Self-dual 2-quasi Abelian Codes

Liren Lin

School of Optical Information and Energy Engineering School of Mathematics and Physics Wuhan Institute of Technology, Wuhan 430205, China

Yun Fan

School of Mathematics and Statistics Central China Normal University, Wuhan 430079, China

August 18, 2021

Abstract

A kind of self-dual quasi-abelian codes of index 2 over any finite field F is introduced. By counting the number of such codes and the number of the codes of this kind whose relative minimum weights are small, such codes are proved to be asymptotically good provided -1 is a square in F. Moreover, a kind of self-orthogonal quasi-abelian codes of index 2 are defined; and such codes always exist. In a way similar to that for self-dual quasi-abelian codes of index 2, it is proved that the kind of the self-orthogonal quasi-abelian codes of index 2 is asymptotically good.

Key words: Finite fields; quasi-abelian codes of index 2; self-dual codes; self-orthogonal codes; asymptotically good.

1 Introduction

Let F be a finite field with cardinality |F| = q which is a power of a prime, where |S| denotes the cardinality of any set S. Let n > 1 be an integer. Any nonempty subset $C \subseteq F^n$ is called a code of length n over F in coding theory. The Hamming weight w(a) for any word $a = (a_1, \dots, a_n) \in F^n$ is defined to be the number of the indexes i that $a_i \neq 0$. The Hamming distance d(a, b) = w(a - b) for $a, b \in F^n$. And $d(C) = \min\{d(c, c') \mid c \neq c' \in C\}$ is said to be the minimum distance of C, while $\Delta(C) = \frac{d(C)}{n}$ is called the relative minimum distance of C. The rate of the code C is defined as $\mathbb{R}(C) = \frac{\log_q |C|}{n}$. A code sequence C_1, C_2, \dots

Email address: yfan@mail.ccnu.edu.cn (Yun Fan);

is said to be asymptotically good if the length n_i of C_i goes to infinity and, for $i = 1, 2, \dots$, both the rate $R(C_i)$ and the relative minimum distance $\Delta(C_i)$ are positively bounded from below. A class of codes is said to be asymptotically good if there is an asymptotic good code sequence C_1, C_2, \dots in the class.

Let G be an abelian group of order n. By FG we denote the group algebra, i.e., an F-vector space with basis G and with multiplication induced by the group multiplication of G. Any ideal C of FG (i.e., any FG-submodule of the regular module FG) is called an abelian code of length n over F, or an FG-code for short. Any element $a = \sum_{x \in G} a_x x \in FG$ is identified with the word $(a_x)_{x \in G} \in F^n$. Hence the Hamming weight w(a) of a and the minimum Hamming weight w(C) of C are defined. The euclidean inner product of $a = (a_x)$ and $b = (b_x)$ is defined to be $\langle a, b \rangle = \sum_{x \in G} a_x b_x$. Then the self-orthogonal codes and self-dual codes are defined as usual, e.g., cf. [10].

Let $(FG)^2 := FG \times FG = \{(a, b) | a, b \in FG\}$, which is an FG-module. Any FG-submodule of $(FG)^2$ is called a *quasi-abelian code of index* 2 (2-quasi-abelian code for short), or a *quasi-FG code of index* 2 (2-quasi-FG code for short).

If G is a cyclic group of order n, then FG-codes and 2-quasi-FG codes are the usual cyclic codes and 2-quasi-cyclic codes, respectively. Note that there is a unique cyclic group of order n (upto isomorphism), but there may be many abelian groups of order n.

It is a long-standing open question whether or not the cyclic codes are asymptotically good, e.g., see [14]. But it has been known for a long time that the 2-quasi cyclic codes are asymptotically good, see [5, 6, 11]. Moreover, the selfdual quasi-cyclic codes with index going to infinity are asymptotically good, see [7, 13]; and the binary (i.e., q = 2) self-dual 2-quasi-cyclic codes are asymptotically good, see [15].

