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

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 \( d \leq n - k + 1 \). If \( d = n - k + 1 \), \( C \) is called a maximum distance separable (MDS) code. MDS codes are of practical and theoretical importance. For example, MDS codes are related to geometric objects called \( n \)-arcs.

The Euclidean dual code \( C^\perp \) of \( C \) is defined as

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

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

\[
C^{\perp H} = \left\{ x \in \mathbb{F}_q^n : \sum_{i=1}^{n} x_i y_i = 0, \forall y \in C \right\}.
\] (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 $R = \mathbb{F}_q[x]/(x^n - 1)$, where $g(x) \mid x^n - 1$ and $(n, q) = 1$. The set $T = \{0 \leq i \leq n-1 \mid g(\alpha^i) = 0\}$ is called the defining set of $C$, where $\text{ord} \alpha = n$.

Let $S_1$ and $S_2$ be unions of cyclotomic classes modulo $n$, such that $S_1 \cap S_2 = \emptyset$ and $S_1 \cup S_2 = \mathbb{Z}_n \setminus \{0\}$ and $aS_1 \mod n = S_{i+1} \mod 2$. Then the triple $\mu_\alpha, S_1$ 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 $\mu_\alpha(D_i) = D_{i+1} \mod 2$. 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, $\mu_\alpha(C_i) = C_{i+1} \mod 2$. 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 $T = \left\{1, 2, \ldots, \frac{n-1}{2}\right\}$. Then $D_1$ is an $\left[\frac{n+1}{2}, \frac{n+1}{2}, 2\right]$ 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 $\left[\frac{n+1}{2}, \frac{n+1}{2}, 2\right]$, and $\mu_{-1}(D_i) = D_{i+1} \mod 2$.

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

$$1 + \gamma^2 n = 0$$

has a solution in $\mathbb{F}_q$. Let $\bar{D}_i = \{\bar{c} \mid c \in D_i\}$ for $1 \leq i \leq 2$ and

$$\bar{c} = (c_0, c_1, \ldots, c_{n-1}, c_n)$$

with $c_w \sim -\gamma \sum_{i=0}^{w-1} c_i$. Then $\bar{D}_1$ and $\bar{D}_2$ 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.

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

(3)

**Proposition 1** [12]

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

where \( a = p_1 \cdots p_s \cdot \).

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

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

where \( n = p_1 \cdots p_h \cdot \)

We cannot obtain \( m \not\equiv 0 \) is a quadratic residue modulo \( n \) from \( \left( \frac{m}{n} \right) = 1 \).

But we have the next proposition.

**Proposition 2** Let \( m \not\equiv 0 \) 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, \((p,r) = 1\).

\[
\left( \frac{p}{r} \right) \left( \frac{r}{p} \right) = (-1)^{\frac{r-1}{2} \cdot \frac{p-1}{2}}.
\]  

(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 \( q = r^i \) and \( r \) be an odd prime. Let \( n \mid q - 1 \) and \( n \) be an odd integer. And
where
\[ n = p_1^{e_1} \cdots p_s^{e_s} q_{s+1}^{e_{s+1}} \cdots q_k^{e_k}, \]

(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) \( q \equiv 3 \pmod{4}. \) So we have that \( t \) is even. Then every quadratic equation with coefficients in \( \mathbb{F}_r, \) such as Eq. (*), has a solution in \( \mathbb{F}_r. \)
(1.2) \( q \equiv 1 \pmod{4} \) and \( 2 \mid t. \) The proof is similar as (1.1).
(1.3) \( q \equiv 1 \pmod{4} \) and \( 2 \nmid t. \)

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

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

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 \( \mathbb{F}_r. \)

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 \( n. \) \( y^2 = q \pmod{n}. \) Let \( q = r^j \) and \( q \equiv 3 \pmod{4}, \) where \( r \) is a prime. Then \( r \equiv 3 \pmod{4} \) and \( t \) is odd. Equation (*) has solutions in \( \mathbb{F}_r \) if and only if Equation (*) has solutions in \( \mathbb{F}_r. \) And \( r \) is a quadratic residue modulo \( n. \)

The Legendre symbol
\[
\left(\frac{-n}{r}\right) = \left(\frac{-1}{r}\right) \left(\frac{p_1}{r}\right)^* \cdots \left(\frac{p_s}{r}\right)^* \left(\frac{p_{s+1}}{r}\right)^* \cdots \left(\frac{p_h}{r}\right)^*
\]

\[
= (-1)^{\sum_{i=1}^{s} e_i} = \begin{cases} 
1, & \sum_{i=1}^{s} e_i \text{ is odd} \\
-1, & \sum_{i=1}^{s} e_i \text{ is even}
\end{cases}
\]

where \( n = p_1^* \cdots p_s^* p_{s+1}^* \cdots p_h^* \), \( p_1 \equiv \cdots \equiv p_s \equiv 3 \pmod{4} \) and \( p_{s+1} \equiv \cdots \equiv p_h \equiv 1 \pmod{4} \).

**Theorem 2** Let \( q = r' \) 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 \( \mu_1(D_i) = D_{s+1}(mod2) \), where even-like duadic codes are MDS self-orthogonal, and \( T_i = \{1, \ldots, n-1\} \). Furthermore,

1. If \( q = 2' \), then \( \tilde{D}_i \) are \( \left[ n+1, \frac{n+1}{2}, \frac{n+3}{2} \right] \) MDS Euclidean self-dual codes.
2. If \( q \equiv 1 \pmod{4} \), then \( \tilde{D}_i \) are \( \left[ n+1, \frac{n+1}{2}, \frac{n+3}{2} \right] \) MDS Euclidean self-dual codes.
3. If \( q \equiv 3 \pmod{4} \) and \( \sum_{i=1}^{s} \) 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 \( n = p_1^* \cdots p_s^* p_{s+1}^* \cdots p_h^* \) and \( p_1 \equiv \cdots \equiv p_s \equiv 3 \pmod{4} \), \( p_{s+1} \equiv \cdots \equiv p_h \equiv 1 \pmod{4} \).

