Scientific Research Publishing

Advances in Pure Mathematics, 2017, 7, 325-333
http://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

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

Hongxi Tong, Xiaoqing Wang

Department of Mathematics, Shanghai University, Shanghai, China
Email: tonghx@shu.edu.cn, 2625453656@qq.com

How to cite this paper: Tong, H.X. and Wang, X.Q. (2017) New MDS Euclidean and Hermitian Self-Dual Codes over Finite Fields. *Advances in Pure Mathematics*, **7**, 325-333.
https://doi.org/10.4236/apm.2017.75019

Received: April 12, 2017
Accepted: May 7, 2017
Published: May 10, 2017

Abstract

In this paper, we construct MDS Euclidean self-dual codes which are extended cyclic duadic codes. And we obtain many new MDS Euclidean self-dual codes. We also construct MDS Hermitian self-dual codes from generalized Reed-Solomon codes and constacyclic codes.

Keywords

MDS Euclidean Self-Dual Codes, MDS Hermitian Self-Dual Codes, Constacyclic Codes, Cyclic Duadic Codes, Generalized Reed-Solomon Codes

1. Introduction

Let $\mathbb{F}_q$ denote a finite field with q elements. An $[n,k,d]$ linear code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. These parameters n, k and d satisfy $d \le n-k+1$. If $d = n-k+1$, C is called a maximum distance separable (MDS) code. MDS codes are of practical and theoretical importance. For examples, MDS codes are related to geometric objects called n-arcs.

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

$$C^{\perp} := \left\{ x \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i y_i = 0, \forall y \in C \right\}. \tag{1}$$

If $q = r^2$, the Hermitian dual code $C^{\perp H}$ of C is defined as

$$C^{\perp H} := \left\{ x \in \mathbb{F}_{r^2}^n : \sum_{i=1}^{n} x_i y_i^r = 0, \forall y \in C \right\}. \tag{2}$$

If C satisfies $C = C^{\perp}$ or $C = C^{\perp H}$, C is called Euclidean self-dual or Hermitian self-dual, respectively. In [1] [2] discussing Euclidean self-dual codes or Hermitian self-dual codes. If C is MDS and Euclidean self-dual or Hermitian self-dual, C is called an MDS Euclidean self-dual code or an MDS Hermitian self-dual code, respectively. In recent years, In [2]-[9] study the MDS self-dual codes. One of these problems in this topic is to determine existence of MDS self-dual codes. When $2 \mid q$, Grassl and Gulliver completely solve the existence of MDS Euclidean self-dual codes in [5]. In [6], Guenda obtain some new MDS Euclidean self-dual codes and MDS Hermitian self-dual codes. In [8], Jin and Xing obtain some new MDS Euclidean self-dual codes from generalized Reed-Solomon codes.

In this paper, we obtain some new Euclidean self-dual codes by studying the solution of an equation in $\mathbb{F}_q$. And we generalize Jin and Xing's results to MDS Hermitian self-dual codes. We also construct MDS Hermitian self-dual codes from constacyclic codes. We discuss MDS Hermitian self-dual codes obtained from extended cyclic duadic codes and obtain some new MDS Hermitian self-dual codes.

2. MDS Euclidean Self-Dual Codes

A cyclic code C of length n over $\mathbb{F}_q$ can be considered as an ideal, $\langle g(x)\rangle$, of the ring $R=\frac{\mathbb{F}_q[x]}{x^n-1}$, where $g(x) \mid x^n-1$ and $(n,q)=1$. The set $T=\left\{0\le i\le n-1 \mid g\left(\alpha^i\right)=0\right\}$ is called the defining set of C, where $ord\,\alpha=n$.

