Des. Codes Cryptogr. (2012) 62:31–42
DOI 10.1007/s10623-011-9489-x

New MDS self-dual codes over finite fields

Kenza Guenda

Received: 27 October 2010 / Revised: 24 January 2011 / Accepted: 8 February 2011 /
Published online: 3 March 2011

Abstract In this paper we construct MDS Euclidean and Hermitian self-dual codes which are extended cyclic duadic codes or negacyclic codes. We also construct Euclidean self-dual codes which are extended negacyclic codes. Based on these constructions, a large number of new MDS self-dual codes are given with parameters for which self-dual codes were not previously known to exist.

Keywords Self-dual codes · MDS codes · Cyclic codes · Negacyclic codes

Mathematics Subject Classification (2000) 94B05 · 94B15

1 Introduction

Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. An $[n, k]$ linear code C over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. A linear code over $\mathbb{F}_q^n$ is said to be constacyclic if it is an ideal of the quotient ring $R_n = \mathbb{F}_q[x]/\langle x^n - a\rangle$. When $a = 1$ the code is called cyclic and when $a = -1$ the code is called negacyclic. For $\mathsf{x} \in C$, the Hamming weight $wt(\mathsf{x})$ is the number of nonzero coordinates in x. The minimum distance d of C is defined as $d = \min\{wt(\mathsf{x}) : 0 \neq \mathsf{x} \in C\}$. If the parameters of the code C satisfy $n - k + 1 = d$, then the code is said to be maximum distance separable (MDS). The minimum distance of a code is related to its error correcting capability. In this sense MDS codes are optimal. Furthermore, MDS codes are related to geometric objects called n-arcs and to combinatorial called orthogonal arrays [14, Chapter 11], which have applications in algebraic geometry.

Communicated by V. A. Zinoviev.

K. Guenda (✉)
Faculty of Mathematics, USTHB, University of Sciences and Technology of Algiers,
B.P 32 El Alia, Bab Ezzouar, Algiers, Algeria
e-mail: kguenda@gmail.com

The Euclidean dual code $C^{\perp}$ of C is defined as $C^{\perp} = \left\{ \mathsf{x} \in \mathbb{F}_q^n : \sum_{i=1}^n x_i y_i = 0 \, \forall \, \mathsf{y} \in C \right\}$. If $q = p^2$ the Hermitian dual code $C^{\perp h}$ of C is defined as $C^{\perp h} = \left\{ \mathsf{x} \in \mathbb{F}_q^n : \sum_{i=1}^n x_i y_i^p = 0 \, \forall \, \mathsf{y} \in C \right\}$. An interesting class of codes is the so-called self-dual codes. A code is called Euclidean self-dual or Hermitian self-dual if it satisfies $C = C^{\perp}$ or $C = C^{\perp h}$, respectively. For $q \equiv 1 \pmod 4$ there exists a self-dual code over $\mathbb{F}_q$ if and only if n is even, and for $q \equiv 3 \pmod 4$ there exists a self-dual code over $\mathbb{F}_q$ if and only if $n \equiv 0 \pmod 4$ [14, Chapter 19]. In this paper, we construct MDS Euclidean and Hermitian self-dual codes which are extended cyclic duadic codes or negacyclic codes. We also construct Euclidean self-dual codes which are extended negacyclic codes. These constructions provide a large number of new MDS self-dual codes with parameters for which self-dual codes were not previously known to exist.

Our results can also be considered as a construction of MDS self-dual codes over finite fields. This has been the subject of many recent research papers [8,12]. Many of the known codes were obtained using a computer search, which is computationally complex. The constructions presented here are much simpler in comparison, which allows us to obtain MDS self-dual codes with large parameters. In [7] Gulliver and Grassl constructed MDS self-dual codes over $\mathbb{F}_q$ of length $q+1$ for $q \leq 49$ by puncturing cyclic or constacyclic codes. We also consider the MDS self-dual codes of length $q+1$, but our construction is totally different from the ones given in [7]. Note that Krishna and Sarwate in [13] considered constacyclic MDS codes. However, the self-duality of these codes was not considered. Blackford [2] studied negacyclic codes over finite fields using multipliers. He gave conditions regarding the existence of Euclidean self-dual codes. We generalize his results to the Hermitian self-dual case, and give necessary and sufficient conditions for the existence of Hermitian self-dual negacyclic codes. Hence, using our previous results, the decomposition of the polynomial x^n+1 and the results of Blackford we construct new MDS Euclidean and Hermitian self-dual codes which are negacyclic. Furthermore, we give conditions on the existence of Euclidean self-dual codes which are extended duadic negacyclic codes.

This paper is organized as follows. In Sect. 2 we construct MDS self-dual codes (Euclidean and Hermitian) which are extended cyclic duadic codes. First we give cyclic MDS codes over $\mathbb{F}_q$ when n divides $q-1$ and n divides q^2+1. Furthermore, by using a result from [6] on the existence of the μ_{-q} splitting we give new MDS Euclidean and Hermitian self-dual codes which are extended duadic codes. In Sect. 3 we generalize the work of [2] to the Hermitian case. We give necessary and sufficient conditions on the existence of negacyclic Hermitian self-dual codes. We construct negacyclic MDS self-dual codes for both the Euclidean and Hermitian cases. In the last Section we construct Euclidean self-dual codes which are extended duadic negacyclic codes.

Several examples of the codes obtained from our papers are given. Some of them reach or even exceed the best known bounds given in [3,8,12].

Throughout this paper $\mathrm{ord}_n(q)$ denotes the multiplicative order of q modulo n, that is the smallest integer r such that $q^r \equiv 1 \pmod n$. Let $\mathcal{Q}_n$ denote the set of nonzero squares modulo n [11]. The set $\mathcal{Q}_n$ is called the quadratic residues modulo n.

