Euclidean and Hermitian Self-Dual MDS Codes over Large Finite Fields

Jon-Lark Kim
Department of Mathematics
810 Oldfather Hall, P.O.Box 880323
University of Nebraska-Lincoln
Lincoln, NE, 68588-0323, USA
e-mail: jlkim@math.unl.edu

Yoonjin Lee
Department of Mathematics, Smith College
Northampton, MA 01063, USA
e-mail: yjlee@math.smith.edu

Abstract

The first author constructed new extremal binary self-dual codes [23] and new self-dual codes over $GF(4)$ with the highest known minimum weights [24]. The method used was to build self-dual codes from a given self-dual code of a smaller length. In this paper we develop a complete generalization of this method for the Euclidean and Hermitian self-dual codes over finite fields $GF(q)$. Using this method we construct many Euclidean and Hermitian self-dual MDS (or near MDS) codes of length up to 12 over various finite fields $GF(q)$, where $q = 8, 9, 16, 25, 32, 41, 49, 53, 64, 81,$ and 128. Our results on the minimum weights of (near) MDS self-dual codes over large fields give a better bound than the Pless-Pierce bound obtained from a modified Gilbert-Varshamov bound.

Index Terms. MDS codes, self-dual codes.

1 Introduction

Self-dual codes over small fields such as binary, ternary, or quaternary fields have intrigued researchers since coding theory was born. For example, two famous binary codes, the extended binary Hamming code of length 8 and the binary Golay code of length 24, are both self-dual. The Tetracode over $GF(3)$ as well as the Hexacode over $GF(4)$ are self-dual. The classification of self-dual codes over $GF(2)$ was attempted first by Pless [31], followed by Pless-Sloane [34], Conway-Pless [9], Conway-Pless-Sloane [11], Conway-Sloane [12], and Bilous-van Rees [6], completing the classification of binary self-dual codes of length up to 32. The classification of self-dual codes over $GF(3)$ was started first by Mallows-Pless-Sloane [29] and then by Conway-Pless-Sloane [10] and Pless-Sloane-Ward [35], completing the classification of ternary self-dual codes of length up to 20. The classification of Hermitian self-dual codes over $GF(4)$ was considered first by MacWilliams-Odlyzko-Sloane-Ward [27], followed by Conway-Pless-Sloane [10], completing the classification of Hermitian self-dual codes of length up to 16. Huffman [20], [21], [22] further classified the extremal Hermitian self-dual codes of length up to 28 over $GF(4)$. One of the reasons why people have been interested in the classification of self-dual codes over $GF(2), GF(3)$, and $GF(4)$ is that the weights in self-dual codes over only these fields are divisible by 2 or 4 for binary self-dual codes, by 3 for ternary self-dual codes and by 2 for the Hermitian self-dual quaternary codes, except for the trivial $[n, n/2, 2]$ self-dual code with q arbitrary and all weights divisible by 2. This is known as the Gleason-Pierce theorem [38] or generally the Gleason-Pierce-Ward theorem [39, pp. 857]. Moreover t-desings hold in extremal self-dual codes over $GF(2)$, $GF(3)$, or $GF(4)$ [32, pp. 110] using the Assmus-Mattson theorem [3]. An extensive discussion of self-dual codes can be found in [37].

The classification of type II Euclidean self-dual codes over $GF(4)$ was attempted by Gaborit-Pless-Solé-Atkin [16], then extended by Betsumiya-Gulliver-Harada-Munemasa [5] up to length 12. Similarly the classification of type I Euclidean self-dual codes over $GF(4)$ was done by Kim-Kim-Kim [25] up to length 10 and the length 12 of the extremal case.

Constructions of self-dual codes over $GF(5), GF(7)$ and $GF(9)$ can be found in [15], [17], [19], [26] and [36]. However, there are only a few papers [1], [4], [18] devoted to constructing self-dual codes over fields of size greater than 9. These papers [1], [4], [18] considered only Euclidean self-dual codes while our paper will discuss Hermitian self-dual codes as well as Euclidean self-dual codes over fields of size at least 8. Our method for constructing self-dual codes works when $q \equiv 1 \pmod 4$ or q is even. We show that all self-dual codes over $GF(q)$ are constructed by this method unless $q \equiv 3 \pmod 4$.

To begin, we give a brief introduction to some basic definitions and facts from coding theory. The interested reader can refer to [28], [37].

A *linear* $[n, k]$ *code* $\mathcal{C}$ over $GF(q)$ is a k-dimensional vector subspace of $GF(q)^n$, where $GF(q)$ is the Galois field with q elements. The *weight* $\mathrm{wt}(\mathbf{c})$ of a codeword $\mathbf{c} \in \mathcal{C}$ is the number of nonzero components of $\mathbf{c}$. The minimum weight d of all nonzero codewords in $\mathcal{C}$ is called the *minimum weight* of $\mathcal{C}$. An $[n, k, d]$ code is an $[n, k]$ code with the minimum weight d. There are two inner products we are interested in. One is the usual inner product $\cdot$ (i.e. *the Euclidean inner product*) on $GF(q)^n$. When q is an even power of any prime, we can also consider the *Hermitian inner product* which is defined as

$$\mathbf{x} * \mathbf{y} = x_1\overline{y_1} + \cdots + x_n\overline{y_n} \in GF(q),$$

for two vectors $\mathbf{x} = (x_1, \cdots, x_n)$ and $\mathbf{y} = (y_1, \cdots, y_n)$, where $\overline{y_i} = y_i^{\sqrt{q}}$ [37, pp. 180].

The *Euclidean dual code* $\mathcal{C}^{\perp_E}$ of $\mathcal{C}$ is defined as

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

Similarly the *Hermitian dual code* $\mathcal{C}^{\perp_H}$ is defined as

$$\mathcal{C}^{\perp_H} = \{\mathbf{x} \in GF(q)^n \mid \mathbf{x} * \mathbf{y} = 0 \text{ for all } \mathbf{y} \in \mathcal{C}\}.$$

If $\mathcal{C} \subset \mathcal{C}^{\perp_E}$ (respectively $\mathcal{C}^{\perp_H}$), then $\mathcal{C}$ is called a *Euclidean (respectively Hermitian) self-orthogonal* code. If $\mathcal{C} = \mathcal{C}^{\perp_E}$ (respectively $\mathcal{C}^{\perp_H}$), then $\mathcal{C}$ is called a *Euclidean (respectively Hermitian) self-dual* code. It is easy to see that $\mathcal{C}^{\perp_H} = \overline{\mathcal{C}^{\perp_E}}$ since $\mathbf{x} * \mathbf{y} = \mathbf{x} \cdot \overline{\mathbf{y}}$. For a (Euclidean or Hermitian) self-dual $[n, k, d]$ code over $GF(q)$, it is known [37] that the minimum weight is bounded by $d \le [n/2] + 1$. A self-dual $[n, n/2, n/2+1]$ code is called *extremal* and is in fact an MDS code. In general, any linear $[n, k, d]$ code over $GF(q)$ achieving the *Singleton bound* $n - k \ge d - 1$ is called an *MDS code.* A linear $[n, k, n-k]$ code over $GF(q)$ is called an *almost MDS code* [13]. An $[n, k, n-k]$ almost MDS code for which the dual code is also an almost MDS code is called a *near MDS code* [14].

