Des. Codes Cryptogr. (2015) 74:355–364
DOI 10.1007/s10623-013-9865-9

On self-dual constacyclic codes over finite fields

Yiansheng Yang · Wenchao Cai

Received: 7 March 2012 / Revised: 9 July 2013 / Accepted: 9 July 2013 /
Published online: 19 July 2013

Abstract This paper is devoted to the study of self-dual codes arising from constacyclic codes. Necessary and sufficient conditions are given for the existence of Hermitian self-dual constacyclic codes over $\mathbb{F}_{q^2}$ of length n. As an application of these necessary and sufficient conditions, some conditions under which MDS Hermitian self-orthogonal and self-dual constacyclic codes exist are obtained.

Keywords Constacyclic codes · Self-dual codes · MDS codes

Mathematics Subject Classification 94B05 · 94B15

1 Introduction

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements. An $[n, k]$ linear code C of length n over $\mathbb{F}_q$ is a k-dimensional subspace of the vector space $\mathbb{F}_q^n$. We call $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1}) \in C$ a codeword. The Hamming weight $w(\mathbf{c})$ of $\mathbf{c} \in \mathbb{F}_q^n$ is the number of nonzero coordinates of $\mathbf{c}$. The minimum distance of C is defined to be $d = \min\{w(\mathbf{c}) \mid 0 \neq \mathbf{c} \in C\}$. An $[n, k, d]$ code, which is defined to be an $[n, k]$ code with the minimum distance d, is said to be *maximum distance separable* (MDS) if $d = n - k + 1$. The Euclidean dual code of C is defined to be $C^{\perp} = \{\mathbf{x} \in \mathbb{F}_q^n \mid \sum_{i=0}^{n-1} x_i y_i = 0, \forall \mathbf{y} \in C\}$. A code C is *Euclidean self-orthogonal* provided $C \subseteq C^{\perp}$ and *Euclidean self-dual* provided $C = C^{\perp}$. Let $(\mathbf{x}, \mathbf{y})_H = \sum_{i=0}^{n-1} x_i y_i^q$ be *the Hermitian inner product* of $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, and C be a code of length n over $\mathbb{F}_{q^2}$. The Hermitian dual code $C^{\perp H}$ of C is defined by $C^{\perp H} = \{\mathbf{x} \in \mathbb{F}_{q^2}^n \mid \sum_{i=0}^{n-1} x_i y_i^q = 0, \forall \mathbf{y} \in C\}$. Hermitian self-orthogonality and

Communicated by D. Jungnickel.

Y. Yang · W. Cai (✉)
Department of Mathematics, College of Science, Shanghai University, Shanghai 200444, China
e-mail: wenchao_cai@126.com

Hermitian self-duality are defined as follows: C is *Hermitian self-orthogonal* if $C \subseteq C^{\perp H}$ and *Hermitian self-dual* if $C = C^{\perp H}$.

Let $\alpha \in \mathbb{F}_q^*$. A linear code C is called α-*constacyclic* [2] provided that for each codeword $(c_0, c_1, \dots, c_{n-1})$ in C, $(\alpha c_{n-1}, c_0, \dots, c_{n-2})$ is also a codeword in C. An α-constacyclic code of length n over $\mathbb{F}_q$ corresponds to the principal ideal $\langle g(x) \rangle$ of the quotient ring $\mathbb{F}_q[x]/(x^n - \alpha)$, where $g(x)$ is a divisor of $x^n - \alpha$. Since the cases when the code length n is divisible by the characteristic of $\mathbb{F}_q$ are cases involving repeated root codes, for the remainder of this paper we assume n and q are relatively prime. Because the code length n must be even if there exist Euclidean or Hermitian self-dual codes, we assume q is an odd prime power.

Self-dual codes are an important class of codes which have been extensively studied in coding theory. This paper is mainly concerned with self-dual codes that are constacyclic codes. In recent years, many papers, for example [3,5,6,9], have been written on this subject. Aydin et al. [1] dealt with constacyclic codes and a constacyclic BCH bound was given. In 2008, Gulliver et al. [6] showed that there exists a Euclidean self-dual MDS code of length q over $\mathbb{F}_q$ when $q = 2^m$ by using a Reed-Solomon (RS) code and its extension. They also constructed many new Euclidean and Hermitian self-dual MDS codes over finite fields. In the same year, Blackford [3] studied negacyclic codes over finite fields by using multipliers. He gave conditions on the existence of Euclidean self-dual codes. Recently, Guenda [5] generalized Blackford's work [3]. She constructed MDS Euclidean and Hermitian self-dual codes from extended cyclic duadic or negacyclic codes and gave necessary and sufficient conditions on the existence of Hermitian self-dual negacyclic codes arising from negacyclic codes. In this paper, we extend Guenda's work to constacyclic codes and study the existence of Hermitian self-dual codes. We give conditions on the existence of MDS Hermitian self-orthogonal and self-dual codes.

2 Preliminaries

Throughout this paper, let q be an odd prime power and n be a positive integer relatively prime to q. Let C be an $[n, k]$ α-constacyclic code over $\mathbb{F}_q$; then the code C is a vector space over $\mathbb{F}_q$ and corresponds to an ideal of $\mathbb{F}_q[x]/(x^n - \alpha)$. By abuse of notation, we let C represent both a set of polynomials and a set of vectors.

