Research Article

Hermitian Self-Orthogonal Constacyclic Codes over Finite Fields

Amita Sahni and Poonam Trama Sehgal

Centre for Advanced Study in Mathematics, Panjab University, Chandigarh 160014, India

Correspondence should be addressed to Amita Sahni; sahniamita05@gmail.com

Received 21 July 2014; Accepted 23 October 2014; Published 12 November 2014

1. Introduction

Let \( F_q^2 \) denote a finite field with \( q^2 \) elements. An \([n,k]_q\) linear code \( C \) of length \( n \) and dimension \( k \) over \( F_q^2 \) is a \( k \)-dimensional subspace of the vector space \( F_q^{n} \). Elements of the subspace \( C \) are called codewords and are written as row vectors \( c = (c_0, c_1, \ldots, c_{n-1}) \). A linear code \( C \) over \( F_q^2 \) is called \( \lambda \)-constacyclic if \( (\lambda c_{n-1}, c_0, \ldots, c_{n-2}) \) is in \( C \) for every \((c_0, c_1, \ldots, c_{n-1}) \) in \( C \). Let \( \vartheta : F_q^{n} \rightarrow F_q^2[x]/(x^n - \lambda) \) be the map given by \( \vartheta((c_0, c_1, \ldots, c_{n-1})) \mapsto c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \mod(x^n - \lambda) \). One can easily check that \( \vartheta \) is an \( F_q^2 \)-module isomorphism. We can therefore identify \( \lambda \)-constacyclic codes of length \( n \) over \( F_q^2 \) with ideals in \( F_q^2[x]/(x^n - \lambda) \). The Hamming weight \( w(c) \) of \( c \in F_q^n \) is the number of nonzero coordinates of \( c \). The minimum distance of \( C \) is defined to be \( d = \min \{w(c); c \neq 0 \in C\} \). An \([n,k,d]_q\) code, that is, a \([n,k]_q\) linear code with minimum distance \( d \), is said to be maximum distance separable (MDS) if \( d = n - k + 1 \). The Hermitian inner product of elements \( u, v \in F_q^n \) is defined as \( \langle u, v \rangle_H = \sum_{i=0}^{n-1} u_i \overline{v_i} \), for \( u = (u_0, u_1, \ldots, u_{n-1}) \) and \( v = (v_0, v_1, \ldots, v_{n-1}) \). For a linear code \( C \) of length \( n \) over \( F_q^2 \), the Hermitian dual code \( C^{\perp_H} \) of \( C \) is defined by \( C^{\perp_H} = \{ v \in F_q^n; \langle u, v \rangle_H = 0, \forall u \in C \} \). If \( C = C^{\perp_H} \), then \( C \) is known as Hermitian self-dual and \( C \) is Hermitian self-orthogonal if \( C \subseteq C^{\perp_H} \).

Aydin et al. [1] dealt with constacyclic codes and a constacyclic BCH bound was given. Gulliver et al. [2] showed that there exists Euclidean self-dual MDS code of length \( q^2 \) over \( F_q^2 \) 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. Blackford [3] studied negacyclic codes over finite fields by using multipliers. He gave conditions on the existence of Euclidean self-dual codes. Recently, Guenda [4] 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 [5] the authors gave a formula to enumerate the number of Euclidean self-dual and self-orthogonal negacyclic codes of length \( n \) over a finite field \( F_q^2 \), where \( q \) is coprime to \( n \). In [6] Yang and Cai gave the necessary and sufficient conditions for the existence of Hermitian self-dual constacyclic codes. They also gave some conditions under which Hermitian self-dual and self-orthogonal MDS codes exist. In this paper, we find necessary and sufficient conditions for the existence of Hermitian self-orthogonal constacyclic codes of length \( n \) over a finite field \( F_q^2 \), \( n \) coprime to \( q \), and also give a characterization of their defining sets. We obtain a formula to calculate the number of these codes. We give conditions for the existence of some MDS Hermitian self-orthogonal constacyclic codes. We also found their number and defining sets (Table 1).
2 Journal of Discrete Mathematics

Table 1: Number of Hermitian self-orthogonal codes over $\mathbb{F}_{2^r}$.

