Finite Fields and Their Applications 18 (2012) 613–633

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Construction of quasi-cyclic self-dual codes

Sunghyu Han [a,1], Jon-Lark Kim [b], Heisook Lee [c], Yoonjin Lee [c,*,2]

[a] School of Liberal Arts, Korea University of Technology and Education, Cheonan 330-708, South Korea
[b] Department of Mathematics, University of Louisville, Louisville, KY 40292, USA
[c] Department of Mathematics, Ewha Womans University, Seoul 120-750, South Korea

ARTICLE INFO

Article history:
Received 2 February 2011
Revised 23 December 2011
Accepted 25 December 2011
Available online 11 January 2012
Communicated by W. Cary Huffman

MSC:
94B05
94B15

Keywords:
Quasi-cyclic self-dual code
Cubic code
Quintic code
Building-up construction

ABSTRACT

There is a one-to-one correspondence between ℓ-quasi-cyclic codes over a finite field $\mathbb{F}_q$ and linear codes over a ring $R = \mathbb{F}_q[Y]/(Y^m - 1)$. Using this correspondence, we prove that every ℓ-quasi-cyclic self-dual code of length $m\ell$ over a finite field $\mathbb{F}_q$ can be obtained by the *building-up* construction, provided that $\mathrm{char}(\mathbb{F}_q) = 2$ or $q \equiv 1 \pmod 4$, m is a prime p, and q is a primitive element of $\mathbb{F}_p$. We determine possible weight enumerators of a binary ℓ-quasi-cyclic self-dual code of length $p\ell$ (with p a prime) in terms of divisibility by p. We improve the result of Bonnecaze et al. (2003) [3] by constructing new binary cubic (i.e., ℓ-quasi-cyclic codes of length 3ℓ) optimal self-dual codes of lengths $30, 36, 42, 48$ (Type I), 54 and 66. We also find quasi-cyclic optimal self-dual codes of lengths 40, 50, and 60. When $m = 5$, we obtain a new 8-quasi-cyclic self-dual $[40, 20, 12]$ code over $\mathbb{F}_3$ and a new 6-quasi-cyclic self-dual $[30, 15, 10]$ code over $\mathbb{F}_4$. When $m = 7$, we find a new 4-quasi-cyclic self-dual $[28, 14, 9]$ code over $\mathbb{F}_4$ and a new 6-quasi-cyclic self-dual $[42, 21, 12]$ code over $\mathbb{F}_4$.

0. Introduction

Self-dual codes have been one of the most interesting classes of linear codes over finite fields and in general over finite rings. They interact with other areas including lattices [12,13], invariant

* Corresponding author.
E-mail addresses: sunghyu@kut.ac.kr (S. Han), jl.kim@louisville.edu (J.-L. Kim), hsllee@ewha.ac.kr (H. Lee), yoonjinl@ewha.ac.kr (Y. Lee).
[1] S. Han was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), which is supported by the Ministry of Education, Science and Technology (2010-0007232).
[2] Y. Lee is supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2011-0003516).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.12.006

Table 1
Binary extremal cubic self-dual codes of lengths up to 66.

Length n	Highest min. wt.	No. of extremal cubic self-dual codes	Ref.
6	2	1	Section 3
12	4	1	Section 3
18	4	1	Section 3
24	8	1	Section 3
30	6	8	Section 3 [3,36]
36	8	13	Section 3 [3,15,25]
42	8	1569	Section 3 [3,5,6]
48	10	$\geqslant 4$	Section 3 [3]
54	10	$\geqslant 7$	Section 3 [3]
60	12	$\geqslant 3$	[3]
66	12	$\geqslant 7$	Section 3 [3]

theory [37], and designs [1]. On the other hand, quasi-cyclic codes have been one of the most practical classes of linear codes. Linear codes which are quasi-cyclic and self-dual simultaneously are an interesting class of codes, and this class of codes is our main topic. We refer to [28] for a basic discussion of codes.

From the module theory over rings, quasi-cyclic codes can be considered as modules over the group algebra of the cyclic group. For a special ring $R = \mathbb{F}_q[Y]/(Y^m - 1)$, Ling and Solé [32,33] consider linear codes over a ring R, where m is a positive integer coprime to q, and they use a correspondence ϕ between (self-dual) quasi-cyclic codes over $\mathbb{F}_q$ and (self-dual, respectively) linear codes over R. We call quasi-cyclic codes over $\mathbb{F}_q$ *cubic*, *quintic*, or *septic* codes depending on $m = 3, 5,$ or 7, respectively. Bonnecaze et al. [3] studied binary cubic self-dual codes, and Bracco et al. [7] considered binary quintic self-dual codes.

In this paper, we focus on construction and classification of quasi-cyclic self-dual codes over a finite field $\mathbb{F}_q$ under the usual permutation or monomial equivalence. We note that the equivalence under the correspondence ϕ may not be preserved; two inequivalent linear codes over a ring R under a permutation equivalence may correspond to two equivalent quasi-cyclic codes over a finite field $\mathbb{F}_q$ under a permutation or monomial equivalence. Hence, we first construct all self-dual codes over the ring R using a building-up construction. Rather than considering the equivalence of these codes over R, we consider the equivalence of their corresponding quasi-cyclic self-dual codes over $\mathbb{F}_q$ to get a complete classification of quasi-cyclic self-dual codes over $\mathbb{F}_q$.

We prove that every ℓ-quasi-cyclic self-dual code of length $m\ell$ over $\mathbb{F}_q$ can be obtained by the *building-up construction*, provided that $\mathrm{char}(\mathbb{F}_q) = 2$ or $q \equiv 1 \pmod 4$, m is a prime p, and q is a primitive element of $\mathbb{F}_p$. Our result shows that the building-up construction is a complete method for constructing all ℓ-quasi-cyclic self-dual codes of length $m\ell$ over $\mathbb{F}_q$ subject to certain conditions of m and q. We determine possible weight enumerators of a binary ℓ-quasi-cyclic self-dual code of length $p\ell$ with p a prime in terms of divisibility by p.

By employing our building-up constructions, we classify binary cubic self-dual codes of lengths up to 24, and we construct binary cubic optimal self-dual codes of lengths $30, 36, 42, 48$ (Type I), 54 and 66. We point out that the advantage of our construction is that we can classify all binary cubic self-dual codes in a more efficient way without searching for all binary self-dual codes. We summarize our result on the classification of binary cubic extremal self-dual codes in Table 1. We also give a complete classification of all binary quintic self-dual codes of even lengths $5\ell \leqslant 30$, and construct such optimal codes of lengths 40, 50, and 60. For various values of m and q, we obtain quintic self-dual codes of length 5ℓ over $\mathbb{F}_3$ and $\mathbb{F}_4$ and septic self-dual codes of length 7ℓ over $\mathbb{F}_2$, $\mathbb{F}_4$, and $\mathbb{F}_5$ which are optimal or have the best known parameters. In particular, we find a new quintic self-dual $[40, 20, 12]$ code over $\mathbb{F}_3$ and a new quintic self-dual $[30, 15, 10]$ code over $\mathbb{F}_4$. We also obtain a new septic self-dual $[28, 14, 9]$ code over $\mathbb{F}_4$ and a new septic self-dual $[42, 21, 12]$ code over $\mathbb{F}_4$.

This paper is organized as follows. Section 1 contains some basic notations and definitions, and Section 2 presents the building-up construction method of quasi-cyclic self-dual codes over finite fields. In Section 3, we construct binary quasi-cyclic self-dual codes, and we find the cubic codes and quintic codes. In Section 4, we construct quasi-cyclic self-dual codes over various fields such as $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$, and $\mathbb{F}_5$, and we obtain the cubic codes, the quintic codes and the septic codes. We use Magma [8] for computations.

1. Preliminaries

We briefly introduce some basic notions about quasi-cyclic self-dual codes. For more detailed description, we refer to [32,33].

Let R be a commutative ring with identity. A *linear code* C of length n over R is defined to be an R-submodule of R^n; in particular, if R is a finite field $\mathbb{F}_q$ of order q, then C is a vector subspace of $\mathbb{F}_q^n$ over $\mathbb{F}_q$. The dual of C is denoted by $C^\perp$, C is *self-orthogonal* if $C \subseteq C^\perp$, and *self-dual* if $C = C^\perp$. We denote the standard shift operator on R^n by T. A linear code C is said to be *quasi-cyclic of index* ℓ or ℓ*-quasi-cyclic* if it is invariant under T^ℓ. A 1-quasi-cyclic code means a cyclic code. Throughout this paper, we assume that the index ℓ divides the code length n.

Let m be a positive integer coprime to the characteristic of $\mathbb{F}_q$, $\mathbb{F}_q[Y]$ be a polynomial ring, and $R := R(\mathbb{F}_q, m) = \mathbb{F}_q[Y]/(Y^m - 1)$. Then it is shown [32] that there is a one-to-one correspondence between ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of length ℓm and linear codes over R of length ℓ, and the correspondence is given by the map ϕ defined as follows. Let C be a quasi-cyclic code over $\mathbb{F}_q$ of length lm and index l with a codeword $\mathbf{c}$ denoted by $\mathbf{c} = (c_{00}, c_{01}, \ldots, c_{0,\ell-1}, c_{10}, \ldots, c_{1,\ell-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,\ell-1})$. Let ϕ be a map $\phi : {\mathbb{F}_q}^{\ell m} \to R^\ell$ defined by

$$\phi(\mathbf{c}) = \big(\mathbf{c}_0(Y), \mathbf{c}_1(Y), \ldots, \mathbf{c}_{\ell-1}(Y)\big) \in R^\ell,$$

where $\mathbf{c}_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in R$, for $j = 0, \ldots, \ell - 1$. We denote by $\phi(C)$ the image of C under ϕ.

A *conjugation* map $^-$ on R is defined as the map that sends Y to $Y^{-1} = Y^{m-1}$ and acts as the identity map on $\mathbb{F}_q$, and it is extended $\mathbb{F}_q$-linearly. On R^ℓ, we define the *Hermitian inner product* by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=0}^{\ell-1} x_j \overline{y_j}$ for $\mathbf{x} = (x_0, \ldots, x_{\ell-1})$ and $\mathbf{y} = (y_0, \ldots, y_{\ell-1})$.

It is proved [32] that for $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^{\ell m}$, $T^{\ell k}(\mathbf{a}) \cdot \mathbf{b} = 0$ for all $0 \leqslant k \leqslant m - 1$ if and only if $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$, where $\cdot$ denotes the standard Euclidean inner product. From this fact, it follows that $\phi(C)^\perp = \phi(C^\perp)$, where $\phi(C)^\perp$ is the dual of $\phi(C)$ with respect to the Hermitian inner product, and $C^\perp$ is the dual of C with respect to the Euclidean inner product. In particular, a quasi-cyclic code C over $\mathbb{F}_q$ is self-dual with respect to the Euclidean inner product if and only if $\phi(C)$ is self-dual over R with respect to the Hermitian inner product [32]. Two linear codes C_1 and C_2 over R are *equivalent* if there is a permutation of coordinates of C_1 sending C_1 to C_2. Similarly, two linear codes over $\mathbb{F}_q$ are equivalent if there is a monomial mapping sending one to another. Note that the equivalence of two linear codes C_1 and C_2 over R implies a permutation equivalence of quasi-cyclic linear codes $\phi^{-1}(C_1)$ and $\phi^{-1}(C_2)$ over $\mathbb{F}_q$, but not conversely in general.

2. Construction of quasi-cyclic self-dual codes

Throughout this paper, let $R = \mathbb{F}_q[Y]/(Y^m - 1)$, and self-dual (or self-orthogonal) codes over R means self-dual (or self-orthogonal) codes with respect to the Hermitian inner product.

We begin with the following lemma regarding the length of self-dual codes.

Lemma 2.1. *Let* $R = \mathbb{F}_q[Y]/(Y^m - 1)$.

(i) *If* $\mathrm{char}(\mathbb{F}_q) = 2$ *or* $q \equiv 1 \pmod 4$, *then there exists a self-dual code over* R *of length* ℓ *if and only if* $2 \mid \ell$.
(ii) *If* $q \equiv 3 \pmod 4$, *then there exists a self-dual code over* R *of length* ℓ *if and only if* $4 \mid \ell$.

Proof. To prove (i) and (ii), we observe the following. Suppose C is a self-dual code of length ℓ over R. We may assume that C_1 in the decomposition of C in [32, Theorem 4.2] is a Euclidean self-dual code over $\mathbb{F}_q$ of length ℓ.