As mentioned above, a nonzero $[n, k]$ α-constacyclic code C has a unique monic *generator polynomial* $g(x)$ of degree $n - k$, where $g(x) \mid (x^n - \alpha)$. The *roots* of the code C are the roots of $g(x)$. So if $\eta_1, \dots, \eta_{n-k}$ are the zeros of $g(x)$ in the splitting field of $x^n - \alpha$, then $\mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in C$ if and only if $c(\eta_1) = \cdots = c(\eta_{n-k}) = 0$, where $c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$. Let $h(x) = (x^n - \alpha)/g(x) = \sum_{i=0}^{k} h_i x^i$, then $h(x)$ is called the *check polynomial* of C [7,10].

Let $C^{(q)}$ denote the code defined by $C^{(q)} = \{\mathbf{c}^q \mid \forall \mathbf{c} = (c_0, c_1, \dots, c_{n-1}) \in C\}$, where $\mathbf{c}^q = (c_0, c_1, \dots, c_{n-1})^q = (c_0^q, c_1^q, \dots, c_{n-1}^q)$.

Lemma 2.1 ([4, Proposition 2.4]) (i) *Let C be an α-constacyclic code over $\mathbb{F}_q$, then the Euclidean dual code $C^{\perp}$ is an α^{-1}-constacyclic code generated by $g^{\perp}(x) = \sum_{i=0}^{k} h_i h_0^{-1} x^{k-i}$.*

(ii) *Let C be an α-constacyclic code over $\mathbb{F}_{q^2}$, then the Hermitian dual code $C^{\perp H}$ is an α^{-q} -constacyclic code generated by $g^{\perp (q)}(x) = \sum_{i=0}^{k} h_i^q h_0^{-q} x^{k-i}$.*

Proof (i) The proof can be found in [4, Proposition 2.4].

(ii) $g^{\perp}(x)$ is the generator polynomial of $C^{\perp}$. Let C^* denote the code generated by $g^{\perp (q)}(x) = \sum_{i=0}^{k} h_i^q h_0^{-q} x^{k-i}$ and $\xi_1, \dots, \xi_k$ be the zeros of $g^{\perp}(x)$, then $\xi_1^q, \dots, \xi_k^q$ are the zeros of $g^{\perp(q)}(x)$. Thus if $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ is a codeword in C, then we have $c_0 + c_1\xi_i + \cdots + c_{n-1}\xi_i^{n-1} = 0$ $(i = 1, \ldots, k)$. It is obvious that $c_0^q + c_1^q\xi_i^q + \cdots + c_{n-1}^q \left(\xi_i^q\right)^{n-1} = 0$ $(i = 1, \ldots, k)$. This implies that $\left(c_0^q, c_1^q, \ldots, c_{n-1}^q\right)$ is a codeword in C^*. So $C^{\perp H} \subset C^*$. Because $\dim C^{\perp H} = \dim C^* = n - k$, we get $C^* = C^{\perp H}$.

Since $C^{\perp}$ is an α^{-1}-constacyclic code generated by $g^{\perp}(x)$, we have

$$\xi_i^n = \alpha^{-1} \Longrightarrow \left(\xi_i^q\right)^n = \left(\alpha^q\right)^{-1} \; (i = 1, \ldots, k).$$

So $\xi_1^q, \ldots, \xi_k^q$ are roots of $x^n - \alpha^{-q}$, which implies $g^{\perp(q)}(x)$ is a divisor of $x^n - \alpha^{-q}$. Therefore, the Hermitian dual code $C^{\perp H}$ is an α^{-q}-constacyclic code. □

Let $r = ord_q(\alpha)$ (i.e., the smallest integer r such that $\alpha^r = 1$) and the multiplicative order of q modulo rn be m [i.e., the smallest integer m such that $q^m \equiv 1 \pmod{rn}$]. There exists $\delta \in \mathbb{F}_{q^m}^*$, called a primitive rnth root of unity, such that $\delta^n = \alpha$. Let $\zeta = \delta^r$, then ζ is a primitive nth root of unity. Therefore, the roots of $x^n - \alpha$ are $\{\delta, \delta^{1+r}, \ldots, \delta^{1+(n-1)r}\}$ and the roots of $x^n - \alpha^{-1}$ are $\{\delta^{-1}, \delta^{-1+r}, \ldots, \delta^{-1+(n-1)r}\}$. Define $O_{r,n}(1)$ and $O_{r,n}(-1)$ as follows:

$$O_{r,n}(1) = \{ir + 1 \mid 0 \le i \le n-1\} \pmod{rn} \subseteq \mathbb{Z}_{rn};$$
$$O_{r,n}(-1) = \{ir - 1 \mid 0 \le i \le n-1\} \pmod{rn} \subseteq \mathbb{Z}_{rn}.$$

The *defining set* of the α-constacyclic code C is defined as $T = \{ir + 1 \in O_{r,n}(1) \mid \delta^{ir+1}$ is a root of $C\}$. It is clear that $T \subset O_{r,n}(1)$ and the dimension of C is $n - |T|$. Let $Cl_q(s)$ be the *q-cyclotomic coset* modulo rn which contains s, i.e. $Cl_q(s) = \{sq^j \pmod{rn} \mid j \in \mathbb{Z}\}$. Assume the generator polynomial of C is $g(x) = \sum_{i=0}^{k} g_i x^i$, where $g_i \in \mathbb{F}_q$. If $g(\nu) = 0$ for some $\nu \in \mathbb{F}_{q^m}$, then

$$g(\nu^q) = \sum_{i=0}^{k} g_i \left(\nu^q\right)^i = \sum_{i=0}^{k} g_i^q \left(\nu^i\right)^q = \left(\sum_{i=0}^{k} g_i \nu^i\right)^q = (g(\nu))^q = 0.$$

Therefore, the defining set T is a union of some q-cyclotomic cosets modulo rn and a union of some q-cyclotomic cosets modulo rn is also the defining set of some α-constacyclic code.