| $r$ | $n$ | $N$ | $|\Lambda^{(1)}|$ |
|-----|-----|-----|----------------|
| 2   | 2   | 3   | 3              |
| 4   | 6   | 27  | 9              |
| 6   | 12  | 729 | 27             |
| 11  | 2   | 3   | 9              |
| 12  | 6   | 27  | 2              |
| 13  | 12  | 729 | 3              |
| 14  | 6   | 27  | 4              |
| 16  | 4   | 9   | 2              |
| 17  | 2   | 3   | 2              |
| 18  | 10  | 243 | 3              |
| 19  | 2   | 3   | 1              |
| 22  | 6   | 27  | 2              |
| 24  | 12  | 729 | 1              |
| 4   | 2   | 3   | 2              |
| 8   | 6   | 27  | 4              |
| 11  | 2   | 3   | 2              |
| 12  | 2   | 3   | 2              |
| 13  | 6   | 27  | 2              |
| 16  | 10  | 243 | 2              |
| 17  | 2   | 3   | 2              |
| 19  | 2   | 3   | 2              |
| 22  | 4   | 9   | 2              |
| 24  | 14  | 2187| 2              |
| 2   | 2   | 3   | 2              |
| 4   | 4   | 9   | 2              |
| 6   | 2   | 3   | 2              |
| 8   | 4   | 9   | 2              |
| 11  | 2   | 3   | 2              |
| 12  | 4   | 9   | 2              |
| 13  | 6   | 27  | 2              |
| 14  | 6   | 27  | 2              |
| 16  | 4   | 9   | 2              |
| 17  | 2   | 3   | 2              |
| 18  | 2   | 3   | 2              |
| 19  | 2   | 3   | 2              |
| 22  | 6   | 27  | 2              |
| 24  | 4   | 9   | 2              |

2. Hermitian Self-Orthogonal Constacyclic Codes

Let $q$ be an odd prime power and $n$ a positive integer relatively prime to $q$. Let $C$ be an $[n,k]$ $\lambda$-constacyclic code over $\mathbb{F}_{q^r}$ with $r = \operatorname{ord}_{\mathbb{F}_{q^r}}(\lambda)$, where \operatorname{ord}_{\mathbb{F}_{q^r}}(\lambda) denotes the order of $\lambda$ in $\mathbb{F}_{q^r}$. Let $g(x)$ be the generator polynomial of $C$. Then $g(x)$ divides $(x^n - \lambda)$. Write $(x^n - \lambda) = g(x)h(x)$. The polynomial $h(x)$ is called the check polynomial of $C$. For $0 \leq s < rn$, let $C_s = \{s, s^2, \ldots, (s^q)^{r^{-1}}\}$ be the $q^r$-cyclotomic coset modulo $s$, where $n_s$ is the least positive integer such that $(s^q)^{rn} \equiv s \pmod{rn}$. Let $\alpha$ be a primitive $rn$th root of unity in some extension field of $\mathbb{F}_{q^r}$ such that $\alpha^{n_s} = \lambda$.

Then the polynomial $M_{(s)}(x) = \prod_{\gamma \in C_s} (x - \alpha^\gamma)$ is the minimal polynomial of $\alpha^s$ over $\mathbb{F}_{q^r}$ and

$$x^n - 1 = \prod_{s \in \Lambda} M_{(s)}(x),$$

where $\Lambda$ is the set of representatives of all the distinct $q^r$-cyclotomic cosets modulo $rn$. As $(x^n - \lambda) | (x^n - 1)$, one can check that the roots of $(x^n - \lambda)$ are precisely $\alpha^{ir+1}$, $0 \leq i < n$.

Define

$$O_{\lambda n}(1) = \{ir + 1; 0 \leq i < n\} \pmod{rn}.$$ 

Hence we have

$$x^n - \lambda = \prod_{s \in \Lambda_{\lambda}} M_{(s)}(x),$$

where $\Lambda_{\lambda} = \Lambda \cap O_{\lambda n}(1)$.

Let $C = \langle g(x) \rangle$ be a $\lambda$-constacyclic code with defining set $T = \{ir + 1 \in O_{\lambda n}(1); \alpha^{ir+1}$ is a root of $g(x)\}$. Clearly $T$ is a union of some $q^r$-cyclotomic cosets $C_s$ mod $rn$ for $s \in \Lambda_{\lambda}$. The Hermitian dual $C^{\perp H}$ of the code $C$ is a $\lambda^{q^r}$-constacyclic code over $\mathbb{F}_{q^r}$ with defining set $T^{\perp H} = -qT$ of $O_{\lambda n}(1) \setminus T \pmod{rn}$ (see Theorem 3.2 of [6]). Write the generator polynomial $g(x)$ of the code $C$ as $g(x) = \prod_{s \in \Lambda_{\lambda}} (M_{(s)}(x))^{\delta_{(s)}}$, where

$$\delta_{(s)} = \begin{cases} 1, & \text{if } s \in T, \\ 0, & \text{if } s \notin T. \end{cases}$$

Then the generator polynomial of the Hermitian dual $C^{\perp H}$ of $C$ is $h^{\perp H}(x) = \prod_{s \in \Lambda_{\lambda}} (M_{(s)}(x))^{1-\delta_{(s)}}$, where

$$\Delta_{(s)} = \begin{cases} 1, & \text{if } s \in T^{\perp H}, \\ 0, & \text{if } s \notin T^{\perp H}. \end{cases}$$

It can be easily verified that $\Delta_{(s)} = 1 - \delta_{(s-q^r)}$ so that $h^{\perp H}(x) = \prod_{s \in \Lambda_{\lambda}} (M_{(s)}(x))^{1-\delta_{(s-q^r)}}$.