The *MDS Conjecture* asserts that if there is a nontrivial $[n, k]$ MDS code over $GF(q)$, then $n \le q+1$, except when q is even and $k = 3$ or $k = q-1$ in which case $n \le q+2$ [32, pp. 95], [28, pp.

328]. MDS codes are equivalent to geometric objects called *n-arcs* [28, pp. 326] and combinatorial objects called *orthogonal arrays* [28, pp. 328]. In this paper we construct many MDS codes which are also self-dual under the Euclidean or Hermitian inner product.

Let A_i be the number of codewords of weight i in an $[n, k]$ code $\mathcal{C}$. Then the *(Hamming) weight enumerator* $W(y)$ of $\mathcal{C}$ is the polynomial

$$W(y) = \sum_{i=0}^{n} A_i y^i.$$

In fact, the weight enumerator of an $[n, k, d]$ MDS code over $GF(q)$ is completely determined by n, k and q [28, pp. 320]. If two linear codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are *permutation equivalent* if there is a permutation of coordinates which sends $\mathcal{C}_1$ to $\mathcal{C}_2$.

It is known [33] that Euclidean or Hermitian self-dual codes over $GF(q)$ satisfy a modified Gilbert-Varshamov bound (see also [37, pp. 253]). The proof given in [33] is not constructive. There are a few known general constructions of self-dual codes over $GF(q)$ including the double-circulant construction, orthogonal designs and weighing matrices [1], [4], [18].

In this paper, we give an efficient construction method for self-dual (self-orthogonal) codes with respect to the Euclidean or Hermitian inner product. Using this method we construct many Euclidean or Hermitian self-dual MDS (or near MDS) codes of lengths up to 12 over finite fields $GF(q)$, where $q = 8, 9, 16, 25, 32, 41, 49, 53, 64, 81, 128$. We used Magma [8] for constructing examples. We summarize our results in Table 1, where the first column denotes the code length, and the columns with q^E (respectively q^H) give the field size q and the attainable minimum weights for Euclidean (respectively Hermitian) self-dual codes from our examples. It turns out that our results (appearing in bold faces) on the minimum weights of (near) MDS self-dual codes improve the Pless-Pierce bound [33] (appearing in the parenthesis) obtained from a modified Gilbert-Varshamov bound.

Table 1: Minimum weights of (near) MDS codes of lengths $n \leq 12$ over $GF(q)$

n	$q^E =$	41	49	53	$q^H =$	9	25	49	81	$q^E =$	8	16	32	64	128
2		2	2	2		2	2	2	2		2	2	2	2	2
4		3	3	3		**3**(2)	3	3	3		3	3	3	3	3
6		4	4	4		**4**(3)	4	4	4		**4**(3)	**4**(3)	4	4	4
8		**5**(4)	**5**(4)	**5**(4)		4	**5**(4)	**5**(4)	5		4	**5**(4)	**5**(4)	**5**(4)	5
10		**6**(5)	**6**(5)	**6**(5)		**5**(4)	**6**(5)	**6**(5)	**6**(5)		**5**(4)	5	**6**(5)	5	5
12		6	**7**(6)	6		**6**(5)	**6**(5)	**7**(6)	**7**(6)		5	**6**(5)	6	6	6

2 Building-up construction for Euclidean self-dual codes

In this section we generalize the building-up construction [23, Theorem 1] for self-dual codes over $GF(2)$ to self-dual codes over $GF(q)$, where q is a power of an odd prime. Our building-up construction requires that -1 be a square in $GF(q)$. It is well-known that -1 is a square in $GF(q)$ if and only if $q \equiv 1 \pmod 4$.

When $q \equiv 1 \pmod 4$, the matrix $G_0 = [1\ c]$ generates a self-dual code $\mathcal{C}_0$ over $GF(q)$ of length 2, where c in $GF(q)$ satisfies $c^2 = -1$ in $GF(q)$. Hence for $q \equiv 1 \pmod 4$ there exists a Euclidean self-dual code over $GF(q)$ of length n if and only if $2 \mid n$ [37, pp. 193].

We give the *building-up construction* below and prove that it holds for any Euclidean self-dual code over $GF(q)$ with $q \equiv 1 \pmod 4$; the proof of the following proposition is analogous to [23, Theorem 1], so it is omitted.

Proposition 2.1. *Assume that q is a power of an odd prime such that $q \equiv 1 \pmod 4$. Let c be in $GF(q)$ such that $c^2 = -1$ in $GF(q)$. Let $G_0 = (L \mid R) = (\mathbf{l}_i \mid \mathbf{r}_i)$ be a generator matrix (not necessarily in standard form) of a Euclidean self-dual code $\mathcal{C}_0$ over $GF(q)$ of length $2n$, where $\mathbf{l}_i$ and $\mathbf{r}_i$ are the rows of the matrices L and R respectively, for $1 \le i \le n$. Let $\mathbf{x} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n})$ be a vector in $GF(q)^{2n}$ with $\mathbf{x} \cdot \mathbf{x} = -1$ in $GF(q)$. Suppose that $y_i := (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n}) \cdot (\mathbf{l}_i \mid \mathbf{r}_i)$ for $1 \le i \le n$. Then the following matrix*

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

generates a self-dual code $\mathcal{C}$ over $GF(q)$ of length $2n+2$.

The following proposition shows that every Euclidean self-dual code over $GF(q)$ with $q \equiv 1 \pmod 4$ can be obtained by the building-up method in Proposition 2.1. It is proved in a similar way as [23, Theorem2].

Proposition 2.2. *Assume that q is a power of an odd prime such that $q \equiv 1 \pmod 4$. Any Euclidean self-dual code $\mathcal{C}$ over $GF(q)$ of length $2n$ with minimum weight $d > 2$ is obtained from some Euclidean self-dual code $\mathcal{C}_0$ over $GF(q)$ of length $2n-2$ (up to permutation equivalence) by the construction method in Proposition 2.1.*

Proof. Let G be a generator matrix of $\mathcal{C}$. Without loss of generality we may assume that $G = (I_n \mid A) = (\mathbf{e}_i \mid \mathbf{a}_i)$, where $\mathbf{e}_i$ and $\mathbf{a}_i$ are the rows of I_n (= the identity matrix) and A, respectively for $1 \le i \le n$. It is sufficient to show that there exists a vector $\mathbf{x} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n-2})$ in $GF(q)^{2n-2}$ and a Euclidean self-dual code $\mathcal{C}_0$ over $GF(q)$ of length $2n-2$ whose extended code $\mathcal{C}_1$ (constructed by the method in Proposition 2.1) is equivalent to $\mathcal{C}$.

