual codes.

The first author was supported by Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2005172) and by the Sogang University Research Grant of 201210058.01. The second author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2009-0093827) and by the NRF grant funded by the Korea government(MEST)(2014-002731).

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 $\mathbb{F}_2 + u\mathbb{F}_2$. 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 $\mathcal{C}_0$ over $GF(q)$ of length $2n$, where $\mathbf{r}_i$ are the row vectors for $1 \le i \le n$. 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 $\mathbf{x}_i \cdot \mathbf{x}_i = -1$ in $GF(q)$ for each $i = 1, 2$. For each $i$, $1 \le i \le n$, let $s_i := \mathbf{x}_1 \cdot \mathbf{r}_i$, $t_i := \mathbf{x}_2 \cdot \mathbf{r}_i$, and $\mathbf{y}_i := (-s_i, -t_i, -\alpha s_i - \beta t_i, -\beta s_i + \alpha t_i)$ be a vector of length 4. Then the following matrix*

$$G = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \mathbf{x}_1 \\ 0 & 1 & 0 & 0 & \mathbf{x}_2 \\ \hline \multicolumn{4}{c|}{\mathbf{y}_1} & \mathbf{r}_1 \\ \multicolumn{4}{c|}{\vdots} & \vdots \\ \multicolumn{4}{c|}{\mathbf{y}_n} & \mathbf{r}_n \end{array}\right]$$

*generates a self-dual code $\mathcal{C}$ 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 $1 + \mathbf{x}_i \cdot \mathbf{x}_i = 0$ in $GF(q)$ for $i = 1, 2$. The first row of $G$ is orthogonal to the second row of $G$ as $\mathbf{x}_1 \cdot \mathbf{x}_2 = 0$ in $GF(q)$. Furthermore, the first row of $G$ is orthogonal to any $(i + 2)$th row of $G$ for $1 \le i \le n$ since the inner product of the first row of $G$ with the $(i + 2)$th row of $G$ is

$$(1, 0, 0, 0) \cdot \mathbf{y}_i + \mathbf{x}_1 \cdot \mathbf{r}_i = -s_i + s_i = 0.$$

Similarly, the second row of $G$ is orthogonal to any $(i + 2)$th row of $G$ for $1 \le i \le n$. We note that $\mathbf{r}_i \cdot \mathbf{r}_j = 0$ for $1 \le i, j \le n$. Any $(i + 2)$th row of $G$ is orthogonal to any $(j + 2)$th row for $1 \le i, j \le n$ because the inner product of the $(i + 2)$th row of $G$ with the $(j + 2)$th row is equal to

$$\mathbf{y}_i \cdot \mathbf{y}_j + \mathbf{r}_i \cdot \mathbf{r}_j = (1 + \alpha^2 + \beta^2)(s_i s_j + t_i t_j) = 0 \quad \text{in } GF(q).$$

Therefore, $\mathcal{C}$ is self-orthogonal; so $\mathcal{C} \subseteq \mathcal{C}^\perp$.

We claim that the code $\mathcal{C}$ 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 $c_1 G_1 + c_2 G_2 = \sum_{i=1}^n d_i(\mathbf{y}_i, \mathbf{r}_i)$ 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 $c_1 = -\sum_{i=1}^n d_i s_i$, $c_2 = -\sum_{i=1}^n d_i t_i$, $0 = -\sum_{i=1}^n d_i(\alpha s_i + \beta t_i)$, $0 = \sum_{i=1}^n d_i(-\beta s_i + \alpha t_i)$; thus $0 = -\sum_{i=1}^n d_i(\alpha s_i + \beta t_i) = \alpha(-\sum_{i=1}^n d_i s_i) + \beta(-\sum_{i=1}^n d_i t_i) = \alpha c_1 + \beta c_2$, that is, we have $\alpha c_1 + \beta c_2 = 0$. 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 $\mathcal{C}$ is of dimension $n + 2$ and $\dim \mathcal{C} + \dim \mathcal{C}^\perp = 2n + 4$, $\mathcal{C}$ and $\mathcal{C}^\perp$ have the same dimension. Since $\mathcal{C} \subseteq \mathcal{C}^\perp$, we have $\mathcal{C} = \mathcal{C}^\perp$, that is, $\mathcal{C}$ 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 $\mathbf{y}_i := (s_i, t_i, \alpha s_i + \beta t_i, \beta s_i - \alpha t_i)$ be a vector of length 4. Then