**Lemma 1.** Let $C$ be a $\lambda$-constacyclic code over $\mathbb{F}_{q^r}$ with $\operatorname{ord}_{\mathbb{F}_{q^r}}(\lambda) = r$. If $C$ is a Hermitian self-orthogonal code, then $r | (q + 1)$.

**Proof.** The proof is similar to [6, Proposition 2.3].

**Theorem 2.** Nontrivial Hermitian self-orthogonal $\lambda$-constacyclic codes of length $n$ over $\mathbb{F}_{q^r}$ exist if and only if $C_s \neq C_{-q^r}$ for some $s \in O_{\lambda n}(1)$.

**Proof.** Let $C$ be a nontrivial Hermitian self-orthogonal $\lambda$-constacyclic code of length $n$ over $\mathbb{F}_{q^r}$ with defining set $T$. Then there exists $s \in O_{\lambda n}(1)$ such that $s \neq 0$ and $s \notin T$. 

Hence \( s \in O_{r, n}(1) \setminus T \) giving us that \(-qs \in T^{-n} \subseteq T\). Thus, \( C_s \neq C_{-qs} \) (as \( s \notin T \) and \(-qs \in T\)). Conversely, let \( s \in O_{r, n}(1) \) be such that \( C_s = C_{-qs} \). Consider \( T = O_{r, n}(1) \setminus C_s \). The code \( C \) is a nontrivial Hermitian self-orthogonal code since \( T^{-n} = -qO_{r, n}(1) \setminus T = -qC_s = C_{-qs} \subseteq T \).

Define \( T_0 = \{ s \in O_{r, n}(1); C_s = C_{-qs} \} \). The following theorem characterizes the defining set of a Hermitian self-orthogonal constacyclic code of length \( n \) over \( \mathbb{F}_q \).

**Theorem 3.** Let \( C \) be a \( \lambda \)-constacyclic code of length \( n \) over \( \mathbb{F}_q \) with the defining set \( T \). Then \( C \) is Hermitian self-orthogonal if and only if \( (i) \ T_0 \subseteq T \) and \( (ii) \) for each \( s \notin T_0 \), at least one of \( s \) and \(-qs \) belongs to \( T \).

**Proof.** Let \( C \) be a \( \lambda \)-constacyclic code. Let \( s \in T_0 \). Then \( C_s = C_{-qs} \). Suppose that \( s \notin T \). Then \(-qs \in T^{-n} \subseteq T \) so that \( C_{-qs} \subseteq T \) and \( C_s \notin T \), which contradicts the hypothesis that \( C_s = C_{-qs} \). Thus, \( T_0 \subseteq T \). Now, let \( s \notin T_0 \). Then either \( s \in T \) or \(-qs \in T^{-n} \subseteq T \), as required.

Conversely, let the defining set be such that \( T_0 \subseteq T \) and for each \( s \notin T_0 \), at least one of \( s \) and \(-qs \) is in \( T \). Then \( T^{-n} = -qO_{r, n}(1) \setminus T = -qC_s \in T \), by condition \((ii)\) so that the code \( C \) having \( T \) as a defining set is a Hermitian self-orthogonal code.

**Corollary 4.** A \( \lambda \)-constacyclic code \( C \) of length \( n \) over \( \mathbb{F}_q \) generated by \( g(x) = \prod_{\lambda \in A_1} (M_\lambda(x))^{a_\lambda} \) is a Hermitian self-orthogonal if and only if \( \delta_\lambda + \delta_{-\lambda} \geq 1 \) for all \( \lambda \in A_1 \).

Define \( A_0 = A_1 \cap T_0 \) and \( A_1 = A \setminus A_0 \). Observe that \( T_0 = \bigcup_{\lambda \in A_1} C_\lambda \).

