IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 1, 2021, accepted July 17, 2021, date of publication July 26, 2021, date of current version July 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3099434

Self-Dual Codes, Symmetric Matrices, and Eigenvectors

JON-LARK KIM[1], (Member, IEEE), AND WHAN-HYUK CHOI[2]
[1]Department of Mathematics, Sogang University, Seoul 04107, Republic of Korea
[2]Department of Biomedical Engineering, UNIST, Ulsan 44919, Republic of Korea

Corresponding author: Whan-Hyuk Choi (choiwh@unist.ac.kr)

The work of Jon-Lark Kim was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government under Grant NRF-2019R1A2C1088676. The work of Whan-Hyuk Choi was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government under Grant NRF-2019R1I1A1A01057755.

ABSTRACT We introduce a consistent and efficient method to construct self-dual codes over $GF(q)$ using symmetric matrices and eigenvectors from a self-dual code over $GF(q)$ of smaller length where $q \equiv 1 \pmod 4$. Using this method, which is called a 'symmetric building-up' construction, we improve the bounds of the best-known minimum weights of self-dual codes with lengths up to 40, which have not significantly improved for almost two decades. We focus on a class of self-dual codes, which includes double circulant codes. We obtain 2967 new self-dual codes over $GF(13)$ and $GF(17)$ up to equivalence. We also compute the minimum weights of quadratic residue(QR) codes that were previously unknown. These are a [20,10,10] QR self-dual code over $GF(23)$, [24,12,12] QR self-dual codes over $GF(29)$ and $GF(41)$, and a [32,16,14] QR self-dual code over $GF(19)$. They have the highest minimum weights so far.

INDEX TERMS Eigenvectors, optimal codes, quadratic residue codes, self-dual codes, symmetric matrix, symmetric self-dual codes.

I. INTRODUCTION

The theory of error-correcting codes, which was born with the invention of computers, has been an interesting topic in mathematics as well as in industry, such as satellites, CD players, and cellular phones. Recently, with the advent of machine learning and artificial intelligence, there have been some studies on the relationship between error-correcting codes and these areas [2], [22], [30], [31]. Especially, self-dual codes have been an important class of linear codes for both practical and theoretical reasons and have received an enormous research effort since the beginning of coding theory.

Due to their algebraic or combinatorial structures, self-dual codes have been studied by coding or cryptography researchers. For example, self-dual codes have been useful in secret-sharing schemes [9]. Moreover, many of the best-known codes are actually self-dual codes. It is well-known that self-dual codes are asymptotically good [28]. Self-dual codes also have close connections to other mathematical structures such as designs, lattices, graph theory, and modular forms [1], [4], [5]. It is also reported that self-dual codes have applications in quantum information theory [32, Chap. 13]. Recently, self-duality for some classes of quasi-cyclic codes has been studied in [10].

On the other hand, coding theorists are interested in finding an *optimal* code, which has the best capability to correct as many errors as possible with a given length. The *minimum distance* of code is the parameter determining the error-correction capability of a code. In particular, *extremal* self-dual codes and *maximal distance separable (MDS)* self-dual codes are optimal codes that meet some upper bounds on the minimum distances. There is a close relationship between optimal codes and self-dual or self-orthogonal codes [26]. The effort to find optimal codes has lasted for decades, and is still ongoing. To see the whole history, we refer to [3], [11]–[14], [37], [39].

As a summary, we present all of the up-to-date results concerning minimum weight bounds and the existence of optimal self-dual codes in Tables 1, 2, and 3. In the tables, the best-known minimum weights are listed. The superscript 'e' indicates the minimum distance of an extremal code when $q = 2, 3, 4$, and '$*$' indicates the minimum distance of an MDS code. The superscript 'o' indicates the minimum

The associate editor coordinating the review of this manuscript and approving it for publication was Zilong Liu.

TABLE 1. **The best-known minimum weights of self-dual codes of length *n* over *GF*(*q*) where $n \le 40$ and $2 \le q \le 4$ [12], [15], [19], [23].**

n	2		3	4^{eucl}		4^{herm}
	type I	type II		d_L	d_H	
2	2^*	-	-	2	2^*	2
4	2^o	-	3^*	2	3^*	2
6	2^o	-	-	4	3^o	4
8	2^o	4^e	3^e	4	4^e	4
10	2^o	-	-	4	4^e	4
12	4^e	-	6^e	6	6^o	4
14	4^e	-	-	6	6^o	6
16	4^e	4^e	6^e	6	6^o	6
18	4^e	-	-	8	$6-7$	8
20	4^e	-	6^e	8	8^e	8
22	6^e	-	-	8	8^e	8
24	6^e	8^e	9^e	?	$8-10$	8
26	6^o	-	-	?	$8-10$	8,10
28	6^o	-	9^e	?	$9-11$	10
30	6^o	-	-	?	$10-12$	12
32	8^e	8^e	9^e	?	$11-12$	10,12
34	6^o	-	-	12	$10-12$	10,12
36	8^e	-	12^e	?	$11-14$	12,14
38	8^e	-	-	?	$11-15$	12,14
40	8^e	8^e	12^e	?	$12-16$	12,14

TABLE 2. **The best-known minimum weights of self-dual codes of length *n* over *GF*(*q*) where $n \le 40$ and $5 \le q \le 19$ [3], [7], [12], [14], [15], [18], [20], [27], [36]. New results from this article are written in bold.**

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

distance of an optimal code with given parameters. If the bound is not determined yet, we put '?' and if there does not exist a self-dual code with a given length, we put '−'. If the bound of the best minimum weight is reported, we indicate the lower and upper bound together.

In Table 1, we list the best-known Lee distances(d_L) and Hamming distances(d_H) of Euclidean self-dual codes over $GF(4)$(denoted by 4^{eucl}) and best-known Hamming distances of Hermitian self-dual codes over $GF(4)$(denoted by 4^{herm}).

Gleason-Pierce-Ward theorem states that self-dual codes over $GF(q)$ have weights divisible by $\delta > 1$ only if $q = 2, 3, 4$. This motivates many researchers to study self-dual codes over small fields. Table 1 gives an updated status of the highest minimum weights of such self-dual codes.

However, these tables also tell that there remain many unknown bounds. Most cases of length ≤ 24 are completely known. However, when $5 \le q \le 20$, most highest minimum weights of self-dual codes over $GF(q)$ are not known if length ≥ 24, as we can see in Tables 2 and 3. However, in general,

TABLE 3. **The best-known minimum weights of self-dual codes of length *n* over *GF*(*q*) where $n \le 40$ and $23 \le q \le 41$ [3], [7], [13], [14], [16], [17], [25], [36], [37], [38]. New results from this article are written in bold.**

n	23	25	27	29	31	37	41
2	-	2^*	-	2^*	-	2^*	2^*
4	3^*	3^*	3^*	3^*	3^*	3^*	3^*
6	-	3^*	-	4^*	-	4^*	4^*
8	5^*	5^*	5^*	5^*	5^*	5^*	5^*
10	-	6^*	-	6^*	-	6^*	6^*
12	7^*	7^*	7^*	7^*	7^*	7^*	7^*
14	-	8^*	-	8^*	-	8^*	8^*
16	9^*	9^*	9^*	9^*	9^*	9^*	9^*
18	-	10^*	-	10^*	-	10^*	10^*
20	**10 − 11**	11^*	?	$10-11$	11^*	?	11^*
22	-	?	-	?	-	?	12^*
24	13^*	$12-13$	?	**12 − 13**	13^*	?	**12 − 13**
26	-	14^*	-	?	-	14^*	?
28	$11-14$	?	15^*	$14-15$	?	?	?
30	-	?	-	16^*	-	?	?
32	?	?	?	?	17^*	?	17^*
34	-	?	-	?	-	?	?
36	?	?	?	?	?	$18-19$	?
38	-	?	-	?	-	20^*	?
40	?	?	?	?	?	?	$20-21$

many self-dual codes over larger finite fields have better minimum weights than those of self-dual codes over smaller fields. This is the main motivation of this paper.

We try to improve the bounds on minimum weights by constructing self-dual codes of longer lengths as many as possible. To this end, we investigate the consistent and efficient method to construct self-dual codes. Consequently, we find a construction method of self-dual codes over $GF(q)$ having a symmetric generator matrix where $q \equiv 1 \pmod 4$. This method can be regarded as a special case of the well-known 'building-up' construction method [25]. However, the method in this paper has significant differences: we improve the efficiency to find the best self-dual code from a self-dual code of a given length and we also focus our concern on one subclass of self-dual codes which have a certain automorphism in their automorphism group. Using this construction method, we obtain 2967 new self-dual codes over $GF(13)$ and $GF(17)$ and improve the lower bounds of best self-dual codes of length up to 40 (Table 4 and 5). We also want to point out that our new construction method includes well-known pure double circulant and bordered double circulant construction; for example, optimal and MDS self-dual codes obtained in [3] and [16] can be obtained equivalently by using our method.

In addition, we construct four new self-dual codes from quadratic residue codes which improve the unknown bound: a [20,10,10] code over $GF(23)$, [24,12,12] codes over $GF(29)$ and $GF(41)$, and a [32,16,14] code over $GF(19)$. We also point out that the $[18, 9, 9]$ quadratic residue code over $GF(13)$, which has been reported previously as an optimal self-dual code [3], is *not* actually a self-dual code. However, since we obtain [18,9,8] self-dual codes over $GF(13)$, the bound of the highest minimum distance of self-dual code over $GF(13)$ of length 18 is turned to 8-9. Our new results are written in bold in Tables 2, 3 and 4. In particular, the highest minimum distances of our results in Table 4 are all of the self-dual codes having symmetric generator matrices. The number of inequivalent codes we obtain is given in Table 5.

TABLE 4. Highest minimum weights of self-dual codes constructed by Theorem 8 vs. previously known highest minimum weights. New results are written in bold.

n	Over $GF(13)$		Over $GF(17)$	
	Our results	Prev. best	Our results	Prev. best
2	2	2	2	2
4	3	3	3	3
6	4	4	4	4
8	5	5	5	5
10	6	6	6	6
12	6	6	7	7
14	8	8	7	7
16	8	8	8	8
18	8	9?	10	10
20	10	10	9	10
22	10	10	10	10
24	10	10	10	10
26	**10**	-	**10**	-
28	**11**	10	**11**	10
30	**11**	-	**12**	-
32	**12**	-	**12**	-
34	**12**	-	**12**	-
36	**13**	-	**13**	-
38	**13**	-	**14**	-
40	**14**	-	**14**	-

TABLE 5. Number of inequivalent self-dual codes newly obtained by using Theorem 8.

n	Over $GF(13)$		Over $GF(17)$	
	min. wt.	# of codes	min. wt.	# of codes
26	10	≥ 1098	10	≥ 352
28	11	≥ 1	11	≥ 106
30	11	≥ 380	12	≥ 2
32	12	≥ 164	12	≥ 2
34	12	≥ 710	12	≥ 2
36	13	≥ 7	13	≥ 64
38	13	≥ 66	14	≥ 2
40	14	≥ 4	14	≥ 7

The paper is organized as follows. Section 2 gives preliminaries and background for self-dual codes over $GF(q)$. In Section 3, we present a construction method of *symmetric self-dual codes* over $GF(q)$ where $q \equiv 1 \pmod 4$. We show that every symmetric self-dual code of length $2n+2$ is constructed from a symmetric self-dual code of length $2n$ by using this construction method. In Section 4, we present the computational results of the best codes obtained by using our method. All computations in this paper were done with the computer algebra system Magma [6].

II. PRELIMINARIES

Let n be a positive integer and q be a power of a prime. A *linear code* $\mathcal{C}$ of length n and dimension k over a finite field $GF(q)$ 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 $\mathcal{C}$. For vectors $\mathbf{x} = (x_i)$ and $\mathbf{y} = (y_i)$, we define the inner product $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i y_i$. The *dual code* $\mathcal{C}^{\perp}$ is defined by

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

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 it is 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 $\mathcal{C}$. If a linear code $\mathcal{C}$ over $GF(q)$ of length n and dimension k has the minimum weight d, we denote $\mathcal{C}$ an $[n, k, d]_q$ code.

The error-capability of a code is determined by the minimum distance, thus the minimum distance is the most important parameter of a code. For a linear code, its minimum distance equals the minimum weight of all the non-zero codewords. It is well-known [21, Chapter 2.4.] that a linear code of length n and dimension k satisfies 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. A self-dual code of length $2n$ over a field is MDS if the minimum weight equals $n+1$.

Let S_n be a 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 of all *γ-monomial transformations of length n*, $\mathcal{M}^n$ 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 only consider γ-monomial transformation in this paper since γ-monomial transformation does preserve the self-duality(see [21, Theorem 1.7.6]). Let $\mathcal{C}\tau = \{\mathbf{c}\tau \mid \mathbf{c} \in \mathcal{C}\}$ for an element τ in $\mathcal{M}^{2n}$ and a code $\mathcal{C}$ of length $2n$. If there exists an element $\mu \in \mathcal{M}^{2n}$ such that $\mathcal{C}\mu = \mathcal{C}'$ for two distinct self-dual codes $\mathcal{C}$ and $\mathcal{C}'$, then $\mathcal{C}$ and $\mathcal{C}'$ are called *equivalent* and denoted by $\mathcal{C} \simeq \mathcal{C}'$. An *automorphism* of $\mathcal{C}$ is an element $\mu \in \mathcal{M}^{2n}$ satisfying $\mathcal{C}\mu = \mathcal{C}$. The set of all automorphisms of $\mathcal{C}$ forms the *automorphism group* Aut($\mathcal{C}$) as a subgroup of $\mathcal{M}^{2n}$.

