Designs, Codes and Cryptography (2022) 90:2735–2751
https://doi.org/10.1007/s10623-021-00968-3

An improved upper bound on self-dual codes over finite fields $GF(11)$, $GF(19)$, and $GF(23)$

Whan Hyuk Choi[1] · **Jon Lark Kim**[2]

Received: 15 February 2021 / Revised: 27 September 2021 / Accepted: 15 October 2021 /
Published online: 5 November 2021

Abstract
This paper gives new methods of constructing *symmetric self-dual codes* over a finite field $GF(q)$ where q is a power of an odd prime. These methods are motivated by the well-known Pless symmetry codes and quadratic double circulant codes. Using these methods, we construct an amount of symmetric self-dual codes over $GF(11)$, $GF(19)$, and $GF(23)$ of every length less than 42. We also find 153 *new* self-dual codes up to equivalence: they are [32, 16, 12], [36, 18, 13], and [40, 20, 14] codes over $GF(11)$, [36, 18, 14] and [40, 20, 15] codes over $GF(19)$, and [32, 16, 12], [36, 18, 14], and [40, 20, 15] codes over $GF(23)$. They all have new parameters with respect to self-dual codes. Consequently, we improve bounds on the highest minimum distance of self-dual codes, which have not been significantly updated for almost two decades.

Keywords Symmetric self-dual code · Optimal code · Self-dual code · Symmetric generator matrix · Anti-orthogonal matrix

Mathematics Subject Classification Primary 94B05 · Secondary 11T71

The author (Whan-Hyuk Choi) is supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea Government (NRF-2019R1I1A1A01057755) and is supported by NRF under the project code 2020K2A9A1A06108874. The author (Jon-Lark Kim) is supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea government (NRF-2019R1A2C1088676) and is supported by NRF under the project code 2020K2A9A1A06108874.

This is one of several papers published in *Designs, Codes and Cryptography* comprising the "Special Issue: On Coding Theory and Combinatorics: In Memory of Vera Pless".

✉ Jon Lark Kim
jlkim@sogang.ac.kr

Whan Hyuk Choi
choiwh@unist.ac.kr

[1] Department of Biomedical Engineering, 50,UNIST-gil, Ulsan 44919, Republic of Korea

[2] Department of Mathematics, Sogang University, Seoul 04107, Republic of Korea

1 Introduction

Coding theory, one of the most interesting areas of applied mathematics, was born almost simultaneously with the invention of modern computers - the beginning of the error-correcting code came from Claude Shannon's paper "A mathematical theory of communication" in 1948, and Richard W. Hamming's paper "Error detecting and error correcting codes" in 1950. These days, binary and nonbinary codes such as q-ary Hamming codes, the binary and ternary Golay codes, and q-ary Reed-Solomon codes are used in internet communication, GPS signals, mobile phones, and computer devices. It is well known that error-correcting codes are closely related to cryptography [7,24]. Moreover, researchers have recently started investigating the relation between error-correcting codes and deep learning [3,18].

On the other hand, self-dual codes have been the subject of much interest and are regarded as one of the most important classes of error-correcting codes. This is because of both theoretical reason and connections to various fields of mathematics such as designs [16], lattices [2], sphere-packings [9], and modular forms [4].

Among various research topics of self-dual codes, it has attained an extensive research effort to find a *best* code; here, *best* refers to having the greatest error correction ability as possible. The error correction capability of a code depends on the minimum distance. Thus, it is crucial to find a method to construct codes having the highest minimum distance. To this end, various techniques were studied involving circulant and bordered circulant matrices [5,14] and quadratic double circulant matrices [12]. Recently, families of codes over rings have been used to construct self-dual codes over finite fields [10,19].

Despite these efforts, there remain many codes to be found, missed by previous construction methods due to computational complexity. In particular, we hardly know about the optimal minimum distances of self-dual codes over finite fields of order ≥ 5 and of lengths ≥ 22. In this case, only the possible bounds of highest minimum distances are known so far. For example, in the case of codes over $GF(11)$, the bounds of highest minimum distances of lengths ≤ 40 are known, as we can see in Table 4. Moreover, there is no information about the lower bound of the self-dual code of length 28.

In 1972, Vera Pless introduced *Pless symmetry codes*, as a generalization of ternary extended Golay code [22,23]. Using this class of codes, Pless obtained many new optimal self-dual codes over $GF(3)$. Three decades later, Gaborit presented a generalization of Pless symmetry codes to different fields, quadratic double circulant codes [12]. He also found many new self-dual codes over $GF(4)$, $GF(5)$, $GF(7)$, and $GF(9)$. We want to remark two things: one is that these two methods used particular symmetric matrices to construct self-dual codes. The other is that these methods have a limitation of lengths; the possible lengths of codes are limited to $2n + 2$ or $2n$ where n is a power of an odd prime. Thus, there needs a new method to fill the gap between these lengths. These are the main motivation of this paper.

If a self-dual code of length $2n$ over $GF(q)$ has a standard generator matrix $G = (I_n \mid A)$ where A is symmetric, it is called *a symmetric self-dual code*. In [8], we introduced a method of *symmetric building-up construction*. This method was to construct symmetric self-dual codes over $GF(q)$ for $q \equiv 1 \pmod 4$. In [8], we showed that this method provides an efficient way to construct all symmetric self-dual codes over $GF(q)$, increasing lengths by two. Stimulated by this result, we have struggled to find a method when $q \equiv 3 \pmod 4$. However, it is not easy to generalize the method in [8]. In [8], the square root of -1 plays the key role, but unfortunately, it is well-known that the square root of -1 does not exist in $GF(q)$ for $q \equiv 3 \pmod 4$. Nevertheless, we find two novel construction methods as follows :

Table 1 The highest minimum distance d_{sym} of symmetric self-dual codes vs. previously best known minimum distance d_{sd} of self-dual codes [5,8,11–13,15,25]

$\frac{p}{n}$	11		19		23	
	d_{sym}	d_{sd}	d_{sym}	d_{sd}	d_{sym}	d_{sd}
4	3	3	3	3	3	3
8	5	5	5	5	5	5
12	7	7	7	7	7	7
16	8	8	8	8	8	9
20	8	10	11	11	9	10
24	9	9	10	10	10	13
28	10	10	11	11	11	11
32	**12**	?	12	14	**12**	?
36	**13**	12	**14**	?	**14**	12
40	**14**	13	**15**	?	**15**	13

New parameters are written in bold

1. **Construction A**
   Let $(I_n \mid A)$ be a generator matrix of a symmetric self-dual code of length $2n$ over $GF(q)$ and assume that $(\mathbf{x}_n, \mathbf{y}_n)$ is a codeword satisfying $\mathbf{x}_n \cdot \mathbf{y}_n = 0$ and $\mathbf{x}_n \cdot \mathbf{x}_n = k$ such that $-1 \pm k$ are squares in $GF(q)$. And let $B = \begin{pmatrix} \alpha\mathbf{x}_n + \beta\mathbf{y}_n \\ \beta\mathbf{x}_n - \alpha\mathbf{y}_n \end{pmatrix}$ where $\alpha^2 + \beta^2 = -1$, $E = \frac{1}{k}(s\mathbf{x}_n^T\mathbf{x}_n + t\mathbf{y}_n^T\mathbf{y}_n - \mathbf{x}_n^T\mathbf{y}_n - \mathbf{y}_n^T\mathbf{x}_n)$ where $s^2 = -1 + k$ and $t^2 = -1 - k$ and let $D = -\frac{1}{k^2}B(A + E_1)B^T BB^T$. Then
   $$\left(\begin{array}{c|c|c|c} I_2 & O & D & B \\ O & I_n & B^T & A + E \end{array}\right)$$
   is a generator matrix of symmetric self-dual code of length $2n + 4$.
2. **Construction B**
   Let $(I_n \mid A)$ be a generator matrix of a symmetric self-dual code of length $2n$ over $GF(q)$, let $P = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$ be a 2×2 matrix such that $P^2 = -I_2$, and let a matrix $M = \begin{pmatrix} \mathbf{x} \\ \beta^{-1}\mathbf{x}(A - \alpha I) \end{pmatrix}$ for a vector $\mathbf{x}$ in $GF(q)^n$. Assume that H is a 2×2 symmetric matrix satisfying $(H + P)(H - P) = -MM^T$ and $H - P$ is non-singular. Then
   $$\left(\begin{array}{c|c|c|c} I_2 & O & H & M \\ O & I_n & M^T & A + M^T(H - P)^{-1}M \end{array}\right)$$
   is a generator matrix of symmetric self-dual code of length $2n + 4$.

Using these methods, we obtain many new self-dual codes. Consequently, we improve the bounds on the minimum distances of self-dual codes. We revised these results in Table 1. In Table 1, new parameters are written in bold. Throughout this paper, d_{sym} denotes the highest minimum distance of a symmetric self-dual code over $GF(p)$ and d_{sd} denotes the previously best-known minimum distance of self-dual codes over $GF(p)$. More precisely, we give *new* self-dual codes with highest minimum weights: they are [32, 16, 12], [36, 18, 13], and [40, 20, 14] codes over $GF(11)$, [36, 18, 14] and [40, 20, 15] codes over $GF(19)$, and [32, 16, 12], [36, 18, 14], and [40, 20, 15] codes over $GF(23)$. We also provide numbers of new symmetric self-dual codes, up to equivalence, in Table 2.

The paper is organized as follows. Section 2 gives preliminaries for self-dual codes over finite fields. In Sect. 3, we present two construction methods for *symmetric self-dual codes*

Table 2 Numbers of new symmetric self-dual codes of length 32, 36 and 40

p	11		19		23	
n	d_{sym}	# of codes	d_{sym}	# of codes	d_{sym}	# of codes
32	12	≥ 44	12	≥ 801	12	≥ 52
36	13	≥ 16	14	≥ 3	14	≥ 2
40	14	≥ 42	15	≥ 2	15	≥ 1

over $GF(q)$, where q is an odd prime power. In Sect. 4, we give the improved bounds of highest minimum distances and the computational results of the best codes obtained using our new methods. All computations in this paper have been done with the computer algebra system MAGMA [6]. We list all our codes with generator matrices in J.-L. Kim's website [20].

We use the following notations throughout this paper.