2 MDS self-dual codes from cyclic Duadic codes

In this section n is an odd integer and q a prime power such that $(n, q) = 1$. For an integer a such that $(a, n) = 1$, the multiplier is a permutation μ_a on $Z_n = \{0, \ldots, n-1\}$ defined by:

$$\mu_a : i \longmapsto ia \pmod n.$$

We recall that a cyclic code C of length n over $\mathbb{F}_q$ is an ideal of the ring $R = \mathbb{F}_q[x]/(x^n - 1)$ generated by a polynomial $g(x)$ which divides $x^n - 1$.C is uniquely determined by its defining set $T = \{0 \leq i \leq 1 |\ g(\alpha^i) = 0\}$, where α is an nth primitive root of the unity. The set T is then a union of cyclotomic classes $C(j) = \{jq^l \pmod n \,|\, l \in \mathbb{N}\}$.

Lemma 1 ([5,11, Proposition 4.7,Theorem 4.4.9]) *Let C be an $[n, k]$ cyclic code over $\mathbb{F}_q$ with defining set $T \subset Z_n = \{0, 1, \ldots, n-1\}$. Then the following holds*:

(i) *The Euclidean dual $C^{\perp}$ is also cyclic and has defining set $\{i \in Z_n : i \notin -T\}$.*
(ii) *The Hermitian dual $C^{\perp h}$ is also cyclic and has defining set $\{i \in Z_n : i \notin -qT$.*

Now, let S_1 and S_2 be unions of cyclotomic classes modulo n, such that $S_1 \cap S_2 = \emptyset$, $S_1 \cup S_2 = Z_n \setminus \{0\}$ and $aS_i \pmod n = S_{i+1 \pmod 2}$. Then the triple μ_a, S_1, S_2 is called a splitting modulo n. The odd-like duadic codes D_1 and D_2 are the cyclic codes over $\mathbb{F}_q$ with defining sets S_1 and S_2, respectively. The even-like duadic codes C_1 and C_2 are the cyclic codes over $\mathbb{F}_q$ with defining sets $\{0\} \cup S_1$ and $\{0\} \cup S_2$, respectively.

Smid proved in [15, Theorem 1] that a duadic code of length n over $\mathbb{F}_q$ exists if and only if $q \in \mathcal{Q}_n$. The proof of the following Lemma can be found in [13].

Lemma 2 *Let q be a prime power and α be a primitive nth root of unity. If n divides $q - 1$, then the polynomial $g_j(x) = \prod_{i=j}^{n-k+j-1} (x - \alpha^i)$ generates an $[n, k]$ MDS code over $\mathbb{F}_q$.*

2.1 Euclidean self-dual MDS codes over $\mathbb{F}_q$

Let n be an odd integer which divides $q - 1$, hence q is a quadratic residue modulo n. Then from [15, Theorem 1], there exists a pair of duadic codes of length n. We now construct some of these duadic codes. Consider the cyclic code D_1 with defining set $T_1 = \left\{1, 2, \ldots, \frac{(n-1)}{2}\right\}$. By Lemma 2, the code D_1 is an $\left[n, \frac{(n+1)}{2}, \frac{(n+1)}{2}\right]$ MDS code over $\mathbb{F}_q$, and by Lemma 1 its dual $C_1 = D_1^{\perp}$ is also cyclic with defining set $T_1 \cup \{0\}$. The code C_1 is self-orthogonal as $T_1 \subset T_1 \cup \{0\}$, and it has dimension $\frac{n-1}{2}$ and minimum distance $\frac{n+3}{2}$. Hence C_1 is also MDS.

This gives that C_1 is an even-like duadic code whose splitting is given by μ_{-1} due to the following Lemma.

Lemma 3 ([11, Theorem 6.4.1]) *Let C be any $\left[n, \frac{n-1}{2}\right]$ cyclic code over $\mathbb{F}_q$, with q a prime power. Then C is self-orthogonal if and only if C is an even like duadic code whose splitting is given by μ_{-1}.*

This gives us a pair of duadic codes $D_1 = C_1^{\perp}$ and $D_2 = C_2^{\perp}$, and a pair of even like duadic codes $C_2 = \mu_{-1}(C_1)$. Hence we have the following result.

Lemma 4 *Let n be an odd integer which divides $q - 1$. Then there exists a pair of MDS codes D_1 and D_2 with parameters $\left[n, \frac{(n+1)}{2}, \frac{(n+1)}{2}\right]$, which are duadic codes with splitting given by μ_{-1}.*

Since n is odd, we want to extend the codes $D_i, i = 1, 2$, in such a way that the extended code is self-dual. This is possible provided that the following Lemma is satisfied.

Lemma 5 ([11, Theorem 6.4.12]) *Let D_1 and D_2 be a pair of odd-like duadic codes of length n over $\mathbb{F}_q$. Assume that*

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

has a solution in $\mathbb{F}_q$. If μ_{-1} gives the splitting from D_1 and D_2, then $\widetilde{D_1}$ and $\widetilde{D_2}$ are self-dual codes, where $\widetilde{D_i} = \{\widetilde{\mathsf{c}} \,|\, \mathsf{c} \in D_i\}$ for $1 \leq i \leq 2$ and $\widetilde{\mathsf{c}} = c_0 \ldots c_n c_\infty$ with $c_\infty = -\gamma \sum_{i=0}^{n-1} c_i$.

In general it is not always possible to find a solution to (1) in $\mathbb{F}_q$. Furthermore, extending an MDS code does not always give an MDS code. However, under some conditions this is possible, as proved by Hill [10]. For $n = q - 1$, $\gamma = 1$ is a solution of (1). Moreover, if the code is a Reed-Solomon code, then from MacWilliams and Sloane [14, Theorem 10.3.1], the extended code is also MDS. In the landmark textbook [11] the solution of (1) is discussed when n is an odd prime. The following Lemma generalizes their results to $n = p^m$.