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

$$(I_n \; A) \,, \qquad (1)$$

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

Proposition 1: Let $\mathcal{C}$ be a self-dual code of length $2n$ over $GF(q)$ with a standard generator matrix $G = (I_n \mid A)$. Then

$$A^T G = (A^T \mid -I_n)$$

is also a generator matrix of $\mathcal{C}$.

Proof: Since $\mathcal{C}$ is self-dual, $AA^T = -I$ and $A^{-1} = -A^T$. Thus A^T is non-singular. This implies that the rank of the rows of $A^T G$ is equal to the rank n of G. Therefore, by the definition of a linear code, the rows of the matrix $A^T G$ form another basis of the code $\mathcal{C}$. It is obvious that

$$A^T G = (A^T I_n \mid A^T A) = (A^T \mid -I_n).$$

□

Corollary 2: Let $G = (I_n \mid A)$ and $G' = (I_n \mid A^T)$ be generator matrices of self-dual codes $\mathcal{C}$ and $\mathcal{C}'$, respectively. Then $\mathcal{C}$ and $\mathcal{C}'$ are equivalent.

Proof: By Proposition 1, it is clear that G' is equal to $(A^T G)p_{\tau_1}\gamma_1$ for the permutation $\tau_1 = (1, n+1)(2, n+2)\cdots(n, 2n) \in S_{2n}$ and $\gamma_1 = diag(-\mathbf{1}_n, \mathbf{1}_n) \in \mathbb{D}^{2n}$ where $\mathbf{1}_n$ denotes all one-vector of length n. Hence, $\mathcal{C}$ and $\mathcal{C}'$ are equivalent. □

Proposition 3: Let $G = (I_n \mid A)$ and $G' = (I_n \mid B)$ be generator matrices of self-dual codes $\mathcal{C}$ and $\mathcal{C}'$, 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 $\mu = \left(\begin{array}{c|c} \mu_1^{-1} & O \\ \hline O & \mu_2 \end{array}\right) \in \mathcal{M}^{2n}$,

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

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

Definition 4: A square matrix A is called *symmetric* if $A^T = A$. If the matrix A in a standard generator matrix $G = (I_n \mid A)$ of a self-dual code $\mathcal{C}$ of length $2n$ over $GF(q)$ is symmetric, we call G *a symmetric generator matrix of* $\mathcal{C}$. If a self-dual code $\mathcal{C}$ has a symmetric generator matrix, we call $\mathcal{C}$ *a symmectric self-dual code*.

Definition 5: Let $\mathcal{C}_1, \mathcal{C}_2$ be self-dual codes of length $2l$ and $2m$ whose standard generator matrices are $(I_l \mid A_1)$ and $(I_m \mid A_2)$, respectively. *The direct sum* of two codes, $\mathcal{C}_1 \oplus \mathcal{C}_2$ is defined by the code having the generator matrix,

$$(I_l \mid A_1) \oplus (I_m \mid A_2) = \left(\begin{array}{c|c|c|c} I_l & O & A_1 & O \\ \hline O & I_m & O & A_2 \end{array}\right).$$

Corollary 6: Let I_n be the identity matrix of order n, A be an $n \times n$ circulant matrix, and 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 $\begin{pmatrix} & \alpha & \beta \cdots \beta \\ & \beta & \\ I_n & \vdots & A \\ & \beta & \end{pmatrix}$, *where α and β are elements in $GF(q)$, is equivalent to a code with symmetric generator matrix.*

Proof: It is clear that a column reversed matrix of a circulant matrix A is symmetric. Thus, the corollary follows directly from Proposition 3. □

We remark that many MDS and optimal self-dual codes are obtained by using the construction method of pure double circulant codes and bordered double circulant codes in [3], [16]. These codes are all equivalent to codes with symmetric generator matrices.

III. CONSTRUCTION OF SYMMETRIC SELF-DUAL CODES

In this section, we introduce a construction method for symmetric self-dual codes over $GF(q)$ where $q \equiv 1 \pmod 4$. We also show that any symmetric self-dual code of length $2n+2$ is obtained from a symmetric self-dual code of length $2n$ by using this method. Thus, this is a complete method to obtain all symmetric self-dual codes. Our construction requires a square root of -1 in $GF(q)$; it is well-known that the equation $x^2 = -1$ has roots in $GF(q)$ if and only if $q \equiv 1 \pmod 4$. Thus, from now on, we assume that q is a power of an odd prime such that $q \equiv 1 \pmod 4$. We note that all arguments in this section can be also applicable even if q is a power of 2. We omit the details.

Lemma 7: Let α be a root of -1 in $GF(q)$. If $\mathcal{C}$ is a self-dual code of length $2n$ over $GF(q)$ with symmetric generator matrix $G = (I_n \mid A)$, then A has an eigenvector $\mathbf{x}^T$ with eigenvalue α or $-\alpha$.

Proof: Since $\mathcal{C}$ is self-dual, $AA^T = -I$. With the assumption that A is symmetric, we have that $A^2 = -I$, and

$$(A - \alpha I)(A + \alpha I) = A^2 + I = -I + I = O.$$

This implies that any non-zero vector $\mathbf{x}^T$ generated by column vectors of $A + \alpha I$, is an eigenvector of A with eigenvalue α if $A \neq -\alpha I$. On the contrary, if $A = -\alpha I$, then it is obvious that any vector $\mathbf{x}^T$ in $GF(q)^n$ is an eigenvector of A with eigenvalue $-\alpha$. Thus, the result follows. □

Theorem 8: Let $(I_n \mid A)$ be generator matrix of a symmetric self-dual code of length $2n$ over $GF(q)$ for $q \equiv 1 \pmod 4$. Let α be a square root of -1.

Suppose that $\mathbf{x}^T$ is a non-zero (column) eigenvector of A corresponding eigenvalue α, where $\mathbf{x}\mathbf{x}^T + 1$ is a non-zero square in $GF(q)$. Take γ be an element of $GF(q)$ satisfying $\gamma^2 = -1 - \mathbf{x}\mathbf{x}^T$ and $\gamma \neq \alpha$. And let $\beta = (\gamma - \alpha)^{-1}$ and $E = \beta \mathbf{x}^T \mathbf{x}$. Then

$$G' = (I_{n+1} \mid A') = \left(\begin{array}{c|c|c|c} 1 & 0 & \gamma & \mathbf{x} \\ \hline 0^T & I_n & \mathbf{x}^T & A + E \end{array}\right)$$

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

On the other hand, suppose that $\mathbf{x}$ *is a zero vector, then*

$$G' = (1 \mid \alpha) \oplus (I_n \mid A) = \left(\begin{array}{c|c|c|c} 1 & 0 & \alpha & 0 \\ 0^T & I_n & 0^T & A \end{array}\right)$$

is a generator matrix of a symmetric self-dual code of length $2n+2$ with minimum weight two.

Proof: Since the row rank of G' is $n+1$, we have only to show that $A'(A')^T$ is equal to $-I_{n+1}$.

By the assumption, we have that $AA^T = -I_n$ and $A\mathbf{x}^T = \alpha \mathbf{x}^T$, thus $AE^T = A(\beta \mathbf{x}^T \mathbf{x}) = \beta(A\mathbf{x}^T)\mathbf{x} = \alpha\beta\mathbf{x}^T\mathbf{x}$ and $EA^T = (AE^T)^T = (\alpha\beta\mathbf{x}^T\mathbf{x})^T = \alpha\beta\mathbf{x}^T\mathbf{x}$. Note that if $q \equiv 1 \pmod 4$, then -1 is a square. Furthermore, since we have assumed that $\mathbf{x}\mathbf{x}^T + 1$ is a non-zero square in $GF(q)$, there always exists $\gamma \in GF(q)$ such that $\gamma^2 = -1 - \mathbf{x}\mathbf{x}^T$. Therefore,

$$\begin{aligned} A'(A')^T &= \left(\begin{array}{c|c} \gamma & \mathbf{x} \\ \hline \mathbf{x}^T & A+E \end{array}\right)\left(\begin{array}{c|c} \gamma & \mathbf{x} \\ \hline \mathbf{x}^T & A+E \end{array}\right)^T \\ &= \left(\begin{array}{c|c} -1 & \gamma\mathbf{x} + \alpha\mathbf{x} + \beta\mathbf{x}(\mathbf{x}^T\mathbf{x})^T \\ \hline \gamma\mathbf{x}^T + A\mathbf{x}^T + E\mathbf{x}^T & -I_n + \mathbf{x}^T\mathbf{x} + 2\alpha\beta\mathbf{x}^T\mathbf{x} + EE^T \end{array}\right). \end{aligned}$$

Since $\mathbf{x}\mathbf{x}^T = -\gamma^2 - 1$, we simplify the (1,2)-block matrix as

$$\begin{aligned}&\gamma\mathbf{x} + \alpha\mathbf{x} + \beta\mathbf{x}(\mathbf{x}^T\mathbf{x})^T \\ &= \gamma\mathbf{x} + \alpha\mathbf{x} + \beta(-\gamma^2 - 1)\mathbf{x} \\ &= (\gamma + \alpha - \beta(\gamma^2 + 1))\mathbf{x} \\ &= \beta(\beta^{-1}(\gamma + \alpha) - (\gamma^2 + 1)) \\ &= \beta((\gamma - \alpha)(\gamma + \alpha) - (\gamma^2 + 1)) \\ &= \beta((\gamma^2 + 1) - (\gamma^2 + 1)) \\ &= O_{1\times n}.\end{aligned}$$

The (2,1)-block matrix $\gamma\mathbf{x}^T + A\mathbf{x}^T + E\mathbf{x}^T = O_{n\times 1}$ since this is the transpose of the (1,2)-block matrix. Finally, it remains to show that the (2,2)-block matrix is equal to $-I_n$. Recall that $\alpha^2 = -1$ and $\beta = (\gamma - \alpha)^{-1}$. Thus,

$$\begin{aligned}&\mathbf{x}^T\mathbf{x} + 2\alpha\beta\mathbf{x}^T\mathbf{x} + EE^T \\ &= \mathbf{x}^T\mathbf{x} + 2\alpha\beta\mathbf{x}^T\mathbf{x} + \beta^2(\mathbf{x}^T\mathbf{x})(\mathbf{x}^T\mathbf{x})^T \\ &= \mathbf{x}^T\mathbf{x} + 2\alpha\beta\mathbf{x}^T\mathbf{x} + \beta^2\mathbf{x}^T(-\gamma^2 - 1)\mathbf{x} \\ &= (1 + 2\alpha\beta - \beta^2\gamma^2 - \beta^2)\mathbf{x}^T\mathbf{x} \\ &= \beta^2(\beta^{-2} + 2\alpha\beta^{-1} - \gamma^2 - 1)\mathbf{x}^T\mathbf{x} \\ &= \beta^2\{(\gamma - \alpha)^2 + 2\alpha(\gamma - \alpha) - \gamma^2 - 1)\}\mathbf{x}^T\mathbf{x} \\ &= \beta^2(\gamma^2 - 2\gamma\alpha - 1 + 2\gamma\alpha + 2 - \gamma^2 - 1)\mathbf{x}^T\mathbf{x} \\ &= O_{n\times n}\end{aligned}$$

and the (2,2)-block matrix is equal to $-I_n$. This completes the proof of the first part.

The 'on the other hand' part is trivial. □

By the construction method of Theorem 8 called the symmetric building-up construction, we obtain symmetric self-dual codes of length $2n + 2$ from a symmetric self-dual code of length $2n$. From now on, we discuss the converse of Theorem 8.

Lemma 9: Suppose that $\mathcal{C}$ is a symmetric self-dual code over $GF(q)$ with generator matrix in the form:

$$\left(\begin{array}{c|c|c|c} 1 & 0 & \gamma & \mathbf{x} \\ \hline 0^T & I_n & \mathbf{x}^T & A \end{array}\right),$$

where $\mathbf{x}$ is a non-zero vector. Let α be a square root of -1 over a finite field $GF(q)$ which is not equal to γ and let $\beta = (\gamma - \alpha)^{-1}$. Then $\mathbf{x}^T$ is an eigenvector of $A - \beta\mathbf{x}^T\mathbf{x}$ with eigenvalue α.

Proof: Since $\mathcal{C}$ is a symmetric self-dual code,

$$\left(\begin{array}{c|c} \gamma & \mathbf{x} \\ \hline \mathbf{x}^T & A \end{array}\right)\left(\begin{array}{c|c} \gamma & \mathbf{x} \\ \hline \mathbf{x}^T & A \end{array}\right)^T = -I_{n+1}.$$

Thus,

$$\begin{cases}\gamma^2 + \mathbf{x}\mathbf{x}^T = -1 \\ \gamma\mathbf{x} + \mathbf{x}A^T = 0 \\ \gamma\mathbf{x}^T + A\mathbf{x}^T = 0^T \\ \mathbf{x}^T\mathbf{x} + AA^T = -I_n.\end{cases} \tag{2}$$

By using these equalities, we show that

$$\begin{aligned}(A - \beta\mathbf{x}^T\mathbf{x})\mathbf{x}^T &= A\mathbf{x}^T - \beta\mathbf{x}^T(\mathbf{x}\mathbf{x}^T) \\ &= -\gamma\mathbf{x}^T - \beta\mathbf{x}^T(-1 - \gamma^2) \\ &= \beta(-\beta^{-1}\gamma + 1 + \gamma^2)\mathbf{x}^T \\ &= \beta(-(\gamma - \alpha)\gamma + 1 + \gamma^2)\mathbf{x}^T \\ &= \beta(\alpha\gamma + 1)\mathbf{x}^T \\ &= (\gamma - \alpha)^{-1}(\alpha\gamma - \alpha^2)\mathbf{x}^T \\ &= \alpha\mathbf{x}^T.\end{aligned}$$

Thus the result follows. □

Theorem 10: Any symmetric self-dual code $\mathcal{C}$ of length $2n + 2$ over $GF(q)$ for a prime $q = 4k + 1$ and a positive integer n can be constructed from some symmetric self-dual code $\mathcal{C}'$ of length $2n$ by the construction method in Theorem 8.