Example 5. Let \( q = 13, n = 15, \) and \( r = 7 \); then \( q^2 = 169 \). We consider the \( \lambda \)-constacyclic code of length 15 over \( \mathbb{F}_{13^2} \), where \( \lambda \in \mathbb{F}_{13^2} \) with order 7. Clearly

\[
O_{13^2}(1) = \{1, 8, 15, 22, 29, 36, 43, 50, 57, 64, 71, 78, 85, 92, 99\},
\]

\[
T_0 = \{15\}. \quad (6)
\]

Define \( T = \{1, 15, 22, 36, 43, 50, 57, 64, 71, 78, 85, 92, 99\} \); then \( T^{-n} = -13O_{r, n}(1) \setminus T = \{1, 22, 36, 43, 50, 57, 64, 92, 99\} \subseteq T \). Hence, the code with defining set \( T \) is a \([15, 7]\) Hermitian self-orthogonal \( \lambda \)-constacyclic code.

**Theorem 6.** The number of Hermitian self-orthogonal \( \lambda \)-constacyclic codes of length \( n \) over \( \mathbb{F}_q \) is \( 3^{|A_1|}/2 \).

**Proof.** Let \( C \) be a Hermitian self-orthogonal \( \lambda \)-constacyclic code of length \( n \) over \( \mathbb{F}_q \) generated by \( g(x) = \prod_{\lambda \in A_1} (M_\lambda(x))^{a_\lambda} \). Then \( \delta_\lambda + \delta_{-\lambda} \geq 1 \) for all \( \lambda \in A_1 \), \( \delta_{\lambda} = \delta_{-\lambda} = 1 \). However, for \( s \in A_1 \), the pairs \( (\delta_\lambda, \delta_{-\lambda}) \) have three choices \((0,1), (1,0), \) and \((1,1)\). Hence, the number of Hermitian self-orthogonal \( \lambda \)-constacyclic codes of length \( n \) over \( \mathbb{F}_q \) is \( 3^{|A_1|}/2 \).

In order to find the number of Hermitian self-orthogonal \( \lambda \)-constacyclic codes of length \( n \) over \( \mathbb{F}_q \), we need to compute the value of \( |A_1| \). Our aim is to prove the following.

**Theorem 7.** Let \( a, r, \) and \( d \) be positive integers such that \( \gcd(a, r) = 1 \). Then the number of solutions for the linear congruence

\[
ax \equiv 1 \pmod{r}
\]

in the set \( A = \{w; 0 \leq w < rd \text{ and } \gcd(w, rd) = 1\} \) is exactly \( \phi(rd)/\phi(r) \).

Since \( \gcd(a, r) = 1 \), the linear congruence \( ax \equiv 1 \pmod{r} \) has a unique solution modulo \( r \). Let it be \( x \equiv b \pmod{r} \). Then \( \gcd(b, r) = 1 \). We write \( A = \{ir + s; 0 \leq s < d, 0 \leq \gcd(ir + s, rd) = 1\} \). The solutions of (7) will be amongst \( A_b = \{ir + b; 0 \leq i < d\} \). Clearly, the elements of \( A_b \) are relatively prime to \( r \). We need to count the number of elements of \( A_b \) which are coprime to \( d \). Also, \( |A_b| = d \). Therefore, the required number \( N = d - |\{ir + b; 0 \leq i < d, \gcd(ir + b, d) > 1\}| \).

**Lemma 8.** Let \( p \) be a prime divisor of \( d \) such that \( p \nmid r \). The number of multiples of \( p \) in \( A_b \) is \( d/p \).

**Proof.** Write \( A_b = \bigcup_{k=0}^{d/p-1} A_{bk} \), where \( A_{bk} = \{kpr + b, (k+1)r + b, \ldots, (k+1)p - 1)r + b\} \) for each \( k, 0 \leq k < d \). Since each \( A_{bk} \) contains \( p \) elements which are pairwise incongruent mod \( p \), each \( A_{bk} \) forms a complete residue system modulo \( p \). Hence exactly one element in each \( A_{bk} \) is divisible by \( p \). Consequently, there exist \( d/p \) elements in \( A_b \), which are divisible by \( p \).

**Lemma 9.** Let \( p_1 \) and \( p_2 \) be two distinct prime divisors of \( d \) with \( \gcd(p_1 p_2, r) = 1 \). Then the number of multiples of \( p_1 \) or \( p_2 \) in \( A_b \) is \( d/p_1 + d/p_2 - d/p_1 p_2 \).

**Proof.** The number of multiples of \( p_1 \) in \( A_b \) equals \( d/p_1 \), while the number of multiples of \( p_2 \) in \( A_b \) is \( d/p_2 \). By a similar argument as in Lemma 8, the number of multiples of \( p_1 \) or \( p_2 \) equals \( d/p_1 p_2 \). Therefore, the required number is \( d/p_1 + d/p_2 - d/p_1 p_2 \).