We note that $\mathbf{a}_i \cdot \mathbf{a}_j = 0$ for $i \ne j$, $1 \le i, j \le n$ and $\mathbf{a}_i \cdot \mathbf{a}_i = -1$ for $1 \le i \le n$ since $\mathcal{C}$ is self-dual. Let c be in $GF(q)$ such that $c^2 = -1$ in $GF(q)$. $\mathcal{C}$ also has the following generator matrix

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

Deleting the first two columns and the second row of G' produces an $(n-1) \times (2n-2)$ matrix

$$G_0 := \left[\begin{array}{ccc|c} 0 & \cdots & 0 & \mathbf{a}_1 - c\mathbf{a}_2 \\ & & & \mathbf{a}_3 \\ & I_{n-2} & & \vdots \\ & & & \mathbf{a}_n \end{array}\right]$$

It is clear that the row space of G_0 has dimension $n-1$ over $GF(q)$. We claim that G_0 is a generator matrix of some Euclidean self-dual code $\mathcal{C}_0$ of length $2n-2$. It suffices to show that any two rows of G_0 are orthogonal to each other. The inner product of the first row of G_0 with itself equals

$$(\mathbf{a}_1 - c\mathbf{a}_2) \cdot (\mathbf{a}_1 - c\mathbf{a}_2) = -(c^2+1) = 0.$$

For $2 \le i \le n-1$, the inner product of the ith row of G_0 with itself equals

$$1 + \mathbf{a}_{i+1} \cdot \mathbf{a}_{i+1} = 0.$$

For $2 \le i \le n-1$, the inner product of the first row of G_0 with the ith row is equal to

$$(\mathbf{a}_1 - c\mathbf{a}_2) \cdot \mathbf{a}_{i+1} = \mathbf{a}_1 \cdot \mathbf{a}_{i+1} - c\mathbf{a}_2 \cdot \mathbf{a}_{i+1} = 0.$$

For $2 \le i, j \le n-1$ with $i \ne j$, the inner product of the ith row with the jth row equals

$$0 + \mathbf{a}_{i+1} \cdot \mathbf{a}_{j+1} = 0.$$

Let $\mathbf{x} = (0, \cdots, 0 \mid \mathbf{a}_1)$ be a row vector of length $2n-2$. Then $\mathbf{x} \cdot \mathbf{x} = \mathbf{a}_1 \cdot \mathbf{a}_1 = -1$ in $GF(q)$. Using the vector $\mathbf{x}$ and the self-dual code $\mathcal{C}_0$, we can construct a self-dual code $\mathcal{C}_1$ with the following generator matrix G_1 by Proposition 2.1. In fact, the $n \times 2n$ matrix

$$G_1 := \left[\begin{array}{cc|cccc}
1 & 0 & 0 & \cdots & 0 & \mathbf{a}_1 \\
\hline
1 & -c & 0 & \cdots & 0 & \mathbf{a}_1 - c\mathbf{a}_2 \\
0 & 0 & & & & \mathbf{a}_3 \\
\vdots & \vdots & & I_{n-2} & & \vdots \\
0 & 0 & & & & \mathbf{a}_n
\end{array}\right]$$

is row equivalent to G.

Hence the given code $\mathcal{C}$ is the same as the code $\mathcal{C}_1$ that is obtained from the code $\mathcal{C}_0$ by the building-up construction in Proposition 2.1. This completes the proof. $\square$

Euclidean self-dual MDS codes of small lengths over prime fields $GF(p)$, $p = 11, 13, 17, 19, 23, 29$, were constructed in [4] and over $GF(31)$ and $GF(37)$ in [18]. We next find some MDS self-dual codes of small lengths for larger fields such as $GF(41), GF(49), GF(53)$ using the building-up construction described above. In order to save space we give a generator matrix of lengths 8 or 10 from which Euclidean self-dual MDS codes of smaller lengths are derived.

Example 2.3. We note that 6 is a primitive element of $GF(41)$. Let us define $c = 6^{\frac{41-1}{4}} = 32$ so that $c^2 = -1$ as in Proposition 2.1. We give a generator matrix G_1^{41} for a Euclidean self-dual MDS $[10, 5, 6]$ code over $GF(41)$.

$$G_1^{41} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 40 & 4 & 40 & 12 \\
36 & 37 & 1 & 0 & 0 & 0 & 1 & 40 & 1 & 18 \\
27 & 38 & 17 & 30 & 1 & 0 & 0 & 1 & 4 & 8 \\
1 & 9 & 5 & 4 & 31 & 33 & 1 & 0 & 1 & 11 \\
28 & 6 & 2 & 18 & 6 & 13 & 16 & 21 & 1 & 32
\end{bmatrix}$$

It has the property that the successive deletion of the first two columns and the first row of G_1^{41} produces Euclidean self-dual MDS codes of lengths $8, 6, 4$, and 2.

For length $n = 12$, we obtain many near MDS Euclidean self-dual $[12, 6, 6]$ codes with distinct weight enumerators. We apply Proposition 2.1 to G_1^{41} with distinct vectors, for example,

$$(14\ 2\ 40\ 1\ 40\ 1\ 0\ 0\ 0\ 0), (27\ 2\ 40\ 1\ 40\ 1\ 0\ 0\ 0\ 0), (10\ 10\ 40\ 1\ 40\ 1\ 0\ 0\ 0\ 0).$$

Each has $A_6 = 880, 960, 720$, respectively.

