New MDS or Near-MDS Self-Dual Codes

T. Aaron Gulliver, *Member, IEEE*, Jon-Lark Kim, *Member, IEEE*, and Yoonjin Lee

***Abstract*—We construct new MDS or near-MDS self-dual codes over large finite fields. In particular we show that there exists a Euclidean self-dual MDS code of length $n = q$ over $GF(q)$ whenever $q = 2^m$ $(m \geq 2)$ using a Reed-Solomon (RS) code and its extension. It turns out that this MDS self-dual code is an extended duadic code. We construct Euclidean self-dual near-MDS codes of length $n = q - 1$ over $GF(q)$ from RS codes when $q \equiv 1 \pmod 4$ and $q \leq 113$. We also construct many new MDS self-dual codes over $GF(p)$ of length 16 for primes $29 \leq p \leq 113$. Finally we construct Euclidean/Hermitian self-dual MDS codes of lengths up to 14 over $GF(q^2)$ where $q = 19, 23, 25, 27, 29$.**

***Index Terms*—MDS codes, Reed-Solomon codes, self-dual codes.**

I. Introduction

Let q be a power of a prime p. An $[n, k]$ code C over $GF(q)$ is a k-dimensional subspace of $GF(q)^n$. The value n is called the length of C. The weight $\mathrm{wt}(\mathbf{x})$ of a vector $\mathbf{x} \in GF(q)^n$ is the number of non-zero components of $\mathbf{x}$. The minimum non-zero weight of all codewords in C is called the minimum weight of C and an $[n, k]$ code with minimum weight d is called an $[n, k, d]$ code. The weight enumerator W of C is given by $W = \sum_{i=0}^{n} A_i y^i$ where A_i is the number of codewords of weight i in C. The dual code $C^\perp$ of C is defined as

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

where (a) $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i\, y_i$ or (b) $\mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{n} x_i\, y_i^p$ if $q = p^2$, for two vectors $\mathbf{x} = (x_1, \ldots, x_n), \mathbf{y} = (y_1, \ldots, y_n) \in GF(q)^n$. A code C is called *(Euclidean) self-dual* or *Hermitian self-dual* if $C = C^\perp$ under the inner product (a) or (b), respectively.

For a (Hermitian) self-dual $[n, k, d]$ code over $GF(q)$, the minimum weight is bounded by $d \leq [n/2] + 1$ [16]. Self-dual codes over $GF(q)$ satisfy a modified Gilbert-Varshamov bound [15]. A (Hermitian) self-dual $[n, n/2, n/2 + 1]$ code over $GF(q)$ is called *extremal* and is in fact an MDS code. In general, any linear $[n, k, d]$ code over $GF(q)$ meeting the *Singleton bound* $n - k \geq d - 1$ with equality is called an *MDS code*. A linear $[n, k, n - k]$ code over $GF(q)$ is called an *almost MDS code* [5]. 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* [6].

The *MDS Conjecture* asserts that if there is a nontrivial $[n, k]$ MDS code over $GF(q)$, then $n \leq q+1$, except when q is even and $k = 3$ or $k = q-1$, in which case $n \leq q+2$ [14, pp. 95], [13, pp. 328]. MDS codes are equivalent to geometric objects called n-*arcs* [13, pp. 326] and combinatorial objects called *orthogonal arrays* [13, pp. 328]. Hence there has recently been great interest in the construction of (near) MDS self-dual codes over large fields (see [3], [7], [10], [12]).

In this paper, we extend the results in [3], [7], [10], [12], where MDS self-dual codes over $GF(q)$ of lengths up to 16 are given for certain (large) values of q. As it is very difficult to calculate the minimum distances of high dimension unstructured codes over large fields, it seems infeasible to construct an MDS self-dual code over $GF(q)$ of length $n \leq q + 2$ (due to the MDS conjecture) for each n, given q. However we show that the maximal length n for which there exists an MDS self-dual code over $GF(q)$ is at least q if q is a power of 2.

More precisely, we show that there exists a Euclidean self-dual MDS code of length $n = q$ over $GF(q)$ whenever $q = 2^m$ $(m \geq 2)$ using a Reed-Solomon (RS) code and its extension. It is worth mentioning that this MDS self-dual code is an extended duadic code. We also describe how to construct Euclidean self-dual near-MDS codes of length $n = q - 1$ over $GF(q)$ from RS codes when $q \equiv 1 \pmod 4$.

In [3], a [16,8,9] MDS self-dual code over GF(23) was presented, and an MDS self-dual code of length 16 over GF(79) was given in [10]. No other MDS [16,8,9] self-dual codes over prime fields were known. For other primes $29 \leq p \leq 113$, we give MDS self-dual codes of length 16 over GF(p). We also construct many new Euclidean/Hermitian self-dual MDS codes of lengths up to 14 over $GF(q^2)$ where $q = 19, 23, 25, 27, 29$ and near-MDS self-dual codes of length 16 over $GF(q^2)$ where $11 \leq q \leq 29$. All calculations were done using Magma [4] and C language programs.

II. Existence of Long Euclidean Self-Dual MDS Codes

A. Euclidean self-dual MDS codes over $GF(2^m)$

This section shows that there exists a Euclidean self-dual MDS code of length $n = q$ over $GF(q)$ where q (> 2) is any power of 2 using a Reed-Solomon code and its extension.

Recall that for any q a prime power, a *Reed-Solomon code* over $GF(q)$ is a BCH code of length $n = q - 1$. The following lemmas are well known.

Lemma II.1. [11, Theorem 5.2.1] *Let C be an RS code over $GF(q)$ of length $n = q - 1$ and designed distance δ. Then*

(i) *C has defining set $T = \{b, b + 1, \cdots, b + \delta - 2\}$ for some integer b,*
(ii) *C has minimum distance $d = \delta$ and dimension $k = n - d + 1$, and*
(iii) *C is MDS.*

Lemma II.2. [11, Theorem 4.4.9] *Let C be an $[n, k]$ cyclic code over $GF(q)$ with defining set $T \subset N = \{0, 1, \cdots, n-1\}$. Then the Euclidean dual $C^\perp$ is also cyclic and has defining set $N \backslash (-1)T$.*

Let q be a power of 2 $(q > 2)$. Now consider an RS code C_1 over $GF(q)$ of *odd* length $n = q-1$ with defining set $T = \{1, 2, \cdots, (n-1)/2\}$. It is an $[n, (n + 1)/2, (n + 1)/2]$ MDS code over $GF(q)$ by Lemma II.1. Its dual $C_1^\perp$ is also cyclic with defining set $T' = \{0, 1, 2, \cdots, (n-1)/2\}$ by Lemma II.2. Let $C_2 := C_1^\perp$. Then C_2 is self-orthogonal (under the Euclidean inner product) as $T \subset T'$. C_2 has dimension $k = (n-1)/2$ and minimum distance $d = (n+3)/2$ being MDS. Therefore C_2 is an even-like duadic code whose splitting is given by μ_{-1} due to the following lemma. See [11] for duadic codes and splitting.

Lemma II.3. [11, Theorem 6.4.1] *Let C be any $[n, (n-1)/2]$ cyclic code over $GF(q)$ with q a prime power. Then C is self-orthogonal if and only if C is an even-like duadic code whose splitting is given by μ_{-1}.*

Further, $D_2 := C_2^\perp = C_1$ is an odd-like duadic code whose splitting is also given by μ_{-1}.

Lemma II.4. [11, Theorem 6.4.12] *Let D_1 and D_2 be a pair of odd-like duadic codes of length n over $GF(q)$. Assume that $1 + \gamma^2 n = 0$*

The work of Y. Lee was supported by KOSEF under Grant R01-2008-000-11721-0.

