On self-dual negacirculant codes of index two and four *

Minjia Shi
School of Mathematical Sciences, Anhui University, Hefei, 230601, China
National Mobile Communications Research Laboratory,
Southeast University, 210096, Nanjing, China
Liqin Qian
School of Mathematical Sciences of Anhui University, Hefei, 230601, China
Patrick Solé
CNRS/LAGA, University of Paris 8, 2 rue de la liberté, 93 526 Saint-Denis, France

Abstract
In this paper, we study a special kind of factorization of $x^n + 1$ over $\mathbb{F}_q$, with $q$ a prime power $\equiv 3 \pmod{4}$ when $n = 2p$, with $p \equiv 3 \pmod{4}$ and $p$ is a prime. Given such a $q$ infinitely many such $p$’s exist that admit $q$ as a primitive root by the Artin conjecture in arithmetic progressions. This number theory conjecture is known to hold under GRH. We study the double (resp. four)-negacirculant codes over finite fields $\mathbb{F}_q$, of co-index such $n$’s, including the exact enumeration of the self-dual subclass, and a modified Varshamov-Gilbert bound on the relative distance of the codes it contains.

Keywords: Negacirculant codes; Self-dual codes; Self-reciprocal polynomials, Artin primitive root conjecture
MSC(2010): 94 B15, 94 B25, 05 E30

1 Introduction

The class of negacirculant codes plays a very significant role in the theory of error-correcting codes as they are a direct generalization of the important family of quasi-cyclic codes, which

---

*This research is supported by National Natural Science Foundation of China (61672036), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133) and the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2015D11) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008).
is known to be asymptotically good [9]. They have been used successfully to construct self-dual codes over fields of odd characteristic [5]. They are a special class of quasi-twisted (QT) codes [8]. A code of length $N$ is \textit{quasi-twisted of index} $l$ for some nonzero scalar $\lambda \in \mathbb{F}_q$, and of \textit{co-index} $n = N/l$ if it is invariant under the power $T^l_\lambda$ of the constashift $T_\lambda$ defined as

$$T_\lambda(x_0, x_1, \ldots, x_{N-1}) \mapsto (\lambda x_{N-1}, x_0, \ldots, x_{N-2}).$$

Thus negacirculant codes are QT codes with $\lambda = -1$.

In the present paper, we study the double (resp. four)-negacirculant codes, i.e., an index 2 (resp. 4) quasi-twisted code with $\lambda = -1$. By [8], QT codes can be decomposed as a direct sum of local rings by the Chinese Remainder Theorem applied to the semilocal ring $R(n, \mathbb{F}_q) = \frac{\mathbb{F}_q[x]}{(x^n - \lambda)}$. This technique is well suited for studying self-dual QT codes. Although [1] has already studied self-dual double-negacirculant codes, we consider a different factorization of $x^n + 1$ over $\mathbb{F}_q$ to study self-dual double negacirculant codes, and we also study the case of index 4. The codes we construct have thus different co-indices, and therefore, different lengths than the codes in [1].

In fact, the number of rings occurring in the decomposition of $R(n, \mathbb{F}_q)$ equals the number of irreducible factors of $x^n + 1$. To simplify the analysis, we consider the case when $n = 2p$, $p \equiv 3 \pmod{4}$, $p$ is a prime power and $x^n + 1$ can be factored into a product of three irreducible polynomials, instead of two for [3, 12]. We demand, to simplify the self-duality conditions, that these factors be self-reciprocal. We give arithmetic conditions bearing on $p, q$ for these two constraints (three factors and self-reciprocity) on the factorization of $x^n + 1$ to hold. These constraints, in turn, are satisfied for infinitely many $p$'s, provided a refinement of the Artin primitive conjecture holds [14]. When this special factorization is thus enforced, we derive exact enumeration formulae, and obtain the asymptotic lower bound on the minimum distance of these double (resp. four)-negacirculant codes. This is an analogue of the Varshamov-Gilbert bound [4, 6, 9].

The paper is organized as follows. The next section collects some background material. In Section 3, we present a special kind of factorization of $x^n + 1$ over $\mathbb{F}_q$. Section 4 derives the enumeration formulae of the self-dual double (resp. four)-negacirculant codes of co-index $n$. In Section 5, we study the asymptotic performance of the double (resp. four)-negacirculant codes. Section 6 is the conclusion of this paper.
2 Preliminaries

2.1 Generator matrix

A matrix over a finite field $\mathbb{F}_q$, with $q$ odd prime, is said to be negacirculant if its rows are obtained by successive negashifts from the first row. Thus, such a matrix is uniquely determined by the polynomial $\in \mathbb{F}_q[x]$ whose $x$-expansion is the first row of the said matrix.

