New Hermitian Self-Dual MDS or Near-MDS Codes over Finite Fields

Djoko Suprijanto[1,2], Yudi Renata[2] & Mustika Ladia Putri[2]

[1]Combinatorial Mathematics Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jalan Ganesha 10, Bandung 40132, Indonesia
[2]Department of Mathematics, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Jalan Ganesha 10, Bandung 40132, Indonesia
Email: djoko@math.itb.ac.id

Abstract. A linear code over a finite field is called Hermitian self-dual if the code is self-dual under the Hermitian inner-product. The Hermitian self-dual code is called MDS or near-MDS if the code attains or almost attains the Singleton bound. In this paper we construct new Hermitian self-dual MDS or near-MDS codes over $GF(9)$, $GF(25)$, and $GF(121)$ of length up to 14.

Keywords: *decoding error probability performance; Hermitian self-dual codes; lexicographical ordering; MDS codes; near-MDS codes.*

1 Introduction

A *linear* $[n,k]$ code C over $GF(q)$ is a k -dimensional subspace of $GF(q)^n$, where $GF(q)$ is the Galois field with q elements. The value n is called *length* of C and every element of C is called *codeword* of C. The *weight* $wt(c)$ of a codeword $c \in C$ is the number of nonzero components of c. The minimum weight d of all nonzero codewords in C is called *minimum weight* of C. An $[n,k,d]$ code is an $[n,k]$ code with minimum weight d. The weight enumerator W of C is given by

$$W(y) = \sum_{k=0}^{n} A_k y^k,$$

where A_k denotes the number of codewords of weight k in C.

The space $GF(q)^n$ is equipped by Hermitian inner-product defined by

$$[x,y] = \sum_{k=1}^{n} x_k \overline{y_k},$$

Received August 1st, 2013, 1st Revision February 5th, 2014, 2nd Revision March25th, 2014, Accepted for publication March 26th, 2014.
Copyright © 2014 Published by ITB Journal Publisher, ISSN: 2337-5760, DOI: 10.5614/j.math.fund.sci.2014.46.1.6

for two vectors $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in $GF(q)^n$, where $\overline{y_k} = y_k{}^{\sqrt{q}}$, and $q = p^m$, for a prime number p and an even m.

The *Hermitian dual code* $C^{\perp}$ of C is defined as

$$C^{\perp} = \left\{ x \in GF(q)^n : [x, c] = 0, \forall c \in \mathrm{C} \right\}.$$

A code C is called *Hermitian self-dual* if $C = C^{\perp}$. From now on, what we mean by self-dual is Hermitian self-dual.

A linear $[n, k, d]$ code over $GF(q)$ satisfies the Singleton bound $d \le n - k + 1$ (see, e.g., [1]). If the equality is attained then the code is called *MDS code*. The $[n, k, n-k]$ code is called *almost MDS code* [2]. An $[n, k, n-k]$ almost MDS code for which the dual code is also an almost MDS is called *near-MDS code* [3].

MDS codes are important in Mathematics since they are equivalent to geometric objects called *n-arcs* [1, p. 326] and also to combinatorial objects called *orthogonal arrays* [1, p. 326]. Moreover, very recently, Dodunekov [4] and Zhou, *et al.* [5] announced the importance of self-dual near-MDS codes in Cryptography, in particular in secret sharing schemes. Hence there is a great interest in the construction of MDS or near-MDS self-dual codes over finite fields (see, e.g., [6-10]).

Kim and his co-authors ([8,10]) used a construction method, called *the building-up method*, to construct self-dual MDS or near-MDS codes. They also showed that every self-dual codes over certain fields can be obtained by their building-up method. In particular, [8] provided three examples, one example, of self-dual near-MDS codes of length 12 over $GF(9)$, $GF(25)$, respectively. Recently, Gulliver, *et al.* [10] gave an example of self-dual MDS code of length 14 and stated that they also found many self-dual near-MDS codes of length 16 over $GF(121)$. From the generator matrix of self-dual near-MDS of length 14 above, they [10] found one self-dual MDS code of length 12, 10, 8, 6, 4, and 2, respectively.

The purpose of this paper is to provide some more examples of MDS or near-MDS self-dual codes. We obtained several new MDS or near-MDS self-dual codes of length 10 and 12 over $GF(9)$, 10, 12, and 14 over $GF(25)$, and 4, 6, 8, and 10 over the field $GF(121)$ which were unknown to exist before.

2 Construction Method

We use the following building-up construction given in [8].

