Abstract

This paper extends the concepts from cyclic duadic codes to negacyclic codes over $F_q$ ($q$ an odd prime power) of oddly even length. Generalizations of defining sets, multipliers, splittings, even-like and odd-like codes are given. Necessary and sufficient conditions are given for the existence of self-dual negacyclic codes over $F_q$ and the existence of splittings of $2N$, where $N$ is odd. Other negacyclic codes can be extended by two coordinates in a way to create self-dual codes with familiar parameters.

© 2008 Elsevier Inc. All rights reserved.

Keywords: Negacyclic and cyclic codes; Self-dual codes; Extended codes

Cyclic duadic codes, originally studied by Leon, Masley and Pless in [5], are generalizations of quadratic residue codes. They can be characterized by both their idempotent generators and their defining sets. More specifically, a pair of cyclic duadic codes of length $n$ has their idempotent generators and defining sets determined by a splitting of $n$. Furthermore, one code can be obtained from the other via a multiplier of the quotient ring $F[x]/(x^n - 1)$. It has been shown (Theorem 9.12, Chapter 1 of [6]) that cyclic duadic codes can be extended in a way to make their extensions self-dual. These extensions have many interesting properties, specifically their large automorphism groups. It has been shown (Theorem 9.6, Chapter 1 of [6]) that cyclic duadic codes of prime length $p$ over $F_q$ exist if and only if $q$ is a quadratic residue modulo $p$.

This paper seeks to extend these concepts to negacyclic codes using multipliers of the quotient ring $F_q[x]/(x^n + 1)$. We determine necessary and sufficient conditions for the existence of negacyclic duadic codes of length $n$, when $n$ and $q$ are relatively prime. In doing so we classify all self-dual negacyclic codes over $F_q$. We also show that negacyclic duadic codes of oddly even
length always exist. We define even-like and odd-like duadic codes, and list some of their properties. Finally, we will extend a class of negacyclic codes in a way as to make their extensions self-dual. We do this by extending codewords by two coordinates, not one.

It should be noted that negacyclic duadic codes have been generalized to consta-abelian duadic codes in a recent paper by Lim [4].

Finally, it should be emphasized that just as in the literature for cyclic duadic codes, throughout this paper it is always assumed that the characteristic of the underlying field is relatively prime to the codewlength.

1. Introduction

Let $R$ be a commutative ring with identity. An $R$-linear code $C$ of length $n$ is an $R$-submodule of $R^n$. $C$ is constacyclic if there is some fixed unit $a \in R$ such that $\sigma_a(C) \subseteq C$, where

$$\sigma_a((c_0, c_1, \ldots, c_{n-1})) = (ac_{n-1}, c_0, \ldots, c_{n-2}).$$

If $a = 1$, $C$ is cyclic. If $a = -1$, $C$ is negacyclic. A constacyclic code corresponds to an ideal of $R[x]/(x^n - a)$ under the correspondence

$$c = (c_0, c_1, \ldots, c_{n-1}) \mapsto c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} \pmod{(x^n - a)}.$$

If $R = \mathbb{F}_q$, a constacyclic code corresponds to an ideal $(f(x))$, where $f(x) | x^n - a$. The roots of the code are the roots of $f(x)$. If $R = \mathbb{F}_q$ and $n$ is odd, then negacyclic codes are scalar equivalent to cyclic codes under the map

$$\phi: \frac{\mathbb{F}_q[x]}{(x^n - 1)} \rightarrow \frac{\mathbb{F}_q[x]}{(x^n + 1)},$$

$$\phi(a(x)) = a(-x).$$

Thus the theory of negacyclic codes of odd length is equivalent to the theory of cyclic codes of odd length. In fact, it is shown in [1] that many constacyclic codes are equivalent to cyclic codes.

2. Negacyclic codes of oddly even length

Throughout this section, let $n = 2n'$, where $n'$ is an odd integer (we say $n$ is oddly even) and assume $q$ is a power of an odd prime that is relatively prime to $n$. Define

$$R_n = \frac{\mathbb{F}_q[x]}{(x^n + 1)}.$$

The roots of $x^n + 1$ are $\delta^{2i+1}$, $0 \leq i \leq n - 1$, where $\delta$ is a primitive 2n-th root of unity in some extension field $F$ of $\mathbb{F}_q$. Let $\xi = \delta^2$, which is a primitive n-th root of unity. Let $O_{2n}$ be the set of odd integers from 1 to $2n - 1$. The defining set of a negacyclic code $C$ of length $n$ is the set

$$T = \{i \in O_{2n}: \delta^i \text{ is a root of } C\}.$$
to see that the dimension of $C$ is $n - |T|$. A constacyclic BCH bound is given in [1] which states that if $T$ has $d - 1$ consecutive odd integers, the minimum distance of $C$ is at least $d$.