For (i), suppose that $\mathrm{char}(\mathbb{F}_q) = 2$ or $q \equiv 1 \pmod 4$. By the above observation, $2 \mid \ell$. Conversely, let $\ell = 2k$. We take a Euclidean self-dual code over $\mathbb{F}_q$ of length 2 using the following generator matrix: $[1\ c]$, where $c^2 = -1$. We can see that this matrix generates a self-dual code C over R of length 2. Then the direct sum of the k copies of C is a self-dual code over R of length $\ell = 2k$.

For (ii), let $q \equiv 3 \pmod 4$. It is well known [41, 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. Hence by the above observation, $4 \mid \ell$. Conversely, let $\ell = 4k$ for some positive integer k. It is known [29, p. 281] that if q is a power of an odd prime with $q \equiv 3 \pmod 4$, then there exist nonzero α and β in $\mathbb{F}_q$ such that $\alpha^2 + \beta^2 + 1 = 0$ in $\mathbb{F}_q$. We take a Euclidean self-dual code over $\mathbb{F}_q$ of length 4 with the following generator matrix:

$$G = \begin{bmatrix} 1 & 0 & \alpha & \beta \\ 0 & 1 & -\beta & \alpha \end{bmatrix},$$

where $\alpha^2 + \beta^2 + 1 = 0$ in $\mathbb{F}_q$. We can see that this matrix generates a self-dual code C over R of length 4. Then the direct sum of the k copies of C is a self-dual code over R of length $\ell = 4k$. $\square$

The following theorem is the building-up constructions for self-dual codes over R, equivalently, ℓ-quasi-cyclic self-dual codes over $\mathbb{F}_q$ for any odd prime power q. The proof is similar to that of [30], so the proof is omitted.

Theorem 2.2. *Let C_0 be a self-dual code over R of length 2ℓ and $G_0 = (\mathbf{r}_i)$ be a $k \times 2\ell$ generator matrix for C_0, where $\mathbf{r}_i$ is the ith row of G_0, $1 \leqslant i \leqslant k$.*

(i) *Assume that* $\mathrm{char}(\mathbb{F}_q) = 2$ *or* $q \equiv 1 \pmod 4$.
Let c be in R such that $c\bar{c} = -1$, $\mathbf{x}$ be a vector in $R^{2\ell}$ with $\langle \mathbf{x}, \mathbf{x} \rangle = -1$, and $y_i = -\langle \mathbf{r}_i, \mathbf{x} \rangle$ for $1 \leqslant i \leqslant k$. Then the following matrix

$$G = \left[\begin{array}{cc|c} 1 & 0 & \mathbf{x} \\ \hline y_1 & cy_1 & \mathbf{r}_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & \mathbf{r}_k \end{array}\right]$$

generates a self-dual code C over R of length $2\ell + 2$.

(ii) *Assume that $q \equiv 3 \pmod 4$ and ℓ is even.*
Let α and β be in R such that $\alpha\overline{\alpha} + \beta\overline{\beta} = -1$ and $\alpha\overline{\beta} = \overline{\alpha}\beta$. Let $\mathbf{x}_1$ and $\mathbf{x}_2$ be vectors in $R^{2\ell}$ such that $\langle \mathbf{x}_1, \mathbf{x}_2 \rangle = 0$ in R and $\langle \mathbf{x}_i, \mathbf{x}_i \rangle = -1$ in R for each $i = 1, 2$. For each i, $1 \leqslant i \leqslant k$, let $s_i = -\langle \mathbf{r}_i, \mathbf{x}_1 \rangle$, $t_i = -\langle \mathbf{r}_i, \mathbf{x}_2 \rangle$, 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

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

generates a self-dual code C over R of length $2\ell + 4$.

The following theorem shows that the converses of Theorem 2.2 hold for self-dual codes over R with some restrictions. It can be proved in a similar way as in [30], thus we omit the proof. The *rank* of a code C means the minimum number of generators of C. The *free rank* of C is defined to be the maximum of the ranks of free R-submodules of C.

Theorem 2.3.

(i) *Assume that* $\mathrm{char}(\mathbb{F}_q) = 2$ *or* $q \equiv 1 \pmod 4$.
Any self-dual code C over R of length $2\ell + 2$ with free rank at least two is obtained from some self-dual code over R of length 2ℓ by the construction method in Theorem 2.2(i).

(ii) *Assume that* $q \equiv 3 \pmod 4$ *and ℓ is even.*
Any self-dual code C over R of length $2\ell + 4$ with free rank at least four is obtained from some self-dual code over R of length 2ℓ by the construction method in Theorem 2.2(ii).

As seen in Theorem 2.3, there is some restriction (i.e. minimum free rank) for the converses. In order to release this restriction, in Theorem 2.7 we find certain conditions of m and q under which the converse is true without the restriction. The following lemma is needed for the proof of Lemma 2.6 and Theorem 2.7, and it finds the explicit criterion for $Y^m - 1$ to have exactly two irreducible factors over $\mathbb{F}_q[Y]$, and it also characterizes the unit group of R.

Lemma 2.4.

(i) *$Y^m - 1$ has exactly two irreducible factors over $\mathbb{F}_q[Y]$ if and only if m is a prime p and q is a primitive element of $\mathbb{F}_p$.*

(ii) *Assume that the condition in* (i) *holds. Then the unit group R^* of R consists of $f(Y)$ in $\mathbb{F}_q[Y]$ of degree $\leqslant p-1$ such that $f(1) \in \mathbb{F}_q^*$ and $\Phi_p(Y) \nmid f(Y)$, where $\Phi_p(Y) = Y^{p-1} + Y^{p-2} + \cdots + Y + 1$. Equivalently, $f(Y)$ in $\mathbb{F}_q[Y]$ of degree $\leqslant p-1$ is not a unit in R if and only if $Y - 1 \mid f(Y)$ or $\Phi_p(Y) \mid f(Y)$ in $\mathbb{F}_q[Y]$. Hence we have $|R^*| = (q-1)(q^{p-1}-1)$.*

(iii) *Assume that the condition in* (i) *holds. Then the ideal $\langle Y - 1\rangle$ of R has cardinality q^{p-1} and the ideal $\langle \Phi_p(Y)\rangle$ of R has cardinality q. That is,* $\dim_{\mathbb{F}_q}\langle \phi^{-1}(Y-1)\rangle = p-1$ *and* $\dim_{\mathbb{F}_q}\langle \phi^{-1}(\Phi_p(Y))\rangle = 1$.

Proof. For (i), we note that a primitive mth root of unity ζ belongs to some extension field of $\mathbb{F}_q$ as $(m,q) = 1$. There exists a prime divisor p of m. If $p \neq m$ then $Y^m - 1 = (Y-1)\Phi_p(Y)(\frac{Y^m-1}{Y^p-1})$ has at least three irreducible factors over $\mathbb{F}_q$. Thus, if $Y^m - 1$ has exactly two irreducible factors over $\mathbb{F}_q[Y]$, then we should have $m = p$. If $m = p$, then $\Phi_p(Y)$ is irreducible if and only if all the roots of $\Phi_p(Y)$ are Galois conjugates over $\mathbb{F}_q$, or equivalently, q is a primitive element of $\mathbb{F}_p$. The other direction is obvious.

To show (ii), by the Chinese Remainder Theorem we have the following canonical isomorphism

$$\psi : R \to \mathbb{F}_q[Y]/(Y-1) \oplus \mathbb{F}_q[Y]/\big(\Phi_p(Y)\big).$$

Then $f(Y)$ is a unit of R if and only if $\psi(f(Y))$ is a unit, equivalently, $f(1) \in \mathbb{F}_q^*$ and $\Phi_p(Y) \nmid f(Y)$, so the result follows.

(iii) is clear. $\square$

Lemma 2.5. *Let F_1 and F_2 be finite fields, and consider a ring $\mathcal{R} = F_1 \times F_2$. Let $e_i \in F_i^{\times}$ for $i = 1, 2$ and $f_1 = (e_1, 0)$, $f_2 = (0, e_2) \in R$. Then every linear code over $\mathcal{R}$ has a generator matrix* (*up to permutation equivalence*) *as follows*:

$$G = \begin{bmatrix} I_{k_1} & A_{12} & A_{13} & A_{14} & A_{15} \\ O & f_1 I_{k_2} & f_2 M_{k_2} & B_{24} & B_{25} \\ O & O & O & \alpha I_{k_3} & \alpha D_{35} \end{bmatrix}, \tag{1}$$

where $\alpha \in \{f_1, f_2\}$, I_{k_i} is the $k_i \times k_i$ identity matrix $i = 1, 2, 3$, M_{k_2} is a $k_2 \times k_2$ diagonal matrix with elements in the main diagonal not contained in $\mathcal{R} f_1$, all the elements of B_{24} and B_{25} are 0 or nonunits in $\mathcal{R}$, A_{1j} ($j = 2, 3, 4, 5$), D_{35} are matrices of appropriate size over $\mathcal{R}$.

Proof. We note that $\mathcal{R} = F_1 \times F_2 = Rf_1 \oplus Rf_2$ is a commutative ring with unity $1_{\mathcal{R}} = (1,1)$, zero $0_{\mathcal{R}} = (0,0)$ and $f_1 f_2 = 0_{\mathcal{R}}$. In fact, the group $\mathcal{R}^*$ of units of $\mathcal{R}$ is $\mathcal{R} - (\mathcal{R}f_1 \cup \mathcal{R}f_2) = F_1^\times \times F_2^\times$, there exist $r_1, r_2 \in \mathcal{R}$ such that $1_{\mathcal{R}} = r_1 f_1 + r_2 f_2$, and $Rf_i = \langle f_i \rangle$ is a maximal ideal of $\mathcal{R}$ for $i = 1, 2$.

Let G_0 be a generator matrix for C. We first note that there are four possible cases for each row of G_0. The first case is that a row contains a unit of $\mathcal{R}$, and the second one is that a row has no units but it contains both a nonzero element in $\langle f_1 \rangle$ and a nonzero element in $\langle f_2 \rangle$. The third case is that a row consists of only the elements in $\langle f_1 \rangle$, and the last case is that a row contains only the elements in $\langle f_2 \rangle$. Below we transform G_0 into G by column permutation and elementary row operations.

We notice that G_0 can be transformed into G_1 such that the first k_1 rows (respectively the first k_1 columns) of G_1 are equal to the first k_1 rows (respectively the first k_1 columns) of G in Eq. (1). Deleting the first k_1 rows and the first k_1 columns of G_1, we make G_2. We may assume that there is no unit component in G_2 (up to row equivalence); otherwise we can increase k_1.

Now assume that the first row of G_2 is $(g_1 f_1, g_2 f_2, \ldots)$ with $g_1 = (a_1, b_1) \notin \langle f_2 \rangle$ and $g_2 = (a_2, b_2) \notin \langle f_1 \rangle$. Since $g_1 = (a_1, b_1) \notin \langle f_2 \rangle$, we have $a_1 \neq 0$, that is, $a_1 \in F_1^\times$, and similarly, $b_2 \in F_2^\times$. Thus there exists $\tilde{g}_1 = (a_1^{-1}, c_2)$ in $\mathcal{R}^*$ such that $g_1 f_1 \tilde{g}_1 = f_1$. Multiplying the first row of G_2 by $\tilde{g}_1$, we may assume that the first row of G_2 is $(f_1, \tilde{g}_2 f_2, \ldots)$ with $\tilde{g}_2 := \tilde{g}_1 g_2 \notin \langle f_1 \rangle$.

We claim that all the components of the first column of G_2 are in $\langle f_1 \rangle$. Suppose $g = (a, b)$ is in the first column of G_2 with $g \notin \langle f_1 \rangle$. If $g \notin \langle f_2 \rangle$, then g is a unit, which is impossible. Thus, $g \in \langle f_2 \rangle$. This leads to a unit component in G_2 (up to row equivalence).