Theorem 2.1 Let $G_0 = (L \mid R) = (l_i \mid r_i)$ be a generator matrix of a self-dual code C_0 over $GF(q^2)$ of length $2n,$ where l_i and r_i are the rows of the matrices L and R respectively, for $1 \le i \le n.$ Let $x = (x_1, ..., x_n, x_{n+1}, ..., x_{2n})$ be a vector in $GF(q^2)^{2n}$ with $[x, x] = -1$ in $GF(q^2).$ Set $\overline{y_i} = [(x_1, ..., x_n, x_{n+1}, ..., x_{2n}), (l_i \mid r_i)]$ for $1 \le i \le n,$ and $c = \zeta^{\frac{q-1}{2}}$ for $(q^2 - 1)$-th root of unity ζ in $GF(q^2)$ (and hence $c\bar{c} = -1$). Then the matrix

$$\begin{pmatrix} 1 & 0 & x_1 & \cdots & x_n & x_{n+1} & \cdots & x_{2n} \\ -y_1 & cy_1 & & & & & & \\ \vdots & \vdots & & L & & & R & \\ -y_n & cy_n & & & & & & \end{pmatrix}$$

generates a self-dual code C over $GF(q^2)$ of length $2n + 2.$

The key point of the above theorem in constructing new self-dual codes is to supply generator matrices of self-dual codes of length 2 shorter than the length of codes we want to construct. The more we supply generator matrices of length $2n$ the bigger the chance to obtain new codes of length $2n + 2.$

Let C be a self-dual code of length $2n + 2,$ and let G be its generator matrix. Without loss of generality we may assume that $G = (I_n \mid A) = (e_i \mid a_i),$ where e_i and a_i are the rows of the identity matrix I_n and $A,$ respectively for $1 \le i \le n.$ Let c be in $GF(q)$ such that $c^2 = -1$ in $GF(q).$ Then C has also the following generator matrix

$$G' := \begin{pmatrix} e_1 - ce_2 & \mid & a_1 - ca_2 \\ -ce_2 & \mid & -ca_2 \\ e_3 & \mid & a_3 \\ \vdots & \mid & \vdots \\ e_n & \mid & a_n \end{pmatrix}.$$

Deleting the first two columns and the second row of $G^{'}$ we obtain an $(n-1)\times 2n$ matrix of the form

$$G_0 := \begin{pmatrix} 0 & \cdots & 0 & | & a_1 - ca_2 \\ & & & | & a_3 \\ & I_{n-2} & & | & \vdots \\ & & & | & a_n \end{pmatrix}.$$

We claim that G_0 is a generator matrix of some self-dual code C_0 of length $2n.$ 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

$$[a_1 - ca_2, a_1 - ca_2] = -(c^2+1) = 0.$$

For $3 \le i \le n,$ the inner-product of the *i*-th row of G_0 with itself equals

$$1 + [a_i, a_i] = 0.$$

For $3 \le i \le n,$ the inner-product of the first row of G_0 with the *i*-th row is equal to

$$[a_1 - ca_2, a_i] = [a_1, a_i] - [ca_2, a_i] = 0.$$

For $3 \le i, j \le n,$ with $i \ne j,$ the inner-product of the *i*-th row with the *j*-th row is equal to

$$0 + [a_i, a_j] = 0.$$

Hence we have the following proposition.

Proposition 2.2 Let $G = (I_n \mid A) = (e_i \mid a_i),$ where e_i and a_i are the rows of the identity matrix I_n and $A,$ respectively for $1 \le i \le n,$ be a generator matrix of a self-dual code C of length $2n+2.$ Then

$$G_0 := \begin{pmatrix} 0 & \cdots & 0 & | & a_1 - ca_2 \\ & & & | & a_3 \\ & I_{n-2} & & | & \vdots \\ & & & | & a_n \end{pmatrix}$$

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

Remark 2.3 Proposition 2.2 above is nothing but the restatement of Proposition 3.2 in [8].

2.1 Construction Algorithm

The method we use here to construct new codes is a combination of subtraction method and building-up method. Subtraction as well as building-up construction method are well known in Coding Theory. Kim's method (Theorem 2.1) is basically a building-up method: it is possible to construct a self-dual $[2n+2, n+1, d+2]$ code from a self-dual $[2n, n, \geq d]$ code. Subtraction method (Proposition 2.2) is a reverse of the building-up method: it is possible to construct a self-dual $[2n, n, \geq d]$ code from a self-dual $[2n+2, n+1, d+2]$ code.