It is known that self-dual 2-quasi-cyclic codes exist if and only if -1 is a square in F, see [13]. In fact, the condition "-1 is a square in F" is also necessary and sufficient for the existence of the self-dual 2-quasi-FG codes for any abelian group G of order n, see Corollary 4.5 below.

The residue integer ring \mathbb{Z}_n modulo n is partitioned into q-cyclotomic cosets, see [10, §4.1]; and {0} is obvious a q-cyclotomic coset which we call the *trivial* q-cyclotomic coset. By $\mu_q(n)$ we denote the minimal size of the non-trivial q-cyclotomic cosets of \mathbb{Z}_n .

By assuming that Artin's primitive root conjecture holds, i.e., for a non-square q, there exist infinitely many odd primes p_1, p_2, \cdots satisfying:

•
$$\mu_q(p_i) = p_i - 1, i = 1, 2, \cdots$$

Alahmadi, Özdemir and Solé [1] proved that, if -1 is a square in F and q is a non-square, then there is an asymptotically good sequence of self-dual 2-quasicyclic codes C_1, C_2, \cdots with code length of C_i equal to $2p_i$ for $i = 1, 2, \cdots$. And they asked an open problem if the dependence on Artin's primitive root conjecture can be removed. In the dissertation [12], it has been proved by a probabilistic method that, if -1 is a square in F, and there are odd integers n_1, n_2, \cdots coprime to q satisfying the following two:

- the multiplicative order of q modulo n_i is odd for $i = 1, 2, \cdots$,
- $\lim_{i \to \infty} \frac{\log_q n_i}{\mu_q(n_i)} = 0;$

then for any abelian groups G_i of order n_i , $i = 1, 2, \dots$, there exists an asymptotically good sequence C_1, C_2, \dots with C_i being self-dual 2-quasi- FG_i codes for $i = 1, 2, \dots$.

It was known for a long time that there exist odd integers n_1, n_2, \cdots coprime to q satisfying that $\lim_{i\to\infty} \frac{\log_q n_i}{\mu_q(n_i)} = 0$, see [4, Lemma 2.6], [9, Lemma II.6] or Lemma 4.15 (and Remark 4.16) below. In fact, this existence is just enough to guarantee the asymptotic goodness of the self-orthogonal 2-quasi-abelian codes, and, to guarantee the asymptotic goodness of the self-dual 2-quasi-abelian codes once -1 is a square in F. More precisely, we have the following.

Theorem 1.1. Let n_1, n_2, \cdots be odd positive integers coprime to q satisfying that $\lim_{i \to \infty} \frac{\log_q n_i}{\mu_q(n_i)} = 0$. Let G_i be any abelian group of order n_i for $i = 1, 2, \cdots$.

(1) There exist self-orthogonal 2-quasi-FG_i codes C_i of dimension $n_i - 1$, $i = 1, 2, \dots$, such that the code sequence C_1, C_2, \dots is asymptotically good.

(2) If -1 is a square in F, then there exist self-dual 2-quasi-FG_i codes C_i , $i = 1, 2, \dots$, such that the code sequence C_1, C_2, \dots is asymptotically good.

We will prove the theorem by counting the number of the self-dual (or selforthogonal) 2-quasi-abelian codes we considered.

In Section 2 we describe fundamentals of abelian group algebras.

In Section 3, we investigate the structure of 2-quasi abelian codes, and introduce the 2-quasi-abelian codes of type I. If the abelian group G is cyclic, then the 2-quasi-FG codes of type I we defined are just the so-called double circulant codes in literature, e.g., see [1, 16].

Section 4 is devoted to the study on the self-dual 2-quasi-abelian codes of type I. First we show a counting formula of the number of such codes. Then we exhibit an estimation of the number of the self-dual 2-quasi-abelian codes of type I whose relative minimum weights are small. Finally, we prove the above Theorem 1.1(2), see Theorem 4.17.