**Remark.** The minimum weight of a negacyclic code of length $n$ with defining set $T$ is no better than that of a cyclic code of length $n/2$ whose roots include $\{-\zeta^{2i} : i \in T\}$. This is because if $c(x) \in F_q[x]/(x^{n/2} - 1)$ is a codeword of the cyclic code, $c(-x^2) \in F_q[x]/(x^n + 1)$ is in the negacyclic code and has the same weight. However, as we will soon see, some specific negacyclic codes are still good. Also, they are interesting because of their relationship with their duals.

### 2.1. A discrete Fourier transform

Let $a \in F_q^n$. Define the discrete Fourier transform (DFT) of $a$ to be the vector $[A_0, \ldots, A_{n-1}] \in F^n$, where

$$A_i = \sum_{j=0}^{n-1} a_j \zeta^{(1+2i)j}, \quad 0 \leq i \leq n - 1.$$ 

($A_i$ is called the $i$th Fourier coefficient of $a$.) We define the DFT of an element $a(x) \in R_n$ to be the DFT of the corresponding vector $a$ (so that $A_i = a(\delta \zeta^i)$). We make $F^n$ into a ring by usual addition and componentwise multiplication ($a \ast b = (a_0 b_0, \ldots, a_{n-1} b_{n-1})$). Finally, we define a generalization of the Mattson–Solomon polynomial of $a$ (and $a(x)$) as

$$A(Z) = \sum_{i=0}^{n-1} A_i Z^i.$$ 

We state the following facts about this transform.

**Lemma 1.** Let

$$\theta : R_n \rightarrow F^n$$

be the negacyclic DFT map defined by $\theta(a(x)) = [A_0, A_1, \ldots, A_{n-1}]$. Suppose $a(x), b(x) \in R_n$. Then

1. $\theta$ is a ring homomorphism.
2. $A_i^q = A_{(qi+2^{n-1})}.$
3. If $0 \leq t \leq n - 1$, then

$$a_t = \frac{1}{n} \delta^{-t} \sum_{i=0}^{n-1} A_i \zeta^{-it} = \frac{1}{n} \delta^{-t} A(\zeta^{-t}).$$

4. $$\sum_{t=0}^{n-1} a_t b_t = \frac{1}{n} \sum_{i=0}^{n-1} A_i B_{-i-1}.$$ 

(All subscripts are calculated modulo $n$.)
Proof. (1) is straightforward. (2) follows from the calculation

\[ A_i^q = a(\delta \zeta^i)^q = a(\delta^q \zeta^{q^i}) = a(\delta \delta^{q-1} \zeta^{q^i}) = a(\delta \zeta^{q^{i+q^{-1}}}) = A_{(qi + q^{-1})} \]

with all subscripts calculated modulo \( n \). For (3), we can completely recover the original vector from its discrete Fourier transform via the calculation

\[ A(\zeta^{-t}) = \sum_{i=0}^{n-1} A_i \zeta^{-it} \]

\[ = \sum_{i=0}^{n-1} \left( \sum_{j=0}^{n-1} a_j \delta^j \zeta^{ij} \right) \zeta^{-it} \]

\[ = \sum_{j=0}^{n-1} a_j \delta^j \sum_{i=0}^{n-1} \zeta^{ij(t-i)} \]

\[ = n a_t \delta^t. \]

The last step follows from the well known fact that \( \sum_{i=0}^{n-1} \zeta^{iv} = 0 \) when \( v \neq 0 \) (mod \( n \)). Finally, (4) follows from (3):

\[ \sum_{t=0}^{n-1} a_t b_t = \frac{1}{n^2} \sum_{t=0}^{n-1} \delta^{-2t} A(\zeta^{-t}) B(\zeta^{-t}) \]

\[ = \frac{1}{n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} A_i B_j \sum_{t=0}^{n-1} \delta^{-2t} \zeta^{-(i+j)t} \]

\[ = \frac{1}{n^2} \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} A_i B_j \sum_{t=0}^{n-1} \zeta^{-(i+j+1)t} \]

\[ = \frac{1}{n} \sum_{i=0}^{n-1} A_i B_{-i-1}. \]

2.2. Duals of negacyclic codes

Recall the (Euclidean) dual of a code \( C \) of length \( n \) over a ring \( R \) is the set

\[ C^\perp = \{ v \in R^n : \langle u, v \rangle = 0 \ \forall u \in C \}, \]

where

\[ \langle u, v \rangle = u_0 v_0 + \cdots + u_{n-1} v_{n-1}. \]

If \( C \subset C^\perp \), then \( C \) is self-orthogonal; if \( C = C^\perp \) then \( C \) is self-dual. If \( C \) equivalent to \( C^\perp \), \( C \) is isodual.
The dual of a negacyclic code is also negacyclic. The proof of this fact is in [2] which uses a characterization of the dual using reciprocal polynomials. We give another presentation and proof using defining sets and the DFT.

**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

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

**Proof.** Let $D$ be the negacyclic code with defining set $T^\perp$, and let $a \in C$, $b \in D$. If $0 \leq i \leq n - 1$ and $A_i \neq 0$, then $2i + 1 \notin T$, which implies $-(2i + 1) \in T^\perp$. Then $B_{-i-1} = b(\delta^{1+2(-i-1)}) = b(\delta^{-1-2i}) = 0$. From (4) of Lemma 1, this means $\sum_{t=0}^{n-1} a_t b_t = 0$, so $D \subseteq C^\perp$. Comparing dimensions, we get $C^\perp = D$. □

We now give a necessary and sufficient condition for the existence of self-dual negacyclic codes.