**Theorem 10.** Let \( p_1, p_2, \ldots, p_m \) be all the distinct prime divisors of \( d \) which are relatively prime to \( r \). The number of elements in \( A_b \) which are not coprime to \( d \) is

\[
N_0 = \sum_{i=1}^{m} \frac{d}{p_i} - \sum_{i \neq j} \frac{d}{p_ip_j} + \sum_{i,j,k,m} \frac{d}{p_ip_jp_k} + \cdots + (-1)^{m-1} \frac{d}{p_1p_2 \cdots p_m}
\]

**Proof.** The proof follows by induction on \( m \) Lemmas 8 and 9.

In order to prove Theorem 7, it is enough to show that \( N = d - N_0 = \phi(rd)/\phi(r) \).
Now,

\[ N = d - \left\{ \sum_{1 \leq i \leq m} \frac{d}{P_i} - \sum_{i \neq j} \frac{d}{P_i P_j} + \sum_{i,j,k \text{ distinct}} \frac{d}{P_i P_j P_k} + \ldots + (-1)^{m-1} \frac{d}{P_1 P_2 \cdots P_m} \right\} \]

(9)

Let \( p_1, p_2, \ldots, p_{m+1} \) be all the distinct prime divisors of \( d \). Also, let \( p_{m+1}, \ldots, p_{m+1}, p_{m+1}, \ldots, p_{m+1}, p_{m+1} \) be all the distinct prime divisors of \( r \). Then \( (d - N_b)\phi(r) = dr\prod_{p|m} (1 - (1/p)) = \phi(rd), \) which completes the proof of Theorem 7.

Pick \( s \in \Lambda_1 \). Let gcd\((rn, s) = m_s\). Define \( \Lambda_{1,m_s} = \{ s \in \Lambda_1; \gcd(rn, s) = m_s \} \).

**Theorem 11.** Consider

\[ |\Lambda_{1,m_s}| = \frac{\phi(rd)}{\gcd(m_s, r)} = 1, \quad \text{if } \gcd(m_s, r) = 1, \]

\[ 0, \quad \text{if } \gcd(m_s, r) \neq 1, \quad (10) \]

where \( d_s = n/m_s \).

**Proof.** As \( s \in \Lambda_1, s \equiv 1 (\mod r), \) so that \( \gcd(r, s) = 1 \). Since \( m_s \) is a divisor of \( s \), we have that \( \gcd(m_s, r) = 1 \). Thus \( |\Lambda_{1,m_s}| = 1 \), whenever \( m_s \) is not coprime to \( r \).

As \( \gcd(rn, s) = \gcd(n, s) \), \( s = m_s s' \).

Also \( \gcd(d_s, s') = \gcd(n/m_s, s/m_s) = 1 \). As \( s \in \Lambda_1, s \equiv 1 (\mod r) \) holds giving us that \( m_s s' \equiv 1 (\mod r) \) holds with \( \gcd(d_s, s') = 1 \) and \( 0 \leq s' < rd_s \). Hence, Theorem 7, there is \( \phi(d_s)/\phi(r) \) number of elements \( s \in \Lambda_{1,m_s} \) satisfying \( 0 \leq s' < rd_s \), \( \gcd(d_s, s') = 1 \), and \( m_s s' \equiv 1 (\mod r) \).

However, we have to calculate the number of such \( s \in \Lambda_1 \). Now, for \( s \in \Lambda_1, \gcd(rn, s) = m_s \),

\[ |C_s| = \gcd(m_s, \phi(d_s)) = \gcd(m_s, \phi(q^2)). \]

Consequently, \( |\Lambda_{1,m_s}| = \phi(d_s)/\gcd(d_s, \phi(q^2)) \), whenever \( \gcd(m_s, r) = 1 \).

**Example 13** (let \( n = 12, r = 3, \) and \( q = 5 \)).

Then \( O_{12}q(1) = \{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34\} \), \( C_1 = \{1, 25, 13\}, C_4 = \{4, 28, 16\}, C_7 = \{7, 31, 19\}, \) and \( C_{10} = \{10, 34, 22\} \). Take \( \Lambda_1 = \{1, 7, 10\} \). Thus \( |\Lambda_{1,1}| = \{1, 7\} \) as \( C_4 = C_{-20} = C_{-50} \).

