On self-dual codes over $\mathbb{F}_5$

Sunghyu Han
Department of Mathematics
University of Louisville
Louisville, KY 40292, USA
Email: sunghyu@yonsei.ac.kr
and
Jon-Lark Kim
Department of Mathematics
University of Louisville
Louisville, KY 40292, USA
Email: jl.kim@louisville.edu

February 2, 2008

Abstract

The purpose of this paper is to improve the upper bounds of the minimum distances of self-dual codes over $\mathbb{F}_5$ for lengths $22, 26, 28, 32 - 40$. In particular, we prove that there is no $[22, 11, 9]$ self-dual code over $\mathbb{F}_5$, whose existence was left open in 1982. We also show that both the Hamming weight enumerator and the Lee weight enumerator of a putative $[24, 12, 10]$ self-dual code over $\mathbb{F}_5$ are unique. Using the building-up construction, we show that there are exactly nine inequivalent optimal self-dual $[18, 9, 7]$ codes over $\mathbb{F}_5$ up to the monomial equivalence, and construct one new optimal self-dual $[20, 10, 8]$ code over $\mathbb{F}_5$ and at least 40 new inequivalent optimal self-dual $[22, 11, 8]$ codes.

Keywords: Optimal codes; self-dual codes; weight enumerators.

1 Introduction

Self-dual codes over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4$ have attracted a lot of attention due to their divisibility property, not shared by other self-dual codes. Nevertheless, self-dual codes over $\mathbb{F}_5$ were first classified up to length 12 by Leon, Pless and Sloan [13] in 1982 and have been extended by Gaborit, Gulliver, Harada, Miyabayashi, Otmani, and Östergård (see [5], [6], [7], [8], and [9]). Self-dual or self-orthogonal codes over $\mathbb{F}_5$ arise in the $\mathbb{F}_5$ span of Hadamard 3-designs of parameters $3-(4n, 2n, n-1)$ when $5 \mid n$ (see [1],[2]). In particular, the $\mathbb{F}_5$ span of skew Hadamard designs of parameters $3-(4n, 2n, n-1)$, where $5 \mid n$, always produce self-dual codes over $\mathbb{F}_5$ [12]. It was also remarked [13] that the Lee weight enumerator of a self-dual code over $\mathbb{F}_5$ is invariant under a three-dimensional representation of the icosahedral group. These invariants were also found by Hirzebruch in connection with cusps of the Hilbert modular surface associated with $\mathbb{Q}(\sqrt{5})$ and later this mystery was explained in a book [4].

In what follows, we give a brief introduction to self-dual codes over $\mathbb{F}_5$. We refer to [10] for any details. A linear $[n, k, d]$ code C means that C has length n, dimension k, and minimum distance d. A code C is *self-orthogonal* if $C \subset C^\perp$ under the usual inner product and *self-dual* if $C = C^\perp$. A self-dual code of length n with the highest minimum distance among self-dual codes of that length is called *optimal*. The *Lee weight* of $x \in \mathbb{F}_5$ is $\min\{x, 5-x\}$ and the *Lee weight* of a vector is the sum of the weights of its components. The Lee weight enumerator of C is $L(x, y, z) = \sum_{\mathbf{v} \in C} x^i y^j z^k$, where $\mathbf{v}$ has i 0's, j ± 1's and k ± 2's, and the Hamming weight enumerator is $W(x, y) = L(x, y, y)$.

Two linear codes C_1 and C_2 over $\mathbb{F}_5$ are *monomially equivalent* if there is a monomial matrix M over $\mathbb{F}_5$ such that $C_2 = C_1 M = \{cM \mid c \in C_1\}$. A monomial matrix over $\mathbb{F}_5$ which maps C to itself is called an *automorphism* of C. The set of all automorphisms of C is called the *automorphism group* $\mathrm{Aut}(C)$ of C. Since a monomial matrix over $\mathbb{F}_5$ does not map in general a self-orthogonal code to a self-orthogonal code, a $(1, -1, 0)$ monomial equivalence was used in [13] and [9] to classify all self-dual codes over $\mathbb{F}_5$ up to length 16. It appears that checking two codes of lengths ≥ 18 over $\mathbb{F}_5$ with respect to the $(1, -1, 0)$ monomial equivalence is much harder than checking them with respect to the $(\pm 1, \pm 2, 0)$ monomial equivalence. Hence in this paper we consider the $(\pm 1, \pm 2, 0)$ monomial equivalence, called the equivalence for brevity, and all codes are checked up to this equivalence.

Our main results are summarized as follows. In Section 2, we improve the upper bounds of the minimum distances of self-dual codes over $\mathbb{F}_5$ for lengths $22, 26, 28, 32-40$ by investigating Hamming weight enumerators and Lee weight enumerators of these codes. In particular, we show that there is no $[22, 11, 9]$ self-dual code over $\mathbb{F}_5$. The existence of such a code was left open in 1982. We also show that both the Hamming weight enumerator and the Lee weight enumerator of a putative $[24, 12, 10]$ self-dual code over $\mathbb{F}_5$ are unique. In Section 3, using the building-up construction [11], we show that there are exactly nine inequivalent optimal self-dual $[18, 9, 7]$ codes over $\mathbb{F}_5$, and construct one new optimal self-dual $[20, 10, 8]$ code over $\mathbb{F}_5$ and at least 40 new inequivalent optimal self-dual $[22, 11, 8]$ codes.

2 Investigation of Hamming and Lee weight enumerators

In this section we investigate Hamming and Lee weight enumerators of possible optimal self-dual codes over $\mathbb{F}_5$. We prove that there is no $[22, 11, 9]$ self-dual code over $\mathbb{F}_5$. So we determine that the optimal minimum distance of any self-dual code over $\mathbb{F}_5$ of length 22 is 8. The existence of a $[22, 11, 9]$ self-dual code over $\mathbb{F}_5$ was left open in [13]. We also prove that if there is a $[24, 12, 10]$ self-dual code over $\mathbb{F}_5$, then its Hamming weight enumerator and Lee weight enumerator are unique and we present them. Furthermore, we improve upper

Table 1: Optimal minimum distances of self-dual codes over $\mathbb{F}_5$

Length	d	N	Reference	Length	d	N	Reference
2	2	1	[13]	22	8	≥ 59	Sections 2, 3
4	2	1	[13]	24	$9-10$	≥ 1	[7, 13]
6	4	1	[13]	26	$9-10$	≥ 1	Section 2, [6, 8]
8	4	1	[13]	28	$10-11$	≥ 20	Section 2, [6, 8]
10	4	3	[13]	30	$10-12$	≥ 204	[6, 8]
12	6	1	[13]	32	$11-12$	≥ 1	Section 2, [6, 8]
14	6	3	[9, 13]	34	$11-12$	≥ 11	Section 2, [6, 8]
16	7	1	[9, 13]	36	$12-13$	≥ 1	Section 2, [6]
18	7	9	Section 3, [9]	38	$12-14$	≥ 1	Section 2, [6]
20	8	≥ 8	Section 3, [13]	40	$13-15$	≥ 1	Section 2, [6]

bounds of optimal minimum distances of self-dual codes over $\mathbb{F}_5$ of lengths $26, 28, 32-40$ in Table 10 in [6]. Our results are summarized in Table 1. In Table 1, the first and the fifth columns give code lengths, the second and the sixth columns give the optimal minimum distances, and the third and the seventh columns give the number of inequivalent optimal self-dual codes which are explained in Section 3. All the computations in this section are done using Maple software.