Our key step to create new codes is to supply known generator matrices G_0 of self-dual $[2n, n, \geq d]$ codes as many as possible, and to use all possible vectors $x \in GF(q^2)$, for each matrix G_0. The algorithm is given in the Table 1 (c.f. [11]).

Table 1 An algorithm to construct MDS or near-MDS self-dual codes by combination of building-up and subtraction method.

Input: C'_{2n+2}, a known $[2n+2, n+1, d]$ self-dual code (not necessarily (near-) MDS).

Output: C_{2n+2}, the set of new $[2n+2, n+1, d]$ self-dual codes, with $d = n$ or $n+1$.

1. Construct a self-dual $[2n, n, d]$ code $C_{2n,1}$ from a given self-dual $[2n+2, n+1, d]$ code C'_{2n+2} by subtraction method (Proposition 2.2).
2. Construct self-dual $[2n+2, n+1, d]$ codes C_{2n+2} from a self-dual $[2n, n, d]$ code $C_{2n,1}$ by the building-up method (Theorem 2.1). Supply all possible values for vector x.
3. Check the equivalence of new self-dual codes C_{2n+2} from Step 2. Let say, we get l inequivalent self-dual $[2n+2, n+1, d]$ codes $C_{2n+2,1}, C_{2n+2,2}, \ldots, C_{2n+2,l}$.
4. For each self-dual code obtained in Step 3, return to Step 1. Denote a new self-dual $[2n, n, d]$ code by $C_{2n,2}$.

3 Results

In this section, we apply the above method to construct some new Hermitian self-dual MDS or near-MDS codes over $GF(9)$, $GF(25)$, and $GF(121)$. All computer calculations were done by MAGMA [12] and MATLAB.

3.1 Self-dual Near-MDS Codes Over $GF(9)$

Let w be a root of a primitive polynomial $x^2+2x+2 \in GF(3)[x]$ and $c := w^2$ be the element defined as in Theorem 2.1.

3.2 Length 10

Kim and Lee [8] constructed a self-dual near-MDS $[10,5,5]$ with the following generator matrix

$$\begin{pmatrix} 1 & 0 & w & w^5 & 1 & w & 1 & 1 & 1 & 1 \\ w^5 & w^2 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ w^2 & w^7 & w^5 & w^2 & 1 & 0 & w & 1 & 1 & 1 \\ 1 & w^5 & w^2 & w^7 & w & w^6 & 1 & 0 & 1 & 1 \\ w^3 & 1 & w^2 & w^7 & w^3 & 1 & w^6 & w^3 & 1 & w \end{pmatrix}.$$

By the building-up method (Theorem 2.1) continues with the subtraction method (Proposition 2.2), we obtained three self-dual near-MDS $[10,5,5]$ with generator matrices given below:

$$C_{10,1} = \begin{pmatrix} 0 & 0 & 0 & 0 & w^4 & w^3 & w & w^2 & w^2 & w \\ 1 & 0 & 0 & 0 & w^5 & w^6 & w & w^4 & 0 & w^5 \\ 0 & 1 & 0 & 0 & w^4 & 1 & w^3 & w^7 & w^2 & w^4 \\ 0 & 0 & 1 & 0 & w^7 & w^3 & w^3 & 1 & w^6 & 0 \\ 0 & 0 & 0 & 1 & w^4 & w & w & w & w & w^5 \end{pmatrix},$$

$$C_{10,2} = \begin{pmatrix} 0 & 0 & 0 & 0 & w^4 & w^3 & w & w^2 & w^2 & w \\ 1 & 0 & 0 & 0 & 1 & w^4 & w^6 & 0 & 1 & w^4 \\ 0 & 1 & 0 & 0 & w^2 & w^5 & w^5 & w^4 & 1 & 1 \\ 0 & 0 & 1 & 0 & w^3 & w & w^5 & w^3 & w^7 & w^4 \\ 0 & 0 & 0 & 1 & w^4 & w & w & w & w & w^5 \end{pmatrix},$$

and

$$C_{10,3} = \begin{pmatrix} 0 & 0 & 0 & 0 & w^4 & w^3 & w & w^2 & w^2 & w \\ 1 & 0 & 0 & 0 & w^2 & 0 & w^2 & w^7 & w & w^3 \\ 0 & 1 & 0 & 0 & w^5 & w^7 & w^6 & w^6 & w^3 & 0 \\ 0 & 0 & 1 & 0 & w^5 & 1 & 0 & w^4 & w^5 & w^7 \\ 0 & 0 & 0 & 1 & w^5 & w^3 & w^2 & w^5 & w^5 & w^3 \end{pmatrix}.$$

Weight enumerator of the above codes is $W_{10,1}(y) = W_{10,2}(y)$ $= 1+128y^5+1040y^6+\cdots$, and $W_{10,3}(y) = 1+160y^5+952y^6+\cdots$, respectively.