Notations	
q	A power of an odd prime number
$GF(q)$	Finite field of order q
d_{sym}	The highest minimum distance of symmetric self-dual codes
d_{sd}	The previous best known minimum distance of self-dual codes
I_n	The identity matrix of degree n
$[n, k, d]_q$ code	A linear code of length n and dimension k over $GF(q)$ with minimum distance d
A^{-1}	The inverse of a matrix A
A^T	The transpose of a matrix A

2 Preliminaries

Let n be a natural number, and $GF(q)$ be the finite field of order q where q is a prime power. A *linear code* $\mathcal{C}$ of length n and dimension k over $GF(q)$ is a k-dimensional subspace of $GF(q)^n$. An element of $\mathcal{C}$ is called a *codeword*. A *generator matrix* of $\mathcal{C}$ is a matrix whose rows form a basis of $\mathcal{C}$; therefore, a generator matrix of a linear code $\mathcal{C}$ of length n and dimension k over $GF(q)$ is a $k \times n$ matrix over $GF(q)$. For vectors $\mathbf{x} = (x_i)$ and $\mathbf{y} = (y_i)$ in $GF(q)^n$, we define the inner product $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$. If vectors are identified with row matrices, the inner product can also be written as a matrix multiplication $\mathbf{x} \cdot \mathbf{y} = \mathbf{x}\mathbf{y}^T$, where $\mathbf{y}^T$ denotes the transpose of $\mathbf{y}$. For a linear code $\mathcal{C}$, the dual code $\mathcal{C}^\perp$ is defined as a set of orthogonal vectors of $\mathcal{C}$, i.e.,

$$\mathcal{C}^\perp = \{\mathbf{x} \in GF(q)^n \mid \mathbf{x} \cdot \mathbf{c} = 0 \, for \ \ all \ \ \mathbf{c} \in \mathcal{C}\}.$$

A linear code $\mathcal{C}$ is called *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$ and *self-orthogonal* if $\mathcal{C} \subset \mathcal{C}^\perp$.

The *weight* of a codeword $\mathbf{c}$ is the number of non-zero symbols in the codeword and denoted by $wt(\mathbf{c})$. The Hamming distance between two codewords $\mathbf{x}$ and $\mathbf{y}$ is defined by $d(\mathbf{x}, \mathbf{y}) = wt(\mathbf{x} - \mathbf{y})$. The *minimum distance* of $\mathcal{C}$, denoted by $d(\mathcal{C})$, is the smallest Hamming distance between distinct codewords in $\mathcal{C}$. A measure for the error-correcting capability of a code is the minimum distance; thus, the minimum distance is regarded as the most important parameter of a code. If a code has the minimum distance that meets some upper bounds, it is called an *optimal code*. It is well-known [17, chapter 2.4.] that a linear code of length n and

Table 3 New quadratic double circulant codes over $GF(q)$ obtained using methods in [12]

length	q	generator matrix	d	length	q	generator matrix	d
28	11	$\mathscr{S}_{13}(3,0)$	10	36	23	$\mathscr{S}_{17}(11,0)$	12
28	17	$\mathscr{S}_{13}(2,0)$	10	40	11	$\mathscr{S}_{19}(3,4)$	13
28	19	$\mathscr{S}_{13}(5,0)$	10	40	13	$\mathscr{S}_{19}(2,4)$	13
28	29	$\mathscr{S}_{13}(4,0)$	10	40	17	$\mathscr{S}_{19}(7,0)$	13
36	11	$\mathscr{S}_{17}(4,0)$	12	40	23	$\mathscr{S}_{19}(2,0)$	13
36	13	$\mathscr{S}_{17}(3,0)$	12	40	29	$\mathscr{S}_{19}(1,3)$	13

dimension k satisfy the Singleton bound,

$$d(\mathcal{C}) \leq n - k + 1.$$

A code that achieves the equality in the Singleton bound is called a *maximum distance separable(MDS)* code. Obviously, a self-dual code of length $2n$ over $GF(q)$ is MDS if the minimum distance equals $n+1$. Although every MDS code is optimal, the MDS conjecture shows that there exists an MDS self-dual code of length $2n$ over $GF(q)$ only if $2n \leq q+1$ for odd q [1]. Therefore, if $2n > q+1$, the minimum distance of self-dual code of length $2n$ over $GF(q)$ is most likely upper bounded by n.

Let I_n be the identity matrix of order n and let A^T denote the transpose of a matrix A. It is well-known that a self-dual code $\mathcal{C}$ of length $2n$ over $GF(q)$ is equivalent to a code with a standard generator matrix

$$\left(I_n \middle| A\right), \tag{1}$$

where A is an $n \times n$ matrix satisfying $AA^T = -I_n$.

A matrix A is called *symmetric* if $A^T = A$. If a self-dual code of length $2n$ over $GF(q)$ has a standard generator matrix $G = (I_n \mid A)$ where A is symmetric, it is called *a symmetric self-dual code*. Since the class of symmetric self-dual codes is a subclass of general self-dual codes, the bound on minimum distances of symmetric self-dual code may be different from that of self-dual codes. However, if a symmetric self-dual code has the same parameter as an optimal(resp. MDS) self-dual code, it is called an *optimal (resp. MDS) symmetric self-dual code*. If the minimum distance of a symmetric self-dual code meets the best known minimum distance of a self-dual code, it is called the *best symmetric self-dual code*.

In [22], Pless introduced Pless symmetry codes as a generalization of ternary extended Golay code and their construction method. As a result, Pless obtained optimal self-dual codes of length 24, 36, 48, and 60 over $GF(3)$. Later in [12] Gaborit presented a generalization of Pless symmetry codes to different fields, quadratic double circulant codes and their construction method. Gaborit obtained many new self-dual codes over $GF(4)$, $GF(5)$, $GF(7)$ and $GF(9)$, and improved the bounds on the highest minimum distances. To use as a reference, we additionally obtain quadratic double circulant codes of lengths ≤ 40 over various finite fields, following the same construction method in [12]. We present these codes in Table 3, following the same notations in [12].

We remark that a self-dual code in the class of Pless symmetry codes or quadratic double circulant codes is equivalent to a symmetric self-dual code. In general, a pure double circulant self-dual code is equivalent to a symmetric self-dual code, and a bordered double circulant self-dual code is equivalent to a symmetric self-dual code under a certain condition. We discuss the equivalence between these codes in the next.

Let S_n be the symmetric group of order n and $\mathbb{D}^n$ be the set of diagonal matrices over $GF(q)$ of order n,

$$\mathbb{D}^n = \{diag(\gamma_i) \mid \gamma_i \in GF(q), \gamma_i^2 = 1\}.$$

The group $\mathcal{M}^n$ of all γ-monomial transformations of length n is defined by

$$\mathcal{M}^n = \{p_\sigma \gamma \mid \gamma \in \mathbb{D}^n, \sigma \in S_n\}$$

where p_σ is the permutation matrix corresponding $\sigma \in S_n$. We note that a γ-monomial transformation preserves the self-orthogonality of a code (see [17, Thm 1.7.6]). Let $\mathcal{C}\tau = \{\mathbf{c}\tau \mid \mathbf{c} \in \mathcal{C}\}$ for an element τ in $\mathcal{M}^n$ and a code $\mathcal{C}$ of length n. If there exists an element $\mu \in \mathcal{M}^n$ such that $\mathcal{C}\mu = \mathcal{C}'$ for two distinct codes $\mathcal{C}$ and $\mathcal{C}'$, then $\mathcal{C}$ and $\mathcal{C}'$ are called *equivalent* and denoted by $\mathcal{C} \simeq \mathcal{C}'$.

Proposition 1 *Let $G = (I_n \mid A)$ and $G' = (I_n \mid B)$ be generator matrices of self-dual codes $\mathcal{C}$ and $\mathcal{C}'$ of length $2n$, respectively. If $A = \mu_1 B \mu_2$ for some $\mu_1, \mu_2 \in \mathcal{M}^n$, then $\mathcal{C}$ and $\mathcal{C}'$ are equivalent.*

Proof For $\mu = \left(\begin{array}{c|c} \mu_1^{-1} & O \\ O & \mu_2 \end{array}\right) \in \mathcal{M}^{2n}$,

$$(I_n \mid A) = (I_n \mid \mu_1 B \mu_2) = (\mu_1^{-1} \mid B\mu_2) = (I_n \mid B)\mu.$$

Thus, $\mathcal{C}$ and $\mathcal{C}'$ are equivalent.

Corollary 1 *Let I_n be the identity matrix of order n, A be an $n \times n$ circulant matrix, B be an $(n-1) \times (n-1)$ circulant matrix. Then,*

(i) *a pure double circulant code over $GF(q)$ with a generator matrix of the form*

$$(I_n \mid A)$$

is equivalent to a code with symmetric generator matrix, and

(ii) *a bordered double circulant code over $GF(q)$ with a generator matrix of the form*

$$\begin{pmatrix} & \alpha & \beta \cdots \beta \\ I_n & \gamma\beta & B \\ & \gamma\beta & \end{pmatrix},$$

where α and β are elements in $GF(q)$ and $\gamma^2 = 1$, is equivalent to a code with symmetric generator matrix.

Proof Let R_n be the $n \times n$ anti-diagonal matrix whose anti-diagonal elements are all 1. Then it is clear that matrices AR_n and BR_{n-1} are symmetric. Thus, the corollary follows directly from Proposition 1.

Let S_{-1} be a set of solutions of the equation $x^2 + y^2 = -1$ over $GF(q)$. Then the cardinality of S_{-1} for an odd prime q is obtained in the next proposition.

Proposition 2 [21] *Let $GF(q)$ be a finite field of order q such that q is a power of an odd prime. The cardinality of the set*

$$S_{-1} = \{(x, y) \in GF(q)^2 \mid x^2 + y^2 + 1 = 0\}$$

is given by

$$|S_{-1}| = q - (-1)^{(q-1)/2} = \begin{cases} q-1, & if\, q \equiv 1 \pmod 4, \\ q+1, & if\, q \equiv 3 \pmod 4. \end{cases}$$

Similarly, we define a set S_{-I_2} of 2×2 symmetric matrices over $GF(q)$ satisfying the matrix equation $X^2 + I_2 = 0$. We also obtain the cardinality of S_{-I_2} in the following corollary.