Proposition 2.2 *There exists a Euclidean self-dual α-constacyclic code over $\mathbb{F}_q$ if and only if $r = 2$.*

Proof By Lemma 2.1, the Euclidean dual code of an α-constacyclic code is an α^{-1}-constacyclic code. To prove that if there is a Euclidean self-dual α-constacyclic code, we need to verify $\alpha^2 = 1$. This indicates that either $r = 1$ or $r = 2$. If $r = 1$, then $\alpha = 1$. It has been proved by Jian et al. [8, Theorem 1] that there exists at least one self-dual cyclic code if and only if q is a power of 2. Since q is odd, this leads to the unique solution $r = 2$.

If $r = 2$, then $\alpha = -1$. Guenda [5] has proved that there exist Euclidean self-dual negacyclic codes over $\mathbb{F}_q$ (i.e. for $r = 2$ there exists a Euclidean self-dual α-constacyclic code over $\mathbb{F}_q$). □

Proposition 2.3 *Let $\alpha \in \mathbb{F}_{q^2}^*$, $r = ord_{q^2}(\alpha)$, and C be an α-constacyclic code over $\mathbb{F}_{q^2}$. If C is a Hermitian self-dual code, then $r \mid q + 1$.*

Proof If the α-constacyclic code C is a Hermitian self-dual code, then $C = C^{\perp H}$. By Lemma 2.1, the Hermitian dual code $C^{\perp H}$ is an α^{-q}-constacyclic code. Hence, we have

$$C = C^{\perp H} \Longrightarrow \alpha = \alpha^{-q} \Longrightarrow \alpha^{q+1} = 1.$$

Since $r = ord_q(\alpha)$, we obtain $r \mid q + 1$. □

3 Hermitian self-dual constacyclic codes over $\mathbb{F}_{q^2}$

This section is devoted to the Hermitian self-dual α-constacyclic codes over $\mathbb{F}_{q^2}$, where $\alpha \in \mathbb{F}_{q^2}^*$. Let $r = ord_{q^2}(\alpha)$, then $r \mid q^2 - 1$. By Proposition 2.3, we can further assume $r \mid q + 1$ and $rs = q + 1$ for some integer s. Note that if $T \subset O_{r,n}(1)$ is a union of some q^2-cyclotomic cosets, C_T is an α-constacyclic code over $\mathbb{F}_{q^2}$ with the defining set T.

Lemma 3.1 $-q O_{r,n}(1) = O_{r,n}(1) \pmod{rn}$.

Proof Since $q + 1 = rs$, for $ir + 1 \in O_{r,n}(1)$, we have

$$-q(ir+1) = -qir - (q+1) + 1 = -qir - rs + 1 = (-qi - s)r + 1 \pmod{rn} \in O_{r,n}(1).$$

By this, we have $-q O_{r,n}(1) = O_{r,n}(1) \pmod{rn}$. □

Let $T^\perp = -\left[O_{r,n}(1)\backslash T\right] \subset O_{r,n}(-1)$ be the defining set of code $C_{T^\perp}$. Then

$$x^n - \alpha = \prod_{i \in O_{r,n}(1)} (x - \delta^i) = \prod_{i \in T} (x - \delta^i) \cdot \prod_{i \in T^\perp} (x - \delta^{-i}) = g(x)h(x),$$

where $g(x)$ is the generator polynomial of C_T. By Lemma 2.1, $g^\perp(x) = \prod_{i \in T^\perp} (x - \delta^i)$. Therefore, $T^\perp$ is the defining set of the α^{-1}-constacyclic code $C_T^\perp$ (i.e. the Euclidean dual code of C_T). Thus we have $C_{T^\perp} = C_T^\perp$.

Let $\bar{T} = -q\left[O_{r,n}(1)\backslash T\right] = qT^\perp$. According to Lemma 3.1, $\bar{T} \subset O_{r,n}(1)$. It is clear that $\bar{T}$ is a union of some q^2-cyclotomic cosets and $|T| + \left|\bar{T}\right| = n$. Similarly, $g^{\perp(q)}(x) = \prod_{i \in T^\perp} (x - \delta^{iq})$. Therefore, $\bar{T}$ is the defining set of the α^{-q}-constacyclic code $C_T^{\perp H}$. Thus we have the following theorem.

Theorem 3.2 *$C_{\bar{T}}$ is the Hermitian dual code of C_T.*

Based on Theorem 3.2, two necessary and sufficient conditions are given as follows:

Corollary 3.3 *Let $T \subset O_{r,n}(1)$ be the defining set of code C_T and let $\bar{T} = -q\left[O_{r,n}(1)\backslash T\right]$. Then*

(i) *C_T is a Hermitian self-orthogonal constacyclic code if and only if $\bar{T} \subset T$;*
(ii) *C_T is a Hermitian self-dual constacyclic code if and only if $\bar{T} = T$.*

Example 3.4 Let $q = 5$, $n = 4$, and $r = 2$, then $q^2 = 25$. Consider the α-constacyclic code of length 4 over $\mathbb{F}_{25}$ with $\alpha = -1$.