Lemma 6 *Let $q = r^t$, with r an odd prime, t an odd integer and $n = p^m$ such that n divides $q - 1$. Then there is a solution to (1) in $\mathbb{F}_q$, whenever one of the following cases hold.*

1. $r \equiv 3 \pmod 4$, $p \equiv 3 \pmod 4$ *and m odd*;
2. $r \equiv 1 \pmod 4$ *and* $p \equiv 1$ *or* $3 \pmod 4$;

Proof As mentioned above, if n divides $q - 1$, then $q \in \mathcal{Q}_p$. This gives that $q \in \mathcal{Q}_r$. Hence if $p \equiv 3 \pmod 4$ and $r \equiv 3 \pmod 4$, there is a solution γ in $\mathbb{F}_q$ to $1 + \gamma^2 p = 0$ [11, Lemma 6.6.17]. If m is odd, hence γ^m is a solution to (1). Now, assume $r \equiv 1 \pmod 4$ and $p \equiv 1$ or $3 \pmod 4$. Then $1 + \gamma^2 p = 0$ [11, Lemma 6.6.17] has a solution in $\mathbb{F}_q$. For the previous case with m odd, γ^m is a solution to (1). Now, assume that m is even. Then there exist p and q such that there is a solution to $1 + \gamma^2 p = 0$ in $\mathbb{F}_q$ [11, Lemma 6.6.17]. This gives $(\gamma^m)^2 = \frac{1}{p^m}$. Since $r \equiv 1 \pmod 4$, -1 is a quadratic residue in $\mathbb{F}_r \subset \mathbb{F}_q$ [11, Lemma 6.2.4]. Then, there exists $a \in \mathbb{F}_q$ such that $a^2 = -1$. Hence $a\gamma^m$ is a solution of (1) in $\mathbb{F}_q$. □

We next give Euclidean self-dual codes which are MDS.

Theorem 7 *Let $q = r^t$ be a prime power (even or odd), and n an odd divisor of $q - 1$. Then there exists a pair D_1, D_2 of MDS odd-like duadic codes of length n, with splitting μ_{-1}, where the even-like duadic codes are MDS self-orthogonal and $T_1 = \left\{1, \ldots, \frac{n-1}{2}\right\}$. Furthermore, the following holds:*

(i) *If $q = 2^t$, with t odd and $n = p$ an odd prime, then the extended codes $\widetilde{D_i}$ are $\left[n + 1, \frac{n+1}{2}, \frac{n+3}{2}\right]$ MDS Euclidean self-dual codes.*
(ii) *If $q = r^t$, with t even and n an odd integer that divides $r - 1$, then the extended codes $\widetilde{D_i}$ for $1 \le i \le 2$ are $\left[n + 1, \frac{n+1}{2}, \frac{n+3}{2}\right]$ MDS Euclidean self-dual codes.*
(iii) *If $q = r^t$, with $r \equiv 3 \pmod 4$, t odd and $n = p^m$, with p a prime such that $p \equiv 3 \pmod 4$ and m odd, then the extended codes $\widetilde{D_i}$ are $\left[n + 1, \frac{n+1}{2}, \frac{n+3}{2}\right]$ MDS Euclidean self-dual codes.*
(iv) *If $q = r^t$, with t odd, p a prime such that $r \equiv p \equiv 1 \pmod 4$ and $n = p^m$, then the extended codes $\widetilde{D_i}$ are $\left[n + 1, \frac{n+1}{2}, \frac{n+3}{2}\right]$ MDS Euclidean self-dual codes.*

Proof Lemma 4 gives a pair D_1, D_2 of MDS odd-like duadic codes of length n, with splitting μ_{-1} and where the even-like duadic codes are MDS self-orthogonal with $T_1 = \left\{1, \ldots, \frac{n-1}{2}\right\}$. If $q = 2^t$, t odd and $n = p$ an odd prime which divides $q - 1$, then $q \in \mathcal{Q}_n$. From [11, Lemma 6.6.17], there is a solution to (1) in $\mathbb{F}_q$. Hence from Lemma 5, the extended codes $\widetilde{D_i}$ are self-dual. If t is even and n an odd integer which divides $r - 1$, from [11] p. 227 there is a solution of (1) in $\mathbb{F}_{r^2} \subset \mathbb{F}_q$, since the coefficients are in $\mathbb{F}_r$. Further, if we assume $r \equiv 3 \pmod 4$, t odd and $n = p^m$ with m odd and such that $p \equiv 3 \pmod 4$, by Lemma 6, there is a solution to (1). Hence from Lemma 5 the extended codes $\widetilde{D_i}$ are self-dual. Similarly if we assume $r \equiv 1 \pmod 4$, t odd and $n = p^m$ such that $p \equiv 1$ or $3 \pmod 4$, we have a solution to (1) by Lemma 6. Hence from Lemma 5 the extended codes $\widetilde{D_i}$ are self-dual. Now we prove that the $\widetilde{D_i}$ are MDS. Let c be a codeword of D_i of weight $\frac{n+1}{2}$. The minimum weight of $\widetilde{D_i}$ is increasing by 1 provided

Table 1 New Euclidean self-dual MDS codes of length N over $\mathbb{F}_q$

N	q
4	79, 97, 13^2, 31^2 (7)
6	9^2, 11^2, 31^2 (7) 53, 197 (11) 61, 73 (12)
8	2^9 (7)
10	19^2 (7) 13^2 (11) 9^2 (12)
14	53^2 (7)
16	31^2 (7)
18	137, 103^2 (7) 197, 233, 269 (11) 109, 181 (12)
20	9^2, 11^2 (12)
22	109, 197 (11)
24	2^{11} (7) 7^2, 193 (12)
26	181, 233 (11) 53, 157 (12)
28	13^2, 281, 337 (12)
30	59^2 (7) 89, 149 (11) 61, 11^2, 181 (12)
32	5^3 (7)
34	101, 13^2 (11) 409 (12)
36	73, 433 (12)
38	113 (11)
42	293, 461 (11)
50	7^2, 149 (11)
54	53, 269 (11)
74	293, 2^9 (7)
84	167 (7)
90	2^{11} (7)