Corollary 2 *Let $K = GF(q)$ where q is a power of odd prime and let S_{-I_2} be a set of 2×2 symmetric matrices over K such that*

$$S_{-I_2} = \{P \in GL_2(K) \mid P^2 = -I_2\}.$$

Then, the cardinality of S_{-I_2} is given by

$$|S_{-I_2}| = q - (-1)^{(q-1)/2} = \begin{cases} q-1, & if\, q \equiv 1 \pmod 4, \\ q+1, & if\, q \equiv 3 \pmod 4. \end{cases}$$

Proof The condition $P^2 = -I_2$ implies that $P^{-1} = -P$. Since we assumed that P is symmetric, it is easy to show that matrix P is in the form $\begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$, where (α, β) is a solution of the equation $x^2 + y^2 = -1$. Thus, the result follows with Proposition 2.

3 Construction method of symmetric self-dual codes

It is well-known that a self-dual over $GF(q)$ of length n for $q \equiv 1 \pmod 4$ exists if and only if $n \equiv 0 \pmod 2$, and a self-dual over $GF(q)$ of length n for $q \equiv 3 \pmod 4$ exists if and only if $n \equiv 0 \pmod 4$ [17, Theorem 9.1.3]. In [8], we have introduced a construction method for symmetric self-dual codes over $GF(q)$ for $q \equiv 1 \pmod 4$. In this section, we introduce two new construction methods for symmetric self-dual codes over $GF(q)$ for $q \equiv 3 \pmod 4$. These methods generate symmetric self-dual codes of lengths increased by four.

Theorem 1 (Construction method 1) *Let $G = (I_n \mid A)$ be a generator matrix of symmetric self-dual code $\mathcal{C}$ of length $2n$ over $GF(q)$ for an odd prime power q. Assume that there exists a codeword $(\mathbf{x}_n, \mathbf{y}_n)$ in $\mathcal{C}$ satisfying $\mathbf{x}_n \cdot \mathbf{y}_n = 0$, $\mathbf{x}_n \cdot \mathbf{x}_n = k (\neq 0)$, and $-1 \pm k$ are squares in $GF(q)$. Then, take an element (α, β) in S_{-1} and let $B = \begin{pmatrix} \alpha \mathbf{x}_n + \beta \mathbf{y}_n \\ \beta \mathbf{x}_n - \alpha \mathbf{y}_n \end{pmatrix}$, $E = \frac{1}{k}(s\mathbf{x}_n^T \mathbf{x}_n + t\mathbf{y}_n^T \mathbf{y}_n - \mathbf{x}_n^T \mathbf{y}_n - \mathbf{y}_n^T \mathbf{x}_n)$ where $s^2 = -1 + k$ and $t^2 = -1 - k$, and let $D = -\frac{1}{k^2} B(A + E)B^T B B^T$. Then*

$$G_1 = (I_{n+2} \mid A_1) = \left(\begin{array}{c|c|c|c} I_2 & O & D & B \\ O & I_n & B^T & A + E \end{array}\right)$$

is a generator matrix of a symmetric self-dual code of length $2n + 4$.

Proof Since the code $\mathcal{C}$ has the generator matrix $G = (I_n \mid A)$, the vector $\mathbf{x}_n G = \mathbf{x}_n (I_n \mid A) = (\mathbf{x}_n, \mathbf{y}_n)$ is a codeword in $\mathcal{C}$ for any $\mathbf{x}_n$ in $GF(q)^n$ and $\mathbf{y}_n = \mathbf{x}_n A$. Hence,

$$\mathbf{x}_n \cdot \mathbf{y}_n = 0 \Leftrightarrow \mathbf{x}_n (\mathbf{x}_n A)^T = \mathbf{x}_n A \mathbf{x}_n^T = 0.$$

Therefore, if there exists a vector $\mathbf{x}_n$ which makes $\mathbf{x}_n A \mathbf{x}_n^T$ become zero for the matrix A, then we let $(\mathbf{x}_n, \mathbf{y}_n) = (\mathbf{x}_n, \mathbf{x}_n A)$ for the assumption in this theorem. If there is no vector $\mathbf{x}_n$

satisfying $\mathbf{x}_n A \mathbf{x}_n^T = 0$, then we cannot apply this theorem on $\mathcal{C}$. It is obvious that the matrix A_1, A, D, and E are symmetric. Thus, we have to show that

$$A_1 A_1^T = \left(\begin{array}{c|c} D & B \\ B^T & A+E \end{array}\right)\left(\begin{array}{c|c} D^T & B \\ B^T & A^T+E^T \end{array}\right) = -I_{n+2}.$$

In other words, we have to show that following three identities hold :

$$D^2 + BB^T = -I_2, \tag{2}$$
$$DB + B(A+E) = O_{2\times n}, \tag{3}$$
$$B^T B + (A+E)^2 = -I_n. \tag{4}$$

Firstly, we verify the equality of (2). By the assumptions, we have that $A^2 = -I_n$, $\alpha^2 + \beta^2 = -1$ and $\mathbf{x}_n \mathbf{x}_n^T = k$. Since $(\mathbf{x}_n, \mathbf{y}_n)$ is a codeword of a self-dual code $\mathcal{C}$, it is also clear that $\mathbf{x}_n \mathbf{x}_n^T + \mathbf{y}_n \mathbf{y}_n^T = 0$ and $(\mathbf{x}_n, \mathbf{y}_n) G^T = \mathbf{x}_n + \mathbf{y}_n A = O_n$. Thus, $\mathbf{y}_n \mathbf{y}_n^T = -k$, $\mathbf{y}_n A = -\mathbf{x}_n$ and $\mathbf{x}_n A = \mathbf{y}_n$. By direct computations, we obtain that

$$\begin{aligned} BAB^T &= \begin{pmatrix} \alpha\mathbf{x}_n A + \beta \mathbf{y}_n A \\ \beta \mathbf{x}_n A - \alpha \mathbf{y}_n A \end{pmatrix}\begin{pmatrix} \alpha\mathbf{x}_n + \beta \mathbf{y}_n \\ \beta \mathbf{x}_n - \alpha \mathbf{y}_n \end{pmatrix}^T \\ &= \begin{pmatrix} \alpha\mathbf{y}_n - \beta \mathbf{x}_n \\ \beta \mathbf{y}_n + \alpha \mathbf{x}_n \end{pmatrix}\left(\alpha\mathbf{x}_n^T + \beta \mathbf{y}_n^T \;\; \beta\mathbf{x}_n^T - \alpha \mathbf{y}_n^T\right) \\ &= \begin{pmatrix} -2k\alpha\beta & k(\alpha^2-\beta^2) \\ k(\alpha^2-\beta^2) & 2k\alpha\beta \end{pmatrix}, \end{aligned}$$

and

$$\begin{aligned} BEB^T &= \frac{1}{k}\begin{pmatrix} \alpha\mathbf{x}_n + \beta \mathbf{y}_n \\ \beta \mathbf{x}_n - \alpha \mathbf{y}_n \end{pmatrix}\left(s\mathbf{x}_n^T\mathbf{x}_n + t\mathbf{y}_n^T\mathbf{y}_n - \mathbf{x}_n^T\mathbf{y}_n - \mathbf{y}_n^T\mathbf{x}_n\right)\begin{pmatrix} \alpha\mathbf{x}_n + \beta \mathbf{y}_n \\ \beta \mathbf{x}_n - \alpha \mathbf{y}_n \end{pmatrix}^T \\ &= \frac{1}{k}\begin{pmatrix} k\alpha s\mathbf{x}_n - k\alpha\mathbf{y}_n - k\beta t\mathbf{y}_n + k\beta\mathbf{x}_n \\ k\beta s\mathbf{x}_n - k\beta\mathbf{y}_n + k\alpha t\mathbf{y}_n - k\alpha\mathbf{x}_n \end{pmatrix}\left(\alpha\mathbf{x}_n^T + \beta\mathbf{y}_n^T \;\; \beta\mathbf{x}_n^T - \alpha\mathbf{y}_n^T\right) \\ &= \begin{pmatrix} k\alpha^2 s + 2k\alpha\beta + k\beta^2 t & k\alpha\beta s + k\beta^2 - k\alpha^2 - k\alpha\beta t \\ k\alpha\beta s + k\beta^2 - k\alpha^2 - k\alpha\beta t & k\alpha^2 t - 2k\alpha\beta + k\beta^2 s \end{pmatrix}. \end{aligned}$$

Therefore,

$$B(A+E)B^T = BAB^T + BEB^T = \begin{pmatrix} k\alpha^2 s + k\beta^2 t & k\alpha\beta s - k\alpha\beta t \\ k\alpha\beta s - k\alpha\beta t & k\alpha^2 t + k\beta^2 s \end{pmatrix},$$

and

$$\begin{aligned} D &= -\frac{1}{k^2}(B(A+E)B^T)BB^T \\ &= -\frac{1}{k}\begin{pmatrix} \alpha^2 s + \beta^2 t & \alpha\beta s - \alpha\beta t \\ \alpha\beta s - \alpha\beta t & \alpha^2 t + \beta^2 s \end{pmatrix} BB^T. \end{aligned}$$

Since $BB^T = k\begin{pmatrix} \alpha^2-\beta^2 & 2\alpha\beta \\ 2\alpha\beta & -\alpha^2+\beta^2 \end{pmatrix}$, we obtain

$$\begin{aligned} D &= -\begin{pmatrix} \alpha^2 s+\beta^2 t & \alpha\beta s-\alpha\beta t \\ \alpha\beta s-\alpha\beta t & \alpha^2 t+\beta^2 s \end{pmatrix}\begin{pmatrix} \alpha^2-\beta^2 & 2\alpha\beta \\ 2\alpha\beta & -\alpha^2+\beta^2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha^2 s-\beta^2 t & \alpha\beta(s+t) \\ \alpha\beta(s+t) & -\alpha^2 t+\beta^2 s \end{pmatrix}. \end{aligned}$$

Hence,

$$\begin{aligned} D^2+BB^T &= \begin{pmatrix} \alpha^2 s-\beta^2 t & -\alpha\beta(s+t) \\ -\alpha\beta(s+t) & \alpha^2 t-\beta^2 s \end{pmatrix}^2 + k\begin{pmatrix} \alpha^2-\beta^2 & 2\alpha\beta \\ 2\alpha\beta & -\alpha^2+\beta^2 \end{pmatrix} \\ &= \begin{pmatrix} -\alpha^2 s^2-\beta^2 t^2 & -\alpha\beta(s^2-t^2) \\ -\alpha\beta(s^2-t^2) & -\alpha^2 t^2-\beta^2 s^2 \end{pmatrix} + k\begin{pmatrix} \alpha^2-\beta^2 & 2\alpha\beta \\ 2\alpha\beta & -\alpha^2+\beta^2 \end{pmatrix} \\ &= \begin{pmatrix} \alpha^2(k-s^2)-\beta^2(k+t^2) & \alpha\beta(2k-s^2+t^2) \\ \alpha\beta(2k-s^2+t^2) & -\alpha^2(k+t^2)+\beta^2(k-s^2) \end{pmatrix}. \end{aligned}$$

Since $s^2 = -1+k$ and $t^2 = -1-k$, we have that $k-s^2 = 1$, $k+t^2 = -1$ and $-s^2+t^2 = 2k$. Therefore,

$$\begin{aligned} D^2+BB^T &= \begin{pmatrix} \alpha^2+\beta^2 & \alpha\beta(2k-2k) \\ \alpha\beta(2k-2k) & \alpha^2+\beta^2 \end{pmatrix} \\ &= -I_2, \end{aligned}$$

which is desired. The identities (3) and (4) are verified by similar computations.

