On linear complementary-dual multinegacirculant codes

Adel Alahmadi[*], Cem Güneri[†], Buket Özkaya[‡],
Hatoon Shoaib[§], Patrick Solé[¶]

Abstract

Linear codes with complementary-duals (LCD) are linear codes that intersect with their dual trivially. Multinegacirculant codes of index 2 that are LCD are characterized algebraically and some good codes are found in this family. Exact enumeration is performed for indices 2 and 3, and for all indices t for a special case of the co-index by using their concatenated structure. Asymptotic existence results are derived for the special class of such codes that are one-generator and have co-index a power of two by means of Dickson polynomials. This shows that there are infinite families of LCD multinegacirculant codes with relative distance satisfying a modified Varshamov-Gilbert bound.

Keywords: LCD codes, quasi-twisted codes, Varshamov-Gilbert bound

1 Introduction

Linear complementary dual codes (LCD) are linear codes that intersect with their dual trivially. They were introduced by Massey in [13], and rediscovered a few years ago in the context of side-channel attacks [3], and recently, in the domain of quantum error correcting codes for entanglement assisted communication [5]. In a recent paper the class of quasi-cyclic LCD codes was shown to be "good" [6]. The main result of the present paper is to show that some classes of one-generator quasi-twisted codes, an odd characteristic analogue of quasi-cyclic codes, are not only good, but better than the Varshamov-Gilbert bound. Some exact enumeration results for index 2 and index 3

[*] Math. Dept., King Abdulaziz University, Jeddah, Saudi Arabia, Email: adelnife2@yahoo.com

[†] Sabancı University, FENS, 34956 Istanbul, Turkey, Email: guneri@sabanciuniv.edu

[‡] Sabancı University, FENS, 34956 Istanbul, Turkey, Email: buketozkaya@sabanciuniv.edu

[§] Math. Dept., King Abdulaziz University, Jeddah, Saudi Arabia, Email: hashoaib@kau.edu.sa

[¶] CNRS/LAGA, Université de Paris 8, 93 526 Saint-Denis, France, Email: sole@math.univ-paris13.fr

are also derived. For a general index t and co-index power of 2, a special enumeration is given which is needed for asymptotic analysis. A construction technique for index 2 (double negacirculant codes), and some examples of optimal or best such codes in modest lengths are given. The main technical ingredients of the proofs are some results on the number of solutions of certain diagonal equations over finite fields, given in the Appendix.

The material is organized as follows. The next section surveys the algebraic structures of the codes we study. Section 3 collects the notions and notations needed in the rest of the paper. Section 4 recalls some known facts on double negacirculant codes. Section 5 describes the factorization of $x^n + 1$ over $\mathbb{F}_q$ when n is a power of 2, and q is odd. Section 6 characterizes algebraically LCD double negacirculant codes and gives some examples with optimum distance in modest lengths. Section 7 contains exact enumeration formulae. Section 8 builds on Section 7 to study the asymptotic performance of multinegacirculant codes of index t where $t \geq 2$. Section 9 recapitulates the results we obtained, and exhibits some challenging open problems. Section 10 is the Appendix mentioned above.

2 Preliminaries

A matrix A over a finite field $\mathbb{F}_q$ is said to be *negacirculant* if its rows are obtained by successive negashifts from the first row. A *negashift* maps the vector $(x_0, \dots, x_{n-1}) \in \mathbb{F}_q^n$ to $(-x_{n-1}, x_0, \dots, x_{n-2})$.

In this paper we consider *double negacirculant* (DN) codes over finite fields, that is, $[2n, n]$ codes with generator matrices of shape (I, A) with I the identity matrix of size n and A a negacirculant matrix of order n. This construction was introduced in [8] under the name *quasi-twisted code.* We prefer to reserve this term for the more general class of codes described in [10]. Before describing this class, we also define negacirculant codes of higher index over finite fields.

Three-negacirculant codes are $[3n, n]$ codes with generator matrices of the shape (I, A, B) with A, B negacirculant matrices of order n. Similarly one can define the t-negacirculant code (for any $t > 3$) and call all such codes multinegacirculant.

A code of length N is *quasi-twisted* of index ℓ where $\ell \mid N$, and co-index $m = \frac{N}{\ell}$ if it is invariant under the power T_α^ℓ of the *constashift* T_α defined as

$$T_\alpha : (x_0, \dots, x_{N-1}) \mapsto (\alpha x_{N-1}, x_0, \dots, x_{N-2}).$$

