Hindawi Publishing Corporation
Journal of Discrete Mathematics
Volume 2014, Article ID 985387, 7 pages
http://dx.doi.org/10.1155/2014/985387

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

Academic Editor: Tamir Tassa

Necessary and sufficient conditions for the existence of Hermitian self-orthogonal constacyclic codes of length n over a finite field $\mathbb{F}_{q^2}$, n coprime to q, are found. The defining sets and corresponding generator polynomials of these codes are also characterised. A formula for the number of Hermitian self-orthogonal constacyclic codes of length n over a finite field $\mathbb{F}_{q^2}$ is obtained. Conditions for the existence of numerous MDS Hermitian self-orthogonal constacyclic codes are obtained. The defining set and the number of such MDS codes are also found.

1. Introduction

Let $\mathbb{F}_{q^2}$ denote a finite field with q^2 elements. An $[n,k]$ linear code C of length n and dimension k over $\mathbb{F}_{q^2}$ is a k-dimensional subspace of the vector space $\mathbb{F}_{q^2}^n$. 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 $\mathbb{F}_{q^2}$ is called λ-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 $\theta : \mathbb{F}_{q^2}^n \to \mathbb{F}_{q^2}[x]/\langle x^n - \lambda\rangle$ be the map given by $\theta((c_0, c_1, \ldots, c_{n-1})) \mapsto c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \bmod (x^n - \lambda)$. One can easily check that θ is an $\mathbb{F}_{q^2}$-module isomorphism. We can therefore identify λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ with ideals in $\mathbb{F}_{q^2}[x]/\langle x^n - \lambda\rangle$. The Hamming weight $w(c)$ of $c \in \mathbb{F}_{q^2}^n$ 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 $[n,k,d]$ code, that is, a $[n,k]$ 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 $u, v \in \mathbb{F}_{q^2}^n$ is defined as $\langle u, v\rangle_H = \sum_{i=0}^{n-1} u_i v_i^q$, 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 $\mathbb{F}_{q^2}$, the Hermitian dual code $C^{\perp_H}$ of C is defined by $C^{\perp_H} = \{v \in \mathbb{F}_{q^2};\ \langle u, v\rangle_H = 0, \forall u \in C\}$. 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 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. 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 formulae to enumerate the number of Euclidean self-dual and self-orthogonal negacyclic codes of length n over a finite field $\mathbb{F}_q$, 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 $\mathbb{F}_{q^2}$, 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).

Table 1: Number of Hermitian self-orthogonal codes over $\mathbb{F}_{25}$.

r	n	N	$\lvert\Lambda_1^{(1)}\rvert$
2	2	2	3
	4	4	9
	6	6	27
	8	4	9
	11	2	3
	12	12	729
	13	6	27
	14	6	27
	16	4	9
	17	2	3
	18	10	243
	19	2	3
	22	6	27
	24	12	729
3	4	2	3
	8	6	27
	11	2	3
	12	2	3
	13	6	27
	16	10	243
	17	2	3
	19	2	3
	22	4	9
	24	6	27
	26	12	729
	28	6	27
	31	10	243
	32	14	2187
6	2	2	3
	4	4	9
	6	2	3
	8	4	9
	11	2	3
	12	4	9
	13	6	27
	14	6	27
	16	4	9
	17	2	3
	18	2	3
	19	2	3
	22	6	27
	24	4	9

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 $[n,k]$ λ-constacyclic code over $\mathbb{F}_{q^2}$ with $r = \mathrm{ord}_{q^2}(\lambda)$, where $\mathrm{ord}_{q^2}(\lambda)$ denotes the order of λ in $\mathbb{F}_{q^2}$. 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 $0 \le s < rn$, let $C_s = \{s, sq^2, \ldots, s(q^2)^{n_s-1}\}$ be the q^2-cyclotomic coset modulo rn containing s, where n_s is the least positive integer such that $s(q^2)^{n_s} \equiv s(\mathrm{mod}\, rn)$. Let α be a primitive rn th root of unity in some extension field of $\mathbb{F}_{q^2}$ such that $\alpha^n = \lambda$. Then the polynomial $M_{(s)}(x) = \prod_{i\in C_s}(x - \alpha^i)$ is the minimal polynomial of α^s over $\mathbb{F}_{q^2}$ and

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

where Λ is the set of representatives of all the distinct q^2-cyclotomic cosets modulo rn. As $(x^n - \lambda) \mid (x^{rn} - 1)$, one can check that the roots of $(x^n - \lambda)$ are precisely α^{ir+1}, $0 \le i < n$. Define

$$O_{r,n}(1) = \{ir + 1;\ 0 \le i < n\}\ (\mathrm{mod}\ rn). \tag{2}$$

Hence we have

$$x^n - \lambda = \prod_{s\in\Lambda_1} M_{(s)}(x), \tag{3}$$

where $\Lambda_1 = \Lambda \cap O_{r,n}(1)$.