As mentioned above, the existence of self-dual 2-quasi-abelian codes is conditional. In Section 5 we discuss a kind of self-orthogonal 2-quasi-FG codes of dimension n-1, where G is any abelian group of order n as before. The existence of such codes is unconditional. The study method for them is similar to that in Section 4. In Theorem 5.10 we complete the proof of Theorem 1.1(1).

2 Abelian codes

From now on we always assume that F is a finite field of cardinality |F| = q, n > 1 is an odd integer with gcd(n, q) = 1, and G is an abelian group of order n.

Let $FG = \{a = \sum_{x \in G} a_x x \mid a_x \in F\}$ be the group algebra of G over F. As mentioned in Section 1, any $\sum_{x \in G} a_x x \in FG$ is viewed as a sequence $(a_x)_{x \in G}$ of F indexed by G, and the Hamming weight, the euclidean inner product etc. are defined as usual.

The map $G \to G$, $x \mapsto x^{-1}$, is an automorphism of G of order 2 (since the order of G is odd). And the following map

$$FG \to FG, \ a \mapsto \overline{a}, \ \text{where } \overline{a} = \sum_{x \in G} a_x x^{-1} \text{ for } a = \sum_{x \in G} a_x x, \quad (2.1)$$

is an algebra automorphism of FG of order 2. Following [9], we call the automorphism Eq.(2.1) the "bar" map of FG. The following is clearly a linear form on FG:

$$\sigma: FG \to F, \quad \sum_{x \in G} a_x x \mapsto a_{1_G}, \tag{2.2}$$

where a_{1_G} is the coefficient of the identity element 1_G in the linear combination $a = \sum_{x \in G} a_x x$. Recall that the euclidean inner product $\langle a, b \rangle = \sum_{x \in G} a_x b_x$ for $a = \sum_{x \in G} a_x x$ and $b = \sum_{x \in G} b_x x$. Then the following holds ([9, Lemma II.4]):

$$\langle a,b\rangle = \sigma(a\overline{b}) = \sigma(\overline{a}b) = \sigma(b\overline{a}) = \sigma(\overline{b}a), \quad \forall \ a,b \in FG.$$

$$(2.3)$$

Since gcd(n,q) = 1, by Maschke's Theorem (see [2, pp. 116-117]), FG is a semisimple algebra, i.e., FG is the direct sum of simple ideals as follows:

$$FG = A_0 \oplus A_1 \oplus \cdots \oplus A_m.$$

Correspondingly, the identity element $1 = 1_G$ of the algebra has a unique decomposition

$$1 = e_0 + e_1 + \dots + e_m,$$

with $e_i \in A_i$, $0 \le i \le m$. It is easy to check that

$$e_i e_j = \begin{cases} e_i, & i = j; \\ 0, & i \neq j; \end{cases} \quad \forall \ 0 \le i, j \le m.$$

Such e_0, e_1, \dots, e_m are called "orthogonal" idempotents (here "orthogonal" is different from the orthogonality defined by inner product). An idempotent $0 \neq e = e^2$ is said to be primitive if it is impossible to write e = e' + e'' for two non-zero idempotents e' and e'' with e'e'' = 0. So we have:

- For $i = 0, 1, \dots, m$, $A_i = FGe_i$ is a simple ring with identity e_i , hence e_i is a primitive idempotent and A_i is a field extension over F. We can assume that $A_0 = FGe_0 = Fe_0$ is the trivial FG-module of dimension 1.
- $E = \{e_0 = \frac{1}{n} \sum_{x \in G} x, e_1, \cdots, e_m\}$ is the set of all primitive idempotents of FG, and $1 = \sum_{e \in E} e$.

• The "bar" map Eq. (2.1) permutes the primitive idempotents e_0, e_1, \cdots, e_m (equivalently, the "bar" map permutes the simple ideals A_0, A_1, \dots, A_m); obviously, $\overline{e}_0 = e_0$.