We therefore may assume that all the components of the first column after f_1 are zero by elementary row operations. Likewise each component of the second column of G_2 is in $\langle f_2 \rangle$. Suppose G_2 has the following form

$$\begin{bmatrix} f_1 & \tilde{g}_2 f_2 & \cdots \\ 0 & \tilde{g}_2' f_2 & \cdots \\ \vdots & \vdots & \end{bmatrix}$$

for some $\tilde{g}_2 = (\tilde{a}_2, \tilde{b}_2)$, $\tilde{g}_2' = (a_2', b_2') \notin \langle f_1 \rangle$, where we have $\tilde{b}_2, b_2' \in F_2^\times$. We add $(0, -b_2'/\tilde{b}_2) \times$ (the first row of G_2) to the second row of G_2. Then we have

$$\begin{bmatrix} f_1 & \tilde{g}_2 f_2 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \end{bmatrix}.$$

In this way, we may assume that the components of the second column after f_2 are all zero. Now assume that the second row of G_2 is $(0, 0, f_1, g_3 f_2, \ldots)$ for some $g_3 \notin \langle f_1 \rangle$. In other words, G_2 has the following form

$$\begin{bmatrix} f_1 & \tilde{g}_2 f_2 & \beta & \gamma & \cdots \\ 0 & 0 & f_1 & g_3 f_2 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \end{bmatrix}.$$

By the same reasoning as above, we may assume that $\beta = \gamma = 0$. Repeating the above process, after some possible column changes, we may thus assume that G_2 has the following form for some k_2.

$$\begin{bmatrix} f_1 I_{k_2} & f_2 M_{k_2} & B \\ O & O & D \end{bmatrix}.$$

The rest of the theorem follows in a similar way. $\square$

Lemma 2.6. *Let m be a prime p and q be a primitive element of $\mathbb{F}_p$. Then a linear code C over the ring $R = \mathbb{F}_q[Y]/(Y^m - 1)$ has a generator matrix G in the following form (up to permutation equivalence):*

$$G = \begin{bmatrix} I_{k_1} & A_{12} & A_{13} & A_{14} & A_{15} \\ O & (Y-1)I_{k_2} & \Phi_p(Y)M_{k_2} & B_{24} & B_{25} \\ O & O & O & \alpha I_{k_3} & \alpha D_{35} \end{bmatrix}, \tag{2}$$

where I_{k_i} is the $k_i \times k_i$ identity matrix $i = 1, 2, 3$, M_{k_2} is a $k_2 \times k_2$ diagonal matrix with nonzero elements in the main diagonal over $\mathbb{F}_q$, all the elements of B_{24} and B_{25} are 0 or nonunits, and α is $Y - 1$ or $\Phi_p(Y)$.

Proof. As m is a prime p and q is a primitive element of $\mathbb{F}_p$, $Y^m - 1$ has exactly two irreducible factors $Y - 1$ and $\Phi_p(Y)$ by Lemma 2.4(i). From Lemma 2.4 and Lemma 2.5, the result follows immediately. □

The following theorem shows that the building-up construction is a complete method for constructing all ℓ-quasi-cyclic self-dual codes of length $m\ell$ over $\mathbb{F}_q$ subject to certain conditions of m and q.

Theorem 2.7. *Every self-dual code C over $R = \mathbb{F}_q[Y]/(Y^m - 1)$ of length $2\ell + 2$ can be obtained by the building-up construction given in Theorem 2.2 (up to permutation equivalence), provided that* $\operatorname{char}(\mathbb{F}_q) = 2$ *or $q \equiv 1 \pmod 4$, m is a prime p, and q is a primitive element of $\mathbb{F}_p$.*

Equivalently, every ℓ-quasi-cyclic self-dual code of length $m\ell$ over $\mathbb{F}_q$ can be obtained as the image under ϕ^{-1} of a code over R which is obtained by the building-up construction subject to the same conditions of m and q as above.

Proof. Let C be a self-dual code of length 2ℓ over R with a generator matrix of the form in (2). Then we first show the following properties:

(i) $k_3 = 0$ and $k_1 + k_2 = \ell$,
(ii) $k_1 \geqslant 1$,
(iii) $k_1 \geqslant 2$ if $2\ell \geqslant 4$.

(i) By the Chinese Remainder Theorem, we have

$$R = \frac{\mathbb{F}_q[Y]}{(Y^p - 1)} \cong \frac{\mathbb{F}_q[Y]}{(Y - 1)} \oplus \frac{\mathbb{F}_q[Y]}{\Phi_p(Y)} \cong \mathbb{F}_q \oplus \mathbb{F}_q^{p-1}.$$

Define $\Psi_1 : R \to \mathbb{F}_q$ and $\Psi_2 : R \to \mathbb{F}_q^{p-1}$ as natural projections. We extend Ψ_1 componentwise:

$$\Psi_1 : M(R, m, n) \to M(\mathbb{F}_q, m, n),$$

where $M(R, m, n)$ and $M(\mathbb{F}_q, m, n)$ are the $m \times n$ matrix spaces over R and $\mathbb{F}_q$, respectively. Similarly we extend Ψ_2. By Theorem 4.2 in [32], $C = C_1 \oplus C_2$, where C_1 is a self-dual code over $\mathbb{F}_q$ and C_2 is a self-dual code over $\mathbb{F}_q^{p-1}$. By the proof of Theorem 6.1 in [33], $\Psi_1(G)$ and $\Psi_2(G)$ are generator matrices for C_1 and C_2, respectively, so we have $\operatorname{rank}(\Psi_1(G)) = \ell = \operatorname{rank}(\Psi_2(G))$. If $\alpha = Y - 1$, then $\operatorname{rank}(\Phi_1(G)) = k_1 + k_2$ and $\operatorname{rank}(\Phi_2(G)) = k_1 + k_2 + k_3$, which shows that $k_3 = 0$ and $k_1 + k_2 = \ell$. It is also shown similarly for the other case $\alpha = \Phi_p(Y)$.

(ii) We claim that there is a unit in the first component of some codeword in C. Suppose there is no unit in the first component of all codewords in C. Then we assume that all the first components are in $\langle Y - 1\rangle$ or $\langle \Phi_p(Y)\rangle$. This is because the first components cannot contain both a nonzero element in $\langle Y - 1\rangle$ and a nonzero element $\langle \Phi_p(Y)\rangle$, since some R-linear combination of those two elements is a unit in R by Lemma 2.4(ii). If all the first components are in $\langle Y-1\rangle$, then $(\Phi_p(Y),0,0,\dots,0)$ is in $C^\perp = C$ which is a contradiction. Similarly, if all the first components are in $\langle \Phi_p(Y)\rangle$, then $(Y-1,0,0,\dots,0)$ is in $C^\perp = C$ which is a contradiction. Therefore there is a unit in the first component of some codeword in C. Hence $k_1 \geqslant 1$.

(iii) From (i) and (ii) we have $k_1 \geqslant 1$ and $k_3 = 0$. We then first observe that the column size of the last block of G in Eq. (2) is exactly k_1 as $k_1 + k_2 = \ell$. To get a contradiction, suppose $k_1 = 1$. Then by Lemma 2.6, G is of the following form with $\gamma, \beta_i \in R$ $(1 \leqslant i \leqslant \ell-1)$;

$$G = \begin{bmatrix} 1 & A_{12} & A_{13} & \gamma \\ 0 & & & \beta_1 \\ \vdots & (Y-1)I_{k_2} & \Phi_p(Y)M_{k_2} & \vdots \\ 0 & & & \beta_{\ell-1} \end{bmatrix}.$$

Let $\mathbf{r}_2$ be the second row of G with $\mathbf{r}_2 = (0, Y-1, 0, \dots, 0, c_1\Phi_p(Y), 0, \dots, 0, \beta_1)$ for some c_1 in $\mathbb{F}_q^*$. Then

$$0 = \langle \mathbf{r}_2, \mathbf{r}_2\rangle = (Y-1)(\overline{Y}-1) + c_1^2\Phi_p(Y)\overline{\Phi_p(Y)} + \beta_1\overline{\beta_1}.$$

But, we can see that $h(Y) := (Y-1)(\overline{Y}-1) + c_1^2\Phi_p(Y)\overline{\Phi_p(Y)} = (2 - Y - \overline{Y}) + c_1^2\Phi_p(Y)\overline{\Phi_p(Y)}$ is a unit in R by Lemma 2.4; in fact, $h(1) = p^2c_1^2 \in \mathbb{F}_q^*$ and $2 - Y - \overline{Y} = -(Y^{p-1} + Y - 2)$ is not divisible by $\Phi_p(Y)$, and so $\Phi_p(Y) \nmid h(Y)$. Therefore, $\beta_1\overline{\beta_1}$ is a unit in R, and hence β_1 is a unit. This is a contradiction because β_1 is 0 or a nonunit by Eq. (2). Therefore $k_1 \geqslant 2$.

Now suppose that C is a self-dual code over R of length $2\ell + 2$. Then $k_1 \geqslant 2$ by (iii) above. Hence Eq. (2) gives a generator matrix in (i) of Theorem 2.3. Thus it follows from (i) of Theorem 2.3 that C is obtained from some self-dual code over R of length 2ℓ by the construction in (i) of Theorem 2.2. □

What follows shows that in the binary cubic self-dual codes we can eliminate the restriction for the converse of the construction in Theorem 2.2 in other words, it shows that any binary cubic self-dual codes can be found by the building-up construction in Theorem 2.2.

Corollary 2.8. *Let $R = \mathbb{F}_2[Y]/(Y^3 - 1)$. Let C be a self-dual code over R of length $2\ell + 2$. Then C is obtained from some self-dual code over R of length 2ℓ by the construction method in Theorem 2.2 (up to equivalence).*

3. Construction of binary quasi-cyclic self-dual codes

In this section we construct binary cubic quasi-cyclic self-dual codes and binary quintic quasi-cyclic self-dual codes by using Theorem 2.2.

3.1. Binary cubic self-dual codes

A. Bonnecaze et al. [3] have studied binary cubic self-dual codes, and they have given a partial list of binary cubic self-dual codes of lengths $\leqslant 72$ by combining binary self-dual codes and Hermitian self-dual codes.

Using Corollary 2.8, we find a complete classification of binary cubic self-dual codes of lengths up to 24 (up to permutation equivalence). To save space, we post the classification up to $n = 30$ in [31].

We note that the classification of binary self-dual codes of lengths up to 32 was given by Pless and Sloane [39] and Conway, Pless and Sloane [10]; hence it is possible to classify all binary cubic self-dual codes of length 32.

Below is the summary.

Theorem 3.1. *Up to permutation equivalence*:

(i) *There is a unique binary cubic self-dual code of length* 6.
(ii) *There are exactly two binary cubic self-dual codes of length* 12*, one of which is extremal.*
(iii) *There are exactly three binary cubic self-dual codes of length* 18*, one of which is extremal.*
(iv) *There are exactly sixteen binary cubic self-dual codes of length* 24*, where the extended Golay code and the odd Golay code of length* 24 *are obtained.*

For even $\ell \geqslant 10$ we have tried to construct as many codes as possible due to computational complexity. Recall that we have summarized the number of extremal cubic self-dual codes of lengths $\leqslant 66$ in Table 1.

Using the following lemma, we determine possible weight enumerators of a binary ℓ-quasi-cyclic self-dual code of length $p\ell$ with p a prime.

Lemma 3.2. *(See [34, Chapter 16, Section 6].) Let C be a binary code and H any subgroup of* $\mathrm{Aut}(C)$*. If A_i is the total number of codewords in C of weight i, and $A_i(H)$ is the number of codewords which are fixed by some non-identity element of H, then*

$$A_i \equiv A_i(H) \pmod{|H|}.$$

We remark that in [34, Chapter 16, Section 6] $A_i(H)$ is defined as the number of codewords which are fixed by some element of H. Since the identity of H always fixes any codeword, we need to consider some non-identity element of H. Thus the codewords of weight i can be divided into two classes, those fixed by some *non-identity* element of H, and the rest. Then just follow the proof of [34, Chapter 16, Section 6].

Corollary 3.3. *Let C be a binary ℓ-quasi-cyclic self-dual code of length $p\ell$ with p a prime. If the weight i is not divisible by p, then A_i is divisible by p. In particular, A_d is a multiple of p if d is not divisible by p.*

Proof. We know from [32, Proposition A.1] that if p denotes a prime, a binary code C of length ℓp is ℓ-quasi-cyclic if and only if $\mathrm{Aut}(C)$ contains a fixed-point free (fpf) permutation of order p. Hence C contains an fpf permutation σ of order p. Let $H = \langle\sigma\rangle$ whose order is p. Since σ is an fpf of order p and any codeword of weight i with $p \nmid i$ cannot be fixed by any non-identity element of H, we have $A_i(H) = 0$. Therefore by the above lemma, $A_i \equiv 0 \pmod{p}$. □

(i) $\ell = 10$, $[30, 15, 6]$ codes.

There are three weight enumerators for self-dual $[30, 15, 6]$ codes [11]:

$$\begin{aligned} W_1 &= 1 + 19y^6 + 393y^8 + 1848y^{10} + 5192y^{12} + \cdots, \\ W_2 &= 1 + 27y^6 + 369y^8 + 1848y^{10} + 5256y^{12} + \cdots, \\ W_3 &= 1 + 35y^6 + 345y^8 + 1848y^{10} + 5320y^{12} + \cdots. \end{aligned}$$

It is known [10,11] that there are precisely three codes with W_1, a unique code with W_2, and precisely nine codes with W_3. Only two cubic self-dual $[30, 15, 6]$ codes are given in [3]. We have constructed three codes with W_1 whose group orders are 576, 1152, 18 432 respectively. We have also constructed five codes with W_3 whose group orders are 30, 192, 1440, 40 320, 645 120. To save space, we post these codes in [31]. In fact, these are all the cubic self-dual $[30, 15, 6]$ codes by the following calculation.