In fact, any $\lambda$-constacyclic code $C$ of length $n$ over $\mathbb{F}_q$ affords a natural structure of module over the auxiliary ring $R(n, \mathbb{F}_q) = \mathbb{F}_q[x]/(x^n - \lambda)$. Then, for $\lambda = -1$, double (resp. four)-negacirculant codes are quasi-twisted codes of index 2 (resp. 4). And double (resp. four)-negacirculant codes are 1 (resp. 2)-generator QT codes.

Double-negacirculant codes:

A double-negacirculant code $C_1$ of length $2n$ is a $[2n, n]$ code over the field $\mathbb{F}_q$ with a generator matrix of the form

$$G_1 = (I_n, H),$$

where $I_n$ is the identity matrix of order $n$, the matrix $H$ is an $n \times n$ negacirculant matrix (i.e., each row is the negashift of the previous one) over $\mathbb{F}_q$. Let $C_h$ be the double-negacirculant codes with the first row of $H$ being the $x$-expansion of $h$ in the ring $R(n, \mathbb{F}_q)$.

Four-negacirculant codes:

A four-negacirculant code $C_2$ of length $4n$ is a $[4n, 2n]$ code over the field $\mathbb{F}_q$ with a generator matrix of the form

$$G_2 = \begin{pmatrix} I_n & 0 & A & B \\ 0 & I_n & -B^t & A^t \end{pmatrix},$$

where $I_n$ is the identity matrix of order $n$, the matrices $A, B$ are the $n \times n$ negacirculant matrices over $\mathbb{F}_q$, and the exponent “$t$” denotes transposition.

By [5] Proposition 1 and the Section 3 in [10], let $A, B$ be commutative matrices over $\mathbb{F}_q$ such that $AA^t + BB^t + I_n = 0$, then $G_2$ generates a self-dual code $C_2$ of length $4n$ and dimension $2n$ over $\mathbb{F}_q$. In [5], many self-dual codes with good parameters are constructed in that way. Let $C_{a,b}$ be the four-negacirculant codes with the first rows of $A, B$ being the $x$-expansion of $a, b$ in the ring $R(n, \mathbb{F}_q)$.

Four-negacirculant codes have systematic generating matrices $G_2$ with $A, B$ are the $n \times n$ negacirculant matrices, as described in above. Algebraically, we can view such a code as an $R$-module in $R^4$, generated by $\langle (1, 0, a(x), b(x)), (0, 1, -b'(x), a'(x)) \rangle$, where $a'(x) = a(-x^{n-1}) \mod x^n + 1$, $b'(x) = b(-x^{n-1}) \mod x^n + 1$, $R = \mathbb{F}_q[x]/(x^n + 1)$. 

3
2.2 Asymptotics

Now, we recall the rate \( r \) and relative distance \( \delta \). If \( C(n) \) is a family of codes of parameters \([n, k_n, d_n]\), the rate \( r \) and relative distance \( \delta \) are defined as

\[
    r = \limsup_{n \to \infty} \frac{k_n}{n},
\]

and

\[
    \delta = \liminf_{n \to \infty} \frac{d_n}{n}.
\]

The \( q \)-ary entropy function is defined by [6]:

\[
    H_q(t) = \begin{cases} 
        t \log_q(q - 1) - t \log_q(t) - (1 - t) \log_q(1 - t), & 0 < t < \frac{q - 1}{q}, \\
        0, & t = 0.
    \end{cases}
\]

This quantity is instrumental in the estimation of the volume of high-dimensional Hamming balls when the base field is \( \mathbb{F}_q \). The result we are using is that the volume of the Hamming ball of radius \( t n \) is, up to subexponential terms, \( q^{n H_q(t)} \), when \( 0 < t < 1 \), and \( n \) goes to infinity [6, Lemma 2.10.3].

3 A special factorization of \( x^n + 1 \) over \( \mathbb{F}_q \)

In this section, we first recall the good integers, a concept introduced by Moree [13], with many applications in Coding Theory [7]. For fixed coprime nonzero integers \( a \) and \( b \), a positive integer \( d \) is said to be good (with respect to \( a \) and \( b \)) if it is a divisor of \( a^k + b^k \) for some integer \( k \geq 1 \). Otherwise, \( d \) is said to be bad. We will require the following lemma.

**Lemma 3.1.** ([7], Proposition 2.7) Let \( a, b \) and \( d > 1 \) be pairwise coprime odd positive integers and let \( \beta \geq 2 \) be an integer. Then \( 2^\beta d \in G_{(a,b)} \) if and only if \( \operatorname{ord}_{2^\beta}(\frac{a}{b}) = 2 \) and \( 2 \parallel \operatorname{ord}_{d}(\frac{a}{b}) \). In this case, \( 2 \parallel \operatorname{ord}_{2^\beta d}(\frac{a}{b}) \).