Since the two self-dual near-MDS [10,5,5] codes constructed by Kim and Lee [7] has weight enumerator $W(y)=1+128y^5+1040y^6+4160y^7+\cdots$ and $W(y)=1+144y^5+960y^6+\cdots$, respectively, then we obtained at least one new self-dual near-MDS $[10,5,5]$ code, namely the code $C_{10,3}$.

3.3 Length 12

Kim and Lee [8] have constructed three self-dual near-MDS $[12,6,6]$ codes. From the above near-MDS $[10,5,5]$ codes, we applied the building-up method (Theorem 2.1) to construct self-dual codes of length 12. We obtained 9 self-dual near-MDS $[12,6,6]$ codes which are not equivalent with the ones constructed by Kim and Lee [8] (see Table 2).

Table 2 Self-dual near-MDS [12,6,6] codes over *GF(9)*.

No	Vector x in Generator Matrix	A_6, A_7
1	$(w^7,w^7,w^7,w^7,w^7,w^5,0,w^5,w^5,w^6)$	480, 3456
2	$(w^7,w^7,w^7,w^7,w^7,w^6,w^3,w^5,0,w^5)$	480, 3456
3	$(w^7,w^7,w^7,w^7,w^7,w^6,w^6,w^4,0,1)$	496, 3360
4	$(w^7,w^7,w^7,w^7,w^7,w^6,w^4,w^6,w^4,0)$	544, 3072
5	$(w^7,w^7,w^7,w^7,w^7,w^6,w^4,1,w^4,0)$	544, 3072
6	$(w^7,w^7,w^7,w^7,w^7,w^4,w^6,w^6,w,w^3)$	544, 3072
7	$(w^7,w^7,w^7,w^7,w^7,w^7,w^7,w^3,0,w^4)$	624, 2592
8	$(w^7,w^7,w^7,w^7,w^7,w^6,0,w,w^7,w^5)$	624, 2592
9	$(w^7,w^7,w^7,w^7,w^7,w^2,w^6,w,w^6,w^5)$	736, 1920

3.4 Self-dual MDS or Near-MDS Codes Over $GF(25)$

Let w be a root of primitive polynomial $x^2+4x+2\in GF(25)[x]$ and $c:=w^2$ be the element defined as in Theorem 2.1.

3.4.1 Length 10

First, the [8] provided a self-dual MDS [10,5,6] code $C_{10}^{'}$:

$$C_{10}^{'}=\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 1 & w & w^{13} & 0 \\ w^5 & w^{19} & 1 & 0 & w^{22} & 1 & 1 & 1 & 1 & 1 \\ w^{19} & w^9 & w^3 & w^{17} & 1 & 0 & w^4 & 1 & 1 & 1 \\ 0 & 0 & w^{13} & w^3 & w^{11} & w & 1 & 0 & w^3 & 1 \\ w^{18} & w^8 & w^3 & w^{17} & w^{18} & w^8 & w^{19} & w^9 & 1 & w^2 \end{pmatrix}.$$

By subtraction method (Proposition 2.2) we obtained a self-dual [8,4] code C_8 :

$$C_8 = \begin{pmatrix} 0 & 0 & 0 & w^2 & w^{10} & w^{21} & w^{17} & w^7 \\ 1 & 0 & 0 & w^{10} & 1 & w & w^{22} & w^3 \\ 0 & 1 & 0 & w^9 & w^{13} & w & w^{16} & w^5 \\ 0 & 0 & 1 & w^{16} & w^5 & w^{18} & w^{22} & w^{19} \end{pmatrix}.$$

Next, by the building-up method (Theorem 2.1) we obtained 13 new (inequivalent) self-dual MDS [10,5,6] codes with the same weight enumerator

$$W(y) = 1 + 5040y^6 + 54720y^7 + 508680y^8 + 2704560y^9 + 6492624y^{10}.$$

The (generator of) new codes are listed in the Table 3 below.