So that \( |\Lambda_{1,1}| = 2 \). By Theorem 12, \( d = 3, 6, 12 \) are possible values of \( d \) on right hand side. Now, \( \chi(9, 5) = \chi(18, 5) = 0 \) as \( 5^3 \equiv -1 (\mod 18) \). However, \( \chi(36, 5) = 1 \) as there does not exist any odd integer \( k \) such that \( 5^k \equiv -1 (\mod 36) \), so that

\[ |\Lambda_{1,1}| = \chi(36, 5)\phi(36) = \chi(8, 25) = \frac{12}{3 \times 2} = 2. \]

We will now investigate the behavior of the function \( \chi(d, q) \).

**Lemma 14.** Let \( m_1 \) and \( m_2 \) be two integers coprime to \( q \) such that \( q^{a_1} \equiv -1 (\mod m_1) \) and \( q^{a_2} \equiv -1 (\mod m_2) \) for some odd integers \( a_1 \) and \( a_2 \). If \( q \equiv -1 (\mod 2^{a_2}b) \), where \( 2^a \| m_1 \) and \( 2^b \| m_2 \), then there exists an odd integer \( k \) such that \( q^k \equiv -1 (\mod m_1 m_2) \).

**Proof.** Write \( m_1 m_2 = 2^{a_2}b \prod_{p|m_2} p^e \), being odd distinct primes, \( e_i \equiv 1 \). Let \( p \) be an odd prime divisor of \( m_1 m_2 \), so that there exists an odd integer \( k (= k_1 \lor k_2) \) such that \( q^k \equiv -1 (\mod p) \). Therefore, \( q^{2a_2} \equiv 1 (\mod p) \). Consequently, \( \text{ord}_p(q) \equiv 2a_2 (\mod p) \). Hence, \( q^{2a_2} \equiv -1 (\mod p) \). Thus, \( q^{a_2} \equiv -1 (\mod m_1 m_2) \), where \( k_{pe} = \text{ord}_p(q)/2 \) is odd. Thus,

\[ q^k \equiv -1 (\mod m_1 m_2), \]

(15)

where \( k = \text{lcm}[k_{pe}, e_i=1] \) is odd.

**Lemma 15.** Let \( a \geq 2 \). Then \( q^k \equiv -1 (\mod 2^a) \) holds for some integer \( k \geq 1 \) and only if \( q \equiv -1 (\mod 2^a) \). In fact, such a \( k \) is odd.

**Proof.** Proof is trivial.

**Theorem 16.** \( \chi(rd, q) = 0 \) if and only if \( q \equiv -1 (\mod 2^{a+b}) \) and \( 2|\text{ord}_r(q) \) for all odd prime divisors \( d \) of \( d \), \( 2^a \| d \) and \( 2^b \| r \).

**Proof.** If \( \chi(rd, q) = 0 \), then there exists an odd integer \( k \) such that \( q^k \equiv -1 (\mod rd) \). Thus \( q^{2a} \equiv -1 (\mod 2^{a+b}) \) so that, by Lemma 15, \( q \equiv -1 (\mod 2^{a+b}) \). Also \( q^k \equiv -1 (\mod p) \) for every odd prime divisor \( p \) of \( d \). Thus, \( q^{2a} \equiv -1 (\mod p) \) showing that \( \text{ord}_r(q)2k \) and \( \text{ord}_r(q) \equiv k \). Therefore, \( 2|\text{ord}_r(q) \) for all odd prime divisors \( p \) of \( d \).

Conversely, let \( q \equiv -1 (\mod 2^{a+b}) \) and \( 2|\text{ord}_r(q) \) for all odd prime divisors \( p \) of \( d \). To prove \( \chi(rd, q) = 0 \), we need to find an odd integer \( k \) such that \( q^k \equiv -1 (\mod rd) \). For any odd prime divisor \( p \) of \( d \), as \( 2|\text{ord}_r(q), q^p \equiv -1 (\mod p) \),
where \( k_p = \text{ord}_p(q)/2 \) is odd. As in the proof of Lemma 14, there exists an odd integer \( k_q \) such that \( q^{k_q} \equiv -1 \pmod{d'} \), where \( d = 2^a d' \). Also, \( q \equiv -1 \pmod{2^a} \). Therefore, \( q^{d} \equiv -1 \pmod{d} \) with \( k_q \) odd. By Lemma 1, \( q \equiv -1 \pmod{r} \). Using Lemma 14, we get that \( q^k \equiv -1 \pmod{rd} \), for some odd integer \( k \).

**Proposition 17.** If \( r \) and \( n \) are coprime, then \( \chi(rd, q) = \chi(d, q) \) for all divisors \( d \) of \( n \).

**Proof.** Since \( q \equiv -1 \pmod{r} \) and \( \gcd(r, d) = 1 \), for some odd integer \( k \), \( q^k \equiv -1 \pmod{rd} \) if and only if \( q^k \equiv -1 \pmod{d} \).