Thus for $\alpha = -1$, DN codes are quasi-twisted codes of index 2, and three-negacirculant codes are quasi-twisted codes of index 3, etc. Such a code affords a natural module structure over the auxiliary ring

$$R(m, \mathbb{F}_q) = \frac{\mathbb{F}_q[x]}{\langle x^m - \alpha \rangle}.$$

In other words, it can be regarded as a code of length ℓ over the ring $R(m, \mathbb{F}_q)$. When this module has one generator over that ring the code is said to be *one-generator*. An algebraic way to study such a code is to decompose the semilocal ring $R(m, \mathbb{F}_q)$ as a direct sum of local rings by the Chinese Remainder Theorem [10], thus following the approach initiated for quasi-cyclic codes in [12]. The benefit of this technique is to reduce the study of QT codes to that of shorter codes over larger alphabets. Besides, the study of duality is made transparent, thus allowing the construction of LCD QT codes, as in, for instance, [10]. The number of rings occurring in the decomposition of $R(m, \mathbb{F}_q)$ equals the number of irreducible factors of $x^m - \alpha$. In the following section we focus on LCD DN codes. These have been explored numerically in [6]. For some specific alphabets, it can be shown that in that case $x^n + 1$ can be factored into the product of two irreducible polynomials [11, 14]. This is a favourable situation in which to apply the Chinese Remainder Theorem approach of [12, 10], as the decomposition of $R(m, \mathbb{F}_q)$ contains only two terms. It allows to derive exact enumeration formulae and, from there, using the so-called expurgated random coding technique, to give an asymptotic lower bound on the minimum distance of these one-generator quasi-twisted codes of fixed arbitrary index. This is an analogue of the Varshamov Gilbert bound.

3 Definitions and Notation

3.1 Codes

Let $\mathbb{F}_q$ denote the finite field of order some prime-power q. We assume throughout that q is odd. In the following, we shall consider codes over $\mathbb{F}_q$ of length $2n$ which is coprime to q. Their generator matrices G will be of the form $G = (I, A)$, where I is the identity matrix of order n and A is an $(n \times n)$-negacirculant matrix. We call such codes *double negacirculant* (DN) codes. We shall denote by $\mathcal{C}_a$ the DN code with first row of A being the $x-$expansion of $a(x)$ in the ring $R(n, \mathbb{F}_q)$. Specifically, if $a(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, then the first row is $(a_0, a_1, \ldots, a_{n-1})$ and the other rows of A are obtained by negashifts of the previous row.

If $\mathcal{C}(m)$ is a family of codes of parameters $[m, k_m, d_m]$, the *rate* R and *relative distance* δ are defined as

$$R = \limsup_{m\to\infty} \frac{k_m}{m},$$

and

$$\delta = \liminf_{m\to\infty} \frac{d_m}{m}.$$

Both limits are finite as they are limits of bounded quantities. Such a family of codes is said to be *good* if $R\delta \neq 0$.

Recall the $q-$ary *entropy function* is defined for $0 < y < \frac{q-1}{q}$ by

$$H_q(y) = y \log_q(q-1) - y \log_q(y) - (1-y)\log_q(1-y).$$

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 yn is, up to subexponential terms, $q^{nH_q(y)}$, when $0 < y < 1$, and n goes to infinity [9, Lemma 2.10.3].

3.2 Polynomials

The *Dickson polynomials* (of the first kind) are given by $D_0(x,\alpha)=2$, and for $m>0$, by

$$D_m(x,\alpha)=\sum_{p=0}^{\lfloor m/2\rfloor}\frac{m}{m-p}\binom{m-p}{p}(-\alpha)^p x^{m-2p}.$$

The D_m satisfy the identity

$$D_m(u+\alpha/u,\alpha)=u^m+(\alpha/u)^m.$$

4 Background on Double Negacirculant Codes

We consider double negacirculant (DN) codes over finite fields. These are $[2n,n]$ codes over $\mathbb{F}_q$, where the codewords are closed under two negashifts. DN codes have systematic generating matrices $G=(I_n : A)$ with A an $n\times n$ negacirculant matrix. Algebraically, we can view such a code as an R-module in R^2, generated by $(1,a(x))$, where $R=\mathbb{F}_q[x]/\langle x^n+1\rangle$. In other words, a DN code is an index 2 quasi-twisted code with $\lambda=-1$ (see [10] for notation and more information on quasi-twisted codes).

If the characteristic of $\mathbb{F}_q$ is 2, then a cyclic shift and a negashift are the same. Hence a DN code is simply a double circulant code. Therefore we assume throughout that q is odd. Moreover, we will assume that n is relatively prime to q.

As in [10], assume that the factorization of x^n+1 into irreducible polynomials over $\mathbb{F}_q$ is of the form

$$x^n+1=\alpha\prod_{i=1}^{s}g_i(x)\prod_{j=1}^{t}h_j(x)h_j^*(x), \tag{1}$$

where $\alpha\in\mathbb{F}_q$, g_j a self-reciprocal polynomial and $*$ denotes reciprocation. Let ξ be a primitive $(2n)^{th}$ root of unity over $\mathbb{F}_q$. Then $\xi^n=-1$ and hence ξ is a root of x^n+1. Moreover, $\xi^{-1}=-\xi^{n-1}$. Assume that $g_i(\xi^{u_i})=0$ and $h_j(\xi^{v_j})=0$ (for all i,j). Then we also have $h_j^*(-\xi^{(n-1)v_j})=0$. By the Chinese Remainder Theorem (CRT) we have

$$\begin{aligned} R &\simeq (\bigoplus_{i=1}^{s}\mathbb{F}_q[x]/\langle g_i\rangle)\oplus(\bigoplus_{j=1}^{t}(\mathbb{F}_q[x]/\langle h_j\rangle\oplus(\mathbb{F}_q[x]/\langle h_j^*\rangle)))\\ &= (\bigoplus_{i=1}^{s}\mathbb{F}_q(\xi^{u_i}))\oplus(\bigoplus_{j=1}^{t}(\mathbb{F}_q(\xi^{v_j})\oplus(\mathbb{F}_q(-\xi^{(n-1)v_j}))).\end{aligned}$$