Proof: We may assume that $\mathcal{C}$ is a symmetric self-dual code with a symmetric generator matrix

$$G = \left(\begin{array}{c|c|c|c} 1 & 0 & \gamma & \mathbf{x} \\ \hline 0^T & I_n & \mathbf{x}^T & A \end{array}\right)$$

where A is an $n \times n$ symmetric matrix, $\gamma \in GF(q)$, and $\mathbf{x}$ is a vector in $GF(q)^n$. If $\mathbf{x}$ is a zero vector, G (or $\mathcal{C}$) is decomposable and gives the second case of Theorem 8.

Therefore, we suppose that $\mathbf{x}$ is a non-zero vector. Since there are two square roots of -1, we can take α as a square root of -1 which is not equal to γ. Let $\beta = (\gamma - \alpha)^{-1}$ and $A' = A - \beta\mathbf{x}^T\mathbf{x}$. It is clear that A' is symmetric. By Lemma 9, $\mathbf{x}^T$ is an eigenvector of A' with eigenvalue α. Consider a symmetric self-dual code C' of length $2n$ with the generator matrix

$$G' = \left(I_n | A'\right).$$

Applying the construction method in Theorem 8 on G', we recover the matrix G as follows.

$$\begin{aligned}G &= \left(\begin{array}{c|c|c|c} 1 & 0 & \gamma & \mathbf{x} \\ \hline 0^T & I_n & \mathbf{x}^T & A' + \beta\mathbf{x}^T\mathbf{x} \end{array}\right) \\ &= \left(\begin{array}{c|c|c|c} 1 & 0 & \gamma & \mathbf{x} \\ \hline 0^T & I_n & \mathbf{x}^T & A \end{array}\right) \text{ because } A' + \beta\mathbf{x}^T\mathbf{x} = A.\end{aligned}$$

Therefore, C can be constructed from a symmetric self-dual code C' of length $2n$ with the generator matrix G' as wanted. □

Remark 11: Theorems 8 and 10 might be regarded as a special case of the well-known 'building-up' construction method [25, Propositions 2.1, 2.2]. But Theorems 8 and 10 have a significant difference. We only have to choose vectors from an eigenspace of A with an eigenvalue of a root of -1. This improves the efficiency to find a best self-dual code from a self-dual code of smaller length. We also point out that all of the self-dual codes used in this method have symmetric generator matrices. Thus, we can focus our concern in one subclass of self-dual codes that have a certain automorphism in their automorphism group.

Example 12: Let $\mathcal{C}_5^{16}$ be a symmetric self-dual [16,8,6] code over $GF(5)$ with generator matrix

$$G = (I_8 \mid A) = \begin{pmatrix} 1&0&0&0&0&0&0&0&1&4&3&3&2&4&0&2\\ 0&1&0&0&0&0&0&0&4&2&0&2&4&3&2&1\\ 0&0&1&0&0&0&0&0&3&0&1&1&3&3&3&4\\ 0&0&0&1&0&0&0&0&3&2&1&0&2&0&0&1\\ 0&0&0&0&1&0&0&0&2&4&3&2&4&1&3&0\\ 0&0&0&0&0&1&0&0&4&3&3&0&1&1&2&2\\ 0&0&0&0&0&0&1&0&0&2&3&0&3&2&3&2\\ 0&0&0&0&0&0&0&1&2&1&4&1&0&2&2&3 \end{pmatrix},$$

which is optimal. Then, the eigenspace of A with eigenvalue $\alpha = 2$ is a subspace of $GF(5)^8$ of dimension four generated by the row vectors of the matrix $\begin{pmatrix} 1&0&0&0&0&3&0&2\\ 0&1&0&0&3&4&2&2\\ 0&0&1&0&4&3&2&1\\ 0&0&0&1&1&0&2&0 \end{pmatrix}$. Among these $5^4 = 625$ eigenvectors, if we choose a vector $\mathbf{x} = 43411113$, then using the construction method in Theorem 8 with $\gamma = 0$ and $\beta = (\gamma - \alpha)^{-1} = 2$, we obtain an 'optimal' symmetric self-dual [18,9,7] code with generator matrix

$$G' = \left(\begin{array}{c|c|c|c} 1 & 0 & \gamma & \mathbf{x} \\ \hline 0^T & I_n & \mathbf{x}^T & A + \beta \mathbf{x}^T \mathbf{x} \end{array}\right)$$

$$= \begin{pmatrix} 1&0&0&0&0&0&0&0&0&0&4&3&4&1&1&1&1&3\\ 0&1&0&0&0&0&0&0&0&4&3&3&0&1&0&2&3&1\\ 0&0&1&0&0&0&0&0&0&3&3&0&4&3&0&4&3&4\\ 0&0&0&1&0&0&0&0&0&4&0&4&3&4&1&1&1&3\\ 0&0&0&0&1&0&0&0&0&1&1&3&4&2&4&2&2&2\\ 0&0&0&0&0&1&0&0&0&1&0&0&1&4&1&3&0&1\\ 0&0&0&0&0&0&1&0&0&1&2&4&1&2&3&3&4&3\\ 0&0&0&0&0&0&0&1&0&1&3&3&1&2&0&4&0&3\\ 0&0&0&0&0&0&0&0&1&4&1&4&3&2&1&3&3&1 \end{pmatrix}$$

We close this section by comparing the complexity of our method with that of the well-known 'building-up' method in [25, Proposition 2.1]. If we apply the 'building-up' method in [25, Proposition 2.1] to the self-dual code $\mathcal{C}_5^{16}$ of length 16 in Example 12 to construct self-dual codes of length 18, a vector is typically chosen from $GF(5)^{15}$, i.e., there are 5^{15} possible choices. In contrast, as we have already seen in Example 12, the number of possible choices of vectors is reduced only to 5^4 when our new method is applied.

In general, according to our computational experience to obtain several best self-dual codes in Table 4, we only need about $q^{\lfloor \frac{n}{2} \rfloor}$ choices of eigenvectors when a given length is $2n$. Due to this reduced complexity, we have succeeded in constructing self-dual codes of lengths greater than 22.

We remark that the building-up method in [25] will generate much more self-dual codes than our method based on symmetric matrices. However, many of them will have low minimum distances as well. Therefore, the result in this paper is justifying that symmetric matrices are efficient samples to derive best known minimum distances of self-dual codes over large finite fields.

IV. COMPUTATIONAL RESULTS OF OPTIMAL OR BEST-KNOWN SELF-DUAL CODES

In this section, we construct optimal self-dual codes over $GF(13)$ and $GF(17)$ by using the method in the previous section. From now on, for the brevity, we denote a symmetric $[2n, k, d]$ self-dual code over $GF(p)$ as $\mathcal{C}_p^{2n}$ and its generator matrix as $(I_n \mid A_p^{2n})$. All the computations are done in Magma [6].

TABLE 6. Constuction of a chain of best-known self-dual codes over GF(13).

Code	α	γ	$\mathbf{x}$	min. wt.
$\mathcal{C}_{13}^{26,1}$				10
$\mathcal{C}_{13}^{28,1}$	8	4	(2,10,8,6,3,1,12,1,11,8,9,11,2)	11
$\mathcal{C}_{13}^{30,1}$	8	11	(10,8,9,2,1,4,12,12,7,12,2,2,6,6)	11
$\mathcal{C}_{13}^{32,1}$	8	11	(5,8,5,2,7,11,11,10,12,2,11,12,3,4,7)	12
$\mathcal{C}_{13}^{34,1}$	5	1	(0,3,7,5,1,10,11,3,7,2,10,12,2,6,12,10)	12
$\mathcal{C}_{13}^{36,1}$	8	6	(3,1,1,5,8,1,6,3,1,4,1,1,3,11,8,2,4)	13
$\mathcal{C}_{13}^{38,1}$	5	3	(8,0,3,2,11,6,8,3,9,3,7,1,7,2,8,11,9,2)	13
$\mathcal{C}_{13}^{40,1}$	5	8	(5,10,5,4,1,8,1,2,3,4,11,5,8,6,3,2,12,9,3)	14

A. OPTIMAL SELF-DUAL CODES OVER $GF(13)$

In [3], the optimal minimum weights of self-dual codes over $GF(13)$ are determined for lengths up to 20 except 12, and the minimum optimal weight of length 12 is determined in [14]. However, we pointed out that the existence of optimal self-dual codes of length 18 turns out to be unknown. This is to be discussed in Remark 14. We obtain a [18,9,8] self-dual code with a symmetric generator matrix G_{13}^{18}, which is now known to have the best-known minimum weight.

$$G_{13}^{18} = \begin{pmatrix} 1&0&0&0&0&0&0&0&0&10&5&5&0&1&9&12&2&3\\ 0&1&0&0&0&0&0&0&0&5&7&11&10&4&4&12&6&5\\ 0&0&1&0&0&0&0&0&0&5&11&5&3&5&3&7&6&5\\ 0&0&0&1&0&0&0&0&0&0&10&3&5&6&6&0&6&2\\ 0&0&0&0&1&0&0&0&0&1&4&5&6&0&10&5&1&9\\ 0&0&0&0&0&1&0&0&0&9&4&3&6&10&12&9&4&6\\ 0&0&0&0&0&0&1&0&0&12&12&7&0&5&9&3&12&1\\ 0&0&0&0&0&0&0&1&0&2&6&6&6&1&4&12&4&10\\ 0&0&0&0&0&0&0&0&1&3&5&5&2&9&6&1&10&11 \end{pmatrix}.$$

In Table 6, we illustrate the chain of self-dual codes constructed by using Theorem 8, successively from [26,13,10] code $\mathcal{C}_{13}^{26,1}$ to [40,20,14] code $\mathcal{C}_{13}^{40,1}$. These self-dual codes are all new and have the best-known minimum weights. The [26,13,10] self-dual code $\mathcal{C}_{13}^{26,1}$ has a generator matrix $(I_{13} \mid A_{13}^{26,1})$ where

$$A_{13}^{26,1} = \begin{pmatrix} 7&7&1&8&3&6&3&8&10&10&10&0&9\\ 7&8&10&8&7&5&7&8&8&11&7&0&4\\ 1&10&11&11&10&9&5&7&10&4&8&7&11\\ 8&8&11&12&7&11&3&12&4&12&11&8&11\\ 3&7&10&7&10&0&8&12&12&7&10&10&1\\ 6&5&9&11&0&8&5&7&3&11&8&4&8\\ 3&7&5&3&8&5&3&4&11&5&6&11&6\\ 8&8&7&12&12&7&4&8&0&4&3&1&9\\ 10&8&10&4&12&3&11&0&4&8&3&10&7\\ 10&11&4&12&7&11&5&4&8&5&9&1&4\\ 10&7&8&11&10&8&6&3&3&9&11&0&8\\ 0&0&7&8&10&4&11&1&10&1&0&5&4\\ 9&4&11&11&1&8&6&9&7&4&8&4&10 \end{pmatrix}.$$

We give generator matrices of new symmetric self-dual codes over $GF(13)$ of lengths up to 40.