Let S_1 and S_2 be unions of cyclotomic classes modulo n, such that $S_1\cap S_2=\varnothing$ and $S_1\cup S_2=\mathbb{Z}_n\setminus\{0\}$ and $aS_i\,(\bmod n)=S_{i+1(\bmod 2)}$. Then the triple μ_a, S_1 and S_2 is called a splitting modulo n. Odd-like codes D_1 and D_2 are cyclic codes over $\mathbb{F}_q$ with defining sets S_1 and S_2, respectively. D_1 and D_2 can be denoted by $\mu_a(D_i)=D_{i+1(\bmod 2)}$. Even-like duadic codes C_1 and C_2 are cyclic codes over $\mathbb{F}_q$ with defining sets $\{0\}\cup S_1$ and $\{0\}\cup S_2$, respectively. Obviously, $\mu_a(C_i)=C_{i+1(\bmod 2)}$. In [10], A duadic code of length n over $\mathbb{F}_q$ exists if and only if q is a quadratic residue modulo n.

Let $n \mid q-1$ and n be an odd integer. D_1 is a cyclic code with defining set $T=\left\{1,2,\cdots,\frac{n-1}{2}\right\}$. Then D_1 is an $\left[n,\frac{n+1}{2},\frac{n+1}{2}\right]$ MDS code. Its dual $C_1=D_1^{\perp}$ is also cyclic with defining set $T\cup\{0\}$. There are a pair of odd-like duadic codes $D_1=C_1^{\perp}$ and $D_2=C_2^{\perp}$ and a pair of even-like duadic codes $C_2=\mu_{-1}(C_1)$.

Lemma 1 [6] Let $n \mid q-1$ and n be an odd integer. There exists a pair of MDS codes D_1 and D_2 with parameters $\left[n,\frac{n+1}{2},\frac{n+1}{2}\right]$, and $\mu_{-1}(D_i)=D_{i+1(\bmod 2)}$.

Lemma 2 [11] Let D_1 and D_2 be a pair of odd-like duadic codes of length n over $\mathbb{F}_q$, $\mu_{-1}(D_i)=D_{i+1(\bmod 2)}$. Assume that

$$1+\gamma^2 n=0 \tag{*}$$

has a solution in $\mathbb{F}_q$. Let $\tilde{D}_i=\{\tilde{c} \mid c\in D_i\}$ for $1\le i\le 2$ and $\tilde{c}=(c_0,c_1,\cdots,c_{n-1},c_\infty)$ with $c_\infty=-\gamma\sum_{i=0}^{n-1}c_i$. Then $\tilde{D}_1$ and $\tilde{D}_2$ are Euclidean self-dual codes.

In [11], the solution of (*) is discussed when n is an odd prime. In [5], the solution of (*) is discussed when n is an odd prime power. Next, we discuss the solution of (*) for any odd integer n with $n \mid q-1$.

Definition 1 (Legendre Symbol) [12] Let p be an prime and a be an integer.

$$\left(\frac{a}{p}\right)=\begin{cases}0, & \text{if } a\equiv 0 \pmod{p},\\ 1, & \text{if } a(\neq 0) \text{ is a quadratic residue modulo } p,\\ -1, & \text{if } a \text{ is not a quadratic residue modulo } p.\end{cases} \tag{3}$$

Proposition 1 [12]

$$\left(\frac{a}{p}\right)=\left(\frac{p_1}{p}\right)\cdots\left(\frac{p_s}{p}\right),$$

where $a = p_1 \cdots p_s$.

Definition 2 (Jacobi Symbol) [12] Let m and $n(\neq 0)$ be two integers.

$$\left(\frac{m}{n}\right)=\left(\frac{m}{p_1}\right)\cdots\left(\frac{m}{p_h}\right),$$

where $n = p_1 \cdots p_h$.

We cannot obtain $m(\neq 0)$ is a quadratic residue modulo n from $\left(\frac{m}{n}\right)=1$. But we have the next proposition.

Proposition 2 Let $m(\neq 0)$ and n be two integers and $(m,n)=1$. If m is a quadratic residue modulo n, then

$$\left(\frac{m}{n}\right)=1.$$

If

$$\left(\frac{m}{n}\right)=-1,$$

then m is not a quadratic residue modulo n.

Proof Obviously.

Lemma 3 (Law of Quadratic Reciprocity) [12] Let p and r be odd primes, $(p,r)=1$.

$$\left(\frac{p}{r}\right)\left(\frac{r}{p}\right)=(-1)^{\frac{r-1}{2}\cdot\frac{p-1}{2}}. \tag{4}$$

Corollary 1 Let p and r be odd primes.