Table 3 Self-dual MDS [10,5,6] codes over *GF(25).*

No	Vector x in Generator Matrix
1	$(1,1,1,1,1,w^7,w^{22},w^{21})$
2	$(1,1,1,1,1,w^{15},w^5,w^2)$
3	$(1,1,1,1,1,w^{17},w^{16},w^{16})$
4	$(1,1,1,1,1,w^{20},w^{13},w^{12})$
5	$(1,1,1,1,w,1,w^{13},0)$
6	$(1,1,1,1,w,w,0,w^4)$
7	$(1,1,1,1,w,w^{14},w^{22},0)$
8	$(1,1,1,1,w,w^{15},w^{20},w^2)$
9	$(1,1,1,1,w,w^{17},1,0)$
10	$(1,1,1,1,w^2,w^{13},w^{19},w^{20})$
11	$(1,1,1,1,w^3,1,w^{20},0)$
12	$(1,1,1,1,w^4,w^8,w^2,w^{10})$
13	$(1,1,1,1,w^5,w^6,w^{11},w^{20})$

Moreover, we also obtained over 30 (inequivalent) near-MDS [10,5,5] codes, some of them are given in Table 4 below.

Table 4 Self-dual near-MDS [10,5,5] codes over *GF(25)*

No	Vector x in Generator Matrix	A_5, A_6, A_7
1	$(0,0,0,0,w,w^6,w,w^{12})$	48, 4800, 55200
2	$(0,0,0,0,1,1,w^4,1)$	96, 4560, 55680
3	$(0,0,0,0,1,1,1,w^{12})$	144, 4320, 56160
4	$(0,0,0,0,1,1,1,w^8)$	192, 4080, 56640
5	$(0,0,0,0,1,1,w^2,w^{23})$	240, 3840, 57120
6	$(0,0,0,0,1,1,w^6,w^3)$	288, 3600, 57600
7	$(0,0,0,0,1,1,,w^7,w^{14})$	336, 3360, 58080

3.4.2 Length 12

For length 12, we obtained many (inequivalent) self-dual near-MDS codes. Some of them are listed below.

Table 5 Self-dual near-MDS [12,6,6] codes over *GF(25)*.

No	Vector x in Generator Matrix	A_6, A_7
1	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{14},w^{9},w^{17},w^{22})$	456, 16272
2	$(1,1,1,1,1,1,w,w^{13},w^{19},w^{20})$	480, 16128
3	$(w^{4},w^{4},w^{4},w^{4},w^{4},w^{4},w^{4},w^{11},w^{15},1)$	504, 15984
4	$(1,1,1,1,1,1,w,w^{15},w,w^{16})$	528, 15840
5	$(w^{4},w^{4},w^{4},w^{4},w^{4},w^{12},w^{13},w^{15},w^{3},0)$	552, 15696
6	$(w^{4},w^{4},w^{4},w^{4},w^{4},w^{12},w^{14},w^{13},1,1)$	600, 15408
7	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{16})$	624, 15264
8	$(w^{4},w^{4},w^{4},w^{4},w^{4},w^{12},w^{14},w^{13},0,w^{21})$	648, 15120
9	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{17},w^{12})$	672, 14976
10	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{2},w)$	696, 15432
11	$(1,1,1,1,1,w^{2},w^{8},w^{19},w^{8},0)$	720, 14688
12	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{13},w^{2})$	744, 15144
13	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{23},w^{20},w^{5},w^{18})$	768, 14400
14	$(1,1,1,1,1,w^{7},w^{17},w,w^{12},w^{20})$	792, 14856
15	$(w^{19},w^{19},w^{19},w^{19},w^{19},w^{23},w^{17},w^{12},w^{4},w^{19})$	816, 14112
16	$(1,1,1,1,1,w^{7},w^{17},w^{2},w^{3},w^{9})$	840, 14568
17	$(1,1,1,1,1,1,1,1,w^{2},w^{17})$	864, 13824
18	$(1,1,1,1,1,w^{7},w^{17},w^{2},w^{3},w^{21})$	888, 14280
19	$(1,1,1,1,1,1,1,1,w^{16},0)$	912, 13536
20	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{15},w^{5},w^{18})$	936, 13992
21	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{20},w^{17})$	960, 13248
22	$(1,1,1,1,1,w^{7},w^{17},w^{4},w^{21},w^{20})$	984, 14904
23	$(w^{4},w^{4},w^{4},w^{4},w^{4},w^{12},w^{14},w^{15},w^{18},w^{17})$	1004, 14184
24	$(w^{19},w^{19},w^{19},w^{19},w^{19},w^{19},w^{20},0,w^{8},w^{22})$	1008, 12960
25	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{18},w^{2},w^{21})$	1032, 14016
26	$(w^{19},w^{19},w^{19},w^{19},w^{19},w^{23},w^{17},w^{15},w^{15},w^{3})$	1056, 12672
27	$(1,1,1,1,1,w^{7},w^{19},w^{8},w^{20},w^{16})$	1080, 13728
28	$(1,1,1,1,1,1,1,w^{21},w^{12},w^{14})$	1104, 12384
29	$(1,1,1,1,1,1,1,w^{16},w^{15},w^{11})$	1152, 12096
30	$(1,1,1,1,1,w^{8},w^{14},w^{23},w^{21},w^{2})$	1200, 11808