We need following two lemmas to introduce the second construction method.

Lemma 1 *Let* $P = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$ *be an element in* S_{-I_2} *and* A *be a symmetric matrix satisfying* $A^2 = -I_n$. *For a vector* $\mathbf{x}$ *in* $GF(q)^n$, *if we let the matrix* $M = \begin{pmatrix} \mathbf{x} \\ \beta^{-1}\mathbf{x}(A-\alpha I) \end{pmatrix}$, *then*

$$MA = PM.$$

Proof Let $\mathbf{y} = \beta^{-1}\mathbf{x}(A-\alpha I)$. Then $\beta\mathbf{y} = \mathbf{x}A - \alpha\mathbf{x}$ and this implies that $\mathbf{x}A = \alpha\mathbf{x} + \beta\mathbf{y}$. On the other hand,

$$\begin{aligned} \mathbf{y}(A+\alpha I) &= \beta^{-1}\mathbf{x}(A-\alpha I)(A+\alpha I) \\ &= \beta^{-1}\mathbf{x}(A^2-\alpha^2 I) \\ &= \beta^{-1}\mathbf{x}(-1-\alpha^2)I \\ &= \beta\mathbf{x}, \text{ since } \alpha^2+\beta^2 = -1 \end{aligned}$$

and this implies that $\mathbf{y}A = \beta\mathbf{x} - \alpha\mathbf{y}$. Therefore,

$$MA = \begin{pmatrix} \mathbf{x}A \\ \mathbf{y}A \end{pmatrix} = \begin{pmatrix} \alpha\mathbf{x}+\beta\mathbf{y} \\ \beta\mathbf{x}-\alpha\mathbf{y} \end{pmatrix} = PM.$$

Lemma 2 *Assume that* $n \times n$ *matrices* H *and* P *are symmetric. If* $(H+P)(H-P)$ *is also symmetric, then* $HP = PH$.

Proof By the assumption, we have

$$\begin{aligned}(H-P)(H+P) &= \{(H-P)(H+P)\}^T \\ &= (H+P)^T(H-P)^T \\ &= (H+P)(H-P),\end{aligned}$$

and by equating both sides, the result follows.

Now, we give the next theorem, which introduces the second construction method.

Theorem 2 (Construction 2) *Let $G = (I_n \mid A)$ be a generator matrix of a symmetric self-dual code $\mathcal{C}$ of length $2n$ over $GF(p)$ for an odd prime p and let S_{-I_2} be the set defined in Corollary 2, and let $P = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$ be an element in S_{-I_2}. Let $M = \begin{pmatrix} \mathbf{x} \\ \beta^{-1}\mathbf{x}(A-\alpha I) \end{pmatrix}$ for a vector $\mathbf{x}$ in $GF(q)^n$. Assume that H is a 2×2 symmetric matrix satisfying the equation*

$$(H+P)(H-P) = -MM^T, \tag{5}$$

and $H-P$ is non-singular. Then

$$G_2 = (I_{n+2} \mid A_2) = \left(\begin{array}{c|c|c|c} I_2 & O & H & M \\ O & I_n & M^T & A+M^T(H-P)^{-1}M \end{array}\right)$$

is a generator matrix of a symmetric self-dual code of length $2n+4$.

Proof It is easy to check that A_2 is symmetric. Therefore, we have only to show that A_2 is anti-orthogonal, i.e.,

$$\left(\begin{array}{c|c} H & M \\ M^T & A+M^T(H-P)^{-1}M \end{array}\right)\left(\begin{array}{c|c} H & M \\ M^T & A+M^T(H-P)^{-1}M \end{array}\right) = -I_{n+2}.$$

In other words, we have to show that following three identities are hold :

$$H^2 + MM^T = -I_2, \tag{6}$$

$$HM + M(A+M^T(H-P)^{-1}M) = O_{2\times n}, \tag{7}$$

$$M^TM + (A+M^T(H-P)^{-1}M)^2 = -I_n. \tag{8}$$

We note that, with the assumption, $MA = PM$ and $HP = PH$ by Lemmas 1 and 2.

First, it is easy to show that the identity (6) is true from the Eq. (5). For the identity (7), we calculate that

$$\begin{aligned}HM + M(A+M^T(H-P)^{-1}M) &= HM + MA + MM^T(H-P)^{-1}M \\ &= (H+P)M + MM^T(H-P)^{-1}M \\ &= ((H+P)(H-P) + MM^T)(H-P)^{-1}M \\ &= O_2(H-P)^{-1}M \\ &= O_{2\times n}\end{aligned}$$

and the result follows.

Finally, for the identity (8), we expand the left hand side of (8):

$$\begin{aligned}&M^TM + (A+M^T(H-P)^{-1}M)^2 \\ &\quad = M^TM + A^2 + AM^T(H-P)^{-1}M + M^T(H-P)^{-1}MA \\ &\qquad + M^T(H-P)^{-1}MM^T(H-P)^{-1}M. \end{aligned} \tag{9}$$

Note that A^2, the second term of (9) equals $-I_n$. We compute the sum of (9) except the last term:

$$\begin{aligned}
&M^TM + A^2 + AM^T(H-P)^{-1}M + M^T(H-P)^{-1}MA\\
&= M^TM - I_n + M^TP(H-P)^{-1}M + M^T(H-P)^{-1}PM\\
&= -I_n + M^T(I_n + P(H-P)^{-1} + (H-P)^{-1}P)M\\
&= -I_n + M^T(H-P)^{-1}((H-P)^2 + (H-P)P + P(H-P))(H-P)^{-1}M\\
&= -I_n + M^T(H-P)^{-1}(H^2-P^2)(H-P)^{-1}M.
\end{aligned}$$

And we put $MM^T = -(H+P)(H-P)$ in the last term of (9) to calculate

$$\begin{aligned}
&M^T(H-P)^{-1}MM^T(H-P)^{-1}M\\
&= -M^T(H-P)^{-1}(H+P)(H-P)(H-P)^{-1}M\\
&= -M^T(H-P)^{-1}(H^2-P^2)(H-P)^{-1}M.
\end{aligned}$$

Therefore, we obtain that

$$M^TM + (A + M^T(H-P)^{-1}M)^2 = -I_n,$$

and this is desired.

We illustrate these new construction methods in the following examples.

Example 1 Let $\mathcal{C}_3^8$ be a symmetric optimal self-dual [8,4,3] code over $GF(3)$ with generator matrix

$$G = \begin{pmatrix} 1&0&0&0&1&1&0&0\\ 0&1&0&0&1&2&0&0\\ 0&0&1&0&0&0&2&1\\ 0&0&0&1&0&0&1&1 \end{pmatrix}.$$

To apply construction method in Theorem 1, take $(\alpha, \beta) = (1, 1)$ and the codeword $(\mathbf{x}_n|\mathbf{y}_n) = (2, 1, 1, 1, 0, 1, 0, 2)$ in $\mathcal{C}_3^8$. Then, we compute that $B = \begin{pmatrix} 2&2&1&0\\ 2&0&1&2 \end{pmatrix}$, $D = \begin{pmatrix} 2&1\\ 1&2 \end{pmatrix}$, and $E = \begin{pmatrix} 0&1&0&2\\ 1&2&2&2\\ 0&2&0&1\\ 2&2&1&0 \end{pmatrix}$.

Finally, we find an optimal symmetric self-dual [12,6,6] over $GF(3)$ code with generator matrix

$$G_1 = \begin{pmatrix} 1&0&0&0&0&0&2&1&2&2&1&0\\ 0&1&0&0&0&0&1&2&2&0&1&2\\ 0&0&1&0&0&0&2&2&1&2&0&2\\ 0&0&0&1&0&0&2&0&2&1&2&2\\ 0&0&0&0&1&0&1&1&0&2&2&2\\ 0&0&0&0&0&1&0&2&2&2&2&1 \end{pmatrix}.$$

Example 2 Let $\mathcal{C}_{19}^8$ be a symmetric self-dual [8,4,3] code over $GF(19)$ with generator matrix

$$G = \begin{pmatrix} 1&0&0&0&18&13&0&0\\ 0&1&0&0&13&1&0&0\\ 0&0&1&0&0&0&1&6\\ 0&0&0&1&0&0&6&18 \end{pmatrix}.$$

To apply construction method in Theorem 2, take $(\alpha, \beta) = (18, 6)$ and $\mathbf{x} = (1, 6, 9, 6)$ in $GF(19)^4$. Then, $M = \begin{pmatrix} 1&6&9&6\\ 13&1&9&9 \end{pmatrix}$ and $H = \begin{pmatrix} 9&12\\ 12&13 \end{pmatrix}$, and finally, we obtain a symmetric [12,6,7] self-dual code over $GF(19)$ of length 12 with generator matrix

$$G_2 = \begin{pmatrix} 1&0&0&0&0&0&9&12&1&6&9&6\\ 0&1&0&0&0&0&12&13&13&1&9&9\\ 0&0&1&0&0&0&1&13&7&17&13&14\\ 0&0&0&1&0&0&6&1&17&14&7&6\\ 0&0&0&0&1&0&9&9&13&7&12&11\\ 0&0&0&0&0&1&6&9&14&6&11&2 \end{pmatrix}.$$

4 Computational results

In this section, we discuss computational results of symmetric self-dual codes over $GF(q)$ for $q = 11, 19, 23$. Using construction methods in Theorems 1 and 2, we obtain many new symmetric self-dual codes of lengths $n \leq 40$ which meet the best known bounds on minimum distances of self-dual codes.