The following two theorems are crucial in this section and stated in [13].

Theorem 2.1 (Klein, Gleason and Pierce)**.** *The Lee weight enumerator of a self-dual code is a polynomial in the following α, β, and γ.*

$$\begin{aligned}
\alpha &= x^2 + 4yz,\\
\beta &= x^4yz - x^2y^2z^2 - x(y^5+z^5) + 2y^3z^3,\\
\gamma &= 5x^6y^2z^2 - 4x^5(y^5+z^5) - 10x^4y^3z^3 + 10x^3(y^6z+yz^6) + 5x^2y^4z^4\\
&\quad -10x(y^7z^2+y^2z^7) + 6y^5z^5 + y^{10} + z^{10}.
\end{aligned}$$

Theorem 2.2. *The Hamming weight enumerator of a self-dual code is an element of the ring*

$$\mathbb{C}[\overline{\alpha}, \overline{\beta}] \oplus \overline{\gamma}\mathbb{C}[\overline{\alpha}, \overline{\beta}] \oplus \overline{\gamma}^2\mathbb{C}[\overline{\alpha}, \overline{\beta}],$$

where

$$\begin{aligned}
\overline{\alpha} &= x^2 + 4y^2,\\
\overline{\beta} &= y^2(x-y)^2(x^2+2xy+2y^2),\\
\overline{\gamma} &= y^4(x-y)^4(5x^2+12xy+8y^2).
\end{aligned}$$

In the Lee weight enumerator, the number a_n of linearly independent invariants of degree n is given in [13] and the number is the coefficient of λ^n in the Taylor series expansion of

$$\frac{1}{(1-\lambda^2)(1-\lambda^6)(1-\lambda^{10})},$$

which for small n is given by

$$\begin{array}{rccccccccccccccccc} n: & 0 & 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 20 & 22 & 24 & 26 & 28 & 30 & 32 \\ a_n: & 1 & 1 & 1 & 2 & 2 & 3 & 4 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 13 & 14. \end{array}$$

Now we present an explicit formula for a_n in the following lemma.

Lemma 2.3.

$$a_n = \sum_{k=0}^{[\frac{n}{10}]} \left(\left[\frac{n-10k}{6} \right] + 1 \right).$$

Proof. a_n is the number of non-negative integer solutions of the following equation.

$$10k + 6j + 2i = n.$$

For each possible k, the number of solutions is

$$\left[\frac{n-10k}{6} \right] + 1,$$

and the claim follows. □

From Lemma 2.3, we see that a_n grows like $n^2/120$ for large n as it is indicated in [13]. Although a_n grows fast, we can still use Lee weight enumerators to improve the minimum distance bounds of self-dual codes over $\mathbb{F}_5$ for some large length n. This fact is explained in the following calculations.

Now we investigate Hamming and Lee weight enumerators of possible optimal self-dual codes over $\mathbb{F}_5$. Here is our strategy:

(i) Check a possible Hamming weight enumerator using Theorem 2.2. We determine some coefficients of the Hamming weight enumerator with a given minimum distance, and then check whether the remaining coefficients are non-negative integers or not. If this step does not give any contradiction, we move to step (ii).

(ii) Check a possible Lee weight enumerator using Theorem 2.1. First, we reduce the Lee weight enumerator into the Hamming weight enumerator by setting $W(x, y) = L(x, y, y)$. Given the minimum distance, we determine some coefficients of $L(x, y, z)$ using the Hamming weight enumerator and then plug in this information into the (original) Lee weight enumerator. Then we determine other coefficients of the Lee weight enumerators as many as possible. Finally we check whether the remaining coefficients are non-negative integers or not.

The highest minimum distance of a self-dual code over $\mathbb{F}_5$ is determined up to lengths $n = 20$ in [13] except length $n = 18$. For the length $n = 18$, it is determined that the highest minimum distance is 7 [9]. So we begin with possible Hamming and Lee weight enumerators with $n = 22$. In this section, a, b, c, s, t, u, and v denote undetermined parameters.

(i) $n = 22$

We have $d \leq 9$ from Table IV in [13] and know that there is a self-dual code with $d = 8$ from [7]. Hence we investigate the Hamming and Lee weight enumerators with $d = 9$. By check strategy (i), we have the following Hamming weight enumerator.

$$\mathbf{W}(1, y) = 1 + (-40a + 2816)y^9 + \cdots + (96a + 363136)y^{22}.$$

As this does not give a contradiction, we consider the following Lee weight enumerator by check strategy (ii).

$$\begin{aligned}
\mathbf{L}(x, y, z) &= \alpha^{11} - 44\alpha^8\beta + 429\alpha^5\beta^2 - 605\alpha^2\beta^3 + 11\alpha^6\gamma - 99\alpha^3\beta\gamma \\
&\quad +(-5s - 88)\beta^2\gamma + s\alpha\gamma^2. \\
&= x^{22} + x^{13}(-20sy^2z^7 + 1408y^2z^7 - 20sy^7z^2 + 1408y^7z^2) + \cdots \\
&\quad +x^2(-88z^{20} - 4sz^{20} + 378400y^5z^{15} + 232sy^5z^{15} + 4576528y^{10}z^{10} \\
&\qquad + 628sy^{10}z^{10} + 232sy^{15}z^5 + 378400y^{15}z^5 - 88y^{20} - 4sy^{20}) \\
&\quad +x(-60sy^3z^{18} + 6688y^3z^{18} + 969056y^8z^{13} - 220sy^8z^{13} + 969056y^{13}z^8 \\
&\qquad - 220sy^{13}z^8 - 60sy^{18}z^3 + 6688y^{18}z^3) \\
&\quad +(4syz^{21} + 28sy^6z^{16} + 32032y^6z^{16} + 299072y^{11}z^{11} + 32sy^{11}z^{11} \\
&\qquad + 28sy^{16}z^6 + 32032y^{16}z^6 + 4sy^{21}z).
\end{aligned}$$

In the expansion of the above Lee weight enumerator, one can see that the coefficient of x^2z^{20} is

$$-88 - 4s$$

and the coefficient of yz^{21} is

$$4s.$$

Since both cannot be non-negative integers, we conclude that the highest minimum distance d is 8.