The Theorem providing the construction is given in brackets

$$-\gamma \mathtt{c}(1) = -\gamma \sum_{i=0}^{n-1} c_i = c_\infty \neq 0. \tag{2}$$

but $\gamma \neq 0$, hence to satisfy (2) it suffices to verify that $\mathtt{c}(1) \neq 0$ since $c(x) = a(x)g(x)$ for some $a(x) \pmod{x^n - 1}$ and $g(x) = \prod_{i=1}^{\frac{n-1}{2}} \left(x - \alpha^i\right)$. Now $g(1) \neq 0$ and $a(1) \neq 0$, otherwise, $a(x)$ is a multiple of $(x-1)g(x)$. Hence by the BCH bound the weight is $\geq 1+\frac{n+1}{2}$, and by the Singleton bound we obtain equality. □

Some new codes obtained using Theorem 7 are given in Table 1.

2.2 Hermitian self-dual MDS codes

Let q be a power of an odd prime r. In this section, we construct MDS self-dual codes over $\mathbb{F}_{q^2}$ of length $n+1$ with $n|q^2+1$.

First, note that when n divides q^2+1, we have $\mathrm{ord}_n\left(q^2\right) = 2$. This implies that all the cyclotomic classes $C(i)$ modulo n are reversible with cardinality 1 or 2, because $|C(i)|$ divides $\mathrm{ord}_n\left(q^2\right)$ [11, Theorem 4.1.4]. It then follows that $C(i) = \{i, -i\}$ for any i. The cyclic code generated by the polynomial

$$g_s(x) = \prod_{i=\frac{n-1}{2}-s}^{i=\frac{n-1}{2}+s+1} \left(x - \alpha^i\right) \text{ with } 0 \leq s \leq \frac{n-1}{2},$$

is an $[n, n-2s-2, 2s+3]$ MDS code. The polynomial $g_s(x)$ has $2s+2$ consecutive roots

$$\alpha^{\frac{n-1}{2}-s}, \alpha^{\frac{n-1}{2}-s+1}, \ldots, \alpha^{\frac{n-1}{2}+1}, \ldots, \alpha^{\frac{n-1}{2}+s+1}.$$

This gives a cyclic MDS code with odd dimension $k = n - 2s - 2$.

Now, consider $n = p^m$ such that n divides q^2+1 and $p^m \equiv 1 \pmod 4$. For $s = \frac{n-1}{4} - 1$, the polynomial g_s generate a cyclic MDS code D_1 with parameters $\left[n, \frac{n+1}{2}, \frac{n+1}{2}\right]$. Lemma 1 gives that the Hermitian dual of D_1 has defining set $Z_n \setminus (-qT)$. Since $\text{ord}_n\left(q^2\right)$ is even (equal to 2), then the multiplier μ_{-q} gives a splitting [6, Proposition 13]. Hence D_1 is an odd-like duadic code and $D_1^{\perp_h} = C_1$ is the even like duadic code with defining set $T \cup \{0\}$. Therefore $C_i \subset C_i^{\perp_h} = D_i$. As for the Euclidean case, the usual extension of an orthogonal code does not always give a self-dual code. Consider the following expression in $\mathbb{F}_{q^2}$

$$1 + \gamma^{q+1} n = 0, \tag{3}$$

which always a solution in $\mathbb{F}_{q^2}$ if we assume $n \in \mathbb{F}_r$. This is because we have $n^q = n$, or equivalently $n^{q+1} = n^2$, so that $1 + \gamma^{q+1} n = 0 \iff n + \gamma^{q+1} n^2 = 0 \iff n + (\gamma n)^{q+1} = 0$. Then (3) is equivalent to

$$n + \gamma^{q+1} = 0 \tag{4}$$

Note that $\left\{a^{q+1} \mid a \in \mathbb{F}_{q^2}\right\} = \mathbb{F}_q$. Hence (4) always has a solution in $\mathbb{F}_{q^2}$, which implies that (3) is solvable in $\mathbb{F}_{q^2}$. For $1 \leq i \leq 2$, the extended codes are $\widetilde{D_i} = \{\widetilde{\mathtt{c}} \mid \mathtt{c} \in D_i\}$, with $\widetilde{\mathtt{c}} = c_0 \ldots c_n c_\infty, c_\infty = -\gamma \sum_{i=0}^{n-1} c_i$ and γ is the solution of (3). Since in this case the splitting is given by μ_{-q}, the codes $\widetilde{D_i}$ are Hermitian self-dual [5, Proposition 4.8]. By a similar argument to that in Theorem 7, the extended codes are also MDS, since the codes D_i are MDS. This proves the following Theorem.

Theorem 8 *Let $q = r^t$ be a prime power, and $n = p^m \in \mathbb{F}_r$ a divisor of q^2+1, where $p^m \equiv 1 \pmod 4$. Then there exists Hermitian self-dual codes over $\mathbb{F}_{q^2}$ which are MDS and extended duadic codes with the splitting given by μ_{-q} and with parameters $\left[n+1, \frac{n+1}{2}, \frac{n+3}{2}\right]$.*

Some new codes obtained using Theorem 8 are given in Table 2.

3 Negacyclic MDS self-dual codes

It was proven in [9] that if n is odd, then the negacyclic codes are equivalent to cyclic codes. Thus we only consider negacyclic codes with even length.