Let $G_i=\mathbb{F}_q[x]/\langle g_i\rangle$, $H_j'=\mathbb{F}_q[x]/\langle h_j\rangle$ and $H_j''=\mathbb{F}_q[x]/\langle h_j^*\rangle$ for simplicity. Note that all of these fields are extensions of $\mathbb{F}_q$. This decomposition naturally extends to R^2 and then a linear code $\mathcal{C}\subset R^2$ decomposes as

$$\mathcal{C}=(\bigoplus_{i=1}^{s}\mathcal{C}_i)\oplus(\bigoplus_{j=1}^{t}(\mathcal{C}_j'\oplus\mathcal{C}_j'')), \tag{2}$$

where each component code (constituent) is a length 2 linear code defined over the respective base field G_i, H'_j, H''_j. More specifically, again by CRT, we have

$$\begin{array}{rcl} \mathcal{C}_i & = & \mathrm{Span}_{G_i}\{(1, a(\xi^{u_i}))\},\ 1 \leq i \leq s, \\ \mathcal{C}'_j & = & \mathrm{Span}_{H'_j}\{(1, a(\xi^{v_j}))\},\ 1 \leq j \leq t, \\ \mathcal{C}''_j & = & \mathrm{Span}_{H''_j}\{(1, a(-\xi^{(n-1)v_j}))\},\ 1 \leq j \leq t. \end{array} \tag{3}$$

The Euclidean dual of C in $\mathbb{F}_q^{2n}$ is also a DN code and its decomposition is as follows ([10, Theorem 3]):

$$\mathcal{C}^{\perp} = (\bigoplus_{i=1}^{s} \mathcal{C}_i^{\perp_H}) \oplus (\bigoplus_{j=1}^{t} (\mathcal{C}_j^{''\perp_E} \oplus \mathcal{C}_j^{'\perp_E})). \tag{4}$$

Here, $\perp_H$ denotes the Hermitian dual on G_i for all $1 \leq i \leq s$, and $\perp_E$ denotes the Euclidean dual on $H_j^{'}$, $H_j^{''}$ for all $1 \leq j \leq t$. For instance,

$$(1, a(\xi^{u_i})) \cdot_{G_i} (1, a(\xi^{u_i})) = 1 + a(\xi^{u_i})a(-\xi^{(n-1)u_i}).$$

Remark 4.1 Let us note that the CRT decomposition described in this section extends naturally to higher indices $t \geq 3$. In this case, the codes are R-submodules of R^t.

5 Factorizations

The complete factorization of $x^{2^n} + 1$ over $\mathbb{F}_q$ with $q \equiv 3 \pmod 4$ is given by the following theorem [14].

Theorem 5.1 *Let $q \equiv 3 \pmod 4$, where $q = 2^A m - 1$, $A \geq 2$, m an odd integer. Let $n \geq 2$.*
(a) If $n < A$, then $x^{2^n} + 1$ is the product of 2^{n-1} irreducible quadratic trinomials over $\mathbb{F}_q$

$$x^{2^n} + 1 = \prod_{\gamma \in \Gamma} (x^2 + \gamma x + 1),$$

where Γ is the set of all roots of $D_{2^{n-1}}(x, 1)$.
(b) If $n \geq A$, then $x^{2^n} + 1$ is the product of 2^{A-1} irreducible trinomials over $\mathbb{F}_q$

$$x^{2^n} + 1 = \prod_{\delta \in \Delta} (x^{n-A+1} + \delta x^{n-A} - 1),$$

where Δ is the set of all roots of $D_{2^{A-1}}(x, -1)$ in $\mathbb{F}_q$.

Example 5.2 If $q = 3$ i.e. $q \equiv 3 \pmod 4$, then $q = 2^2.1 - 1$ implies that $A = 2$, $m = 1$, and $\Delta = \{1, 2\}$, then by Theorem 5.1:

$$x^{2^n} + 1 = (x^{2^{n-1}} + x^{2^{n-2}} + 2)(x^{2^{n-1}} + 2x^{2^{n-2}} + 2).$$

Theorem 5.3 *Let $q \equiv 1 \pmod 4$, where $q = 2^A m + 1$, $A \geq 2$, m is odd integer. Denote by U_k the set of all primitive 2^kth roots of unity in $\mathbb{F}_q$. If $n \geq 2$, then*

(a) If $n \leq A$, then $ord_{2^{n+1}}(q) = 1$ and $x^{2^n} + 1$ is the product of 2^n linear factors over $\mathbb{F}_q$

$$x^{2^n} + 1 = \prod_{u \in U_{n+1}} (x + u).$$

(b) If $n \geq A + 1$, then $ord_{2^{n+1}}(q) = 2^{n-A}$ and $x^{2^n} + 1$ is the product of 2^A irreducible binomials over $\mathbb{F}_q$ of degree 2^{n-A}

$$x^{2^n} + 1 = \prod_{u \in U_{A+1}} (x^{2^{n-A}} + u).$$

Example 5.4 If $q = 5$ i.e. $q \equiv 1 \pmod 4$, then $q = 2^2.1 + 1$ implies that $A = 1$, $m = 1$, and $U_2 = \{2, 3\}$, then by Theorem 5.3:

$$x^{2^n} + 1 = (x^{2^{n-1}} + 2)(x^{2^{n-1}} + 3).$$

6 Constructions and Examples

In this section, we characterize linear complementary-dual ($\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$) DN codes. The proof is very similar to the double circulant case ([6, Theorem 5.1]).