$$G1 = \left[\begin{array}{c|c} \mathbf{y}_1 & \mathbf{r}_1 \\ \vdots & \vdots \\ \mathbf{y}_n & \mathbf{r}_n \end{array}\right]$$

  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 $\mathbf{x}_1' = (1\ 0\ 0\ 0\ \mathbf{x}_1)$ such that $\mathbf{x}_1' \cdot \mathbf{x}_1' = 0$ and $U_2$ the set of all coset representatives of the form $\mathbf{x}_2' = (0\ 1\ 0\ 0\ \mathbf{x}_2)$ such that $\mathbf{x}_2' \cdot \mathbf{x}_2' = 0$.

- Step 3:

  For any $\mathbf{x}_1' \in U_1$ and $\mathbf{x}_2' \in U_2$ such that $\mathbf{x}_1' \cdot \mathbf{x}_2' = 0$, the following matrix

$$G = \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & \mathbf{x}_1 \\ 0 & 1 & 0 & 0 & \mathbf{x}_2 \\ \hline & & \mathbf{y}_1 & & \mathbf{r}_1 \\ & & \vdots & & \vdots \\ & & \mathbf{y}_n & & \mathbf{r}_n \end{array}\right]$$

  generates a self-dual code $\mathcal{C}$ 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 $\mathbf{x}_1$ and $\mathbf{x}_2$. 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 $1 \le i \le n$. 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 $\mathcal{C}$ over $GF(q)$ of length $2n$ with even $n \ge 4$ is obtained from some self-dual code $\mathcal{C}_0$ 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 $\mathcal{C}$. Let $I_n$ denote the identity matrix of order $n$. Without loss of generality we may assume that $G = (I_n \mid A) = (\mathbf{e}_i \mid \mathbf{a}_i)$, where $\mathbf{e}_i$ and $\mathbf{a}_i$ are the row vectors of $I_n$ and $A$, respectively for $1 \le i \le n$. It is enough to show that there exist vectors $\mathbf{x}_1, \mathbf{x}_2$ in $GF(q)^{2n-4}$

and a self-dual code $\mathcal{C}_0$ over $GF(q)$ of length $2n-4$ whose extended code $\mathcal{C}_1$ (constructed by the method in Proposition 2.2) is equivalent to $\mathcal{C}$.

We note that $\mathbf{a}_i \cdot \mathbf{a}_j = 0$ for $i \neq j$, $1 \leq i, j \leq n$ and $\mathbf{a}_i \cdot \mathbf{a}_i = -1$ for $1 \leq i \leq n$ since $\mathcal{C}$ 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

$$G' := \left[\begin{array}{c|c} \mathbf{e}_1 + \alpha\mathbf{e}_3 + \beta\mathbf{e}_4 & \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4 \\ \mathbf{e}_2 + \beta\mathbf{e}_3 - \alpha\mathbf{e}_4 & \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4 \\ \mathbf{e}_3 & \mathbf{a}_3 \\ \mathbf{e}_4 & \mathbf{a}_4 \\ \vdots & \vdots \\ \mathbf{e}_n & \mathbf{a}_n \end{array}\right].$$

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

$$G_0 := \left[\begin{array}{ccc|c} 0 & \cdots & 0 & \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4 \\ 0 & \cdots & 0 & \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4 \\ & & & \mathbf{a}_5 \\ & I_{n-4} & & \vdots \\ & & & \mathbf{a}_n \end{array}\right].$$