We find the best symmetric self-dual codes of length n over $GF(q)$ for $q = 11, 19, 23$ and $n \leq 40$ except for the case that $q = 11$ with $n = 16$ or 20, for the case that $q = 19$ with $n = 32$, and for the case that $q = 23$ with $n = 20$ or 24. Moreover, we also find more than 151 self-dual codes with new parameters: 90 inequivalent self-dual codes of length 32, 36 and 40 over $GF(11)$, 5 inequivalent self-dual codes of length 36 and 40 over $GF(19)$ and 56 inequivalent self-dual codes of length 32, 26 and 40 over $GF(23)$. Among them, we introduce five symmetric self-dual codes with their generator matrices in this section.

At the end of this section, we summarize the known bounds on the highest minimum distances of self-dual codes in Table 7.

4.1 Symmetric self-dual codes over *GF*(11)

Proposition 3 *There exist the best symmetric self-dual codes over* $GF(11)$ *of length* $n = 4, 8, 12, 24, 28, 32, 36, 40$. *In particular,* $[4, 2, 3]_{11}$, $[8, 4, 5]_{11}$ *and* $[12, 6, 7]_{11}$ *symmetric self-dual codes are MDS. Moreover,* $[32, 16, 12]_{11}$, $[36, 18, 13]_{11}$ *and* $[40, 20, 14]_{11}$ *codes are new.*

We give the highest minimum distance d_{sym} of symmetric self-dual codes and the previously best known minimum distance d_{sd} of self-dual codes in Table 4. In this table, new parameters are written in bold. We present three symmetric self-dual codes having new parameters:

– $[32, 16, 12]_{11}$ code with a generator matrix $(I_{16} \mid A_{11}^{32})$ where

$$A_{11}^{32} = \begin{pmatrix}
6 & 7 & 7 & 1 & 2 & 8 & 5 & 9 & 9 & 8 & 1 & 6 & 4 & 7 & 10 & 6 \\
7 & 9 & 7 & 8 & 0 & 8 & 4 & 8 & 6 & 10 & 2 & 6 & 9 & 7 & 8 & 10 \\
7 & 7 & 6 & 0 & 8 & 2 & 4 & 9 & 1 & 6 & 8 & 7 & 6 & 9 & 0 & 4 \\
1 & 8 & 0 & 7 & 0 & 7 & 10 & 2 & 1 & 9 & 9 & 3 & 3 & 2 & 8 & 0 \\
2 & 0 & 8 & 0 & 10 & 10 & 8 & 10 & 3 & 0 & 10 & 8 & 0 & 8 & 10 & 0 \\
8 & 8 & 2 & 7 & 10 & 7 & 10 & 2 & 9 & 7 & 7 & 0 & 6 & 1 & 0 & 3 \\
5 & 4 & 4 & 10 & 8 & 10 & 10 & 7 & 8 & 5 & 2 & 5 & 4 & 8 & 3 & 9 \\
9 & 8 & 9 & 2 & 10 & 2 & 7 & 0 & 3 & 2 & 8 & 10 & 7 & 8 & 4 & 6 \\
9 & 6 & 1 & 1 & 3 & 9 & 8 & 3 & 0 & 1 & 5 & 10 & 7 & 7 & 8 & 10 \\
8 & 10 & 6 & 9 & 0 & 7 & 5 & 2 & 1 & 9 & 9 & 1 & 1 & 9 & 4 & 4 \\
1 & 2 & 8 & 9 & 10 & 7 & 2 & 8 & 5 & 9 & 3 & 7 & 7 & 2 & 9 & 4 \\
6 & 6 & 7 & 3 & 8 & 0 & 5 & 10 & 10 & 1 & 7 & 7 & 2 & 6 & 8 & 2 \\
4 & 9 & 6 & 3 & 0 & 6 & 4 & 7 & 7 & 1 & 7 & 2 & 5 & 7 & 7 & 6 \\
7 & 7 & 9 & 2 & 8 & 1 & 8 & 8 & 7 & 9 & 2 & 6 & 7 & 4 & 1 & 5 \\
10 & 8 & 0 & 8 & 10 & 0 & 3 & 4 & 8 & 4 & 9 & 8 & 7 & 1 & 7 & 2 \\
6 & 10 & 4 & 0 & 0 & 3 & 9 & 6 & 10 & 4 & 4 & 2 & 6 & 5 & 2 & 9
\end{pmatrix}$$

– $[36, 18, 13]_{11}$ code with a generator matrix $(I_{18} \mid A_{11}^{36})$ where

$$A_{11}^{36} = \begin{pmatrix}
5 & 10 & 6 & 7 & 5 & 4 & 7 & 1 & 9 & 4 & 4 & 7 & 7 & 8 & 1 & 8 & 8 & 8 \\
10 & 10 & 8 & 7 & 6 & 4 & 5 & 8 & 9 & 7 & 10 & 1 & 3 & 0 & 5 & 8 & 9 & 9 \\
6 & 8 & 10 & 6 & 4 & 2 & 4 & 6 & 10 & 0 & 1 & 5 & 6 & 9 & 1 & 9 & 5 & 1 \\
7 & 7 & 6 & 3 & 4 & 3 & 4 & 2 & 1 & 10 & 4 & 1 & 5 & 3 & 7 & 8 & 4 & 6 \\
5 & 6 & 4 & 4 & 6 & 3 & 7 & 4 & 8 & 9 & 9 & 9 & 9 & 10 & 0 & 4 & 5 & 9 \\
4 & 4 & 2 & 3 & 3 & 1 & 7 & 2 & 2 & 0 & 3 & 7 & 6 & 6 & 5 & 1 & 1 & 4 \\
7 & 5 & 4 & 4 & 7 & 7 & 6 & 4 & 10 & 7 & 1 & 2 & 9 & 1 & 4 & 0 & 6 & 7 \\
1 & 8 & 6 & 2 & 4 & 2 & 4 & 3 & 7 & 8 & 4 & 1 & 1 & 1 & 2 & 2 & 1 & 4 \\
9 & 9 & 10 & 1 & 8 & 2 & 10 & 7 & 3 & 8 & 7 & 6 & 9 & 9 & 3 & 3 & 1 & 7 \\
4 & 7 & 0 & 10 & 9 & 0 & 7 & 8 & 8 & 0 & 5 & 0 & 0 & 8 & 0 & 4 & 8 & 10 \\
4 & 10 & 1 & 4 & 9 & 3 & 1 & 4 & 7 & 5 & 2 & 10 & 3 & 3 & 2 & 0 & 1 & 3 \\
7 & 1 & 5 & 1 & 9 & 7 & 2 & 1 & 6 & 0 & 10 & 0 & 0 & 8 & 6 & 5 & 0 & 0 \\
7 & 3 & 6 & 5 & 9 & 6 & 9 & 1 & 9 & 0 & 3 & 0 & 9 & 7 & 6 & 7 & 5 & 0 \\
8 & 0 & 9 & 3 & 10 & 6 & 1 & 1 & 9 & 8 & 3 & 8 & 7 & 8 & 8 & 1 & 5 & 10 \\
1 & 5 & 1 & 7 & 0 & 5 & 4 & 2 & 3 & 0 & 2 & 6 & 6 & 8 & 10 & 0 & 8 & 7 \\
8 & 8 & 9 & 8 & 4 & 1 & 0 & 2 & 3 & 4 & 0 & 5 & 7 & 1 & 0 & 2 & 9 & 2 \\
8 & 9 & 5 & 4 & 5 & 1 & 6 & 1 & 1 & 8 & 1 & 0 & 5 & 5 & 8 & 9 & 4 & 10 \\
8 & 9 & 1 & 6 & 9 & 4 & 7 & 4 & 7 & 10 & 3 & 0 & 0 & 10 & 7 & 2 & 10 & 6
\end{pmatrix}$$

Table 4 The best known minimum distances of symmetric self-dual codes over $GF(11)$

$[n, k, d]_p$	$d_{sym.}$	$d_{sd.}$	Refs.	$[n, k, d]_p$	$d_{sym.}$	$d_{sd.}$	Refs.
$[4, 2, 3]_{11}$	3	3	[5]	$[24, 12, 9]_{11}$	9	9−12	[5]
$[8, 4, 5]_{11}$	5	5	[5]	$[28, 14, 10]_{11}$	10	10−14	[25]
$[12, 6, 7]_{11}$	7	7	[5]	$\mathbf{[32, 16, 12]_{11}}$	**12**	?−16	–
$[16, 8, 8]_{11}$	8	8	[5]	$\mathbf{[36, 18, 13]_{11}}$	**13**	12−18	Table 3
$[20, 10, 8]_{11}$	8	10	[5]	$\mathbf{[40, 20, 14]_{11}}$	**14**	13−20	Table 3