(ii) $n = 24$

The highest possible minimum distance is 10 [13, Table IV]. Further there is a self-dual code with $d = 9$ [13]. So we investigate the Lee weight enumerator with $d = 10$. By check strategy (i), we have the following Hamming weight enumerator.

$$\mathbf{W}(1, y) = 1 + (64a + 13536)y^{10} + \cdots + (144a + 1167872)y^{24}.$$

Hence we have a possible Hamming weight enumerator. By check strategy (ii), we have the following Lee weight enumerator.

$$\begin{aligned}
\mathbf{L}(x, y, z) &= \alpha^{12} - 48\alpha^9\beta + 564\alpha^6\beta^2 - 1252\alpha^3\beta^3 + (25s - 864)\beta^4 + 12\alpha^7\gamma \\
&\quad -156\alpha^4\beta\gamma + (-10s + 288)\alpha\beta^2\gamma + s\alpha^2\gamma^2.
\end{aligned}$$

In the expansion of the Lee weight enumerator, the coefficient of x^2yz^{21} is

$$-32s + 1152,$$

and the coefficient of x^4z^{20} is
$$16s-576.$$
The possible value of s is 36, and the possible Hamming and Lee weight enumerators are unique as shown below.

$$\begin{aligned}\mathbf{W}(1,y) &= 1+15840y^{10}+29568y^{11}+212352y^{12}+620928y^{13}+2308416y^{14}\\ &+5325056y^{15}+13940784y^{16}+22800096y^{17}+39525024y^{18}+46451328y^{19}\\ &+49038528y^{20}+35560448y^{21}+20372352y^{22}+6766848y^{23}+1173056y^{24}. \end{aligned} \tag{1}$$

$$\begin{aligned}\mathbf{L}(x,y,z) &= x^{24}+528x^{14}z^{10}+14784x^{14}y^5z^5+528x^{14}y^{10}+14784x^{13}y^3z^8\\ &+14784x^{13}y^8z^3+2688x^{12}yz^{11}+206976x^{12}y^6z^6+2688x^{12}y^{11}z+310464x^{11}y^4z^9\\ &+310464x^{11}y^9z^4+51744x^{10}y^2z^{12}+2204928x^{10}y^7z^7+51744x^{10}y^{12}z^2+1408x^9z^{15}\\ &+2661120x^9y^5z^{10}+2661120x^9y^{10}z^5+1408x^9y^{15}+561792x^8y^3z^{13}\\ &+12817200x^8y^8z^8+561792x^8y^{13}z^3+16368x^7yz^{16}+11383680x^7y^6z^{11}\\ &+11383680x^7y^{11}z^6+16368x^7y^{16}z+2224992x^6y^4z^{14}+35075040x^6y^9z^9\\ &+2224992x^6y^{14}z^4+73920x^5y^2z^{17}+23151744x^5y^7z^{12}+23151744x^5y^{12}z^7\\ &+73920x^5y^{17}z^2+3489024x^4y^5z^{15}+42060480x^4y^{10}z^{10}+3489024x^4y^{15}z^5\\ &+128128x^3y^3z^{18}+17652096x^3y^8z^{13}+17652096x^3y^{13}z^8+128128x^3y^{18}z^3\\ &+1788864x^2y^6z^{16}+16794624x^2y^{11}z^{11}+1788864x^2y^{16}z^6+29568xy^4z^{19}\\ &+3353856xy^9z^{14}+3353856xy^{14}z^9+29568xy^{19}z^4+576y^2z^{22}+122496y^7z^{17}\\ &+926912y^{12}z^{12}+122496y^{17}z^7+576y^{22}z^2. \end{aligned} \tag{2}$$

We still have that the highest minimum distance d is 9 or 10.

(iii) $n=26$
We know that the highest minimum distance d satisfies $9 \le d \le 11$ [6, Table 10]. First we investigate the Hamming and Lee weight enumerators with $d=11$. By check strategy (i), we have the following Hamming weight enumerator.

$$\mathbf{W}(1,y)=1+\Big(-\frac{576}{5}a+\frac{222976}{5}\Big)y^{11}+\cdots+\Big(\frac{92142592}{25}+\frac{6208}{25}a\Big)y^{26}.$$

It is not certain whether the above Hamming weight enumerator gives a contradiction or not. By check strategy (ii), we have the following Lee weight enumerator.

$$\begin{aligned}\mathbf{L}(x,y,z) &= \alpha^{13}-52\alpha^{10}\beta+715\alpha^7\beta^2-2275\alpha^4\beta^3+25s\alpha\beta^4+13\alpha^8\gamma\\ &\quad -221\alpha^5\beta\gamma+(520-10s)\alpha^2\beta^2\gamma+s\alpha^3\gamma^2+\Big(-\frac{6136}{25}-\frac{64}{25}s\Big)\beta\gamma^2\\ &= x^{26}+(-156+16s)x^{16}z^{10}+(-32s+312)x^{16}y^5z^5+\cdots. \end{aligned}$$

Looking at the coefficient of $x^{16}z^{10}$, we have $-156+16s=0$, i.e., $s=\frac{39}{4}$ and

$$\mathbf{L}(x,y,z)=x^{26}+21736x^{15}y^3z^8+21736x^{15}y^8z^3-\frac{9672}{5}x^{14}yz^{11}+\cdots.$$

Hence we have non-integer coefficients in the Lee weight enumerator. Next we investigate the Hamming and Lee weight enumerators with $d = 10$. By check strategy (i) and (ii), we have the following Hamming and Lee weight enumerators.

$$\mathbf{W}(1, y) = 1 + (6136 + 64a + 25b)y^{10} + \cdots + (3717120 + 576a + 128b)y^{26}.$$

$$\begin{aligned}\mathbf{L}(x, y, z) &= \alpha^{13} - 52\alpha^{10}\beta + 715\alpha^7\beta^2 - 2275\alpha^4\beta^3 + 25s\alpha\beta^4 + 13\alpha^8\gamma \\ &\quad -221\alpha^5\beta\gamma + (520 - 10s)\alpha^2\beta^2\gamma + s\alpha^3\gamma^2 + t\beta\gamma^2 \\ &= x^{26} + (-156 + 16s)x^{16}z^{10} + (6448 + 32s + 25t)x^{16}y^5z^5 + \cdots .\end{aligned}$$

There is no contradiction in the Hamming and Lee weight enumerators. Therefore, the highest minimum distance d is 9 or 10.

(iv) $n = 28$
The highest minimum distance d satisfies $10 \leq d \leq 12$ from Table 10 in [6]. As above, we investigate the Hamming and Lee weight enumerators with $d = 12$. By check strategy (i), we have the following Hamming weight enumerator.

$$\mathbf{W}(1, y) = 1 + \Big(\frac{884912}{5} + \frac{5296}{25}a\Big)y^{12} + \cdots + \Big(\frac{11008}{25}a + \frac{59531776}{5}\Big)y^{28}.$$

It is not certain whether the Hamming weight enumerator gives a contradiction or not. By check strategy (ii), we have the following Lee weight enumerator.

$$\begin{aligned}\mathbf{L}(x, y, z) &= \alpha^{14} - 56\alpha^{11}\beta + 882\alpha^8\beta^2 - 3738\alpha^5\beta^3 + (1680 + 25s)\alpha^2\beta^4 + 14\alpha^9\gamma \\ &\quad -294\alpha^6\beta\gamma + (1008 - 10s)\alpha^3\beta^2\gamma + \Big(\frac{72}{5}s - 2968\Big)\beta^3\gamma + s\alpha^4\gamma^2 \\ &\quad +\Big(\frac{-136}{25}s + \frac{2408}{5}\Big)\alpha\beta\gamma^2 \\ &= x^{28} + (-280 + 16s)x^{18}z^{10} + \cdots .\end{aligned}$$