3.4.3 Length 14

Again, from self-dual codes of length 12, by the building-up method, we obtained over 20 (inequivalent) self-dual near-MDS [14,7,7] codes. The codes as well as their weight enumerators are listed below.

Table 6 Self-dual near-MDS [14,7,7] codes over *GF(25)*.

No	vector x in generator matrix	$A_7,\ A_8$
1	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{23},w^{13},w^{4},w^{9})$	1920, 58632
2	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},1,w^{17},w^{21},1)$	1968, 58296
3	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{17},w^{18},w^{20},w^{4})$	2016, 57960
4	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{15},w^{18},w^{13},w^{2})$	2064, 57624
5	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{15},w^{3},w^{8},w^{4})$	2112, 57288
6	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{15},1,w^{12},w^{7})$	2160, 56952
7	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{16},w^{17},1)$	2208, 56616
8	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{15},w^{22},w^{21})$	2256, 56280
9	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{14},w^{23},w^{21})$	2304, 55944
10	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{14},w^{10},1)$	2352, 55608
11	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{14},w^{8},w^{2})$	2400, 55272
12	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{10},w^{6},w^{8})$	2448, 54936
13	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{6},w^{9},w^{7})$	2496, 54600
14	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{1},w^{11},w^{6})$	2544, 54264
15	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},1,w^{8},w^{9})$	2592, 53928
16	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{20},w^{14},w^{4})$	2640, 53592
17	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{16},w^{7})$	2688, 53256
18	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{14},w^{19},w^{14},w^{21})$	2544, 54264
19	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{15},w,w^{21},w^{8})$	2784, 52584
20	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{15},w^{13},w^{6},w^{18})$	2832, 52248
21	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{17},w^{3},w^{17},w^{8})$	2880, 51912
22	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{19},w,w^{4},w^{17})$	2928, 51576
23	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{20},w^{12},w^{15},w^{23})$	2976, 51240
24	$(w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{13},w^{17},w^{3},w^{9},w^{20})$	3024, 50904

3.5 Self-dual MDS or Near-MDS Codes Over $GF(121)$

Let w be a root of primitive polynomal $x^2+5x+2 \in GF(121)[x]$ and $c := w^2$ be the element defined in Theorem 2.1.

3.5.1 Length 4

From a self-dual code $(1\ w^5)$ of length 2, by the building-up method, we obtained a self-dual MDS [4,2,3] code

$$\begin{pmatrix} 1 & 0 & 1 & w^6 \\ w^{33} & w^{98} & 1 & w^5 \end{pmatrix}$$

having weight enumerator $1+480y^3+14160y^4$. We also obtained a self-dual near-MDS [4,2,2] code

$$\begin{pmatrix} 1 & 0 & 0 & w^{5} \\ 1 & w^{65} & 1 & w^{5} \end{pmatrix}$$

having weight enumerator $1+240y^{3}+14400y^{4}$.

3.5.2 Length 6

From the above MDS code, again by the building-up method, we obtained three (inequivalent) self-dual MDS [6,3,4] codes with the same weight enumerator $1+1800y^{4}+84240y^{5}+1685520y^{6}$.

Table 7 Self-dual MDS [6,3,4] codes over *GF(121).*

No	Vector x in Generator Matrix
1	$(0,1,1,w^{3})$
2	$(0,1,1,w^{43})$
3	$(0,1,1,w^{63})$

We also obtained several (inequivalent) self-dual near-MDS [6,3,3] codes as given below.