On the other hand, we have noticed that Munemasa has posted all binary self-dual $[30, 15]$ codes in [36]. Let C_i be the ith code in his list. By Magma, C_i has $d = 6$ if and only if $i \in$

$\{11, 61, 98, 119, 174, 184, 217, 350, 379, 397, 419, 487, 697\}$. We have further checked that the three codes with W_1 denoted by $C_{397}, C_{419}, C_{697}$ are all cubic and only five out of the nine codes with W_3, denoted by $C_{119}, C_{174}, C_{184}, C_{350}, C_{487}$, are cubic. We have also checked that there is no cubic code with W_2.

Theorem 3.4. *Up to permutation equivalence, there are exactly* 8 *binary cubic self-dual* $[30, 15, 6]$ *codes.*

(ii) $\ell = 12$, $[36, 18, 8]$ codes.

There are two weight enumerators for self-dual $[36, 18, 8]$ codes (refer to [11,35]):

$$W_1 = 1 + 225y^8 + 2016y^{10} + \cdots,$$
$$W_2 = 1 + 289y^8 + 1632y^{10} + \cdots.$$

For cubic codes, $p = 3$ should divide A_8 by Corollary 3.3. Therefore any binary cubic self-dual $[36, 18, 8]$ code has weight enumerator W_1. Bonnecaze et al. [3] gave one code CSD_{36} with W_1 and group order 288. We have found 9 inequivalent cubic self-dual $[36, 18, 8]$ codes with W_1 and groups orders 18, 24, 36, 48, 96, 240, 288, 384, and 12 960. We have checked by Magma that our code with group order 288 is equivalent to CSD_{36}. Hence there are at least 9 extremal cubic self-dual codes of length 36. These codes are posted in [31].

It is shown [35] that there are exactly 41 binary self-dual $[36, 18, 8]$ codes and exactly 25 codes among them have $A_8 = 225$. However we have noticed that many generator matrices in [35] do not produce self-dual codes. This was confirmed by Gaborit [14] and was corrected in his website [15]. From the corrected list of the binary self-dual $[36, 18, 8]$ codes [15], we have checked that only 13 of the 25 self-dual $[36, 18, 8]$ codes with $A_8 = 22$ are cubic by further investigating the existence of a fixed point free automorphism of order 3 in each code. Let C_i be the ith code from the list of [15]. Then C_i is cubic if and only if $i \in \{1, 3, 6, 7, 8, 9, 11, 12, 14, 16, 21, 22, 25\}$.

Independently, Harada and Munemasa [25] have recently classified all binary self-dual $[36, 16]$ codes including the extremal self-dual $[36, 16, 8]$ codes. They confirmed that there are exactly 41 extremal self-dual $[36, 16, 8]$ codes and exactly 25 codes among them have $A_8 = 225$. Let C_i be the ith code from the list of [25]. Then C_i is cubic if and only if $i \in \{1, 4, 12, 13, 15, 16, 19, 21, 24, 26, 27, 31, 33\}$.

Theorem 3.5. *Up to permutation equivalence, there are exactly* 13 *binary cubic self-dual* $[36, 18, 8]$ *codes.*

(iii) $\ell = 14$, $[42, 21, 8]$ codes.

There are two weight enumerators for self-dual $[42, 21, 8]$ codes [5,27]:

$$W_1 = 1 + 164y^8 + 679y^{10} + \cdots,$$
$$W_2 = 1 + (84 + 8\beta)y^8 + (1449 - 24\beta)y^{10} + \cdots \quad \big(\beta \in \{0, 1, \ldots, 22, 24, 26, 28, 32, 42\}\big).$$

By Corollary 3.3, 3 should divide A_8. Therefore any binary cubic self-dual $[42, 21, 8]$ code has weight enumerator W_2, where 3 divides $84+8\beta$, that is, β is a multiple of 3. Bonnecaze et al. [3] gave one code with W_2 and $\beta = 0$. We have found 14 inequivalent cubic self-dual $[42, 21, 8]$ codes with $\beta = 0, 3, 6, 9, 12$ with group orders 3, 6, 12, and 36. It is shown that if a self-dual code satisfies W_2 with $\beta \in \{24, 26, 28, 32, 42\}$, it is equivalent to one of the eight codes in [5, Table 1]. If it is cubic, then β should be $\beta = 24$ or 42 by the divisibility condition on β. For $\beta = 24$, there are three codes denoted by $C_{24,1}, C_{24,2}, C_{24,3}$ [5]. We have checked that only $C_{24,2}$ has a fixed point free automorphism of order 3; hence it is cubic. For $\beta = 42$, there is only one code denoted by C_{42} [5]. We have checked that it has a fixed point free automorphism of order 3; hence it is cubic.

We have found [6, Table 5] where it is shown that there are exactly 1569 binary self-dual $[42, 21, 8]$ codes with a fixed point free automorphism of order 3 and weight enumerator W_2. This table confirms the above calculations.

Theorem 3.6. *Up to permutation equivalence, there are exactly* 1569 *binary cubic self-dual* $[42, 21, 8]$ *codes.*

(iv) $\ell = 16$, $[48, 24, 10]$ codes.

There are two weight enumerators for self-dual $[48, 24, 10]$ codes [27]:

$$W_1 = 1 + 704y^{10} + 8976y^{12} + \cdots,$$
$$W_2 = 1 + 768y^{10} + 8592y^{12} + \cdots.$$

By Corollary 3.3, any binary cubic self-dual $[48, 24, 10]$ code has weight enumerator W_2. Bonnecaze et al. [3] gave one code with W_2 with no group order given. We have found four inequivalent codes with W_2 and group orders $3, 6, 12$, and 24. See Table 2 for details, where the first column gives the code name, the second and third columns the X vector and the base matrix in Theorem 2.2, the fourth column the corresponding weight enumerator of the binary code, and the last column the order of the automorphism group of the binary code.

(v) $\ell = 18$, $[54, 27, 10]$ codes.

There are two weight enumerators for self-dual $[48, 24, 10]$ codes [27]:

$$W_1 = 1 + (351 - 8\beta)y^{10} + (5031 + 24\beta)y^{12} + \cdots \quad (0 \leqslant \beta \leqslant 43),$$
$$W_2 = 1 + (351 - 8\beta)y^{10} + (5543 + 24\beta)y^{12} + (43\,884 + 32\beta)y^{14} + \cdots \quad (12 \leqslant \beta \leqslant 43).$$

Any binary cubic self-dual $[54, 27, 10]$ code has W_1 or W_2 as its weight enumerator; in both cases, 3 divides β with the same reasoning as above. Bonnecaze et al. [3] gave two codes, one with W_1 and $\beta = 0$ and the other with W_2 and $\beta = 12$ (and group order 3). We have found four inequivalent codes with W_1 and $\beta = 0, 3, 6, 9$ (all group orders 3) and three inequivalent codes with W_2 and $\beta = 12, 15, 18$ (all group orders 3). See Table 2 for more details.

(vi) $\ell = 20$.

We have not found any self-dual $[60, 30, 12]$ codes even though there are at least three cubic self-dual $[60, 30, 12]$ codes [3] with W_2 and $\beta = 10$ in the notation of [27].

(vii) $\ell = 22$, $[66, 33, 12]$ codes.

There are three possible weight enumerators for self-dual $[66, 33, 12]$ codes [27]:

$$W_1 = 1 + 1690y^{12} + 7990y^{14} + \cdots,$$
$$W_2 = 1 + (858 + 8\beta)y^{12} + (18\,678 - 24\beta)y^{14} + \cdots \quad (0 \leqslant \beta \leqslant 778),$$

and

$$W_3 = 1 + (858 + 8\beta)y^{12} + (18\,166 - 24\beta)y^{14} + \cdots \quad (14 \leqslant \beta \leqslant 756).$$

Table 2
Binary extremal Type I cubic self-dual codes of length $n = 48, 54, 66$.

Codes $C_{n,i}$	X vector	Using gen. matrix	Weight enumerator	|Aut|
$C_{48,1}$	$(Y, Y+1, Y^2+1, Y^2, 0, 1, 0,$ $Y^2, 0, Y^2+Y, 0, Y^2+Y, Y^2, 0)$	G_{14}	W_2	3
$C_{48,2}$	$(Y^2+Y, 0, Y^2+Y+1, 1, Y, 1, Y+1,$ $Y^2+1, Y^2+1, 1, Y^2+Y+1, 1, Y^2, Y^2)$	G_{14}	W_2	24
$C_{48,3}$	$(Y^2, Y^2+Y+1, Y^2, 0, Y, 0, Y^2+Y+1,$ $Y^2+Y, 0, Y+1, Y, Y^2+1, Y, Y^2+1)$	G_{14}	W_2	12
$C_{48,4}$	$(0, 0, Y^2+Y, Y^2+Y+1, Y+1, Y,$ $1, Y^2+Y, Y^2+1, Y^2, Y+1, Y^2, Y, 1)$	G_{14}	W_2	6
$C_{54,1}$	$(Y^2+Y+1, Y^2+1, Y^2+1, Y^2+1, Y^2+1, Y^2+Y, Y^2+Y+1,$ $Y^2+Y+1, Y^2+Y, Y^2, 0, Y+1, 1, 0, Y^2+Y+1, Y^2+Y+1)$	G_{16}	W_2, $\beta = 18$	3
$C_{54,2}$	$(Y+1, Y+1, Y+1, 1, Y+1, 1, Y^2+Y+1, Y, Y^2,$ $Y^2+Y, Y^2, 1, Y+1, Y^2, 1, Y+1)$	G_{16}	W_1, $\beta = 9$	3
$C_{54,3}$	$(Y, Y^2, Y+1, 0, 1, Y^2, Y, Y^2+1, 1, Y^2+Y, 1, Y,$ $Y^2+Y+1, 1, Y^2+Y+1, Y^2+1)$	G_{16}	W_2, $\beta = 15$	3
$C_{54,4}$	$(Y^2+Y, Y^2+Y+1, Y^2+Y, 1, Y^2+1, Y+1, 0, Y^2+Y,$ $Y^2, 1, 1, 0, Y^2+1, Y, 1, Y^2+1)$	G_{16}	W_1, $\beta = 3$	3
$C_{54,5}$	$(1, Y, Y, Y, Y+1, Y^2, Y, 0, Y+1, Y^2+Y, Y^2,$ $Y^2+Y+1, Y^2, Y^2+Y, 0, Y+1)$	G_{16}	W_1, $\beta = 0$	3
$C_{54,6}$	$(Y^2, 0, Y^2, Y^2+Y+1, Y^2+Y, 0, 0,$ $Y^2+1, 0, Y^2+Y, Y, 0, Y^2, Y^2+Y, Y+1, 0)$	G_{16}	W_2, $\beta = 12$	3
$C_{54,7}$	$(Y^2+Y+1, Y^2+Y, Y^2+Y, Y+1, Y, Y^2, Y^2+Y, Y^2+Y+1,$ $Y^2+Y+1, Y^2+1, Y^2+Y, Y^2, Y^2+1, Y^2+Y+1, Y+1, 0)$	G_{16}	W_1, $\beta = 6$	3
$C_{66,1}$	$(Y^2+1, 1, Y+1, 1, 0, 0, Y^2+Y+1, 0, 1, Y^2,$ $1, Y, Y+1, 1, 1, Y^2+Y, 0, Y+1, 0, 0)$	G_{20}	W_2, $\beta = 46$	3
$C_{66,2}$	$(Y^2+Y+1, Y^2+Y+1, 0, 1, Y, Y^2, Y^2, 1, Y^2+Y+1, Y^2+Y+1,$ $Y^2+1, Y^2, Y^2+1, 0, Y^2+Y+1, Y^2+Y+1, Y^2+1, 0, Y, Y+1)$	G_{20}	W_2, $\beta = 17$	3
$C_{66,3}$	$(0, 0, Y^2+Y, 1, Y^2+Y, Y^2+Y+1, Y+1, 1, Y+1, Y, Y^2+Y+1,$ $Y, Y^2+1, Y+1, Y^2, Y+1, Y+1, Y^2+Y+1, Y, Y+1)$	G_{20}	W_2, $\beta = 23$	3
$C_{66,4}$	$(Y^2, Y^2+1, Y^2, Y^2, Y+1, 0, 1, 0, 1, Y^2+1, Y^2+1,$ $1, Y^2+Y, Y+1, 1, Y, Y+1, Y^2+1, 0, Y^2)$	G_{20}	W_2, $\beta = 26$	3
$C_{66,5}$	$(Y, Y, Y^2, Y^2+1, Y+1, Y, 0, Y+1, Y^2+Y+1, 0, Y^2+1,$ $Y^2+Y+1, 1, Y, Y^2+Y+1, Y^2+Y, 0, Y^2+1, Y^2+Y, 0)$	G_{20}	W_2, $\beta = 43$	3

By Corollary 3.3, any binary cubic self-dual $[66, 33, 12]$ code should have weight enumerator W_2 with β in the given range as above since A_{14} should be divisible by 3. Bonnecaze et al. [3] gave two codes with W_2 and $\beta = 21, 30$. Using G_{20} with various values of X in Table 2, we have constructed five inequivalent codes with W_2 and $\beta = 17, 23, 26, 43, 46$. All have automorphism group of order 3.