For use later, we review the factorization of the polynomial $x^n + 1$ over $\mathbb{F}_q[x]$. This can be found in [1,13]. We also assume $(n, q) = 1$, so that $x^n + 1$ does not have multiple roots. The roots of $x^n + 1$ are $\delta, \delta\xi, \ldots, \delta\xi^{n-1}$, where ξ is a primitive nth root of unity and $\delta^n = -1$. Hence $\xi = \delta^2$, where δ is a primitive $2n$th root of unity. Thus δ lies in an extension field $\mathbb{F}_{q^s}$, with s equal to the multiplicative order of q modulo $2n$. Let ω be a primitive element of $\mathbb{F}_{q^s}$, hence we can take $\delta = \omega^t$ and $\xi = \omega^{2t}$, with $t = \frac{q^s-1}{2n}$. Then the following holds.

$$x^n + 1 = \prod_{i=0}^{n-1} \left(x - \delta\xi^i\right) = \prod_{i=0}^{n-1} \left(x - \omega^{t(1+2i)}\right) = \prod_{i=0}^{n-1} \left(x - \delta^{(1+2i)}\right).$$

Table 2 New Hermitian self-dual MDS codes of length N over $\mathbb{F}_{q^2}$

N	q
6	37, 43, 47, 53, 63, 67, 73 ,83 (8)
12	5^2, 37, 7^2, 97 (16)
14	31, 47, 73, 83 (8)
20	41, 61, 9^2, 101, 181 (16)
24	5^2, 7^2, 73, 97, 11^2 (16)
28	29, 113, 197 (16)
36	37, 73, 109 (16)
40	41, 9^2, 11^2 (16)
42	73 (8) 43, 127 (16)
44	89, 353 (16)
48	7^2, 97, 193, 241, 337 (16)
52	53, 157, 313 (16)
54	83 (8)
60	61, 181 (6)

The Theorem providing the construction is given in brackets

Each irreducible factor of $x^n + 1$ corresponds to a cyclotomic class modulo $2n$.δ^{2i+1} and δ^{2j+1} are said to be conjugate if they are roots of the same irreducible factor of $x^n + 1$.

Denote by O_{2n} the set of odd integers from 1 to $2n - 1$. The defining set of the negacyclic code C of length n is $T = \{i \in O_{2n} : \delta^i \text{ is a root of } C\}$. It is the union of q-cyclotomic classes modulo $2n$. The dimension of the negacyclic code with defining set T is $n - |T|$. Aydin et al. [1] gave a negacyclic BCH bound. That is, if T has $d-1$ consecutive odd integers, then the minimum distance is at least d.

Lemma 9 ([2, Theorem 2]) *If C is a negacyclic code with defining set T, then $C^\perp$ (the Euclidean dual of C) is a negacyclic code with defining set*

$$T^\perp = \{i \in O_{2n} : -i \pmod{2n} \notin T\}$$

Let $s \in \{1, \ldots, 2n-1\}$ such that $(s, 2n) = 1$, then a multiplier of R_n is the map

$$\begin{aligned} \mu_s : R_n &\longrightarrow R_n \\ a(x) &\longmapsto a(x^s) \pmod{x^n + 1}, \end{aligned} \tag{5}$$

μ_s is an automorphism of R_n. If C is an ideal of R_n with defining set T, then $\mu_s(C)$ is an ideal of R_n with defining set $\{i \in O_{2n} \mid si \in T\}$.$\mu_s$ induces the following map

$$\begin{aligned} \mu'_s : O_{2n} &\longrightarrow O_{2n} \\ i &\longmapsto \mu'_s(i) = si \pmod{2n}, \end{aligned} \tag{6}$$

The multiplier $\mu_{2n-1} = \mu_{-1}$ has the effect of replacing x by x^{-1}, since $x^{2n} = 1$ in R_n.

Lemma 10 ([2, Theorem 3]) *If $N = 2^a n'$ for some odd integer n', then self-dual negacyclic codes over $\mathbb{F}_q$ of length N exist if and only if*

$$q \neq -1 \pmod{2^{a+1}}.$$

If $a = 1$, then self-dual negacyclic codes over $\mathbb{F}_q$ of length N exist if and only if

$$q \equiv 1 \pmod 4.$$

As a Corollary of Lemma 10 the negacyclic code of length $q+1$ and defining set $T = \{i \text{ odd} : 1 \leq i \leq q\}$ is an Euclidean self-dual MDS code over $\mathbb{F}_q$ as proven in [2]. The following result is more general than that given in [2].

Theorem 11 *Let $n = 2n'$ for some odd integer n', q an odd prime power such that $q \equiv 1 \pmod 4$, $q+1 = 2n''$, with $n'|n''$ and n'' odd. Then there exists an MDS negacyclic Euclidean self-dual code with parameters $[n, n/2, n/2+1]$ having defining set*

$$T = \left\{ \frac{q+1}{2} + i : -(n'-1) \leq i \text{ even } \leq (n'-1) \right\}.$$

Proof Consider a negacyclic code C with such a length n over $\mathbb{F}_q$. Assume $\delta^{2i'+1}$ is a root of C, hence $\left(\delta^{2i'+1}\right)^{q+1} = \delta^{2i'(q+1)}\delta^{q+1} = \delta^{2jn}\delta^{q+1} = \delta^{q+1}$. Then for an odd $i \in O_{2n}$, the conjugate of δ^i is $\delta^{iq} = \delta^{q+1-i}$. Hence we have $C(i) = \{i, q+1-i\}$. It is clear that for $i \in O_{2n}$ we have $|C(i)| \leq 2$ and $i = q+1-i \pmod{2n} \iff i = \frac{q+1}{2} + kn$. Hence for i even such that $1 \leq i \leq (n'-1)$, we have $\left|C\left(\frac{q+1}{2}+i\right)\right| = \left|\left\{\frac{q+1}{2}+i, \frac{q+1}{2}-i\right\}\right| = 2$ and for $i = 0$, $\left|C\left(\frac{q+1}{2}\right)\right| = 1$. Now, consider a negacyclic code with the following defining set

$$T = \bigcup_{i=0}^{n'-1} C\left(\frac{q+1}{2}+i\right) = \left\{ \frac{q+1}{2} + i : -(n'-1) \leq i \text{ even } \leq (n'-1) \right\}.$$