We are now ready to describe the main factorization result of this paper.

**Theorem 3.2.** Let \( n = 2p \), with \( p \equiv 3 \pmod{4} \), an odd prime. Let \( q \equiv 3 \pmod{4} \), denote a prime power \( \neq p \). Assume \( \operatorname{ord}_{4p}(q) = p - 1 \). Then \( x^n + 1 \) can be factored into the product of 3 irreducible polynomials over \( \mathbb{F}_q \), namely

\[
    x^n + 1 = (x^2 + 1)g_1(x)g_2(x),
\]

where \( \deg(g_1(x)) = \deg(g_2(x)) = p - 1 \). If, furthermore, the order of \( q \) mod \( p \) is \( \equiv 2 \pmod{4} \), then both \( g_1(x) \) and \( g_2(x) \) are self-reciprocal. In particular, if \( q \) is primitive modulo \( p \), then we have the said factorization in three factors with both \( g_1(x) \) and \( g_2(x) \) self-reciprocal.
Proof. If \( n = 2p, p \) is odd prime, \( q \equiv 3 \pmod{4} \), then \( x^{2p} + 1 = (x^2 + 1)Q_{4p}(x) \), where \( Q_r(.) \) denotes the cyclotomic polynomial of order \( r \). As is well-known its degree is \( \phi(r) \), Euler’s totient function that counts the number of integers \( m \) with \( 1 \leq m \leq r \) that are relatively prime to \( r \). It is easy to check that \( Q_{4p}(x) \) divides \( x^{4p} - 1 = (x^{2p} - 1)(x^{2p} + 1) \), but not \( x^{2p} - 1 \), the said factorization follows. Note that, since \( q \equiv 3 \pmod{4} \), \( x^2 + 1 \) is an irreducible polynomial over \( \mathbb{F}_q \). We compute \( \phi(4p) = \phi(4)\phi(p) = 2(p-1) \).

We need \( Q_{4p}(x) \) to be factored into 2 distinct monic irreducible polynomials in \( \mathbb{F}_q[x] \) of the same degree \( d \). By Theorem 3.47 in [11], we obtain \( d = \frac{\phi(4p)}{2} = p - 1 \), where \( d \) is the multiplicative order of \( q \) modulo \( 4p \), that is the least positive integer \( j \) such that \( q^j \equiv 1 \pmod{4p} \). Thus \( \text{ord}_{4p}(q) = p - 1 \).

The following observation shows that the order of \( q \) mod \( p \) is \( \equiv 2 \pmod{4} \), then \( g_1(x), g_2(x) \) are self-reciprocal polynomials. If \( x^n + 1 = (x^2 + 1)g_1(x)g_2(x) \), let \( \alpha \) be a root of \( g_1(x) \), i.e., \( g_1(\alpha) = 0 \), assume that \( g_1(x) \) is a self-reciprocal polynomial, then \( g_1(\alpha^{-1}) = 0 \), and \( \alpha^{-1} \in \{\alpha, \alpha^q, \ldots, \alpha^{q^{ord_q(\alpha)}}{-1}\} \). Thus there exists an integer \( i \) such that \( \alpha^{-1} = \alpha^q^i \). Since \( \alpha \) is of order \( 4p \), this yields \( q^i \equiv -1 \pmod{4p} \), where \( 0 \leq i \leq p - 2 \) and \( i \) is an odd integer. We obtain that \( 4p \mid q^i + 1 \), which shows \( 4p \) is a good integer for \( a = q \), and \( b = 1 \).

According to Lemma 3.1 we have \( 4p \in G_{(q,1)} \) if and only if \( 2 \parallel \text{ord}_p(q) \) (Note that the condition \( \text{ord}_d(q) = 2 \) is equivalent to \( q \equiv 3 \pmod{4} \)). The necessary condition in Lemma 3.1 that \( 2 \parallel \text{ord}_p(q) \) is equivalent to \( p \equiv 3 \pmod{4} \).

If \( q \) is primitive modulo \( p \), that is if \( \text{ord}_p(q) = p - 1 \) then we claim that \( \text{ord}_{4p}(q) = p - 1 \). Indeed \( q^{p-1} \equiv 1 \pmod{p} \). Since \( q \equiv 3 \pmod{4} \), and \( p \) is odd then \( q^{p-1} \equiv 1 \pmod{4} \). By the CRT on integers we have \( q^{p-1} \equiv 1 \pmod{4p} \), hence that \( \equiv 2 \pmod{4} \), divides \( p - 1 \). But \( \text{ord}_p(q) \) divides \( \text{ord}_{4p}(q) \) by definition of the order. That gives us \( \text{ord}_{4p}(q) = p - 1 \) and the three factor factorization. Since \( p \equiv 3 \pmod{4} \), we have \( \text{ord}_p(q) = p - 1 \equiv 2 \pmod{4} \), and the condition of self-reciprocity is also satisfied.

\[ \square \]

Remark 3.3. It is important to observe that \( \text{ord}_p(q) \) divides \( \text{ord}_{4p}(q) \) but may be not equal as shows the example \( p = 11, q = 27 \) when \( \text{ord}_{4p}(q) = 10 \) but \( \text{ord}_p(q) = 5 \).