Example 2.4. Let w be a root of a primitive polynomial x^2+6x+3 in $GF(7)[x]$. Then $c = w^{\frac{q-1}{4}} = w^{12}$. We give a generator matrix G_1^{49} for a Euclidean self-dual MDS $[12, 6, 7]$ code over $GF(49)$ which produces Euclidean self-dual MDS codes of lengths $10, 8, 6, 4$, and 2 by deleting as above.

$$G_1^{49} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 6 & 5 & 5 & w^{20} \\ w^{35} & w^{23} & 1 & 0 & 1 & 1 & 1 & 1 & 1 & w^{10} & w^{19} & w^{9} \\ w^{5} & w^{41} & w^{14} & w^{2} & 1 & 0 & 1 & 1 & 1 & w & w^{17} & w^{3} \\ w^{28} & 2 & w^{34} & w^{22} & w^{3} & w^{39} & 1 & 0 & 1 & 1 & 1 & w^{4} \\ 0 & 0 & 2 & w^{4} & w^{5} & w^{41} & 6 & w^{12} & 1 & 0 & 1 & w^{20} \\ 4 & w^{20} & w^{14} & w^{2} & 4 & w^{20} & w^{30} & w^{18} & 2 & w^{4} & 1 & w^{12} \end{bmatrix}$$

Example 2.5. We note that 2 is a primitive element of $GF(53)$. Hence $c = 30$. We give a generator matrix G_1^{53} of a Euclidean self-dual MDS $[10, 5, 6]$ code over $GF(53)$ which produces Euclidean self-dual MDS codes of lengths $8, 6, 4$, and 2 by deleting as above.

$$G_1^{53} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 52 & 15 & 43 & 34 \\ 30 & 1 & 1 & 0 & 0 & 0 & 1 & 52 & 48 & 48 \\ 16 & 50 & 24 & 22 & 1 & 0 & 0 & 1 & 31 & 16 \\ 36 & 33 & 3 & 16 & 27 & 38 & 1 & 0 & 3 & 19 \\ 32 & 47 & 4 & 39 & 1 & 23 & 10 & 18 & 1 & 30 \end{bmatrix}$$

For length $n = 12$, we find many near MDS Euclidean self-dual codes. We use G_1^{53} with various vectors, for example,

$$(0\ 0\ 0\ 0\ 1\ 52\ 1\ 52\ 1\ 10), (0\ 0\ 0\ 0\ 1\ 52\ 1\ 52\ 1\ 43), (0\ 0\ 0\ 0\ 1\ 52\ 1\ 52\ 7\ 23).$$

Each has $A_6 = 728, 1040, 624$, respectively.

Remark 2.6. More examples of Euclidean self-dual MDS codes over $GF(q)$, where $q \equiv 1 \pmod 4$, $q \geq 61$ will appear elsewhere.

3 Building-up construction for Hermitian self-dual codes

Hermitian self-orthogonal codes over $GF(q^2)$ have been of interest because of their connection to q-ary quantum stabilizer codes [2, Corollary 1]. Hermitian self-dual codes over $GF(4)$ have been well studied since they satisfy the divisibility condition according to the Gleason-Pierce-Ward theorem [39, pp. 857]. Also they are closely related to binary quantum stabilizer codes [7].

In this section we extend the *building-up construction* method [24] for Hermitian self-dual codes over $GF(4)$ to Hermitian self-dual codes over $GF(q^2)$, where q is a power of an odd prime.

We give the *building-up construction* for any Hermitian self-dual codes over $GF(q^2)$ as follows; its proof is straightforward.

Proposition 3.1. *Let $G_0 = (L \mid R) = (\mathbf{l}_i \mid \mathbf{r}_i)$ be a generator matrix (not necessarily in standard form) of a Hermitian self-dual code $\mathcal{C}_0$ over $GF(q^2)$ of length $2n$, where $\mathbf{l}_i$ and $\mathbf{r}_i$ are the rows of the $n \times n$ matrices L and R respectively, for $1 \leq i \leq n$. Let $\mathbf{x} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n})$ be a vector in $GF(q^2)^{2n}$ with $\mathbf{x} * \mathbf{x} = -1$ in $GF(q^2)$. Set $\overline{y_i} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n}) * (\mathbf{l}_i \mid \mathbf{r}_i)$ for $1 \leq i \leq n$, and $c = \zeta^{\frac{q-1}{2}}$ for a primitive (q^2-1)th root of unity ζ in $GF(q^2)$; then $c\overline{c} = -1$. The* *following matrix*

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

then generates a Hermitian self-dual code $\mathcal{C}$ over $GF(q^2)$ of length $2n+2$.

In what follows, we state that every Hermitian self-dual code over $GF(q^2)$ can be constructed by the building-up method given in Proposition 3.1. The proof of this claim is almost the same as that of Proposition 2.2 and is left to the reader.

Proposition 3.2. *Any Hermitian self-dual code $\mathcal{C}$ over $GF(q^2)$ of length $2n$ with minimum weight $d > 2$ is obtained from some Hermitian self-dual code $\mathcal{C}_0$ over $GF(q^2)$ of length $2n-2$ (up to permutation equivalence) by the building-up construction method in Proposition 3.1.*

Example 3.3. We describe our building-up construction for Hermitian self-dual codes over $GF(3^2)$. Let w be a root of the irreducible polynomial x^2+2x+2 in $GF(3)[x]$. Hence w satisfies $w^2 = w+1$. Note that $w\overline{w} = w^4 = -1$. So w is a primitive element of $GF(9)$. We give a generator matrix $G_1^{9,H}$ for a Hermitian self-dual MDS $[6,3,4]$ code. As before, the successive deletion of the first two columns and the first row of $G_1^{9,H}$ produces Hermitian self-dual MDS codes of lengths 4 and 2.

$$G_1^{9,H} = \begin{bmatrix} 1 & 0 & w & 1 & 1 & 1 \\ w & w^6 & 1 & 0 & 1 & 1 \\ w^3 & 1 & w^6 & w^3 & 1 & w \end{bmatrix}.$$

For length 8 we obtain many Hermitian self-dual $[8,4,4]$ codes over $GF(9)$. We use $G_1^{9,H}$ as our base generator matrix with vectors, for example, $(0\ 1\ 1\ 1\ 1\ 1), (w\ w\ 1\ 1\ 1\ 1), (0\ 2\ 1\ 1\ 1\ 1)$. Each of these has distinct weight enumerator

$$W_{8,1} = 1 + 32y^4 + 320y^5 + \cdots, W_{8,2} = 1 + 48y^4 + 256y^5 + \cdots, W_{8,3} = 1 + 96y^4 + 64y^5 + \cdots,$$

respectively. These are near MDS codes.

For length 10 we find many Hermitian self-dual $[10,5,5]$ codes over $GF(9)$. We use the following generator matrix

$$G_2^{9,H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ w^5 & w^2 & 1 & 0 & w & 1 & 1 & 1 \\ w^2 & w^7 & w & w^6 & 1 & 0 & 1 & 1 \\ w^2 & w^7 & w^3 & 1 & w^6 & w^3 & 1 & w \end{bmatrix}$$

with $(w\ w^5\ 1\ w\ 1\ 1\ 1\ 1)$ and $(w^3\ w^5\ 1\ w\ 1\ 1\ 1\ 1)$. The first code has $W_{10,1} = 1+128y^5+1040y^6+\cdots$, and the second code has $W_{10,2} = 1 + 144y^5 + 960y^6 + \cdots$. These are near MDS codes.