Let $C = \langle g(x)\rangle$ be a λ-constacyclic code with defining set $T = \{ir + 1 \in O_{r,n}(1);\ \alpha^{ir+1}$ is a root of $g(x)\}$. Clearly T is a union of some q^2-cyclotomic cosets C_s mod rn for $s \in \Lambda_1$. The Hermitian dual $C^{\perp_H}$ of the code C is a λ^{-q}-constacyclic code over $\mathbb{F}_{q^2}$ with defining set $T^{\perp_H} = -q[O_{r,n}(1) \setminus T]$ mod rn (see Theorem 3.2 of [6]). Write the generator polynomial $g(x)$ of the code C as $g(x) = \prod_{s\in\Lambda_1}(M_{(s)}(x))^{\delta_{(s)}}$, where

$$\delta_{(s)} = \begin{cases} 1, & \text{if } s \in T, \\ 0, & \text{if } s \notin T. \end{cases} \tag{4}$$

Then the generator polynomial of the Hermitian dual $C^{\perp_H}$ of C is $h^{\perp_H}(x) = \prod_{s\in\Lambda_1}(M_{(s)}(x))^{\Delta_{(s)}}$, where

$$\Delta_{(s)} = \begin{cases} 1, & \text{if } s \in T^{\perp_H}, \\ 0, & \text{if } s \notin T^{\perp_H}. \end{cases} \tag{5}$$

It can be easily verified that $\Delta_{(s)} = 1 - \delta_{(-qs)}$ so that $h^{\perp_H}(x) = \prod_{s\in\Lambda_1}(M_{(s)}(x))^{1-\delta_{(-qs)}}$.

Lemma 1. *Let C be a λ-constacyclic code over $\mathbb{F}_{q^2}$ with $\mathrm{ord}_{q^2}(\lambda) = r$. If C is a Hermitian self-orthogonal code, then $r \mid (q + 1)$.*

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

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

Proof. Let C be a nontrivial Hermitian self-orthogonal λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set T. Then there exists $s \in O_{r,n}(1)$ such that $s \neq 0$ and $s \notin T$.

Hence $s \in O_{r,n}(1) \setminus T$ giving us that $-qs \in T^{\perp_H} \subseteq T$. 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 $C_s \neq C_{-qs}$. Consider $T = O_{r,n}(1) \setminus C_s$. The code C is a nontrivial Hermitian self-orthogonal code since $T^{\perp_H} = -q[O_{r,n}(1) \setminus T] = -qC_s = C_{-qs} \subseteq T$. □

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 $\mathbb{F}_{q^2}$.

Theorem 3. *Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ with the defining set T. Then C is Hermitian self-orthogonal if and only if (i) $T_0 \subset T$ and (ii) for each $s \notin T_0$, at least one of s and $-qs$ belongs to T.*

Proof. Let C be a Hermitian self-orthogonal constacyclic code. Let $s \in T_0$. Then $C_s = C_{-qs}$. Suppose that $s \notin T$. Then $-qs \in T^{\perp_H} \subseteq T$ so that $C_{-qs} \subset T$ and $C_s \nsubseteq T$, 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 $-qs \in T^{\perp_H} \subseteq T$, as required.

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

Corollary 4. *A λ-constacyclic code C of length n over $\mathbb{F}_{q^2}$ generated by $g(x) = \prod_{s\in\Lambda_1}(M_{(s)}(x))^{\delta_{(s)}}$ is a Hermitian self-orthogonal if and only if $\delta_{(s)} + \delta_{(-qs)} \geq 1$ for all $s \in \Lambda_1$.*

Define $\Lambda_1^{(0)} = \Lambda_1 \cap T_0$ and $\Lambda_1^{(1)} = \Lambda_1 \setminus \Lambda_1^{(0)}$. Observe that $T_0 = \bigcup_{s\in\Lambda_1^{(0)}} C_s$.