T.A. Gulliver is with the Department of of Electrical and Computer Engineering, University of Victoria, P.O. Box 3055, STN CSC, Victoria, BC, V8W 3P6 Canada (e-mail: agullive@ece.uvic.ca) .

J.-L. Kim is with the Department of Mathematics, University of Louisville, Louisville, KY 40292, USA (e-mail: jl.kim@louisville.edu) .

Y. Lee is with the Department of Mathematics, Ewha Womans University 11-1 Daehyun-Dong, Seodaemun-Gu, Seoul, 120-750, S. Korea, (e-mail: yoonjinl@ewha.ac.kr) .

has a solution γ in $GF(q)$. Then if μ_{-1} gives the splitting from D_1 and D_2 then $\widetilde{D}_1$ and $\widetilde{D}_2$ are self-dual. Here $\widetilde{D} = \{\tilde{\mathbf{c}} \mid \mathbf{c} \in D\}$ where $\tilde{\mathbf{c}} = c_0 \cdots c_{n-1} c_\infty$ and $c_\infty = -\gamma \sum_{i=0}^{n-1} c_i$.

Since $n = q-1$, the equation $1+\gamma^2 n = 0$ has a solution $\gamma = 1$ in $GF(q)$. Therefore the extension $\widetilde{D}$ is the same as the usual extension obtained by adding an overall parity check $c_\infty = -\sum_{i=0}^{n-1} c_i$ to $\mathbf{c} = c_0 \cdots c_{n-1}$.

We summarize what we know about D_2. D_2 is an $[n, (n+1)/2, (n+1)/2]$ RS code over $GF(q)$ and also an odd-like duadic code. Usually extension by an overall parity check does not increase the minimum distance. However we have a positive result in the case of RS codes as follows.

Lemma II.5. [13, Ch. 10] *Let C be the $[n = q^m - 1, k, d]$ RS code with defining set $\{1, \cdots, d-1\}$. Then extending each codeword $\mathbf{c} = c_0 \cdots c_{n-1}$ of C by adding an overall parity check $c_\infty = -\sum_{i=0}^{n-1} c_i$ produces an $[n+1, k, d+1]$ code.*

Therefore by extending D_2 we obtain the following theorem.

Proposition II.6. *For any even $q = 2^m (> 2)$, there exists a Euclidean self-dual MDS code over $GF(q)$ with parameters $[q,\ q/2,\ (q+2)/2]$ which is an extended duadic code or an extended RS code.*

B. Euclidean self-dual near-MDS codes over $GF(q)$

In this section we construct Euclidean self-dual near-MDS codes of *even* length $n = q-1$ over $GF(q)$ from RS codes when $q \equiv 1 \pmod 4$.

Let q be a power of an odd prime. Now consider an RS code C_1 over $GF(q)$ of even length $n = q-1$ with defining set $T = \{1, 2, \cdots, (n/2)-1\}$. It is an $[n, n-(n/2-1), n/2]$ MDS code over $GF(q)$ by Lemma II.1. Its dual $C_1^\perp$ is also cyclic with defining set $T' = \{0, 1, 2, \cdots, (n/2)-1, n/2\}$ by Lemma II.2. Let $C_2 := C_1^\perp$. Then C_2 is self-orthogonal (under the Euclidean inner product) as $T \subset T'$. C_2 has dimension $k = (n/2)-1$ and minimum distance $d = (n/2)+2$ being MDS. Note that as C_2 has even length n and dimension $n/2-1$, extending by one coordinate as in Section II-A does not produce a self-dual code of length $n+1$ since self-dual codes exist only for even lengths.

It is well known [11] that if $q \equiv 3 \pmod 4$ then there is no Euclidean self-dual code over $GF(q)$ of length $n \equiv 2 \pmod 4$. Hence we further assume that $q \equiv 1 \pmod 4$.

Consider the two dimensional quotient vector space $C_2^\perp / C_2$. Suppose that there is a nonzero vector $\mathbf{v} \in C_2^\perp / C_2$ such that $\mathbf{v} \cdot \mathbf{v} = 0$. Then this space is a hyperbolic plane $P =< \mathbf{v}, \mathbf{w} >$, where $\mathbf{v} \cdot \mathbf{v} = 0$, $\mathbf{w} \cdot \mathbf{w} = 0$, and $\mathbf{v} \cdot \mathbf{w} = 1$. Note that the vectors $a\mathbf{v}$ and $b\mathbf{w}$ ($a, b \in GF(q)$) are the only self-orthogonal vectors of P [1, Ch. III]. Hence we obtain two self-dual codes $C := C_2 + < \mathbf{v} >$ and $C' := C_2 + < \mathbf{w} >$ (regarding $\mathbf{v}$ and $\mathbf{w}$ as representatives of $C_2^\perp / C_2$). Since the weight of $\mathbf{v}$ (resp. $\mathbf{w}$) and its nonzero scalar multiple is at least $n/2$, C (resp. C') has minimum distance at least $n/2$.

C_2 can be obtained as `C2:=Dual(ReedSolomonCode(GF(q), n/2))` in Magma. Using this representation, we have found vectors $\mathbf{v} \in C_2^\perp / C_2$ such that $\mathbf{v} \cdot \mathbf{v} = 0$ and $\mathrm{wt}(\mathbf{v}) = n/2$ for any $q \equiv 1 \pmod 4$ up to 113. See Table I, where we omit zeroes on the left of $\mathbf{v}$. For example, when $q = 5$, $\mathbf{v} = 1\ 2$ means $\mathbf{v} = 0\ 0\ 1\ 2$. In the lower part of the table, w denotes a primitive element of $GF(q)$ where $q = 9, 25, 49, 81$. The corresponding minimal polynomials of w over $GF(q)$ are $x^2 + 2x + 2$, $x^2 + 4x + 2$, $x^2 + 6x + 3$, and $x^4 + 2x^3 + 2$, respectively.

Hence we obtain the following.