Using the following matrix $G_3^{9,H}$ as a base generator matrix with

$$(1\ 2\ w^6\ w^3\ 1\ 1\ 1\ 1\ 1\ 1), (w^6\ w^6\ w^3\ 1\ 1\ 1\ 1\ 1\ 1\ 1), (w^2\ w^7\ w^2\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$$

we get Hermitian self-dual $[12,6,6]$ codes.

$$G_3^{9,H} = \begin{bmatrix} 1 & 0 & w & w^5 & 1 & w & 1 & 1 & 1 & 1 \\ w^5 & w^2 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ w^2 & w^7 & w^5 & w^2 & 1 & 0 & w & 1 & 1 & 1 \\ 1 & w^5 & w^2 & w^7 & w & w^6 & 1 & 0 & 1 & 1 \\ w^3 & 1 & w^2 & w^7 & w^3 & 1 & w^6 & w^3 & 1 & w \end{bmatrix}$$

They have weight enumerators, respectively,

$W_{12,1} = 1+480y^6+3456y^7+\cdots, W_{12,2} = 1+496y^6+3360y^7+\cdots, W_{12,3} = 1+544y^6+3072y^7+\cdots.$

These are near MDS codes.

For length $n = 14$ we find many Hermitian self-dual $[14, 7, 6]$ codes easily. Since its minimum weight is much smaller than the MDS codes, we omit the details.

Example 3.4. Let w be a root of the primitive polynomial $x^2 + 4x + 2$ in $GF(5)[x]$. Let $c := w^{\frac{5-1}{2}}$ be the element defined as in Proposition 3.1. We give a generator matrix $G_1^{25,H}$ for a Hermitian self-dual MDS $[10, 5, 6]$ code over $GF(25)$ as follows which produces Hermitian self-dual MDS codes of lengths $8, 6, 4$, and 2 by deleting as above.

$$G_1^{25,H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & w & w^{13} & 0 \\ w^5 & w^{19} & 1 & 0 & w^{22} & 1 & 1 & 1 & 1 & 1 \\ w^{19} & w^9 & w^3 & w^{17} & 1 & 0 & w^4 & 1 & 1 & 1 \\ 0 & 0 & w^{13} & w^3 & w^{11} & w & 1 & 0 & w^3 & 1 \\ 3 & w^8 & w^3 & w^{17} & 3 & w^8 & w^{19} & w^9 & 1 & w^2 \end{bmatrix}$$

Using $G_1^{25,H}$ and $(1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ w\ w^2)$ we get a Hermitian self-dual near MDS $[12, 6, 6]$ code whose generator matrix has $-y_1 = w^5, cy_1 = w^{19}, -y_2 = w^{10}, cy_2 = 1, -y_3 = w^3, cy_3 = w^{17}, -y_4 = w^{21}, cy_4 = w^{11}, -y_5 = w^{17}, cy_5 = w^7$ using the notation in Proposition 3.1

Example 3.5. Let w be a root of the primitive polynomial $x^2 + 6x + 3$ in $GF(7)[x]$. Let $c := w^{\frac{7-1}{2}}$. We give a generator matrix $G_1^{49,H}$ for a Hermitian self-dual MDS $[12, 6, 7]$ code over $GF(49)$ which produces Hermitian self-dual MDS codes of lengths $10, 8, 6, 4$, and 2 by deleting as above.

$$G_1^{49,H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & w^2 & w^{47} & w^{21} & w^{18} \\ w^5 & 4 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & w & w^9 & w^{27} \\ 3 & w^{35} & w^{31} & w^{10} & 1 & 0 & 1 & 1 & 1 & 1 & w & w^3 \\ w^{30} & w^9 & w^{11} & w^{38} & w^{44} & w^{23} & 1 & 0 & 1 & 1 & 1 & w^7 \\ w^{39} & w^{18} & w^{46} & w^{25} & w^{41} & w^{20} & w^{28} & w^7 & 1 & 0 & 1 & w^5 \\ w^{44} & w^{23} & w^{39} & w^{18} & w^{33} & w^{12} & w^{46} & w^{25} & w^{12} & w^{39} & 1 & w^3 \end{bmatrix}$$

Example 3.6. Let w be a root of the primitive polynomial $x^4 + 2x^3 + 2$ in $GF(3)[x]$. Let $c := w^{\frac{9-1}{2}}$. We give a generator matrix $G_1^{81,H}$ for a Hermitian self-dual MDS $[12, 6, 7]$ code over $GF(81)$ which produces Hermitian self-dual MDS codes of lengths $10, 8, 6, 4$, and 2 by deleting as above..

$$G_1^{81,H} = \begin{bmatrix} 1 & 0 & w^{16} & w^{37} & w & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ w^{78} & w^{42} & 1 & 0 & 1 & 1 & 1 & 1 & 1 & w & 1 & w^{22} \\ w^{68} & w^{32} & w^{68} & w^{32} & 1 & 0 & 1 & 1 & 1 & 1 & w & w^{11} \\ w^{69} & w^{33} & w^{18} & w^{62} & w^{44} & w^8 & 1 & 0 & 1 & 1 & 1 & w^4 \\ w^{66} & w^{30} & w^{69} & w^{33} & w^{33} & w^{77} & w^{67} & w^{31} & 1 & 0 & 1 & 1 \\ w^{56} & w^{20} & w^3 & w^{47} & w^{52} & w^{16} & w^{34} & w^{78} & w^{31} & w^{75} & 1 & w^4 \end{bmatrix}$$

4 Building-up construction for the case of even characteristic

In the sections 2 and 3 we discussed the building-up constructions for the case of odd characteristic. In this section we show that in the case of even characteristic the building-up constructions work for both Euclidean and Hermitian self-dual codes as well.

We begin with the Euclidean self dual codes over $GF(2^m)$ with a positive integer m. We prove that the building-up construction holds for any Euclidean self-dual codes over $GF(2^m)$. The following proposition can be proved in a very similar way as [23, Theorem 1], hence we omit its proof.

Proposition 4.1. *Let $G_0 = (L \mid R) = (\mathbf{l}_i \mid \mathbf{r}_i)$ be a generator matrix (not necessarily in standard form) of a Euclidean self-dual code $\mathcal{C}_0$ over $GF(2^m)$ of length $2n$, where $\mathbf{l}_i$ and $\mathbf{r}_i$ are the rows of the $n \times n$ matrices L and R respectively, for $1 \le i \le n$. Let $\mathbf{x} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n})$ be a vector in $GF(2^m)^{2n}$ with $\mathbf{x} \cdot \mathbf{x} = 1$ in $GF(2^m)$. Set $y_i = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n}) \cdot (\mathbf{l}_i \mid \mathbf{r}_i)$ for $1 \le i \le n$. Then the following matrix*

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

generates a Euclidean self-dual code $\mathcal{C}$ over $GF(2^m)$ of length $2n+2$.