Bold values represent new parameters

– $[40, 20, 14]_{11}$ code with a generator matrix $(I_{20} \mid A_{11}^{40})$ where

$$A_{11}^{40} = \begin{pmatrix}
5&4&6&1&7&10&5&5&8&8&10&4&9&5&9&5&8&3&9&6\\
4&2&6&3&1&2&1&2&5&8&2&4&5&9&1&7&5&7&3&4\\
6&6&2&9&4&4&9&5&1&8&6&2&6&9&10&5&6&0&5&0\\
1&3&9&5&3&10&2&4&10&3&1&10&9&7&8&9&10&7&0&0\\
7&1&4&3&7&3&8&0&1&7&7&6&0&5&7&10&9&6&5&0\\
10&2&4&10&3&6&0&9&3&9&4&8&9&0&3&4&6&8&0&5\\
5&1&9&2&8&0&4&6&1&2&4&8&6&3&8&5&5&4&3&3\\
5&2&5&4&0&9&6&3&4&7&8&8&3&2&10&3&2&3&3&7\\
8&5&1&10&1&3&1&4&0&7&9&3&2&9&9&2&9&9&1&6\\
8&8&8&3&7&9&2&7&7&5&3&9&3&0&5&8&5&6&8&8\\
10&2&6&1&7&4&4&8&9&3&6&6&1&5&7&10&2&3&8&6\\
4&4&2&10&6&8&8&8&3&9&6&6&10&5&2&6&7&6&6&1\\
9&5&6&9&0&9&6&3&2&3&1&10&4&9&4&7&3&2&8&10\\
5&9&9&7&5&0&3&2&9&0&5&5&9&2&6&8&2&10&8&0\\
9&1&10&8&7&3&8&10&9&5&7&2&4&6&1&3&6&1&7&4\\
5&7&5&9&10&4&5&3&2&8&10&6&7&8&3&4&9&2&5&3\\
8&5&6&10&9&6&5&2&9&5&2&7&3&2&6&9&4&9&3&6\\
3&7&0&7&6&8&4&3&9&6&3&6&2&10&1&2&9&6&7&1\\
9&3&5&0&5&0&3&3&1&8&8&6&8&8&7&5&3&7&3&10\\
6&4&0&0&0&5&3&7&6&8&6&1&10&0&4&3&6&1&10&2
\end{pmatrix}$$

4.2 Symmetric self-dual codes over *GF*(19)

Proposition 4 *There exist the best symmetric self-dual codes over* $GF(19)$ *of length* $n = 4, 8, 12, 16, 20, 24, 28, 36, 40$. *Among them,* $[4, 2, 3]_{19}$, $[8, 4, 5]_{19}$, $[12, 6, 7]_{19}$, *and* $[20, 10, 11]_{19}$ *codes are MDS. Moreover,* $[36, 18, 14]_{19}$ *and* $[40, 20, 15]_{19}$ *codes are new.*

We give the highest minimum distance d_{sym} of symmetric self-dual codes and the previously best known minimum distance d_{sd} of self-dual codes in Table 5. In this table, new parameters are written in bold. We present two symmetric self-dual codes having new parameters:

– $[32, 16, 12]_{19}$ code with a generator matrix $(I_{16} \mid A_{19}^{32})$ where

$$A_{19}^{32} = \begin{pmatrix}
15&16&3&3&5&6&5&11&8&15&10&16&1&2&2&11\\
16&0&10&17&2&1&15&3&5&3&8&5&10&1&8&9\\
3&10&3&15&14&12&16&6&5&0&6&12&18&7&0&2\\
3&17&15&2&12&14&3&3&4&16&12&15&14&7&10&3\\
5&2&14&12&7&15&14&16&2&16&8&3&4&14&12&1\\
6&1&12&14&15&4&18&3&0&15&8&0&16&9&13&18\\
5&15&16&3&14&18&9&10&2&0&5&5&10&3&0&11\\
11&3&6&3&16&3&10&7&17&17&0&6&16&3&8&5\\
8&5&5&4&2&0&2&17&8&14&12&18&16&7&2&6\\
15&3&0&16&16&15&0&17&14&7&1&16&13&3&9&12\\
10&8&6&12&8&8&5&0&12&1&8&12&13&16&16&11\\
16&5&12&15&3&0&5&6&18&16&12&8&8&6&16&4\\
1&10&18&14&4&16&10&16&16&13&13&8&4&3&2&18\\
2&1&7&7&14&9&3&3&7&3&16&6&3&14&13&13\\
2&8&0&10&12&13&0&8&2&9&16&16&2&13&4&6\\
11&9&2&3&1&18&11&5&6&12&11&4&18&13&6&14
\end{pmatrix}$$

Table 5 The best known minimum distances of self-dual codes over $GF(19)$

$[n, k, d]_p$	d_{sym}	d_{sd}	Refs.	$[n, k, d]_p$	d_{sym}	d_{sd}	Refs.
$[4, 2, 3]_{19}$	3	3	[5]	$[24, 12, 10]_{19}$	10	10−12	[25]
$[8, 4, 5]_{19}$	5	5	[5]	$[28, 14, 11]_{19}$	11	11−14	[25]
$[12, 6, 7]_{19}$	7	7	[5]	$[32, 16, 12]_{19}$	12	14−16	[8]
$[16, 8, 8]_{19}$	8	8−9	[5]	$\mathbf{[36, 18, 14]_{19}}$	**14**	?−18	–
$[20, 10, 11]_{19}$	11	11	[5]	$\mathbf{[40, 20, 15]_{19}}$	**15**	? − 20	–

Bold values represent new parameters

– $[36, 18, 14]_{19}$ code with a generator matrix $(I_{18} \mid A_{19}^{36})$ where

$$A_{19}^{36} = \begin{pmatrix}
16 & 14 & 4 & 15 & 10 & 15 & 17 & 7 & 4 & 16 & 16 & 14 & 3 & 7 & 5 & 2 & 5 & 12 \\
14 & 13 & 18 & 11 & 15 & 17 & 11 & 5 & 5 & 11 & 16 & 16 & 12 & 4 & 17 & 0 & 16 & 4 \\
4 & 18 & 18 & 12 & 18 & 12 & 2 & 6 & 12 & 18 & 14 & 1 & 10 & 16 & 10 & 6 & 13 & 6 \\
15 & 11 & 12 & 7 & 1 & 8 & 1 & 3 & 1 & 12 & 11 & 5 & 5 & 7 & 7 & 2 & 10 & 8 \\
10 & 15 & 18 & 1 & 7 & 9 & 14 & 14 & 7 & 12 & 13 & 16 & 16 & 2 & 16 & 9 & 16 & 4 \\
15 & 17 & 12 & 8 & 9 & 2 & 7 & 15 & 5 & 12 & 2 & 9 & 2 & 10 & 14 & 18 & 12 & 9 \\
17 & 11 & 2 & 1 & 14 & 7 & 11 & 13 & 16 & 1 & 16 & 17 & 4 & 11 & 4 & 11 & 9 & 18 \\
7 & 5 & 6 & 3 & 14 & 15 & 13 & 9 & 0 & 16 & 3 & 3 & 8 & 7 & 10 & 14 & 4 & 7 \\
4 & 5 & 12 & 1 & 7 & 5 & 16 & 0 & 12 & 17 & 1 & 7 & 4 & 0 & 9 & 0 & 17 & 18 \\
16 & 11 & 18 & 12 & 12 & 12 & 1 & 16 & 17 & 3 & 1 & 17 & 12 & 12 & 16 & 12 & 9 & 11 \\
16 & 16 & 14 & 11 & 13 & 2 & 16 & 3 & 1 & 1 & 15 & 17 & 4 & 12 & 10 & 0 & 7 & 4 \\
14 & 16 & 1 & 5 & 16 & 9 & 17 & 3 & 7 & 17 & 17 & 8 & 7 & 6 & 18 & 1 & 11 & 18 \\
3 & 12 & 10 & 5 & 16 & 2 & 4 & 8 & 4 & 12 & 4 & 7 & 14 & 0 & 9 & 9 & 6 & 15 \\
7 & 4 & 16 & 7 & 2 & 10 & 11 & 7 & 0 & 12 & 12 & 6 & 0 & 18 & 5 & 13 & 13 & 4 \\
5 & 17 & 10 & 7 & 16 & 14 & 4 & 10 & 9 & 16 & 10 & 18 & 9 & 5 & 13 & 7 & 0 & 7 \\
2 & 0 & 6 & 2 & 9 & 18 & 11 & 14 & 0 & 12 & 0 & 1 & 9 & 13 & 7 & 12 & 17 & 3 \\
5 & 16 & 13 & 10 & 16 & 12 & 9 & 4 & 17 & 9 & 7 & 11 & 6 & 13 & 0 & 17 & 2 & 17 \\
12 & 4 & 6 & 8 & 4 & 9 & 18 & 7 & 18 & 11 & 4 & 18 & 15 & 4 & 7 & 3 & 17 & 10
\end{pmatrix}$$

– $[40, 20, 15]_{19}$ code with a generator matrix $(I_{20} \mid A_{19}^{40})$ where

$$A_{19}^{40} = \begin{pmatrix}
8 & 7 & 12 & 5 & 0 & 13 & 15 & 11 & 16 & 6 & 17 & 14 & 6 & 6 & 6 & 4 & 18 & 14 & 13 & 14 \\
7 & 16 & 13 & 4 & 13 & 3 & 1 & 13 & 4 & 11 & 5 & 12 & 6 & 4 & 13 & 16 & 11 & 6 & 6 & 16 \\
12 & 13 & 5 & 6 & 13 & 11 & 12 & 12 & 16 & 9 & 3 & 0 & 16 & 17 & 2 & 8 & 6 & 14 & 6 & 9 \\
5 & 4 & 6 & 1 & 7 & 15 & 0 & 4 & 16 & 14 & 1 & 8 & 0 & 9 & 12 & 9 & 10 & 5 & 16 & 2 \\
0 & 13 & 13 & 7 & 17 & 17 & 18 & 17 & 16 & 16 & 8 & 0 & 1 & 13 & 14 & 3 & 11 & 6 & 9 & 14 \\
13 & 3 & 11 & 15 & 17 & 9 & 0 & 0 & 11 & 2 & 11 & 1 & 11 & 13 & 15 & 16 & 16 & 15 & 0 & 0 \\
15 & 1 & 12 & 0 & 18 & 0 & 0 & 14 & 4 & 15 & 13 & 8 & 14 & 17 & 17 & 9 & 0 & 5 & 15 & 0 \\
11 & 13 & 12 & 4 & 17 & 0 & 14 & 6 & 12 & 5 & 18 & 18 & 12 & 8 & 3 & 13 & 15 & 10 & 11 & 18 \\
16 & 4 & 16 & 16 & 16 & 11 & 4 & 12 & 7 & 2 & 10 & 3 & 4 & 16 & 1 & 13 & 16 & 8 & 12 & 17 \\
6 & 11 & 9 & 14 & 16 & 2 & 15 & 5 & 2 & 12 & 12 & 12 & 8 & 5 & 14 & 3 & 5 & 1 & 17 & 9 \\
17 & 5 & 3 & 1 & 8 & 11 & 13 & 18 & 10 & 12 & 18 & 0 & 16 & 8 & 11 & 18 & 5 & 17 & 10 & 10 \\
14 & 12 & 0 & 8 & 0 & 1 & 8 & 18 & 3 & 12 & 0 & 16 & 1 & 11 & 14 & 10 & 14 & 7 & 7 & 17 \\
6 & 6 & 16 & 0 & 1 & 11 & 14 & 12 & 4 & 8 & 16 & 1 & 6 & 10 & 7 & 13 & 9 & 6 & 4 & 0 \\
6 & 4 & 17 & 9 & 13 & 13 & 17 & 8 & 16 & 5 & 8 & 11 & 10 & 5 & 5 & 9 & 11 & 7 & 13 & 4 \\
6 & 13 & 2 & 12 & 14 & 15 & 17 & 3 & 1 & 14 & 11 & 14 & 7 & 5 & 6 & 13 & 10 & 15 & 14 & 8 \\
4 & 16 & 8 & 9 & 3 & 16 & 9 & 13 & 13 & 3 & 18 & 10 & 13 & 9 & 13 & 13 & 15 & 17 & 0 & 17 \\
18 & 11 & 6 & 10 & 11 & 16 & 0 & 15 & 16 & 5 & 5 & 14 & 9 & 11 & 10 & 15 & 8 & 6 & 18 & 17 \\
14 & 6 & 14 & 5 & 6 & 15 & 5 & 10 & 8 & 1 & 17 & 7 & 6 & 7 & 15 & 17 & 6 & 7 & 11 & 17 \\
13 & 6 & 6 & 16 & 9 & 0 & 15 & 11 & 12 & 17 & 10 & 7 & 4 & 13 & 14 & 0 & 18 & 11 & 13 & 5 \\
14 & 16 & 9 & 2 & 14 & 0 & 0 & 18 & 17 & 9 & 10 & 17 & 0 & 4 & 8 & 17 & 17 & 17 & 5 & 17
\end{pmatrix}$$