TABLE I
EUCLIDEAN SELF-DUAL NEAR-MDS $[n, n/2, d]$ CODES OVER $GF(q)$ FROM RS CODES

q	n	d	$\mathbf{v}$ (of length n with zeroes on the left omitted)
5	4	2	1 2
13	12	6	1 10 5 1 11 8
17	16	8	1 15 11 13 16 10 8 4
29	28	14	1 26 5 6 28 2 3 7 5 17 15 2 7 12
37	36	18	1 34 5 20 2 11 28 24 25 35 33 17 29 25 9 7 19 31
41	40	20	1 15 31 12 28 14 9 5 3 24 30 27 37 40 38 6 15 33 29 9
53	52	26	1 50 5 39 30 45 52 44 39 46 41 32 24 31 47 11 51 4 5 23 28 52 49 44 37 30
61	60	30	1 58 5 11 16 42 38 20 54 58 20 47 48 54 44 57 16 40 32 37 33 45 24 52 26 54 1 55 33 11
73	72	36	1 35 29 40 31 51 44 54 57 52 1 33 50 34 40 68 57 10 51 67 11 15 42 37 15 46 17 67 71 53 63 39 58 20 69 46
89	88	44	1 87 47 11 31 32 53 41 58 70 59 2 19 79 86 74 45 26 39 67 77 66 19 52 53 9 83 72 24 1 3 16 66 68 41 66 75 59 67 20 14 18 4 21 55
97	96	48	1 47 38 49 78 50 5 42 77 8 29 45 9 25 73 38 79 35 22 24 5 74 60 93 9 38 76 84 43 1 91 8 60 43 65 93 20 41 79 52 51 84 33 30 11 37 64 75
101	100	50	1 98 5 8 65 9 34 10 83 24 50 66 73 74 44 62 19 46 11 45 40 5 56 4 95 41 61 55 51 97 55 9 45 89 87 36 68 23 47 96 63 22 1 37 11 44 21 50 30 10
109	108	54	1 64 32 62 23 6 99 63 100 7 40 21 107 64 48 54 103 11 89 83 92 48 77 44 42 94 58 61 59 78 74 34 51 93 95 103 73 20 71 58 68 43 70 12 96 30 101 106 20 105 25 75 68 33
113	112	56	1 111 59 6 56 50 61 17 15 40 79 56 58 77 7 110 102 87 97 35 90 82 55 67 39 108 86 18 69 47 75 20 12 34 13 107 40 99 51 61 45 105 88 79 64 55 78 112 84 11 41 49 23 94 30 15
9	8	4	$w\ 1\ w^2\ w^7\ 0$
25	24	12	$w^7\ 1\ w^{14}\ w^{22}\ w\ w^{14}\ w^{20}\ w^{19}\ w^4\ w^8\ 2\ w\ 0$
49	48	24	$w^2\ 1\ w^{47}\ w^{38}\ 4\ w^{45}\ w^{41}\ w^{27}\ w^{19}\ 2\ w^{47}\ w^4\ 2\ w^{35}\ w^{28}\ w^7\ w^{39}\ w^{29}\ w^9\ w^{20}\ w^2\ w^{35}\ w^{12} w^{38}\ 0$
81	40	20	$w^9\ 1\ w^{73}\ w^{46}\ w^{74}\ w^{66}\ w^{45}\ w^{43}\ w^{38}\ w^{37}\ w^{27}\ w^{41}\ w^{45}\ w^8\ w^{37}\ w^{13}\ w^{68}\ w^{10}\ w^{27}\ w^{73}\ w^{13}\ w^7\ w^{30}\ w^{48}\ w^{33}\ w^{17}\ w^{28}\ w^{25}\ w^{61}\ w^7\ w^{57}\ w^{18}\ w^{63}\ w^{25}\ w^6\ w^{54}\ w^{66}\ w^{53}\ w^{20}\ w^{69}\ 0$

Proposition II.7. *For any odd $q \equiv 1 \pmod 4$ such that $q \leq 113$, there exists a Euclidean self-dual near-MDS code over $GF(q)$ with parameters $[n = q-1, k = n/2, d = n/2]$.*

Remark II.8. We have checked that when $q = 13$, C and C' as defined above are equivalent. In general, we conjecture that C and C' for any $q \equiv 1 \pmod 4$ are equivalent. We also conjecture that Proposition II.7 is true for any $q \equiv 1 \pmod 4$.

III. CONSTRUCTION OF SHORT MDS SELF-DUAL CODES

Codes with generator matrices of the form

$$\begin{pmatrix} & I_n & & R & \end{pmatrix}, \tag{1}$$

and

$$\begin{pmatrix} & & \alpha & \beta & \cdots & \beta \\ & & \gamma & & & \\ & & \vdots & & R' & \\ & I_{n+1} & \gamma & & & \end{pmatrix}, \tag{2}$$

are called *pure double circulant* and *bordered double circulant*, respectively, where I_n is the identity matrix of order n, R and R' are $n \times n$ circulant matrices and $\alpha, \beta, \gamma \in GF(q)$. The two families are called double circulant (DC) codes.

A code which has generator matrix of the form

$$\begin{pmatrix} I_n & N \end{pmatrix}, \tag{3}$$

is called a *quasi-twisted* (QT) code, where N is an $n \times n$ negacirculant matrix. Here a negacirculant matrix has the form

$$\begin{pmatrix} r_0 & r_1 & r_2 & \cdots & r_{n-1} \\ -r_{n-1} & r_0 & r_1 & \cdots & r_{n-2} \\ -r_{n-2} & -r_{n-1} & r_0 & \cdots & r_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ -r_1 & -r_2 & -r_3 & \cdots & r_0 \end{pmatrix}.$$

The following building-up constructions are given in [12].

Proposition III.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 $GF(q)$ under the Euclidean inner product. Suppose that $y_i := (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n}) \cdot (\mathbf{l}_i \mid \mathbf{r}_i)$ for $1 \le i \le n$ under the Euclidean inner product. Then the following matrix*

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

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

Proposition III.2. *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 $1 \le i \le n$. Let $\mathbf{x} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n})$ be a vector in $GF(q^2)^{2n}$ with $\mathbf{x} \cdot \mathbf{x} = -1$ in $GF(q^2)$ under the Hermitian inner product. Set $\overline{y_i} = (x_1, \cdots, x_n, x_{n+1}, \cdots, x_{2n}) \cdot (\mathbf{l}_i \mid \mathbf{r}_i)$ under the Hermitian inner product for $1 \le i \le n$, and $c = w^{\frac{q-1}{2}}$ for a primitive (q^2-1)th root of unity w in $GF(q^2)$. Then we have that $c\bar{c} = -1$. The following matrix*

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

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

A. Self-dual MDS codes of lengths ≤ 16 over $GF(q)$, $q \le 113$

Example III.3. Let w be a primitive element of $GF(8)$ whose minimal polynomial is $x^3 + x + 1$. The DC code with first row $w^4, w^2, w^3, 1, 1$ is a Euclidean self-dual near-MDS $[12, 6, 6]$ code over $GF(8)$. This code improves a previously known self-dual $[12, 6, 5]$ code over $GF(8)$ [12]. Moreover this code is optimal [9].

Example III.4. Let w be a primitive element of $GF(9)$ whose minimal polynomial is $x^2 + x + 2$. The DC code with first row w^7, w^6, w^7, w, w is a Hermitian self-dual MDS $[10, 5, 6]$ code over $GF(9)$. This code improves a previously known Hermitian self-dual $[10, 5, 5]$ code over $GF(9)$ [12]. The DC code with first row w^6, w^7, w^6, w, w is a Euclidean self-dual MDS $[10, 5, 6]$ code over $GF(9)$.

Glynn [8] proved that there are exactly two non-equivalent 10-arcs in PG$(4, 9)$. Correspondingly, there are only two non-equivalent $[10, 5, 6]$ codes over GF(9), namely, the Reed-Solomon code and the so called Glynn code. The second code corresponds to the only known $(q+1)$-arc in PG(N, q), q odd, $2 <= N <= q-2$, which is not a normal rational curve. It was shown in [2] that the Reed-Solomon code is Euclidean but not Hermitian self-dual while the Glynn code is Hermitian but not Euclidean self-dual. The Glynn code is a representative of an interesting family of Hermitian self-dual codes over GF(q^2) [16]. Hence the DC codes constructed in Example III.4 are equivalent to the above classical examples.

Example III.5. Let w be a primitive element of $GF(16)$ whose minimal polynomial is $x^4 + x + 1$. The DC code with first row $w^4, w^2, w^8, w, 1$ is a Euclidean self-dual MDS $[10, 5, 6]$ code over $GF(16)$. The DC code with first row $w^3, w^3, w^{11}, w^{10}, w^3, w, w$ is a Euclidean self-dual near-MDS $[14, 7, 7]$ code over $GF(16)$. Both codes are new.

The DC code with first row $w^{14}, w^{14}, 1$ is a Hermitian self-dual MDS $[6, 3, 4]$ code over $GF(16)$. The DC code with first row $1, 1, 1, 0$ is a Hermitian self-dual near-MDS $[8, 4, 4]$ code over $GF(16)$. Hermitian self-dual codes with parameters $[6, 3, 4]$ or $[8, 4, 4]$ were also constructed in [12].