The following generator matrices G_{14}, G_{16}, and G_{20} are used in Table 2 for constructing binary extremal cubic self-dual codes of $n = 48, 54, 66$

$$G_{14} = \begin{pmatrix} 1, 0, Y^2+Y, Y+1, 1, Y, Y^2+Y+1, Y, Y, 0, Y^2+Y, Y^2, 1, 0 \\ Y, Y, 1, 0, Y^2, Y^2+Y+1, Y^2+Y, Y^2+Y+1, Y^2+Y+1, Y^2+1, Y^2, Y+1, Y, Y \\ Y^2+1, Y^2+1, 0, 0, 1, 0, 0, Y^2+Y, Y, Y^2, Y^2+1, Y, Y^2+Y+1, Y^2+Y+1 \\ 1, 1, Y^2+1, Y^2+1, Y^2+1, Y^2+1, 1, 0, Y^2, Y^2+Y, Y^2, Y^2+Y+1, Y^2+1, Y^2+Y \\ 1, 1, 1, 1, 0, 0, Y^2+Y+1, Y^2+Y+1, 1, 0, Y+1, Y^2+1, Y^2+Y, Y^2+Y+1 \\ Y^2+Y+1, Y^2+Y+1, Y, Y, 1, 1, Y+1, Y+1, 1, 1, 1, 0, Y+1, Y^2+Y+1 \\ Y^2, Y^2, 1, 1, Y^2+Y+1, Y^2+Y+1, Y^2, Y^2, Y^2, Y^2, Y, Y, 1, 1 \end{pmatrix},$$

$$G_{16} = \begin{pmatrix} 1, 0, Y^2+Y, 0, Y^2, Y^2, Y^2+Y+1, Y+1, 1, Y, Y^2, Y^2, 1, Y^2, Y+1, 0 \\ Y+1, Y+1, 1, 0, Y^2, Y, 1, Y^2, Y^2+1, 1, Y, Y^2, Y^2+Y+1, Y, Y+1, Y+1 \\ Y, Y, Y+1, Y+1, 1, 0, Y^2, Y^2+Y+1, Y^2+Y, Y^2+Y+1, Y^2+Y+1, Y^2+1, Y^2, Y+1, Y, Y \\ Y^2+Y, Y^2+Y, Y^2+Y, Y^2+Y, 0, 0, 1, 0, 0, Y^2+Y, Y, Y^2, Y^2+1, Y, Y^2+Y+1, Y^2+Y+1 \\ 0, 0, 1, 1, Y^2+1, Y^2+1, Y^2+1, Y^2+1, 1, 0, Y^2, Y^2+Y, Y^2, Y^2+Y+1, Y^2+1, Y^2+Y \\ 1, 1, Y^2+Y, Y^2+Y, 1, 1, 0, 0, Y^2+Y+1, Y^2+Y+1, 1, 0, Y+1, Y^2+1, Y^2+Y, Y^2+Y+1 \\ Y+1, Y+1, Y^2+Y+1, Y^2+Y+1, Y, Y, 1, 1, Y+1, Y+1, 1, 1, 1, 0, Y+1, Y^2+Y+1 \\ Y^2+Y+1, Y^2+Y+1, Y, Y, 1, 1, Y^2+Y+1, Y^2+Y+1, Y^2, Y^2, Y^2, Y^2, Y, Y, 1, 1 \end{pmatrix},$$

$$G_{20} = \begin{pmatrix} 1, 0, 0, Y^2+1, Y^2+Y+1, Y, Y^2, Y^2, 1, Y^2+Y, 0, 1, Y+1, 1, Y^2, Y, Y+1, Y^2+1, 1, 1 \\ Y, Y, 1, 0, Y+1, Y+1, Y+1, 1, Y+1, 1, Y^2+Y+1, Y, Y^2, Y^2+Y, Y^2, 1, Y+1, Y^2, 1, Y+1 \\ Y^2+Y+1, Y^2+Y+1, Y^2+1, Y^2+1, 1, 0, Y^2+Y, 0, Y^2, Y^2, Y^2+Y+1, Y+1, 1, Y, Y^2, Y^2, 1, Y^2, Y+1, 0 \\ 0, 0, 0, 0, Y+1, Y+1, 1, 0, Y^2, Y, 1, Y^2, Y^2+1, 1, Y, Y^2, Y^2+Y+1, Y, Y+1, Y+1 \\ Y+1, Y+1, Y^2+Y, Y^2+Y, Y, Y, Y+1, Y+1, 1, 0, Y^2, Y^2+Y+1, Y^2+Y, Y^2+Y+1, Y^2+Y+1, Y^2+1, Y^2, Y+1, Y, Y \\ 0, 0, Y, Y, Y^2+Y, Y^2+Y, Y^2+Y, Y^2+Y, 0, 0, 1, 0, 0, Y^2+Y, Y, Y^2, Y^2+1, Y, Y^2+Y+1, Y^2+Y+1 \\ Y^2+Y+1, Y^2+Y+1, 0, 0, 0, 0, 1, 1, Y^2+1, Y^2+1, Y^2+1, Y^2+1, 1, 0, Y^2, Y^2+Y, Y^2, Y^2+Y+1, Y^2+1, Y^2+Y \\ Y+1, Y+1, 1, 1, 1, 1, Y^2+Y, Y^2+Y, 1, 1, 0, 0, Y^2+Y+1, Y^2+Y+1, 1, 0, Y+1, Y^2+1, Y^2+Y, Y^2+Y+1 \\ Y^2+Y+1, Y^2+Y+1, Y^2+1, Y^2+1, Y+1, Y+1, Y^2+Y+1, Y^2+Y+1, Y, Y, 1, 1, Y+1, Y+1, 1, 1, 1, 0, Y+1, Y^2+Y+1 \\ Y^2+Y+1, Y^2+Y+1, 1, 1, Y^2+Y+1, Y^2+Y+1, Y, Y, 1, 1, Y^2+Y+1, Y^2+Y+1, Y^2, Y^2, Y^2, Y^2, Y, Y, 1, 1 \end{pmatrix}.$$

3.2. Binary quintic self-dual codes

In this subsection, we give the classification of binary quintic self-dual codes of even lengths up to 30 (up to permutation equivalence) by using Theorem 2.7 since 2 is a primitive element of $\mathbb{F}_5$. Using the known classification of binary self-dual codes of lengths up to 30, one can also classify binary quintic self-dual codes of these lengths. To save space, we post the classification result in [31]. We know from [10, Table F] that there are exactly 13 optimal binary self-dual $[30, 15, 6]$ codes with three distinct weight enumerators W_1, W_2, W_3 from Section 3.1. Exactly nine of them have the weight enumerator $W_3 = 1 + 35y^6 + 345y^8 + 1848y^{10} + 5320y^{12} + \cdots$. By Corollary 3.3, W_3 is the only possible weight enumerator for a binary extremal quintic self-dual code. We have checked that only four codes are binary quintic optimal self-dual codes of length 30.

Theorem 3.7. *Up to permutation equivalence*:

(i) *There is a unique quintic self-dual code of length* 10.
(ii) *There are exactly three quintic self-dual codes of length* 20, *two of which are extremal.*
(iii) *There are exactly eleven quintic self-dual codes of length* 30, *four of which are optimal.*

Making successive random choices of $\mathbf{x}$ from $G_{6,2}$ by using the building-up construction in Theorem 2.2 with $c = 1$, we obtain $G_{12} = [L \mid R]$, where L and R are given below

$$L = \begin{bmatrix} 1 & 0 & Y^4+Y^2+Y & Y^4+Y^3+Y^2+1 & Y^4+Y^3+Y^2 & Y^3+Y \\ Y^4+Y^2+Y & Y^4+Y^2+Y & 1 & 0 & Y^4+Y^2 & Y^3+Y+1 \\ Y^4+Y^3+Y^2+Y+1 & Y^4+Y^3+Y^2+Y+1 & Y^4+Y^3+Y+1 & Y^4+Y^3+Y+1 & 1 & 0 \\ Y^4+Y^2 & Y^4+Y^2 & 1 & 1 & Y^4 & Y^4 \\ Y^4+Y^2+1 & Y^4+Y^2+1 & Y^3+1 & Y^3+1 & Y^4+Y^3+Y^2+Y & Y^4+Y^3+Y^2+Y \\ Y^4+Y^2+Y & Y^4+Y^2+Y & Y^3+Y^2+1 & Y^3+Y^2+1 & Y^4+Y^2+1 & Y^4+Y^2+1 \end{bmatrix},$$

$$R = \begin{bmatrix} Y^4+Y^3+Y & Y^4+Y^2+Y & Y^4+1 & Y^3+Y^2+Y & Y^4+Y^2+Y & Y \\ Y^2+Y & Y^4+Y^3+Y^2+Y & Y^4+Y^3+Y^2+Y & Y^2+Y & Y^4+Y^3 & Y^4+Y^2 \\ Y^4+Y^3+Y^2 & Y^3+Y & Y & Y^2 & Y^3+Y & Y^4+Y \\ 1 & 0 & 0 & 0 & Y+1 & Y^3+Y+1 \\ Y^4+Y^2+1 & Y^4+Y^2+1 & 1 & 0 & 0 & 1 \\ Y^2 & Y^2 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

We verify that the corresponding binary quintic self-dual code of G_{12} has parameters $[60, 30, 12]$. The deletion of the first two columns and the first row of G_{12} is denoted by G_{10}, and similarly we obtain G_8 from G_{10}. Their corresponding binary quintic self-dual codes have parameters $[40, 20, 8]$ (Type II) and $[50, 25, 10]$. We summarize their corresponding weight enumerators of G_8, G_{10}, G_{12} respectively as follows

$$1 + 285y^8 + 21\,280y^{12} + 239\,970y^{16} + 525\,504y^{20} + \cdots,$$

$$1 + 516y^{10} + 7720y^{12} + 55\,880y^{14} + 291\,990y^{16} + 1\,077\,265y^{18} + 2\,810\,424y^{20} + 5\,287\,640y^{22} + 7\,245\,780y^{24} + \cdots,$$

$$1 + 3195y^{12} + 29\,760y^{14} + 284\,625y^{16} + 1\,728\,000y^{18} + 7\,769\,400y^{20} + 26\,392\,320y^{22} + 67\,226\,760y^{24} + 130\,060\,800y^{26} + 193\,151\,475y^{28} + 220\,449\,152y^{30} + \cdots.$$

The first one is the unique extremal weight enumerator, the second weight enumerator corresponds to W_2 with $\beta = 2$ in [27], and the third weight enumerator corresponds to W_2 with $\beta = 10$ in [27]. The orders of the automorphism groups are 10, 5, and 20 respectively.

4. Construction of quasi-cyclic self-dual codes over various finite fields

In this section we find quasi-cyclic self-dual codes over $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$ and $\mathbb{F}_5$ which are optimal or have best known self-dual codes by applying the building-up construction in Theorem 2.2.

4.1. Cubic self-dual codes over $\mathbb{F}_4$ and $\mathbb{F}_5$

In [21], we have given cubic self-dual codes over $\mathbb{F}_4$ and $\mathbb{F}_5$ that are optimal or have best known parameters. In particular, we have the following.

Theorem 4.1. *There are at least two monomially inequivalent* $[24, 12, 9]$ *self-dual codes over* $\mathbb{F}_5$*, one of which is cubic and denoted by* CSD_{24}^5.