Theorem 6.1 *Let $\mathcal{C} = \langle (1, a(x)) \rangle \subset R^2$ be a double negacirculant code over $\mathbb{F}_q$. Then, $\mathcal{C}$ is linear complementary-dual if and only if* $\gcd(1 + a(x)a(-x^{n-1}), x^n + 1) = 1$.

Proof. Let ξ be a primitive $(2n)^{th}$ root of unity, and assume that $x^n + 1$ factors as in (1). Constituents of $\mathcal{C}$ are described in (3). Note that each constituent is a 1-dimensional space in the two dimensional ambient space. Hence, the dual of any constituent is 1-dimensional too.

Note that in terms of constituents, we have that $\mathcal{C}$ is linear complementary-dual if and only if $\mathcal{C}_i$ is linear complementary-dual relative to Hermitian product in G_i^2 for all i, and $\mathcal{C}_j' \cap \mathcal{C}_j''^\perp = \{0\}$, $\mathcal{C}_j'' \cap \mathcal{C}_j'^\perp = \{0\}$ for all j.

Observe that $\mathcal{C}_i \cap \mathcal{C}_i^{\perp_{G_i}} \neq \{0\}$ if and only if $\mathcal{C}_i = \mathcal{C}_i^{\perp_{G_i}}$, which is equivalent to

$$1 + a(\xi^{u_i})a(-\xi^{(n-1)u_i}) = 0.$$

On the other hand, $\mathcal{C}_j' \cap \mathcal{C}_j''^\perp \neq \{0\}$ if and only if $\mathcal{C}_j' = \mathcal{C}_j''^\perp$, which is equivalent to

$$1 + a(\xi^{v_j})a(-\xi^{(n-1)v_j}) = 0.$$

The last intersection $\mathcal{C}_j'' \cap \mathcal{C}_j'^\perp \neq \{0\}$ does not bring a new condition. Therefore, being LCD for $\mathcal{C}$ is equivalent to the polynomial $a(x)a(-x^{n-1}) + 1$ not vanishing at any root of $x^n + 1$. $\square$

The following table displays the best possible distances for double negacirculant LCD codes $\mathcal{C} = \langle (1, a(x)) \rangle \subset R^2$, where $\mathcal{C}$ is DN of length $2n$ and dimension n and index 2. The search was done in Magma ([2]) for $q = 5$ and random $a(x) \in R$ satisfying the conditions in the above Theorem. Entries marked with $*$ are optimal or have best-known parameters.

$\boldsymbol{n}$	3	4	6	7	8	9	11	12	13	14	16	17
$\boldsymbol{d}$	4*	4*	6*	6*	7*	7*	8*	9*	9	9	11*	11*
$\boldsymbol{d*}$	4	4	6	6	7	7	8	9	10	11	11	11
$\boldsymbol{r}$	480	128	384	28	64	36	44	48	52	56	64	68

Here, d is the minimum distance, $d*$ is the highest minimum distance of a linear code of given length and dimension [4], and r is the size of automorphism group.

7 Enumeration

In this section we use repeatedly the following observation. If a quasi-twisted code has one generator as a module over the ring $R(m, \mathbb{F}_q)$, then it is either self-orthogonal or LCD.

7.1 Index 2

We give a general enumeration formula that is not needed for asymptotics, but of interest in its own right. Recall that the so-called *quadratic character* η of $\mathbb{F}_q$ is defined as $\eta(x) = 1$ if $x \in \mathbb{F}_q$ is a nonzero square and $\eta(x) = -1$ if not.

Proposition 7.1 *Let q be an odd prime power, and $n \geq 1$ be an integer coprime to q. Assume that the factorization of $x^n + 1$ into irreducible polynomials over $\mathbb{F}_q$ is of the form*

$$x^n + 1 = \alpha \prod_{i=1}^{s} g_i(x) \prod_{j=1}^{t} h_j(x) h_j^*(x),$$

with $\alpha \in \mathbb{F}_q^*$, and g_i a self-reciprocal polynomial of degree $2d_i$, the polynomial h_j is of degree e_j and $*$ denotes reciprocation. If n is odd, then let $g_1 = x + 1$. The number of LCD double negacirculant codes over $\mathbb{F}_q$ of length $2n$ is

- $(q-2) \prod_{i=2}^{s} (q^{2d_i} - q^{d_i} - 2) \prod_{j=1}^{t} (q^{e_j} - 1)(q^{e_j} - 2)$ *if* $\eta(-1) = 1$ *and,*
- $q \prod_{i=2}^{s} (q^{2d_i} - q^{d_i} - 2) \prod_{j=1}^{t} (q^{e_j} - 1)(q^{e_j} - 2)$ *if* $\eta(-1) = -1$,

if n is odd and it is

$$\prod_{i=1}^{s}(q^{2d_i}-q^{d_i}-2)\prod_{j=1}^{t}(q^{e_j}-1)(q^{e_j}-2),$$

when n is even.