The DC code with first row $w^3, w^7, w, 1, 1$ is a Hermitian self-dual MDS $[10, 5, 6]$ code over $GF(16)$, improving on a Hermitian self-dual $[10, 5, 5]$ code [12]. The DC code with first row $1, w, w^{12}, w, 1, 0$ is a Hermitian self-dual near-MDS $[12, 6, 6]$ code over $GF(16)$, having the same parameters as in [12]. The DC code with first row $w^{10}, w, w^5, w^{12}, w, 1, 0$ is the first Hermitian self-dual near-MDS $[14, 7, 7]$ code over $GF(16)$.

Example III.6. In [3], a [16,8,9] MDS self-dual code over GF(23) was presented, and an MDS self-dual code of length 16 over GF(79) was given in [10]. No other MDS [16,8,9] self-dual codes over prime fields are known. For other primes $29 \le p \le 113$, we give MDS self-dual codes of length 16 over GF(p) in Table II. Hence we have the following.

Proposition III.7. *There exists an MDS self-dual code over $GF(p)$ of length 16 for primes $23 \le p \le 113$.*

B. Hermitian self-dual MDS codes over $GF(q^2)$ with $q \ge 11$

In [12], Hermitian self-dual (near) MDS codes of lengths ≤ 12 over $GF(q^2)$ with $q = 3, 5, 7, 9$ are constructed. Using the building-up construction (Proposition III.2) in Section III, we obtain Hermitian self-dual (near) MDS codes over $GF(q^2)$ with $11 \le q \le 29$ and lengths ≤ 16. In particular, we show the following.

Proposition III.8. *There exist Hermitian self-dual MDS codes over $GF(q^2)$ of length 14 when $q = 19, 23, 25, 27, 29$ and of lengths ≤ 12 when $11 \le q \le 29$. There exist Hermitian self-dual near-MDS codes over $GF(q^2)$ of length 16 when $11 \le q \le 29$.*

Example III.9. Let w be a primitive element of $GF(11^2)$ whose minimal polynomial is $x^2 + 7x + 2$. Define $c = w^{\frac{11-1}{2}} = w^5$ so that $c\bar{c} = -1$. We give below a generator matrix $G_1^{121,H}$ for a Hermitian self-dual near-MDS $[14, 7, 7]$ code over $GF(121)$.

TABLE II
MDS SELF-DUAL CODES OF LENGTH 16 FROM CIRCULANT AND NEGACIRCULANT MATRICES

p	code	α,β,γ	first row							
29	DC	$2,7,7$	14	13	11	8	5	3	2	
31	QT		9	25	17	29	14	16	2	1
37	QT		26	18	14	16	18	12	6	2
41	QT		21	30	32	21	18	4	3	1
43	QT		2	13	5	10	3	26	2	1
47	QT		7	37	32	19	27	9	2	1
53	QT		41	30	48	49	49	35	2	1
59	QT		26	21	39	55	13	11	2	1
61	QT		37	30	53	43	14	29	5	1
67	QT		27	64	17	25	54	7	2	1
71	QT		47	68	58	36	70	12	2	1
73	QT		46	8	45	7	70	29	2	1
83	QT		8	49	16	52	54	6	2	1
89	QT		36	41	16	65	37	45	2	1
97	QT		75	20	80	64	67	18	2	1
101	QT		83	4	22	96	67	3	2	1
103	QT		74	82	66	46	8	2	2	1
107	QT		19	51	100	24	77	1	2	1
109	QT		71	44	54	54	16	3	2	1
113	QT		36	21	47	89	45	1	2	1

$$\begin{pmatrix} 1\ 0\ w^{30}\ w^{71}\ w^{40}\ w^{116}\ w^{55}\ w^{17}\ w^{69}\ w^{64}\ w^{86}\ w^{35}\ w^{89}\ w^{45} \\ w^{34}\ w^{29}\ 1\ 0\ w^{112}\ w^{50}\ w^{116}\ w^{2}\ w^{102}\ w^{67}\ w^{34}\ 3\ 4\ w^{19} \\ w^{88}\ w^{83}\ w^{82}\ w^{77}\ 1\ 0\ w^{21}\ w^{54}\ w^{109}\ w^{6}\ w^{74}\ w^{50}\ w^{115}\ w^{74} \\ w^{103}\ w^{98}\ w^{105}\ w^{100}\ w^{53}\ 5\ 1\ 0\ w^{66}\ w^{51}\ w^{37}\ w^{69}\ w^{5}\ w^{66} \\ w^{104}\ w^{99}\ w^{56}\ w^{51}\ w^{112}\ w^{107}\ 8\ w^{31}\ 1\ 0\ w^{94}\ w^{59}\ 7\ w^{114} \\ w^{109}\ w^{104}\ w^{27}\ w^{22}\ w^{78}\ w^{73}\ w^{107}\ w^{102}\ 7\ w^{79}\ 1\ 0\ w^{71}\ w^{63} \\ w^{25}\ w^{20}\ w^{109}\ w^{104}\ w^{90}\ w^{85}\ w^{5}\ 1\ 10\ w^{55}\ 6\ w^{103}\ 1\ w^{5} \end{pmatrix}$$

Property (i): *The successive deletion of the first two columns and the first row of the generator matrix produces Hermitian self-dual MDS codes of lengths* $12, 10, 8, 6, 4$, *and* 2. *We also find many Hermitian self-dual near-MDS* $[16, 8, 8]$ *codes.*

Example III.10. Let w be a primitive element of $GF(13^2)$ whose minimal polynomial is $x^2 - x + 2$. Define $c = w^{\frac{13-1}{2}} = w^6$ so that $c\bar{c} = -1$. We give below a generator matrix $G_2^{169,H}$ for a Hermitian self-dual near-MDS $[14, 7, 7]$ code over $GF(169)$.

$$\begin{pmatrix} 1\ 0\ w^{129}\ w^{123}\ w^{85}\ w^{77}\ w^{64}\ w^{121}\ 8\ w^{164}\ w^{152}\ w^{94}\ w^{48}\ w^{130} \\ w^{23}\ w^{17}\ 1\ 0\ w^{92}\ w^{122}\ w^{78}\ w^{86}\ w^{3}\ w^{68}\ w^{121}\ w\ w^{152}\ w^{21} \\ w^{120}\ w^{114}\ w^{153}\ w^{147}\ 1\ 0\ w^{24}\ w^{20}\ w^{131}\ w^{34}\ w^{89}\ w^{90}\ w^{105}\ w^{108} \\ w^{9}\ w^{3}\ w^{81}\ w^{75}\ w^{115}\ w^{109}\ 1\ 0\ w^{128}\ w^{167}\ w^{152}\ w^{93}\ w^{152}\ w^{54} \\ w^{88}\ w^{82}\ w^{133}\ w^{127}\ w^{44}\ w^{38}\ w^{136}\ w^{130}\ 1\ 0\ 8\ w^{87}\ w^{152}\ w^{8} \\ w^{159}\ w^{153}\ w^{22}\ w^{16}\ w^{45}\ w^{39}\ w^{159}\ w^{153}\ w^{155}\ w^{149}\ 1\ 0\ w^{125}\ w^{89} \\ w^{20}\ 2\ w^{97}\ w^{91}\ w^{99}\ w^{93}\ w^{8}\ w^{2}\ w^{37}\ w^{31}\ w^{141}\ w^{135}\ 1\ w^{6} \end{pmatrix}$$

Example III.11. Let w be a primitive element of $GF(17^2)$ whose minimal polynomial is $x^2 - x + 3$. Define $c = w^{\frac{17-1}{2}} = w^8$ so that $c\bar{c} = -1$. We give below a generator matrix $G_3^{289,H}$ for a Hermitian self-dual near-MDS $[14, 7, 7]$ code over $GF(289)$.