We notice that $r \mid q + 1$ and $O_{2,4}(1) = \{1, 3, 5, 7\}$. Let $T = \{3, 5\}$, then $\bar{T} = -5\left[O_{2,4}(1)\backslash T\right] = \{3, 5\} \pmod 8$. By Corollary 3.3, the code C_T with defining set $T = \{3, 5\}$ is a Hermitian self-dual negacyclic code.

Example 3.5 Let $q^2 = 31^2$, $n = 16$, and $r = 4$. Now we consider the α-constacyclic code of length 16 over $\mathbb{F}_{31^2}$ with α a primitive 4th root of unity.

Clearly, $O_{4,16}(1) = \{1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61\}$ and $r \mid q + 1$. Let $T = \{33, 37, 41, 45, 49, 53, 57, 61\}$, then

$$\bar{T} = -31\left[O_{4,16}(1)\backslash T\right] = \{33, 37, 41, 45, 49, 53, 57, 61\} \pmod{64}.$$

Hence, $\bar{T} = T$. By Corollary 3.3, C_T is a Hermitian self-dual α-constacyclic code.

Lemma 3.6 *Let n be an odd integer with $n \mid q+1$, then there exists an integer m such that $n \mid \frac{q^{2m+1}+1}{q+1}$ and $n \mid 2m+1$.*

Proof

$$\begin{aligned}\frac{q^{2m+1}+1}{q+1} &= \sum_{j=0}^{2m}(-1)^j q^j = \sum_{i=0}^{2m}\sum_{j=i}^{2m}\tbinom{j}{i}(q+1)^i(-1)^i \\ &= \sum_{i=0}^{2m}(q+1)^i(-1)^i\sum_{j=i}^{2m}\tbinom{j}{i} = \sum_{i=0}^{2m}(q+1)^i(-1)^i\tbinom{2m+1}{i+1} \\ &= \left(\sum_{i=1}^{2m}(q+1)^{i-1}(-1)^i\tbinom{2m+1}{i+1}\right)(q+1)+(2m+1).\end{aligned}$$

We can choose an integer m such that $n \mid 2m+1$, which further implies that $n \mid \frac{q^{2m+1}+1}{q+1}$. $\square$

Lemma 3.7 *Let n be an odd integer with prime decomposition $n = p_1^{t_1}p_2^{t_2}\cdots p_s^{t_s}$, where p_i are such that $p_i \mid q+1$, $p_i \neq p_j, t_i > 0\,(1 \le i \le s)$. Then there exists an integer m such that $n \mid \frac{q^{2m+1}+1}{q+1}$.*

Proof First, let $n_1 = p_1^{t_1}$. We use induction to prove that there exists m_t such that $n_1 \mid \frac{q^{2m_t+1}+1}{q+1}$ and $p_1 \mid 2m_t+1$.

When $t_1 = 1$, by Lemma 3.6, there exists m_1 such that $p_1 \mid \frac{q^{2m_1+1}+1}{q+1}$ and $p_1 \mid 2m_1+1$. When $t_1 \ge 2$, assume there exists m_{t-1} such that $p_1^{t_1-1} \mid \frac{q^{2m_{t-1}+1}+1}{q+1}$ and $p_1 \mid 2m_{t-1}+1$. Then by the proof of Lemma 3.6, we know

$$\begin{aligned}\frac{q^{(2m_{t-1}+1)(2m_{t-1}+1)}+1}{q+1} &= \frac{q^{2m_{t-1}+1}+1}{q+1}\,\frac{\left(q^{2m_{t-1}+1}\right)^{2m_{t-1}+1}+1}{q^{2m_{t-1}+1}+1} \\ &= \frac{q^{2m_{t-1}+1}+1}{q+1}\left[\left(\sum_{i=1}^{2m_{t-1}}(q^{2m_{t-1}+1}+1)^{i-1}(-1)^i\tbinom{2m_{t-1}+1}{i+1}\right)\right. \\ &\qquad \left.(q^{2m_{t-1}+1}+1)+(2m_{t-1}+1)\right].\end{aligned}$$

According to the assumption, we have

$$p_1 \mid \left[\left(\sum_{i=1}^{2m_{t-1}}(q^{2m_{t-1}+1}+1)^{i-1}(-1)^i\tbinom{2m_{t-1}+1}{i+1}\right)(q^{2m_{t-1}+1}+1)+(2m_{t-1}+1)\right]$$

and $p_1^{t_1-1} \mid \frac{q^{2m_{t-1}+1}+1}{q+1}$, thus $p_1^{t_1} \mid \frac{q^{(2m_{t-1}+1)(2m_{t-1}+1)}+1}{q+1}$. Let $2m_t+1 = (2m_{t-1}+1)^2$. It follows that $p_1^{t_1} \mid \frac{q^{2m_t+1}+1}{q+1}$ and $p_1 \mid 2m_t+1$.

Next, we prove there exists some m such that $n \mid \frac{q^{2m+1}+1}{q+1}$.