Proof. We use the Chinese Remainder Theorem (CRT) decomposition of $R(n,\mathbb{F}_q)$, as explained in §4. Since we are counting LCD quasi-twisted codes of index 2, we are reduced to count certain codes of length 2 and dimension 1 over some extension $\mathbb{F}_Q$ of $\mathbb{F}_q$.

In the case of $Q=q$ which happens for n odd we have to count Euclidean self-orthogonal codes of length 2 and dimension one over $\mathbb{F}_q$. They are of the form $\langle[1,a]\rangle$, with a a square root of -1. We thus have q or $q-2$ coefficients a giving LCD codes, depending on $\eta(-1)=-1$ or $\eta(-1)=1$.

A *self-reciprocal* factor $g_i(x)$ of degree $2d_i$ leads to counting LCD hermitian codes of length 2 over $\mathbb{F}_Q$, where $Q=q^{2d_i}$. The Hermitian self-dual codes of length 2 and dimension 1 over $\mathbb{F}_Q$ are of the form $\langle[1,a]\rangle$, with $a\in\mathbb{F}_Q$, a solution of $1+a^{1+\sqrt{Q}}=0$. By finite field theory, this equation in a admits $q^{d_i}+1$ roots in $\mathbb{F}_{q^{2d_i}}$. The number of LCD codes sought for is then $(q^{2d_i}-1)-(q^{d_i}+1)$. Note that the number of linear codes of length 2 over some $\mathbb{F}_Q$ admitting, along with their dual, a systematic form is $Q-1$, all of dimension 1. We are thus excluding the code $\langle[1,0]\rangle$, of dual $\langle[0,1]\rangle$.

In case of *reciprocal pairs* $(h'(x),h''(x))$, we need two codes of length 2 over $\mathbb{F}_Q$ that is, $C'=\langle[1,a']\rangle$, and $C''=\langle[1,a'']\rangle^{\perp}$, satisfying the condition that both $C'\cap C''^{\perp}$ and $C''\cap C'^{\perp}$ are trivial . This boils down to the condition $a'a''\neq -1$. So we have $q^{e_j}-1$ choices for a', and $a''\in H_j''\setminus\{0,-\frac{1}{a'}\}$. This gives $q^{e_j}-2$ choices for a''. Hence, in total we obtain $(q^{e_j}-1)(q^{e_j}-2)$ choices. □

We assume now that q is such that x^n+1, for n a power of 2, has only two irreducible factors over $\mathbb{F}_q$, say $h'(x)$ and $h''(x)$, and that they are reciprocals of each other. Thus, $x^n+1=h'(x)h''(x)$. For convenience, let $K'=\frac{\mathbb{F}_q[x]}{\langle h'(x)\rangle}$ and $K''=\frac{\mathbb{F}_q[x]}{\langle h''(x)\rangle}$. These two fields are both isomorphic to $\mathbb{F}_{q^{n/2}}$. By Theorems 5.1 and 5.3, this is the case if $q=4m\pm 1$, with m odd. For instance this happens if $q=3,5$ but not if $q=7$. The following will be used in our asymptotic study and it is a consequence of Proposition 7.1.

Corollary 7.2 *Let q be odd, and n be a power of 2. If x^n+1 factors as a product of two irreducible polynomials over $\mathbb{F}_q$, then the number of LCD double negacirculant codes over $\mathbb{F}_q$ of length $2n$ is $(q^{\frac{n}{2}}-1)(q^{\frac{n}{2}}-2)$.*

7.2 Index 3

Proposition 7.3 *Let q be odd, and n be coprime to q. Assume that the factorization of x^n+1 into irreducible polynomials over $\mathbb{F}_q$is of the form*

$$x^n+1=\alpha\prod_{i=1}^{s}g_i(x)\prod_{j=1}^{t}h_j(x)h_j^*(x),$$

with $\alpha \in \mathbb{F}_q^*$, and g_i a self-reciprocal polynomial of degree $2d_i$, the polynomial h_j is of degree e_j and $*$ denotes reciprocation. If n is odd, then let $g_1 = x+1$. The number of LCD index-3 negacirculant codes over $\mathbb{F}_q$ of length $3n$ and 1-generator $< [1,a,b] >$ is then

$$(q^2 - q + \eta(-1)) \prod_{i=2}^{s} [q^{2d_i} - (q^{d_i}+1)(q^{2d_i} - q^{d_i})] \prod_{j=1}^{t} (q^{4e_j} - q^{3e_j} + q^{e_j})$$

if n is odd, and

$$\prod_{i=1}^{s} [q^{2d_i} - (q^{d_i}+1)(q^{2d_i} - q^{d_i})] \prod_{j=1}^{t} (q^{4e_j} - q^{3e_j} + q^{e_j})$$

if n is even.