**Theorem 3.** If $N = 2^n n'$ for some odd integer $n'$, then self-dual negacyclic codes over $F_q$ of length $N$ exist if and only if

$$q \not\equiv -1 \pmod{2^{a+1}}.$$ 

**Proof.** A negacyclic code with defining set $T$ is self-dual if and only if

$$T = \{ i \in O_{2N}: -i \pmod{2n} \notin T \},$$

which can happen if and only if there is no such $i \in O_{2N}$ such that $cl_q(i) = cl_q(-i)$ modulo $2n$, which means that there is no odd integer $i$ and integer $m$ such that $-i \equiv q^m i \pmod{2N}$. If such an $i$ exists, then $2^{a+1} n' | (q^m + 1)i$. Since $n'$ is odd we can choose $i$ such that $n' \equiv i \pmod{2N}$. We need only check that $2^{a+1} | (q^m + 1)$, or alternatively $q^m \equiv -1 \pmod{2^{a+1}}$. First note that this cannot happen if $m$ is even, since then $q^m \equiv 1 \pmod{4}$. Thus $m$ must be odd, and

$$q^m + 1 = (q + 1)(q^{m-1} - q^{m-2} + \cdots + 1).$$

Since the last factor is odd, $q + 1$ and $q^m + 1$ has the same power of 2 in their factorizations. Thus it is sufficient only to check that $q \equiv -1 \pmod{2^{a+1}}$. □

**Corollary 4.** If $n = 2^n n'$, for some odd integer $n'$, then self-dual negacyclic codes over $F_q$ of length $n$ exist if and only if

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

For example, self-dual negacyclic codes of oddly even length exist over $F_5$ but not over $F_3$.

It turns out that some of the maximum distance separable (MDS) negacyclic codes over $F_q$ of length $q + 1$ (discovered by Krishna and Sarwate in [3]) are self-dual. We give another proof of this result using our notation and adding the statement about duality.
Corollary 5. Let \( q \) be a power of an odd prime. There is a self-dual MDS negacyclic code over \( F_q \) of length \( q + 1 \) having defining set
\[
T = \{ i \text{ odd}: 1 \leq i \leq q \}.
\]

Proof. This code is clearly self-dual, since the dimension is \( (q + 1)/2 \) and if \( q + 1 = 2^n n \) for some odd \( n \), it is impossible for \( 2^{a + 1} \) to divide \( q + 1 \), so \( q \not\equiv -1 \pmod{2^{a+1}} \). The set \( T \) is invariant under multiplication by \( q \), since if there are some odd integers \( i, j \) that are less than \( q + 1 \) such that \( q_i \equiv q + 1 + j \pmod{2q + 2} \), then it follows that \( 2(q + 1) \mid (q + 1)i - q - 1 - j - i \), which implies that \( 2q + 2 \mid i + j \), which means \( j \equiv -i \pmod{2q + 2} \). But this would mean that \( qi \equiv -i \pmod{2q + 2} \), which we have already shown cannot happen. Thus by the BCH Bound, the minimum distance is at least \( (q + 3)/2 \), which makes the code MDS. \( \square \)

3. Multipliers of \( R_n \)

Let \( s \) be an integer in \( \{1, \ldots, 2n - 1\} \) such that \( (s, 2n) = 1 \). Define a multiplier of \( R_n \) to be the map \( \mu_s : R_n \to R_n \),
\[
\mu_s(a(x)) = a(x^s) \pmod{(x^n + 1)}.
\]

\( \mu_s \) 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 with defining set \( \{i: si \in T\} \). \( \mu_s \) induces a map \( \mu'_s : O_{2n} \to O_{2n} \) defined by
\[
\mu'_s(i) = si \pmod{2n}.
\]

\( \mu_s \) also induces a corresponding automorphism of \( F_q^n \).

Example 1. \( \mu_{n+1} \) has the effect of replacing \( x \) with \( -x \), since \( x^{n+1} = -x \) in \( R_n \).
\[
\mu_{n+1}((a_0, a_1, a_2, \ldots, a_{n-1})) = (a_0, -a_1, a_2, -a_3, \ldots, -a_{n-1}).
\]
In fact, \( (\mu_s(a(x))) = (a(-x)) \).