In the following proposition, we state that every Euclidean self-dual code over $GF(2^m)$ can be constructed by the building-up method in Proposition 4.1. The proof is similar to [23, Theorem2] and is omitted.

Proposition 4.2. *Any Euclidean self-dual code $\mathcal{C}$ over $GF(2^m)$ of length $2n$ with minimum weight $d > 2$ is obtained from some Euclidean self-dual code $\mathcal{C}_0$ over $GF(2^m)$ of length $2n-2$ (up to permutation equivalence) by the construction method in Proposition 4.1.*

Similarly we show that the building-up construction method also holds for any Hermitian self-dual codes over $GF(2^m)$.

Proposition 4.3. *Let $G_0 = (L \mid R) = (\mathbf{l}_i \mid \mathbf{r}_i)$ be a generator matrix (not necessarily in standard form) of a Hermitian self-dual code $\mathcal{C}_0$ over $GF(2^m)$ of length $2n$, where $\mathbf{l}_i$ and $\mathbf{r}_i$ are the rows of the $n \times n$ matrices L and R respectively, for $1 \le i \le n$. Let $\mathbf{x} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n})$ be a vector in $GF(2^m)^{2n}$ with $\mathbf{x} * \mathbf{x} = 1$ in $GF(2^m)$. Set $\overline{y_i} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n}) * (\mathbf{l}_i \mid \mathbf{r}_i)$ for $1 \le i \le n$. The following matrix*

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

then generates a Hermitian self-dual code $\mathcal{C}$ over $GF(2^m)$ of length $2n+2$.

Proposition 4.4. *Any Hermitian self-dual code $\mathcal{C}$ over $GF(2^m)$ of length $2n$ with minimum weight $d > 2$ is obtained from some Hermitian self-dual code $\mathcal{C}_0$ over $GF(2^m)$ of length $2n-2$ (up to permutation equivalence) by the construction method in Proposition 4.3.*

Euclidean self-dual codes over $GF(4)$ were studied in [5], [16], [25], and Hermitian self-dual codes over $GF(4)$ were well discussed in [37]. In what follows we give examples of Euclidean or Hermitian self-dual (near) MDS codes over $GF(8)$, $GF(16)$, $GF(32)$, $GF(64)$, or $GF(128)$. In order to save space we start from a generator matrix of lengths $8, 10$ or 12 from which we can derive MDS self-dual codes of smaller lengths.

Example 4.5. We give a generator matrix G_1^8 for a Euclidean self-dual near MDS $[8, 4, 4]$ code over $GF(8)$ below. Its weight enumerator is $A(y) = 1 + 28y^4 + 280y^5 + \cdots$.

$$G_1^8 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & w & w & 0 \\ w^5 & w^5 & 1 & 0 & 1 & w^2 & w & w^4 \\ w^6 & w^6 & w^2 & w^2 & 1 & 0 & w & w^3 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

It has the property that the successive deletion of the first two columns and the first row of G_1^8 produces Euclidean self-dual MDS codes of lengths $6, 4, 2$.

Using G_1^8 and $(1\ 1\ 1\ 1\ w\ w\ w^4\ w^5)$ we get a near MDS Euclidean self-dual $[10, 5, 5]$ code over $GF(8)$.

Example 4.6. We give a generator matrix $G_1^{16,E}$ for a Euclidean self-dual MDS $[8, 4, 5]$ code over $GF(16)$ below.

$$G_1^{16,E} = \begin{bmatrix} 1 & 0 & 1 & 1 & w^3 & 0 & w^6 & w^8 \\ w^7 & w^7 & 1 & 0 & 1 & w^4 & w^{14} & w^9 \\ w^6 & w^6 & w^{13} & w^{13} & 1 & 0 & w & w^4 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

The successive deletion of the first two columns and the first row of $G_1^{16,E}$ produces Euclidean self-dual MDS codes of lengths $6, 4, 2$ as above.

Furthermore using $G_1^{16,E}$ and $(1\ 1\ 1\ 1\ w\ w\ w^2\ w^8)$ we get a near MDS Euclidean self-dual $[10, 5, 5]$ code. Its generator matrix $G_2^{16,E}$ has $y_1 = w^8,\ y_2 = w^4,\ y_3 = w^8,\ y_4 = 1$. Now we use $G_2^{16,E}$ and $(1\ 1\ 1\ 1\ 1\ w\ w\ w\ w\ 0)$ to get a near MDS Euclidean self-dual $[12, 6, 6]$ code.

We can have a similar result for Hermitian self-dual MDS codes over $GF(16)$. The following generator matrix $G_1^{16,H}$ for a Hermitian self-dual near MDS $[8, 4, 4]$ code over $GF(16)$ produces Hermitian self-dual MDS codes of length $6, 4$, and 2 by deleting as above.

$$G_1^{16,H} = \begin{bmatrix} 1 & 0 & w^7 & w^8 & 1 & 1 & 1 & 1 \\ w^6 & w^6 & 1 & 0 & 0 & 1 & 1 & 1 \\ w^2 & w^2 & w^5 & w^5 & 1 & 0 & w^2 & w \\ w^4 & w^4 & w^5 & w^5 & w^5 & w^5 & 1 & 1 \end{bmatrix}$$

A near MDS Hermitian self-dual $[10, 5, 5]$ code over $GF(16)$ is obtained by using $G_1^{16,H}$ and $(0\ 1\ 1\ 1\ 1\ 1\ 1\ 1)$. Its generator matrix $G_2^{16,H}$ has $y_1 = w^{11},\ y_2 = w^6,\ y_3 = w_4,\ y_4 = w_4$. Using $G_2^{16,H}$ and $(0\ w\ 1\ w\ 1\ 1\ 1\ 1\ 1\ 1)$ we get a near MDS Hermitian self-dual $[12, 6, 6]$ code.