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

$$O_{7,15}(1) = \{1, 8, 15, 22, 29, 36, 43, 50, 57, 64, 71, 78, 85, 92, 99\}, \tag{6}$$

$T_0 = \{15\}$. Let $T = \{1, 15, 22, 36, 43, 50, 64, 99\}$; then $T^{\perp_H} = -13[O_{7,15}(1) \setminus T] = \{1, 22, 36, 43, 50, 64, 99\} \subset T$. Hence, the code with defining set T is a $[15, 7]$ Hermitian self-orthogonal λ-constacyclic code.

Theorem 6. *The number of Hermitian self-orthogonal λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ is $3^{|\Lambda_1^{(1)}|/2}$.*

Proof. Let C be a Hermitian self-orthogonal λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ generated by $g(x) = \prod_{s\in\Lambda_1}(M_{(s)}(x))^{\delta_{(s)}}$. Then $\delta_{(s)} + \delta_{(-qs)} \geq 1$. For $s \in \Lambda_1^{(0)}$, $\delta_{(s)} = \delta_{(-qs)} = 1$. However for $s \in \Lambda_1^{(1)}$, the pairs $(\delta_{(s)}, \delta_{(-qs)})$ have three choices $(0, 1)$, $(1, 0)$, and $(1, 1)$. Hence, the number of Hermitian self-orthogonal λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$ is $3^{|\Lambda_1^{(1)}|/2}$. □

In order to find the number of Hermitian self-orthogonal λ-constacyclic codes of length n over $\mathbb{F}_{q^2}$, we need to compute the value of $|\Lambda_1^{(1)}|$. 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*

$$ax \equiv 1 \pmod{r} \tag{7}$$

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

Since $\gcd(a, r) = 1$, the linear congruence $ax \equiv 1 (\bmod r)$ has a unique solution modulo r. Let it be $x \equiv b (\bmod r)$. Then $\gcd(b, r) = 1$. We write $A = \{ir + s;\ 0 \leq i < d, 0 \leq s < r, \gcd(ir + s, rd) = 1\}$. 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 $A_b = \bigcup_{k=0}^{(d/p)-1} A_b^{(k)}$, where $A_b^{(k)} = \{kpr + b, (kp + 1)r + b, \ldots, ((k + 1)p - 1)r + b\}$ for each k, $0 \leq k < d/p$. Since each $A_b^{(k)}$ contains p elements which are pairwise incongruent mod p, each $A_b^{(k)}$ forms a complete residue system mod p. Hence exactly one element in each $A_b^{(k)}$ 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 $gcd(p_1p_2, r) = 1$. Then the number of multiples of p_1 or p_2 in A_b is $d/p_1 + d/p_2 - d/p_1p_2$.*

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 both p_1 and p_2 equals d/p_1p_2. Therefore the required number is $d/p_1 + d/p_2 - d/p_1p_2$. □

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*

$$N_0 = \sum_{1\leq i\leq m} \frac{d}{p_i} - \sum_{\substack{1\leq i,\, j\leq m \\ i\neq j}} \frac{d}{p_ip_j} + \sum_{\substack{1\leq i,j,k\leq m \\ i,j,k \text{ distinct}}} \frac{d}{p_ip_jp_k} + \cdots + (-1)^{m-1} \frac{d}{p_1p_2\cdots p_m}. \tag{8}$$

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,

$$N = d - \left\{ \sum_{1\le i\le m} \frac{d}{p_i} - \sum_{\substack{1\le i,\, j\le m \\ i\ne j}} \frac{d}{p_i p_j} + \sum_{\substack{1\le i,j,k\le m \\ i,j,k \text{ distinct}}} \frac{d}{p_i p_j p_k} + \cdots + (-1)^{m-1} \frac{d}{p_1 p_2 \cdots p_m} \right\} \tag{9}$$

$$= d \left\{ \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right) \right\}.$$

Let $p_1, p_2, \ldots, p_{m+l}$ be all the distinct prime divisors of d. Also, let $p_{m+1}, \ldots, p_{m+l}, p_{m+l+1}, \ldots, p_{m+l+k}$ be all the distinct prime divisors of r. Then $(d - N_0)\phi(r) = dr\prod_{i=1}^{m+l+k}(1 - (1/p_i)) = \phi(rd)$, 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*

$$\left|\Lambda_{1,m_s}\right| = \begin{cases} \dfrac{\phi(rd_s)}{ord_{rd_s}(q^2)\,\phi(r)}, & \text{if } gcd(m_s, r) = 1, \\ 0, & \text{if } gcd(m_s, r) \ne 1, \end{cases} \tag{10}$$

where $d_s = n/m_s$.