Assume there exist two different integers i and j such that $0 \leq i \leq n'-1$, $0 \leq j \leq n'-1$ and $C\left(\frac{q+1}{2}+i\right) = C\left(\frac{q+1}{2}+j\right)$. Hence $\frac{q+1}{2}+i = \frac{q+1}{2}+j+2kn \iff i-j = 2kn$, that is $i-j$ is a multiple of $2n$. But we have $i-j \leq n$, which is impossible. Furthermore, from Lemma 10 we have $C(i) \neq C(-i) \pmod{2n}$. If we assume the existence of two different integers i' and j' in T such that $C(i') = C(-j')$, then there exists i and j such that $i' = \frac{q+1}{2}+i$ and $j' = \frac{q+1}{2}+j$. But, $C(i') = C(-j') \iff \frac{q+1}{2}+i = 2kn - \frac{q+1}{2} - j \iff -(q+1+2k'n) = i+j = n\left(-\frac{q+1}{n}+2k\right)$, this gives that n divides $i+j$, which is impossible since $-(n'-1) \leq i, j \leq (n'-1)$. This implies that $-T \cap T = \emptyset$ and the redundancy of the code is equal to n', hence the code is self-dual. The code is MDS, since there are n' successive roots and hence by the BCH bound the minimum distance is at least $n'+1$, then by the Singleton bound we have equality. □

Some new codes obtained using Theorem 11 are given in Table 1.

Theorem 12 *Let $n = 2^a n'$ for some odd integer n', q an odd prime power such that $q \equiv 1 \pmod{2^{a+1}n''}$, $n'|n''$ and n'' odd. Then there exists an MDS negacyclic Euclidean self-dual code with parameters $[n, n/2, n/2+1]$ having defining set*

$$T = \{i \text{ odd} : 1 \leq i \leq n-1\}.$$

Proof In this case we have $\xi \in \mathbb{F}_q$, and hence $\xi^q = \xi$. We will show that the conjugate of $\delta^{2i+1} = \delta\xi^i$ is exactly itself. This means that each cyclotomic class contains only one element, namely

$$\left(\delta\xi^i\right)^q = \delta^q\xi^i = \delta\delta^{q-1}\xi = \delta\left(\delta^{2n}\right)^{\frac{q-1}{2n}}\xi^i = \delta\xi^i.$$

Now we consider the negacyclic code with defining set $T = \{i \text{ odd} : 1 \le i \le n-1\}$. By Lemma 10 we have $C(i) \neq C(-i)$. Furthermore, for different i and j in T we cannot have $C(i) = C(-j)$. Otherwise we will have $2nk - i = j$, since in each class there is only one element. Hence $i + j = 2nk$, which is impossible, because $i \le n-1$ and $j \le n-1$. This implies $-T \cap T = \emptyset$ and $|T| = \frac{n}{2}$. Then from Lemma 9 we obtain $T^{\perp} = T$ and so the code is self-dual. By the BCH bound the minimum distance is $\frac{n}{2} + 1$. □

Some new codes obtained from Theorem 12 are given in Table 1.

Lemma 13 *Let C be a negacyclic code of length n over $\mathbb{F}_{q^2}$ with defining set T. Then the Hermitian dual is a negacyclic code with defining set*

$$T^{\perp h} = O_{2n} \setminus (-iq).$$

Proof Let $\overline{C} = \left\{\left(a_0^q, \ldots, a_{n-1}^q\right) : (a_0, \ldots, a_{n-1}) \in C\right\}$. By an argument analogous to that in [5, Proposition 3.1], one can show that $\overline{C} = \mu_q(C)$. Furthermore, since μ_q is an automorphism on R_n, the code $\overline{C}$ is negacyclic with defining set $T_{\overline{C}} = qT = \{iq : i \in T\}$. By noticing that $C^{\perp h} = \overline{C}^{\perp}$, we get that

$$T_{\overline{C}}^{\perp} = \{i \in O_{2n} : -i \pmod{2n} \notin qT\}.$$

The automorphism μ_q induces a permutation acting on the elements of O_{2n}. Thus we have

$$-i \pmod{2n} \notin qT \iff -qi \pmod{2n} \notin q^2T. \tag{7}$$

But over $\mathbb{F}_{q^2}$, all the cyclotomic classes are stable by multiplication by q^2, hence (7) is equivalent to $-qi \pmod{2n} \notin T$. Then

$$T^{\perp h} = \{i \in O_{2n} : -iq \pmod{2n} \notin T\} = O_{2n} \setminus (-q)T.$$

□

Proposition 14 *If $N = 2^a n'$ for some odd integer n', then there exists a Hermitian self-dual code over $\mathbb{F}_{q^2}$ of length N if and only if*

$$q \neq -1 \pmod{2^{a+1}}. \tag{8}$$

Proof From Lemma 13, the code C is Hermitian self-dual if and only if we have $T = O_{2n} \setminus (-iqT)$. Hence C is Hermitian self-dual if its defining set T satisfies the following

$$2N - iq \notin T \iff i \in T. \tag{9}$$

Then, if there exists an odd $i \in O_{2N}$ such that $C_{q^2}(i) = C_{q^2}(-qi) \pmod{2N}$, the code C is not self-dual. If such an i exists, then there is an integer m such that $-iq \equiv q^{2m} i \pmod{2N}$. Hence, $2^{a+1} n' k = \left(q^{2m-1} + 1\right) qi$, which gives $2^{a+1} n' \mid \left(q^{2m-1} + 1\right) qi$. Since n' is odd we can choose i such that $n' \equiv i \pmod{2N}$. We need only check that $2^{a+1} \mid \left(q^{2m-1} + 1\right) q$. Since q is odd, it follows that $2^{a+1} \mid q^{2m-1} + 1$. Furthermore, we have $q^{2m-1} + 1 = (q+1)(q^{2m-2} - q^{2m-3} + \cdots - 1$, since the last factor is odd, and $q+1$ and $q^{2m-1} + 1$ have the same power of 2 in their factorization. Thus it is sufficient to check only that $q \equiv -1 \pmod{2^{a+1}}$. □

For $a = 1$, (8) becomes $q \equiv 1 \pmod 4$, hence we have the following Corollary.