We claim that $G_0$ is a generator matrix of some self-dual code $\mathcal{C}_0$ of length $2n-4$. We first show that $G_0$ generates a self-orthogonal code $\mathcal{C}_0$ as follows. The inner product of the first row of $G_0$ with itself is equal to

$$\mathbf{a}_1 \cdot \mathbf{a}_1 + \alpha^2 \mathbf{a}_3 \cdot \mathbf{a}_3 + \beta^2 \mathbf{a}_4 \cdot \mathbf{a}_4 = -(1 + \alpha^2 + \beta^2) = 0,$$

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 $1 + \mathbf{a}_{i+2} \cdot \mathbf{a}_{i+2} = 0$. The inner product of the first row of $G_0$ with the second row is $\alpha\beta\mathbf{a}_3 \cdot \mathbf{a}_3 - \alpha\beta\mathbf{a}_4 \cdot \mathbf{a}_4 = 0$. 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 $|\mathcal{C}_0| = q^{n-2}$, so $\mathcal{C}_0$ is self-dual. First of all, we note that both vectors $\mathbf{v}_1 := \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4$ and $\mathbf{v}_2 := \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4$ in the first two rows of $G_0$ contain units. Otherwise, both vectors are zero vectors. Then $\mathbf{a}_1 = -(\alpha\mathbf{a}_3 + \beta\mathbf{a}_4)$, then $-1 = \mathbf{a}_1 \cdot \mathbf{a}_1 = (\alpha\mathbf{a}_3 + \beta\mathbf{a}_4) \cdot (\alpha\mathbf{a}_3 + \beta\mathbf{a}_4) = -(\alpha^2 + \beta^2) = 1$, i.e., $-1 = 1$ in $GF(q)$, which is impossible since $q$ is odd. So, $\mathbf{v}_1$ is a nonzero vector, and hence it contains a unit. Similarly, it is also true for $\mathbf{v}_2$. We can also show that $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent. If not, $\mathbf{v}_1 = c\mathbf{v}_2$ for some $c$ in $GF(q)^*$. Then by taking inner products of both sides with $\mathbf{a}_1$, we have $\mathbf{a}_1 \cdot \mathbf{v}_1 = c\mathbf{a}_1 \cdot \mathbf{v}_2$, so we get $-1 = 0$, a contradiction. Therefore it follows that $G_0$ is equivalent to a standard form of matrix $[I_{n-2} \mid * \,]$, so that $|\mathcal{C}_0| = q^{n-2}$, that is, $\mathcal{C}_0$ is self-dual.

Let $\mathbf{x}_1 = (0, \ldots, 0 \mid \mathbf{a}_1)$ and $\mathbf{x}_2 = (0, \ldots, 0 \mid \mathbf{a}_2)$ be row vectors of length $2n-4$. Then for $i = 1, 2$, $\mathbf{x}_i \cdot \mathbf{x}_i = \mathbf{a}_i \cdot \mathbf{a}_i = -1$ in GF$(q)$ and $\mathbf{x}_1 \cdot \mathbf{x}_2 =$

$\mathbf{a}_1 \cdot \mathbf{a}_2 = 0$ in GF$(q)$. Using the vectors $\mathbf{x}_1, \mathbf{x}_2$ and the self-dual code $\mathcal{C}_0$, we can construct a self-dual code $\mathcal{C}_1$ with the following $n \times 2n$ generator matrix $G_1$ by Proposition 2.2:

$$G_1 := \left[\begin{array}{cccc|ccc c}
1 & 0 & 0 & 0 & 0 & \cdots & 0 & \mathbf{a}_1 \\
0 & 1 & 0 & 0 & 0 & \cdots & 0 & \mathbf{a}_2 \\
\hline
1 & 0 & \alpha & \beta & 0 & \cdots & 0 & \mathbf{a}_1 + \alpha\mathbf{a}_3 + \beta\mathbf{a}_4 \\
0 & 1 & \beta & -\alpha & 0 & \cdots & 0 & \mathbf{a}_2 + \beta\mathbf{a}_3 - \alpha\mathbf{a}_4 \\
0 & 0 & 0 & 0 & & & & \mathbf{a}_5 \\
\vdots & \vdots & \vdots & \vdots & & I_{n-4} & & \vdots \\
0 & 0 & 0 & 0 & & & & \mathbf{a}_n
\end{array}\right].$$