(1) When $p\equiv 1 \pmod 4$ or $r \equiv 1 \pmod 4$,

$$\left(\frac{p}{r}\right)=\left(\frac{r}{p}\right).$$

(2) When $p \equiv r \equiv 3 \pmod 4$,

$$\left(\frac{p}{r}\right)=-\left(\frac{r}{p}\right).$$

Theorem 1 Let $q = r^t$ and r be an odd prime. Let $n \mid q-1$ and n be an odd integer. And

$$n = p_1^{e_1} \cdots p_s^{e_s} p_{s+1}^{e_{s+1}} \cdots p_h^{e_h},$$

where

$$p_1 \equiv \cdots \equiv p_s \equiv 3 \pmod 4, \quad p_{s+1} \equiv \cdots \equiv p_h \equiv 1 \pmod 4.$$

(1) When $q \equiv 1 \pmod 4$, there is a solution to (*) in $\mathbb{F}_q$.

(2) Let $q \equiv 3 \pmod 4$. If $\sum_{i=1}^{s} e_i$ is an odd integer, there is a solution to (*) in $\mathbb{F}_q$.

Proof (1) $q \equiv 1 \pmod 4$.

(1.1) $r \equiv 3 \pmod 4$. So we have that t is even. Then every quadratic equation with coefficients in $\mathbb{F}_r$, such as Eq. (*), has a solution in $\mathbb{F}_{r^2} \subseteq \mathbb{F}_q$.

(1.2) $r \equiv 1 (\bmod 4)$ and $2 \mid t$. The proof is similar as (1.1).

(1.3) $r \equiv 1 (\bmod 4)$ and $2 \nmid t$.

$$1 = \left(\frac{q}{n}\right) = \left(\frac{r}{n}\right) = \left(\frac{r}{p_1}\right)^{e_1} \cdots \left(\frac{r}{p_h}\right)^{e_h} = \left(\frac{p_1}{r}\right)^{e_1} \cdots \left(\frac{p_h}{r}\right)^{e_h} = \left(\frac{n}{r}\right).$$

So n is a quadratic residue modulo r. And -1 is a quadratic residue modulo r. So there is a solution to (*) in $\mathbb{F}_q$.

(2) $q \equiv 3 \pmod 4$. Then $r \equiv 3 \pmod 4$ and t is odd.

$$\begin{aligned} 1 &= \left(\frac{q}{n}\right) = \left(\frac{r}{n}\right) = \left(\frac{r}{p_1}\right)^{e_1} \cdots \left(\frac{r}{p_s}\right)^{e_s} \left(\frac{r}{p_{s+1}}\right)^{e_{s+1}} \cdots \left(\frac{r}{p_h}\right)^{e_h} \\ &= (-1)^{e_1} \left(\frac{p_1}{r}\right)^{e_1} \cdots (-1)^{e_s} \left(\frac{p_s}{r}\right)^{e_s} \left(\frac{p_{s+1}}{r}\right)^{e_{s+1}} \cdots \left(\frac{p_h}{r}\right)^{e_h} \\ &= (-1)^{\sum_{i=1}^{s} e_i} \left(\frac{p_1}{r}\right)^{e_1} \cdots \left(\frac{p_s}{r}\right)^{e_s} \left(\frac{p_{s+1}}{r}\right)^{e_{s+1}} \cdots \left(\frac{p_h}{r}\right)^{e_h} = (-1)^{\sum_{i=1}^{s} e_i} \left(\frac{n}{r}\right). \end{aligned}$$

If $\sum_{i=1}^{s} e_i$ is odd, n is not a quadratic residue modulo r. And -1 is not a quadratic residue modulo r. So $-n$ is a quadratic residue modulo r. There is a solution to (*) in $\mathbb{F}_q$.

Remark In fact, $n \mid q-1$, and n is an odd integer and $q \equiv 3 \pmod 4$. We can easily prove that there is a solution to (*) in $\mathbb{F}_q$ if and only if $\sum_{i=1}^{s} e_i$ is an odd integer.