Then we can write the set E of all primitive idempotents as

$$E = \{e_0\} \cup \{e_1, \cdots, e_r\} \cup \{e_{r+1}, \overline{e}_{r+1}, \cdots, e_{r+s}, \overline{e}_{r+s}\},$$
(2.4)

where $\overline{e}_i = e_i$ for $i = 1, \dots, r$, $\overline{e}_{r+j} \neq e_{r+j}$ for $j = 1, \dots, s$ and 1 + r + 2s = m. For $j = 1, \dots, s$, the restriction of the "bar" map to A_{r+j} induces a map:

$$A_{r+j} = FGe_{r+j} \longrightarrow \overline{A}_{r+j} = FG\overline{e}_{r+j}, \quad a \longmapsto \overline{a},$$

which is an *F*-algebra isomorphism. It is easy to check that $A_{r+j} + \overline{A}_{r+j}$ are invariant by the automorphism "bar". So we set

$$\widehat{e}_{r+j} = e_{r+j} + \overline{e}_{r+j}, \quad \widehat{A}_{r+j} = FG\widehat{e}_{r+j} = A_{r+j} + \overline{A}_{r+j}, \quad j = 1, \cdots, s;
\widehat{E} = \{e_0, e_1, \cdots, e_r, \widehat{e}_{r+1}, \cdots, \widehat{e}_{r+s}\}.$$
(2.5)

Then

$$1 = \sum_{e \in \widehat{E}} e; \qquad \overline{e} = e, \ \forall \ e \in \widehat{E}; \qquad ee' = \begin{cases} e, \ e = e'; \\ 0, \ e \neq e'; \end{cases} \forall \ e, e' \in \widehat{E}; \tag{2.6}$$

and we have a decomposition of FG written in several ways:

$$FG = FGe_0 \bigoplus \left(\bigoplus_{i=1}^r FGe_i \right) \bigoplus \left(\bigoplus_{j=1}^s \left(FGe_{r+j} \bigoplus FG\overline{e}_{r+j} \right) \right)$$

$$= A_0 \bigoplus \left(\bigoplus_{i=1}^r A_i \right) \bigoplus \left(\bigoplus_{j=1}^s \left(A_{r+j} \bigoplus \overline{A}_{r+j} \right) \right)$$

$$= A_0 \bigoplus \left(\bigoplus_{i=1}^r A_i \right) \bigoplus \left(\bigoplus_{j=1}^s \widehat{A}_{r+j} \right)$$

$$= FGe_0 \bigoplus \left(\bigoplus_{i=1}^r FGe_i \right) \bigoplus \left(\bigoplus_{j=1}^s FG\widehat{e}_{r+j} \right).$$

(2.7)

For an ideal A of FG, we denote $A^{\flat} = \{a \mid a \in A, \overline{a} = a\}.$

Lemma 2.1. Keep the notation as above.

(1) $A_0^{\flat} = A_0 = FGe_0 = Fe_0.$

(2) $(FG)^{\flat}$ is a subalgebra of FG as follows:

$$(FG)^{\flat} = Fe_0 \bigoplus \left(\bigoplus_{i=1}^r A_i^{\flat} \right) \bigoplus \left(\bigoplus_{j=1}^s (\widehat{A}_{r+j})^{\flat} \right); \tag{2.8}$$

and $\dim(FG)^{\flat} = 1 + \frac{n-1}{2}$. (3) For $j = 1, \cdots, s$,

(3) For
$$j = 1, \dots,$$

$$(\widehat{A}_{r+j})^{\flat} = (A_{r+j} + \overline{A}_{r+j})^{\flat} = \{a + \overline{a} \mid a \in A_{r+j}\};$$

in particular, $\dim(\widehat{A}_{r+j})^{\flat} = \dim(A_{r+j} + \overline{A}_{r+j})^{\flat} = \dim A_{r+j} = \dim \overline{A}_{r+j}$.

(4) For $i = 1, \dots, r$, dim A_i is even, and dim $A_i^{\flat} = \frac{1}{2} \dim A_i$.