Corollary 15 *If $N = 2n'$, for some odd integer n', then Hermitian self-dual negacyclic codes over $\mathbb{F}_{q^2}$ of length n exist if and only if*

$$q \equiv 1 \pmod 4.$$

Theorem 16 *Let $n = 2^a n'$, $a > 1$ and $q \equiv 1 \pmod{2^a n''}$, such that $n' | n''$ and n'' is odd. Then there exists an MDS negacyclic code of length n which is Hermitian self-dual with defining set*

$$T = \{i \ odd : 1 \leq i \leq n-1\}.$$

Proof If $q \equiv 1 \pmod{2^a n''}$, then $q \neq -1 \pmod{2^{a+1}}$. Otherwise $q = -1 + k2^{a+1}$ and $q = 1 + 2^a n'' k'$, and by summing the two quantities of q and dividing both sides by 2, we have $q = 2^{a-1}(n''k' + 2k)$. Since $a > 1$, this implies that q is even, which is impossible. Hence by Proposition 14 we have $C_{q^2}(-qi) \neq \{i\}$, since we have proven that $q \neq -1 + k2^{a+1}$. For these parameters we have $\xi \in \mathbb{F}_{q^2}$. Then by an argument similar to that in Theorem 12, we have that $C_{q^2}(i) = \{i\}$. Hence the code is Hermitian self-dual. By the BCH bound the minimum distance is $n/2 + 1$. □

Some new codes over $\mathbb{F}_{q^2}$ obtained using Theorem 16 are given in Table 2.

4 New self-dual codes from Negacyclic codes

A generalization of the splitting of n to obtain negacyclic codes was introduced in [2]. A q splitting modulo n is a multiplier μ_s of R_n that induces a partition of O_{2n} such that

1. $O_{2n} = S_1 \cup S_2 \cup X$
2. S_1, S_2 and X are unions of q cyclotomic classes.
3. $\mu_s'(S_i) = S_{i+1 \pmod 2}$ and $\mu_s'(X) = X$.

A q splitting is of Type I if $X = \emptyset$. A q splitting is of Type II if $X = \left\{\frac{n}{2}, \frac{3n}{2}\right\}$.

Definition 17 A negacyclic code C of length n over $\mathbb{F}_q$ is duadic if there exists a splitting such that the defining set is one of S_i or $S_i \cup X$ for $i = 1$ or 2. If the splitting is of Type II, then there exist polynomials $A_i(x)$ such that $x^n + 1 = A_1(x)A_2(x)(x^2 + 1)$ and $\mu_s(A_i(x)) = A_{i+1 \pmod 2}(x)$.

Remark 18 An Euclidean (respectively Hermitian) self-dual negacyclic code is duadic with multiplier μ_{-1} (respectively μ_{-q}) if it is obtained from a Type I splitting.

Next, we consider negacyclic codes of length $n = 2p^t$ with p an odd prime.

Lemma 19 ([2, Theorem 8]) *If p and q are distinct odd primes, $q \equiv 3 \pmod 4$ and $r = \mathrm{ord}_{2p^t}(q)$, then the following holds.*

1. *There exists a q splitting of $n = 2p^t$ of Type II.*
2. *μ_{-1} gives a splitting of n of Type II if and only if $r \neq 2 \pmod 4$.*

Lemma 20 *Let t be the order of q modulo p, and z be the largest integer such that $p^z | (q^t - 1)$. Hence if $z = 1$, we have $\mathrm{ord}_{p^r} q = p^{r-1}t$.*

Proof Let $u = q^t \equiv 1 \mod p$. If we assume that $z = 1$, then $u \neq 1 \mod p^2$. It is a well known fact from elementary number theory [4, p. 87] that $u \mod p^r$ is an element of order p^{r-1} in the group $\left(\mathbb{Z}_{p^r}\right)^*$ if and only if $u \neq 1 \mod p^2$. Hence $\mathrm{ord}_{p^r} q = p^{r-1}t$. □

Remark 21 We have $r = \mathrm{ord}_{2p^t}(q) = lcm(\mathrm{ord}_2(q), \mathrm{ord}_{p^t}(q)) = \mathrm{ord}_{p^t}(q)$, since q is odd. Hence if $z = 1$, by Lemma 20 we have $\mathrm{ord}_{p^t}(q) = p^{t-1}\,\mathrm{ord}_p(q)$, so if $\mathrm{ord}_p(q)$ is odd or $\mathrm{ord}_p(q) \equiv 0 \pmod 4$, then $r \neq 2 \pmod 4$. Hence from Lemma 19 the multiplier μ_{-1} gives a splitting of n of Type II.

Lemma 22 *Let p and q be distinct odd primes. Then we have the following.*

1. *If $p \equiv 1 \pmod 4$ and $\left(\frac{q}{p}\right) = -1$, then $\mathrm{ord}_p(q) \equiv 0 \pmod 4$.*
2. *If $\left(\frac{q}{p}\right) = 1$ and $p \equiv 3 \pmod 4$, then $\mathrm{ord}_p(q)$ is odd.*

Proof Assume that q is not a quadratic residue modulo p. Then from [11, Lemma 6.2.2] $\mathrm{ord}_p(q)$ is not a divisor of $\frac{p-1}{2}$, so from Fermat's Little Theorem $\mathrm{ord}_p(q) = p - 1$. Hence $\mathrm{ord}_p(q) \equiv 0 \pmod 4$ since $p \equiv 1 \pmod 4$.