Remark 3.4. According to the definition of good integers, in fact, \( d = 4p, a = q, b = 1 \) and \( k = i \) in Theorem 3.2. That is to say, the three conditions “if the order of \( q \) mod \( p \) is \( \equiv 2 \pmod{4} \)” “if there exists an odd integer \( i \) such that \( q^i \equiv -1 \pmod{4p} \), where \( 0 \leq i \leq p - 2 \)” and “if \( 4p \) is a good integer for some integer \( 0 \leq i \leq p - 2 \) and \( i \) is odd integer” are equivalent. Since \( i \) is an odd integer, we say that \( 4p \) is an oddly-good in the sense of [3].

Example 3.5. Let \( n = 14 \), i.e., \( p = 7, q = 3 \), i.e., \( q \equiv 3 \pmod{4} \), then \( \text{ord}_{28}(3) = 6 \) and \( \text{ord}_7(3) = 6 \equiv 2 \pmod{4} \). By Theorem 3.2 we obtain

\[ x^{14} + 1 = (x^2 + 1)(x^6 + x^5 + x^3 + x + 1)(x^6 + 2x^5 + 2x^3 + 2x + 1), \]
there exists an odd integer \( i = 3 \) such that \( q^3 \equiv -1 \pmod{4p} \).

**Example 3.6.** Let \( n = 22 \), i.e., \( p = 11 \), \( q = 7 \), i.e., \( q \equiv 3 \pmod{4} \), then \( \text{ord}_{11}(7) = 10 \) and \( \text{ord}_{11}(7) = 10 \equiv 2 \pmod{4} \). By Theorem 3.2, we obtain

\[
x^{22} + 1 = (x^2 + 1)(x^{10} + 2x^9 + 5x^8 + 2x^7 + 6x^6 + 5x^5 + 6x^4 + 2x^3 + 5x^2 + 2x + 1) \\
\cdot (x^{10} + 5x^9 + 5x^8 + 6x^6 + 2x^5 + 6x^4 + 5x^3 + 5x^2 + 5x + 1),
\]

there exists an odd integer \( i = 5 \) such that \( q^5 \equiv -1 \pmod{4p} \).

**Example 3.7.** Let \( n = 6 \), i.e., \( p = 3 \), \( q = 11 \), i.e., \( q \equiv 3 \pmod{4} \), then \( \text{ord}_{11}(11) = 2 \) and \( \text{ord}_{11}(11) = 2 \equiv 2 \pmod{4} \). By Theorem 3.2, we obtain

\[
x^6 + 1 = (x^2 + 1)(x^2 + 5x + 1)(x^2 + 6x + 1),
\]

there exists an odd integer \( i = 1 \) such that \( q \equiv -1 \pmod{4p} \).

The next result shows what happens in the three factors factorization when \( 4p \) is not a good integer w.r.t. \( q \) and 1.

**Theorem 3.8.** Let \( n = 2p, p \equiv 3 \pmod{4}, p \) an odd prime, \( q \equiv 3 \pmod{4} \), and \( \text{ord}_{1p}(q) = p - 1 \), if the order of \( q \) mod \( p \) is \( \not\equiv 2 \pmod{4} \), then \( x^n + 1 \) can be factored into the product of 3 irreducible polynomials over \( \mathbb{F}_q \):

\[
x^n + 1 = (x^2 + 1)f_1(x)f_2(x),
\]

where \( f_1(x) \) and \( f_2(x) \) are reciprocal polynomials of each other with \( \text{deg}(f_1(x)) = \text{deg}(f_2(x)) = p - 1 \) and \( p \not\equiv q \).

**Proof.** Since \( \frac{x^{2p} + 1}{x^2 + 1} \) is self-reciprocal, either \( g_1(x) \) and \( g_2(x) \) are both self-reciprocal, or they are reciprocal of each other. As the good character of \( 4p \) is equivalent to the first case of that alternative, by the proof of the preceding theorem, the result follows. \( \square \)

**Example 3.9.** Let \( n = 22 \), i.e., \( p = 11 \), \( q = 3 \), i.e., \( q \equiv 3 \pmod{4} \), then \( \text{ord}_{11}(3) = 10 \) and \( \text{ord}_{11}(3) = 5 \not\equiv 2 \pmod{4} \). By Theorem 3.2, we obtain

\[
x^{22} + 1 = (x^2 + 1)(x^{10} + 2x^6 + 2x^4 + 2x^2 + 1)(x^{10} + 2x^8 + 2x^6 + 2x^4 + 1),
\]

there does not exist an odd integer \( i \) such that \( q^i \equiv -1 \pmod{4p} \), where \( 0 \leq i \leq p - 2 \).