Applying Construction A [12], we can construct the odd Leech lattice O_{24} using the idea in [24]. In [24, Proposition 4] it is shown that for a self-dual $[24, 12, d \geqslant 8]$ code C over $\mathbb{F}_5$, the corresponding lattice $A_5(C)$ by Construction A is the odd Leech lattice O_{24} if there is no codeword $\mathbf{x} \in \mathbf{C}$ with $n_0(\mathbf{x}) = 14$, $n_1(\mathbf{x}) = 10$, and $n_2(\mathbf{x}) = 0$, where $n_i(\mathbf{x})$ denotes the number of coordinates of $\mathbf{x}$ with $\pm i$ for $i = 0, 1, 2$. We have calculated the complete weight enumerator of CSD_{24}^5 by Magma and checked that there is no such $\mathbf{x}$ in CSD_{24}^5. Thus $A_5(CSD_{24}^5) = O_{24}$. Since it is known [12] that one of the two even unimodular neighbors of O_{24} is the Leech lattice Λ_{24}, we have another way to construct Λ_{24} using our new code CSD_{24}^5, rather than $\mathbb{Q}_{24}$ used in [38].

4.2. Quintic self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_4$

In this section, we find more quintic self-dual codes over $\mathbb{F}_3$ and $\mathbb{F}_4$ which are optimal or best known self-dual codes by using the building-up construction in Theorem 2.2.

- Case: $q = 3$.

Using (ii) of Theorem 2.2 with $\alpha = 1$ and $\beta = 1$, we obtain the following $I_8 = [L \mid R]$:

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ Y^4+2Y^2+Y & 2Y^4+2Y^3+Y & 2Y^3+2Y^2+2Y & 2Y^4+Y^3+2Y^2 \\ Y^4+2Y^3+Y^2+2Y+1 & 2Y^2+Y & Y^4+2Y^3+1 & Y^4+2Y^3+2Y^2+Y+1 \end{bmatrix},$$

$$R = \begin{bmatrix} Y^2+1 & 2Y^4+Y^2+Y+2 & 2Y^3 & Y^4+2Y^3+2Y+1 \\ 2Y^4+Y^2+Y+2 & 2Y^4+Y^3+Y^2+2Y+1 & Y^4+2Y^3+2Y^2+1 & Y^4+2Y^3+Y+1 \\ Y^4+Y^2+2 & 2Y^4+Y^3+2Y^2+2Y+1 & Y^4+2Y^3+2Y^2+Y & Y^3+2Y+1 \\ 2Y^4+2Y^3+2 & 2Y^4+Y^3+2Y^2+2 & Y & 2Y^3+2Y^2+Y+2 \end{bmatrix}.$$

We also obtain a 2 by 4 matrix I_4 by deleting the first four columns and the first two rows of I_8. The corresponding ternary quasi-cyclic self-dual codes are all extremal self-dual codes. More specifically, I_4 induces a $[20, 10, 6]$ code and I_8 induces a $[40, 20, 12]$ code, and the orders of the automorphism groups are $2^8 \cdot 3 \cdot 5, 10$, respectively. There are exactly six extremal $[20, 10, 6]$ self-dual codes, and our code with the generator matrix I_4 corresponds to 19th code in Table III [40].

We denote the code with the generator matrix I_8 by QSD_{40}^3. There are at least 118 $[40, 20, 12]$ ternary extremal self-dual codes. More precisely, the 15 codes with automorphisms of prime order $r > 5$ were found in [26]. It was reported in [22] that there are five more $[40, 20, 12]$ ternary extremal self-dual codes. But we have checked that the codes $C_{40,w1}$ and $C_{40,w3}$ in [22, Table 6] have minimum weight 9. Hence three codes were found in [22], and we have verified that these three codes are not equivalent to QSD_{40}^3. There are 100 codes in [23] whose automorphism group orders are greater than $|\mathrm{Aut}(QSD_{40}^3)| = 10$. In what follows, we give the generator matrix $[L \mid R]$ of QSD_{40}^3:

$$L = \begin{bmatrix}
1&0&0&0&1&2&0&1&0&0&0&0&0&1&0&2&0&0&0&0\\
0&1&0&0&2&1&1&1&0&0&0&0&1&2&0&1&0&0&0&0\\
0&0&0&0&2&1&0&1&1&1&2&0&0&2&1&2&2&0&2&2\\
1&0&1&1&2&2&0&2&2&1&0&1&0&0&1&1&1&2&0&2\\
0&0&0&0&0&2&0&1&1&0&0&0&1&2&0&1&0&0&0&0\\
0&0&0&0&2&2&1&1&0&1&0&0&2&1&1&1&0&0&0&0\\
1&2&0&2&1&2&1&0&0&0&0&0&2&1&0&1&1&1&2&0\\
1&0&1&1&2&2&0&0&1&0&1&1&2&2&0&2&2&1&0&1\\
0&0&0&0&0&0&2&2&0&0&0&0&0&2&0&1&1&0&0&0\\
0&0&0&0&0&1&2&2&0&0&0&0&2&2&1&1&0&1&0&0\\
0&2&2&1&0&1&2&1&1&2&0&2&1&2&1&0&0&0&0&0\\
2&0&2&2&2&1&0&2&1&0&1&1&2&2&0&0&1&0&1&1\\
0&0&0&0&1&1&0&0&0&0&0&0&0&0&2&2&0&0&0&0\\
0&0&0&0&1&1&2&0&0&0&0&0&0&1&2&2&0&0&0&0\\
2&0&2&2&1&2&2&0&0&2&2&1&0&1&2&1&1&2&0&2\\
1&2&0&2&0&2&0&2&2&0&2&2&2&1&0&2&1&0&1&1\\
0&0&0&0&0&1&0&2&0&0&0&0&1&1&0&0&0&0&0&0\\
0&0&0&0&1&2&0&1&0&0&0&0&1&1&2&0&0&0&0&0\\
1&1&2&0&0&2&1&2&2&0&2&2&1&2&2&0&0&2&2&1\\
2&1&0&1&0&0&1&1&1&2&0&2&0&2&0&2&2&0&2&2
\end{bmatrix},$$

$$R=\begin{bmatrix}
1&1&0&0&0&0&0&0&0&0&2&2&0&0&0&0&0&2&0&1\\
1&1&2&0&0&0&0&0&0&1&2&2&0&0&0&0&2&2&1&1\\
1&2&2&0&0&2&2&1&0&1&2&1&1&2&0&2&1&2&1&0\\
0&2&0&2&2&0&2&2&2&1&0&2&1&0&1&1&2&2&0&0\\
0&1&0&2&0&0&0&0&1&1&0&0&0&0&0&0&0&0&2&2\\
1&2&0&1&0&0&0&0&1&1&2&0&0&0&0&0&0&1&2&2\\
0&2&1&2&2&0&2&2&1&2&2&0&0&2&2&1&0&1&2&1\\
0&0&1&1&1&2&0&2&0&2&0&2&2&0&2&2&2&1&0&2\\
1&2&0&1&0&0&0&0&0&1&0&2&0&0&0&0&1&1&0&0\\
2&1&1&1&0&0&0&0&1&2&0&1&0&0&0&0&1&1&2&0\\
2&1&0&1&1&1&2&0&0&2&1&2&2&0&2&2&1&2&2&0\\
2&2&0&2&2&1&0&1&0&0&1&1&1&2&0&2&0&2&0&2\\
0&2&0&1&1&0&0&0&1&2&0&1&0&0&0&0&0&1&0&2\\
2&2&1&1&0&1&0&0&2&1&1&1&0&0&0&0&1&2&0&1\\
1&2&1&0&0&0&0&0&2&1&0&1&1&1&2&0&0&2&1&2\\
2&2&0&0&1&0&1&1&2&2&0&2&2&1&0&1&0&0&1&1\\
0&0&2&2&0&0&0&0&0&2&0&1&1&0&0&0&1&2&0&1\\
0&1&2&2&0&0&0&0&2&2&1&1&0&1&0&0&2&1&1&1\\
0&1&2&1&1&2&0&2&1&2&1&0&0&0&0&0&2&1&0&1\\
2&1&0&2&1&0&1&1&2&2&0&0&1&0&1&1&2&2&0&2
\end{bmatrix}.$$

As a summary, we have the following theorem.

Theorem 4.2. *There are at least* 119 *monomially inequivalent self-dual* $[40,20,12]$ *codes over* $\mathbb{F}_3$.

- Case: $q=4$.

Applying a similar process as before up to code length $\ell=6$ with $c=1$, we find the following $J_6=[L \mid R]$:

$$L=\begin{bmatrix}
1 & 0 & Y^4+Y^3+Y^2+Y+1\\
\omega Y^4+\omega^2Y^3+Y^2+Y & \omega Y^4+\omega^2Y^3+Y^2+Y & 1\\
\omega^2Y^4+\omega^2Y^3+\omega Y^2+\omega Y+\omega & \omega^2Y^4+\omega^2Y^3+\omega Y^2+\omega Y+\omega & \omega^2Y^2+Y
\end{bmatrix},$$

$$R=\begin{bmatrix}
Y^4+Y^3+\omega Y^2+Y & Y^4+\omega Y^3+\omega^2Y^2+\omega^2Y+1 & \omega^2Y^4+Y^3+Y^2+\omega\\
0 & Y^4+Y^3+Y^2+Y+\omega & \omega^2Y^4+Y^3+\omega^2Y^2+\omega Y\\
\omega^2Y^2+Y & Y^4+Y^3+Y^2+Y+\omega & Y^4+\omega Y^3+\omega^2Y^2+\omega
\end{bmatrix},$$

where ω is a generator of $\mathbb{F}_4^*$. The corresponding quaternary quasi-cyclic Euclidean self-dual codes are all optimal or have the best known parameters. See [20] for the generator matrices of these quaternary codes. By successively deleting the first two columns and the first row of J_6, we obtain J_4 and J_2. More precisely, J_2 induces a $[10,5,4]$ code (optimal), J_4 induces a $[20,10,8]$ code (optimal), and J_6 induces a $[30,15,10]$ code (best known). The quaternary code corresponding to J_4 is equivalent to XQ_{19} [42]. We denote the quaternary code corresponding to the generator matrix J_6 by QSD_{30}^4 whose generator matrix $G(QSE_{30}^4)$ is given below. We have computed that QSD_{30}^4 has minimum distance 10, $A_{10}=1893$, and the automorphism group of order 30. As far as we know, only one self-dual $[30,15,10]$ code over $\mathbb{F}_4$ was known before, and that code is the one denoted by $(f_2;11;25)$ [17]. (It was reported to us that the code denoted by $(f_2;11;15)$ [17] is an error since it has minimum distance 6.) The code $(f_2;11;25)$ has minimum distance 10, $A_{10}=1854$, and the automorphism group of order 90. Therefore the two codes QSD_{30}^4 and $(f_2;11;25)$ are not equivalent. We note that the minimum Lee weight d_L of these codes in the sense of [2] and [18] is 10 and that only one self-dual $[30,15,9]$ code over $\mathbb{F}_4$ with $d_L=10$ is given in [2, Table VIII].

As a summary, we have the following theorem.