- A symmetric self-dual [28,14,11] code

$$\begin{pmatrix} 4&2&10&8&6&3&1&12&1&11&8&9&11&2\\ 2&6&2&10&5&8&12&10&1&11&6&12&1&8\\ 10&2&9&3&6&6&9&3&12&0&4&4&5&12\\ 8&10&3&8&12&4&7&7&5&1&1&3&11&7\\ 6&5&6&12&3&9&3&11&4&7&0&4&11&8\\ 3&8&6&4&9&11&9&12&8&7&1&0&5&6\\ 1&12&9&7&3&9&11&2&10&10&9&9&11&1\\ 12&10&3&7&11&12&2&6&1&4&7&5&4&0\\ 1&1&12&5&4&8&10&1&11&7&2&4&8&2\\ 11&11&0&1&7&7&10&4&7&3&12&1&9&8\\ 8&6&4&1&0&1&9&7&2&12&2&4&5&0\\ 9&12&4&3&4&0&9&5&4&1&4&7&11&10\\ 11&1&5&11&11&5&11&4&8&9&5&11&4&5\\ 2&8&12&7&8&6&1&0&2&8&0&10&5&9 \end{pmatrix}.$$

- A symmetric self-dual [30,15,11] code

$$\begin{pmatrix}
11 & 10 & 8 & 9 & 2 & 1 & 4 & 12 & 12 & 7 & 12 & 2 & 2 & 6 & 6 \\
10 & 7 & 7 & 1 & 6 & 5 & 12 & 2 & 0 & 7 & 12 & 6 & 7 & 5 & 9 \\
8 & 7 & 10 & 0 & 11 & 12 & 10 & 5 & 3 & 11 & 4 & 7 & 0 & 4 & 11 \\
9 & 1 & 0 & 10 & 9 & 9 & 5 & 6 & 0 & 7 & 10 & 10 & 10 & 10 & 4 \\
2 & 6 & 11 & 9 & 5 & 4 & 11 & 2 & 2 & 1 & 9 & 11 & 0 & 2 & 11 \\
1 & 5 & 12 & 9 & 4 & 12 & 6 & 7 & 2 & 2 & 11 & 5 & 9 & 0 & 10 \\
4 & 12 & 10 & 5 & 11 & 6 & 12 & 12 & 2 & 0 & 10 & 8 & 7 & 0 & 1 \\
12 & 2 & 5 & 6 & 2 & 7 & 12 & 7 & 11 & 12 & 6 & 4 & 4 & 9 & 12 \\
12 & 0 & 3 & 0 & 2 & 2 & 2 & 11 & 2 & 3 & 0 & 2 & 0 & 2 & 11 \\
7 & 7 & 11 & 7 & 1 & 2 & 0 & 12 & 3 & 10 & 9 & 11 & 0 & 9 & 3 \\
12 & 12 & 4 & 10 & 9 & 11 & 10 & 6 & 0 & 9 & 12 & 7 & 9 & 7 & 6 \\
2 & 6 & 7 & 10 & 11 & 5 & 8 & 4 & 2 & 11 & 7 & 12 & 1 & 9 & 4 \\
2 & 7 & 0 & 10 & 0 & 9 & 7 & 4 & 0 & 0 & 9 & 1 & 4 & 2 & 1 \\
6 & 5 & 4 & 10 & 2 & 0 & 0 & 9 & 2 & 9 & 7 & 9 & 2 & 3 & 4 \\
6 & 9 & 11 & 4 & 11 & 10 & 1 & 12 & 11 & 3 & 6 & 4 & 1 & 4 & 8
\end{pmatrix}$$

- A symmetric self-dual [32,16,12] code

$$\begin{pmatrix}
11 & 5 & 8 & 5 & 2 & 7 & 11 & 11 & 10 & 12 & 2 & 11 & 12 & 3 & 4 & 7 \\
5 & 2 & 6 & 12 & 8 & 5 & 2 & 5 & 7 & 6 & 6 & 0 & 9 & 7 & 4 & 9 \\
8 & 6 & 11 & 3 & 2 & 3 & 4 & 11 & 7 & 6 & 8 & 11 & 12 & 2 & 7 & 6 \\
5 & 12 & 3 & 1 & 12 & 1 & 0 & 11 & 0 & 10 & 10 & 5 & 1 & 5 & 2 & 1 \\
2 & 8 & 2 & 12 & 7 & 5 & 12 & 8 & 4 & 8 & 4 & 0 & 5 & 12 & 4 & 0 \\
7 & 5 & 3 & 1 & 5 & 4 & 8 & 2 & 8 & 4 & 10 & 0 & 0 & 7 & 7 & 10 \\
11 & 2 & 4 & 0 & 12 & 8 & 9 & 3 & 9 & 7 & 5 & 8 & 10 & 7 & 6 & 1 \\
11 & 5 & 11 & 11 & 8 & 2 & 3 & 9 & 1 & 7 & 3 & 7 & 0 & 5 & 6 & 5 \\
10 & 7 & 7 & 0 & 4 & 8 & 9 & 1 & 10 & 12 & 10 & 8 & 5 & 1 & 5 & 5 \\
12 & 6 & 6 & 10 & 8 & 4 & 7 & 7 & 12 & 11 & 11 & 5 & 11 & 12 & 5 & 0 \\
2 & 6 & 8 & 10 & 4 & 10 & 5 & 3 & 10 & 11 & 7 & 12 & 6 & 2 & 3 & 12 \\
11 & 0 & 11 & 5 & 0 & 0 & 8 & 7 & 8 & 5 & 12 & 9 & 12 & 7 & 0 & 10 \\
12 & 9 & 12 & 1 & 5 & 0 & 10 & 0 & 5 & 11 & 6 & 12 & 8 & 0 & 12 & 6 \\
3 & 7 & 2 & 5 & 12 & 7 & 7 & 5 & 1 & 12 & 2 & 7 & 0 & 7 & 6 & 8 \\
4 & 4 & 7 & 2 & 4 & 7 & 6 & 6 & 5 & 5 & 3 & 0 & 12 & 6 & 4 & 9 \\
7 & 9 & 6 & 1 & 0 & 10 & 1 & 5 & 5 & 0 & 12 & 10 & 6 & 8 & 9 & 7
\end{pmatrix}$$

- A symmetric self-dual [34,17,12] code

$$\begin{pmatrix}
1 & 0 & 3 & 7 & 5 & 1 & 10 & 11 & 3 & 7 & 2 & 10 & 12 & 2 & 6 & 12 & 10 \\
0 & 11 & 5 & 8 & 5 & 2 & 7 & 11 & 11 & 10 & 12 & 2 & 11 & 12 & 3 & 4 & 7 \\
3 & 5 & 3 & 4 & 5 & 4 & 4 & 10 & 6 & 5 & 11 & 5 & 4 & 1 & 9 & 8 & 8 \\
7 & 8 & 4 & 2 & 4 & 10 & 5 & 1 & 9 & 11 & 9 & 10 & 3 & 2 & 11 & 12 & 8 \\
5 & 5 & 5 & 4 & 11 & 1 & 8 & 9 & 4 & 1 & 1 & 4 & 3 & 5 & 4 & 0 & 8 \\
1 & 2 & 4 & 10 & 1 & 10 & 9 & 6 & 4 & 12 & 1 & 8 & 10 & 11 & 4 & 1 & 4 \\
10 & 7 & 4 & 5 & 8 & 9 & 5 & 0 & 1 & 10 & 12 & 11 & 9 & 8 & 5 & 3 & 11 \\
11 & 11 & 10 & 1 & 9 & 6 & 0 & 8 & 11 & 6 & 8 & 10 & 1 & 11 & 10 & 12 & 6 \\
3 & 11 & 6 & 9 & 4 & 4 & 1 & 11 & 10 & 12 & 12 & 2 & 11 & 5 & 7 & 10 & 4 \\
7 & 10 & 5 & 11 & 1 & 12 & 10 & 6 & 12 & 1 & 2 & 12 & 0 & 8 & 10 & 10 & 7 \\
2 & 12 & 11 & 9 & 1 & 1 & 12 & 8 & 12 & 2 & 10 & 6 & 12 & 10 & 9 & 12 & 8 \\
10 & 2 & 5 & 10 & 4 & 8 & 11 & 10 & 2 & 12 & 6 & 8 & 8 & 1 & 0 & 12 & 0 \\
12 & 11 & 4 & 3 & 3 & 10 & 9 & 1 & 11 & 0 & 12 & 8 & 12 & 6 & 2 & 3 & 6 \\
2 & 12 & 1 & 2 & 5 & 11 & 8 & 11 & 5 & 8 & 10 & 1 & 6 & 7 & 10 & 6 & 1 \\
6 & 3 & 9 & 11 & 4 & 4 & 5 & 10 & 7 & 10 & 9 & 0 & 2 & 10 & 11 & 1 & 6 \\
12 & 4 & 8 & 12 & 0 & 1 & 3 & 12 & 10 & 10 & 12 & 12 & 3 & 6 & 1 & 7 & 5 \\
10 & 7 & 8 & 8 & 8 & 4 & 11 & 6 & 4 & 7 & 8 & 0 & 6 & 1 & 6 & 5 & 8
\end{pmatrix}$$

- A symmetric self-dual [36,18,13] code

$$\begin{pmatrix}
6 & 3 & 1 & 1 & 5 & 8 & 1 & 6 & 3 & 1 & 4 & 1 & 1 & 3 & 11 & 8 & 2 & 4 \\
3 & 3 & 5 & 8 & 6 & 6 & 6 & 1 & 0 & 8 & 1 & 7 & 2 & 1 & 5 & 7 & 9 & 4 \\
1 & 5 & 4 & 11 & 12 & 1 & 8 & 4 & 3 & 4 & 8 & 5 & 8 & 3 & 0 & 12 & 3 & 5 \\
1 & 8 & 11 & 9 & 8 & 1 & 10 & 1 & 2 & 12 & 3 & 4 & 11 & 9 & 2 & 5 & 7 & 6 \\
5 & 6 & 12 & 8 & 9 & 10 & 1 & 3 & 0 & 0 & 1 & 0 & 1 & 2 & 7 & 4 & 7 & 11 \\
8 & 6 & 1 & 1 & 10 & 5 & 10 & 10 & 10 & 0 & 11 & 10 & 0 & 4 & 0 & 11 & 5 & 5 \\
1 & 6 & 8 & 10 & 1 & 10 & 3 & 6 & 11 & 10 & 10 & 7 & 1 & 2 & 12 & 0 & 0 & 2 \\
6 & 1 & 4 & 1 & 3 & 10 & 6 & 0 & 4 & 11 & 11 & 9 & 8 & 0 & 1 & 7 & 10 & 12 \\
3 & 0 & 3 & 2 & 0 & 10 & 11 & 4 & 10 & 3 & 0 & 0 & 2 & 3 & 1 & 11 & 9 & 0 \\
1 & 8 & 4 & 12 & 0 & 0 & 10 & 11 & 3 & 3 & 10 & 5 & 8 & 3 & 6 & 3 & 9 & 2 \\
4 & 1 & 8 & 3 & 1 & 11 & 10 & 11 & 0 & 10 & 6 & 0 & 10 & 7 & 12 & 7 & 6 & 12 \\
1 & 7 & 5 & 4 & 0 & 10 & 7 & 9 & 0 & 5 & 0 & 3 & 12 & 4 & 11 & 5 & 11 & 6 \\
1 & 2 & 8 & 11 & 1 & 0 & 1 & 8 & 2 & 8 & 10 & 12 & 1 & 0 & 2 & 9 & 11 & 11 \\
3 & 1 & 3 & 9 & 2 & 4 & 2 & 0 & 3 & 3 & 7 & 4 & 0 & 1 & 9 & 3 & 0 & 0 \\
11 & 5 & 0 & 2 & 7 & 0 & 12 & 1 & 1 & 6 & 12 & 11 & 2 & 9 & 5 & 5 & 8 & 5 \\
8 & 7 & 12 & 5 & 4 & 11 & 0 & 7 & 11 & 3 & 7 & 5 & 9 & 3 & 5 & 5 & 6 & 3 \\
2 & 9 & 3 & 7 & 7 & 5 & 0 & 10 & 9 & 9 & 6 & 11 & 11 & 0 & 8 & 6 & 5 & 1 \\
4 & 4 & 5 & 6 & 11 & 5 & 2 & 12 & 0 & 2 & 12 & 6 & 11 & 0 & 5 & 3 & 1 & 0
\end{pmatrix}$$

- A symmetric self-dual [38,19,13] code

$$\begin{pmatrix}
3 & 8 & 0 & 3 & 2 & 11 & 6 & 8 & 3 & 9 & 3 & 7 & 1 & 7 & 2 & 8 & 11 & 9 & 2 \\
8 & 0 & 3 & 2 & 6 & 0 & 10 & 8 & 7 & 6 & 2 & 2 & 10 & 12 & 8 & 5 & 3 & 5 & 9 \\
0 & 3 & 3 & 5 & 8 & 6 & 6 & 6 & 1 & 0 & 8 & 1 & 7 & 2 & 1 & 5 & 7 & 9 & 4 \\
3 & 2 & 5 & 6 & 8 & 2 & 5 & 9 & 6 & 9 & 6 & 4 & 10 & 4 & 0 & 1 & 2 & 9 & 2 \\
2 & 6 & 8 & 8 & 7 & 10 & 8 & 2 & 11 & 6 & 9 & 9 & 3 & 4 & 7 & 7 & 7 & 11 & 4 \\
11 & 0 & 6 & 2 & 10 & 7 & 3 & 9 & 6 & 9 & 3 & 8 & 1 & 8 & 4 & 2 & 2 & 3 & 0 \\
6 & 10 & 6 & 5 & 8 & 3 & 0 & 12 & 1 & 9 & 4 & 3 & 7 & 5 & 11 & 2 & 4 & 4 & 12 \\
8 & 8 & 6 & 9 & 2 & 9 & 12 & 10 & 7 & 1 & 11 & 8 & 3 & 12 & 7 & 6 & 8 & 3 & 7 \\
3 & 7 & 1 & 6 & 11 & 6 & 1 & 7 & 2 & 10 & 0 & 7 & 1 & 4 & 10 & 2 & 10 & 3 & 9 \\
9 & 6 & 0 & 9 & 6 & 9 & 9 & 1 & 10 & 2 & 9 & 1 & 2 & 3 & 7 & 4 & 7 & 1 & 4 \\
3 & 2 & 8 & 6 & 9 & 3 & 4 & 11 & 0 & 9 & 5 & 6 & 10 & 4 & 0 & 7 & 6 & 2 & 12 \\
7 & 2 & 1 & 4 & 9 & 8 & 3 & 8 & 7 & 1 & 6 & 1 & 3 & 5 & 0 & 10 & 1 & 7 & 5 \\
1 & 10 & 7 & 10 & 3 & 1 & 7 & 3 & 1 & 2 & 10 & 3 & 9 & 2 & 3 & 7 & 6 & 0 & 5 \\
7 & 12 & 2 & 4 & 4 & 8 & 5 & 12 & 4 & 3 & 4 & 5 & 2 & 9 & 6 & 0 & 3 & 12 & 4 \\
2 & 8 & 1 & 0 & 7 & 4 & 11 & 7 & 10 & 7 & 0 & 0 & 3 & 6 & 12 & 1 & 5 & 4 & 11 \\
8 & 5 & 5 & 1 & 7 & 2 & 2 & 6 & 2 & 4 & 7 & 10 & 7 & 0 & 1 & 12 & 0 & 11 & 10 \\
11 & 3 & 7 & 2 & 7 & 2 & 4 & 8 & 10 & 7 & 6 & 1 & 6 & 3 & 5 & 0 & 3 & 2 & 5 \\
9 & 5 & 9 & 9 & 11 & 3 & 4 & 3 & 3 & 1 & 2 & 7 & 0 & 12 & 4 & 11 & 2 & 10 & 5 \\
2 & 9 & 4 & 2 & 4 & 0 & 12 & 7 & 9 & 4 & 12 & 5 & 5 & 4 & 11 & 10 & 5 & 5 & 11
\end{pmatrix}$$