Let $n_i = p_i^{t_i}$ for $1 \le i \le s$. The case $s=1$ has been proven above. Similarly, there exists $m_s^{'}$ such that $n_s \mid \frac{q^{2m_s^{'}+1}+1}{q+1}$. Let $n' = n_1n_2\cdots n_{s-1}$. We assume that there exists m' such that

$n' \mid \frac{q^{2m'+1}+1}{q+1}$. Let $2m+1 = (2m'+1)(2m_s'+1)$. Then

$$\frac{q^{2m+1}+1}{q+1} = \frac{q^{(2m'+1)(2m_s'+1)}+1}{q+1}$$
$$= \frac{q^{2m'+1}+1}{q+1}\left[\left(\sum_{i=1}^{2m_s'}(q^{2m_s'+1}+1)^{i-1}(-1)^i\binom{2m_s'+1}{i+1}\right)\right.$$
$$\left.(q^{2m_s'+1}+1)+(2m_s'+1)\right].$$

Because $n' \mid \frac{q^{2m'+1}+1}{q+1}$, we have $n' \mid \frac{q^{2m+1}+1}{q+1}$. Similarly, we have $n_s \mid \frac{q^{2m+1}+1}{q+1}$. Since $(n', n_s) = 1$, we obtain $n'n_s \mid \frac{q^{2m+1}+1}{q+1}$, i.e., $n \mid \frac{q^{2m+1}+1}{q+1}$. □

Proposition 3.8 *Hermitian self-dual* α*-constacyclic codes over* $\mathbb{F}_{q^2}$ *of length* n *exist if and only if* $Cl_{q^2}(j) \neq Cl_{q^2}(-qj)$ *for any* $j \in O_{r,n}(1)$.

Proof Assume the q^2-cyclotomic cosets of $O_{r,n}(1)$ are

$$Cl_{q^2}(j_1), Cl_{q^2}(j_2), \ldots, Cl_{q^2}(j_t)$$

denoted simply by $Cl_1, Cl_2, \ldots, Cl_t$ for convenience. By Lemma 3.1, $-qCl_i, i \in \{1, 2, \ldots, t\}$, is also a q^2-cyclotomic coset of $O_{r,n}(1)$. Let $Cl_{\bar{i}} = -qCl_i$ and σ be a permutation of $\{1, 2, \ldots, t\}$ which satisfies $\sigma(i) = \bar{i}$ for any $i \in \{1, 2, \ldots, t\}$. Because $q^2Cl_i = Cl_i$ for any $i \in \{1, 2, \ldots, t\}$, we obtain $Cl_{\sigma(\bar{i})} = Cl_{\sigma^2(i)} = Cl_i$. This implies $\sigma^2(i) = i$, i.e., σ^2 is the identity permutation of $\{1, 2, \ldots, t\}$.

Now we prove necessity. Assume there exists a Hermitian self-dual code C_T with defining set $T \subset O_{r,n}(1)$. Then by Corollary 3.3, $\bar{T} = -q[O_{r,n}(1)\backslash T] = T$. Therefore, if there exists j such that $Cl_{q^2}(j) = Cl_{q^2}(-qj)$, we will have the following two cases.

Case 1: If $j \in T$, then $-qj \in T$. By the fact that $\bar{T} = -q[O_{r,n}(1)\backslash T] = T$, there exists some $i \notin T$ such that $-qi = j$. Thus $q^2 i = -qj \notin T$. This is a contradiction.

Case 2: If $j \notin T$, by the fact that $\bar{T} = -q[O_{r,n}(1)\backslash T] = T$, we have $-qj \in T$. Because $Cl_{q^2}(j) = Cl_{q^2}(-qj) \subset T$, we have $j \in T$ which contradicts the assumption.

Next, we prove the sufficiency. We assume $Cl_{q^2}(j) \neq Cl_{q^2}(-qj)$ for any $j \in O_{r,n}(1)$. This implies $\sigma(i) \neq i$ for any $i \in \{1, 2, \ldots, t\}$. Since $\sigma^2(i) = i, \sigma$ must be a product of mutually disjoint transpositions like $(a_1\, b_1)(a_2\, b_2)\cdots(a_k\, b_k)$. We might assume $t = 2k$ and let $\sigma(i) = k+i$ and $\sigma(k+i) = i$ for $1 \leq i \leq k$. If we let $T = Cl_1 \cup Cl_2 \cup \cdots \cup Cl_k$, then the code C_T with defining set T is a Hermitian self-dual code. Therefore, if $Cl_{q^2}(j) \neq Cl_{q^2}(-qj)$ for $\forall j \in O_{r,n}(1)$, there exist Hermitian self-dual codes. □

Based on this proposition, we have the following theorem. This theorem is an extension of Theorem 3 in [3] (the case of $b = 1$ and $r' = 1$).

Theorem 3.9 *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* $r \mid q+1$, *and let* $\alpha \in \mathbb{F}_{q^2}^*$ *has order* r. *Then Hermitian self-dual* α *-constacyclic codes over* $\mathbb{F}_{q^2}$ *of length* n *exist if and only if* $b > 0$ *and* $q+1 \not\equiv 0 \pmod{2^{a+b}}$.

Proof n' can be written as $n' = r_1^{t_1} \cdots r_j^{t_j} r_{j+1}^{t_{j+1}} \cdots r_s^{t_s}$, where $r_1, \ldots, r_s$ are distinct primes, $r_1, \ldots, r_j \mid r$, and $r_{j+1}, \ldots, r_s \nmid r$. Assume $n_1 = r_1^{t_1} \cdots r_j^{t_j}$, $n_2 = r_{j+1}^{t_{j+1}} \cdots r_s^{t_s}$, and $n' = n_1 n_2$. Since $r_{j+1}, \ldots, r_s \nmid r$, it follows $(n_2, r) = 1$. Because $r_1, \ldots, r_j \mid r$, we know $r_1, \ldots, r_j \mid q+1$. By Lemma 3.7, there exists m such that $n_1 \mid \frac{q^{2m+1}+1}{q+1}$.