**Example 3.10.** Let \( n = 14 \), i.e., \( p = 7 \), \( q = 11 \), i.e., \( q \equiv 3 \pmod{4} \), then \( \text{ord}_{11}(11) = 6 \) and \( \text{ord}_{11}(11) = 3 \not\equiv 2 \pmod{4} \). By Theorem 3.2, we obtain

\[
x^{14} + 1 = (x^2 + 1)(x^6 + 4x^4 + 4x^2 + 1)(x^6 + 6x^4 + 4x^2 + 1),
\]

there does not exist an odd integer \( i \) such that \( q^i \equiv -1 \pmod{4p} \), where \( 0 \leq i \leq p - 2 \).
4 Exact enumeration

We shall need the following result on a special diagonal equation over a finite field.

**Lemma 4.1.** [2] If $q$ is odd, and $n$ is coprime with $q$, then the number of solutions $(a,b)$ in $\mathbb{F}_q^2$ of the equation $a^{1+q} + b^{1+q} = -1$ is $(q+1)(q^2-q)$.

This result is now used to count certain self-dual QT codes.

**Theorem 4.2.** Let $n = 2p, p \equiv 3 \pmod{4}, p$ an odd prime. Let $q$ be a prime power satisfying $q \equiv 3 \pmod{4}$, $\text{ord}_p(q) = p-1$ and $(p,q) = 1$. If the order of $q$ mod $p$ is $\equiv 2 \pmod{4}$, then $x^n + 1$ can be factored into the product of 3 irreducible polynomials over $\mathbb{F}_q$:

$$x^n + 1 = (x^2 + 1)g_1(x)g_2(x),$$

where $g_1(x), g_2(x)$ are self-reciprocal polynomials over $\mathbb{F}_q$ with $\deg(g_1(x)) = \deg(g_2(x)) = p - 1$. If these conditions are satisfied then

1. the number of self-dual double-negacirculant codes of length $2n$ over $\mathbb{F}_q$ with generator $\langle (1, h) \rangle$ is $(q+1)(q^{\frac{p-1}{2}}+1)^2$.

2. the number of self-dual four-negacirculant codes of length $4n$ over $\mathbb{F}_q$ with 2-generator $\langle (1,0,a,b), (0,1,-b', a') \rangle$ is $(q+1)(q^2-q)(q^{\frac{p-1}{2}}+1)^2(q^{p-1}-q^{\frac{p-1}{2}})^2$.

**Proof.** (1) Let $\mathbb{F}_q^* = \langle \zeta \rangle$ and $\varepsilon = \zeta^{q-1}$. A factor $x^2 + 1$ of degree 2 leads to counting self-dual Hermitian codes of length 2 over $\mathbb{F}_q^2$, that is to count the solutions of the equation $1 + hh^q = 0$ over that field. Solving this equation gives the desired result. Furthermore, all the roots of the equation $1 + hh^q = 0$ are simple and are given by the 1 + $q$ distinct elements $\zeta^{\frac{q-1}{2}}, \varepsilon \zeta^{\frac{q-1}{2}}, \ldots, \varepsilon^q \zeta^{\frac{q-1}{2}}$ of $\mathbb{F}_{q^2}$.

Similar to the above discussion, then the number of Hermitian self-dual codes over $\mathbb{F}_{q^{p-1}}$ for the self-reciprocal factor $g_j(x), j = 1, 2$ of degree $p - 1$ is $1 + q^{\frac{p-1}{2}}$. Thus the conclusion (1) holds.

(2) In case of a self-reciprocal factor $x^2 + 1$ of degree 2, we calculate the number of Hermitian self-dual codes of length 4 over $\mathbb{F}_q^2$. Writing the generator matrix of such a code in the form $\langle (1,0,a_1,b_1), (0,1,-b'_1,a'_1) \rangle$, we must count the solutions of the equation:

\[
\begin{cases}
1 + a_1a_1^q + b_1b_1^q = 0, \text{i.e., } a_1^{1+q} + b_1^{1+q} = -1,
1 + a'_1a'_1^q + b'_1b'_1^q = 0, \text{i.e., } a'_1^{1+q} + b'_1^{1+q} = -1.
\end{cases}
\]

In fact, we know that there exists a $i$ such that $a'_1 = a_1^q, b'_1 = b_1^q, i = 0, 1$, if $a_1, b_1$ is determined, then $a'_1, b'_1$ will be determined, thus here we only need to compute the number
of solutions of the equation \( a_1^{1+q} + b_1^{1+q} = -1 \) (\(^*\)). According to Lemma 5.1, then the number of solutions \((a_1, b_1)\) in \(\mathbb{F}_{q^2}\) of \((\text{\(^*\)})\) is \((q + 1)(q^2 - q)\).