Proof. As $s \in \Lambda_1$, $s \equiv 1 (\bmod r)$, so that $\gcd(r, s) = 1$. Since m_s is a divisor of s, we have that $\gcd(m_s, r) = 1$. Thus $|\Lambda_{1,m_s}| = 0$, whenever m_s is not coprime to r.

As $\gcd(rn, s) = \gcd(n, s) = m_s$, we write $s = m_s s'$. Also $\gcd(d_s, s') = \gcd(n/m_s, s/m_s) = 1$. As $s \in \Lambda_1$, $s \equiv 1(\bmod r)$ holds giving us that $m_s s' \equiv 1(\bmod r)$ holds with $\gcd(d_s, s') = 1$ and $0 \le s' < rd_s$ ($\because 0 \le s < rn$). By Theorem 7, there is $\phi(rd_s)/\phi(r)$ number of elements $s = m_s s'$ in $O_{r,n}(1)$ satisfying $0 \le s' < rd_s$, $\gcd(d_s, s') = 1$, and $m_s s' \equiv 1(\bmod r)$. However, we have to calculate the number of such s in Λ_1. Now, for $s \in \Lambda_1$, $\gcd(rn, s) = m_s$,

$$\left|C_s\right| = \operatorname{ord}_{rn/m_s}\left(q^2\right) = \operatorname{ord}_{rd_s}\left(q^2\right). \tag{11}$$

Consequently, $|\Lambda_{1,m_s}| = \phi(rd_s)/\operatorname{ord}_{rd_s}(q^2)\phi(r)$, whenever $\gcd(m_s, r) = 1$. □

Define

$$\chi(d, q) = \begin{cases} 0, & \text{if } q^k \equiv -1 \,(\bmod d) \text{ for} \\ & \text{some odd integer } k, \\ 1, & \text{otherwise.} \end{cases} \tag{12}$$

Observe that, for $s \in \Lambda_1$, $C_s = C_{-qs}$ holds if and only if $\chi(rd_s, q) = 0$, where $d_s = n/m_s$, $m_s = \gcd(s, n)$ as defined earlier. Recall that, for $s \in \Lambda_1$, $\gcd(m_s, r) = 1$.

Theorem 12. *One has*

$$\left|\Lambda_1^{(1)}\right| = \sum_{\substack{d|n \\ gcd(n/d,r)=1}} \frac{\chi(rd, q)\,\phi(rd)}{\phi(r)\, ord_{\mathrm{rd}}(q^2)}. \tag{13}$$

Proof. The proof follows from Theorem 11 and the above definition. □

Example 13 (let $n = 12$, $r = 3$, and $q = 5$). Then $O_{r,n}(1) = \{1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34\}$, $C_1 = \{1, 25, 13\}$, $C_4 = \{4, 28, 16\}$, $C_7 = \{7, 31, 19\}$, and $C_{10} = \{10, 34, 22\}$. Take $\Lambda_1 = \{1, 4, 7, 10\}$. Thus $\Lambda_1^{(1)} = \{1, 7\}$ (as $C_4 = C_{-20}$ and $C_{10} = C_{-50}$) 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 $5^3 \equiv -1(\bmod 18)$. However, $\chi(36, 5) = 1$ as there does not exist any odd integer k such that $5^k \equiv -1(\bmod 36)$, so that

$$\left|\Lambda_1^{(1)}\right| = \frac{\chi(36, 5)\,\phi(36)}{\phi(3)\,\operatorname{ord}_{36}(25)} = \frac{12}{3 \times 2} = 2. \tag{14}$$

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 $q^{k_1} \equiv -1(\bmod m_1)$ and $q^{k_2} \equiv -1(\bmod m_2)$ for some odd integers k_1 and k_2. If $q \equiv -1(\bmod 2^{a+b})$, where $2^a \| m_1$ and $2^b \| m_2$, then there exists an odd integer k such that $q^k \equiv -1(\bmod m_1 m_2)$.*