Example 2. \( \mu_{2n-1} \) (also denoted as \( \mu_{-1} \)) has the effect of replacing \( x \) with \( x^{-1} \), since \( x^{2n} = 1 \) in \( R_n \).
\[
\mu_{-1}((a_0, a_1, a_2, a_3, \ldots, a_{n-1})) = (a_0, -a_{n-1}, -a_{n-2}, \ldots, -a_1).
\]
In fact,
\[
(\mu_{-1}(a(x))) = (a^*(x)),
\]
where \( a^*(x) \) is the reciprocal polynomial of \( a(x) \). (This is true even though \( \mu_{-1}(a(x)) \not= a^*(x) \).)
Note that these automorphisms not only permute the coordinates but also change some of their signs.
3.1. Splittings of $n$

A $q$-splitting of $n$ is a multiplier $\mu_s$ of $n$ that induces a partition of $O_{2n}$ such that

1. $O_{2n} = A \cup B \cup X$.
2. $A$, $B$, and $X$ are unions of $q$-cyclotomic cosets.
3. $\mu_s'(A) = B$, $\mu_s'(B) = A$ and $\mu_s'(X) = X$.

A $q$-splitting is of Type I if $X = \emptyset$. A $q$-splitting is of Type II if $X = \{ \frac{n}{2}, \frac{3n}{2} \}$. A negacyclic code $C$ of length $n$ over $F_q$ is duadic if such a splitting exists and the defining set is one of the subsets $A$, $B$, $A \cup X$, or $B \cup X$. (Note that if $q \equiv 3 \pmod{4}$, every multiplier leaves the set $\{ \frac{n}{2}, \frac{3n}{2} \}$ invariant.)

If $s$ gives a splitting of Type I, then

$$x^n + 1 = A(x)B(x)$$

for some $A(x), B(x) \in F_q[x]$ such that

$$\mu_s\left(\left( A(x) \right) \right) = \left( B(x) \right), \quad \mu_s\left(\left( B(x) \right) \right) = \left( A(x) \right).$$

If $s$ gives a splitting of Type II, then

$$x^n + 1 = A(x)B(x)(x^2 + 1)$$

for some $A(x), B(x) \in F_q[x]$ such that

$$\mu_s\left(\left( A(x) \right) \right) = \left( B(x) \right), \quad \mu_s\left(\left( B(x) \right) \right) = \left( A(x) \right).$$

If $\delta^i$ is a root of $A(x)$, then $\delta^{si}$ is a root of $B(x)$ and vice versa.

**Example 3.** Let $n = 12$, $q = 5$. Then $\mu_{-1}$ gives a splitting of Type I which induces the partition of $O_{24}$:

$$A = \{1, 5, 3, 15, 7, 11\}, \quad B = \{23, 19, 21, 9, 17, 13\}, \quad X = \emptyset.$$  

Note that the negacyclic code with defining set $A$ is a self-dual $[12, 6, 5]$ code over $F_5$.

**Example 4.** Let $n = 18$ and $q = 11$. Then $\mu_{-1}$ induces the following partition of $O_{36}$:

$$\{1, 11, 13, 35, 25, 23\} \cup \{5, 19, 29, 31, 17, 7\} \cup \{3, 33, 9, 27, 15, 21\}$$

while $\mu_5$ is a Type II splitting and gives a different partition:

$$\{1, 11, 13, 35, 25, 23, 3, 33\} \cup \{5, 19, 29, 31, 17, 7, 15, 21\} \cup \{9, 27\}.$$  

A self-dual negacyclic code is duadic with multiplier $\mu_{-1}$ and comes from a Type I splitting. Thus if $q \equiv 1 \pmod{4}$, there is always a $q$-splitting of $n$. There are no $q$-splittings of Type I if $q \equiv 3 \pmod{4}$, since $\mu'_s$ leaves $\{ \frac{n}{2}, \frac{3n}{2} \}$ invariant.
3.2. \( q \)-Splittings of Type II

The goal of this subsection is to show that every oddly even codelength has a splitting of Type I or Type II.

We start by examining codes of length \( n = 2^pt \), where \( p \) is an odd prime. Let \( \mathcal{U}_{4^pt} \) be the set of residues modulo \( 4^pt \) that are relatively prime to \( 4^p \). It is a group with respect to multiplication, and

\[
\mathcal{O}_{2n} = \bigcup_{i=0}^{t} p^i \mathcal{U}_{4^pt}.
\]

We will split \( \mathcal{O}_{2n} \) by splitting each of the subsets \( p^i \mathcal{U}_{4^pt} \). We will need the following lemmas.

**Lemma 6.** Let \( p, q \) be distinct primes. Suppose there is an element \( a \in \mathcal{U}_{4^pt} \) such that \( a/q \in \langle q \rangle \) in \( \mathcal{U}_{4^pt} \) and \( a^2 = 1 \) (mod \( 4^pt \)). Then \( a \not\equiv q^m \) (mod \( 4^pt \)) for any \( m \) and \( i = 1, \ldots, t \).

**Proof.** Suppose \( a \equiv q^m \) (mod \( 4^pt \)). Then

\[
a = q^m + 4ptk \quad \text{(mod } 4^pt+1),
\]

\[
a^p = q^{mp} + 4pt+1kq^{(p-1)m} \quad \text{(mod } 4^pt+1),
\]

\[
a = q^{mp} + 4pt+1kq^{(p-1)m} \quad \text{(mod } 4^pt+1)
\]

since \( p \) is odd. So now \( a \in \langle q \rangle \) (mod \( 4^pt+1 \)). Continuing in this way we eventually get \( a \in \langle q \rangle \) (mod \( 4^pt \)), a contradiction. \( \square \)

**Lemma 7.** Let \( p, q \) be distinct odd primes and \( q \equiv -1 \) (mod \( 4^p \)). Then there exists a \( q \)-splitting of \( \mathcal{O}_{4^pt} \) such that \( X = \{p^t, 3p^t\} \). Moreover, this splitting can be given using either \( 4pt - 1 \) or \( 2pt + 1 \).