Let $n \mid q-1$, $q \equiv 1 \pmod n$. q is a quadratic residue modulo n. $y^2 \equiv q \pmod n$. Let $q = r^t$ and $q \equiv 3 \pmod 4$, where r is a prime. Then $r \equiv 3 (\bmod 4)$ and t is odd. Equation (*) has solutions in $\mathbb{F}_q$ if and only if Equation (*) has solutions in $\mathbb{F}_r$. And r is a quadratic residue modulo n. $\left(yr^{-\frac{t-1}{2}}\right)^2 \equiv r \pmod n$. Let p be an odd prime divisor of n. r is a quadratic residue modulo p. Then $\left(\frac{r}{p}\right) = 1$. By Law of Quadratic Reciprocity, $p \mid n$,

$$\left(\frac{p}{r}\right) = \begin{cases} 1, & p \equiv 1 \pmod 4 \\ -1, & p \equiv 3 \pmod 4 \end{cases}.$$

The Legendre symbol

$$\left(\frac{-n}{r}\right)=\left(\frac{-1}{r}\right)\left(\frac{p_1}{r}\right)^{e_1}\cdots\left(\frac{p_s}{r}\right)^{e_s}\left(\frac{p_{s+1}}{r}\right)^{e_{s+1}}\cdots\left(\frac{p_h}{r}\right)^{e_h}$$
$$=\left(-1\right)^{1+\sum_{i=1}^{s}e_i}=\begin{cases}1, & \sum_{i=1}^{s}e_i \text{ is odd}\\ -1, & \sum_{i=1}^{s}e_i \text{ is even}\end{cases},$$

where $n=p_1^{e_1}\cdots p_s^{e_s}p_{s+1}^{e_{s+1}}\cdots p_h^{e_h}$, $p_1\equiv\cdots\equiv p_s\equiv 3\left(\bmod 4\right)$ and $p_{s+1}\equiv\cdots\equiv p_h\equiv 1\left(\bmod 4\right)$.

Theorem 2 Let $q=r^t$ be a prime power, $n\mid q-1$ and n be an odd integer. Then there exists a pair D_1, D_2 of MDS odd-like duadic codes of length n and $\mu_{-1}\left(D_i\right)=D_{i+1(\bmod 2)}$, where even-like duadic codes are MDS self-orthogonal, and $T_1=\left\{1,\cdots,\frac{n-1}{2}\right\}$. Furthermore,

(1) If $q=2^t$, then $\tilde{D}_i$ are $\left[n+1,\frac{n+1}{2},\frac{n+3}{2}\right]$ MDS Euclidean self-dual codes.

(2) If $q\equiv 1\left(\bmod 4\right)$, then $\tilde{D}_i$ are $\left[n+1,\frac{n+1}{2},\frac{n+3}{2}\right]$ MDS Euclidean self-dual codes.

(3) If $q\equiv 3\left(\bmod 4\right)$ and $\sum_{i=1}^{s}e_i$ is an odd integer, then $\tilde{D}_i$ are $\left[n+1,\frac{n+1}{2},\frac{n+3}{2}\right]$ MDS Euclidean self-dual codes, where $n=p_1^{e_1}\cdots p_s^{e_s}p_{s+1}^{e_{s+1}}\cdots p_t^{e_h}$ and $p_1\equiv\cdots\equiv p_s\equiv 3\left(\bmod 4\right)$, $p_{s+1}\equiv\cdots\equiv p_h\equiv 1\left(\bmod 4\right)$.

Proof Obviously, D_i are $\left[n,\frac{n+1}{2},\frac{n+1}{2}\right]$ MDS odd-like duadic codes. If there is a solution to (*), we want to prove $\tilde{D}_i$ are $\left[n+1,\frac{n+1}{2},\frac{n+3}{2}\right]$ MDS Euclidean self-dual codes, and we only need to prove that

$$c\in D_i \text{ and } wt\left(c\right)=\frac{n+1}{2}, \text{ then } wt\left(\tilde{c}\right)=\frac{n+1}{2}+1.$$

This is equivalent to prove that $c_\infty\neq 0$. It can be proved similarly by which proved in [5].