In case of a self-reciprocal factor \( g_1(x) \) of degree \( p - 1 \), we calculate the number of Hermitian self-dual codes of length 4 over \(\mathbb{F}_{q^p-1}\). Writing the generator matrix of such a code in the form \(\langle (1,0,a_2,b_2),(0,1,-b'_2,a'_2)\rangle\), it suffices to solve the following system of two equations:

\[
\begin{align*}
1 + a_2a_2q^{\frac{q-1}{2}} + b_2b_2q^{\frac{q-1}{2}} &= 0, \text{i.e., } a_2^{1+q} + b_2^{1+q} = -1, \\
1 + a'_2a'_2q^{\frac{q-1}{2}} + b'_2b'_2q^{\frac{q-1}{2}} &= 0, \text{i.e., } a'_2^{1+q} + b'_2^{1+q} = -1.
\end{align*}
\]

(1)

Applying Lemma 4.1 then the number of solutions \((a_2, b_2)\) in \(\mathbb{F}_{q^p-1}\) of (1) is \((q^{\frac{p-1}{2}} + 1)(q^{p-1} - q^{\frac{p-1}{2}})\).

By working in the same way as the case \( g_1(x) \), for the self-reciprocal factor \( g_2(x) \) of degree \( p - 1 \), we can also deduce that the number of Hermitian self-dual codes over \(\mathbb{F}_{q^p-1}\) is \((q^{\frac{p-1}{2}} + 1)(q^{p-1} - q^{\frac{p-1}{2}})\). This completes the proof of statement (2). \(\square\)

5 Asymptotics of double (resp. four)-negacirculant codes

In this section, assume that \( q \equiv 3 \pmod{4} \) and \( p \) is an odd prime with \( p \equiv 3 \pmod{4} \). Set \( n = 2p \). As discussed in Section 3, we consider \( x^n + 1 = (x^2 + 1)g_1(x)g_2(x) \), where \( g_1(x), g_2(x) \) are self-reciprocal polynomials over \(\mathbb{F}_q\) with \(\deg(g_1(x)) = \deg(g_2(x)) = p - 1\). By the Chinese Remainder Theorem (CRT), we have

\[
\mathbb{F}_q[x]/\langle x^n + 1 \rangle \simeq \mathbb{F}_q[x]/\langle x^2 + 1 \rangle \oplus \mathbb{F}_q[x]/(g_1(x)) \oplus \mathbb{F}_q[x]/(g_2(x))
\]

\[
\simeq \mathbb{F}_{q^2} \oplus \mathbb{F}_{q^p-1} \oplus \mathbb{F}_{q^p-1}.
\]

Lemma 5.1. If \( u \neq 0 \) has Hamming weight < \( 2p \),

1. there are at most \( q^2(q^{\frac{2n}{2}} - 1) \) vectors \( h \) such that \( u \in C_h = \langle (1, h) \rangle \) and \( C_h = C_h^\perp \).

2. there are at most \( q^4(q^{\frac{2n}{2}} - 1)(q^{\frac{n}{2}} - q^{\frac{n}{2}})q^{\frac{n}{2}} \) pairs \((a,b)\) such that \( u \in C_{a,b} = \langle (1,0,a,b),(0,1,-b',a') \rangle \) and \( C_{a,b} = C_{a,b}^\perp \).

Proof. (1) Let \( C_h = \langle (1, h) \rangle \) and \( u = (v, w) \) with \( v, w \) vectors of length \( n \). The condition of \( u \in C_h \) is equivalent to the equations modulo \( x^n + 1: w = vh \). By hypothesis \( u \neq 0 \) and \( wt(u) < 2p, \) imply \( v, w \) cannot both in \( \langle g_1(x)g_2(x) \rangle \backslash \{0\}. \)

If \( v \equiv 0 \pmod{g_1(x)g_2(x)} \), then \( wt(u) = 2p \), it is a contradiction.

If \( v \notin \langle g_1(x)g_2(x) \rangle \backslash \{0\} \), we have the following cases:
• If \( v \equiv 0 \pmod{g_1(x)} \), then \( 1 + hh^{\frac{p-1}{2}} = 0 \) has \( 1 + q^{\frac{p-1}{2}} \) solutions, and \( v \not\equiv 0 \pmod{g_2(x)} \), then \( h = \frac{w}{v} \mod g_2(x) \) has a unique solution. By the CRT in this case, there are at most \( q^2(q^{\frac{p-1}{2}} + 1) \) vector \( h \) such that \( u \in C_h = \langle (1, h) \rangle \) and \( C_h = C_{\overline{h}} \). (The \( q^2 \) comes from the factor \( (x^2 + 1) \)).