**Proof.** Let \( Q = \langle q \rangle \), in \( \mathcal{U}_{4^pt} \). First we note that

\[
\mathcal{U}_{4^pt} \cong C_2 \times C_{p-1} \times C_{pt-1},
\]

a product of three cyclic groups, so \( \mathcal{U}_{4^pt} \) contains exactly three elements of order 2, and \( Q \) contains at most one of them. Either \( 2pt + 1 \) or \( 4pt - 1 \) is not in \( Q \); call this element \( a \). We will show that \( \mu_a \) gives the necessary splitting. If \( hQ \) is a coset of \( \langle q \rangle \) in \( \mathcal{U}_{4^pt} \), then \( hQ \) and \( ahQ \) have to be distinct. Let

\[
h_1Q, \ldots, h_sQ, ah_1Q, \ldots, h_sQ
\]

be the cosets of \( \mathcal{U}_{4^pt} \) modulo \( Q \). Let \( A' = h_1Q \cup \cdots \cup h_sQ, B' = ah_1Q \cup \cdots \cup ah_sQ \), and then let

\[
A = \bigcup_{j=0}^{t-1} p^j A', \quad B = \bigcup_{j=0}^{t-1} ap^j B', \quad X = \{p^t, 3p^t\}.
\]
A and $B$ are clearly unions of $q$-cyclotomic cosets. $X$ is a $q$-cyclotomic coset since $q \equiv -1 \pmod{4}$. Since $O_{4p^r} = \bigcup_{i=1}^{l} p^{-i}U_{4p^r}$, and $p^{i-1}U_{4p^r} = p^{i-1}A \cup p^{i-1}B'$, we have $O_{4p^r} = A \cup B \cup X$. (Note $X = p^iU_{4p^r}$.) Finally, if $p^{i-j}h_jQ = p^{i-j}ah_jQ$ for some $i, j$, then this shows $a \in Q \pmod{4p^j}$, in contradiction to the previous lemma, so $A, B, X$ are pairwise disjoint and form a $q$-splitting. □

**Theorem 8.** If $p, q$ are distinct odd primes, $q \equiv -1 \pmod{4}$, and $r$ is the order of $q$ modulo $2p^r$, then

1. $s = 4p^r - 1$ gives a splitting of $2p^t$ of Type II if and only if $r \not\equiv 2 \pmod{4}$, in which case

$$x^{2p^r} + 1 = \lambda A(x)A^*(x)(x^2 + 1)$$

for some $\lambda \in F_q$, $A(x) \in F_q[x]$.

2. $s = 2p^r + 1$ gives a splitting of $2p^t$ of Type II if and only if $r$ is even, in which case

$$x^{2p^r} + 1 = \lambda A(x)A(-x)(x^2 + 1)$$

for some $\lambda \in F_q$, $A(x) \in F_q[x]$.

In short, either $4p^r - 1$ or $2p^r + 1$ gives a splitting of $2p^r$.

**Proof.** From the proof of the previous theorem, we know $\mu_a$ will give a splitting of $2p^r$ if and only if $a \not\in \langle q \rangle$ modulo $4p^r$.

If $4p^r - 1 \in \langle q \rangle$, then $q^m \equiv -1 \pmod{4p^r}$ for some $m$, and since $q \equiv -1 \pmod{4}$, $m$ must be odd. But $q^m \equiv -1 \pmod{2p^r}$ and $q^{rm} \equiv 1 \pmod{2p^r}$, so $r$ must be even. In fact, since $q^{2m} \equiv 1 \pmod{2p^r}$, $r \mid 2m$, so $r$ is odd even. Conversely, suppose that $r$ is oddly even. Then $r = 2k$ for some odd integer $k$. As $q^{2k} \equiv 1 \pmod{2p^r}$, $2p^r \mid (q^k + 1)(q^k - 1)$. Clearly $2p^r \mid q^k - 1$ because of the minimality of $2k$. Since $(q^k + 1, q^k - 1) = 2$, it follows that $2p^r \mid q^k + 1$ and since $q^k \equiv -1 \pmod{4}$, $4p^r \mid q^k + 1$, so that $-1 \in \langle q \rangle$.