**Corollary 18.** There does not exist any nontrivial Hermitian self-orthogonal \( \lambda \)-constacyclic code of length \( n \) over \( \mathbb{F}_{q^2} \) if and only if \( q \equiv -1 \pmod{2^{a+1}} \) and \( 2 \mid \text{ord}_p(q) \) for all prime divisors \( p \) of \( n \), where \( 2^a \mid n \) and \( 2^b \mid r \), for \( r = \text{ord}_d(\lambda) \).

**Proof.** The proof follows easily from Theorems 12 and 16.

For \( n \) odd, we have \( a = 0 \). The condition \( q \equiv -1 \pmod{2^{a+1}} \) reads as \( q \equiv -1 \pmod{2^2} \), which is always true as \( r \mid (q + 1) \). Hence, we have the following.

**Corollary 19.** There does not exist any nontrivial Hermitian self-orthogonal \( \lambda \)-constacyclic code of odd length \( n \) over \( \mathbb{F}_{q^2} \) if and only if \( 2 \mid \text{ord}_p(q) \) for all prime divisors \( p \) of \( n \).

### 3. MDS Hermitian Self-Orthogonal Constacyclic Codes Over \( \mathbb{F}_{q^2} \)

Let \( C \) be a \( \lambda \)-constacyclic code of length \( n \) over \( \mathbb{F}_{q^2} \) and \( \text{ord}_{q^2}(\lambda) = r \). Let \( a \) be a primitive \( rm \) th root of unity in some extension field of \( \mathbb{F}_{q^2} \) such that \( a^\lambda = \lambda \). Then roots of \( C \) are of the form \( a^{r+1} \), \( 0 \leq i \leq n-1 \). Put \( \xi = a^r \).

**Theorem 20.** Let the generator polynomial of \( C \) have roots that include the set \( \{a^{i+1}; 1 \leq i \leq n-d-1 \} \). Then the minimum distance of \( C \) is at least \( d \).

**Proof.** See [1, Theorem 2.2]

By Lemma 1, \( r \mid (q + 1) \). Write \( q + 1 = rs_0 \).

**Theorem 21.** Let \( n \) be a divisor of \( (q-1) \). Let \( T = \text{O}_{r,n}(1) \setminus T_{l,m} \), where \( T_{l,m} = \{ir + 1; 1 \leq i \leq m \} \pmod{mn} \) for each \( m \leq [(n-1-s_0)/2] \) and each \( l \geq l_0 \), with

\[
l_0 = \begin{cases} 
\frac{s_0 - 1}{2}, & \text{if } n \text{ is even}, \\
\frac{s_0 - 2}{2}, & \text{if } n \text{ is odd}.
\end{cases}
\]

Then the code \( C \) with defining set \( T \) is a Hermitian self-orthogonal \( \lambda \)-constacyclic MDS code with parameters \( [n, m-l+1, n-m+1] \).

**Proof.** Let \( l, m \) be as above and

\[
T_{l,m} = \{ir + 1; 1 \leq i \leq m \} \pmod{mn}.
\]

Each \( T_{l,m} \) has \( m-l+1 \) elements. If \( C \) denotes the code with dimension \( T = \text{O}_{r,n}(1) \setminus T_{l,m} \), then the dimension of \( C \), \( \dim C = m - l + 1 \). Let \( l = \{i; l \leq i \leq m \} \). Then the set \( T = \{0, 1, \ldots (n-1)\} \) has \( n-(m-l+1) = n-m-l+1 \) consecutive elements modulo \( n \). By Theorem 20, the minimum distance of \( C \) is at least \( (n-m+l) \). However, using the singleton bound, the minimum distance is at most \( (n-m+l) \). Consequently, the minimum distance of \( C \) equals \( (n-m+l) \), proving that \( C \) is an MDS code.

In order to prove that \( C \) is self-orthogonal, it is enough to prove that \( T_{l,m} \cap (-qT_{l,m}) = \emptyset \). We have \( -q(i+1) \equiv (n-i-s_0)\text{ mod }mn \). Let \( I_1 = \{i; l \leq i \leq m \} \pmod{mn} \) and \( I_2 = \{n-i-s_0; i \in I_1 \} \pmod{mn} \). Then \( T_{l,m} \cap (-qT_{l,m}) = \emptyset \) if and only if \( I_1 \cap I_2 = \emptyset \). Let \( i \in I_1 \cap I_2 \), then \( i = n-j-s_0 \) for some \( j \in I_1 \) so that

\[
s_0 + i + j = n \equiv 0 \pmod{n}.
\]

As \( i, j \) are from \( I_1 \), \( l \leq i \leq j \leq m = [(n-s_0 - 1)/2] \). Thus \( s_0 < 2l \leq 2l + i + j \leq 2[(n-s_0 - 1)/2] \leq n-s_0 < 1 < n-s_0 \) so that

\[
0 < s_0 + i + j < n.
\]

Consequently, there does not exist any \( i, j \) such that both (18) and (19) hold, thereby showing that \( C \) is a Hermitian self-orthogonal constacyclic MDS code.