From the coefficient of $x^{18}z^{10}$, we have $-280 + 16s = 0$, i.e., $s = \frac{35}{2}$ and

$$\mathbf{L}(x, y, z) = x^{26} + \frac{39312}{5}x^{16}yz^{11} + \cdots .$$

We have non-integer coefficients in the Lee weight enumerator. Next we investigate the Hamming and Lee weight enumerators with $d = 11$. By check strategy (i), we have the following Hamming weight enumerator.

$$\mathbf{W}(1, y) = 1 + \Big(- 40b - \frac{1088}{5}a + 19264\Big)y^{11} + \cdots .$$

There is no contradiction in the Hamming weight enumerator. By check strategy (ii), we have the following Lee weight enumerator.

$$\begin{aligned}\mathbf{L}(x, y, z) &= \alpha^{14} - 56\alpha^{11}\beta + 882\alpha^8\beta^2 - 3738\alpha^5\beta^3 + (1680 + 25s)\alpha^2\beta^4 + 14\alpha^9\gamma \\ &\quad -294\alpha^6\beta\gamma + (1008 - 10s)\alpha^3\beta^2\gamma + (-\frac{64}{5}s - 560 - 5t)\beta^3\gamma + s\alpha^4\gamma^2 \\ &\quad +t\alpha\beta\gamma^2 \\ &= x^{28} + (-280 + 16s)x^{18}z^{10} + \cdots .\end{aligned}$$

We have $-280 + 16s = 0$, i.e., $s = \frac{35}{2}$ as the coefficient of $x^{18}z^{10}$ needs to be zero. Hence

$$\mathbf{L}(x, y, z) = x^{28} + (-20t + 7728)x^{17}y^3z^8 + \cdots .$$

This gives no contradiction to the Lee weight enumerator. Therefore the highest minimum distance d is 10 or 11.

(v) $n = 30$
The highest minimum distance d satisfies $10 \leq d \leq 12$ from Table 10 in [6]. First we investigate the Hamming and Lee weight enumerators with $d = 12$. By check strategy (i) and (ii), we have the following Hamming and Lee weight enumerators.

$$\mathbf{W}(1, y) = 1 + (66200 + 560a + 64b)y^{12} + \cdots + .$$

$$\begin{aligned}
\mathbf{L}(x, y, z) \quad = \quad & \alpha^{15} - 60\alpha^{12}\beta + 1065\alpha^9\beta^2 - 5705\alpha^6\beta^3 + (5280 + 25s)\alpha^3\beta^4 \\
& +(25t - 6912 + 136s)\beta^5 \\
& +\gamma(15\alpha^{10} - 375\alpha^7\beta + (1800 - 10s)\alpha^4\beta^2 + (-10t + 600 - 40s)\alpha\beta^3) \\
& +\gamma^2(s\alpha^5 + t\alpha^2\beta) \\
& +\gamma^3 u.
\end{aligned}$$

There is no contradiction in the Hamming and Lee weight enumerators. In other words, there are possible Hamming and Lee weight enumerators with $d = 12$. We still have that the highest minimum distance d is $10, 11$ or 12.

(vi) $n = 32$
We note that the highest minimum distance d satisfies $11 \leq d \leq 13$ from Table 10 in [6] and Theorem 1.1 in [8]. First we investigate the Lee weight enumerator with $d = 13$. By check strategy (i), we have the following Hamming weight enumerator.

$$\mathbf{W}(1, y) = 1 + \Big(\frac{1429248}{5} - 1408a - \frac{576}{5}b\Big)y^{13} + \cdots .$$

This Hamming weight enumerator is not enough to derive a contradiction. On the other hand, by check strategy (ii), we have the following Lee weight enumerator.

$$\begin{aligned}
\mathbf{L}(x, y, z) \quad = \quad & \alpha^{16} - 64\alpha^{13}\beta + 1264\alpha^{10}\beta^2 - 8240\alpha^7\beta^3 + (12160 + 25s)\alpha^4\beta^4 \\
& +(-4928 + 136s + 25t)\alpha\beta^5 \\
& +\gamma(16\alpha^{11} - 464\alpha^8\beta + (2944 - 10s)\alpha^5\beta^2 + (-1600 - 10t - 40s)\alpha^2\beta^3) \\
& +\gamma^2\Big(s\alpha^6 + t\alpha^3\beta + \Big(- \frac{25728}{25} - \frac{112}{5}s - \frac{64}{25}t - 5u\Big)\beta^2\Big) \\
& +\gamma^3 u\alpha \\
= \quad & x^{32} + (16s - 576)x^{22}z^{10} + \cdots .
\end{aligned}$$

It follows from the coefficient of $x^{22}z^{10}$ that $s = 36$ and

$$\mathbf{L}(x, y, z) = x^{32} + (16t + 2944)x^{20}yz^{11} + \cdots .$$

Similarly from the coefficient $x^{20}yz^{11}$, we have $t = -184$ and

$$\mathbf{L}(x,y,z) = x^{32} + \cdots + \Big(-32u - \frac{310592}{25}\Big)x^{12}z^{20} + \cdots + \Big(180u + \frac{1314816}{25}\Big)x^3y^2z^{27} + \cdots .$$

Both $-32u - \frac{310592}{25}$ and $180u + \frac{1314816}{25}$ cannot be non-negative. Next we investigate the Hamming weight enumerator with $d = 12$. By check strategy (i), we have the following Hamming weight enumerator.

$$\mathbf{W}(1,y) = 1 + (25728 + 560a + 25c + 64b)y^{12} + \cdots + .$$

There is no contradiction in the Hamming weight enumerator. By check strategy (ii), we have the following Lee weight enumerator.

$$\begin{aligned}
\mathbf{L}(x,y,z) &= \alpha^{16} - 64\alpha^{13}\beta + 1264\alpha^{10}\beta^2 - 8240\alpha^7\beta^3 + (12160 + 25s)\alpha^4\beta^4 \\
&\quad +(-4928 + 136s + 25t)\alpha\beta^5 \\
&\quad +\gamma(16\alpha^{11} - 464\alpha^8\beta + (2944 - 10s)\alpha^5\beta^2 + (-1600 - 10t - 40s)\alpha^2\beta^3) \\
&\quad +\gamma^2(s\alpha^6 + t\alpha^3\beta + u\beta^2) \\
&\quad +\gamma^3 v\alpha \\
&= x^{32} + (16s - 576)x^{22}z^{10} + \cdots .
\end{aligned}$$

We have $s = 36$ from the coefficient of $x^{22}z^{10}$. But we have no further information in the Lee weight enumerator. Thus the highest minimum distance d is 11 or 12.