The proof consists of two parts. First we prove the necessity. If r is odd, which is equivalent to $b = 0$, clearly, we have $(r, 2^a n_2) = 1$. There exists $i \in \mathbb{Z}$ such that $2^a n_2 \mid ir+1$. Thus by $n_1 \mid \frac{q^{2m+1}+1}{q+1}$, we have

$$\begin{aligned}(q+1)2^a n_1 n_2 \mid (q^{2m+1}+1)(ir+1) &\Longrightarrow (q+1)n \mid (q^{2m+1}+1)(ir+1)\\ \Longrightarrow rn \mid (q^{2m+1}+1)(ir+1).\end{aligned}$$

Therefore, $ir+1 = q^{2m}(-q(ir+1)) \pmod{rn}$. This implies $Cl_{q^2}(ir+1) = Cl_{q^2}(-q(ir+1))$. Since $ir+1 \in O_{r,n}(1)$, by Proposition 3.8, there is no Hermitian self-dual α -constacyclic code over $\mathbb{F}_{q^2}$, which contradicts the assumption. Therefore, r must be even, i.e., $b > 0$.

Let $q+1 = 2^c rt$ with $c \geq 0$ and $(t, 2) = 1$. If $q+1 \equiv 0 \pmod{2^{a+b}}$, then $c \geq a$. Because $(n_2, r) = 1$, there exists $i' \in \mathbb{Z}$ such that $n_2 \mid i'r+1$. Since $n_1 \mid \frac{q^{2m+1}+1}{q+1}$, we have

$$\begin{aligned}(q+1)n_1 n_2 \mid (q^{2m+1}+1)(i'r+1) &\Longrightarrow 2^c rtn_1 n_2 \mid (q^{2m+1}+1)(i'r+1)\\ &\Longrightarrow rn \mid (q^{2m+1}+1)(i'r+1).\end{aligned}$$

Similarly, we have $Cl_{q^2}(i'r+1) = Cl_{q^2}(-q(i'r+1))$. By Proposition 3.8, we get a contradiction. So it is necessary to have $q+1 \not\equiv 0 \pmod{2^{a+b}}$.

Now we prove the sufficiency. Assume $b > 0$ and $q+1 \not\equiv 0 \pmod{2^{a+b}}$. If there is no Hermitian self-dual code, by Proposition 3.8, there exists $ir+1 \in O_{r,n}(1)$ such that $Cl_{q^2}(ir+1) = Cl_{q^2}(-q(ir+1))$. Therefore, for some $m \in \mathbb{Z}^+$,

$$rn \mid (q^{2m+1}+1)(ir+1) \Longrightarrow 2^{a+b} r'n' \mid \frac{q^{2m+1}+1}{q+1}(q+1)(ir+1).$$

Since $b > 0$, $ir+1$ must be odd. Together with the fact that $\frac{q^{2m+1}+1}{q+1}$ is odd, we get $2^{a+b} \mid q+1$, which contradicts the assumption that $q+1 \not\equiv 0 \pmod{2^{a+b}}$. □

4 MDS hermitian self-dual constacyclic codes over $\mathbb{F}_{q^2}$

We study MDS Hermitian self-dual constacyclic codes over $\mathbb{F}_{q^2}$ in this section. The following theorem will give the BCH bound for constacyclic codes (cf. [1, Theorem 2.2]).

Theorem 4.1 *Let C be an α-constacyclic code of length n over $\mathbb{F}_{q^2}$. Let $r = ord_{q^2}(\alpha)$. Let δ be a primitive rnth root of unity in an extension field of $\mathbb{F}_{q^2}$ such that $\delta^n = \alpha$, and let $\zeta = \delta^r$. Assume the generator polynomial of C has roots that include the set $\{\delta\zeta^i \mid i_1 \leq i \leq i_1+d-1\}$. Then the minimum distance of $C \geq d$.*

Example 4.2 Let $q^2 = 17^2$, $n = 8$ and $r = 18$. We consider the α-constacyclic code of length 8 over $\mathbb{F}_{17^2}$ with α a primitive 18th root of unity.

Obviously, we have $O_{18,8}(1) = \{1, 19, 37, 55, 73, 91, 109, 127\}$ and $r \mid q+1$. Let $T = \{73, 91, 109, 127\}$, then $\bar{T} = -17\left[O_{18,8}(1)\backslash T\right] = \{73, 91, 109, 127\} \pmod{144}$. Thus $\bar{T} = T$. By Corollary 3.3, C_T is a Hermitian self-dual α-constacyclic code.

Table 1 $[n, k, d]$ Hermitian self-dual codes over $\mathbb{F}_{q^2}$ (where $q \leq 19$)