Proof. Write $m_1 m_2 = 2^{a+b}\prod_{i=1}^{m} p_i^{e_i}$, p_i being odd distinct primes, $e_i \ge 1$. Let p be an odd prime divisor of $m_1 m_2$, so that there exists an odd integer $t (= k_1$ *or* $k_2)$ such that $q^t \equiv -1(\bmod p)$. Therefore, $q^{2t} \equiv 1(\bmod p)$. Consequently, $\operatorname{ord}_p(q) \mid 2t$ but $\operatorname{ord}_p(q) \nmid t$, giving us that $2 \| \operatorname{ord}_p(q)$. For $e \ge 1$ we have $2 \| \operatorname{ord}_{p^e}(q)$, since $\operatorname{ord}_{p^e}(q) = p^f \operatorname{ord}_p(q)$ for some positive integer f. Hence $q^{k_{p,e}} \equiv -1(\bmod p^e)$, where $k_{p,e} = \operatorname{ord}_{p^e}(q)/2$ is odd. Thus,

$$q^k \equiv -1 \,(\bmod m_1 m_2), \tag{15}$$

where $k = lcm\{k_{p_i,e_i}\}_{i=1}^{m}$ is odd. □

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

Proof. Proof is trivial. □

Theorem 16. *$\chi(rd, q) = 0$ if and only if $q \equiv -1(\bmod 2^{a+b})$ and $2 \| ord_p(q)$ for all odd prime divisors p of d, where $2^a \| d$ and $2^b \| r$.*

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

Conversely, let $q \equiv -1(\bmod 2^{a+b})$ and $2 \| \operatorname{ord}_p(q)$ for all odd prime divisors p of d. To prove $\chi(rd, q) = 0$, we need to find an odd integer k such that $q^k \equiv -1(\bmod rd)$. For any odd prime divisor p of d, as $2 \| \operatorname{ord}_p(q)$, $q^{k_p} \equiv -1(\bmod p)$,

where $k_p = \mathrm{ord}_p(q)/2$ is odd. As in the proof of Lemma 14, there exists an odd integer k_d such that $q^{k_d} \equiv -1 (\mathrm{mod}\, d')$, where $d = 2^a d'$. Also, $q \equiv -1 (\mathrm{mod}\, 2^a)$. Therefore, $q^{k_d} \equiv -1 (\mathrm{mod}\, d)$ with k_d odd. By Lemma 1, $q \equiv -1 (\mathrm{mod}\, r)$. Using Lemma 14, we get that $q^k \equiv -1 (\mathrm{mod}\, rd)$, 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 $q \equiv -1 (\mathrm{mod}\, r)$ and $\gcd(r, d) = 1$, for some odd integer k, $q^k \equiv -1 (\mathrm{mod}\, rd)$ if and only if $q^k \equiv -1 (\mathrm{mod}\, d)$. □

Corollary 18. *There does not exist any nontrivial Hermitian self-orthogonal λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ if and only if $q \equiv -1 (\mathrm{mod}\, 2^{a+b})$ and $2 \| ord_p(q)$ for all odd prime divisors p of n, where $2^a \| n$ and $2^b \| r$, for $r = ord_{q^2}(\lambda)$.*

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

For n odd, we have $a = 0$. The condition $q \equiv -1 (\mathrm{mod}\, 2^{a+b})$ reads as $q \equiv -1 (\mathrm{mod}\, 2^b)$, 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 λ-constacyclic code of odd length n over $\mathbb{F}_{q^2}$ if and only if $2 \| ord_p(q)$ for all prime divisors p of n.*

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

Let C be a λ-constacyclic code of length n over $\mathbb{F}_{q^2}$ and $\mathrm{ord}_{q^2}(\lambda) = r$. Let α be a primitive rn th root of unity in some extension field of $\mathbb{F}_{q^2}$ such that $\alpha^n = \lambda$. Then roots of C are of the form α^{ir+1}, $0 \le i \le n-1$. Put $\zeta = \alpha^r$.