- A symmetric self-dual [40,20,14] code

$$\begin{pmatrix}
8 & 5 & 10 & 5 & 4 & 1 & 8 & 1 & 2 & 3 & 4 & 11 & 5 & 8 & 6 & 3 & 2 & 12 & 9 & 3 \\
5 & 7 & 3 & 4 & 1 & 8 & 7 & 12 & 7 & 8 & 7 & 4 & 11 & 10 & 4 & 7 & 7 & 5 & 11 & 7 \\
10 & 3 & 3 & 11 & 11 & 5 & 5 & 9 & 6 & 4 & 2 & 4 & 10 & 2 & 6 & 5 & 3 & 4 & 9 & 6 \\
5 & 4 & 11 & 7 & 3 & 1 & 2 & 12 & 5 & 6 & 11 & 9 & 5 & 3 & 12 & 6 & 4 & 1 & 11 & 9 \\
4 & 1 & 11 & 3 & 7 & 5 & 4 & 2 & 3 & 10 & 10 & 12 & 2 & 12 & 12 & 4 & 8 & 5 & 8 & 6 \\
1 & 8 & 5 & 1 & 5 & 3 & 4 & 4 & 7 & 12 & 3 & 4 & 2 & 10 & 6 & 8 & 12 & 11 & 1 & 5 \\
8 & 7 & 5 & 2 & 4 & 4 & 11 & 10 & 10 & 1 & 11 & 2 & 4 & 5 & 11 & 12 & 3 & 8 & 1 & 8 \\
1 & 12 & 9 & 12 & 2 & 4 & 10 & 9 & 4 & 2 & 6 & 12 & 9 & 1 & 7 & 12 & 7 & 8 & 7 & 0 \\
2 & 7 & 6 & 5 & 3 & 7 & 10 & 4 & 7 & 9 & 8 & 1 & 7 & 4 & 3 & 9 & 3 & 3 & 9 & 9 \\
3 & 8 & 4 & 6 & 10 & 12 & 1 & 2 & 9 & 5 & 1 & 11 & 12 & 9 & 10 & 0 & 4 & 9 & 12 & 12 \\
4 & 7 & 2 & 11 & 10 & 3 & 11 & 6 & 8 & 1 & 3 & 2 & 12 & 4 & 11 & 11 & 11 & 10 & 0 & 8 \\
11 & 4 & 4 & 9 & 12 & 4 & 2 & 12 & 1 & 11 & 2 & 2 & 7 & 9 & 0 & 11 & 10 & 11 & 9 & 10 \\
5 & 11 & 10 & 5 & 2 & 2 & 4 & 9 & 7 & 12 & 12 & 7 & 5 & 12 & 2 & 5 & 9 & 8 & 9 & 10 \\
8 & 10 & 2 & 3 & 12 & 10 & 5 & 1 & 4 & 9 & 4 & 9 & 12 & 0 & 5 & 11 & 8 & 12 & 11 & 0 \\
6 & 4 & 6 & 12 & 12 & 6 & 11 & 7 & 3 & 10 & 11 & 0 & 2 & 5 & 8 & 12 & 4 & 1 & 4 & 10 \\
3 & 7 & 5 & 6 & 4 & 8 & 12 & 12 & 9 & 0 & 11 & 11 & 5 & 11 & 12 & 2 & 3 & 4 & 0 & 1 \\
2 & 7 & 3 & 4 & 8 & 12 & 3 & 7 & 3 & 4 & 11 & 10 & 9 & 8 & 4 & 3 & 9 & 8 & 4 & 12 \\
12 & 5 & 4 & 1 & 5 & 11 & 8 & 8 & 3 & 9 & 10 & 11 & 8 & 12 & 1 & 4 & 8 & 12 & 12 & 4 \\
9 & 11 & 9 & 11 & 8 & 1 & 1 & 7 & 9 & 12 & 0 & 9 & 9 & 11 & 4 & 0 & 4 & 12 & 11 & 1 \\
3 & 7 & 6 & 9 & 6 & 5 & 8 & 0 & 9 & 12 & 8 & 10 & 10 & 0 & 10 & 1 & 12 & 4 & 1 & 1
\end{pmatrix}$$

B. OPTIMAL SELF-DUAL CODES OVER GF(17)

We consruct [26,13,10] and [28,14,11] self-dual codes over GF(17) which are new, succesively from a [24,12,9] self-dual code by using Theorem 8 as follows. At first, we obtain a [24,12,9] code with generator matrix $(I_{12} \mid A_{17}^{24,1})$ where

$$A_{17}^{24,1} = \begin{pmatrix}
10 & 8 & 15 & 7 & 4 & 13 & 10 & 11 & 6 & 12 & 5 & 2 \\
8 & 3 & 5 & 14 & 15 & 14 & 0 & 6 & 12 & 8 & 9 & 9 \\
15 & 5 & 13 & 1 & 9 & 0 & 6 & 9 & 14 & 3 & 8 & 9 \\
7 & 14 & 1 & 2 & 3 & 15 & 6 & 5 & 14 & 0 & 12 & 10 \\
4 & 15 & 9 & 3 & 15 & 2 & 2 & 12 & 12 & 14 & 9 & 14 \\
13 & 14 & 0 & 15 & 2 & 9 & 3 & 2 & 13 & 8 & 0 & 8 \\
10 & 0 & 6 & 6 & 2 & 3 & 7 & 14 & 4 & 2 & 0 & 5 \\
11 & 6 & 9 & 5 & 12 & 2 & 14 & 12 & 3 & 15 & 13 & 16 \\
6 & 12 & 14 & 14 & 12 & 13 & 4 & 3 & 7 & 1 & 5 & 0 \\
12 & 8 & 3 & 0 & 14 & 8 & 2 & 15 & 1 & 5 & 13 & 13 \\
5 & 9 & 8 & 12 & 9 & 0 & 0 & 13 & 5 & 13 & 10 & 12 \\
2 & 9 & 9 & 10 & 14 & 8 & 5 & 16 & 0 & 13 & 12 & 1
\end{pmatrix}.$$

By taking $\gamma = 4$ and an eigenvector (5, 11, 16, 1, 11, 8, 3, 4, 8, 4, 6, 6) of $A_{17}^{12,9}$ corresponding eigenvalue $\alpha = 13$, we obtain a [26,13,10] self-dual code with generator matrix $(I_{13} \mid A_{17}^{26,1})$ where

$$A_{17}^{26,1} = \begin{pmatrix}
4 & 5 & 11 & 16 & 1 & 11 & 8 & 3 & 4 & 8 & 4 & 6 & 6 \\
5 & 11 & 0 & 8 & 14 & 13 & 1 & 14 & 5 & 11 & 6 & 13 & 10 \\
11 & 0 & 16 & 10 & 9 & 11 & 8 & 2 & 3 & 6 & 5 & 13 & 13 \\
16 & 8 & 10 & 11 & 3 & 14 & 16 & 12 & 0 & 13 & 11 & 3 & 4 \\
1 & 14 & 9 & 3 & 0 & 15 & 16 & 0 & 14 & 15 & 9 & 0 & 15 \\
11 & 13 & 11 & 14 & 15 & 11 & 13 & 4 & 9 & 6 & 11 & 13 & 1 \\
8 & 1 & 8 & 16 & 16 & 13 & 0 & 6 & 6 & 4 & 12 & 6 & 14 \\
3 & 14 & 2 & 12 & 0 & 4 & 6 & 6 & 7 & 7 & 12 & 15 & 3 \\
4 & 5 & 3 & 0 & 14 & 9 & 6 & 7 & 14 & 7 & 0 & 16 & 2 \\
8 & 11 & 6 & 13 & 15 & 6 & 4 & 7 & 7 & 15 & 5 & 11 & 6 \\
4 & 6 & 5 & 11 & 9 & 11 & 12 & 12 & 0 & 5 & 7 & 16 & 16 \\
6 & 13 & 13 & 3 & 0 & 13 & 6 & 15 & 16 & 11 & 16 & 6 & 8 \\
6 & 10 & 13 & 4 & 15 & 1 & 14 & 3 & 2 & 6 & 16 & 8 & 14
\end{pmatrix}.$$

Again, by taking $\gamma = 4$ and an eigenvector (14, 11, 12, 0, 11, 11, 0, 10, 12, 15, 11, 0, 4) of $A_{17}^{26,1}$ corresponding eigenvalue $\alpha = 13$, we obtain a [28,14,11] self-dual code with generator matrix $(I_{14} \mid A_{17}^{28,1})$ where [28,14,11] self-dual code:

$$A_{17}^{28,1} = \begin{pmatrix}
4 & 14 & 11 & 12 & 0 & 11 & 11 & 0 & 10 & 12 & 15 & 11 & 0 & 4 \\
14 & 3 & 3 & 15 & 16 & 16 & 9 & 8 & 12 & 8 & 13 & 2 & 6 & 13 \\
11 & 3 & 7 & 8 & 8 & 10 & 9 & 1 & 15 & 13 & 4 & 2 & 13 & 7 \\
12 & 15 & 8 & 0 & 10 & 0 & 2 & 8 & 0 & 4 & 3 & 13 & 13 & 2 \\
0 & 16 & 8 & 10 & 11 & 3 & 14 & 16 & 12 & 0 & 13 & 11 & 3 & 4 \\
11 & 16 & 10 & 0 & 3 & 13 & 11 & 16 & 1 & 5 & 8 & 5 & 0 & 12 \\
11 & 9 & 9 & 2 & 14 & 11 & 7 & 13 & 5 & 0 & 16 & 7 & 13 & 15 \\
0 & 8 & 1 & 8 & 16 & 16 & 13 & 0 & 6 & 6 & 4 & 12 & 6 & 14 \\
10 & 12 & 15 & 0 & 12 & 1 & 5 & 6 & 10 & 5 & 13 & 13 & 15 & 8 \\
12 & 8 & 13 & 4 & 0 & 5 & 0 & 6 & 5 & 15 & 4 & 8 & 16 & 8 \\
15 & 13 & 4 & 3 & 13 & 8 & 16 & 4 & 13 & 4 & 7 & 15 & 11 & 5 \\
11 & 2 & 2 & 13 & 11 & 5 & 7 & 12 & 13 & 8 & 15 & 3 & 16 & 13 \\
0 & 6 & 13 & 13 & 3 & 0 & 13 & 6 & 15 & 16 & 11 & 16 & 6 & 8 \\
4 & 13 & 7 & 2 & 4 & 12 & 15 & 14 & 8 & 8 & 5 & 13 & 8 & 16
\end{pmatrix}.$$

In Table 7, we illustrate a chain of self-dual codes constructed by using Theorem 8, successively from a [28,14,10] code to a [40,20,14] code. The [28,14,10] self-dual code $\mathcal{C}_{17}^{28,2}$

TABLE 7. Constuction of a chain of best-known self-dual codes over GF(17).