q	r	n	k	d	T	q	r	n	k	d	T
5	2	4	2	3	{3, 5}	17	6	8	4	5	{19, 25, 31, 37}
5	6	4	2	3	{1, 7}	17	18	8	4	5	{1, 19, 37, 55}
7	4	4	2	3	{1, 5}	17	2	10	5	$\geqslant 4$	{1, 9, 13, 15, 17}
7	8	4	2	$\geqslant 2$	{1, 17}	17	6	10	5	$\geqslant 4$	{1, 19, 25, 31, 49}
7	8	6	3	4	{1, 9, 17}	17	18	10	5	$\geqslant 4$	{1, 37, 55, 73, 109}
9	2	4	2	3	{1, 3}	17	2	12	6	$\geqslant 5$	{1, 3, 11, 13, 15, 17}
9	10	4	2	3	{1, 11}	17	6	12	6	$\geqslant 5$	{1, 7, 13, 19, 31, 43}
9	2	8	4	5	{5, 7, 9, 11}	17	18	12	6	$\geqslant 3$	{1, 19, 73, 91, 145, 163}
9	10	8	4	5	{1, 11, 21, 31}	17	2	14	7	$\geqslant 5$	{5, 7, 11, 13, 15, 17, 23}
11	2	4	2	3	{1, 3}	17	6	14	7	$\geqslant 5$	{1, 7, 19, 25, 31, 37, 55}
11	4	4	2	$\geqslant 2$	{1, 9}	17	18	14	7	$\geqslant 5$	{1, 19, 37, 55, 91, 109, 199}
11	6	4	2	3	{1, 7}	17	2	16	8	9	{9, 11, 13, 15, 17, 19, 21, 23}
11	12	4	2	$\geqslant 2$	{1, 25}	17	6	16	8	9	{43, 49, 55, 61, 67, 73, 79, 85}
11	4	6	3	4	{1, 5, 9}	17	18	16	8	9	{1, 19, 37, 55, 73, 91, 109, 127}
11	12	4	2	$\geqslant 2$	{1, 25, 49}	19	2	4	2	3	{1, 3}
11	2	8	4	$\geqslant 3$	{1, 3, 9, 11}	19	4	4	2	$\geqslant 2$	{1, 9}
11	4	8	4	$\geqslant 2$	{1, 9, 17, 25}	19	10	4	2	3	{1, 11}
11	6	8	4	$\geqslant 3$	{1, 7, 25, 31}	19	20	4	2	$\geqslant 2$	{1, 41}
11	12	8	4	$\geqslant 2$	{1, 24, 49, 73}	19	4	6	3	4	{5, 9, 13}
11	4	10	5	6	{17, 21, 25, 29, 33}	19	20	6	3	4	{1, 21, 41}
11	12	10	5	6	{1, 13, 25, 37, 49}	19	2	8	4	$\geqslant 3$	{1, 3, 9, 11}
13	2	4	2	3	{3, 5}	19	4	8	4	$\geqslant 2$	{1, 9, 17, 25}
13	14	4	2	3	{1, 15}	19	10	8	4	$\geqslant 3$	{1, 11, 41, 51}
13	2	6	3	4	{1, 3, 5}	19	20	8	4	$\geqslant 2$	{1, 41, 81, 121}
13	14	6	3	4	{1, 15, 29}	19	4	10	5	6	{1, 5, 9, 13, 17}
13	2	8	4	$\geqslant 3$	{1, 7, 9, 15}	19	20	10	5	$\geqslant 2$	{1, 41, 81, 121, 161}
13	14	8	4	$\geqslant 3$	{1, 15, 57, 71}	19	2	12	6	$\geqslant 5$	{1, 7, 15, 17, 19, 21}
13	2	10	5	$\geqslant 4$	{1, 9, 13, 15, 17}	19	4	12	6	$\geqslant 4$	{1, 17, 21, 25, 41, 45}
13	14	10	5	$\geqslant 4$	{1, 15, 29, 57, 113}	19	10	12	6	$\geqslant 5$	{1, 11, 51, 61, 71, 81}
13	2	12	6	7	{7, 9, 11, 13, 15, 17}	19	20	12	6	$\geqslant 4$	{1, 21, 41, 121, 141, 161}}
13	14	12	6	7	{1, 15, 29, 43, 57, 71}	19	4	14	7	$\geqslant 5$	{{1, 5, 9, 13, 21, 25, 45}}
17	2	4	2	3	{1, 3}	19	20	14	7	$\geqslant 5$	{1, 21, 61, 81, 101, 121, 181}
17	6	4	2	3	{7, 13}	19	2	16	8	$\geqslant 3$	{1, 3, 9, 11, 17, 19, 25, 27}
17	18	4	2	3	{1, 19}	19	4	16	8	$\geqslant 2$	{1, 9, 17, 25, 33, 41, 49, 57}
17	2	6	3	4	{1, 3, 5}	19	10	16	8	$\geqslant 3$	{1, 11, 41, 51, 81, 91, 121, 131}}
17	6	6	3	4	{1, 7, 13}	19	20	16	8	$\geqslant 2$	{1, 41, 81, 121, 161, 201, 241, 281}
17	18	6	3	$\geqslant 2$	{1, 37, 73}	19	4	18	9	10	{29, 33, 37, 41, 45, 49, 53, 57, 61}
17	2	8	4	5	{1, 3, 5, 7}	19	20	18	9	10	{1, 21, 41, 61, 81, 101, 121, 141, 161}

Furthermore, we notice that the generator polynomial of C_T has roots:

$$\delta^{1+4r}, \delta^{1+5r}, \delta^{1+6r}, \delta^{1+7r}.$$

By Theorem 4.1, the minimum distance d is at least 5. Since $n-k+1 = 8-4+1 = 5$, C_T is an [3,4,7] MDS Hermitian self-dual α-constacyclic code.

Example 4.2 shows that there exist MDS Hermitian self-dual constacyclic codes. The following theorem is a generalization of Example 4.2.

Theorem 4.3 *Let $\alpha \in \mathbb{F}_{q^2}^*$ have order r with $rs = q+1$ for some positive integer s. Let n be even and $n \mid q-1$. Let*

$$T = O_{r,n}(1) \backslash \left\{ ir+1 \mid -[\frac{s-1}{2}] \leq i \leq [\frac{n-1-s}{2}] \right\} \pmod{rn}.$$

Then the following holds.