• The case \( v \not\equiv 0 \pmod{g_1(x)} \) and \( v \equiv 0 \pmod{g_2(x)} \) is a similar to the preceding.

• If \( v \not\equiv 0 \pmod{g_1(x)} \) and \( v \not\equiv 0 \pmod{g_2(x)} \), then \( h = \frac{w}{v} \mod g_1(x)g_2(x) \) has a unique solution.

(2) Let \( C_{a,b} = \langle (1, 0, a, b), (0, 1, -b', a') \rangle \) and \( u = (c, d, e, f) \) with \( c, d, e, f \) vectors of length \( n \). The condition of \( u \in C_{a,b} \) leads to the following equations modulo \( x^n + 1 \):

\[
\begin{align*}
    e &= ca - db', \\
    f &= cb + da'.
\end{align*}
\]

The hypotheses \( u \not\equiv 0 \) and \( wt(u) < 2p \), imply that there cannot have any two of \( \{c, d, e, f\} \) both in \( (g_1(x)g_2(x))\setminus\{0\} \). Since \( c, d \) cannot be both in \( (g_1(x)g_2(x))\setminus\{0\} \), without loss of generality, let \( d \notin (g_1(x)g_2(x)) \). It requires to consider three cases:

1) If \( d \equiv 0 \pmod{g_1(x)} \) and \( d \not\equiv 0 \pmod{g_2(x)} \);

2) If \( d \not\equiv 0 \pmod{g_1(x)} \) and \( d \equiv 0 \pmod{g_2(x)} \);

3) If \( d \not\equiv 0 \pmod{g_1(x)} \) and \( d \not\equiv 0 \pmod{g_2(x)} \).

Next, we will discuss successively these three cases in turn:

1) If \( d \equiv 0 \pmod{g_1(x)} \), we have

\[
\begin{align*}
    e &= ca \mod g_1(x), \\
    f &= cb \mod g_1(x).
\end{align*}
\]

• a) If \( c \not\equiv 0 \pmod{g_1(x)} \), then there exists unique pair \((a, b)\) \((mod \ g_1(x))\).

• b) If \( c \equiv 0 \pmod{g_1(x)} \), then \( c, d, e, f \equiv 0 \pmod{g_1(x)} \), and the above system does not bring any information on \( a \) and \( b \).

But we know that \( C_{a,b} = C_{\overline{a},\overline{b}} \), and thus \( a^{1+q^{\frac{p-1}{2}}} + b^{1+q^{\frac{p-1}{2}}} = -1 \). Therefore, there are at most \( (q^{\frac{p-1}{2}} + 1)(q^{p-1} - q^{\frac{p-1}{2}}) \) pairs \((a, b)\) \((mod \ g_1(x))\). And because \( d \not\equiv 0 \pmod{g_2(x)} \), we obtain \( b' = \frac{ca - db}{d} \mod g_2(x) \). Thus, for a given \( a, b \) is unique. Note that there are \( q^{p-1} \) choices for \( a \).
All the above show that, by the CRT in case 1), there are at most \(q^4(q^{\frac{p-1}{2}} + 1)(q^{p-1} - q^{\frac{p-1}{2}})q^{p-1}\) pairs \((a, b)\) such that \(u \in C_{a,b} = \langle (1, 0, a, b), (0, 1, -b', a') \rangle\) and \(C_{a,b} = C_{a,b}^\perp\) (The \(q^4\) comes from the factor \((x^2 + 1)\)).

2) This case is symmetric to 1) in the discussion, hence it is omitted.

3) In this case, for given \(a\), there exists unique \(b \mod (g_1(x)g_2(x))\). There are \(q^n\) choices for \(a\), i.e., there are \(q^n\) pairs \((a, b)\). Note that this is dominated by the count in 1, which is of order \(O(q^{\frac{3n}{2}})\).

Hence, combining these three scenarios, we obtain that there are at most \(q^4(q^{\frac{n-2}{2}} + 1)(q^{\frac{n-2}{2}} - q^{\frac{n-2}{2}})q^{\frac{n-2}{2}}\) pairs \((a, b)\) such that \(u \in C_{a,b} = \langle (1, 0, a, b), (0, 1, -b', a') \rangle\) and \(C_{a,b} = C_{a,b}^\perp\). □

We are now ready to present the main results in this section.

**Theorem 5.2.** Under the hypotheses of Theorem 3.2, if \(q\) is prime power and \(q \equiv 3 \pmod{4}\), and \(n = 2p\), then

1. there are infinite families of self-dual double-negacirculant codes of length \(2n\) over \(\mathbb{F}_q\), of relative distance \(\delta\), satisfying \(H_q(\delta) \geq \frac{1}{8}\).