$$\begin{pmatrix} 1\ 0\ w^{243}\ w^{241}\ w^{202}\ w^{82}\ w^{92}\ w^{75}\ w^{116}\ w^{135}\ w^{103}\ w^{5}\ w^{245}\ w^{278} \\ w^{49}\ w^{41}\ 1\ 0\ w^{244}\ w^{146}\ w^{61}\ w^{15}\ w^{51}\ w^{231}\ w^{75}\ w^{187}\ w^{113}\ w^{223} \\ w^{35}\ w^{27}\ w^{242}\ 12\ 1\ 0\ 7\ w^{275}\ w^{75}\ w^{28}\ w^{22}\ 9\ 15\ w^{8} \\ w^{245}\ w^{237}\ w^{253}\ w^{245}\ w^{161}\ w^{153}\ 1\ 0\ w^{96}\ w^{240}\ w^{215}\ w^{225}\ w^{68}\ w^{268} \\ w^{87}\ w^{79}\ w^{105}\ w^{97}\ w^{78}\ w^{70}\ w^{10}\ w^{2}\ 1\ 0\ w^{28}\ w^{281}\ w^{238}\ w^{244} \\ 13\ w^{64}\ w^{61}\ w^{53}\ w^{35}\ w^{27}\ w^{163}\ w^{155}\ w^{104}\ w^{96}\ 1\ 0\ w^{171}\ 3 \\ w^{282}\ w^{274}\ w^{151}\ w^{143}\ w^{134}\ 11\ w^{25}\ w^{17}\ w^{38}\ w^{30}\ w^{111}\ w^{103}\ 1\ w^{8} \end{pmatrix}$$

Example III.12. Let w be a primitive element of $GF(19^2)$ whose minimal polynomial is $x^2 - x + 2$. Define $c = w^{\frac{19-1}{2}} = w^9$ so that $c\bar{c} = -1$. We give below a generator matrix $G_4^{361,H}$ for a Hermitian self-dual MDS $[14, 7, 8]$ code over $GF(361)$.

$$\begin{pmatrix} 1\ 0\ 15\ w^{103}\ w^{83}\ w^{345}\ w^{265}\ w^{109}\ w^{79}\ 1\ w^{143}\ w^{292}\ w^{177}\ w^{95} \\ w^{55}\ w^{46}\ 1\ 0\ w^{96}\ 1\ w^{136}\ w^{24}\ w^{352}\ w^{228}\ w^{341}\ w^{201}\ w^{89}\ w^{266} \\ w^{35}\ w^{26}\ w^{31}\ w^{22}\ 1\ 0\ w^{106}\ w^{214}\ w^{212}\ w^{117}\ w^{94}\ w^{57}\ w^{247}\ w^{133} \\ 14\ w^{131}\ w^{295}\ w^{286}\ w^{270}\ w^{261}\ 1\ 0\ w^{124}\ w^{351}\ w^{42}\ w^{268}\ w^{28}\ w^{254} \\ w^{334}\ w^{325}\ w^{99}\ w^{90}\ w^{8}\ w^{359}\ w^{253}\ w^{244}\ 1\ 0\ w^{83}\ w^{279}\ w^{337}\ w^{324} \\ w^{210}\ w^{201}\ w^{69}\ 8\ w^{358}\ w^{349}\ w^{203}\ w^{194}\ w^{122}\ w^{113}\ 1\ 0\ 8\ w^{102} \\ w^{205}\ w^{196}\ w^{224}\ w^{215}\ w^{185}\ w^{176}\ w^{191}\ w^{182}\ w^{133}\ w^{124}\ w^{265}\ w^{256}\ 1\ w^{9} \end{pmatrix}$$

Example III.13. Let w be a primitive element of $GF(23^2)$ whose minimal polynomial is $x^2 - 2x + 5$. Define $c = w^{\frac{23-1}{2}} = w^{11}$ so that $c\bar{c} = -1$. We give below a generator matrix $G_5^{529,H}$ for a Hermitian self-dual MDS $[14, 7, 8]$ code over $GF(529)$.

$$\begin{pmatrix} 1\ 0\ w^{255}\ w^{261}\ w^{10}\ w^{157}\ w^{208}\ w^{70}\ w^{94}\ w^{25}\ w^{527}\ w^{287}\ w^{141}\ w^{392} \\ w^{87}\ w^{76}\ 1\ 0\ w^{306}\ w^{12}\ w^{279}\ w^{258}\ w^{364}\ w^{370}\ w^{365}\ w^{327}\ w^{305}\ w^{368} \\ w^{348}\ w^{337}\ w^{414}\ w^{403}\ 1\ 0\ w^{3}\ w^{269}\ w^{332}\ 0\ w^{450}\ w^{197}\ w^{33}\ w^{197} \\ w^{126}\ w^{115}\ w^{274}\ w^{263}\ w^{402}\ w^{391}\ 1\ 0\ w^{445}\ w^{219}\ w^{102}\ w^{475}\ w^{493}\ w^{218} \\ w^{358}\ w^{347}\ w^{305}\ w^{294}\ w^{205}\ w^{194}\ w^{112}\ w^{101}\ 1\ 0\ w^{403}\ w^{45}\ w^{433}\ w^{466} \\ w^{458}\ w^{447}\ w^{33}\ w^{22}\ w^{429}\ w^{418}\ w^{443}\ 6\ w^{413}\ w^{402}\ 1\ 0\ w^{375}\ w^{249} \\ w^{97}\ w^{86}\ w^{36}\ w^{25}\ w^{338}\ w^{327}\ w^{143}\ w^{132}\ w^{197}\ w^{186}\ w^{435}\ w^{424}\ 1\ w^{11} \end{pmatrix}$$

Example III.14. Let w be a primitive element of $GF(25^2)$ whose minimal polynomial is $x^4 - x^2 - x + 2$. Define $c = w^{\frac{25-1}{2}} = w^{12}$ so that $c\bar{c} = -1$. We give below a generator matrix $G_6^{625,H}$ for a Hermitian self-dual MDS $[14, 7, 8]$ code over $GF(625)$.

$$\begin{pmatrix} 1\ 0\ w^{393}\ w^{481}\ w^{295}\ w^{170}\ w^{262}\ w^{600}\ w^{305}\ w^{356}\ w^{394}\ w^{249}\ w^{98}\ w^{198} \\ w^{615}\ w^{603}\ 1\ 0\ w^{473}\ w^{111}\ w^{79}\ w^{486}\ w^{69}\ w^{495}\ w^{119}\ w\ w^{493}\ w^{447} \\ w^{270}\ w^{258}\ w^{579}\ w^{567}\ 1\ 0\ w^{130}\ w^{442}\ w^{226}\ w^{103}\ w^{117}\ w^{412}\ w^{5}\ w^{595} \\ w^{273}\ w^{261}\ w^{56}\ w^{44}\ w^{41}\ w^{29}\ 1\ 0\ w^{280}\ w^{440}\ w^{99}\ w^{235}\ w^{27}\ w^{226} \\ w^{382}\ w^{370}\ w^{404}\ w^{392}\ w^{172}\ w^{160}\ w^{402}\ w^{390}\ 1\ 0\ w^{205}\ w^{557}\ w^{570}\ w^{343} \\ w^{518}\ w^{506}\ w^{224}\ w^{212}\ w^{535}\ w^{523}\ w^{346}\ w^{334}\ w^{169}\ w^{157}\ 1\ 0\ w^{253}\ w^{209} \\ w^{351}\ w^{339}\ w^{327}\ w^{315}\ w^{566}\ w^{554}\ w^{181}\ w^{169}\ w^{571}\ w^{559}\ w^{318}\ w^{306}\ 1\ w^{12} \end{pmatrix}$$