Table 8 Self-dual near-MDS [6,3,3] codes over *GF(121).*

No	Vector x in Generator Matrix	A_3, A_4, A_5, A_6
1	$(0,0,1,w^{16})$	120, 1440, 84600, 1685400
2	$(0,0,w,w^{53})$	240, 1080, 84960, 168580
3	$(0,0,w^{6},1)$	480, 14880, 56640, 1699560
4	$(0,1,w^{31},w^{47})$	600, 14520, 57000, 1699440

3.5.3 Length 8

Again, from self-dual codes of length 6, by the building-up method, we obtained a self-dual MDS [8,4,5] code

$$\begin{pmatrix} 1 & 0 & w^{9} & w^{9} & w^{9} & w^{9} & w^{9} & w^{11} \\ w^{37} & w^{102} & 1 & 0 & 0 & 1 & 1 & w^{3} \\ w^{7} & w^{72} & w^{69} & w^{14} & 1 & 0 & 1 & w^{6} \\ w^{69} & w^{14} & w^{60} & w^{5} & w^{33} & w^{98} & 1 & w^{5} \end{pmatrix}$$

having weight enumerator

$$W(y)=1+6720y^{5}+389760y^{6}+13372800y^{7}+200589600y^{8}.$$

There are also several (inequivalent) self-dual near-MDS [8,4,4] codes as given below.

Table 9 Self-dual near-MDS [8,4,4] codes over *GF(121)*.

No	Vector x in Generator Matrix	A_4, A_5, A_6
1	$(w^9, w^9, w^9, w^9, w^9, w^{41})$	240, 5760, 391200
2	$(w^9, w^9, w^9, w^9, w^{10}, w^{27})$	480, 4800, 392640
3	$(w^9, w^9, w^9, w^{13}, w^{85}, w^{87})$	720, 3840, 394080
4	$(w^9, w^9, w^9, w^{12}, w^{110}, w^{26})$	960, 2880, 395520
5	$(w^9, w^9, w^9, w^{11}, w^{25}, w^{41})$	1200, 1920, 396960

3.5.4 Length 10

From self-dual codes of length 8, by the building-up method, we obtained a self-dual MDS [10,5,6] code

$$\begin{pmatrix} 1 & 0 & w^{29} & w^{29} & w^{29} & w^{29} & w^{29} & w^{34} & w^{100} & w^{97} \\ w^{69} & w^{14} & 1 & 0 & w^{9} & w^{9} & w^{9} & w^{9} & w^{9} & w^{11} \\ w^{100} & w^{45} & w^{37} & w^{102} & 1 & 0 & 0 & 1 & 1 & w^{3} \\ w^{88} & w^{33} & w^{7} & w^{72} & w^{69} & w^{14} & 1 & 0 & 1 & w^{6} \\ w^{14} & w^{79} & w^{69} & w^{14} & w^{60} & w^{5} & w^{33} & w^{98} & 1 & w^{5} \end{pmatrix}$$

with weight enumerator

$$W(\mathrm{y}) = 1 + 25200\,\mathrm{y}^6 + 1656000 y^7 + 74601000 y^8 + \cdots.$$

There are also several (inequivalent) self-dual near-MDS codes as given below.

Table 10 Self-dual near-MDS [10,5,5] codes over *GF(121)*.

No	Vector x in Generator Matrix	A_5, A_6, A_7
1	$(w^{29}, w^{29}, w^{29}, w^{29}, w^{29}, w^{34}, w^{100}, w^{77})$	240, 24000, 1658400
2	$(w^{29}, w^{29}, w^{29}, w^{29}, w^{29}, w^{34}, w^{100}, w^{87})$	480, 22800, 1660800
3	$(w^{29}, w^{29}, w^{29}, w^{29}, w^{29}, w^{34}, w^{101}, w^{39})$	720, 21600, 1663200
4	$(w^{29}, w^{29}, w^{29}, w^{29}, w^{29}, w^{34}, w^{100}, w^{79})$	960, 20400, 1665600
5	$(w^{29}, w^{29}, w^{29}, w^{29}, w^{29}, w^{35}, w^{5}, w^{112})$	1200, 19200, 1668000
6	$(w^{29}, w^{29}, w^{29}, w^{29}, w^{29}, w^{39}, w^{25}, w^{33})$	1440, 18000, 16704000

4 Remark

Let C and C' be two linear $[n,k,d]$ codes which have weight distributions $(A_0, A_1, \cdots, A_n)$ and $(A_0', A_1', \ldots, A_n')$, respectively. It is also well known (see [13]) that from viewpoint of decoding error probability, the code C performs better than C' if $(A_0, A_1, \ldots, A_n) \prec (A_0', A_1', \ldots, A_n')$, where $\prec$ means lexicographical ordering. In the above tables, we short the MDS or near-MDS codes due to their performance with respect to decoding error probability. Moreover, recently Buyuklieva, *et al*. [14] proved that in binary case self-dual codes perform better than non self-dual codes, for the codes with the same parameters. It is interesting to know whether the similar situation happens for the non-binary case, in particular in the case of Euclidean self-dual or Hermitian self-dual (near-) MDS codes, etc. This observation, which is now in preparation, will be published elsewhere in a separate paper.