Theorem 20. *Let the generator polynomial of C have roots that include the set $\{\alpha\zeta^i;\ i_1 + 1 \le i \le i_1 + d - 1\}$. 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 $T = O_{r,n}(1) \setminus T_{l,m}$, where $T_{l,m} = \{ir + 1;\ l \le i \le m\}$ $(\mathrm{mod}\, rn)$ for each $m \le \lfloor (n - 1 - s_0)/2 \rfloor$ and each $l \ge l_0$, with*

$$l_0 = \begin{cases} -\left\lfloor \dfrac{s_0 - 1}{2} \right\rfloor, & \text{if } n \text{ is even,} \\ -\left\lfloor \dfrac{s_0 - 2}{2} \right\rfloor, & \text{if } n \text{ is odd.} \end{cases} \tag{16}$$

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

Proof. Let l, m be as above and

$$T_{l,m} = \{ir + 1;\ l \le i \le m\}\,(\mathrm{mod}\, rn). \tag{17}$$

Each $T_{l,m}$ has $m - l + 1$ elements. If C denotes the code with defining set $T = O_{r,n}(1) \setminus T_{l,m}$, then the dimension of C, $\dim C = m - l + 1$. Let $I = \{i;\ l \le i \le m\}$. Then the set $\widehat{I} = \{0, 1, \ldots (n-1)\} \setminus I$ 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 $-q(ir + 1) \equiv (n - i - s_0)r + 1 (\mathrm{mod}\, rn)$. Let $I_1 = \{i;\ l \le i \le m\} (\mathrm{mod}\, n)$ and $I_2 = \{n - i - s_0;\ i \in I_1\} (\mathrm{mod}\, n)$. 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

$$s_0 + i + j = n \equiv 0\,(\mathrm{mod}\, n). \tag{18}$$

As $i, j \in I_1$, $l_0 \le l \le i$, $j \le m \le \lfloor (n - s_0 - 1)/2 \rfloor$. Thus $-s_0 < 2l_0 \le 2l \le i + j \le 2\lfloor (n - s_0 - 1)/2 \rfloor \le n - s_0 - 1 < n - s_0$ so that

$$0 < s_0 + i + j < n. \tag{19}$$

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, $l = l_0 = -\lfloor (s_0 - 1)/2 \rfloor$ and $m = \lfloor (n - s_0 - 1)/2 \rfloor$, 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 λ-constacyclic MDS codes of length n which can be obtained from above theorem. Then N is given by*

$$N = \begin{cases} \dfrac{n(n-2)}{8}, & \text{if } s \text{ is even, } n \text{ even,} \\ \dfrac{n(n+2)}{8}, & \text{if } s \text{ is odd, } n \text{ even,} \\ \dfrac{(n-1)(n+1)}{8}, & \text{if } s \text{ is even, } n \text{ odd,} \\ \dfrac{(n-3)(n-1)}{8}, & \text{if } s \text{ is odd, } n \text{ odd.} \end{cases} \tag{20}$$

Proof. The required number N equals the number of $T_{l,m} = \{ir + 1;\ l \le i \le m\} (\mathrm{mod}\ rn)$; that is, we need to select $m - l + 1$ consecutive integers from the set $\{i;\ l_0 \le i \le m_0 = \lfloor (n - 1 - s_0)/2 \rfloor\}$. The number of ways of selecting t consecutive integers from the set $\{i;\ e \le i \le f\}$ is $(f - e - t + 2)$. Thus, the number of such codes is $N = \sum_{j=1}^{m_0 - l_0 + 1} j = (m_0 - l_0 + 1)(m_0 - l_0 + 2)/2$. Hence the result follows. □

Tables 2 and 3 list $[n, k, d]$ Hermitian self-orthogonal MDS codes over $\mathbb{F}_{q^2}$ for $q \le 11$. 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 $\mathbb{F}_{q^2}$.