When $q=2^t$, there is a solution to (*) in $\mathbb{F}_{2^t}$, $\tilde{D}_i$ are $\left[n+1,\frac{n+1}{2},\frac{n+3}{2}\right]$ MDS Euclidean self-dual codes by Lemma 2.

We can obtain (2) and (3) from Theorem 1 and Lemma 2. Theorem 2 is proved.

We list some new MDS Euclidean self-dual codes in the next Table 1.

3. MDS Hermitian Self-Dual Codes

Let $n\le q^2$. We choose n distinct elements $\left\{\alpha_1,\cdots,\alpha_n\right\}$ from $\mathbb{F}_{q^2}$ and n non-zero elements $\left\{v_1,\cdots,v_n\right\}$ from $\mathbb{F}_{q^2}$. The generalized Reed-Solomon code

Table 1. Some new MDS Euclidean self-dual codes.

n	q
4	2^2, 7
6	2^4, 3^4
8	2^3, 3^6
10	2^6, 5^6
12	3^5
14	2^{12}, 3^6
16	31, 31^2, 31^3
18	3^{16}
20	5^9
22	5^6
24	3^{11}
26	7^4
28	7^9
30	59
156	5^4

$$GRS_k(\alpha, v) := \left\{ \left(v_1 f(\alpha_1), \cdots, v_n f(\alpha_n) \right) : f(x) \in \mathbb{F}_{q^2}[x], \deg f(x) \le k-1 \right\}$$

is a q^2-ary $[n, k, n-k+1]$ MDS code, where $\alpha = (\alpha_1, \cdots, \alpha_n)$ and $v = (v_1, \cdots, v_n)$.

Theorem 3 Let $n \le q$ and $2 \mid n$. Let $\{\alpha_1, \cdots, \alpha_n\}$ be n distinct elements from $\mathbb{F}_q \left(\subseteq \mathbb{F}_{q^2} \right)$ and $u_i = \prod_{1 \le j \le n, j \ne i} \left(\alpha_i - \alpha_j \right)^{-1}$, $1 \le i \le n$. Then there exist $v_i \in \mathbb{F}_{q^2}$ such that $u_i = v_i^2$, for $i = 1, \cdots, n$, and the generalized Reed-Solomon code $GRS_{\frac{n}{2}}(\alpha, v)$ is an $\left[n, \frac{n}{2}, \frac{n}{2}+1 \right]$ MDS Hermitian self-dual code over $\mathbb{F}_{q^2}$, where $\alpha = (\alpha_1, \cdots, \alpha_n)$ and $v = (v_1, \cdots, v_n)$.

Proof Obviously, $u_i (\ne 0) \in \mathbb{F}_q \left(\subseteq \mathbb{F}_{q^2} \right)$ for $1 \le i \le n$. So there exist $v_i (\ne 0) \in \mathbb{F}_{q^2}$ such that $u_i = v_i^2$ for $1 \le i \le n$. The generalized Reed-Solomon code $GRS_{\frac{n}{2}}(\alpha, v)$ is an $\left[n, \frac{n}{2}, \frac{n}{2}+1 \right]$ MDS code over $\mathbb{F}_{q^2}$. For proving the generalized Reed-Solomon code $GRS_{\frac{n}{2}}(\alpha, v)$ is Hermitian self-dual over $\mathbb{F}_{q^2}$, we only prove

$$\left(v_1 \alpha_1^l, \cdots, v_n \alpha_n^l \right) \cdot \left(v_1^q \alpha_1^{kq}, \cdots, v_n^q \alpha_n^{kq} \right) = 0, \ 0 \le l, k \le \frac{n}{2} - 1.$$

From the choose of α_i, v_i and [8, Corollary 2.3],

$$\begin{aligned} &\left(v_1 \alpha_1^l, \cdots, v_n \alpha_n^l \right) \cdot \left(v_1^q \alpha_1^{kq}, \cdots, v_n^q \alpha_n^{kq} \right) \\ &= \left(v_1 \alpha_1^l, \cdots, v_n \alpha_n^l \right) \cdot \left(v_1 \alpha_1^k, \cdots, v_n \alpha_n^k \right) = 0, \ 0 \le l, k \le \frac{n}{2} - 1. \end{aligned}$$

So the generalized Reed-Solomon code $GRS_{\frac{n}{2}}(\alpha,v)$ is an $\left[n,\frac{n}{2},\frac{n}{2}+1\right]$ MDS Hermitian self-dual code over $\mathbb{F}_{q^2}$.