If $2p^r + 1 \in \langle q \rangle$, then $2p^r + 1 \equiv q^m \pmod{4p^r}$ for some integer $m$, which must be odd since $q \equiv -1 \pmod{4}$. As $r \mid m$, $r$ must be odd. Conversely, if $r$ is odd, $q^r = 1 + 2p^r k$ for some integer $k$. Then

$$q^r = 1 + 2p^r + 2p^r(k - 1).$$

Since $q^r \equiv -1 \pmod{4}$, $k - 1$ is even, so $q^r \equiv 1 + 2p^r \pmod{4p^r}$, and $1 + 2p^r \in \langle q \rangle$. □

**Theorem 9.** Let $q \equiv 3 \pmod{4}$, $n = 2p_1^{e_1} \cdots p_t^{e_t}$, where the $p_i$’s are distinct odd primes, and let $a_i$ be an integer that gives a splitting of $2p_i^{e_i}$. Then $n$ has a splitting of Type II. Moreover, this splitting is given by $\mu_a$, where $a$ is the unique integer in $O_{2n}$ such that $a \equiv a_i \pmod{2p_i^{e_i}}$.

**Proof.** We prove the case $t = 2$ and leave the rest to an induction exercise. Let $n = 2p_1^{e_1}p_2^{e_2}$. By the Chinese Remainder Theorem, there exists an isomorphism

$$\Phi : Z_{2n} \to Z_{4} \times Z_{p_1^{e_1}} \times Z_{p_2^{e_2}},$$

$$\Phi(x) = (x \pmod{4}, x \pmod{p_1^{e_1}}, x \pmod{p_2^{e_2}}).$$
The elements of $O_{2n}$ correspond to the triples $(\pm 1, x_1, x_2)$ where $x_1 \in \mathbb{Z}_{p_1^{e_1}}$ and $x_2 \in \mathbb{Z}_{p_2^{e_2}}$.
the elements of $O_{2p_1^{e_1}}$ correspond to those of the form $(\pm 1, x_1, 0)$ and the elements of $O_{2p_2^{e_2}}$ correspond to those of the form $(\pm 1, 0, x_2)$. For $i = 1, 2$, $a_i$ gives a splitting of $2p_i^{e_i}$ of Type II, so there exist sets $A_i, B_i \subset \mathbb{Z}_{p_i^{e_i}}$ such that

$$
\Phi(O_{p_1^{e_1}}) = (\{\pm 1\} \times A_1 \times \{0\}) \cup (\{\pm 1\} \times B_1 \times \{0\}) \cup (\{\pm 1\} \times \{0\} \times \{0\}),
$$

$$
\Phi(O_{p_2^{e_2}}) = (\{\pm 1\} \times \{0\} \times A_2) \cup (\{\pm 1\} \times \{0\} \times B_2) \cup (\{\pm 1\} \times \{0\} \times \{0\}),
$$

where $a_iA_i = B_i$, $a_iB_i = A_i$, $qA_i \subset A_i$, $qB_i \subset B_i$, and $A_i \cup B_i \cup \{0\}$ is a partition of $\mathbb{Z}_{p_i^{e_i}}$. Then let

$$
A = \Phi^{-1}(\{\pm 1\} \times A_1 \times \{0\}) \cup (\{\pm 1\} \times \{0\} \times A_2),
$$

$$
B = \Phi^{-1}(\{\pm 1\} \times B_1 \times \{0\}) \cup (\{\pm 1\} \times \{0\} \times A_2),
$$

$$
X = \Phi^{-1}(\{\pm 1\} \times \{0\} \times \{0\}) = \{p_1^{e_1} p_2^{e_2}, 3p_1^{e_1} p_2^{e_2}\}.
$$

Then $A$, $B$, and $X$ give the desired partition of $O_{2n}$.

Thus we see that there is much looser criteria for the existence of negacyclic duadic codes of oddly even length than for cyclic duadic codes of odd length.

**Corollary 10.** If $q \equiv 3 \pmod{4}$, and $n$ is oddly even, then there exists a polynomial $A(x)$ and a multiplier $\mu_s$ such that

$$
x^{n} + 1 = A(x)B(x)(x^2 + 1),
$$

where $\mu_s((A(x))) = (B(x))$ and $\mu_s((B(x))) = (A(x))$.

If $A(x)$, $B(x)$ are as above, let

$$
C_1 = ((x^2 + 1)A(x)), \quad C_2 = ((x^2 + 1)B(x)),
$$

$$
D_1 = (A(x)), \quad D_2 = (B(x)).
$$

$C_1, C_2$ are a pair of even-like negacyclic duadic codes. $D_1, D_2$ are a pair of odd-like negacyclic duadic codes. A vector $(c_0, c_1, \ldots, c_{n-1})$ is even-like if

$$
\sum_{i=0}^{(n-1)/2} (-1)^i c_{2i} = \sum_{i=0}^{(n-1)/2} (-1)^i c_{2i+1} = 0.
$$

Otherwise it is odd-like.

We summarize the properties of these codes in the following theorem.
Theorem 11. Let $C_1, C_2, D_1$ and $D_2$ be the negacyclic duadic codes defined above, with multiplier $\mu_s$.