Example 4.7. In what follows, we give a generator matrix G_1^{32} for a near MDS Euclidean self-dual $[12, 6, 6]$ code over $GF(32)$. It has the weight enumerator $A(y) = 1 + 930y^6 + 18972y^7 + \cdots$. The successive deletion of the first two columns and the first row gives Euclidean self-dual MDS codes of lengths $10, 8, 6, 4$, and 2.

$$G_1^{32} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & w & w & w & w^3 & w^6 \\ w^{18} & w^{18} & 1 & 0 & 1 & 1 & 1 & w & w & w^2 & w^{18} & w^{11} \\ w^3 & w^3 & w^{30} & w^{30} & 1 & 0 & 1 & 1 & w & w^4 & w & w^{10} \\ w^{26} & w^{26} & w^3 & w^3 & w^4 & w^4 & 1 & 0 & 1 & w^2 & w^9 & w^{24} \\ w^4 & w^4 & w^{10} & w^{10} & w^4 & w^4 & w^{26} & w^{26} & 1 & 0 & w & w^{18} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Example 4.8. The following generator matrix $G_1^{64,E}$ for a near MDS Euclidean self-dual $[10, 5, 5]$ code over $GF(64)$ produces Euclidean self-dual MDS codes of lengths $8, 6, 4$, and 2 by deleting as above. Its weight enumerator is $A(y) = 1 + 378y^5 + 11340y^6 + \cdots$.

$$G_1^{64,E} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & w & w & w^2 & w^{49} \\ w^{20} & w^{20} & 1 & 0 & 1 & 1 & w & w & w^{56} & w \\ w^{32} & w^{32} & w^{44} & w^{44} & 1 & 0 & 1 & w & w^{33} & w^{29} \\ w^{49} & w^{49} & w & w & w^{23} & w^{23} & 1 & 0 & w & w^{56} \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Similarly the following matrix $G_1^{64,H}$ for a near MDS Hermitian self-dual $[12, 6, 6]$ code over $GF(64)$ gives Hermitian self-dual MDS codes of lengths $10, 8, 6, 4$, and 2 by deleting as before. Its weight enumerator is $A(y) = 1 + 630y^6 + 46116y^7 + \cdots$.

$$G_1^{64,H} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ w^{50} & w^{50} & 1 & 0 & w^3 & w & 1 & 1 & 1 & 1 & 1 & 1 \\ w^{41} & w^{41} & w^{59} & w^{59} & 1 & 0 & w^{10} & w & 1 & 1 & 1 & 1 \\ w^{61} & w^{61} & w^{61} & w^{61} & w^{39} & w^{39} & 1 & 0 & 0 & 1 & 1 & 1 \\ w^{40} & w^{40} & w^{43} & w^{43} & w^{18} & w^{18} & w^{50} & w^{50} & 1 & 0 & w^3 & w \\ w^{16} & w^{16} & w^{16} & w^{16} & w^{57} & w^{57} & w^{22} & w^{22} & w^{22} & w^{22} & 1 & 1 \end{bmatrix}$$

Example 4.9. The following generator matrix for a near MDS Euclidean self-dual $[10, 5, 5]$ code over $GF(128)$ produces Euclidean self-dual MDS codes of lengths $8, 6, 4$, and2 by deleting as before.

$$G_1^{128} = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & w & w & w & w^7 \\ w^{15} & w^{15} & 1 & 0 & 1 & 1 & w & w & w^3 & w^{63} \\ w^7 & w^7 & w^{97} & w^{97} & 1 & 0 & 1 & w & w & 0 \\ w^7 & w^7 & w^{63} & w^{63} & w^{14} & w^{14} & 1 & 0 & w & w^7 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Remark 4.10. The building-up construction method given in the sections 2, 3 and 4 can also be used for (Euclidean or Hermitian) self-orthogonal codes.

In Section 2 we discussed Euclidean self-dual codes for the case that $q \equiv 1 \pmod 4$. For the following remarks we assume that q is a power of an odd prime such that $q \equiv 3 \pmod 4$.

Remark 4.11. In the case of $q \equiv 3 \pmod 4$, the necessary and sufficient condition for the existence of Euclidean self-dual codes over $GF(q)$ is the following (for the proof, refer to [30]): There exists a Euclidean self-dual code over $GF(q)$ of length n if and only if $4 \mid n$.

Remark 4.12. For the construction of Euclidean self-orthogonal codes of the maximum dimension over $GF(q)$ with $q \equiv 3 \pmod 4$, we can use a slightly modified version of the building-up construction method in Section 2 as follows. It can be proved in a similar way as in Proposition 2.1.

Let $G_0 = (\mathbf{r}_i)$ be a generator matrix (not necessarily in standard form) of a Euclidean self-dual code $\mathcal{C}_0$ over $GF(q)$ of length $4n$, where $\mathbf{r}_i$ are the row vectors of G_0 for $1 \le i \le 2n$. Take $\mathbf{x} = (x_1, \cdots, x_{2n}, x_{2n+1}, \cdots, x_{4n})$ to be a vector in $GF(q)^{4n}$ with $\mathbf{x} \cdot \mathbf{x} = -1$ in $GF(q)$. Let α and β be in $GF(q)^*$ such that $\alpha^2 + \beta^2 + 1 = 0$ in $GF(q)$; it is a known fact that in a finite field of odd characteristic, every element is the sum of two squares.

Suppose that $y_i := \mathbf{x} \cdot \mathbf{r}_i$ for $1 \le i \le 2n$. Then the following matrix

$$G_1 = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & x_1 & \cdots & x_{4n} \\ \hline -y_1 & \alpha y_1 & \beta y_1 & & & \\ \vdots & \vdots & \vdots & & G_0 & \\ -y_{2n} & \alpha y_{2n} & \beta y_{2n} & & & \end{array}\right]$$

generates a self-orthogonal code $\mathcal{C}$ over $GF(q)$ of length $4n+3$ and dimension $2n+1$.

Remark 4.13. From a given Euclidean self-dual code $\mathcal{C}_0$ over $GF(q)$ of length $4n$ with minimum weight $d > 2$, we can construct a Euclidean self-dual code $\mathcal{C}$ over $GF(q)$ of length $4n-4$ as follows. This is a generalization of "*subtraction*" method [37, pp. 276] for ternary self-dual codes:

Let α and β be as above and G_0 be a generator matrix of $\mathcal{C}_0$. Without loss of generality assume $G = (I_n \mid A) = (\mathbf{e}_i \mid \mathbf{a}_i)$, where $\mathbf{e}_i$ and $\mathbf{a}_i$ are the rows of I_n (= the identity matrix) and A, respectively for $1 \le i \le 2n$. $\mathcal{C}$ also has the following generator matrix

$$G_1 := \left[\begin{array}{c|c} \mathbf{e}_1 + \alpha\mathbf{e}_2 + \beta\mathbf{e}_3 & \mathbf{a}_1 + \alpha\mathbf{a}_2 + \beta\mathbf{a}_3 \\ \mathbf{e}_2 & \mathbf{a}_2 \\ \mathbf{e}_3 & \mathbf{a}_3 \\ \mathbf{e}_4 - \beta\mathbf{e}_2 + \alpha\mathbf{e}_3 & \mathbf{a}_4 - \beta\mathbf{a}_2 + \alpha\mathbf{a}_3 \\ \mathbf{e}_5 & \mathbf{a}_5 \\ \vdots & \vdots \\ \mathbf{e}_{2n+2} & \mathbf{a}_{2n} \end{array}\right]$$

Deleting the second row, the third row and the first four columns of G_1, we get the following $(2n-2) \times (4n-4)$ matrix:

$$G_2 := \left[\begin{array}{ccc|c} 0 & \cdots & 0 & \mathbf{a}_1 + \alpha\mathbf{a}_2 + \beta\mathbf{a}_3 \\ 0 & \cdots & 0 & \mathbf{a}_4 - \beta\mathbf{a}_2 + \alpha\mathbf{a}_3 \\ & & & \mathbf{a}_5 \\ & I_{2n-4} & & \vdots \\ & & & \mathbf{a}_{2n} \end{array}\right]$$

Then it is easy to establish that G_2 generates a self-dual code $\mathcal{C}$ of length $4n-4$.