Example III.15. Let w be a primitive element of $GF(27^2)$ whose minimal polynomial is $x^6 + 2x^4 + x^2 + 2x + 2$. Define $c = w^{\frac{27-1}{2}} = w^{13}$ so that $c\bar{c} = -1$. We give below a generator matrix $G_7^{729,H}$ for a Hermitian self-dual MDS $[14, 7, 8]$ code over $GF(729)$.

$$\begin{pmatrix} 1\ 0\ w^{455}\ w^{176}\ w^{682}\ w^{464}\ w^{394}\ w^{610}\ w^{533}\ w^{53}\ w^{195}\ w^{259}\ w^{578}\ w^{608} \\ w^{413}\ w^{400}\ 1\ 0\ w^{45}\ w^{121}\ w^{310}\ w^{63}\ w^{152}\ w^{272}\ w^{619}\ w^{652}\ w^{585}\ w^{135} \\ w^{35}\ w^{22}\ w^{571}\ w^{558}\ 1\ 0\ w^{187}\ w^{435}\ w^{106}\ w^{329}\ w^{152}\ w^{38}\ w^{202}\ w^{149} \\ w^{327}\ w^{314}\ w^{156}\ w^{143}\ w^{631}\ w^{618}\ 1\ 0\ w^{668}\ w^{441}\ w^{187}\ w^{207}\ w^{516}\ w^{488} \\ w^{646}\ w^{633}\ w^{305}\ w^{292}\ w^{488}\ w^{475}\ w^{673}\ w^{660}\ 1\ 0\ 1\ w^{622}\ w^{642}\ w^{204} \\ w^{542}\ w^{529}\ w^{287}\ w^{274}\ w^{215}\ w^{202}\ w^{449}\ w^{436}\ w^{663}\ w^{650}\ 1\ 0\ w^{374}\ w^{695} \\ w^{428}\ w^{415}\ w^{245}\ w^{232}\ w^{187}\ w^{174}\ w^{585}\ w^{572}\ w^{160}\ w^{147}\ w^{74}\ w^{61}\ 1\ w^{13} \end{pmatrix}$$

Example III.16. Let w be a primitive element of $GF(29^2)$ whose minimal polynomial is $x^2 - 5x + 2$. Define $c = w^{\frac{29-1}{2}} = w^{14}$ so that $c\bar{c} = -1$. We give below a generator matrix $G_8^{841,H}$ for a Hermitian self-dual MDS $[14, 7, 8]$ code over $GF(841)$.

$$\begin{pmatrix} 1\ 0\ w^{615}\ w^{755}\ w^{581}\ w^{106}\ w^{331}\ w^{23}\ w^{523}\ w^{399}\ w^{699}\ w^{54}\ w^{511}\ w^{489} \\ w^{511}\ w^{497}\ 1\ 0\ w^{372}\ w^{361}\ w^{523}\ w^{113}\ w^{424}\ w^{637}\ w^{7}\ w^{711}\ w^{176}\ w^{76} \\ w^{137}\ w^{123}\ w^{242}\ w^{228}\ 1\ 0\ w^{266}\ w^{614}\ w^{58}\ w^{417}\ w^{776}\ w^{482}\ w^{286}\ w^{391} \\ w^{250}\ w^{236}\ w^{15}\ w\ w^{773}\ w^{759}\ 1\ 0\ w^{291}\ w^{434}\ w^{814}\ w^{182}\ w^{471}\ w^{827} \\ w^{110}\ w^{96}\ w^{212}\ w^{198}\ w^{779}\ w^{765}\ w^{167}\ w^{153}\ 1\ 0\ w^{31}\ w^{702}\ w^{399}\ w^{534} \\ 23\ w^{586}\ w^{611}\ w^{597}\ w^{64}\ w^{50}\ w^{624}\ w^{610}\ w^{705}\ w^{691}\ 1\ 0\ w^{121}\ w^{794} \\ w^{458}\ w^{444}\ w^{797}\ w^{783}\ w^{119}\ w^{105}\ w^{171}\ w^{157}\ w^{23}\ w^{9}\ w^{121}\ w^{107}\ 1\ w^{14} \end{pmatrix}$$

We note that Property (i) holds for Examples III.10–III.16 as in Example III.9.

C. Euclidean self-dual MDS codes over $GF(q^2)$ with $q \geq 11$

In [12], Euclidean self-dual MDS codes of lengths ≤ 12 over $GF(q^2)$ with $q = 7$ are constructed. Using the building-up construction (Proposition III.1) in Section III with $c = w^{\frac{q^2-1}{4}}$ for a primitive (q^2-1)th root of unity w in $GF(q^2)$, we obtain Euclidean self-dual (near) MDS codes over $GF(q^2)$ with $9 \leq q \leq 29$ and lengths ≤ 16. In particular, we show the following.

Proposition III.17. *There exist Euclidean self-dual MDS codes over* $GF(q^2)$ *of length* 14 *when* $q = 19, 23, 25, 27, 29$ *and of lengths*

≤ 12 *when* $9 \leq q \leq 29$. *There exist Euclidean self-dual near-MDS codes over* $GF(q^2)$ *of length* 16 *when* $9 \leq q \leq 29$.

Example III.18. Let w be a primitive element of $GF(9^2)$ whose minimal polynomial is $x^4 + 2x^3 + 2$. Define $c = w^{\frac{81-1}{4}} = w^{20}$ so that $c^2 = -1$. We give below a generator matrix $G_0^{81,E}$ for a Euclidean self-dual near-MDS $[14, 7, 7]$ code over $GF(81)$.

$$\begin{pmatrix} 1\ 0\ w^{27}\ w^{9}\ w^{33}\ w^{33}\ w^{65}\ w^{76}\ w^{24}\ w^{16}\ w^{57}\ w^{9}\ w^{32}\ w^{51} \\ w^{76}\ w^{56}\ 1\ 0\ w^{38}\ w^{78}\ w^{46}\ w^{39}\ 1\ w^{75}\ w^{37}\ w^{73}\ w^{72}\ w^{73} \\ w^{44}\ w^{24}\ w^{17}\ w^{77}\ 1\ 0\ w\ w^{72}\ w^{70}\ w^{15}\ w^{50}\ w^{7}\ w^{26}\ w^{11} \\ w^{79}\ w^{59}\ w^{34}\ w^{14}\ w^{68}\ w^{48}\ 1\ 0\ w^{9}\ w^{41}\ w^{51}\ w^{25}\ w^{52}\ w^{35} \\ w^{57}\ w^{37}\ w^{4}\ w^{64}\ w^{53}\ w^{33}\ 1\ w^{60}\ 1\ 0\ w^{50}\ w^{56}\ w^{66}\ w^{48} \\ w^{35}\ w^{15}\ w^{34}\ w^{14}\ w^{76}\ w^{56}\ w^{67}\ w^{47}\ w^{17}\ w^{77}\ 1\ 0\ w^{35}\ w^{65} \\ w^{59}\ w^{39}\ w^{75}\ w^{55}\ w^{49}\ w^{29}\ w^{73}\ w^{53}\ w^{57}\ w^{37}\ w^{25}\ w^{5}\ 1\ w^{20} \end{pmatrix}$$

Property (ii): *The successive deletion of the first two columns and the first row of the generator matrix produces Euclidean self-dual MDS codes of lengths* $12, 10, 8, 6, 4$, *and* 2. *We also find many Euclidean self-dual near-MDS* $[16, 8, 8]$ *codes.*

Example III.19. Let w be a primitive element of $GF(11^2)$ whose minimal polynomial is $x^2 + 7x + 2$. Define $c = w^{\frac{121-1}{4}} = w^{30}$ so that $c^2 = -1$. We give below a generator matrix $G_1^{121,E}$ for a Euclidean self-dual near-MDS $[14, 7, 7]$ code over $GF(121)$.