Clearly $G_1$ is row equivalent to $G$. Hence the given code $\mathcal{C}$ is the same as the code $\mathcal{C}_1$ that is obtained from the code $\mathcal{C}_0$ by the building-up construction in Proposition 2.2. This completes the proof. □

*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:

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

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 $\mathbf{x}_1$ and $\mathbf{x}_2$ 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 1. New $[16, 8, 7]$ self-dual codes over $GF(7)$ using $C_{1,1}$ in [7]

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

**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 $\mathbf{x}_1$ and $\mathbf{x}_2$ 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

| # | $\mathbf{x_1} = (0\dots 0x_9\dots x_{20})$ | $\mathbf{x_2} = (0\dots 0x_9\dots x_{20})$ | $A_9, A_{10}, A_{11}, A_{12}$ |
|---|---|---|---|
| 1 | 2 6 2 3 2 1 6 1 6 1 0 0 | 4 4 3 5 3 2 1 1 6 1 0 0 | 948, 8496, 65520, 425484 |
| 2 | 2 2 5 1 3 1 6 1 6 1 0 0 | 3 5 4 4 6 4 2 1 6 1 0 0 | 894, 8802, 64572, 427236 |
| 3 | 6 4 4 1 4 1 6 1 6 1 0 0 | 3 6 2 6 1 2 2 1 6 1 0 0 | 936, 8436, 65580, 427704 |
| 4 | 2 6 2 3 5 1 6 1 6 1 0 0 | 5 3 3 4 4 2 1 1 6 1 0 0 | 882, 8592, 65544, 427086 |
| 5 | 5 6 5 4 5 1 6 1 6 1 0 0 | 2 1 3 5 1 5 1 1 6 1 0 0 | 774, 8706, 66204, 426204 |
| 6 | 1 4 2 2 1 2 6 1 6 1 0 0 | 3 3 5 6 3 4 2 1 6 1 0 0 | 948, 8466, 65520, 426306 |
| 7 | 4 5 3 4 4 2 6 1 6 1 0 0 | 1 3 5 1 2 1 2 1 6 1 0 0 | 936, 8982, 63516, 426750 |
| 8 | 1 6 4 6 4 3 6 1 6 1 0 0 | 2 1 6 3 2 6 2 1 6 1 0 0 | 966, 8502, 65148, 426792 |
| 9 | 1 3 3 1 1 3 6 1 6 1 0 0 | 5 2 2 3 2 4 2 1 6 1 0 0 | 966, 8700, 64500, 425730 |
| 10 | 4 6 1 6 3 4 6 1 6 1 0 0 | 5 1 6 3 6 2 2 1 6 1 0 0 | 846, 8796, 65448, 424134 |

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

[1] C. Aguilar Melchor and P. Gaborit, *On the classification of extremal* $[36,18,8]$ *binary self-dual codes*, IEEE Trans. Inform. Theory, **54** (2008), no. 10, 4743–4750.

[2] C. Aguilar-Melchor, P. Gaborit, J.-L. Kim, L. Sok, and P. Solé, *Classification of extremal and* $s$*-extremal binary self-dual codes of length* 38, IEEE Trans. Inform. Theory **58** (2012), no. 4, 2253–2262.

[3] R. Alfaro and K. Dhul-Qarnayn, *Constructing self-dual codes over* $\mathbb{F}_q[u]/(u^t)$, Des. Codes Cryptogr. **74** (2015), no. 2, 453–465.

[4] R. A. Brualdi and V. Pless, *Weight enumerators of self-dual codes*, IEEE Trans. Inform. Theory **37** (1991), no. 4, 1222–1225.