(vii) $n = 34$

The highest minimum distance d satisfies $11 \le d \le 14$ from Table 10 in [6]. First we investigate the Hamming and Lee weight enumerator with $d = 14$. By check strategy (i), we calculate the Hamming weight enumerator. But it is not certain whether the Hamming weight enumerator gives a contradiction or not. By check strategy (ii), we have the following Lee weight enumerator.

$$\mathbf{L}(x,y,z) = x^{34} + (16s - 748)x^{24}z^{10} + \cdots .$$

This gives $s = \frac{187}{4}$ and we have

$$\mathbf{L}(x,y,z) = x^{34} + (16t + 5304)x^{22}yz^{11} + \cdots .$$

So $t = -\frac{663}{2}$ and we have

$$\mathbf{L}(x,y,z) = x^{34} + \cdots + \Big(16v - \frac{312596}{25}\Big)x^4z^{30} + \cdots + \Big(-320v + \frac{1092896}{25}\Big)xy^{29}z^4 + \cdots .$$

We have a contradiction. Next we investigate the Hamming and Lee weight enumerators with $d = 13$. By check strategy (i), we checked that the Hamming weight enumerator does not give any contradiction. By check strategy (ii), we have the following Lee weight enumerator.

$$\mathbf{L}(x,y,z) = x^{34} + (16s - 748)x^{24}z^{10} + \cdots .$$

Thus $s = \frac{187}{4}$ and we have

$$\mathbf{L}(x,y,z) = x^{34} + (16t + 5304)x^{22}yz^{11} + \cdots .$$

So $t = -\frac{663}{2}$ and we have

$$\begin{aligned}\mathbf{L}(x,y,z) &= x^{34} + \cdots + \Big(-4u - 24v - \frac{11084}{5}\Big)x^4z^{30} + \cdots + (8v+4u)x^2y^{31}z \\ &\quad + \cdots + 16vy^{32}z^2.\end{aligned}$$

We have a contradiction. Next we investigate the Hamming and Lee weight enumerators with $d = 12$. We checked that the Hamming and Lee weight enumerator do not give any contradiction. So the highest minimum distance d is 11 or 12.

(viii) $n = 36, 38, 40$
It follows from Table 10 in [6] that the highest minimum distance d satisfies $12 \leq d \leq 15, 12 \leq d \leq 16, 13 \leq d \leq 17$ for self-dual codes over $\mathbb{F}_5$ with $n = 36, 38, 40$ respectively. Using the same method as above, we have checked that there is no self-dual code over $\mathbb{F}_5$ with the parameters [36, 18, 15], [36, 18, 14], [38, 19, 16], [38, 19, 15], [40, 20, 17], and [40, 20, 16]. We have also checked that there are possible Hamming and Lee weight enumerators for self-dual [36, 18, 13], [38, 19, 14] and [40, 20, 15] codes over $\mathbb{F}_5$. Therefore, for the lengths $36, 38, 40$, the highest minimum distance d is $12 - 13, 12 - 14, 13 - 15$, respectively.

We summarize our theorems as follows.

Theorem 2.4. *There is no self-dual* $[22, 11, 9]$ *code over* $\mathbb{F}_5$. *The highest minimum distance of self-dual codes of length* 22 *is* 8.

Theorem 2.5. *If there is a self-dual* $[24, 12, 10]$ *code over* $\mathbb{F}_5$, *the Hamming and Lee weight enumerators are unique and given by (1), (2) respectively.*

Theorem 2.6. *There are no self-dual codes over* $\mathbb{F}_5$ *with parameters* $[26, 13, 11]$, $[28, 14, 12]$, $[32, 16, 13]$, $[34, 17, 14]$, $[34, 17, 13]$, $[36, 18, 15]$, $[36, 18, 14]$, $[38, 19, 16]$, $[38, 19, 15]$, $[40, 20, 17]$, *and* $[40, 20, 16]$. *The highest minimum distances of self-dual codes over* $\mathbb{F}_5$ *of lengths* 26, 28, 32, 34, 36, 38, 40 *are* $9-10$, $10-11$, $11-12$, $11-12$, $12-13$, $12-14$, $13-15$, *respectively.*

Remark 2.7. We expect that the method in this section can be used for the self-dual codes over $\mathbb{F}_5$ with length $n > 40$ and that the upper bound of the highest minimum distance of Table 10 in [6] might be improved with increasing computational complexity.

3 Construction of optimal codes

The classification of self-dual codes over $\mathbb{F}_5$ of lengths up to 16 was done in [9, 13] with respect to the $(1, -1, 0)$ monomial equivalence. We have checked that all the $(1, -1, 0)$ monomially inequivalent self-dual codes of each length up to 16 in [9, 13] are also inequivalent with respect to the $(\pm 1, \pm 2, 0)$ monomial equivalence.

In this section, we construct optimal self-dual codes over $\mathbb{F}_5$ with code length $n = 18, 20, 22$ by the building-up construction [11]. For $n = 18$, we find all inequivalent optimal codes. For $n = 20$, we find one new optimal code. For $n = 22$, we find 40 new inequivalent optimal codes. We have stated the number of inequivalent optimal codes in Table 1. All the computations in this section are done using Magma [3]. We start with the following building-up theorem.

Theorem 3.1 ([11]). *Assume that q is a power of an odd prime such that $q \equiv 1 \pmod 4$. Let c be in $\mathbb{F}_q$ such that $c^2 = -1$ in $\mathbb{F}_q$. Let $G_0 = (L|R) = (\mathbf{l}_i|\mathbf{r}_i)$ be a generator matrix (not necessarily in standard form) of a Euclidean self-dual code C_0 over $\mathbb{F}_q$ of length $2n$, where $\mathbf{l}_i$ and $\mathbf{r}_i$ are the rows of the matrices L and R, respectively, for $1 \le i \le n$. Let $\mathbf{x} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n})$ be a vector in $\mathbb{F}_q^{2n}$ with $\mathbf{x} \cdot \mathbf{x} = -1$ in $\mathbb{F}_q$. Suppose that $y_i = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n}) \cdot (\mathbf{l}_i|\mathbf{r}_i)$ for $1 \le i \le n$. Then the following matrix*

$$G = \left[\begin{array}{cc|cccccc} 1 & 0 & x_1 & \cdots & x_n & x_{n+1} & \cdots & x_{2n} \\ \hline -y_1 & cy_1 & & & & & & \\ \vdots & \vdots & & L & & & R & \\ -y_n & cy_n & & & & & & \end{array}\right]$$

generates a self-dual code C over $\mathbb{F}_q$ of length $2n + 2$.

Theorem 3.2 ([11]). *Assume that q is a power of an odd prime such that $q \equiv 1 \pmod 4$. Any Euclidean self-dual code C over $\mathbb{F}_q$ of length $2n + 2$ with minimum distance $d > 2$ is obtained from some Euclidean self-dual code C_0 over GF(q) of length $2n$ (up to permutation equivalence) by the construction method in Theorem 3.1.*

In the following theorem, we improve Theorem 3.1 from a computational view point.

Theorem 3.3. *Assume that q is a power of an odd prime such that $q \equiv 1 \pmod 4$. Let EC be the set of standard generator matrices of representatives for permutation equivalence (resp. $(1, -1, 0)$ monomial equivalence) classes for all the self-dual codes over $\mathbb{F}_q$ of length $2n$. Then we can construct all the self-dual codes over $\mathbb{F}_q$ of length $2n + 2$ with minimum distance $d > 2$ up to permutation equivalence (resp. $(1, -1, 0)$ monomial equivalence) by the building-up construction from the set EC using only $\mathbf{x} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n})$ with $x_1 = x_2 = \cdots = x_{n-1} = 0$.*

Proof. The main idea of this proof comes from the proof of Theorem 3.2. So we give a brief proof of Theorem 3.2 and then we give the proof of Theorem 3.3. For more details of the proof of Theorem 3.2, refer to [11].