$$\begin{pmatrix} 1\ 0\ w^{70}\ w^{20}\ w^{73}\ w^{23}\ w^{106}\ w^{95}\ w^{35}\ w^{10}\ w^{37}\ 3\ w^{53}\ 10 \\ w^{118}\ w^{88}\ 1\ 0\ w^{16}\ w^{86}\ w^{3}\ w^{35}\ w^{87}\ w^{89}\ w^{3}\ w^{64}\ w^{79}\ w^{2} \\ w^{15}\ w^{105}\ w^{47}\ w^{17}\ 1\ 0\ w^{10}\ w^{62}\ w^{34}\ w^{58}\ w^{15}\ w^{7}\ w^{14}\ w^{75} \\ w^{65}\ w^{35}\ w^{39}\ w^{9}\ w^{13}\ w^{103}\ 1\ 0\ 0\ w^{23}\ w^{98}\ w^{63}\ w^{70}\ w^{61} \\ w^{80}\ w^{50}\ w^{56}\ w^{26}\ w^{104}\ w^{74}\ w^{76}\ w^{46}\ 1\ 0\ w^{28}\ w^{61}\ w^{101}\ w^{114} \\ w^{43}\ w^{13}\ w^{46}\ w^{16}\ 5\ w^{18}\ w^{82}\ w^{52}\ w^{13}\ w^{103}\ 1\ 0\ 6\ w^{102} \\ w^{56}\ w^{26}\ w^{76}\ w^{46}\ w^{32}\ w^{2}\ w^{34}\ w^{4}\ w^{58}\ w^{28}\ 3\ w^{66}\ 1\ w^{30} \end{pmatrix}$$

Example III.20. Let w be a primitive element of $GF(13^2)$ whose minimal polynomial is $x^2 - x + 2$. Define $c = w^{\frac{169-1}{4}} = w^{42} = 8$ so that $c^2 = -1$. We give below a generator matrix $G_2^{169,E}$ for a Euclidean self-dual near-MDS $[14, 7, 7]$ code over $GF(169)$.

$$\begin{pmatrix} 1\ 0\ w^{55}\ w^{135}\ w^{83}\ w^{26}\ w^{142}\ w^{108}\ w^{110}\ w^{148}\ w^{40}\ w^{123}\ w^{86}\ w \\ w^{97}\ w^{55}\ 1\ 0\ w^{60}\ w^{159}\ 11\ w^{72}\ w^{142}\ w\ w^{122}\ w^{116}\ w^{31}\ w^{108} \\ w^{12}\ w^{138}\ w^{5}\ w^{131}\ 1\ 0\ w^{8}\ w^{4}\ w^{37}\ w^{33}\ w^{62}\ 8\ w^{20}\ w^{21} \\ w^{104}\ w^{62}\ w^{95}\ w^{53}\ w\ w^{127}\ 1\ 0\ w^{104}\ w^{18}\ w^{159}\ w^{120}\ w^{164}\ w^{163} \\ w^{99}\ w^{57}\ w^{52}\ w^{10}\ w^{21}\ w^{147}\ w^{130}\ w^{88}\ 1\ 0\ w^{86}\ w^{123}\ w^{120}\ w^{62} \\ w^{23}\ w^{149}\ w^{92}\ w^{50}\ w^{76}\ w^{34}\ w^{131}\ w^{89}\ w^{160}\ w^{118}\ 1\ 0\ 3\ 4 \\ w^{103}\ w^{61}\ w^{11}\ w^{137}\ w^{128}\ w^{86}\ w^{92}\ w^{50}\ w^{108}\ w^{66}\ 4\ 7\ 1\ 8 \end{pmatrix}$$

A Euclidean self-dual MDS $[14, 7, 8]$ code over $GF(13)$ is constructed in [3]. It is also a Euclidean self-dual MDS $[14, 7, 8]$ code over $GF(13^2)$ as $GF(13)$ is a subfield of $GF(13^2)$.

Example III.21. Let w be a primitive element of $GF(17^2)$ whose minimal polynomial is $x^2 - x + 3$. Define $c = w^{\frac{289-1}{4}} = w^{72} = 13$ so that $c^2 = -1$. We give below a generator matrix $G_3^{289,E}$ for a Euclidean self-dual near-MDS $[14, 7, 7]$ code over $GF(289)$.

$$\begin{pmatrix} 1\ 0\ 3\ w^{227}\ w^{201}\ w^{112}\ w^{154}\ w^{42}\ w^{138}\ w^{253}\ w^{101}\ w^{119}\ w^{67}\ w^{29} \\ w^{224}\ w^{152}\ 1\ 0\ w^{266}\ 12\ w^{8}\ w^{78}\ w^{276}\ w^{285}\ w^{45}\ w^{256}\ w^{110}\ 12 \\ w^{148}\ w^{76}\ w^{284}\ w^{212}\ 1\ 0\ w^{113}\ w^{208}\ w^{93}\ w^{155}\ w^{33}\ w^{26}\ 2\ w^{235} \\ w^{24}\ w^{240}\ w^{278}\ w^{206}\ 11\ 10\ 1\ 0\ w^{206}\ w^{26}\ w^{103}\ w^{158}\ w^{87}\ w^{92} \\ w^{83}\ w^{11}\ w^{34}\ w^{250}\ w^{30}\ w^{246}\ 9\ 2\ 1\ 0\ w^{106}\ w^{59}\ w^{283}\ w^{264} \\ w^{80}\ w^{8}\ w^{256}\ w^{184}\ w^{257}\ w^{185}\ 9\ 2\ w^{29}\ w^{245}\ 1\ 0\ w^{86}\ w^{141} \\ w^{225}\ w^{153}\ w^{251}\ w^{179}\ w^{39}\ w^{255}\ w^{266}\ w^{194}\ w^{282}\ w^{210}\ w^{70}\ w^{286}\ 1\ 13 \end{pmatrix}$$

Example III.22. Let w be a primitive element of $GF(19^2)$ whose minimal polynomial is $x^2 - x + 2$. Define $c = w^{\frac{361-1}{4}} = w^{90}$ so that $c^2 = -1$. We give below a generator matrix $G_4^{361,E}$ for a Euclidean self-dual MDS $[14, 7, 8]$ code over $GF(361)$.

$$\begin{pmatrix} 1\ 0\ w^{292}\ w^{34}\ w^{8}\ w^{7}\ w^{72}\ w^{184}\ w^{165}\ w^{67}\ w^{112}\ w^{126}\ w^{239}\ w^{235} \\ w^{219}\ w^{129}\ 1\ 0\ w^{232}\ w^{42}\ w^{81}\ w^{121}\ 8\ w^{61}\ w^{104}\ 16\ w^{161}\ w^{262} \\ w^{207}\ w^{117}\ w^{136}\ w^{46}\ 1\ 0\ w^{31}\ w^{278}\ w^{59}\ w^{263}\ w^{175}\ w^{246}\ w^{306}\ w^{316} \\ w^{56}\ w^{326}\ w^{39}\ w^{309}\ w^{262}\ w^{172}\ 1\ 0\ w^{318}\ w^{14}\ w^{147}\ w^{306}\ w^{203}\ w^{124} \\ w^{311}\ w^{221}\ w^{182}\ w^{92}\ w^{239}\ w^{149}\ w^{28}\ w^{298}\ 1\ 0\ w^{241}\ w^{69}\ w^{211}\ w^{281} \\ w^{355}\ w^{265}\ w^{10}\ 6\ w^{255}\ w^{165}\ 14\ w^{50}\ w^{87}\ w^{357}\ 1\ 0\ w^{102}\ w^{25} \\ w^{291}\ w^{201}\ w^{298}\ w^{208}\ 11\ w^{150}\ w^{16}\ w^{286}\ w^{137}\ w^{47}\ w^{287}\ w^{197}\ 1\ w^{90} \end{pmatrix}$$