If $q \in \mathcal{Q}_p$, then from [11, Lemma 6.2.2] $\mathrm{ord}_p(q)$ is a divisor of $\frac{p-1}{2}$. Since $p \equiv 3 \pmod 4$ we have that $\frac{p-1}{2}$ is odd. This implies that $\mathrm{ord}_p(q)$ is also odd. □

Assume, that the following equation

$$2 + \gamma^2 n = 0 \tag{10}$$

has a solution in $\mathbb{F}_q$. If $\mathsf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_q^n$, define

$$\widetilde{\mathsf{a}} = (a_0, \ldots, a_{n-1}, a_\infty, a_*) \in \mathbb{F}_q^{n+2},$$

where

$$a_\infty = \gamma \sum_{i=0}^{\frac{n-1}{2}} (-1)^i a_{2i}, \quad a_* = \gamma \sum_{i=0}^{\frac{n-1}{2}} (-1)^i a_{2i+1}.$$

The set $\widetilde{C} = \{\widetilde{\mathsf{a}} = (a_0, \ldots, a_{n-1}, a_\infty, a_*) \in \mathbb{F}_q^{n+2} : (a_0, \ldots, a_{n-1}) \in C\}$ is a linear code of $\mathbb{F}_q$.

Lemma 23 ([2, Theorem 12]) *Let q be a prime, γ a solution of (10) in $\mathbb{F}_q$, and suppose that D_1 and D_2 are odd-like negacyclic duadic codes of length $n = 2p^t$, with multiplier μ_{-1} of Type II. Then for $i = 1, 2$, the codes $\widetilde{D_i}$ are Euclidean self-dual.*

Lemma 24 *Let q and p be distinct odd primes such that $q \equiv p \equiv 3 \pmod 4$, $n = 2p^t$, with t odd. Hence (10) has a solution in $\mathbb{F}_q$.*

Proof There is a solution for $2 + 2p\gamma^2 = 0$ in $\mathbb{F}_q$ if and only if there is a solution of $1 + p\gamma^2 = 0$ in $\mathbb{F}_q$. If we assume $p \equiv 3 \pmod 4$, the last equation has a solution $\gamma \in \mathbb{F}_q$ from [11, Lemma 6.6.17]. If t is odd γ^t is a solution of (10). □

Theorem 25 *Let p and q be two odd primes such that $q \in \mathcal{Q}_p$, $q \equiv p \equiv 3 \pmod 4$ and $z = 1$. Then there exist negacyclic duadic codes D_i for $1 \leq i \leq 2$ of length $n = 2p^t$, t odd, with splitting of Type II given by μ_{-1}, and such that $\widetilde{D_i}$ are self-dual for $i = 1, 2$.*

Proof If we have such p and q, from Lemma 22 $\mathrm{ord}_{2p^t}(q)$ is odd. Hence from Remark 21 μ_{-1} gives a splitting of n of Type II. Furthermore, from Lemma 24 (10) has a solution in $\mathbb{F}_q$. Hence from Lemma 23, the codes D_i can be extended to Euclidean self-dual codes $\widetilde{D_i}$, for $i = 1$ and 2. □

Gulliver and Harada [8] proved the existence of MDS self-dual codes of length 18 over $\mathbb{F}_p$, when $17 \leq p \leq 97$. However, for $101 \leq p \leq 300$ they gave quasi-twisted self-dual $[18, 9, 9]_p$ codes obtained from unimodular lattices [8, Table 3]. In Table 1, MDS self-dual codes of length 18 are given for $p = 109$, 137, 181, 197, 233, and 269.

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. Blackford T.: Negacyclic duadic codes. Finite Fields Appl. **14**(4), 930–943 (2008).
3. Betsumiya K., Georgiou S., Gulliver T.A., Harada M., Koukouvinos C.: On self-dual codes over some prime fields. Disc. Math. **262**, 37–58 (2003).
4. Demazure M.: Cours D'Algèbre: Primalité. Divisibilité. Codes. Cassini, Paris (1997).
5. Dicuangco L., Moree P., Solé P.: The lengths of hermitian self-dual extended duadic codes. J. Pure Appl. Algebra **209**(1), 223–237 (2007).
6. Guenda K.: Quantum duadic and affine invariant codes. Int. J. Quantum Inf. **7**(1), 373–384 (2009).
7. Gulliver T.A., Grassl M.: On self-dual MDS codes. In: Proceedings of IEEE International Symposium Information Theory, Toronto, Canada, July (2008).
8. Gulliver T.A., Harada M.: MDS self-dual codes of lengths 16 and 18. Int. J. Inform. Coding Theory **1**(2), 208–213 (2010).
9. Dinh H.Q., Lopez-Permount S.R.: Cyclic and negacyclic codes over finite chain rings. IEEE. Trans. Inform. Theory **50**(8), 1728–1744 (2004).
10. Hill R.: An extension theorem for linear codes. Des. Codes Cryptogr. **17**(1–3), 151–157 (1999).
11. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
12. Kotsireas I.S., Koukouvinos C., Simos D.: MDS and near-MDS self-dual codes over large prime fields. Advan. Math Commun. **3**(4), 349–361 (2009).
13. Krishna A., Sarwate D.V.: Pseudo-cyclic maximum-distance-seperable codes. IEEE Trans. Inform. Theory **36**(4), 880–884 (1990).
14. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. Elsevier, North-Holland (1977).
15. Smid M.H.M.: Duadic codes. IEEE. Trans. Inform. Theory **33**(3), 432–433 (1983).