Theorem 4.3. *There are at least two monomially inequivalent self-dual* $[30, 15, 10]$ *codes over* $\mathbb{F}_4$.

$$G\left(QSD_{30}^{4}\right) = \begin{bmatrix} 1\,0\,1\,0\,1\,w\,0\,0\,1\,1\,w^2\,0\,0\,0\,1\,w\,w^2\,1\,0\,0\,1\,1\,w\,1\,0\,0\,1\,1\,1\,w^2 \\ 0\,0\,1\,0\,w\,0\,1\,1\,0\,0\,1\,w\,1\,1\,0\,0\,1\,w^2\,w^2\,w^2\,0\,0\,1\,1\,w\,w\,0\,0\,1\,w^2 \\ w\,w\,0\,0\,w\,w\,w\,w\,1\,1\,1\,0\,w\,w\,w^2\,w^2\,1\,w^2\,w^2\,w^2\,0\,0\,1\,w\,w^2\,w^2\,0\,0\,1\,1 \\ 0\,0\,1\,1\,1\,w^2\,1\,0\,1\,0\,1\,w\,0\,0\,1\,1\,w^2\,0\,0\,0\,1\,w\,w^2\,1\,0\,0\,1\,1\,w\,1 \\ w\,w\,0\,0\,1\,w^2\,0\,0\,1\,0\,w\,0\,1\,1\,0\,0\,1\,w\,1\,1\,0\,0\,1\,w^2\,w^2\,w^2\,0\,0\,1\,1 \\ w^2\,w^2\,0\,0\,1\,1\,w\,w\,0\,0\,w\,w\,w\,w\,1\,1\,1\,0\,w\,w\,w^2\,w^2\,1\,w^2\,w^2\,w^2\,0\,0\,1\,w \\ 0\,0\,1\,1\,w\,1\,0\,0\,1\,1\,1\,w^2\,1\,0\,1\,0\,1\,w\,0\,0\,1\,1\,w^2\,0\,0\,0\,1\,w\,w^2\,1 \\ w^2\,w^2\,0\,0\,1\,1\,w\,w\,0\,0\,1\,w^2\,0\,0\,1\,0\,w\,0\,1\,1\,0\,0\,1\,w\,1\,1\,0\,0\,1\,w^2 \\ w^2\,w^2\,0\,0\,1\,w\,w^2\,w^2\,0\,0\,1\,1\,w\,w\,0\,0\,w\,w\,w\,w\,1\,1\,1\,0\,w\,w\,w^2\,w^2\,1\,w^2 \\ 0\,0\,1\,w\,w^2\,1\,0\,0\,1\,1\,w\,1\,0\,0\,1\,1\,1\,w^2\,1\,0\,1\,0\,1\,w\,0\,0\,1\,1\,w^2\,0 \\ 1\,1\,0\,0\,1\,w^2\,w^2\,w^2\,0\,0\,1\,1\,w\,w\,0\,0\,1\,w^2\,0\,0\,1\,0\,w\,0\,1\,1\,0\,0\,1\,w \\ w\,w\,w^2\,w^2\,1\,w^2\,w^2\,w^2\,0\,0\,1\,w\,w^2\,w^2\,0\,0\,1\,1\,w\,w\,0\,0\,w\,w\,w\,w\,1\,1\,1\,0 \\ 0\,0\,1\,1\,w^2\,0\,0\,0\,1\,w\,w^2\,1\,0\,0\,1\,1\,w\,1\,0\,0\,1\,1\,1\,w^2\,1\,0\,1\,0\,1\,w \\ 1\,1\,0\,0\,1\,w\,1\,1\,0\,0\,1\,w^2\,w^2\,w^2\,0\,0\,1\,1\,w\,w\,0\,0\,1\,w^2\,0\,0\,1\,0\,w\,0 \\ w\,w\,1\,1\,1\,0\,w\,w\,w^2\,w^2\,1\,w^2\,w^2\,w^2\,0\,0\,1\,w\,w^2\,w^2\,0\,0\,1\,1\,w\,w\,0\,0\,w\,w \end{bmatrix}.$$

4.3. *Septic self-dual codes over* $\mathbb{F}_2$, $\mathbb{F}_4$, *and* $\mathbb{F}_5$

In this section, we find septic self-dual codes over $\mathbb{F}_q$ which are optimal or have the best known self-dual codes by using the building-up construction in Theorem 2.2.

- Case: $q = 2$.

We do a similar process as before up to the length $\ell = 8$ with $c = 1$, so we get $K_8 = [L \mid R]$ as follows

$$L = \begin{bmatrix} 1 & 0 & Y^4+Y^3+Y^2 & Y^6+Y^5+Y^4+Y^2+Y+1 \\ Y^6+Y^5+Y^3+Y^2+1 & Y^6+Y^5+Y^3+Y^2+1 & 1 & 0 \\ Y^5+Y+1 & Y^5+Y+1 & Y^6+Y^4+Y^3+Y^2 & Y^6+Y^4+Y^3+Y^2 \\ Y^5+Y^4+Y^3+Y+1 & Y^5+Y^4+Y^3+Y+1 & Y^6 & Y^6 \end{bmatrix},$$

$$R = \begin{bmatrix} Y^4+Y & Y^6+Y^4+Y^3 & Y^6+Y^3+Y+1 & Y^6+Y^5+Y^4+Y^3+1 \\ Y^3+1 & Y^4+Y^3+Y^2+1 & Y^5+Y^2+Y & Y^6+Y^5+Y^4+1 \\ 1 & 0 & Y^6+Y^4+Y+1 & Y \\ Y^6+Y^5+Y^4+Y^3+Y^2 & Y^6+Y^5+Y^4+Y^3+Y^2 & Y^3+Y^2+1 & Y^3+Y+1 \end{bmatrix}.$$

The corresponding binary quasi-cyclic self-dual codes are all optimal self-dual codes. By successively deleting the first two columns and the first row of K_8, we obtain K_6, K_4, and K_2. More specifically, K_2 induces a $[14, 7, 4]$ code, K_4 induces a $[28, 14, 6]$ code, K_6 induces a $[42, 21, 8]$ code, and K_8 induces a Type II $[56, 28, 12]$ code. The weight enumerator of the $[42, 21, 8]$ code corresponds to W_2 with $\beta = 0$ in [27].

- Case: $q = 4$.

Doing a similar process as before up to the length $\ell = 6$ with $c = 1$, we find the following $M_6 = [L \mid R]$:

$$L = \begin{bmatrix} 1 & 0 & \omega Y^6 + \omega^2 Y^5 + Y^3 + Y + \omega \\ \omega^2 Y^5 + 1 & \omega^2 Y^5 + 1 & 1 \\ Y^6 + \omega^2 Y^4 + \omega^2 Y^2 + \omega^2 Y + \omega^2 & Y^6 + \omega^2 Y^4 + \omega^2 Y^2 + \omega^2 Y + \omega^2 & \omega^2 Y^5 + Y^3 + Y^2 + Y + \omega^2 \end{bmatrix},$$

$$R = \begin{bmatrix} \omega^2 Y^6 + Y^5 + \omega^2 Y^4 + Y^2 + \omega Y + \omega^2 & \omega^2 Y^6 + \omega Y^5 + \omega Y^2 + \omega^2 Y & Y^6 + \omega Y^5 + Y^4 + \omega^2 Y^3 + \omega^2 Y + 1 \\ 0 & \omega Y^6 + Y^5 + \omega^2 Y^3 + \omega^2 Y^2 & Y^5 + \omega Y^4 + \omega Y^3 + \omega^2 Y^2 \\ \omega^2 Y^5 + Y^3 + Y^2 + Y + \omega^2 & Y^6 + \omega Y^5 + \omega Y^4 + Y^3 + \omega^2 Y^2 + Y + \omega^2 & \omega^2 Y^6 + Y^5 + \omega^2 Y^3 + \omega^2 Y^2 + \omega^2 \end{bmatrix}.$$

The corresponding quaternary quasi-cyclic self-dual codes are all optimal or have the best known parameters. By successively deleting the first two columns and the first row of M_6, we obtain M_4 and M_2. More specifically, M_2 induces an optimal self-dual $[14, 7, 6]$ code over $\mathbb{F}_4$, M_4 induces a self-dual code over $\mathbb{F}_4$ with the best known parameters $[28, 14, 9]$, and M_6 induces a self-dual code over $\mathbb{F}_4$ with the best known parameters $[42, 21, 12]$. We denote these codes by $SSD^4_{14}, SSD^4_{28}, SSD^4_{42}$, respectively. We verified that SSD^4_{14} is equivalent to QDC_{14} [16] which is the only known self-dual $[14, 7, 6]$ code over $\mathbb{F}_4$.

Only two self-dual $[28, 14, 9]$ codes over $\mathbb{F}_4$ were known, and one is XQ_{27} [42] and the other is $D_{II,28}$ [2]. The number A_9 of minimum weight codewords of XQ_{27} ($D_{II,28}$, respectively) is 3276 (1092, respectively). On the other hand, our code SSD^4_{28} has $A_9 = 630$. This shows that SSD^4_{28} is a new code. Furthermore, we have checked that SSD^4_{28} is a Type II code over $\mathbb{F}_4$ with minimum Lee weight $d_L = 12$. We recall that a Euclidean self-dual code over $\mathbb{F}_4$ is called *Type II* if its binary image under the Gray map ϕ is Type II (see [18]), where the Gray map ϕ from $GF(4)^n$ to $GF(2)^{2n}$ is defined as $\phi(\omega\mathbf{x} + \overline{\omega}\mathbf{y}) = (\mathbf{x}, \mathbf{y})$ for $\mathbf{x}, \mathbf{y} \in GF(2)^n$ and $(\mathbf{x}, \mathbf{y})$ is the binary vector of length $2n$. We have calculated that $|\mathrm{Aut}(\phi(SSD^4_{28}))| = 7$, $|\mathrm{Aut}(\phi(D_{II,28}))| = 28$, and $|\mathrm{Aut}(\phi(XQ_{27}))| = 2^3 \cdot 3^4 \cdot 7 \cdot 13$.

We have also checked that both $D_{II,28}$ and XQ_{27} are Type II codes over $\mathbb{F}_4$ with $d_L = 12$. We therefore find that there are at least three Lee-extremal Type II $[28, 14, d_L = 12]$ codes over $\mathbb{F}_4$.

We are aware of two papers [4] and [9], in which six Euclidean self-dual $[28, 14, 9]$ codes over $\mathbb{F}_4$ are known to exist. However their generator matrices and the number of minimum weight codewords are not given explicitly. Hence we omit the equivalence check of their codes with SSD^4_{28}.

For length 42, there has been only one self-dual $[42, 21, 12]$ code over $\mathbb{F}_4$, denoted by $(f_2; 11; 17)$ [17]. This code has $A_{12} = 945$, but our code SSD^4_{42} has $A_{12} = 323$ and $d_L = 12$. Hence they are inequivalent, and this implies that SSD^4_{42} is a new code.

In what follows, we give the generator matrix $[L \mid R]$ of SSD^4_{28}:

$$L = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 \\
\omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0 & 1 & 1 & \omega^2 & \omega^2 & 1 & 1 \\
0 & 0 & \omega & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & \omega & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\omega^2 & \omega^2 & \omega & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 \\
0 & 0 & 0 & \omega & 0 & 0 & 1 & 1 & 0 & 0 & \omega & 0 & 1 & 0 \\
0 & 0 & \omega & 0 & \omega^2 & \omega^2 & \omega & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 \\
0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & \omega & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & \omega^2 & 0 & 0 & \omega & 0 & \omega^2 & \omega^2 & \omega & 1 & 0 & 0 \\
0 & 0 & \omega^2 & \omega^2 & 0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & \omega & 0 & 0 \\
1 & 1 & \omega^2 & \omega^2 & 1 & 1 & 1 & \omega^2 & 0 & 0 & \omega & 0 & \omega^2 & \omega^2 \\
0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & \omega^2 & \omega & 0 & 0 \\
1 & 1 & 1 & 0 & 1 & 1 & \omega^2 & \omega^2 & 1 & 1 & 1 & \omega^2 & 0 & 0
\end{bmatrix},$$

$$R=\begin{bmatrix}
\omega^2 & \omega & 0 & 0 & 0 & \omega & 0 & 0 & 1 & 1 & 0 & 0 & \omega & 0\\
1 & \omega^2 & 0 & 0 & \omega & 0 & \omega^2 & \omega^2 & \omega & 1 & 0 & 0 & 1 & \omega^2\\
\omega^2 & \omega^2 & 0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & \omega & 0 & 0 & 1 & 1\\
\omega^2 & \omega^2 & 1 & 1 & 1 & \omega^2 & 0 & 0 & \omega & 0 & \omega^2 & \omega^2 & \omega & 1\\
0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & \omega\\
1 & 0 & 1 & 1 & \omega^2 & \omega^2 & 1 & 1 & 1 & \omega^2 & 0 & 0 & \omega & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & \omega^2 & \omega\\
\omega^2 & \omega^2 & 1 & 1 & 1 & 0 & 1 & 1 & \omega^2 & \omega^2 & 1 & 1 & 1 & \omega^2\\
\omega & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2\\
1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0 & 1 & 1 & \omega^2 & \omega^2\\
1 & 1 & 0 & 0 & \omega & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\omega & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0\\
0 & \omega & 0 & 0 & 1 & 1 & 0 & 0 & \omega & 0 & 1 & 0 & 0 & 0\\
\omega & 0 & \omega^2 & \omega^2 & \omega & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2
\end{bmatrix}.$$