q	n	r	N	k	d	T
5	4	1	1	1	4	$\{0, 1, 2\}$
5	4	2	3	2	3	$\{3, 5\}$
				1	4	$\{1, 3, 5\}$
				1	4	$\{3, 5, 7\}$
5	4	3	1	1	4	$\{4, 7, 10\}$
5	4	6	3	2	3	$\{13, 19\}$
				1	4	$\{7, 13, 19\}$
				1	4	$\{1, 13, 19\}$
7	3	1	1	1	3	$\{0, 2\}$
7	3	2	1	1	3	$\{1, 3\}$
7	3	4	1	1	3	$\{5, 9\}$
7	6	1	3	2	5	$\{0, 1, 2, 3\}$
				1	6	$\{0, 1, 2, 3, 4\}$
				1	6	$\{0, 1, 2, 3, 5\}$
7	6	2	3	2	5	$\{3, 5, 7, 9\}$
				1	6	$\{1, 3, 5, 7, 9\}$
				1	6	$\{3, 5, 7, 9, 11\}$
7	6	4	3	2	5	$\{9, 13, 17, 21\}$
				1	6	$\{1, 9, 13, 17, 21\}$
				1	6	$\{5, 9, 13, 17, 21\}$
7	6	8	6	3	4	$\{25, 33, 41\}$
				2	5	$\{17, 25, 33, 41\}$
				2	5	$\{1, 25, 33, 41\}$
				1	6	$\{9, 17, 25, 33, 41\}$
				1	6	$\{1, 17, 25, 33, 41\}$
				1	6	$\{1, 9, 25, 33, 41\}$
11	5	1	3	2	4	$\{0, 3, 4\}$
				1	5	$\{0, 2, 3, 4\}$
				1	5	$\{0, 1, 3, 4\}$
11	5	2	3	2	4	$\{1, 3, 5\}$
				1	5	$\{1, 3, 5, 9\}$
				1	5	$\{1, 3, 5, 7\}$
11	5	3	3	2	4	$\{4, 7, 10\}$
				1	5	$\{1, 4, 7, 10\}$
				1	5	$\{4, 7, 10, 13\}$
11	5	4	1	1	5	$\{5, 9, 13, 17\}$
11	5	6	3	2	4	$\{13, 19, 25\}$
				1	5	$\{7, 13, 19, 25\}$
				1	5	$\{1, 13, 19, 25\}$
11	5	12	1	1	5	$\{25, 37, 49, 1\}$
11	10	1	10	4	7	$\{0, 1, 2, 3, 4, 5\}$
				3	8	$\{0, 1, 2, 3, 4, 5, 9\}$
				3	8	$\{0, 1, 2, 3, 4, 5, 6\}$
				2	9	$\{0, 1, 2, 3, 4, 5, 8, 9\}$
				2	9	$\{0, 1, 2, 3, 4, 5, 6, 9\}$
				2	9	$\{0, 1, 2, 3, 4, 5, 6, 7\}$
				1	10	$\{0, 1, 2, 3, 4, 5, 7, 8, 9\}$
				1	10	$\{0, 1, 2, 3, 4, 5, 6, 8, 9\}$
				1	10	$\{0, 1, 2, 3, 4, 5, 6, 7, 9\}$
				1	10	$\{0, 1, 2, 3, 4, 5, 6, 7, 8\}$
11	10	2	10	4	7	$\{5, 7, 9, 11, 13, 15\}$
				3	8	$\{3, 5, 7, 9, 11, 13, 15\}$
				3	8	$\{5, 7, 9, 11, 13, 15, 17\}$
				2	9	$\{1, 3, 5, 7, 9, 11, 13, 15\}$
				2	9	$\{3, 5, 7, 9, 11, 13, 15, 17\}$
				2	9	$\{5, 7, 9, 11, 13, 15, 17, 19\}$
				1	10	$\{1, 3, 5, 7, 9, 11, 13, 15, 19\}$
				1	10	$\{1, 3, 5, 7, 9, 11, 13, 15, 17\}$
				1	10	$\{3, 5, 7, 9, 11, 13, 15, 17, 19\}$
				1	10	$\{1, 5, 7, 9, 11, 13, 15, 17, 19\}$

Table 3: $[n, k, d]$ Hermitian self-orthogonal MDS codes over $\mathbb{F}_{q^2}$.