[5] J. Cannon and C. Playoust, *An Introduction to Magma*, University of Sydney, Sydney, Australia, 1994.

[6] S. T. Dougherty, *Shadow codes and weight enumerators*, IEEE Trans. Inform. Theory **41** (1995), no. 3, 762–768.

[7] T. A. Gulliver and M. Harada, *New optimal self-dual codes over* $GF(7)$, Graphs Combin. **15** (1999), no. 2, 175–186.

[8] T. A. Gulliver, M. Harada, and H. Miyabayashi, *Double circulant and quasi-twisted self-dual codes over* $\mathbb{F}_5$ *and* $\mathbb{F}_7$, Adv. Math. Commun. **1** (2007), no. 2, 223–238.

[9] T. A. Gulliver, J.-L. Kim, and Y. Lee, *New MDS or near-MDS self-dual codes*, IEEE Trans. Inform. Theory **54** (2008), no. 9, 4354–4360.

[10] S. Han, *A method for constructing self-dual codes over* $\mathbb{Z}_{2^m}$, Des. Codes Cryptogr. **75** (2015), no. 2, 253–262.

[11] S. Han, H. Lee, and Y. Lee, *Constructions of self-dual codes over* $\mathbb{F}_2 + u\mathbb{F}_2$, Bull. Korean Math. Soc. **49** (2012), no. 1, 135–143.

[12] M. Harada, *The existence of a self-dual* $[70, 35, 12]$ *code and formally self-dual codes*, Finite Fields Appl. **3** (1997), no. 2, 131–139.

[13] ———, personal communication on April 25, 2009.

[14] M. Harada and P. R. J. Östergård, *Self-dual and maximal self-orthogonal codes over* $\mathbb{F}_7$, Discrete Math. **256** (2002), no. 1-2, 471–477.

[15] W. C. Huffman, *On the classification and enumeration of self-dual codes*, Finite Fields Appl. **11** (2005), no. 3, 451–490.

[16] K. F. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York-Berlin, 1982.

[17] J.-L. Kim, *New extremal self-dual codes of lengths* $36, 38$ *and* $58$, IEEE Trans. Inform. Theory **47** (2001), 386–393.

[18] ———, http://maths.sogang.ac.kr/jlkim/preprints.html.

[19] J.-L. Kim and Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A **105** (2004), no. 1, 79–95.

[20] ———, *Construction of MDS Self-dual codes over Galois rings*, Des. Codes Cryptogr. **45** (2007), no. 2, 247–258.

[21] ———, *Self-dual codes using the building-up construction*, IEEE International Symposium on Information Theory, 2400–2402, June 28 - July 3, Seoul, Korea, 2009.

[22] H. Lee and Y. Lee, *Construction of self-dual codes over finite rings* $\mathbb{Z}_{p^m}$, J. Combin. Theory Ser. A **115** (2008), no. 3, 407–422.

[23] J. S. Leon, V. Pless, and N. J. A. Sloane, *On ternary self-dual codes of length 24*, IEEE Trans. Inform. Theory **27** (1981), no. 2, 176–180.

[24] V. Pless, *On the classification and enumeration of self-dual codes*, J. Combin. Theory Ser. A **18** (1975), no. 3, 313–335.

[25] V. Pless and V. Tonchev, *Self-dual codes over* $GF(7)$, IEEE Trans. Inform. Theory **33** (1987), no. 5, 723–727.

[26] E. Rains and N. J. A. Sloane, *Self-dual codes*, in: V. S. Pless, W. C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam. The Netherlands, 1998.

Jon-Lark Kim
Department of Mathematics
Sogang University
Seoul 121-742, Korea
*E-mail address*: jlkim@sogang.ac.kr

Yoonjin Lee
Department of Mathematics
Ewha Womans University
Seoul 120-750, Korea
*E-mail address*: yoonjinl@ewha.ac.kr