Let C be a self-dual codes over $\mathbb{F}_q$ of length $2n + 2$ with minimum distance $d > 2$. There is a self-dual code $\mathcal{C}'$ which is permutation equivalent to C and has generator matrix $G = (I_{n+1}|A) = (\mathbf{e}_i|\mathbf{a}_i)$ where $\mathbf{e}_i$ and $\mathbf{a}_i$ are the rows of I_{n+1} (= the identity matrix) and A, respectively, for $1 \le i \le n + 1$. Let c be in $\mathbb{F}_q$ such that $c^2 = -1$ in $\mathbb{F}_q$. Then G is row equivalent to the following generator matrix

$$G' = \left[\begin{array}{c|c} \mathbf{e}_1 - c\,\mathbf{e}_2 & \mathbf{a}_1 - c\,\mathbf{a}_2 \\ -c\,\mathbf{e}_2 & -c\,\mathbf{a}_2 \\ \mathbf{e}_3 & \mathbf{a}_3 \\ \vdots & \vdots \\ \mathbf{e}_{n+1} & \mathbf{a}_{n+1} \end{array}\right].$$

Deleting the first two columns and the second row of G' produces an $n \times 2n$ matrix

$$G_0 = \left[\begin{array}{ccc|c} 0 & \cdots & 0 & \mathbf{a}_1 - c\,\mathbf{a}_2 \\ & & & \mathbf{a}_3 \\ & I_{n-1} & & \vdots \\ & & & \mathbf{a}_{n+1} \end{array}\right].$$

Then G_0 is a generator matrix of some Euclidean self-dual code C_0 of length $2n$. Let $\mathbf{x} = (0, \cdots, 0|\mathbf{a}_1)$ be a row vector of length $2n$. Using the vector $\mathbf{x}$ and G_0, we can construct a self-dual code with the following generator matrix G_1 by Theorem 3.1.

$$G_1 = \left[\begin{array}{cc|cccc} 1 & 0 & 0 & \cdots & 0 & \mathbf{a}_1 \\ \hline 1 & -c & 0 & \cdots & 0 & \mathbf{a}_1 - c\,\mathbf{a}_2 \\ 0 & 0 & & & & \mathbf{a}_3 \\ \vdots & \vdots & & I_{n-1} & & \vdots \\ 0 & 0 & & & & \mathbf{a}_{n+1} \end{array}\right].$$

In fact, G_1 is row equivalent to G. So, we can construct C using G_0 and $\mathbf{x}$ by the building-up construction up to permutation equivalence.

Now we give the proof of Theorem 3.3. There exists $G_0' \in EC$ such that G_0' is permutation equivalent (resp. $(1, -1, 0)$ monomial equivalent) to G_0. Since the first $n-1$ columns of both G_0 and G_0' are the same up to row interchanges, we can make G_0' up to row equivalence by applying a permutation (resp. a permutation and possible -1 scaling) only on the last $n+1$ coordinates of G_0. Let $\mathbf{x}'$ be the vector by applying the same permutation (resp. the permutation and the possible -1 scaling) only on the last $n+1$ coordinates of $\mathbf{x}$. Let C'' be the self-dual code by the building-up construction using G_0' and $\mathbf{x}'$. Then C'' is permutation equivalent (resp. $(1, -1, 0)$ monomial equivalent) to C. □

3.1 Length 18

Only one optimal $[18, 9, 7]$ self-dual code is known. This code is the unique pure double circulant $[18, 9, 7]$ self-dual code in [7].

We have found all inequivalent optimal self-dual codes using Theorem 3.3 and the generator matrices in <URL:http://www.tcs.hut.fi/∼pat/sd5/8–8>. There are exactly 9 inequivalent such codes. In Table 2, the first column denotes the constructed codes. The second column denotes the base matrices in the building-up construction. The number #534 denotes the 534th generator matrix in <URL:http://www.tcs.hut.fi/∼pat/sd5/8–8>. We list

Table 2: All optimal inequivalent $[18,9,7]$ self-dual codes over $\mathbb{F}_5$

codes	base matrices	$(x_n, x_{n+1}, \cdots, x_{2n})$	$W(a)$	$\lvert\mathrm{Aut}\rvert$
$C_{BU18,1}$	#534	(130222110)	-21	12
$C_{BU18,2}$	#534	(113033120)	-24	24
$C_{BU18,3}$	#534	(422330101)	-27	8
$C_{BU18,4}$	#534	(411110331)	-33	64
$C_{BU18,5}$	#533	(201422210)	-18	72
$C_{BU18,6}$	#532	(323424010)	-30	24
$C_{BU18,7}$	#532	(401323120)	-33	48
$C_{BU18,8}$	#531	(421320031)	-18	192
$C_{BU18,9}$	#528	(222031110)	-33	24

the matrices (I, G_i). In order to save space, only G_i is given using the form $g_1, g_2, \cdots, g_8$ where, g_j is the jth row.

$$G_{534} = 22211000, 42110110, 33311210, 30022101, 10343221, 20314212, 14443142, 01423342$$
$$G_{533} = 22211000, 42110110, 33311210, 14340101, 34412411, 00144412, 14331022, 22034142$$
$$G_{532} = 22211000, 42110110, 33311210, 14340101, 10012411, 43444412, 14331022, 41434142$$
$$G_{531} = 22211000, 43220100, 01302120, 00322011, 23340421, 14233402, 33030322, 04011142$$
$$G_{528} = 22211000, 43220100, 30102120, 40431011, 24441421, 42343402, 31333322, 00023142$$

The third column denotes $\mathbf{x}$ in the building-up construction. We take $x_1 = x_2 = \cdots = x_7 = 0$ as noted in Theorem 3.3. The fourth column denotes a in the weight enumerator of the following equation [8].

$$\begin{aligned} W_{5,18} = \quad & 1 + (-72 - 8a)y^7 + (2700 + 20a)y^8 + (5328 + 16a)y^9 + (27000 - 64a)y^{10} \\ & +(53928 - 24a)y^{11} + (187152 + 112a)y^{12} + (260568 + 56a)y^{13} \\ & +(457272 - 216a)y^{14} + (412224 + 64a)y^{15} + (361872 + 124a)y^{16} \\ & +(148320 - 104a)y^{17} + (36832 + 24a)y^{18}. \end{aligned}$$

The fifth column denotes the orders of the automorphism groups of the constructed codes.

We have checked that there is no optimal $[18,9,7]$ self-dual codes from the unique optimal $[16,8,7]$ self-dual code using the building-up construction. We have also checked that the unique pure double circulant self-dual $[18,9,7]$ code in [7] is equivalent to $C_{BU18,5}$.