Code	α	γ	$\mathbf{x}$	min. wt.
$\mathcal{C}_{17}^{28,2}$				10
$\mathcal{C}_{17}^{30,1}$	13	14	(14,14,0,0,15,9,9,8,1,12,1,2,8,15)	12
$\mathcal{C}_{17}^{32,1}$	4	11	(9,4,10,11,6,4,0,9,7,7,14,4,15,13,7)	12
$\mathcal{C}_{17}^{34,1}$	4	1	(3,16,5,0,0,0,11,7,7,0,6,6,5,7,2,11,)	12
$\mathcal{C}_{17}^{36,1}$	4	7	(10,4,7,7,6,14,9,5,6,9,8,14,13,7,4,6,14)	13
$\mathcal{C}_{17}^{38,1}$	13	4	(1,9,8,8,10,7,13,1,9,1,10,9,0,10,16,5,2,9)	14
$\mathcal{C}_{17}^{40,1}$	4	9	(12,9,13,3,0,3,0,12,15,16,3,6,15,6,15,13,10,10,2)	14

has a generator matrix $(I_{14} \mid A_{17}^{28,2})$ where

$$A_{17}^{28,2} = \begin{pmatrix}
4 & 2 & 4 & 9 & 9 & 7 & 16 & 7 & 13 & 4 & 14 & 11 & 1 & 7 \\
2 & 14 & 16 & 14 & 12 & 3 & 1 & 0 & 3 & 0 & 5 & 3 & 4 & 16 \\
4 & 16 & 4 & 2 & 0 & 5 & 16 & 13 & 2 & 3 & 12 & 9 & 16 & 2 \\
9 & 14 & 2 & 16 & 12 & 0 & 15 & 14 & 8 & 16 & 7 & 14 & 11 & 9 \\
9 & 12 & 0 & 12 & 12 & 7 & 0 & 4 & 13 & 2 & 10 & 1 & 9 & 1 \\
7 & 3 & 5 & 0 & 7 & 13 & 12 & 5 & 2 & 7 & 14 & 5 & 2 & 13 \\
16 & 1 & 16 & 15 & 0 & 12 & 4 & 14 & 11 & 8 & 9 & 8 & 11 & 1 \\
7 & 0 & 13 & 14 & 4 & 5 & 14 & 13 & 8 & 11 & 5 & 8 & 16 & 3 \\
13 & 3 & 2 & 8 & 13 & 2 & 11 & 8 & 14 & 9 & 12 & 9 & 9 & 6 \\
4 & 0 & 3 & 16 & 2 & 7 & 8 & 11 & 9 & 3 & 1 & 16 & 10 & 11 \\
14 & 5 & 12 & 7 & 10 & 14 & 9 & 5 & 12 & 1 & 7 & 4 & 14 & 1 \\
11 & 3 & 9 & 14 & 1 & 5 & 8 & 8 & 9 & 16 & 4 & 6 & 11 & 4 \\
1 & 4 & 16 & 11 & 9 & 2 & 11 & 16 & 9 & 10 & 14 & 11 & 15 & 1 \\
7 & 16 & 2 & 9 & 1 & 13 & 1 & 3 & 6 & 11 & 1 & 4 & 1 & 11
\end{pmatrix}.$$

We give generator matrices of new self-dual codes over $GF(17)$ of even lengths from 30 to 40.

- A symmetric self-dual [30,15,12] code

$$\begin{pmatrix}
14 & 14 & 14 & 0 & 0 & 15 & 9 & 9 & 8 & 1 & 12 & 1 & 2 & 8 & 15 \\
14 & 13 & 11 & 4 & 9 & 15 & 14 & 6 & 0 & 10 & 2 & 11 & 5 & 11 & 13 \\
14 & 11 & 6 & 16 & 14 & 1 & 10 & 8 & 10 & 0 & 15 & 2 & 14 & 14 & 5 \\
0 & 4 & 16 & 4 & 2 & 0 & 5 & 16 & 13 & 2 & 3 & 12 & 9 & 16 & 2 \\
0 & 9 & 14 & 2 & 16 & 12 & 0 & 15 & 14 & 8 & 16 & 7 & 14 & 11 & 9 \\
15 & 15 & 1 & 0 & 12 & 16 & 6 & 16 & 5 & 11 & 12 & 8 & 14 & 10 & 5 \\
9 & 14 & 10 & 5 & 0 & 6 & 9 & 8 & 9 & 11 & 13 & 6 & 6 & 6 & 12 \\
9 & 6 & 8 & 16 & 15 & 16 & 8 & 0 & 1 & 3 & 14 & 1 & 9 & 15 & 0 \\
8 & 0 & 10 & 13 & 14 & 5 & 9 & 1 & 9 & 16 & 5 & 13 & 7 & 12 & 4 \\
1 & 10 & 0 & 2 & 8 & 11 & 11 & 3 & 16 & 15 & 4 & 13 & 11 & 0 & 4 \\
12 & 2 & 15 & 3 & 16 & 12 & 13 & 14 & 5 & 4 & 11 & 13 & 6 & 4 & 4 \\
1 & 11 & 2 & 12 & 7 & 8 & 6 & 1 & 13 & 13 & 13 & 8 & 6 & 5 & 16 \\
2 & 5 & 14 & 9 & 14 & 14 & 6 & 9 & 7 & 11 & 6 & 6 & 10 & 10 & 0 \\
8 & 11 & 14 & 16 & 11 & 10 & 6 & 15 & 12 & 0 & 4 & 5 & 10 & 11 & 2 \\
15 & 13 & 5 & 2 & 9 & 5 & 12 & 0 & 4 & 4 & 4 & 16 & 0 & 2 & 15
\end{pmatrix}$$

- A symmetric self-dual [32,16,12] code

$$\begin{pmatrix}
11 & 9 & 4 & 10 & 11 & 6 & 4 & 0 & 9 & 7 & 7 & 14 & 4 & 15 & 13 & 7 \\
9 & 11 & 7 & 5 & 2 & 15 & 8 & 9 & 6 & 0 & 10 & 13 & 11 & 14 & 15 & 7 \\
4 & 7 & 8 & 7 & 3 & 10 & 10 & 14 & 16 & 4 & 14 & 10 & 6 & 16 & 16 & 0 \\
10 & 5 & 7 & 13 & 5 & 8 & 14 & 10 & 16 & 3 & 10 & 1 & 15 & 16 & 1 & 15 \\
11 & 2 & 3 & 5 & 14 & 9 & 16 & 5 & 1 & 7 & 13 & 8 & 11 & 1 & 0 & 13 \\
6 & 15 & 10 & 8 & 9 & 9 & 13 & 0 & 13 & 3 & 14 & 11 & 8 & 5 & 10 & 15 \\
4 & 8 & 10 & 14 & 16 & 13 & 11 & 6 & 9 & 9 & 15 & 3 & 3 & 8 & 15 & 9 \\
0 & 9 & 14 & 10 & 5 & 0 & 6 & 9 & 8 & 9 & 11 & 13 & 6 & 6 & 6 & 12 \\
9 & 6 & 16 & 16 & 1 & 13 & 9 & 8 & 14 & 10 & 12 & 15 & 11 & 4 & 5 & 9 \\
7 & 0 & 4 & 3 & 7 & 3 & 9 & 9 & 10 & 16 & 6 & 2 & 0 & 5 & 8 & 11 \\
7 & 10 & 14 & 10 & 13 & 14 & 15 & 11 & 12 & 6 & 5 & 1 & 0 & 9 & 13 & 11 \\
14 & 13 & 10 & 1 & 8 & 11 & 3 & 13 & 15 & 2 & 1 & 5 & 4 & 2 & 13 & 1 \\
4 & 11 & 6 & 15 & 11 & 8 & 3 & 6 & 11 & 0 & 0 & 4 & 3 & 0 & 10 & 3 \\
15 & 14 & 16 & 16 & 1 & 5 & 8 & 6 & 4 & 5 & 9 & 2 & 0 & 13 & 16 & 15 \\
13 & 15 & 16 & 1 & 0 & 10 & 15 & 6 & 5 & 8 & 13 & 13 & 10 & 16 & 6 & 15 \\
7 & 7 & 0 & 15 & 13 & 15 & 9 & 12 & 9 & 11 & 11 & 1 & 3 & 15 & 15 & 5
\end{pmatrix}$$

- A symmetric self-dual [34,17,12] code

$$\begin{pmatrix}
1 & 3 & 16 & 5 & 0 & 0 & 0 & 11 & 7 & 7 & 0 & 6 & 6 & 5 & 7 & 2 & 11 \\
3 & 8 & 10 & 16 & 10 & 11 & 6 & 10 & 10 & 2 & 7 & 1 & 8 & 16 & 8 & 11 & 13 \\
16 & 10 & 5 & 3 & 5 & 2 & 15 & 6 & 0 & 14 & 0 & 12 & 15 & 7 & 5 & 10 & 5 \\
5 & 16 & 3 & 11 & 7 & 3 & 10 & 3 & 8 & 10 & 4 & 4 & 0 & 9 & 10 & 7 & 10 \\
0 & 10 & 5 & 7 & 13 & 5 & 8 & 14 & 10 & 16 & 3 & 10 & 1 & 15 & 16 & 1 & 15 \\
0 & 11 & 2 & 3 & 5 & 14 & 9 & 16 & 5 & 1 & 7 & 13 & 8 & 11 & 1 & 0 & 13 \\
0 & 6 & 15 & 10 & 8 & 9 & 9 & 13 & 0 & 13 & 3 & 14 & 11 & 8 & 5 & 10 & 15 \\
11 & 10 & 6 & 3 & 14 & 16 & 13 & 16 & 3 & 6 & 9 & 10 & 15 & 13 & 5 & 2 & 14 \\
7 & 10 & 0 & 8 & 10 & 5 & 0 & 3 & 4 & 3 & 9 & 14 & 16 & 0 & 1 & 7 & 9 \\
7 & 2 & 14 & 10 & 16 & 1 & 13 & 6 & 3 & 9 & 10 & 15 & 1 & 5 & 16 & 6 & 6 \\
0 & 7 & 0 & 4 & 3 & 7 & 3 & 9 & 9 & 10 & 16 & 6 & 2 & 0 & 5 & 8 & 11 \\
6 & 1 & 12 & 4 & 10 & 13 & 14 & 10 & 14 & 15 & 6 & 10 & 6 & 7 & 12 & 9 & 6 \\
6 & 8 & 15 & 0 & 1 & 8 & 11 & 15 & 16 & 1 & 2 & 6 & 10 & 11 & 5 & 9 & 13 \\
5 & 16 & 7 & 9 & 15 & 11 & 8 & 13 & 0 & 5 & 0 & 7 & 11 & 6 & 11 & 1 & 13 \\
7 & 8 & 5 & 10 & 16 & 1 & 5 & 5 & 1 & 16 & 5 & 12 & 5 & 11 & 8 & 0 & 12 \\
2 & 11 & 10 & 7 & 1 & 0 & 10 & 2 & 7 & 6 & 8 & 9 & 9 & 1 & 0 & 16 & 2 \\
11 & 13 & 5 & 10 & 15 & 13 & 15 & 14 & 9 & 6 & 11 & 6 & 13 & 13 & 12 & 2 & 10
\end{pmatrix}$$

- A symmetric self-dual [36,18,13] code

$$\begin{pmatrix}
7 & 10 & 4 & 7 & 7 & 6 & 14 & 9 & 5 & 6 & 9 & 8 & 14 & 13 & 7 & 4 & 6 & 14 \\
10 & 6 & 5 & 11 & 0 & 3 & 7 & 13 & 5 & 10 & 3 & 4 & 13 & 4 & 0 & 9 & 5 & 1 \\
4 & 5 & 2 & 8 & 14 & 1 & 7 & 1 & 11 & 1 & 14 & 12 & 14 & 14 & 14 & 2 & 2 & 9 \\
7 & 11 & 8 & 10 & 8 & 2 & 12 & 2 & 12 & 14 & 1 & 13 & 5 & 0 & 12 & 3 & 7 & 15 \\
7 & 0 & 14 & 8 & 16 & 4 & 13 & 14 & 9 & 5 & 14 & 0 & 14 & 2 & 14 & 8 & 4 & 3 \\
6 & 3 & 1 & 2 & 4 & 8 & 16 & 9 & 7 & 5 & 0 & 2 & 4 & 10 & 12 & 7 & 13 & 9 \\
14 & 7 & 7 & 12 & 13 & 16 & 0 & 0 & 11 & 16 & 9 & 16 & 16 & 12 & 4 & 14 & 11 & 16 \\
9 & 13 & 1 & 2 & 14 & 9 & 0 & 2 & 11 & 1 & 6 & 10 & 5 & 16 & 12 & 0 & 11 & 6 \\
5 & 5 & 11 & 12 & 9 & 7 & 11 & 11 & 13 & 13 & 4 & 11 & 5 & 14 & 2 & 6 & 12 & 9 \\
6 & 10 & 1 & 14 & 5 & 5 & 16 & 1 & 13 & 16 & 4 & 8 & 8 & 8 & 14 & 9 & 2 & 3 \\
9 & 3 & 14 & 1 & 14 & 0 & 9 & 6 & 4 & 4 & 2 & 0 & 6 & 6 & 9 & 11 & 7 & 14 \\
8 & 4 & 12 & 13 & 0 & 2 & 16 & 10 & 11 & 8 & 0 & 9 & 15 & 14 & 13 & 10 & 7 & 3 \\
14 & 13 & 14 & 5 & 14 & 4 & 16 & 5 & 5 & 8 & 6 & 15 & 13 & 10 & 0 & 8 & 3 & 9 \\
13 & 4 & 14 & 0 & 2 & 10 & 12 & 16 & 14 & 8 & 6 & 14 & 10 & 4 & 13 & 11 & 1 & 0 \\
7 & 0 & 14 & 12 & 14 & 12 & 4 & 12 & 2 & 14 & 9 & 13 & 0 & 13 & 11 & 9 & 15 & 6 \\
4 & 9 & 2 & 3 & 8 & 7 & 14 & 0 & 6 & 9 & 11 & 10 & 8 & 11 & 9 & 2 & 8 & 8 \\
6 & 5 & 2 & 7 & 4 & 13 & 11 & 11 & 12 & 2 & 7 & 7 & 3 & 1 & 15 & 8 & 11 & 13 \\
14 & 1 & 9 & 15 & 3 & 9 & 16 & 6 & 9 & 3 & 14 & 3 & 9 & 0 & 6 & 8 & 13 & 13
\end{pmatrix}$$