Next we construct MDS Hermitian self-dual codes from constacyclic codes.

Let C be an $[n,k]$ λ-constacyclic code over $\mathbb{F}_{q^2}$ and $(n,q)=1$. C is considered as an ideal, $\langle g(x)\rangle$, of $\frac{F_{q^2}[x]}{x^n-\lambda}$, where $g(x)|(x^n-\lambda)$. Simply, $C=\langle g(x)\rangle$.

Lemma 4 [2] Let $\lambda\in\mathbb{F}_{q^2}^*$, $r=\mathrm{ord}_{q^2}(\lambda)$, and C be a λ-constacyclic code over $\mathbb{F}_{q^2}$. If C is Hermitian self-dual, then $r\,|\,q+1$.

Lemma 5 [2] Let $n=2^a n'$ $(a>0)$ and $r=2^b r'$ be integers such that $2\nmid n'$ and $2\nmid r'$. Let q be an odd prime power such that $(n,q)=1$ and $r\,|\,q+1$, and let $\lambda\in\mathbb{F}_{q^2}$ has order r. Then Hermitian self-dual λ-constacyclic codes over $\mathbb{F}_{q^2}$ of length n exist if and only if $b>0$ and $q\not\equiv-1\left(\bmod 2^{a+b}\right)$.

Let $r=\mathrm{ord}_{q^2}(\lambda)$ and $r\,|\,q+1$.

$$O_{r,n}=\{1+rj\mid j=0,1,\cdots,n-1\}.$$

Then $\alpha^i\left(i\in O_{r,n}\right)$ are all solutions of $x^n-\lambda=0$ in some extension field of $\mathbb{F}_{q^2}$, where $\mathrm{ord}\alpha=rn$. C is called a λ-constacyclic code with defining set $T\subseteq O_{r,n}$, if

$$C=\langle g(x)\rangle \text{ and } g\left(\alpha^i\right)=0,\ \forall i\in T.$$

Theorem 4 Let $n=2^a n'(a>0)$ and $r=2^b r'(b>0)$. $rn\,|\,q^2-1$. $\lambda\in\mathbb{F}_{q^2}^*$ with $\mathrm{ord}\lambda=r$. $q\not\equiv-1\left(\bmod 2^{a+b}\right)$. If $rn\,|\,2(q+1)$, there exists an MDS Hermitian self-dual code C over $\mathbb{F}_{q^2}$ with length n, C is a λ-constacyclic code with defining set

$$T=\left\{1+rj\,|\,0\le j\le\frac{n}{2}-1\right\}.$$

Proof If $rn\,|\,q^2-1$, $C_{q^2}(i)=\{i\}$, for $i\in O_{r,n}$, where $C_{q^2}(i)$ denote the q^2-cyclotomic coset of $i \bmod rn$. And $|T|=\frac{n}{2}$, C is an $\left[n,\frac{n}{2},\frac{n}{2}+1\right]$ MDS λ-constacyclic code by the BCH bound of constacyclic code.

When $rn\,|\,2(q+1)$, $q=\frac{rnl}{2}-1$. Because $q\not\equiv-1\left(\bmod 2^{a+b}\right)$, l is odd.

$$(-q)(1+rj)=-q-qrj\equiv1-\frac{rnl}{2}+rj\equiv1+r\left(\frac{n}{2}+j\right)(\bmod rn).$$

So

$$(-q)T\cap T=\varnothing.$$

C is MDS Hermitian self-dual by the relationship of roots of a constacyclic code and its Hermitian dual code's roots.

Remark The MDS Hermitian self-dual constacyclic code obtained from Theorem 4 is different with the MDS Hermitian self-dual constacyclic code in

[12], because $(q+1, q-1) = 2$ for an odd prime power q.