Proof. (1). Obvious.

(2). For any $a \in FG$, by Eq.(2.7), we assume $a = \sum_{e \in \widehat{E}} a_e$ with $a_e \in FGe$ for $e \in \widehat{E}$. Then $\overline{a} = \sum_{e \in \widehat{E}} \overline{a}_e$. For any $e \in \widehat{E}$, since $\overline{e} = e$ and $\overline{FGe} = FG\overline{e} = FGe$, we have $\overline{a}_e \in FGe$, then $a = \overline{a}$ iff $a_e = \overline{a}_e$ for $e \in \widehat{E}$, i.e., Eq.(2.8) holds.

For any $1 \neq x \in G$, $\overline{x} = x^{-1} \neq x$ (because the order *n* of *G* is odd). Thus, $a = \sum_{x \in G} a_x x \in (FG)^{\flat}$ if and only if $a_{x^{-1}} = a_x$ for all $1 \neq x \in G$. In other words, except for $1 \in G$, there are $\frac{n-1}{2}$ coefficients of $a \in (FG)^{\flat}$ which can be chosen from *F* freely. That is, dim $(FG)^{\flat} = 1 + \frac{n-1}{2}$.

(3). For $a \in A_{r+j}$ and $b \in \overline{A}_{r+j}$, since $\overline{a} \in \overline{A}_{r+j}$ and $\overline{b} \in A_{r+j}$, then

$$a+b \in (A_{r+j}+\overline{A}_{r+j})^{\flat} \iff \overline{a}+\overline{b}=a+b \iff \overline{a}=b \text{ and } \overline{b}=a.$$

(4). For $i = 1, \dots, r$, since A_i is a finite field and the "bar" map is an automorphism of it of order ≤ 2 , then we have

 $\dim A_i^{\flat} = \begin{cases} \dim A_i, & \text{``bar'' is the identity automorphism of } FGe_i; \\ \frac{1}{2} \dim A_i, & \text{otherwise.} \end{cases}$

In particular, $\frac{1}{2} \dim A_i \leq \dim A_i^{\flat}$. By (3),

$$\dim(\widehat{A}_{r+j})^{\flat} = \dim A_{r+j} = \frac{1}{2}\dim(A_{r+j} + \overline{A}_{r+j})$$

By Eq.(2.8),

$$1 + \frac{n-1}{2} = 1 + \sum_{i=1}^{r} \dim A_{i}^{\flat} + \sum_{j=1}^{s} \dim(\widehat{A}_{r+j})^{\flat}$$

$$\geq 1 + \frac{1}{2} \sum_{i=1}^{r} \dim A_{i} + \frac{1}{2} \sum_{j=1}^{s} (\dim A_{r+j} + \dim \overline{A}_{r+j}) = 1 + \frac{n-1}{2}.$$

So, for $i = 1, \dots, r$, every " $\frac{1}{2} \dim A_i \leq \dim A_i^{\flat}$ " has to be an equality; that is, $\frac{1}{2} \dim A_i = \dim A_i^{\flat}$, for $i = 1, \dots, r$.

Set

$$\widehat{E}^{\dagger} = \widehat{E} - \{e_0\} = \{e_1, \cdots, e_r, \, \widehat{e}_{r+1}, \cdots, \widehat{e}_{r+s}\}.$$
(2.9)

By Lemma 2.1, for any $e \in \hat{E}^{\dagger}$, dim FGe is even. Denote

$$n_{e} = \frac{1}{2} \dim FGe, \ e \in \widehat{E}^{\dagger}; n_{i} = n_{e_{i}}, \ i = 1, \cdots, r; \ n_{r+j} = n_{\widehat{e}_{r+j}}, \ j = 1, \cdots, s;$$

then

$$n = 1 + 2\sum_{e \in \widehat{E}^{\dagger}} n_e = 1 + 2\left(\sum_{i=1}^r n_i + \sum_{j=1}^s n_{r+j}\right).$$
(2.10)

Remark 2.2. For any ideal $A \leq FG$, there is a unique subset $E_A \subseteq E$ such that

$$A = \bigoplus_{e \in E_A} FGe = FGe_A$$
, where $e_A = \sum_{e \in E_A} e$.