q	n	r	N	k	d	T
11	10	3	10	4	7	$\{10, 13, 16, 19, 22, 25\}$
				3	8	$\{7, 10, 13, 16, 19, 22, 25\}$
				3	8	$\{10, 13, 16, 19, 22, 25, 28\}$
				2	9	$\{4, 7, 10, 13, 16, 19, 22, 25\}$
				2	9	$\{7, 10, 13, 16, 19, 22, 25, 28\}$
				2	9	$\{1, 10, 13, 16, 19, 22, 25, 28\}$
				1	10	$\{1, 4, 7, 10, 13, 16, 19, 22, 25\}$
				1	10	$\{4, 7, 10, 13, 16, 19, 22, 25, 28\}$
				1	10	$\{1, 7, 10, 13, 16, 19, 22, 25, 28\}$
				1	10	$\{1, 4, 10, 13, 16, 19, 22, 25, 28\}$
11	10	4	15	5	6	$\{17, 21, 25, 29, 33\}$
				4	7	$\{13, 17, 21, 25, 29, 33\}$
				4	7	$\{17, 21, 25, 29, 33, 37\}$
				3	8	$\{9, 13, 17, 21, 25, 29, 33\}$
				3	8	$\{13, 17, 21, 25, 29, 33, 37\}$
				3	8	$\{1, 17, 21, 25, 29, 33, 37\}$
				2	9	$\{5, 9, 13, 17, 21, 25, 29, 33\}$
				2	9	$\{9, 13, 17, 21, 25, 29, 33, 37\}$
				2	9	$\{1, 13, 17, 21, 25, 29, 33, 37\}$
				2	9	$\{1, 5, 17, 21, 25, 29, 33, 37\}$
				1	10	$\{1, 5, 9, 13, 17, 21, 25, 29, 33\}$
				1	10	$\{5, 9, 13, 17, 21, 25, 29, 33, 37\}$
				1	10	$\{1, 9, 1317, 21, 25, 29, 33, 37\}$
				1	10	$\{1, 5, 1317, 21, 25, 29, 33, 37\}$
				1	10	$\{1, 5, 9, 17, 21, 25, 29, 33, 37\}$
11	10	6	10	4	7	$\{25, 31, 37, 43, 49, 55\}$
				3	8	$\{19, 25, 31, 37, 43, 49, 55\}$
				3	8	$\{1, 25, 31, 37, 43, 49, 55\}$
				2	9	$\{13, 19, 25, 31, 37, 43, 49, 55\}$
				2	9	$\{1, 19, 25, 31, 37, 43, 49, 55\}$
				2	9	$\{1, 7, 25, 31, 37, 43, 49, 55\}$
				1	10	$\{7, 13, 19, 25, 31, 37, 43, 49, 55\}$
				1	10	$\{1, 13, 19, 25, 31, 37, 43, 49, 55\}$
				1	10	$\{1, 7, 19, 25, 31, 37, 43, 49, 55\}$
				1	10	$\{1, 7, 13, 25, 31, 37, 43, 49, 55\}$
11	10	12	15	5	6	$\{61, 73, 85, 97, 109\}$
				4	7	$\{49, 61, 73, 85, 97, 109\}$
				4	7	$\{1, 61, 73, 85, 97, 109\}$
				3	8	$\{37, 49, 61, 73, 85, 97, 109\}$
				3	8	$\{1, 49, 61, 73, 85, 97, 109\}$
				3	8	$\{1, 13, 61, 73, 85, 97, 109\}$
				2	9	$\{25, 37, 49, 61, 73, 85, 97, 109\}$
				2	9	$\{1, 37, 49, 61, 73, 85, 97, 109\}$
				2	9	$\{1, 13, 49, 61, 73, 85, 97, 109\}$
				2	9	$\{1, 13, 25, 61, 73, 85, 97, 109\}$
				1	10	$\{13, 25, 37, 49, 61, 73, 85, 97, 109\}$
				1	10	$\{1, 25, 37, 49, 61, 73, 85, 97, 109\}$
				1	10	$\{1, 13, 37, 49, 61, 73, 85, 97, 109\}$
				1	10	$\{1, 13, 25, 49, 61, 73, 85, 97, 109\}$
				1	10	$\{1, 13, 25, 3761, 73, 85, 97, 109\}$

Conflict of Interests

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

References

[1] N. Aydin, I. Siap, and D. K. Ray-Chaudhuri, "The structure of 1-generator quasi-twisted codes and new linear codes," *Designs, Codes and Cryptography*, vol. 24, no. 3, pp. 313–326, 2001.

[2] T. A. Gulliver, J.-L. Kim, and Y. Lee, "New MDS or near-MDS self-dual codes," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4354–4360, 2008.

[3] T. Blackford, "Negacyclic duadic codes," *Finite Fields and Their Applications*, vol. 14, no. 4, pp. 930–943, 2008.

[4] K. Guenda, "New MDS self-dual codes over finite fields," *Designs, Codes and Cryptography*, vol. 62, no. 1, pp. 31–42, 2012.

[5] A. Sahni and P. T. Sehgal, "Enumeration of self-dual and self-orthogonal negacyclic codes over finite fields," In press.

[6] Y. Yang and W. Cai, "On self-dual constacyclic codes over finite fields," *Designs, Codes, and Cryptography*, 2013.

[7] H. Q. Dinh and S. R. Lopez-Permouth, "Cyclic and negacyclic codes over finite chain rings," *IEEE Transactions on Information Theory*, vol. 50, no. 8, pp. 1728–1744, 2004.