- A symmetric self-dual [38,19,14] code

$$\begin{pmatrix}
4 & 1 & 9 & 8 & 8 & 10 & 7 & 13 & 1 & 9 & 1 & 10 & 9 & 0 & 10 & 16 & 5 & 2 & 9 \\
1 & 5 & 9 & 5 & 8 & 4 & 9 & 5 & 7 & 4 & 4 & 6 & 7 & 14 & 10 & 9 & 11 & 2 & 13 \\
9 & 9 & 14 & 14 & 3 & 7 & 13 & 11 & 12 & 13 & 9 & 10 & 12 & 13 & 11 & 1 & 4 & 3 & 9 \\
8 & 5 & 14 & 10 & 16 & 7 & 8 & 3 & 2 & 3 & 2 & 7 & 4 & 14 & 7 & 13 & 7 & 4 & 1 \\
8 & 8 & 3 & 16 & 1 & 1 & 9 & 8 & 3 & 4 & 15 & 11 & 5 & 5 & 10 & 11 & 8 & 9 & 7 \\
10 & 4 & 7 & 7 & 1 & 3 & 0 & 8 & 11 & 16 & 2 & 1 & 7 & 14 & 6 & 0 & 10 & 15 & 10 \\
7 & 9 & 13 & 8 & 9 & 0 & 12 & 4 & 12 & 0 & 8 & 13 & 12 & 4 & 6 & 9 & 5 & 2 & 2 \\
13 & 5 & 11 & 3 & 8 & 8 & 4 & 2 & 8 & 15 & 7 & 4 & 3 & 16 & 7 & 13 & 3 & 10 & 3 \\
1 & 7 & 12 & 2 & 3 & 11 & 12 & 8 & 0 & 10 & 16 & 3 & 9 & 5 & 13 & 14 & 7 & 7 & 5 \\
9 & 4 & 13 & 3 & 4 & 16 & 0 & 15 & 10 & 4 & 12 & 11 & 2 & 5 & 4 & 3 & 1 & 10 & 0 \\
1 & 4 & 9 & 2 & 15 & 2 & 8 & 7 & 16 & 12 & 14 & 1 & 7 & 8 & 5 & 16 & 16 & 15 & 2 \\
10 & 6 & 10 & 7 & 11 & 1 & 13 & 4 & 3 & 11 & 1 & 6 & 7 & 6 & 10 & 12 & 13 & 1 & 4 \\
9 & 7 & 12 & 4 & 5 & 7 & 12 & 3 & 9 & 2 & 7 & 7 & 0 & 15 & 4 & 14 & 5 & 5 & 11 \\
0 & 14 & 13 & 14 & 5 & 14 & 4 & 16 & 5 & 5 & 8 & 6 & 15 & 13 & 10 & 0 & 8 & 3 & 9 \\
10 & 10 & 11 & 7 & 10 & 6 & 6 & 7 & 13 & 4 & 5 & 10 & 4 & 10 & 8 & 16 & 13 & 12 & 7 \\
16 & 9 & 1 & 13 & 11 & 0 & 9 & 13 & 14 & 3 & 16 & 12 & 14 & 0 & 16 & 9 & 2 & 2 & 7 \\
5 & 11 & 4 & 7 & 8 & 10 & 5 & 3 & 7 & 1 & 16 & 13 & 5 & 8 & 13 & 2 & 3 & 5 & 3 \\
2 & 2 & 3 & 4 & 9 & 15 & 2 & 10 & 7 & 10 & 15 & 1 & 5 & 3 & 12 & 2 & 5 & 3 & 11 \\
9 & 13 & 9 & 1 & 7 & 10 & 2 & 3 & 5 & 0 & 2 & 4 & 11 & 9 & 7 & 7 & 3 & 11 & 4
\end{pmatrix}$$

- A symmetric self-dual [40,20,14] code

$$\begin{pmatrix}
9 & 12 & 9 & 13 & 3 & 0 & 3 & 0 & 12 & 15 & 16 & 3 & 6 & 15 & 6 & 15 & 13 & 10 & 10 & 2 \\
12 & 9 & 9 & 13 & 5 & 8 & 7 & 7 & 1 & 3 & 10 & 15 & 4 & 11 & 11 & 12 & 3 & 12 & 9 & 7 \\
9 & 9 & 11 & 12 & 7 & 8 & 6 & 9 & 13 & 0 & 9 & 6 & 10 & 0 & 1 & 3 & 12 & 12 & 3 & 3 \\
13 & 13 & 12 & 7 & 15 & 3 & 8 & 13 & 15 & 0 & 7 & 10 & 12 & 0 & 15 & 16 & 11 & 13 & 12 & 4 \\
3 & 5 & 7 & 15 & 5 & 16 & 2 & 8 & 0 & 11 & 16 & 14 & 14 & 13 & 4 & 16 & 14 & 13 & 10 & 9 \\
0 & 8 & 8 & 3 & 16 & 1 & 1 & 9 & 8 & 3 & 4 & 15 & 11 & 5 & 5 & 10 & 11 & 8 & 9 & 7 \\
3 & 7 & 6 & 8 & 2 & 1 & 15 & 0 & 5 & 3 & 12 & 14 & 8 & 16 & 4 & 15 & 1 & 16 & 4 & 1 \\
0 & 7 & 9 & 13 & 8 & 9 & 0 & 12 & 4 & 12 & 0 & 8 & 13 & 12 & 4 & 6 & 9 & 5 & 2 & 2 \\
12 & 1 & 13 & 15 & 0 & 8 & 5 & 4 & 7 & 10 & 16 & 4 & 15 & 5 & 10 & 9 & 0 & 10 & 0 & 1 \\
15 & 3 & 0 & 0 & 11 & 3 & 3 & 12 & 10 & 11 & 7 & 8 & 4 & 3 & 6 & 7 & 2 & 3 & 3 & 11 \\
16 & 10 & 9 & 7 & 16 & 4 & 12 & 0 & 16 & 7 & 11 & 8 & 3 & 16 & 14 & 1 & 14 & 16 & 8 & 3 \\
3 & 15 & 6 & 10 & 14 & 15 & 14 & 8 & 4 & 8 & 8 & 9 & 8 & 16 & 15 & 14 & 0 & 5 & 4 & 10 \\
6 & 4 & 10 & 12 & 14 & 11 & 8 & 13 & 15 & 4 & 3 & 8 & 3 & 8 & 3 & 11 & 14 & 8 & 13 & 3 \\
15 & 11 & 0 & 0 & 13 & 5 & 16 & 12 & 5 & 3 & 16 & 16 & 8 & 11 & 16 & 15 & 2 & 1 & 1 & 0 \\
6 & 11 & 1 & 15 & 4 & 5 & 4 & 4 & 10 & 6 & 14 & 15 & 3 & 16 & 10 & 11 & 2 & 3 & 15 & 8 \\
15 & 12 & 3 & 16 & 16 & 10 & 15 & 6 & 9 & 7 & 1 & 14 & 11 & 15 & 11 & 2 & 4 & 9 & 8 & 13 \\
13 & 3 & 12 & 11 & 14 & 11 & 1 & 9 & 0 & 2 & 14 & 0 & 14 & 2 & 2 & 4 & 2 & 11 & 11 & 2 \\
10 & 12 & 12 & 13 & 13 & 8 & 16 & 5 & 10 & 3 & 16 & 5 & 8 & 1 & 3 & 9 & 11 & 6 & 8 & 7 \\
10 & 9 & 3 & 12 & 10 & 9 & 4 & 2 & 0 & 3 & 8 & 4 & 13 & 1 & 15 & 8 & 11 & 8 & 6 & 15 \\
2 & 7 & 3 & 4 & 9 & 7 & 1 & 2 & 1 & 11 & 3 & 10 & 3 & 0 & 8 & 13 & 2 & 7 & 15 & 15
\end{pmatrix}$$

Additionally, we constructed a best [34,17,13] self-dual code $\mathcal{C}_{17}^{34,2}$ with generator matrix $(I_{17} \mid A_{17}^{34,2})$ where

$$A_{17}^{34,2} = \begin{pmatrix}
3 & 1 & 3 & 1 & 3 & 10 & 14 & 6 & 2 & 9 & 14 & 15 & 10 & 8 & 16 & 2 & 0 \\
1 & 5 & 6 & 3 & 7 & 1 & 9 & 15 & 15 & 0 & 10 & 9 & 4 & 13 & 16 & 11 & 7 \\
3 & 6 & 3 & 12 & 16 & 11 & 2 & 15 & 3 & 14 & 6 & 13 & 11 & 12 & 13 & 1 & 4 \\
1 & 3 & 12 & 3 & 11 & 16 & 7 & 0 & 12 & 15 & 0 & 9 & 3 & 11 & 2 & 1 & 10 \\
3 & 7 & 16 & 11 & 13 & 7 & 2 & 3 & 4 & 9 & 3 & 7 & 4 & 15 & 7 & 5 & 6 \\
10 & 1 & 11 & 16 & 7 & 7 & 14 & 13 & 2 & 1 & 5 & 1 & 14 & 5 & 8 & 8 & 15 \\
14 & 9 & 2 & 7 & 2 & 14 & 8 & 8 & 6 & 1 & 9 & 6 & 3 & 9 & 5 & 5 & 13 \\
6 & 15 & 15 & 0 & 3 & 13 & 8 & 5 & 11 & 14 & 3 & 3 & 14 & 2 & 16 & 7 & 2 \\
2 & 15 & 3 & 12 & 4 & 2 & 6 & 11 & 5 & 7 & 15 & 15 & 10 & 7 & 8 & 2 & 12 \\
9 & 0 & 14 & 15 & 9 & 1 & 1 & 14 & 7 & 2 & 0 & 10 & 4 & 15 & 9 & 13 & 6 \\
14 & 10 & 6 & 0 & 3 & 5 & 9 & 3 & 15 & 0 & 16 & 9 & 16 & 0 & 14 & 4 & 3 \\
15 & 9 & 13 & 9 & 7 & 1 & 6 & 3 & 15 & 10 & 9 & 10 & 5 & 9 & 2 & 7 & 3 \\
10 & 4 & 11 & 3 & 4 & 14 & 3 & 14 & 10 & 4 & 16 & 5 & 9 & 12 & 2 & 7 & 2 \\
8 & 13 & 12 & 11 & 15 & 5 & 9 & 2 & 7 & 15 & 0 & 9 & 12 & 3 & 10 & 15 & 13 \\
16 & 16 & 13 & 2 & 7 & 8 & 5 & 16 & 8 & 9 & 14 & 2 & 2 & 10 & 11 & 16 & 10 \\
2 & 11 & 1 & 1 & 5 & 8 & 5 & 7 & 2 & 13 & 4 & 7 & 7 & 15 & 16 & 15 & 5 \\
0 & 7 & 4 & 10 & 6 & 15 & 13 & 2 & 12 & 6 & 3 & 3 & 2 & 13 & 10 & 5 & 14
\end{pmatrix}.$$

C. QUADRATIC RESIDUE CODES OVER $GF(q)$

In addition to our results on self-dual codes over $GF(13)$ and $GF(17)$, we want to construct self-dual codes over other finite fields. In [3], it is reported that some optimal self-dual codes are obtained from quadratic residue codes following

[7, Theorem 15]. We also obtain new quadratic residue codes in the following theorem. Among them, a [32, 16, 14] code over $GF(19)$, a [20, 10, 10] code over $GF(23)$, a [24, 12, 12] code over $GF(29)$, and a [24, 12, 12] code over $GF(41)$ give the best-known minimum weights which were unknown so far.

Theorem 13: The following quadratic residue codes are self-dual:

a [24, 12, 10] *code over* $GF(13)$,
a [32, 16, 14] *code over* $GF(19)$,
a [20, 10, 10] *code over* $GF(23)$,
a [24, 12, 12] *code over* $GF(29)$,
a [24, 12, 12] *code over* $GF(31)$,
a [24, 12, 12] *code over* $GF(41)$,
a [32, 16, 14] *code over* $GF(41)$.

Remark 14: The [18, 9, 9] linear code, quadratic residue code over $GF(13)$ of length 18, is reported as an optimal self-dual code of that parameter in [3] referring to [7, Theorem 15]. But we point out that the quadratic residue code over $GF(13)$ of length 18 is not self-dual, which has generator

$$A = \begin{pmatrix} 1 & 8 & 10 & 11 & 4 & 11 & 10 & 8 & 4 \\ 5 & 2 & 6 & 0 & 5 & 7 & 9 & 11 & 11 \\ 2 & 8 & 9 & 2 & 8 & 1 & 1 & 12 & 6 \\ 1 & 10 & 5 & 7 & 6 & 6 & 11 & 9 & 10 \\ 4 & 7 & 11 & 10 & 10 & 11 & 7 & 4 & 0 \\ 9 & 11 & 6 & 6 & 7 & 5 & 10 & 1 & 10 \\ 12 & 1 & 1 & 8 & 2 & 9 & 8 & 2 & 6 \\ 11 & 9 & 7 & 5 & 0 & 6 & 2 & 5 & 11 \\ 8 & 10 & 11 & 4 & 11 & 10 & 8 & 1 & 4 \end{pmatrix}.$$

For the details of the self-duality of quadratic residue codes, we refer to [21, Chap. 6.6]. Theorem 6.6.18 in [21] implies that quadratic residue code over $GF(13)$ of length 18 is an iso-dual code, i.e., the code is equivalent to its dual. Therefore, the existence of an optimal self-dual code over $GF(13)$ of length 18 turns out unknown, and that is the reason why we put '?' in Table 4.