Table 3: Optimal inequivalent $[20, 10, 8]$ self-dual codes over $\mathbb{F}_5$

code	$W(a)$	$\lvert\text{Aut}\rvert$	Reference	code	$W(a)$	$\lvert\text{Aut}\rvert$	Reference
Q_{20}	40	13680	[13]	$Q_{20,3}$	0	80	[8]
$C_{20,1}$	40	7680	[7]	$Q_{20,4}$	0	80	[8]
$C_{20,5}$	0	320	[7]	$Q_{20,5}$	0	160	[8]
QDC_{20}	40	11520	[5]	$C_{BU20,1}$	0	32	Section 3.2

We list generator matrix $(I, G_{BU18,i})$ for $C_{BU18,i}$.

$$
\begin{aligned}
G_{BU18,1} = \quad & 130222110, 143320201, 123134342, 244401244, 331020131, \\
& 232313230, 313002142, 020314212, 014443142 \\
G_{BU18,2} = \quad & 012110333, 140223031, 240042234, 324334431, 142204302, \\
& 312241422, 401400134, 302033033, 001423342 \\
G_{BU18,3} = \quad & 422330101, 413231432, 224002134, 441242323, 134234002, \\
& 434104314, 111211013, 020314212, 211234221 \\
G_{BU18,4} = \quad & 411110331, 430121022, 224002134, 441242323, 432443423, \\
& 434104314, 111211013, 222100341, 014443142 \\
G_{BU18,5} = \quad & 201422210, 342224314, 400232413, 114144202, 411332123, \\
& 131324243, 034412411, 433110320, 131310114 \\
G_{BU18,6} = \quad & 323424010, 232404301, 113140142, 401231023, 124240302, \\
& 100224243, 242320140, 220202141, 241144201 \\
G_{BU18,7} = \quad & 401323120, 430222044, 340403321, 042110110, 124240302, \\
& 241103330, 424133324, 134323004, 100210114 \\
G_{BU18,8} = \quad & 421320031, 411432222, 423200413, 142231242, 100313212, \\
& 203344240, 122301013, 014233402, 330013143 \\
G_{BU18,9} = \quad & 222031110, 411002101, 322220321, 443202013, 430134033, \\
& 140404103, 424423334, 442320310, 031333322
\end{aligned}
$$

By the above arguments, we have the following theorem.

Theorem 3.4. *There are exactly 9 inequivalent optimal self-dual* $[18, 9, 7]$ *codes over* $\mathbb{F}_5$ *up to the monomial equivalence.*

3.2 Length 20

There are 7 inequivalent previously known optimal $[20, 10, 8]$ self-dual codes. These are in Table 3. The second and the sixth columns in the Table 3 denote a in the weight enumerator of the following equation [8].

$$\begin{aligned} W_{5,20} = \quad & 1 + (1280+25a)y^8 + (3200-80a)y^9 + (24848-36a)y^{10} + (58560+360a)y^{11} \\ & +(248480-170a)y^{12} + (464960-680a)y^{13} + (1175840+700a)y^{14} \\ & +(1568000+472a)y^{15} + (2267240-935a)y^{16} + (1896720+120a)y^{17} \\ & +(1398960+480a)y^{18} + (541760-320a)y^{19} + (115776+64a)y^{20}. \end{aligned}$$

Remark 3.5. We have checked that $C_{20,7}$ in [7] is equivalent to Q_{20}, and $Q_{20,2}$ [8] is equivalent to QDC_{20}. It is interesting to note that the above seven inequivalent codes can be represented by the seven double circulant and quasi-twisted self-dual codes in [8] up to equivalence.

We construct a new inequivalent $[20, 10, 8]$ code, denoted by $C_{BU20,1}$. We give a generator matrix $(I, G_{BU20,2})$ for this code, where

$$\begin{aligned} G_{BU20,1} = \quad & 0223431010, 4124344443, 4023213431, 4412304332, 0403240433 \\ & 1102140314, 2444303122, 1201012032, 4140132101, 2034140111. \end{aligned}$$

The above code $C_{BU20,1}$ is constructed using the building-up construction with (I, G), where

$$\begin{aligned} G = \quad & 013112023, 402203424, 403240433, 112241222, 414000443, \\ & 211113440, 130031243, 004342432, 040404142, \end{aligned} \tag{3}$$

and the vector $\mathbf{x} = (x_1, \cdots, x_{18})$ where $(x_9, \cdots, x_{18}) = (0223431010)$ and the rest coordinates are given zeros.

In summary, we have the following theorem.

Theorem 3.6. *There are at least 8 inequivalent optimal self-dual* $[20, 10, 8]$ *codes over* $\mathbb{F}_5$.

Remark 3.7. We have the following question. "Are there two self-dual codes over $\mathbb{F}_5$ which are equivalent with respect to the $(\pm 1, \pm 2, 0)$ monomial equivalence but are not equivalent with respect to the $(1, -1, 0)$ monomial equivalence?" By our Magma calculation there are no such codes up to code length $n = 16$. But we find two such codes with code length $n = 18$. One is $C_{BU18,4}$ and the other is the code $C'_{BU18,4}$ with generator matrix (I, G) in Equation (3). We can check that the two codes are equivalent with respect to the $(\pm 1, \pm 2, 0)$ monomial equivalence by Magma. And we have checked that $C_{BU18,4}$ does not generate any self-dual codes by the building-up construction which are $(\pm 1, \pm 2, 0)$ monomially equivalent to $C_{BU20,1}$. This implies that $C_{BU18,4}$ and $C'_{BU18,4}$ are not equivalent with respect to the $(1, -1, 0)$ monomial equivalence.

3.3 Length 22

Previously there were 19 inequivalent optimal $[22, 11, 8]$ self-dual codes. Ten of them are

$$\begin{aligned} & (f_1; 1; 4), (f_1; 1; 6), (f_1; 1; 17), (f_1; 1; 21), (f_1; 1; 27), \\ & (f_1; 1; 28), (f_1; 1; 34), (f_1; 1; 44), (f_1; 1; 59), (f_1; 1; 73) \end{aligned}$$

Table 4: New optimal inequivalent $[22, 11, 8]$ self-dual codes over $\mathbb{F}_5$ by the building-up construction from $C_{20,1}$