4.3 Symmetric self-dual codes over *GF*(23)

Proposition 5 *There exist the best symmetric self-dual codes over* $GF(23)$ *of length* $n = 4, 8, 12, 28, 32, 36, 40$. *Among them,* $[4, 2, 3]_{23}$, $[8, 4, 5]_{23}$ *and* $[12, 6, 7]_{23}$ *codes are MDS. Moreover,* $[32, 16, 12]_{23}$, $[36, 18, 14]_{23}$ *and* $[40, 20, 15]_{23}$ *codes are new.*

We give the highest minimum distance d_{sym} of symmetric self-dual codes and the previously best known minimum distance d_{sd} of self-dual codes in Table 6. In this table, new parameters are written in bold. We present three symmetric self-dual codes having new parameters:

Table 6 Tne best known minimum distances of symmetric self-dual codes over $GF(23)$

$[n, k, d]_p$	$d_{sym.}$	$d_{sd.}$	Refs.	$[n, k, d]_p$	$d_{sym.}$	$d_{sd.}$	Refs.
$[4, 2, 3]_{23}$	3	3	[5]	$[24, 12, 10]_{23}$	10	13	[26]
$[8, 4, 5]_{23}$	5	5	[5]	$[28, 14, 11]_{23}$	11	11−14	[25]
$[12, 6, 7]_{23}$	7	7	[5]	$\mathbf{[32, 16, 12]_{23}}$	**12**	?−16	–
$[16, 8, 8]_{23}$	8	9	[5]	$\mathbf{[36, 18, 14]_{23}}$	**14**	13−18	Table 3
$[20, 10, 9]_{23}$	9	10−11	[8]	$\mathbf{[40, 20, 15]_{23}}$	**15**	14−20	Table 3

Bold values represent new parameters

– $[32, 16, 12]_{23}$ code with a generator matrix $(I_{16} \mid A_{23}^{32})$ where

$$A_{23}^{32} = \begin{pmatrix}
20 & 4 & 11 & 18 & 21 & 7 & 19 & 7 & 15 & 6 & 18 & 18 & 2 & 10 & 5 & 12 \\
4 & 1 & 19 & 12 & 11 & 19 & 20 & 8 & 10 & 3 & 11 & 0 & 3 & 6 & 18 & 18 \\
11 & 19 & 12 & 20 & 9 & 2 & 0 & 22 & 21 & 21 & 9 & 6 & 21 & 16 & 13 & 9 \\
18 & 12 & 20 & 2 & 13 & 7 & 4 & 7 & 22 & 18 & 5 & 15 & 0 & 5 & 11 & 20 \\
21 & 11 & 9 & 13 & 9 & 20 & 8 & 19 & 11 & 12 & 11 & 21 & 19 & 14 & 19 & 20 \\
7 & 19 & 2 & 7 & 20 & 3 & 12 & 19 & 5 & 2 & 22 & 1 & 21 & 21 & 22 & 13 \\
19 & 20 & 0 & 4 & 8 & 12 & 12 & 4 & 19 & 7 & 17 & 11 & 8 & 4 & 1 & 0 \\
7 & 8 & 22 & 7 & 19 & 19 & 4 & 1 & 0 & 0 & 16 & 16 & 8 & 15 & 9 & 3 \\
15 & 10 & 21 & 22 & 11 & 5 & 19 & 0 & 22 & 1 & 2 & 12 & 13 & 12 & 10 & 5 \\
6 & 3 & 21 & 18 & 12 & 2 & 7 & 0 & 1 & 14 & 5 & 5 & 22 & 18 & 11 & 1 \\
18 & 11 & 9 & 5 & 11 & 22 & 17 & 16 & 2 & 5 & 10 & 20 & 18 & 12 & 6 & 18 \\
18 & 0 & 6 & 15 & 21 & 1 & 11 & 16 & 12 & 5 & 20 & 13 & 16 & 17 & 5 & 22 \\
2 & 3 & 21 & 0 & 19 & 21 & 8 & 8 & 13 & 22 & 18 & 16 & 3 & 5 & 7 & 6 \\
10 & 6 & 16 & 5 & 14 & 21 & 4 & 15 & 12 & 18 & 12 & 17 & 5 & 7 & 18 & 2 \\
5 & 18 & 13 & 11 & 19 & 22 & 1 & 9 & 10 & 11 & 6 & 5 & 7 & 18 & 3 & 0 \\
12 & 18 & 9 & 20 & 20 & 13 & 0 & 3 & 5 & 1 & 18 & 22 & 6 & 2 & 0 & 6
\end{pmatrix}$$

– $[36, 18, 14]_{23}$ code with a generator matrix $(I_{18} \mid A_{23}^{36})$ where

$$A_{23}^{36} = \begin{pmatrix}
14 & 8 & 18 & 22 & 3 & 17 & 6 & 3 & 2 & 7 & 14 & 2 & 22 & 12 & 6 & 8 & 12 & 19 \\
8 & 18 & 5 & 14 & 21 & 10 & 12 & 16 & 15 & 0 & 18 & 16 & 0 & 20 & 3 & 1 & 2 & 6 \\
18 & 5 & 3 & 13 & 8 & 0 & 20 & 1 & 13 & 12 & 22 & 19 & 14 & 9 & 14 & 15 & 22 & 18 \\
22 & 14 & 13 & 9 & 7 & 1 & 1 & 17 & 10 & 9 & 22 & 14 & 1 & 11 & 11 & 15 & 19 & 12 \\
3 & 21 & 8 & 7 & 20 & 9 & 0 & 2 & 10 & 19 & 7 & 5 & 16 & 0 & 16 & 3 & 15 & 19 \\
17 & 10 & 0 & 1 & 9 & 22 & 1 & 13 & 4 & 13 & 5 & 10 & 14 & 0 & 14 & 17 & 2 & 8 \\
6 & 12 & 20 & 1 & 0 & 1 & 3 & 13 & 20 & 13 & 1 & 19 & 2 & 6 & 12 & 12 & 2 & 0 \\
3 & 16 & 1 & 17 & 2 & 13 & 13 & 21 & 13 & 16 & 17 & 4 & 6 & 6 & 5 & 12 & 9 & 1 \\
2 & 15 & 13 & 10 & 10 & 4 & 20 & 13 & 22 & 2 & 6 & 5 & 14 & 14 & 13 & 16 & 13 & 8 \\
7 & 0 & 12 & 9 & 19 & 13 & 13 & 16 & 2 & 17 & 9 & 21 & 17 & 4 & 2 & 7 & 20 & 7 \\
14 & 18 & 22 & 22 & 7 & 5 & 1 & 17 & 6 & 9 & 20 & 15 & 4 & 22 & 13 & 0 & 17 & 14 \\
2 & 16 & 19 & 14 & 5 & 10 & 19 & 4 & 5 & 21 & 15 & 13 & 2 & 15 & 20 & 20 & 3 & 18 \\
22 & 0 & 14 & 1 & 16 & 14 & 2 & 6 & 14 & 17 & 4 & 2 & 0 & 2 & 9 & 0 & 11 & 1 \\
12 & 20 & 9 & 11 & 0 & 0 & 6 & 6 & 14 & 4 & 22 & 15 & 2 & 1 & 7 & 7 & 5 & 15 \\
6 & 3 & 14 & 11 & 16 & 14 & 12 & 5 & 13 & 2 & 13 & 20 & 9 & 7 & 13 & 1 & 9 & 20 \\
8 & 1 & 15 & 15 & 3 & 17 & 12 & 12 & 16 & 7 & 0 & 20 & 0 & 7 & 1 & 1 & 4 & 9 \\
12 & 2 & 22 & 19 & 15 & 2 & 2 & 9 & 13 & 20 & 17 & 3 & 11 & 5 & 9 & 4 & 18 & 15 \\
19 & 6 & 18 & 12 & 19 & 8 & 0 & 1 & 8 & 7 & 14 & 18 & 1 & 15 & 20 & 9 & 15 & 15
\end{pmatrix}$$