Example III.23. Let w be a primitive element of $GF(23^2)$ whose minimal polynomial is $x^2 - 2x + 5$. Define $c = w^{\frac{529-1}{4}} = w^{132}$ so that $c^2 = -1$. We give below a generator matrix $G_5^{529,E}$ for a Euclidean self-dual MDS $[14, 7, 8]$ code over $GF(529)$.

$$\begin{pmatrix} 1\ 0\ w^{339}\ w^{128}\ w^{285}\ w^{110}\ w^{190}\ w^{95}\ w^{339}\ w^{52}\ w^{200}\ w^{501}\ w^{93}\ w^{36} \\ w^{372}\ 9\ 1\ 0\ w^{221}\ w^{527}\ w^{413}\ w^{124}\ w^{201}\ w^{285}\ w^{399}\ w^{331}\ w^{440}\ w^{371} \\ w^{104}\ w^{500}\ w^{274}\ w^{142}\ 1\ 0\ w^{98}\ w^{217}\ w^{53}\ w^{301}\ w^{119}\ w^{330}\ w^{256}\ w^{236} \\ w^{156}\ 5\ w^{503}\ w^{371}\ w^{431}\ w^{299}\ 1\ 0\ w^{354}\ w^{115}\ w^{48}\ w^{386}\ w^{319}\ w^{510} \\ w^{181}\ w^{49}\ w^{220}\ w^{88}\ w^{437}\ w^{305}\ 21\ w^{180}\ 1\ 0\ w^{387}\ w^{91}\ w^{242}\ w^{11} \\ w^{41}\ w^{437}\ w^{290}\ w^{158}\ w^{163}\ w^{31}\ w^{92}\ w^{488}\ w^{207}\ w^{75}\ 1\ 0\ w^{148}\ w^{7} \\ w^{83}\ w^{479}\ w^{400}\ w^{268}\ w^{488}\ w^{356}\ w^{297}\ w^{165}\ w^{254}\ w^{12}\ w^{69}\ w^{465}\ 1\ w^{132} \end{pmatrix}$$

We note that Property (ii) holds for Examples III.19–III.23 as in Example III.18.

In a similar manner, we have constructed Euclidean self-dual MDS $[14, 7, 8]$ codes over $GF(25^2)$, $GF(27^2)$, and $GF(29^2)$ satisfying Property (ii) (omitted). We remark that since there exist Euclidean self-dual MDS $[14, 7, 8]$ codes over $GF(29)$ from Example III.6 or [10], these are also Euclidean self-dual MDS $[14, 7, 8]$ codes over $GF(29^2)$.

ACKNOWLEDGMENT

The authors wish to thank one of the referees for her/his valuable comments on the MDS $[10, 5, 6]$ codes over GF(9) in Example III.4.

REFERENCES

[1] E. Artin, *Geometric Algebra*, Interscience Publishers, Inc., New York-London, 1957

[2] T. Baicheva, I. Bouyukliev, S. Dodunekov, and W. Willems, "On the $[10, 5, 6]_9$ Reed-Solomon and Glynn codes", *Mathematica Balkanica,* New Series, vol. 18, pp. 67–78, 2004.

[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, pp. 37–58, 2003.

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

[5] M.A. De Boer, "Almost MDS codes," *Designs, Codes and Cryptography*, vol. 9, pp. 143–155, 1996.

[6] S. Dodunekov and I.N. Landjev, "On near-MDS codes," *J. Geom.*, vol. 54, No. 1-2, pp. 30–43, 1995.

[7] S. Georgiou and C. Koukouvinos, "MDS self-dual codes over large prime fields," *Finite Fields Appl.*, vol. 8, pp. 455–470, 2002.

[8] D.G. Glynn, "The non-classical 10-arc of PG(4,9)," *Discrete Math.*, vol. 59, pp. 43–51, 1986.

[9] M. Grassl, Code tables: Bounds on the parameters of various types of codes, http://www.codetables.de.

[10] M. Harada and H. Kharaghani, "Orthogonal designs and MDS self-dual codes," *Austral. J. Combin.*, vol. 35, pp. 57–67, 2006.

[11] W.C. Huffman and V.S. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press, Cambridge, UK, 2003.

[12] J.-L. Kim and Y. Lee, "Euclidean and Hermitian self-dual MDS codes over large finite fields," *J. Combin. Theory Ser. A,* vol. 105, pp. 79–95, 2004.

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

[14] 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., Elsevier, Amsterdam, The Netherlands.

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

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

Biographies

T. Aaron Gulliver:

T. Aaron Gulliver (SM'01) received the Ph.D. degree in Electrical Engineering from the University of Victoria, Victoria, BC, Canada in 1989. From 1989 to 1991 he was employed as a Defence Scientist at Defence Research Establishment Ottawa, Ottawa, ON, Canada. He has held academic positions at Carleton University, Ottawa, and the University of Canterbury, Christchurch, New Zealand. He joined the University of Victoria in 1999 and is a Professor in the Department of Electrical and Computer Engineering.

In 2002, he became a Fellow of the Engineering Institute of Canada. He was registration chair for the 1995 IEEE International Symposium on Information Theory which was held in Whistler, BC, Canada. In 2001 and 2005, he was the co-chair of the IEEE Pacific Rim Conference on Communications, Computers and Signal Processing. He was also the co-chair of the 2003 IEEE Information Theory Workshop held in Paris. He has been on the organizing committees of numerous other international conferences. He is currently an Editor for IEEE Transactions on Wireless Communications. From 2000-2003, he was Secretary and a member of the Board of Governors of the IEEE Information Theory Society.

His research interests include source coding, error correcting codes, cryptography, iterative codes and decoding, wireless, ad hoc and sensor networks, cognitive radio, MIMO systems and space-time coding, and ultra wideband communications.

Jon-Lark Kim:

Jon-Lark Kim (S'01–A'03) received the B.S. degree in Mathematics from POSTECH, Pohang, Korea, in 1993, the M.S. degree in Mathematics from Seoul National University, Seoul, Korea, in 1997, and the Ph.D. degree in Mathematics from the University of Illinois at Chicago, in 2002 under the guidance of Professor Vera Pless. From 2002 to 2005, he was with the Department of Mathematics at the University of Nebraska-Lincoln as a Research Assistant Professor. Since 2005, he has been an Assistant Professor in the Department of Mathematics at the University of Louisville, KY.

He was awarded a 2004 Kirkman Medal of the Institute of Combinatorics and its Applications. He is a member of the editorial board of the International J. of Information and Coding Theory. His areas of interest include algebraic coding theory with connections to combinatorics, graph theory, finite geometry, number theory, algebraic geometry, and quantum information.

Yoonjin Lee:

Yoonjin Lee received the B.S. degree in Mathematics Education from Ewha W. University, Korea, in 1992, the M.S. degree in Mathematics from Ewha W. University in 1994, and the Ph.D. degree in Mathematics from Brown University, Providence, US, in 1999 under the supervision of Professor Michael Rosen. Since getting her doctoral degree, she has worked as a faculty member of the Department of Mathematics at several universities is US and Cananda such as Arizona State University (1999-2000), University of Delware (2000-2002), Smith College (2002-2005) and very recently at Simon Fraser University (2005-2007). In the fall of 2007, she joined the Department of Mathematics of Ewha W. University, which is her alma mater.

Her research centers on Algebraic Number Theory with emphasis on the following aspects: Arithmetic of algebraic function fields, Drinfeld modules and torsions of elliptic curves. She is also very interested in Algebraic Coding Theory and pairing-based cryptography.