Remark 15: We also point out that the quadratic residue code over $GF(17)$ of length 14 is MDS and isodual code with generator matrix in the standard form $(I \mid A)$ where

$$A = \begin{pmatrix} 1 & 5 & 2 & 4 & 2 & 5 & 10 \\ 12 & 10 & 12 & 16 & 11 & 11 & 11 \\ 6 & 8 & 5 & 2 & 11 & 7 & 3 \\ 10 & 5 & 11 & 11 & 5 & 10 & 1 \\ 7 & 11 & 2 & 5 & 8 & 6 & 3 \\ 11 & 11 & 16 & 12 & 10 & 12 & 11 \\ 5 & 2 & 4 & 2 & 5 & 1 & 10 \end{pmatrix}.$$

The new results are updated in Tables 2 and 3, and their generator matrices are as follows.

- A [32, 16, 14] code over $GF(19)$

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

- A [20, 10, 10] code over $GF(23)$

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

- A [24, 12, 12] code over $GF(29)$

$$\begin{pmatrix} 28 & 18 & 21 & 4 & 14 & 23 & 19 & 7 & 25 & 16 & 19 & 1 \\ 19 & 5 & 25 & 3 & 28 & 12 & 10 & 2 & 25 & 11 & 3 & 11 \\ 3 & 23 & 0 & 13 & 19 & 17 & 13 & 18 & 14 & 6 & 12 & 8 \\ 12 & 19 & 3 & 10 & 19 & 4 & 21 & 16 & 8 & 25 & 10 & 25 \\ 10 & 6 & 12 & 21 & 15 & 21 & 17 & 9 & 27 & 22 & 9 & 15 \\ 9 & 22 & 20 & 5 & 11 & 11 & 24 & 12 & 16 & 28 & 25 & 6 \\ 25 & 23 & 19 & 7 & 3 & 16 & 0 & 23 & 25 & 22 & 17 & 10 \\ 17 & 9 & 14 & 9 & 1 & 18 & 12 & 26 & 4 & 14 & 18 & 22 \\ 18 & 12 & 8 & 0 & 18 & 22 & 24 & 2 & 11 & 6 & 20 & 4 \\ 20 & 6 & 27 & 15 & 10 & 22 & 19 & 0 & 24 & 10 & 3 & 13 \\ 3 & 24 & 1 & 15 & 2 & 28 & 23 & 27 & 12 & 5 & 11 & 10 \\ 11 & 8 & 25 & 15 & 6 & 10 & 22 & 4 & 13 & 10 & 28 & 28 \end{pmatrix}$$

- A [24, 12, 12] code over $GF(41)$

$$\begin{pmatrix} 40 & 25 & 28 & 4 & 19 & 33 & 29 & 12 & 37 & 23 & 26 & 40 \\ 26 & 5 & 35 & 6 & 2 & 22 & 17 & 4 & 34 & 13 & 3 & 25 \\ 3 & 33 & 3 & 23 & 31 & 26 & 17 & 22 & 16 & 6 & 17 & 28 \\ 17 & 29 & 8 & 17 & 28 & 3 & 25 & 18 & 8 & 35 & 15 & 4 \\ 15 & 11 & 19 & 30 & 19 & 25 & 19 & 9 & 37 & 32 & 14 & 19 \\ 14 & 34 & 29 & 4 & 10 & 8 & 29 & 15 & 24 & 2 & 37 & 33 \\ 37 & 32 & 23 & 4 & 39 & 19 & 1 & 36 & 40 & 34 & 24 & 29 \\ 24 & 11 & 16 & 9 & 40 & 26 & 20 & 0 & 9 & 21 & 25 & 12 \\ 25 & 14 & 8 & 39 & 26 & 35 & 39 & 7 & 18 & 8 & 27 & 37 \\ 27 & 6 & 37 & 23 & 18 & 37 & 31 & 2 & 33 & 12 & 3 & 23 \\ 3 & 34 & 4 & 25 & 7 & 1 & 32 & 36 & 14 & 5 & 16 & 26 \\ 16 & 13 & 37 & 22 & 8 & 12 & 29 & 4 & 18 & 15 & 40 & 1 \end{pmatrix}$$

V. CONCLUSION

In this paper, we have introduced a new construction method of symmetric self-dual codes. Using this construction method, we have constructed many new self-dual codes. We have also obtained new quadratic residue codes. Consequently, we have improved the bounds of the highest minimum weights of self-dual codes over some finite fields, which stayed unknown for almost two decades because of their computational complexity issue. Our computational results give twenty new highest minimum weights of self-dual codes and 2967 new self-dual codes up to equivalence.

As future work, we will work on the highest minimum weights of self-dual codes over $GF(q)$ where $q \equiv 3 \pmod 4$. Furthermore, we will focus on q^2 even or $q^2 \equiv 1 \pmod 4$ so that Hermitian self-dual or self-orthogonal codes over $GF(q^2)$ will result in quantum codes as well.

REFERENCES

[1] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura, "Type II codes, even unimodular lattices, and invariant rings," *IEEE Trans. Inf. Theory*, vol. 45, no. 4, pp. 1194–1205, May 1999.

[2] I. Be'Ery, N. Raviv, T. Raviv, and Y. Be'Ery, "Active deep decoding of linear codes," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 728–736, Feb. 2020.

[3] K. Betsumiya, S. Georgiou, T. A. Gulliver, M. Harada, and C. Koukouvinos, "On self-dual codes over some prime fields," *Discrete Math.*, vol. 262, nos. 1–3, pp. 37–58, Feb. 2003.

[4] M. F. Bollauf, S. I. R. Costa, and R. Zamir, "Lattice construction C^* from self-dual codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 537–541, doi: 10.1109/ISIT44484.2020.9174473.

[5] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY, USA: Springer, 1999.

[6] J. Cannon and C. Playoust, *An Introduction to Magma*. Sydney, NSW, Australia: Univ. Sydney, 1994.

[7] M. A. De Boer, "Almost MDS codes," *Des., Codes Cryptogr.*, vol. 9, no. 2, pp. 143–155, Oct. 1996.

[8] S. M. Dodunekov and I. N. Landjev, "Near-MDS codes over some small fields," *Discrete Math.*, vol. 213, nos. 1–3, pp. 55–65, Feb. 2000.

[9] S. T. Dougherty, S. Mesnager, and P. Solé, "Secret-sharing schemes based on self-dual codes," in *Proc. IEEE Inf. Theory Workshop*, May 2008, pp. 338–342.

[10] R. T. Eldin and H. Matsui, "On reversibility and self-duality for some classes of quasi-cyclic codes," *IEEE Access*, vol. 8, pp. 143285–143293, 2020, doi: 10.1109/ACCESS.2020.3013958.

[11] W. Fang, S.-T. Xia, and F.-W. Fu, "Construction of MDS Euclidean self-dual codes via two subsets," *IEEE Trans. Inf. Theory*, vol. 67, no. 8, pp. 5005–5015, Aug. 2021, doi: 10.1109/TIT.2021.3085768.

[12] P. Gaborit and A. Otmani, "Experimental constructions of self-dual codes," *Finite Fields Their Appl.*, vol. 9, no. 3, pp. 372–394, Jul. 2003.

[13] S. Georgiou, "MDS self-dual codes over large prime fields," *Finite Fields Their Appl.*, vol. 8, no. 4, pp. 455–470, Oct. 2002.

[14] M. Grass and T. A. Gulliver, "On self-dual MDS codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, ON, Canada, Jul. 2008, pp. 1954–1957.

[15] M. Grassl and T. A. Gulliver, "On circulant self-dual codes over small fields," *Des., Codes Cryptogr.*, vol. 52, no. 1, pp. 57–81, Jul. 2009, doi: 10.1007/s10623-009-9267-1.

[16] T. A. Gulliver, J. L. Kim, and Y. Lee, "New MDS or near-MDS self-dual codes," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4354–4360, Sep. 2008.

[17] T. A. Gulliver and M. Harada, "MDS self-dual codes of lengths 16 and 18," *Int. J. Inf. Coding Theory*, vol. 1, no. 2, pp. 208–213, 2010.

[18] S. Han and J.-L. Kim, "On self-dual codes over $\mathbb{F}_5$," *Des. Codes Cryptogr.*, vol. 48, no. 1, pp. 43–58, 2008.

[19] M. Harada and A. Munemasa. *Database of Self-Dual Codes*. Accessed: Jul. 22, 2021. [Online]. Available: https://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm

[20] M. Harada and P. R. Ostergard, "On the classification of self-dual codes over $\mathbb{F}_5$," *Graphs Combinatorics*, vol. 19, no. 2, pp. 203–214, 2003.

[21] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[22] L. Huang, H. Zhang, R. Li, Y. Ge, and J. Wang, "AI coding: Learning to construct error correction codes," *IEEE Trans. Commun.*, vol. 68, no. 1, pp. 26–39, Jan. 2020.

[23] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Their Appl.*, vol. 11, no. 3, pp. 451–490, Aug. 2005.

[24] L. Jin and C. Xing, "New MDS self-dual codes from generalized Reed–Solomon codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 3, pp. 1434–1438, Mar. 2017.

[25] J.-L. Kim and Y. Lee, "Euclidean and Hermitian self-dual MDS codes over large finite fields," *J. Combinat. Theory A*, vol. 105, no. 1, pp. 79–95, Jan. 2004.

[26] J.-L. Kim, Y.-H. Kim, and N. Lee, "Embedding linear codes into self-orthogonal codes and their optimal minimum distances," *IEEE Trans. Inf. Theory*, vol. 67, no. 6, pp. 3701–3707, Jun. 2021, doi: 10.1109/TIT.2021.3066599.

[27] J. S. Leon, V. Pless, and N. J. A. Sloane, "Self-dual codes over $GF(5)$," *J. Combinat. Theory A*, vol. 32, no. 2, pp. 178–194, 1982.

[28] F. J. MacWilliams, N. J. A. Sloane, and J. G. Thompson, "Good self dual codes exist," *Discrete Math.*, vol. 3, nos. 1–3, pp. 153–162, 1972.

[29] A. Aguilar-Melchor, P. Gaborit, J.-L. Kim, L. Sok, and P. Sole, "Classification of extremal and s-extremal binary self-dual codes of length 38," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2253–2262, Apr. 2012.

[30] P. Mills, "Solving for multi-class using orthogonal coding matrices," *Social Netw. Appl. Sci.*, vol. 1, no. 11, p. 1451, Nov. 2019, doi: 10.1007/s42452-019-1437-9.

[31] E. Nachmani, E. Marciano, L. Lugosch, W. J. Gross, D. Burshtein, and Y. Be'ery, "Deep learning methods for improved decoding of linear codes," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 1, pp. 119–131, Feb. 2018.

[32] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, vol. 17. Berlin, Germany: Springer, 2006.

[33] Y. H. Park, "The classification of self-dual modular codes," *Finite Fields Their Appl.*, vol. 17, no. 5, pp. 442–460, Sep. 2011.

[34] V. Pless and N. J. A. Sloane, "On the classification and enumeration of self-dual code," *J. Combinat. Theory A*, vol. 18, no. 3, pp. 313–335, 1975.

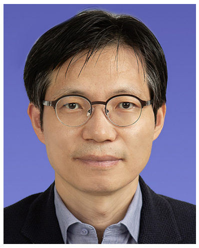
[35] V. Pless and V. Tonchev, "Self-dual codes over $GF(7)$," *IEEE Trans. Inf. Theory*, vol. IT-33, no. 5, pp. 723–727, Sep. 1987.

[36] M. Shi, L. Sok, P. Solé, and S. Calkavur, "Self-dual codes and orthogonal matrices over large finite fields," *Finite Fields Their Appl.*, vol. 54, pp. 297–314, Nov. 2018.

[37] L. Sok, "Explicit constructions of MDS self-dual codes," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3603–3615, Jun. 2020, doi: 10.1109/TIT.2019.2954877.

[38] L. Sok, "New families of self-dual codes," 2020, *arXiv:2005.00726*. [Online]. Available: http://arxiv.org/abs/2005.00726

[39] A. Zhang and K. Feng, "A unified approach to construct MDS self-dual codes via Reed–Solomon codes," *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3650–3656, Jun. 2020, doi: 10.1109/TIT.2020.2963975.



JON-LARK KIM (Member, IEEE) received the B.S. degree in mathematics from POSTECH, the M.S. degree in mathematics from Seoul National University, South Korea, in 1997, and the Ph.D. degree from the Department of Mathematics, University of Illinois at Chicago, in 2002. He was an Associate Professor with the University of Louisville, until 2012. He is currently a Professor with the Department of Mathematics, Sogang University, and the Director of Sogang Artificial Intelligence Laboratories, Seoul, South Korea. He has authored more than 60 research articles and a book titled as *Selected Unsolved Problems in Coding Theory*. His research interests include coding theory, cryptography, informatics, and artificial intelligence. He is a member of the Editorial Board of *Designs, Codes and Cryptography*. He was a recipient of the 2004 Kirkman Medal from the Institute of Combinatorics and its Applications. He is a Co-Editor of *Concise Encyclopedia of Coding Theory* (2021) published by Chapman and Hall/CRC.

WHAN-HYUK CHOI received the B.S. degree in mechanics and aerospace engineering from Seoul National University, Seoul, South Korea, in 2000, and the M.S. and Ph.D. degrees in mathematics from Kangwon National University, Chuncheon, South Korea, in 2017. From 2018 to 2019, he was a Research Professor with Kangwon National University. From 2020 to 2021, he was a Research Associate with Sogang University, Seoul. He is currently a Visiting Professor with the Department of Biomedical Engineering, UNIST, Ulsan, South Korea. His research interests include error-correcting codes over finite fields, designing DNA codes related to DNA computing and DNA data storage, and bio-informatics.