1. $\mu_s(C_1) = C_2$, $\mu_s(C_2) = C_1$.
2. $\mu_s(D_1) = D_2$, $\mu_s(D_2) = D_1$.
3. If $e_1(x), e_2(x)$ are the respective idempotent generators of $C_1, C_2$, then $1 - e_1(x), 1 - e_2(x)$ are the respective idempotent generators of $D_1, D_2$.
4. $C_1 \cap C_2 = \{0\}$, $C_1 + C_2 = (x^2 + 1)$.
5. $C_i$ has dimension $\frac{n-2}{2}$, $D_i$ has dimension $\frac{n+2}{2}$ for $i = 1, 2$.
6. $D_1 \oplus C_2 = D_2 \oplus C_1 = F_q^n$.
7. If $s = 2n - 1$, then $C_1^\perp = D_1$ and $C_2^\perp = D_2$.
8. If $d$ is the minimum distance of $D_1$, then
   a. $d \geq \sqrt{\frac{n}{2}}$.
   b. If $s = 2n - 1$, then $d^2 - d + 1 \geq \frac{n}{2}$.

Proof. The proofs of these results are similar to those for cyclic duadic codes. To prove (8), we let $c(x)$ be a codeword of $D_1$ of minimum weight $d$. $c(x^s) \in D_2$, so

$$c(x)c(x^s) \in D_1 \cap D_2 = (1 - x^2 + x^4 - \cdots + x^{\frac{n+2}{2}}).$$

The minimum weight of this code is $\frac{n}{2}$. Since $c(x)c(x^s)$ has at most $d^2$ nonzero terms $(d^2 - d + 1)$ terms if $s = 2n - 1$), the weight bound is established. $\Box$

Observe the lower bound on the minimum distance is no better than the similar bound for cyclic duadic codes having half the length. Nevertheless, these codes are interesting because of their relationship with their duals.

4. Extended negacyclic codes

Although self-dual negacyclic codes might not exist for certain codelengths, in some cases these codes may be extended in a different way to create new self-dual codes.

Suppose $q$ is a prime such that $-\frac{2}{n}$ is a quadratic residue of $q$. (So $\gamma^2 n + 2 = 0$ for some $\gamma \in F_q^n$.) If $a = (a_0, \ldots, a_{n-1}) \in F_q^n, define$

$$\hat{a} = (a_0, \ldots, a_{n-1}, a_\infty, a_s) \in F_q^{n+2},$$

where

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

If $C$ is a set of vectors of length $n$, then $\hat{C}$ is defined to be the set $\{\hat{a} : a \in C\}$. We call this the negacyclic extension of $C$. (Note that $C$ and $\hat{C}$ have the same dimension.) We can extend the negacyclic shift $\sigma$ to a transformation $\tilde{\sigma} : F_q^{n+2} \rightarrow F_q^{n+2}$ by

$$\tilde{\sigma}(a_0, \ldots, a_{n-1}, a_\infty, a_s) = (-a_{n-1}, a_0, \ldots, a_{n-2}, -a_s, a_\infty).$$
Then if $\mathcal{C}$ is negacyclic, $\hat{\mathcal{C}}$ is invariant under $\tilde{\sigma}_1$. We can also extend the map $\mu_{-1}$ to $\tilde{\mu}_{-1}$: $F_{q}^{n+2} \rightarrow F_{q}^{n+2}$ as

$$\tilde{\mu}_{-1}((a_0, a_1, \ldots, a_{n-1}, a_{\infty}, a_{\ast})) = (a_0, -a_{n-1}, -a_{n-2}, \ldots, -a_1, a_{\infty}, -a_{\ast}).$$

**Theorem 12.** Suppose $q$ is a prime such that $\frac{q^2 - 1}{n} = \gamma^2$ for some $\gamma \in F_q^\ast$, and suppose that $\mathcal{D}_1, \mathcal{D}_2$ are odd-like negacyclic duadic codes with multiplier $\mu_{s}$ of Type II.

1. If $s = 2n - 1$, then $\hat{\mathcal{D}}_i$ is self-dual for $i = 1, 2$.
2. If $\mu_{-1}(\mathcal{D}_i) = \mathcal{D}_i$ for $i = 1, 2$, then $\hat{\mathcal{D}}_1 = \hat{\mathcal{D}}_2$ and $\hat{\mathcal{D}}_1^\perp = \hat{\mathcal{D}}_2^\perp = \hat{\mathcal{D}}_1$.

**Proof.** (1) Let $a, b \in \hat{\mathcal{D}}_i$. Let $\omega = \delta^{n/2}$, a primitive 4th root of unity, and let $a'(x) = a_0 + a_2x + \cdots + a_{n-2}x^{\frac{n-2}{2}}$, and $a''(x) = a_1 + a_3x + \cdots + a_{n-1}x^{\frac{n-1}{2}}$, so that $a(x) = a'(x^2) + xa''(x^2)$. Define $b'(x)$ and $b''(x)$ in the same way. Note $a_{\infty} = \gamma a'(-1), a_{\ast} = \gamma a''(-1), b_{\infty} = \gamma b'(-1), b_{\ast} = \gamma b''(-1)$. We know from Lemma 1 that