– $[40, 20, 15]_{23}$ code with a generator matrix $(I_{20} \mid A_{23}^{40})$ where

$$A_{23}^{40} = \begin{pmatrix}
3 & 3 & 17 & 18 & 20 & 7 & 20 & 7 & 8 & 12 & 14 & 0 & 8 & 22 & 18 & 0 & 0 & 8 & 9 & 19 \\
3 & 8 & 11 & 22 & 1 & 4 & 11 & 4 & 4 & 9 & 8 & 20 & 7 & 21 & 19 & 16 & 13 & 9 & 22 & 10 \\
17 & 11 & 8 & 10 & 0 & 11 & 3 & 6 & 20 & 11 & 3 & 20 & 15 & 1 & 14 & 4 & 11 & 8 & 19 & 6 \\
18 & 22 & 10 & 1 & 0 & 6 & 14 & 2 & 1 & 15 & 22 & 19 & 11 & 1 & 2 & 3 & 5 & 12 & 12 & 16 \\
20 & 1 & 0 & 0 & 12 & 5 & 0 & 15 & 0 & 5 & 20 & 1 & 13 & 16 & 21 & 14 & 8 & 21 & 10 & 3 \\
7 & 4 & 11 & 6 & 5 & 15 & 2 & 7 & 9 & 0 & 22 & 15 & 1 & 16 & 22 & 2 & 8 & 13 & 16 & 7 \\
20 & 11 & 3 & 14 & 0 & 2 & 17 & 4 & 17 & 6 & 0 & 6 & 14 & 5 & 19 & 8 & 11 & 11 & 17 & 5 \\
7 & 4 & 6 & 2 & 15 & 7 & 4 & 5 & 9 & 19 & 16 & 19 & 7 & 12 & 12 & 14 & 11 & 15 & 22 & 3 \\
8 & 4 & 20 & 1 & 0 & 9 & 17 & 9 & 12 & 10 & 13 & 18 & 5 & 6 & 19 & 10 & 21 & 5 & 5 & 10 \\
12 & 9 & 11 & 15 & 5 & 0 & 6 & 19 & 10 & 5 & 2 & 16 & 14 & 13 & 5 & 6 & 5 & 9 & 20 & 14 \\
14 & 8 & 3 & 22 & 20 & 22 & 0 & 16 & 13 & 2 & 0 & 14 & 10 & 9 & 10 & 19 & 7 & 12 & 7 & 21 \\
0 & 20 & 20 & 19 & 1 & 15 & 6 & 19 & 18 & 16 & 14 & 13 & 18 & 4 & 9 & 10 & 4 & 11 & 2 & 9 \\
8 & 7 & 15 & 11 & 13 & 1 & 14 & 7 & 5 & 14 & 10 & 18 & 15 & 19 & 6 & 20 & 20 & 12 & 15 & 22 \\
22 & 21 & 1 & 1 & 16 & 16 & 5 & 12 & 6 & 13 & 9 & 4 & 19 & 9 & 16 & 6 & 17 & 20 & 8 & 12 \\
18 & 19 & 14 & 2 & 21 & 22 & 19 & 12 & 19 & 5 & 10 & 9 & 6 & 16 & 17 & 14 & 13 & 15 & 3 & 13 \\
0 & 16 & 4 & 3 & 14 & 2 & 8 & 14 & 10 & 6 & 19 & 10 & 20 & 6 & 14 & 15 & 4 & 1 & 9 & 12 \\
0 & 13 & 11 & 5 & 8 & 8 & 11 & 11 & 21 & 5 & 7 & 4 & 20 & 17 & 13 & 4 & 12 & 22 & 18 & 19 \\
8 & 9 & 8 & 12 & 21 & 13 & 11 & 15 & 5 & 9 & 12 & 11 & 12 & 20 & 15 & 1 & 22 & 18 & 14 & 8 \\
9 & 22 & 19 & 12 & 10 & 16 & 17 & 22 & 5 & 20 & 7 & 2 & 15 & 8 & 3 & 9 & 18 & 14 & 20 & 5 \\
19 & 10 & 6 & 16 & 3 & 7 & 5 & 3 & 10 & 14 & 21 & 9 & 22 & 12 & 13 & 12 & 19 & 8 & 5 & 2
\end{pmatrix}$$

Table 7 Bounds on the highest minimum distances of self-dual codes over $GF(p)$ for primes $5 \leq p \leq 23$ up to lengths 40

$n\backslash q$	5	7	11	13	17	19	23
2	2^*	–	–	2^*	2^*	–	–
4	2^o	3^*	3^*	3^*	3^*	3^*	3^*
6	4^*	–	–	4^*	4^*	–	–
8	4^o	5^*	5^*	5^*	5^*	5^*	5^*
10	4^o	–	–	6^*	6^*	–	–
12	6^o	6^o	7^*	6^o	7^*	7^*	7^*
14	6^o	–	–	8^*	7–8	–	–
16	7^o	7^o	8^o	8^o	8–9	8–9	9^*
18	7^o	–	–	8–9	10^*	–	–
20	8^o	9^o	10^o	10^o	10^o	11^*	10–11
22	8^o	–	–	10–11	10–11	–	–
24	9–10	9–11	9–12	10–12	10–12	10–12	13^*
26	9–10	–	–	10–13	10–13	–	–
28	10–11	11–13	10–14	11–14	11–14	11–14	11–14
30	10–12	–	–	11–15	12–15	–	–
32	11–13	13–14	**12–16**	12–16	12–16	14–16	**12–16**
34	11–14	–	–	12–17	13–17	–	–
36	12–15	13–16	**13–18**	13–18	13–18	**14–18**	**14–18**
38	12–16	–	–	13–19	14–19	–	–
40	13–17	14–18	**14–20**	14–20	14–20	**15–20**	**15–20**

Bold values represent new parameters In this table, ^{o} denotes optimal code and * denotes MDS code. [5,8,11–13,15,25,26]

5 Conclusions

In this article, we introduced new construction methods of symmetric self-dual codes over finite fields. Then we have constructed many new symmetric self-dual codes, including 153 self-dual codes with new parameters, up to equivalence. This paper contributes in two ways. One is to provide new construction methods of symmetric self-dual codes over $GF(q)$ for the challenging case of $q \equiv 3 \pmod 4$. The other is to improve bounds on the highest minimum distance of self-dual codes, which have not been significantly updated for almost two decades because of computational complexity. We believe that our methods can produce more results for self-dual codes over larger finite fields and/or of longer lengths.

Acknowledgements The authors sincerely thank Dr. Markus Grassl for his helpful comments which was crucial for the implementation.

References

1. Ball S.: On sets of vectors of a finite vector space in which every subset of basis size is a basis. J. Eur. Math. Soc. **14**(3), 733–748 (2012).
2. Bannai E., Dougherty S.T., Harada M., Oura M.: Type II codes, even unimodular lattices, and invariant rings. IEEE Trans. Inform. Theory **45**(4), 1194–1205 (1999).

3. Be'Ery I., Raviv N., Raviv T., Be'Ery Y.: Active deep decoding of linear codes. IEEE Trans. Commun. **68**(2), 728–736 (2019).
4. Bernhard R.: Codes and Siegel modular forms. Discret. Math. **148**(1–3), 175–204 (1996).
5. Betsumiya K., Georgiou S., Gulliver T.A., Harada M.: On self-dual codes over some prime fields. Discret. Math. **262**(1–3), 37–58 (2003).
6. Cannon J.: Playoust: An Introduction to Magma. University of Sydney, Sydney (1994).
7. Çalkavur S., Solé P.: Secret sharing, zero sum sets, and Hamming codes. Mathematics **8**(10), 1644 (2020).
8. Choi W.-H., Kim J.-L.: Self-dual codes, symmetric matrices, and eigenvectors. IEEE Access **9**, 104294–104303 (2021). https://doi.org/10.1109/ACCESS.2021.3099434.
9. Conway J.H., Sloane N.J.A.: Sphere Packings, Lattices and Groups, 3rd edn Springer, New York (1999).
10. Dougherty S.T., Gildea J., Kaya A.: 2^n Bordered constructions of self-dual codes from group rings. Finite Fields Appl. **67**, 101692 (2020).
11. De Boer M.A.: Almost MDS codes. Des. Codes Cryptogr. **9**(2), 143–155 (1996).
12. Gaborit P.: Quadratic double circulant codes over fields. J. Comb. Theory Ser. A **97**(1), 85–107 (2002).
13. Grassl M.D.: On self-dual MDS codes. In: ISIT 2008, Toronto, Canada, July 6–11, pp. 1954–1957 (2008).
14. Grassl M., Gulliver T.A.: On circulant self-dual codes over small fields. Des. Codes Cryptogr. **52**(1), 57 (2009). https://doi.org/10.1007/s10623-009-9267-1.
15. Gulliver T.A., Kim J.-L., Lee Y.: New MDS or near-MDS self-dual codes. IEEE Trans. Inform. Theory **54**(9), 4354–4360 (2008).
16. Harada M., Munemasa A., Tonchev V.D.: Self-dual codes and the nonexistence of a quasi-symmetric 2-(37, 9, 8) design with intersection numbers 1 and 3. J. Comb. Des. **25**(10), 469–476 (2017).
17. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2010).
18. Huang L., Zhang H., Li R., Ge Y., Wang J.: AI coding: learning to construct error correction codes. IEEE Trans. Commun. **68**(1), 26–39 (2019).
19. Kim H.J., Lee Y.: Extremal quasi-cyclic self-dual codes over finite fields. Finite Fields Appl. **52**, 301–318 (2018).
20. Kim J.-L.: Generator matrices for this paper. https://cicagolab.sogang.ac.kr/cicagolab/2657.html.
21. Park Y.H.: The classification of self-dual modular codes. Finite Fields Appl. **17**(5), 442–460 (2011).
22. Pless V.: Symmetry codes and their invariant subcodes. J. Comb. Theory Ser. A **18**(1), 116–125 (1975).
23. Pless V.: Symmetry codes over GF (3) and new five-designs. J. Comb. Theory Ser. A **12**(1), 119–142 (1972).
24. Sendrier N.: Code-based cryptography: state of the art and perspectives. IEEE Secur. Privacy **15**(4), 44–50 (2017).
25. Shi M., Sok L., Solé P., Çalkavur S.: Self-dual codes and orthogonal matrices over large finite fields. Finite Fields Appl. **54**, 297–314 (2018).
26. Sok L.: Explicit constructions of MDS self-dual codes. IEEE Trans. Inform. Theory **66**(6), 2954877 (2020). https://doi.org/10.1109/TIT.2019.2954877.
27. Sok L.: New families of self-dual codes. Des. Codes Cryptogr. **89**, 823–841 (2021). https://doi.org/10.1007/s10623-021-00847-x.