If $r = 2$, C is negacyclic. Theorem 4 can be stated as follow.

Corollary 2 Let $n = 2^a n'(a \geq 1)$ and n' is odd. Let

$$q \equiv -1\left(\bmod 2^a n''\right) \text{ and } q \equiv 2^a - 1\left(\bmod 2^{a+1}\right),$$

where $n' \mid n''$ and n'' is odd. Then there exists an MDS Hermitian self-dual code C of length n which is negacyclic with defining set

$$T = \left\{1 + 2j \mid j = 0, 1, \cdots, \frac{n}{2} - 1\right\}.$$

Especially, when $a = 1$, Corollary 2 is similar as [5, Theorem 11].

From Theorem 3 and Theorem 4, we obtain the next theorem.

Theorem 5 Let $n \leq q+1$ and n be even. There exists an MDS Hermitian self-dual code with length n over $\mathbb{F}_{q^2}$.

4. Conclusion

In this paper, we obtain many new MDS Euclidean self-dual codes by solving the Equation (*) in $\mathbb{F}_q$. We generalize the work of [8] to MDS Hermitian self-dual codes, and we construct new MDS Hermitian self-dual codes from constacyclic codes. We obtain that there exists an MDS Hermitian self-dual code with length n over $\mathbb{F}_{q^2}$, where $n \leq q+1$ and n is even. And we also discuss these MDS Hermitian self-dual codes, which are extended cyclic duadic codes. Some new MDS Hermitian self-dual codes are obtained.

References

[1] Dicuangco, L., Moree, P. and Solé, P. (2007) The Lengths of Hermitian Self-Dual Extended Duadic Codes. *Journal of Pure and Applied Algebra*, **209**, 223-237. https://doi.org/10.1016/j.jpaa.2006.05.024

[2] Yang, Y.S. and Cai, W.C. (2015) On Self-Dual Constacyclic Codes over Finite Fields. *Designs, Codes and Cryptography*, **74**, 355-364. https://doi.org/10.1007/s10623-013-9865-9

[3] Aaron Gulliver, T., Kim, J.L. and Lee, Y. (2008) New MDS or Near-MDS Self-Dual Codes. *IEEE Transactions on Information Theory*, **54**, 4354-4360. https://doi.org/10.1109/TIT.2008.928297

[4] Georgiou, S. and Koukouvinos, C. (2002) MDS Self-Dual Codes over Large Prime Fields. *Finite Fields and Their Applications*, **8**, 455-470. https://doi.org/10.1016/S1071-5797(02)90353-9

[5] Grassel, M. and Aaron Gulliver, T. (2008) On Self-Dual MDS Codes. *Proceedings of ISIT*, Barcelona, 2008, 1954-1957.

[6] Guenda, K. (2012) New MDS Self-Dual Codes over Finite Fields. *Designs, Codes and Cryptography*, **62**, 31-42. https://doi.org/10.1007/s10623-011-9489-x

[7] Harada, M. and Kharaghani, H. (2008) Orthogonal Designs and MDS Self-Dual Codes. *The Australasian Journal of Combinatorics*, **35**, 57-67.

[8] Jin, L.F. and Xing, C.P. (2016) New MDS Self-Dual Codes from Generalized Reed-Solomon Codes. Arxiv: 1601.04467v1

[9] Kim, J.L. and Lee, Y. (2004) Euclidean and Hermitian Self-Dual MDS Codes over Large Finite Fields. *Journal of Combinatorial Theory*, *Series A*, **105**, 79-95.

https://doi.org/10.1016/j.jcta.2003.10.003

[10] Smid, M.H.M. (1983) Duadic Codes. *IEEE Transactions on Information Theory*, **33**, 432-433.

[11] Huffman, W.C. and Pless, V. (2003) Fundamentals of Erro-Correcting Codes. Cambridge University Press, Cambridge. https://doi.org/10.1017/CBO9780511807077

[12] Pang, C.D. and Pang, C.B. (2002) Elementary Number Theory. Beijing University Press, Beijing. (In Chinese)