$$\sum_{i=0}^{n-1} a_i b_i = \frac{1}{n} \sum_{i=0}^{n-1} A_i B_{-1-i}$$

$$= \frac{1}{n} [A_{\frac{n-2}{4}} B_{\frac{3(n-2)}{4}} + A_{\frac{3(n-2)}{4}} B_{\frac{n-2}{4}}]$$

$$= \frac{1}{n} [a(\omega)b(-\omega) + a(-\omega)b(\omega)]$$

$$= \frac{2}{n} [a'(-1)b'(-1) + a''(-1)b''(-1)]$$

$$= \frac{2}{n} \gamma^{-2} [a_{\infty} b_{\infty} + a_{\ast} b_{\ast}]$$

so that

$$\langle a, b \rangle = \frac{2}{n} \gamma^{-2} [a_{\infty} b_{\infty} + a_{\ast} b_{\ast}] + [a_{\infty} b_{\infty} + a_{\ast} b_{\ast}]$$

$$= \left( \frac{2}{n} \gamma^{-2} + 1 \right) [a_{\infty} b_{\infty} + a_{\ast} b_{\ast}]$$

$$= \frac{1}{n} \gamma^{-2} (2 + n\gamma^2) [a_{\infty} b_{\infty} + a_{\ast} b_{\ast}]$$

$$= 0.$$ 

Thus $\hat{\mathcal{D}}_i \subset \hat{\mathcal{D}}_i^\perp$ for $i = 1, 2$, and comparing dimensions, we see $\hat{\mathcal{D}}_i = \hat{\mathcal{D}}_i^\perp$.

(2) Assume $\mu_{-1}(\mathcal{D}_i) = \mathcal{D}_i$. Let $T_1 = \{i: 0 \leq i < n: A_i = 0 \forall a(x) \in \mathcal{D}_i\}$, and define $T_2$ similarly. Then

$$[0, n - 1] = T_1 \cup T_2 \cup \left\{ \frac{n-2}{4}, \frac{3n-2}{4} \right\}.$$
Then if \( a(x) \in D_1 \) and \( b(x) \in D_2 \),
\[
\sum_{i=0}^{n-1} A_i B_{-i-1} = \sum_{i \in T_1} A_i B_{-i-1} + \sum_{i \in T_2} A_i B_{-i-1} + A_{n-2} B_{\frac{3n-2}{4}} + A_{\frac{n-2}{4}} B_{\frac{n-2}{4}}.
\]

Clearly the first sum is zero since \( A_i = 0 \) for all \( i \in T_1 \). Since the defining set of \( D_1 \) is invariant under multiplication by \(-1\), so is the defining set of \( D_2 \). Thus \( B_i = 0 \) if and only if \( B_{-i-1} = 0 \), so the second sum is zero. Thus we have that
\[
\sum_{i=0}^{n-1} a_i b_i = \frac{1}{n} [A_{\frac{n-2}{4}} B_{\frac{3(n-2)}{4}} + A_{\frac{3(n-2)}{4}} B_{\frac{n-2}{4}}],
\]
so the proof can proceed as in the first case. \(\Box\)

As a consequence, we obtain an infinite class of ternary self-dual codes.

**Corollary 13.** If \( p \) is a prime such that \( p \equiv 5 \pmod{6} \) and the order of \( 3 \) modulo \( 2p \) is not oddly even, then there exists a ternary self-dual extended negacyclic \([2p+2, p+1, d]\) code with \( d \geq \sqrt{p} \).

Note that in this case \( 2p \equiv 1 \pmod{3} \), we can take \( \gamma \) to be 1.

**Example 5.** \( p = 5 \)
\[
x^{10} + 1 = (x^4 + x^3 + 2x + 1)(x^4 + 2x^3 + x + 1)(x^2 + 1),
\]
\( A = \{1, 3, 9, 7\}, \quad B = \{11, 13, 19, 17\}, \quad X = \{5, 15\}. \)

Here \( D_1 = (A(x)), \quad D_2 = (B(x)), \quad \mu_1(D_1) = D_2, \) and \( \mu_1(D_1) = D_2 \). Also, \( \hat{D}_1 = \{ (d, d_\infty, d_\ast) : d \in D_1 \} \), where
\[
\begin{align*}
d_0 - d_2 + d_4 - d_6 + d_8 &= d_\infty, \\
d_1 - d_3 + d_5 - d_7 + d_9 &= d_\ast.
\end{align*}
\]

In this example, \( \hat{D}_1 \) is a self-dual \([12, 6, 6]\) ternary code. Note these are the same parameters of the extended ternary Golay code.

Despite this example, the ternary extended negacyclic codes of length \( 2p + 2 \) are different from and (in some cases) not as good as the Pless symmetry codes. The Pless symmetry code of length 24 has minimum distance 9, while the extended negacyclic code of the same length has a codeword of weight 6. The Pless symmetry code of length 48 has minimum distance 15, while the extended negacyclic codes have a codeword of weight 9.

### 5. Conclusion

We have seen that we can create new self-dual codes from negacyclic and extended negacyclic codes. It would be interesting to generalize these results to other constacyclic codes, particularly to codes over \( F_4 \) which might yield new Hermitian self-dual codes.
References