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

This is equivalent to prove that \( c_{\alpha} \neq 0 \). It can be proved similarly by which proved in [5].

When \( q = 2' \), there is a solution to (*) in \( \mathbb{F}_{q'} \), \( \tilde{D}_i \) 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 \( n \leq q^2 \). We choose \( n \) distinct elements \( \{\alpha_1, \cdots, \alpha_n\} \) from \( \mathbb{F}_q \) and \( n \) non-zero elements \( \{v_1, \cdots, v_n\} \) from \( \mathbb{F}_{q^2} \). The generalized Reed-Solomon code
Table 1. Some new MDS Euclidean self-dual codes.

<table>
<thead>
<tr>
<th>n</th>
<th>q</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$2^1, 7$</td>
</tr>
<tr>
<td>6</td>
<td>$2^1, 3^4$</td>
</tr>
<tr>
<td>8</td>
<td>$2^1, 3^4$</td>
</tr>
<tr>
<td>10</td>
<td>$2^1, 5^6$</td>
</tr>
<tr>
<td>12</td>
<td>$3^1$</td>
</tr>
<tr>
<td>14</td>
<td>$2^{15}, 3^4$</td>
</tr>
<tr>
<td>16</td>
<td>$31, 31^2, 31^3$</td>
</tr>
<tr>
<td>18</td>
<td>$3^{16}$</td>
</tr>
<tr>
<td>20</td>
<td>$5^8$</td>
</tr>
<tr>
<td>22</td>
<td>$5^8$</td>
</tr>
<tr>
<td>24</td>
<td>$3^{11}$</td>
</tr>
<tr>
<td>26</td>
<td>$7^4$</td>
</tr>
<tr>
<td>28</td>
<td>$7^9$</td>
</tr>
<tr>
<td>30</td>
<td>$59$</td>
</tr>
<tr>
<td>156</td>
<td>$5^4$</td>
</tr>
</tbody>
</table>

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

\[ GRS_n(\alpha, v) := \left\{ (v_1 f(\alpha_1), \ldots, v_n f(\alpha_n)) : f(x) \in \mathbb{F}_q[x], \deg f(x) \leq k-1 \right\} \]

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

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

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

\[ \left(v_1 \alpha_i^l, \ldots, v_n \alpha_i^l \right) \cdot \left(v_1 \alpha_i^k, \ldots, v_n \alpha_i^k \right) = 0, \quad 0 \leq l, k \leq \frac{n}{2} - 1. \]

From the choose of \( \alpha_i, v_i \), and [8, Corollary 2.3],

\[ \left(v_1 \alpha_i^l, \ldots, v_n \alpha_i^l \right) \cdot \left(v_1 \alpha_i^k, \ldots, v_n \alpha_i^k \right) = \left(v_1 \alpha_i^l, \ldots, v_n \alpha_i^l \right) \cdot \left(v_1 \alpha_i^k, \ldots, v_n \alpha_i^k \right) = 0, \quad 0 \leq l, k \leq \frac{n}{2} - 1. \]
So the generalized Reed-Solomon code $GRS_n(\alpha, v)$ is an $\begin{bmatrix} n & n \frac{n}{2} \frac{n}{2} + 1 \end{bmatrix}$

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 $\begin{bmatrix} n & k \end{bmatrix}$ $\lambda$-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 $\lambda \in \mathbb{F}_q^*$, $r = \text{ord}_q(\lambda)$, and $C$ be a $\lambda$-constacyclic code over $\mathbb{F}_{q^2}$. If $C$ is Hermitian self-dual, then $r \mid q + 1$.

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

Let $r = \text{ord}_{q^2}(\lambda)$ and $r \mid q + 1$.

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

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

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

**Theorem 4** Let $n = 2^r n' (a > 0)$ and $r = 2^s r' (b > 0)$. $rn \mid q^2 - 1$. $\lambda \in \mathbb{F}_{q^2}$ with $\text{ord}\lambda = r$. $q \not\equiv -1 (\text{mod } 2^{a+b})$. If $rn \mid 2(q + 1)$, there exists an MDS Hermitian self-dual code $C$ over $\mathbb{F}_{q^2}$ with length $n$, $C$ is a $\lambda$-constacyclic code with defining set $T = \{1 + rj \mid 0 \leq j \leq \frac{n}{2} - 1\}$.

Proof If $rn \mid q^2 - 1$, $C_{q^2}(i) = \{i\}$, for $i \in O_{r, n}$, where $C_{q^2}(i)$ denote the $q^2$-cyclotomic coset of $i \text{mod } rn$. And $|T| = \frac{n}{2}$, $C$ is an $\begin{bmatrix} n & n \frac{n}{2} \frac{n}{2} + 1 \end{bmatrix}$ MDS $\lambda$-constacyclic code by the BCH bound of constacyclic code.

When $rn \mid 2(q + 1)$, $q = \frac{rn}{2} - 1$. Because $q \not\equiv -1 (\text{mod } 2^{a+b})$, $l$ is odd.

$(-q)(1 + rj) = -q - qrfj = 1 - \frac{rn}{2} + rj = 1 + r\left(\frac{n}{2} + j\right) (\text{mod } rn)$.

So $(-q)T \cap T = \emptyset$.

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

$$q = -1 \left( \mod 2^an' \right)$$

and

$$q = 2^a - 1 \left( \mod 2^{a+1} \right),$$

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

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

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