**Remark 22.** For \( n \) even, \( l = l_0 = -[(s_0 - 1)/2] \) and \( m = [(n-s_0 - 1)/2] \), the codes obtained from above theorem are the same as given by Theorem 4.3 of [6].

**Proposition 23.** Let \( N \) be the number of Hermitian self-orthogonal \( \lambda \)-constacyclic MDS codes of length \( n \) which can be obtained from above theorem. Then \( N \) is given by

\[
N = \begin{cases} 
\frac{n(n-2)}{8}, & \text{if } s \text{ is even, } n \text{ even}, \\
\frac{n(n+2)}{8}, & \text{if } s \text{ is odd, } n \text{ even}, \\
\frac{n(n-1)(n+1)}{8}, & \text{if } s \text{ is even, } n \text{ odd,} \\
\frac{(n-3)(n-1)}{8}, & \text{if } s \text{ is odd, } n \text{ odd.}
\end{cases}
\]

**Proof.** The required number \( N \) equals the number of \( T_{l,m} = \{ir + 1; 1 \leq i \leq m \} \pmod{mn} \); that is, we need to select \( m-l+1 \) consecutive integers from the set \( \{i; l \leq i \leq m \} \). The number of ways of selecting \( t \) consecutive integers from the set \( \{i; e \leq i \leq f \} \) is \( f - e + 2 \). Thus, the number of such codes is

\[
N = \sum_{j=1}^{m-n-l+1} j = (m_0 - l_0 + 1)(m_0 - l_0 + 2)/2.
\]

Hence the result follows.

Tables 2 and 3 list \([n, k, d] \) Hermitian self-orthogonal MDS codes over \( \mathbb{F}_{q^2} \) for \( q \leq 11 \). Here \( n, k, \) and \( d \) denote, respectively, the length, dimension, and minimum distance of the code while \( T \) denotes the defining set. \( N \) denotes the number of such Hermitian self-orthogonal MDS codes.
### Table 2: \([n, k, d]\) Hermitian self-orthogonal MDS codes over \(F_{q^2}\).

<table>
<thead>
<tr>
<th>(q)</th>
<th>(n)</th>
<th>(r)</th>
<th>(N)</th>
<th>(k)</th>
<th>(d)</th>
<th>(T)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>([0, 1, 2])</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>4</td>
<td>([1, 3, 5])</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>([4, 7, 10])</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>([0, 2])</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>([1, 3])</td>
</tr>
<tr>
<td>7</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>([5, 9])</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>([0, 2, 3, 4])</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>([1, 3, 5])</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>([4, 7, 10])</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>([5, 9, 13, 17])</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>([7, 13, 19])</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>([1, 9, 13, 17, 21])</td>
</tr>
<tr>
<td>11</td>
<td>8</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>([9, 17, 25, 33, 41])</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>([0, 2, 3, 4])</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>([1, 3, 5])</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>5</td>
<td>([4, 7, 10])</td>
</tr>
<tr>
<td>11</td>
<td>5</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>([5, 9, 13, 17])</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>([7, 13, 19, 25])</td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>4</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>([1, 9, 13, 17, 21])</td>
</tr>
<tr>
<td>11</td>
<td>8</td>
<td>6</td>
<td>1</td>
<td>6</td>
<td>([9, 17, 25, 33, 41])</td>
<td></td>
</tr>
</tbody>
</table>

### Table 3: \([n, k, d]\) Hermitian self-orthogonal MDS codes over \(F_{q^2}\).

<table>
<thead>
<tr>
<th>(q)</th>
<th>(n)</th>
<th>(r)</th>
<th>(N)</th>
<th>(k)</th>
<th>(d)</th>
<th>(T)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>10</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>([10, 13, 16, 19, 22, 25])</td>
</tr>
<tr>
<td>11</td>
<td>10</td>
<td>4</td>
<td>15</td>
<td>([17, 21, 25, 29, 33])</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>6</td>
<td>10</td>
<td>([25, 31, 37, 43, 49, 55])</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>10</td>
<td>6</td>
<td>([49, 61, 73, 85, 97, 109])</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.
References


Submit your manuscripts at http://www.hindawi.com