Remark 4.14. From the examples obtained in this paper, it appears that the main conjecture for $[n,k]$ MDS codes over $GF(q)$ (mentioned in Section 1) is true for self-dual codes.

Acknowledgement We would like to thank Dr. J.L. Walker for proofreading our earlier version and the anonymous referees for their valuable comments.

References

[1] K.T. Arasu and T.A. Gulliver, Self-dual codes over $\mathbb{F}_p$ and weighing matrices, IEEE Trans. Inform. Theory 47 (2001) 2051–2055.

[2] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, IEEE Trans. Inform. Theory 47 (2001) 3065–3072.

[3] E.F. Assmus, Jr. and H.F. Mattson, Jr., New 5-designs, J. Combin. Theory Ser. A 6 (1969) 122–151.

[4] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada, and C. Koukouvinos, On self-dual codes over some prime fields, Discrete Math. 262 (2003) 37–58.

[5] K. Betsumiya, T.A. Gulliver, M. Harada, and A. Munemasa, On type II codes over $\mathbb{F}_4$, IEEE Trans. Inform. Theory 47 (2001) 2242–2248.

[6] R.T. Bilous and G.H.J. van Rees, An enumeration of binary self-dual codes of length 32, Designs, Codes and Cryptography 26 (2002) 61–86.

[7] A.R. Calderbank, E.M. Rains, P.W. Shor, and N.J.A. Sloane, Quantum error correction via codes over $GF(4)$, IEEE Trans. Inform. Theory 44 (1998) 1369–1387.

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

[9] J.H. Conway and V. Pless, On the enumeration of self-dual codes, J. Combin. Theory Ser. A 28 (1980) 26–53.

[10] J.H. Conway, V. Pless, and N.J.A. Sloane, Self-dual codes over $GF(3)$ and $GF(4)$ of length not exceeding 16, IEEE Trans. Inform. Theory 25 (1979) 312–322.

[11] J.H. Conway, V. Pless, and N.J.A. Sloane, The binary self-dual codes of length up to 32: A revised enumeration, J. Combin. Theory Ser. A 60 (1992) 183–195.

[12] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, IEEE Trans. Inform. Theory 36 (1990) 1319–1333.

[13] M.A. De Boer, Almost MDS codes, Designs, Codes and Cryptography 9 (1996) 143–155.

[14] S. Dodunekov and I.N. Landjev, On near-MDS codes, J. Geom. 54 (1995) no. 1-2, 30-43.

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

[16] P. Gaborit, V. Pless, P. Solé, and O. Atkin, Type II codes over $\mathbb{F}_4$, Finite Felds Appl. 8 (2002) 171–183.

[17] S. Georgiou and C. Koukouvinos, Self-dual codes over $GF(7)$ and orthogonal designs, Utilitas Math. 60 (2001) 79–89.

[18] S. Georgiou and C. Koukouvinos, MDS self-dual codes over large prime fields, Finite Fields and Their Appl. 8 (2002) 455–470.

[19] T.A. Gulliver and M. Harada, New optimal self-dual codes over $GF(7)$, Graphs and Combin. 15 (1999) 175–186.

[20] W.C. Huffman, On extremal self-dual quaternary codes of lengths 18 to 28, I, IEEE Trans. Inform. Theory 36 (1990) 651–660.

[21] W.C. Huffman, On extremal self-dual quaternary codes of lengths 18 to 28, II, IEEE Trans. Inform. Theory 37 (1991) 1206–1216.

[22] W.C. Huffman, Characterization of quaternary extremal codes of lengths 18 and 20, IEEE Trans. Inform. Theory 43 (1997) 1613–1616.

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

[24] J.-L. Kim, New self-dual codes over GF(4) with the highest known minimum weights, IEEE Trans. Inform. Theory 47 (2001) 1575–1580.

[25] D.K. Kim, H.K. Kim. and J.-L. Kim, Euclidean type I codes over $GF(4)$, preprint.

[26] J.S. Leon, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(5)$, J. Combin. Theory Ser. A 32 (1982) 178–194.

[27] F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane and H.N. Ward, Self-dual codes over $GF(4)$, J. Combin. Theory Ser. A 25 (1978) 288–318.

[28] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

[29] C.L. Mallows, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$, SIAM J. Appl. Math. 31 (1976) 649–666.

[30] V. Pless, The number of isotropic subspaces in a finite geometry, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 39 (1965) 418–421.

[31] V. Pless, A classification of self-orthogonal codes over $GF(2)$, Discrete Math. 3 (1972) 209–246.

[32] V.S. Pless, W.C. Huffman and R.A. Brualdi, An introduction to algebraic codes, in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, Eds. Amsterdam. The Netherlands: Elsevier, 1998.

[33] V. Pless and J.N. Pierce, Self-dual codes over $GF(q)$ satisfy a modified Varshamov-Gilbert bound, Inform. and Control 23 (1973) 35–40.

[34] V. Pless and N.J.A. Sloane, On the classification and enumeration of self-dual codes, J. Combin. Theory Ser. A 18 (1975) 313–335.

[35] V. Pless, N.J.A. Sloane and H.N. Ward, Ternary codes of minimum weight 6 and the classification of self-dual codes of length 20, IEEE Trans. Inform. Theory 26 (1980) 305–316.

[36] V. Pless and V.D. Tonchev, Self-dual codes over $GF(7)$, IEEE Trans. Inform. Theory 33 (1987) 723–727.

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

[38] N.J.A. Sloane, Self-dual codes and lattices, Relations Between Combinatorics and Other Parts of Mathematics, Proc. Symp. Pure Math. vol 34, Amer. Math. Soc., Providence, RI (1979) 273–308.

[39] H.N. Ward, Quadratic residue codes and divisibility, in Handbook of Coding Theory, V. S. Pless and W. C. Huffman, Eds. Amsterdam. The Netherlands: Elsevier, 1998.