We also give the generator matrix $[L \mid R]$ of SSD^4_{42} in the following:

$$L=\begin{bmatrix}
1 & 0 & \omega & \omega^2 & 0 & 1 & 0 & 0 & 1 & \omega & \omega^2 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 & 0 & 0 & 1\\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & 0\\
\omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0 & \omega^2 & \omega^2 & 1 & 1 & \omega^2 & \omega^2 & 0 & 0 & 1\\
0 & 0 & \omega & \omega^2 & \omega^2 & 1 & 1 & 0 & \omega & \omega^2 & 0 & 1 & 0 & 0 & 1 & \omega & \omega^2 & \omega^2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & \omega & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
1 & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0 & \omega^2 & \omega^2 & 1\\
0 & 0 & \omega^2 & 1 & \omega & \omega & 0 & 0 & \omega & \omega^2 & \omega^2 & 1 & 1 & 0 & \omega & \omega^2 & 0 & 1 & 0 & 0 & 1\\
\omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \omega & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & \omega^2 & \omega^2 & \omega & 1 & 1 & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1\\
0 & 0 & 0 & \omega^2 & 0 & 1 & 0 & 0 & \omega^2 & 1 & \omega & \omega & 0 & 0 & \omega & \omega^2 & \omega^2 & 1 & 1 & 0 & \omega\\
0 & 0 & 0 & 0 & 0 & \omega & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \omega & 0 & 1 & 1 & 1\\
\omega^2 & \omega^2 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & \omega^2 & \omega & 1 & 1 & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2\\
0 & 0 & 1 & 0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^2 & 0 & 1 & 0 & 0 & \omega^2 & 1 & \omega & \omega & 0 & 0 & \omega\\
0 & 0 & 0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & 0 & 0 & \omega & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 0 & 0 & 0\\
0 & 0 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & \omega^2 & \omega & 1 & 1 & 1 & 0\\
0 & 0 & 0 & 1 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^2 & 0 & 1 & 0 & 0 & \omega^2\\
0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & 0 & 0 & \omega & \omega^2 & \omega^2 & 0\\
\omega^2 & \omega^2 & 1 & 1 & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2\\
0 & 0 & 1 & \omega & \omega^2 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & \omega^2 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & 0 & 0 & 0\\
\omega^2 & \omega^2 & 1 & 1 & 1 & 0 & \omega^2 & \omega^2 & 1 & 1 & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & 0
\end{bmatrix},$$

$$R=\begin{bmatrix}
0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^2 & 0 & 1 & 0 & 0 & \omega^2 & 1 & \omega & \omega & 0 & 0 & \omega & \omega^2 & \omega^2 & 1\\
0 & \omega^2 & \omega & 0 & 0 & 0 & 0 & 0 & \omega & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \omega & 0\\
1 & 1 & \omega^2 & \omega^2 & \omega^2 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & \omega^2 & \omega & 1 & 1 & 1 & 0 & 0 & 1 & \omega^2\\
1 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^2 & 0 & 1 & 0 & 0 & \omega^2 & 1 & \omega & \omega\\
0 & \omega^2 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & 0 & 0 & \omega & \omega^2 & \omega^2 & 0 & 0 & 1 & 1\\
1 & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & 0 & 0 & \omega & 0 & 0 & 0 & \omega^2 & \omega^2 & \omega & 1\\
\omega & \omega^2 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & \omega^2 & 0 & 0 & 0 & \omega^2 & 0 & 1\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega & 0 & 0 & 0 & 0 & 0 & \omega\\
1 & 1 & 0 & \omega^2 & \omega^2 & 1 & 1 & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 1 & \omega^2 & \omega^2 & \omega^2 & 0 & 0 & \omega & 0\\
\omega^2 & 0 & 1 & 0 & 0 & 1 & \omega & \omega^2 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0 & 0 & 0 & 1 & 0 & 0 & \omega^2\\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2 & 0 & 0 & 0 & 0 & \omega^2 & \omega\\
\omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0 & \omega^2 & \omega^2 & 1 & 1 & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 1 & \omega^2\\
\omega^2 & \omega^2 & 1 & 1 & 0 & \omega & \omega^2 & 0 & 1 & 0 & 0 & 1 & \omega & \omega^2 & \omega^2 & 0 & 0 & 0 & 1 & \omega & 0\\
0 & \omega & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \omega^2 & \omega^2\\
0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0 & \omega^2 & \omega^2 & 1 & 1 & \omega^2 & \omega^2\\
1 & \omega & \omega & 0 & 0 & \omega & \omega^2 & \omega^2 & 1 & 1 & 0 & \omega & \omega^2 & 0 & 1 & 0 & 0 & 1 & \omega & \omega^2 & \omega^2\\
0 & 1 & 1 & 0 & 0 & 0 & 0 & \omega & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
\omega^2 & \omega & 1 & 1 & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & 1 & 1 & 1 & 0\\
\omega^2 & 0 & 1 & 0 & 0 & \omega^2 & 1 & \omega & \omega & 0 & 0 & \omega & \omega^2 & \omega^2 & 1 & 1 & 0 & \omega & \omega^2 & 0 & 1\\
0 & 0 & \omega & \omega^2 & \omega^2 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & \omega & 0 & 1 & 1 & 1 & 0 & 0 & 0\\
0 & \omega & 0 & 0 & 0 & \omega^2 & \omega^2 & \omega & 1 & 1 & 1 & 0 & 0 & 1 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2 & \omega^2
\end{bmatrix}.$$

The above results are summarized as follows.

Theorem 4.4. *There are at least three monomially inequivalent Euclidean self-dual* $[28, 14, 9]$ *codes over* $\mathbb{F}_4$*, all of which are Lee-extremal Type II. There are at least two monomially inequivalent Euclidean self-dual* $[42, 21, 12]$ *codes over* $\mathbb{F}_4$.

- Case: $q = 5$.

Doing a similar process as before up to the length $\ell = 4$ with $c = 2$, we obtain the following $N_4 = [L \mid R]$:

$$L = \begin{bmatrix} 1 & 0 \\ 2Y^5 + 4Y^4 + Y^3 + Y + 1 & 4Y^5 + 3Y^4 + 2Y^3 + 2Y + 2 \end{bmatrix},$$

$$R = \begin{bmatrix} 3Y^5 + 2Y^4 + Y^3 + 3Y^2 + 4Y & 4Y^6 + 3Y^4 + 3Y^3 + Y^2 + 3Y + 1 \\ Y^4 + 3Y^3 + Y^2 + 4Y + 3 & Y^6 + 2Y^5 + 4Y^4 + 4Y^3 + 3Y^2 + 2Y + 3 \end{bmatrix}.$$

The corresponding quaternary quasi-cyclic self-dual codes are all optimal or have best known parameters. By deleting the first two columns and the first row of N_4, we obtain N_2. More specifically, N_2 induces an optimal self-dual $[14, 7, 6]$ code over $\mathbb{F}_5$, and N_4 induces a self-dual code over $\mathbb{F}_5$ with the best known parameters $[28, 14, 10]$ code, denoted by SSD^5_{28}. We checked that SSD^5_{28} is monomially equivalent to $Q_{28,4}$ in [19].

Acknowledgments

We thank an anonymous referee for his/her helpful comments, which improved the clarity of this paper. We also give thanks to M. Harada and A. Munemasa for a discussion of Section 4.1 in this paper, to C. Huffman for helpful comments, and to Boran Kim for her help in some part of computations done in this paper.

References

[1] E.R. Assmus, J.D. Key, Designs and Their Codes, Cambridge University Press, Cambridge, 1992.
[2] K. Betsumiya, T.A. Gulliver, M. Harada, A. Munemasa, On Type II codes over $\mathbb{F}_4$, IEEE Trans. Inform. Theory 47 (6) (2001) 2242–2248.
[3] A. Bonnecaze, A.D. Bracco, S.T. Dougherty, L.R. Nochefranca, P. Solé, Cubic self-dual binary codes, IEEE Trans. Inform. Theory 49 (9) (2003) 2253–2259.
[4] D. Boucher, F. Ulmer, Coding with skew polynomial rings, J. Symbolic Comput. 44 (12) (2009) 1644–1656, a special issue of Gröbner Bases in Cryptography, Coding and Algebraic Combinatorics.
[5] S. Bouyuklieva, M. Harada, A. Munemasa, Determination of weight enumerators of binary extremal self-dual $[42, 21, 8]$ codes, Finite Fields Appl. 14 (2008) 177–187.
[6] S. Bouyuklieva, N. Yankov, R. Russeva, Classification of the binary self-dual $[42, 21, 8]$ codes having an automorphism of order 3, Finite Fields Appl. 13 (2007) 605–615.
[7] A.D. Bracco, A.M. Natividad, P. Solé, On quintic quasi-cyclic codes, Discrete Appl. Math. 156 (18) (2008) 3362–3375.
[8] J. Cannon, C. Playoust, An Introduction to Magma, University of Sydney, Sydney, Australia, 1994.
[9] P. Cayrel, C. Chabot, A. Necer, Quasi-cyclic codes as codes over rings of matrices, Finite Fields Appl. 16 (2) (2010) 100–115.
[10] J.H. Conway, V. Pless, N.J.A. Sloane, The binary self-dual codes of length up to 32, a revised enumeration, J. Combin. Theory Ser. A 60 (2) (1992) 183–195.
[11] J.H. Conway, N.J.A. Solane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory 36 (1990) 1319–1333.
[12] J.H. Conway, N.J.A. Sloane, Sphere Packing, Lattices and Groups, third ed., Springer-Verlag, New York, 1999.
[13] W. Ebeling, Lattices and Codes. A Course Partially Based on Lectures by F. Hirzebruch, Adv. Lectures Math., Vieweg, Braunschweig, 1994.
[14] P. Gaborit, Personal communication, January 23, 2011.
[15] P. Gaborit, http://www.unilim.fr/pages-perso/philippe.gaborit, January 23, 2011.
[16] P. Gaborit, Quadratic double circulant codes over fields, J. Combin. Theory Ser. A 97 (2002) 85–107.
[17] P. Gaborit, A. Otmani, Experimental constructions of self-dual codes, Finite Fields Appl. 9 (2003) 372–394.
[18] P. Gaborit, V. Pless, P. Solé, O. Atkin, Type II codes over $\mathbb{F}_4$, Finite Fields Appl. 8 (2002) 171–183.
[19] T.A. Gulliver, M. Harada, H. Miyabayashi, Double circulant and quasi-twisted self-dual codes over $\mathbb{F}_5$ and $\mathbb{F}_7$, Adv. Math. Commun. 1 (2007) 223–238.
[20] S. Han, http://kutacc.kut.ac.kr/~sunghyu/data/qcsd/m5q4.pdf.

[21] S. Han, J.-L. Kim, H. Lee, Y. Lee, Construction of cubic self-dual codes, in: Proc. of 2009 IEEE ISIT, 2009, pp. 2396–2399.
[22] M. Harada, New extremal ternary self-dual codes, Australas. J. Combin. 17 (1998) 133–145.
[23] M. Harada, W. Holzmann, H. Kharaghani, M. Khorvash, Extremal ternary self-dual codes constructed from negacirculant matrices, Graphs Combin. 23 (4) (2007) 401–417.
[24] M. Harada, H. Kharaghani, Orthogonal designs, self-dual codes, and the Leech lattice, J. Combin. Des. 13 (2005) 184–194.
[25] M. Harada, A. Munemasa, Classification of self-dual codes of length 36, preprint, available at http://arxiv.org/abs/1012.5464v1.
[26] W.C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, IEEE Trans. Inform. Theory 38 (4) (1992) 1395–1400.
[27] W.C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields Appl. 11 (2005) 451–490.
[28] W.C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, Cambridge, 2003.
[29] K.F. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York/Berlin, 1982.
[30] J.-L. Kim, Y. Lee, Euclidean and Hermitian self-dual MDS codes over large finite fields, J. Combin. Theory Ser. A 105 (2004) 79–95.
[31] Y. Lee, http://math.ewha.ac.kr/~yoonjinl/classification.pdf.
[32] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I. Finite fields, IEEE Trans. Inform. Theory 47 (2001) 2751–2760.
[33] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes III, generator theory, IEEE Trans. Inform. Theory 51 (2005) 2692–2700.
[34] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, The Netherlands, 1977.
[35] C.A. Melchor, P. Gaborit, On the classification of extremal binary self-dual codes, IEEE Trans. Inform. Theory 54 (2008) 4743–4750.
[36] A. Munemasa, http://www.math.is.tohoku.ac.jp/~munemasa/research/codes/sd2.htm.
[37] G. Nebe, E.M. Rains, N.J.A. Sloane, Self-Dual Codes and Invariant Theory, Springer, Berlin, 2006.
[38] M. Ozeki, Quinary code construction of the Leech lattice, Nihonkai Math. J. 2 (1991) 155–167.
[39] V. Pless, N.J.A. Sloane, On the classification and enumeration of self-dual codes, J. Combin. Theory Ser. A 18 (1975) 313–335.
[40] V. Pless, N.J.A. Sloane, H.N. Ward, Ternary codes of minimum weight 6 and the classification of the self-dual codes of length 20, IEEE Trans. Inform. Theory 26 (1980) 305–316.
[41] E. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, The Netherlands, 1998.
[42] J.H. van Lint, F.J. MacWilliams, Generalized quadratic residue codes, IEEE Trans. Inform. Theory 24 (1978) 730–737.