Proof. We use the Chinese Remainder Theorem (CRT) decomposition of $R(n, \mathbb{F}_q)$, again. Since we are counting LCD quasi-twisted codes of index 3 and generator matrix of the shape $< [1,a,b] >$, we are reduced to counting codes of length 3 and dimension 1 over some extension $\mathbb{F}_Q$ of $\mathbb{F}_q$ with certain properties.

In the case $Q = q$ we are reduced to counting LCD codes of parameters $[3,1]$ over $\mathbb{F}_q$. We can invoke Corollary 10.3 to obtain the factor $q^2 - q + \eta(-1)$ in the stated formula.

A factor $g_i(x)$ of degree $2d_i$ leads to counting *self-orthogonal hermitian codes* of length 3 over $\mathbb{F}_Q$, where $Q = q^{2d_i}$. Writing the generator matrix of such a code in the form $\langle [1,a,b] \rangle$, we must count the solutions of the equation $1 + aa^{q^{d_i}} + bb^{q^{d_i}} = 0$ (or equivalently, $a^{1+q^{d_i}} + b^{1+q^{d_i}} = -1$). Then by Corollary 10.1 the number N of the solutions of that equation is $(\sqrt{Q}+1)(Q-\sqrt{Q})$ where $Q = q^{2d_i}$ i.e. $N = (q^{d_i}+1)(q^{2d_i} - q^{d_i})$. By complementation the number of LCD codes of index 3 is then $Q^2 - N$.

In case of *reciprocal pairs* $(h'(x), h''(x))$, there are two dual constituent codes of length 3 over $\mathbb{F}_Q$ that is, $\langle [1,a',b'] \rangle$ and $\langle [1,a'',b''] \rangle^{\perp}$. By the condition for self-orthogonality we have to enumerate the cases when $[1,a',b'] \perp_E [1,a'',b'']$ which means counting the solutions of the equation $1 + a'a'' + b'b'' = 0$. Then, by Corollary 10.4 the number of the solutions of that equation is $(Q^3 - Q)$ where $Q = q^{e_j}$. Thus, by complementation, the number of corresponding LCD codes is $Q^4 - Q^3 + Q$. □

The following will be used in our asymptotic study and it is a consequence of Proposition 7.3.

Corollary 7.4 *Let q be odd, and n be a power of 2. If $x^n + 1$ factors as a product of two irreducible polynomials over $\mathbb{F}_q$, then the number of LCD three-negacirculant codes over $\mathbb{F}_q$ of length $3n$ is $q^{2n} - q^{\frac{3n}{2}} + q^{\frac{n}{2}}$.*

7.3 Index $t > 3$

For higher indices, we do not have exact enumeration formula as in Propositions 7.1 and 7.3. However, we have the following analogue of Corollaries 7.2 and 7.4, which is enough for asymptotic purposes in the next Section.

Proposition 7.5 *Let q be odd, and n be a power of 2. If x^n+1 factors as a product of two irreducible polynomials over $\mathbb{F}_q$, then the number of LCD t-negacirculant codes over $\mathbb{F}_q$ of length tn is $q^{n(t-1)} - \left(q^{\frac{n}{2}(2t-3)} - \eta((-1)^{t-1})q^{\frac{n}{2}(t-2)}\right)$.*

Proof. We use the Chinese Remainder Theorem (CRT) decomposition of $R(n,\mathbb{F}_q)$, as explained in §4. There are two LCD codes of length t over $\mathbb{F}_q$, $C' = \langle [1, a_1', a_2', ..., a_{t-1}'] \rangle$ and $C'' = \langle [1, a_1'', a_2'', ..., a_{t-1}'']^\perp \rangle$. For LCD condition we need to have both $C' \cap C''^\perp$ and $C'' \cap C'^\perp$ are trivial. This boils down to the condition:

$$a_1'a_1'' + a_2'a_2'' + ... + a_{t-1}'a_{t-1}'' \neq -1.$$

Now we need to count the solution of the above equation then by Corollary 10.4 the number N of the solutions of that equation is $Q^{2t-3} - \eta((-1)^{t-1})Q^{t-2}$ where $Q = q^{\frac{n}{2}}$. Thus by complementation, the number of corresponding LCD codes is $Q^{(2t-2)} - (Q^{2t-3} - \eta((-1)^{t-1})Q^{t-2})$. Hence,

$$N = q^{n(t-1)} - \left(q^{\frac{n}{2}(2t-3)} - \eta((-1)^{t-1})q^{\frac{n}{2}(t-2)}\right).$$

□

8 Asymptotics

In this section, we assume that x^n+1, for n a power of 2, has only two irreducible factors, say $h'(x)$ and $h''(x)$, and that they are reciprocal of each other. Thus, $x^n+1 = h'(x)h''(x)$. For convenience, let $K' = \frac{\mathbb{F}_q[x]}{\langle h'(x) \rangle}$ and $K'' = \frac{\mathbb{F}_q[x]}{\langle h''(x) \rangle}$. By part (b) of both Theorems 5.1 and 5.3 (with $A = 2$ and $A = 1$, respectively), we obtain such reciprocal pair of irreducible polynomials.