2. there are infinite families of self-dual four-negacirculant codes of length \(4n\) over \(\mathbb{F}_q\), of relative distance \(\delta\), satisfying \(H_q(\delta) \geq \frac{1}{16}\).

**Proof.** Observe first that the infinitude of the primes \(p \equiv 3 \pmod{4}\), admitting a fixed number \(q\) as a primitive root is guaranteed by [14, Theorem 3], which derives (under GRH) a density for this family of primes.

(1) The double-negacirculant codes containing a vector of weight \(d \sim 2\delta n\) or less are by standard entropic estimates and Lemma 5.1 of order at most \(q^n \times q^{2nH_q(\delta)}\), up to subexponential terms. This number will be less than the total number of self-dual four-negacirculant codes which is by Theorem 4.2 of the order of \(q^{\frac{3n}{2}}\).

(2) The four-negacirculant codes containing a vector of weight \(d \sim 4\delta n\) or less are by standard entropic estimates and Lemma 5.1 of order at most \(q^{5n} \times q^{4nH_q(\delta)}\), up to subexponential terms. This number will be less than the total number of self-dual four-negacirculant codes which is by Theorem 4.2 of the order of \(q^{\frac{3n}{2}}\). □

**Remark 5.3.** The rates of the codes in this result are both \(1/2\). Thus our bounds are below the Varshamov-Gilbert bound for the linear codes which would be \(H_q(\delta) \geq \frac{1}{2}\).
6 Conclusion

In this paper, we have studied the class of self-dual double (resp. four)-negacirculant codes over finite fields. Motivated by [1], A. Alahmadi et al. have studied the special factorization $x^n + 1$ when it factors into two irreducible factors reciprocal of each other for $n$ a power of 2. Here, we have studied another special kind of decomposition, for $n$ twice an odd prime, when $x^n + 1$ factors into three irreducible and self-reciprocal polynomials. Further, we have derived an exact enumeration formula for this family of self-dual double (resp. four)-negacirculant codes. The modified Varshamov-Gilbert bound on the relative minimum distance we derived relies on some deep number-theoretic conjectures (Artin primitive root in arithmetic progression or Generalized Riemann Hypothesis). It would be a worthwhile study to consider more general factorizations of $x^n + 1$, and also to look at QT codes with more than two generators.

References

[1] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaiib, P. Solé, On self-dual double negacirculant codes, Discrete Applied Mathematics, 222 (2017) 205-212.

[2] A. Alahmadi, C. Güneri, B. Özkaya, H. Shoaiib, P. Solé, On linear complementary-dual multinegacirculant codes, submitted for publication.

[3] I. F. Blake, S. Gao, R. C. Mullin, Explicit factorization of $x^{2^k} + 1$ over $F_p$ with prime $p \equiv 3 \pmod{4}$, Applicable Algebra in Engineering, Communication and Computing, 4 (1993) 89-94.

[4] V. Chepyzhov, A Varshamov-Gilbert bound for quasi-twisted codes of rate $\frac{1}{n}$, in: Proceedings of the joint Swedish-Russian International workshop on Information Theory, MÖlle, Sweden, (1993) 214-218.

[5] Masashi Harada, W. Holzmann, H. Kharaghani, M. Khorvash, Extremal ternary self-dual codes constructed from negacirculant matrices, Graphs and Combinatorics, 23 (2007) 401–417.

[6] W. C. Huffman, V. Pless, Fundamentals of error correcting codes, Cambridge University Press, 2003.

[7] S. Jitman, Good integers and some applications in coding theory, arXiv: 1611.04539v2, 2017.
[8] Y. Jia, On quasi-twisted codes over finite fields, Finite Fields and their Applications, 18 (2012) 237-257.

[9] T. Kasami, A Gilbert-Varhamov bound for quasi-cyclic codes of rate \( \frac{1}{2} \), IEEE Transactions on Information Theory, 20 (1974) 679.

[10] A. Kaya, B. Yildiz, A. Pasa, New extremal binary self-dual codes from a modified four circulant construction, Discrete Mathematics, 339 (2016) 1086-1094.

[11] R. Lidl, H. Niederreiter, P. M. Cohn, Finite fields, Cambridge University Press, 1997.

[12] H. Meyn, Factorization of the cyclotomic polynomial \( x^{2^n} + 1 \) over finite fields, Finite Fields and their Applications, (1996) 439-442.

[13] P. Moree, On the divisors of \( a^k + b^k \). Acta Arithmetica, 80 (1997) 197–212.

[14] P. Moree, On primes in arithmetic progression having a prescribed primitive root, Functiones Et Approximatio, 78 (1999) 85-98.