codes	$(x_{10}, x_{11}, \cdots, x_{20})$	$W(a, b)$	$\lvert\mathrm{Aut}\rvert$
$C_{BU22,1}$	(33131120000)	$(44, 8)$	24
$C_{BU22,2}$	(22431420000)	$(36, 8)$	4
$C_{BU22,3}$	(12214141000)	$(36, 8)$	8
$C_{BU22,4}$	(23220441000)	$(36, 8)$	4
$C_{BU22,5}$	(43232110000)	$(32, 8)$	4
$C_{BU22,6}$	(44332310000)	$(32, 8)$	4
$C_{BU22,7}$	(24213420000)	$(28, 8)$	8
$C_{BU22,8}$	(32120241000)	$(28, 8)$	8
$C_{BU22,9}$	(31144341000)	$(28, 8)$	4
$C_{BU22,10}$	(23312011000)	$(28, 8)$	8
$C_{BU22,11}$	(11134211000)	$(28, 8)$	8
$C_{BU22,12}$	(21434320000)	$(24, 8)$	8
$C_{BU22,13}$	(12134141000)	$(24, 8)$	4
$C_{BU22,14}$	(34033241000)	$(24, 8)$	4
$C_{BU22,15}$	(42230241000)	$(24, 8)$	8
$C_{BU22,16}$	(14431241000)	$(24, 8)$	4
$C_{BU22,17}$	(40223341000)	$(24, 8)$	4
$C_{BU22,18}$	(22021341000)	$(24, 8)$	8
$C_{BU22,19}$	(20323441000)	$(24, 8)$	8
$C_{BU22,20}$	(22342401000)	$(24, 8)$	8
$C_{BU22,21}$	(22431301000)	$(24, 8)$	4
$C_{BU22,22}$	(44431311000)	$(24, 8)$	8
$C_{BU22,23}$	(20342311000)	$(24, 8)$	16
$C_{BU22,24}$	(12112141000)	$(20, 8)$	4
$C_{BU22,25}$	(20332111000)	$(20, 8)$	12
$C_{BU22,26}$	(12101322000)	$(20, 8)$	24
$C_{BU22,27}$	(10114234100)	$(20, 8)$	24
$C_{BU22,28}$	(31023241000)	$(16, 8)$	32
$C_{BU22,29}$	(43244411000)	$(16, 8)$	8
$C_{BU22,30}$	(11104234100)	$(8, 8)$	24
$C_{BU22,31}$	(23142301000)	$(5, 11)$	8
$C_{BU22,32}$	(32331101000)	$(1, 11)$	24
$C_{BU22,33}$	(13031321000)	$(1, 11)$	12
$C_{BU22,34}$	(21302201100)	$(0, 8)$	64
$C_{BU22,35}$	(22312401000)	$(-3, 11)$	8
$C_{BU22,36}$	(33242332000)	$(-7, 11)$	32
$C_{BU22,37}$	(12124302000)	$(-7, 11)$	32
$C_{BU22,38}$	(44202342000)	$(-11, 11)$	96
$C_{BU22,39}$	(40334144100)	$(-11, 11)$	24
$C_{BU22,40}$	(42223344100)	$(-11, 11)$	24

in [6]. The other 9 are bordered double circulant self-dual codes,

$$B_{22,1}, B_{22,2}, B_{22,3}, B_{22,4}, B_{22,5}, B_{22,6}, B_{22,7}, B_{22,8}, B_{22,9}$$

in [8].

Remark 3.8. In fact, three inequivalent pure double circulant [22,11,9] self-dual codes and three inequivalent bordered double circulant [22,11,9] self-dual codes are presented in [7]. These are updated as 10 inequivalent pure double circulant [22,11,9] self-dual codes and 9 inequivalent bordered double circulant [22,11,9] self-dual codes [8]. The ten pure double circulant codes in [8] are equivalent to the ten codes in [6]. Specifically, the following are equivalent pair.

$$\begin{aligned}
&(P_{22,1}, (f_1; 1; 59)), (P_{22,2}, (f_1; 1; 73)), (P_{22,3}, (f_1; 1; 17)), (P_{22,4}, (f_1; 1; 28)),\\
&(P_{22,5}, (f_1; 1; 6)), (P_{22,6}, (f_1; 1; 4)), (P_{22,7}, (f_1; 1; 44)), (P_{22,8}, (f_1; 1; 34)),\\
&(P_{22,9}, (f_1; 1; 21)), (P_{22,10}, (f_1; 1; 27)).
\end{aligned}$$

So all the previously known 19 $[22, 11, 8]$ self-dual codes can be represented by the 19 double circulant self-dual codes in [8] up to equivalence.

We have tried some building-up construction from $C_{20,1}$ in [7]. ($C_{20,1}$ is the pure double circulant codes with generator matrix $G = (I, R)$. And the first row of R is (2442212000).) We found 40 new inequivalent optimal self-dual codes. These codes are shown in Table 4. The third column in the Table 4 denotes a, b in the weight enumerator of the following equation [8].

$$\begin{aligned}
W_{5,22} = \quad & 1 + (440 + 5a + 25b)y^8 + (2112 - 8a - 80b)y^9 + (17864 - 20a + 64b)y^{10}\\
& +(48576 + 16a + 40b)y^{11} + (255552 + 82a - 314b)y^{12}\\
& +(596640 - 40a + 760b)y^{13} + (1939696 - 164a + 20b)y^{14}\\
& +(3443968 + 40a - 2248b)y^{15} + (6994108 + 253a + 1865b)y^{16}\\
& +(8766296 - 64a + 2008b)y^{17} + (10750520 - 240a - 3260b)y^{18}\\
& +(8358592 + 72a + 160b)y^{19} + (5348992 + 180a + 1984b)y^{20}\\
& +(1938816 - 144a - 1280b)y^{21} + (365952 + 32a + 256b)y^{22}.
\end{aligned}$$

In summary, we have the following theorem.

Theorem 3.9. *There are at least 59 inequivalent optimal self-dual* $[22, 11, 8]$ *codes over* $\mathbb{F}_5$.

We expect that there are many more inequivalent optimal $[22, 11, 8]$ self-dual codes.

4 Conclusion

We have made use of the Hamming weight enumerators and the Lee weight enumerators of self-dual codes over $\mathbb{F}_5$ to improve the best known upper bounds for the minimum distances of self-dual codes over $\mathbb{F}_5$ for lengths $22, 26, 28, 32 - 40$. In particular, we have solved one of open problems left in [13], proving that there is no $[22, 11, 9]$ self-dual code over $\mathbb{F}_5$. Using the building-up construction, we construct new optimal self-dual codes of lengths $18, 20$, and 22, providing new examples other than the known double circulant codes or quasi-twisted codes [8].

ACKNOWLEDGMENT

The authors wish to thank the reviewers for valuable remarks which helped us to improve this article. S. Han was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD)(KRF-2007-357-C00010), and J.-L. Kim was supported in part by a Project Completion Grant from the University of Louisville.

References

[1] Assmus Jr. EF, Key JD (1992) Hadamard Matrices and Their Designs: A Coding-Theoretic Approach. Transactions of the American Mathematical Society. 330:269–293.

[2] Assmus Jr. EF, Key JD (1992) Designs and their Codes. Cambridge.

[3] Cannon J, Playoust C (1994) An Introduction to Magma, University of Sydney, Sydney, Australia.

[4] Ebelin W (2002) Lattices and Codes. Friedrich Vieweg and Sohn Verlag.

[5] Gaborit P (2002) Quadratic double circulant codes over fields. J. Combin. Theory Ser. A 97:85–107.

[6] Gaborit P, Otmani A (2003) Experimental constructions of self-dual codes. Finite Fields Appl. 9:372–394.

[7] Gulliver TA, Harada M (2000) Double circulant self-dual codes over $GF(5)$. Ars Combin. 56:3–13.

[8] Gulliver TA, Harada M, Miyabayashi H (2007) Double circulant self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$. Advances in Math. of Communications 1:223–238.

[9] Harada M, Östergård PRJ (2003) On the classification of self-dual codes over $\mathbb{F}_5$. Graphs and Combin. 19:203–214.

[10] Huffman WC, Pless VS (2003) Fundamentals of Error-correcting Codes. Cambridge: Cambridge University Press.

[11] Kim J-L, Lee Y (2004) Euclidean and Hermitian self-dual MDS codes over large finite fields. J. Combin. Theory Ser. A 105:79–95.

[12] Kim J-L, Solé P (2007) Skew Hadamard designs and their codes, to appear in Designs, Codes, and Cryptography.

[13] Leon JS, Pless V, Sloane NJA (1982) Self-dual codes over GF(5). J. Combin. Theory Ser. A 32:178–194.