Lemma 8.1 *If $u \neq 0$ has Hamming weight $< n$, there are at most $(q^{\frac{(t-1)n}{2}} - 1)$ polynomials with x-expansion $a_1, a_2, ..., a_{t-1}$ such that $u \in \mathcal{C}_{a_1,a_2,...,a_{t-1}} =< [1, a_1, a_2, ..., a_{t-1}] >$, and $\mathcal{C}_{a_1,a_2,...,a_{t-1}}$ is LCD.*

Proof. Let $\mathcal{C}_{a_1,a_2,...,a_{t-1}} =< [1, a_1, a_2, ..., a_{t-1}] >$, and let $u = (b_1, b_2, ..., b_{t-1}, b_t)$, with $b_1, b_2, ..., b_{t-1}, b_t$ vectors of length n. The condition $u \in \mathcal{C}_{a_1,a_2,...,a_{t-1}}$ is equivalent to the equations,

$$b_{i+1}' = a_i'b_1' \quad \text{over} \quad K,' \quad \text{for all} \quad i = 1, ..., t-1$$

$$b_{i+1}'' = a_i''b_1'' \quad \text{over} \quad K'', \quad \text{for all} \quad i = 1, ..., t-1$$

where (b_1', b_1''), denotes the image by the CRT in $K' \times K''$ of the polynomial with x-expansion b_1. Then we have, since $\mathcal{C}_{a_1,a_2,...,a_{t-1}}$ is LCD, that

$$\langle[1, a_1', a_2', ..., a_{t-1}']\rangle \bigcap \langle[1, a_1'', a_2'', ..., a_{t-1}'']\rangle^{\perp} = \{0\},$$

which implies $a_1'a_1'' + a_2'a_2'' + ... + a_{t-1}'a_{t-1}'' \neq -1$.

For all $i = 1, 2, ..., t-1$:

(i) If $b_1' \neq 0$, then $a_i' = \frac{b_{i+1}'}{b_1'}$ has a unique solution.

(ii) If $b_1' = 0$, then
(a)If $b_{i+1}' \neq 0$, then we have no solution.
(b)If $b_{i+1}' = 0$, then a_i' is undetermined i.e. we have $q^{\frac{(t-1)n}{2}} - 1$ choices for a_i' for all i.

Similarly, we have the same solutions for a_i'' for all i. Therefore, for given $u = (b_1, b_2, ..., b_{t-1}, b_t)$, there are at most $q^{\frac{(t-1)n}{2}} - 1$ choices for a_i for all i. □

Recall the $q-$ary *entropy function* defined for $0 < y < \frac{q-1}{q}$ by

$$H_q(y) = y\log_q(q-1) - y\log_q(y) - (1-y)\log_q(1-y).$$

Theorem 8.2 *If q is odd integer, and n is a power of 2, then, for any fixed integer $t \geq 2$, there are infinite families of LCD index t negacirculant codes of relative distance δ satisfying $H_q(\delta) \geq \frac{t-1}{2t}$.*

Proof. The negacirculant codes of index t containing a vector of weight $d \sim t\delta n$ or less are by standard entropic estimates and Lemma 8.1 of the order $(q^{\frac{(t-1)n}{2}} - 1) \times q^{tnH_q(\delta)}$, up to subexponential terms. This number will be less than the total number of negacirculant codes of index t which is, by Proposition 7.5, of the order of $(q^{2(t-1)\frac{n}{2}}) = q^{(t-1)n}$. □

9 Conclusion

In this paper, we have studied LCD quasi-twisted codes of index t, where $t \geq 2$ emphasizing the aspects of enumeration for $t = 2$ and $t = 3$, and, for fixed t, asymptotic performance. It is an open problem to derive exact enumeration formulas for $t > 3$. It is also an open question to study the asymptotic performance of quasi-twisted codes with more than one generator in their module structure.

Acknowledgments: Patrick Solé thanks Prof. Wolfmann for helpful discussions. Güneri and Özkaya are supported by TÜBİTAK project 215E200, which is associated with the SECODE project in the scope of CHIST-ERA Program. Solé is also supported by the SECODE project.

References

[1] A. Alahmadi, H. Shoaib, C. Güneri, B. Özkaya, P. Solé, On self-dual double negacirculant codes, to appear in Disc. Appl. Math.

[2] W. Bosma , J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput., vol. 24, 235265, 1997.

[3] C. Carlet and S. Guilley, Complementary dual codes for counter-measures to side-channel attacks, Proceedings of the 4th ICMCTA Meeting, Palmela, Portugal, 2014.

[4] M. Grassl, Tables of linear Codes and Quantum Codes, `www.codetables.de`.

[5] K. Guenda, S. Jitman, T.A. Gulliver, Constructions of Good Entanglement-Assisted Quantum Error Correcting Codes, `arxiv 2016`.

[6] C. Güneri, B. Özkaya, P. Solé, Quasi-cyclic complementary dual codes, Finite Fields Appl., vol. 42, 67-80, 2016.

[7] M. Harada, W. Holzmann, H. Kharaghani, M. Khorvash, Extremal ternary self-dual codes constructed from negacirculant matrices, Graphs and Combinatorics, Vol. 23 Issue 4, 401-417 ,2007.