5 Conclusion

As mentioned above there are many self-dual (near-) MDS codes over $GF(9)$, $GF(25)$, and $GF(121)$ of several small lengths constructed by the building-up method as well as our simple algorithm, which combine building-up and subtraction method. To our best knowledge it was unnoticed before in any scientific publication. We concern also with self-dual near-MDS codes because of two reasons: (1) From perspective of capability of error-correcting codes, it is well-known fact that self-dual MDS and self-dual near-MDS are not very different; (2) From cryptographic application, in particular in secret sharing schemes, self-dual near-MDS instead of self-dual MDS codes are important (see, e.g., [11],[12]). There is some expectation to obtain many more self-dual MDS or near-MDS codes over these fields. It will be very good if someone can provide complete classifications of such codes.

Acknowledgement

The authors would like to thank the anonymous referees for careful reading and many helpful suggestions. The research was supported in part by *Riset dan Inovasi KK ITB Tahun 2013* Number 212/I.1.C01/PL/2013. This research has been initiated by partial support from *Riset dan Inovasi KK ITB Tahun 2012* Number 398/I.1.C01/PL/2012.

References

[1] MacWilliams, F.J. & Sloane, N.J.A., *The Theory of Error-Correcting Codes*, Elsevier, Amsterdam, 1977.

[2] de Boer, M.A., *Almost MDS Codes*, Designs, Codes, and Cryptography, **9**(2), pp.143-155, 1996.

[3] Dodunekov, S. & Landjev, I.N., *On Near-MDS Codes*, J. Geom., **54**(1-2), pp. 30-43, 1995.

[4] Dodunekov, S., *Applications of Near-MDS Codes in Cryptography*, in Enhancing Cryptographic Primitive with Techniques from Error-

Correcting Codes, Preneel, B., *et al.* (eds), IOS Press, Amsterdam, pp. 81-86, 2009.

[5] Zhou, Y., Wang, F., Xin, Y., Luo, S., Qing, S. & Yang, Y., *A Secret Sharing Schemes Based on Near-MDS Codes*, Proceedings of IC-NIDC 2009, pp. 833-836, 2009.

[6] Georgiou, S. & Koukouvinos, C., *MDS Self-Dual Codes Over Large Prime Fields*, Finite Field Appl., **8**(4), pp. 455-470, 2002.

[7] Betsumiya, K., Georgiou, S., Gulliver, T.A., Harada, M. & Koukouvinos, C., *On Self-Dual Codes Over Some Prime Fields*, Discrete Math., **262**(1-3), pp. 37-58, 2003.

[8] Kim, J.-L. & Lee, Y., *Euclidean and Hermitian Self-Dual MDS Codes Over Larger Finite Fields*, J. Combin. Theory Ser. A, **105**(1), pp. 79-95, 2004.

[9] Harada, M. & Kharaghani, H., *Orthogonal Designs and MDS Self-dual Codes*, Austral. J. Combin., **35**, pp. 57-67, 2006.

[10] Gulliver, T.A., Kim, J.-L. & Lee, Y., *New MDS or Near-MDS Self-Dual Codes*, IEEE Inform. Theory, **54**(9), pp. 4354-4360, 2008.

[11] Elviyenty, M. & Suprijanto, D., *An Algorithm to Construct New (near-) MDS or (near-)MDR Self-Dual Codes over Finite Rings* $\mathbb{Z}_{p^m}$, in The 5thInternational Conference On Research And Education In Mathematics (ICREM 5)AIP Conf. Proc., **1450**, pp. 205-210, 2012.

[12] Bosma, W. & Canon. J, *Handbook of Magma Functions*, Sydney, Australia, 2006. (preprint).

[13] Faldum, A., Lafuente, J., Ochoa, G. & Willems, W., *Error Probabilities for Bounded Distance Decoding*, Designs, Codes, and Crypt., **40**(2), pp. 237-252, 2006.

[14] Bouyuklieva, S., Malevich, A. & Willems, W., *On the Performance of Binary Extremal Self-Dual Codes*, Adv. Math. Commun., **5**(2), pp. 267-274, 2011.