(i) *If s is odd, then C_T is a Hermitian self-dual α -constacyclic MDS code with parameters $[n, \frac{n}{2}, \frac{n}{2}+1]$;*
(ii) *If s is even, then C_T is a Hermitian self-orthogonal α-constacyclic MDS code with parameters $[n, \frac{n}{2}-1, \frac{n}{2}+2]$.*

Proof Let $T_1 = \left\{ir+1 \mid -[\frac{s-1}{2}] \leq i \leq [\frac{n-1-s}{2}]\right\} \pmod{rn}$. If s is odd, then T_1 has $\frac{n}{2}$ elements, and therefore, the dimension of C_T is $\frac{n}{2}$; if s is even, then T_1 has $\frac{n}{2}-1$ elements, and therefore, the dimension of C_T is $\frac{n}{2}-1$. Let $I_1 = \left\{i \mid -[\frac{s-1}{2}] \leq i \leq [\frac{n-1-s}{2}]\right\} \pmod{n}$. The set $\{0, 1, \ldots, n-1\} \backslash I_1$ has $\frac{n}{2}$ consecutive elements (modulo n) when s is odd and $\frac{n}{2}+1$ consecutive elements when s is even. Using the Singleton Bound and Theorem 4.1, the minimum distance of C_T is $\frac{n}{2}+1$ when s is odd and $\frac{n}{2}+2$ when s is even, making C_T MDS.

The proof is complete if we show that C_T is Hermitian self-orthogonal. By Corollary 3.3, this can be verified if we show $T_1 \cap (-qT_1) = \varnothing$ where we reduce the entries in T_1 and $-qT_1$ modulo rn before taking the intersection. Since $n \mid q-1$, we know $-q \equiv -1 \pmod{n}$, which implies that $-qr \equiv -r \pmod{rn}$. So $-q(ir+1) \equiv -ir-q \equiv -ir-(q+1)+1 \equiv (-i-s)r+1 \equiv (n-i-s)r+1 \pmod{rn}$. Therefore, showing that $T_1 \cap (-qT_1) = \varnothing$ is equivalent to showing that $I_1 \cap I_2 = \varnothing$, where $I_2 = \{n-i-s \mid i \in I_1\} \pmod{n}$ and the intersection $I_1 \cap I_2$ is taken after reducing modulo n. Consider the case that s is odd. The elements of I_1 are the $\frac{n}{2}$ consecutive integers $-(\frac{s-1}{2}), \ldots, \frac{n-1-s}{2}$. Using this, the elements of I_2 are the $\frac{n}{2}$ consecutive integers $\frac{n+1-s}{2}, \ldots, n-(\frac{s+1}{2})$. These two lists together make up n consecutive integers, and hence, when reducing modulo n, $I_1 \cap I_2 = \varnothing$. Consider the case that s is even. The elements of I_1 are the $\frac{n}{2}-1$ consecutive integers $-\frac{s}{2}+1, \ldots, \frac{n-s}{2}-1$. Using this, the elements of I_2 are the $\frac{n}{2}-1$ consecutive integers $\frac{n-s}{2}+1, \ldots, n-\frac{s}{2}-1$. These two lists together make up $n-1$ consecutive integers, excluding the single integer $\frac{n-s}{2}$. Therefore, when reducing modulo n, $I_1 \cap I_2 = \varnothing$. □

Table 1 gives some Hermitian self-dual codes over $\mathbb{F}_{q^2}$ for $q \leq 19$ with lower bounds on the minimum distance d.

5 Conclusion

We have studied Hermitian self-dual codes arising from constacyclic codes in this paper. In Sect. 3, necessary and sufficient conditions have been given for the existence of Hermitian self-dual constacyclic codes over $\mathbb{F}_{q^2}$ of length n. In Sect. 4, we have given conditions for the existence of MDS Hermitian self-orthogonal and self-dual constacyclic codes over $\mathbb{F}_{q^2}$.

Acknowledgment The authors wish to thank the reviewers for their valuable comments and suggestions which greatly helped us to improve this paper.

References

1. Aydin N., Siap I., Ray-Chaudhuri D.J.: The structure of 1-generator quasi-twisted codes and new linear codes. Des. Codes Cryptogr. **24**(3), 313–326 (2001).
2. Berlekamp E.R.: Algebraic Coding Theory. McGraw-Hill, New York (1968).
3. Blackford T.: Negacyclic duadic codes. Finite Fields Appl. **14**(4), 930–943 (2008).
4. Dinh H.Q.: Constacyclic codes of length p^s over $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$. J. Algebra **324**(5), 940–950 (2010).
5. Guenda K.: New MDS self-dual codes over large finite fields. Des. Codes Cryptogr. **62**(1), 31–42 (2011).
6. Gulliver T.A., Kim J.L., Lee Y.: New MDS or near MDS self-dual codes. IEEE Trans. Inf. Theory **54**(9), 4354–4360 (2008).
7. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, New York (2003).
8. Jian Y., Ling S., Xing C.: On self-dual cyclic codes over finite fields. IEEE Trans. Inf. Theory **57**(4), 2243–2251 (2011).
9. Kim J.L., Lee Y.: Euclidean and Hermitian self-dual MDS codes over large finite fields. Comb. Theory A **105**(1), 79–95 (2004).
10. Pedersen P., Dahl C.: Classification of pseudo-cyclic MDS codes. IEEE Trans. Inf. Theory **37**(2), 365–370 (1991).