[8] R. Hill, P. Greenough, Optimal quasi-twisted codes, Proc. Intern. Worksop of Comb. Cod. and Crypt., Bulgaria (1992).

[9] W. C. Huffman and Vera Pless, Fundamentals of Error Correcting Codes, Cambridge University Press, (2003).

[10] Y. Jia, On quasi-twisted codes over finite fields, Finite Fields Appl., vol. 18, 237-257, 2012.

[11] R. Lidl, H. Niederreiter, *Finite Fields*, Addison-Wesley, Reading, MA (1983).

[12] S. Ling, P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, IEEE Trans. Inform. Theory, vol. 47, 2751-2760, 2001.

[13] J.L. Massey, Linear codes with complementary duals, Discrete Math., vol. 106-107, 337-342, 1992.

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

[15] J. Wolfmann, The number of solutions of certain diagonal equations over finite fields, J. of Number Theory, **42**, 247–257 (1992)

10 Appendix

10.1 Norm function

For all $x \in \mathbb{F}_{q^n}$, the norm of x over $\mathbb{F}_q$ is a map $Norm : \mathbb{F}_{q^n} \to \mathbb{F}_q$ defined by

$$Norm(x) = x^{(q^n-1)/(q-1)}.$$

Moreover, Norm is a multiplicative homomorphism which is surjective ([11, Theorem 2.28]). $Norm(0) = 0$, so it maps $\mathbb{F}^*_{q^n}$ onto $\mathbb{F}^*_q$, where each nonzero element in $\mathbb{F}^*_q$ has a preimage of size $(q^n - 1)/(q - 1)$ in $\mathbb{F}^*_{q^n}$.

Hence, for $n = 2$, we have $Norm(x) = x^{1+q}$ for all $x \in \mathbb{F}^*_{q^2}$. It is a $(q+1)$ to 1 map.

Corollary 10.1 *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 $(q + 1)(q^2 - q)$.*

Proof. We could invoke [15, Corollary 4], with $b^n = 1$, $\eta = (1)^{t/r+1} = 1$, but we prefer to give a self-contained argument. If $b^{1+q} = -1$, then $a = 0$. By the norm map, there are $(1+q)$ such $b \in \mathbb{F}^*_{q^2}$. Then, we have $q+1$ solutions in $\mathbb{F}^*_{q^2}$ of this form. If $b^{1+q} \neq -1$, then $a^{1+q} = -1 - b^{1+q}$ has $(q + 1)$ distinct solutions by the norm and $b^{1+q} \neq -1$ is true for $(q^2 - (q + 1))$ elements in $\mathbb{F}_{q^2}$. Therefore, we have $(q^2 - q - 1)(q + 1)$ solutions for this case. Hence, in total we have $(q + 1) + (q^2 - q - 1)(q + 1) = (q + 1)(q^2 - q)$ solutions in $\mathbb{F}^*_{q^2}$. □

10.2 Quadratic Forms

We quote Theorem 6.26 of [11]. Define the function v as $v(x) = -1$ if x is nonzero and $v(0) = q - 1$.

Theorem 10.2 *Let f denote a quadratic form in an even number n of variables over $\mathbb{F}_q$, with q odd. Denote by Δ the discriminant of f. Given $b \in \mathbb{F}_q$, the number of solutions in $(x_1, \ldots, x_n) \in \mathbb{F}^n_q$ of*

$$f(x_1, \ldots, x_n) = b$$

is

$$q^{n-1} + v(b)\eta((-1)^{\frac{n}{2}}\Delta)q^{\frac{n-2}{2}}.$$

From this general statement, we derive two results useful for our purposes.

Corollary 10.3 *If q is odd, then the number of solutions (x, y) in $\mathbb{F}_q$ of the equation $x^2 + y^2 = -1$ is*

$$q - \eta(-1).$$

Proof. Follows by the previous Theorem with $b = -1$, $n = 2$, $f = x^2 + y^2$, $\Delta = 1$. □

Recall that $\eta(-1) = 1$ if and only if q is a square or if q is not a square, but the characteristic of $\mathbb{F}_q$ is $\equiv 1 \pmod 4$.

Corollary 10.4 *The number of solutions of $x_1y_1 + x_2y_2 + ... + x_{t-1}y_{t-1} = -1$ is*

$$q^{2t-3} - \eta((-1)^{t-1})q^{t-2}.$$

Proof. Letting $A_1 = x_1 + y_1$, $A_1' = x_1 - y_1$, $A_2 = x_2 + y_2$, $A_2' = x_2 - y_2, ...,$ $A_{t-1} = x_{t-1} + y_{t-1}$, $A_{t-1}' = x_{t-1} - y_{t-1}$, the above equation can be cast into the following diagonal form.

$${A_1}^2 - {A_1'}^2 + {A_2}^2 - {A_2'}^2 + ... + {A_{t-1}}^2 - {A_{t-1}'}^2 = -4$$

Now we can apply the above Theorem with $n = 2(t-1)$, $b = -4$, $\Delta = 1$, to obtain the stated result. □