So any ideal A is a ring with identity e_A and with the unit group

$$A^{\times} = \prod_{e \in E_A} (FGe)^{\times},$$

where $(FGe)^{\times} = FGe - \{0\}$ since FGe is a finite field. Thus, for $a \in A$, FGa = A if and only if $a \in A^{\times}$, if and only if $ae \neq 0$ for all $e \in E_A$.

In particular, the multiplicative unit group of FG is as follows:

$$(FG)^{\times} = F^{\times}e_0 \times \left(\underset{i=1}{\overset{r}{\times}} A_i^{\times}\right) \times \left(\underset{j=1}{\overset{s}{\times}} \left(A_{r+j}^{\times} \times \overline{A}_{r+j}^{\times}\right)\right).$$

3 2-quasi-abelian codes

Keep the notation in Section 2.

The outer direct sum $(FG)^2 := FG \times FG = \{(a, b) \mid a, b \in FG\}$ is an FGmodule. Any FG-submodule C of $(FG)^2$, denoted by $C \leq (FG)^2$, is said to be a 2-quasi-abelian code, or a 2-quasi-FG code. Denote by w(a, b) the Hamming weight of $(a, b) \in (FG)^2$, and by w(C) the minimum Hamming weight of C. Note that C is a linear code of length 2n. The relative minimum distance $\Delta(C) = \frac{w(C)}{2n}$, and the rate $R(C) = \frac{\dim C}{2n}$.

For any $(a, b) \in (FG)^2$, by Eq.(2.6) we have

$$(a,b) = 1 \cdot (a,b) = e_0(a,b) + e_1(a,b) + \dots + e_r(a,b) + \widehat{e}_{r+1}(a,b) + \dots + \widehat{e}_{r+s}(a,b).$$

Thus for any $C \leq (FG)^2$,

$$C = e_0 C \oplus e_1 C \oplus \dots \oplus e_r C \oplus \widehat{e}_{r+1} C \oplus \dots \oplus \widehat{e}_{r+s} C.$$
(3.1)

Lemma 3.1. (1) As FG-modules we have a direct sum decomposition:

$$(FG)^2 = (Fe_0)^2 \oplus (FGe_1)^2 \oplus \dots \oplus (FGe_r)^2 \oplus (FG\widehat{e}_{r+1})^2 \oplus \dots \oplus (FG\widehat{e}_{r+s})^2.$$

(2) For any $e \neq e' \in \widehat{E} = \{e_0, e_1, \cdots, e_r, \widehat{e}_{r+1}, \cdots, \widehat{e}_{r+s}\}$, the submodules $(FGe)^2$ and $(FGe')^2$ of $(FG)^2$ are orthogonal, i.e., $\langle (FGe)^2, (FGe')^2 \rangle = 0$.

(3) For any $e \in \widehat{E}$, the orthogonal submodule $((FGe)^2)^{\perp} = \bigoplus_{e' \in \widehat{E} - \{e\}} (FGe')^2$.

Proof. (1). This is checked by Eq.(3.1) and the following: for $e \in \widehat{E}$,

$$e(FG)^{2} = \{(ea, eb) \mid a, b \in FG\} = FGe \times FGe = (FGe)^{2}.$$

(2). Note that $\overline{e'} = e'$ and ee' = 0. For $(ae, be) \in (FGe)^2$ and $(a'e', b'e') \in (FGe')^2$, where $a, b, a', b' \in FG$, by Eq.(2.3) we have

$$\langle (ae, be), (a'e', b'e') \rangle = \sigma(ae \overline{a'e'}) + \sigma(be \overline{b'e'})$$

= $\sigma(aee^{\overline{a'}} \overline{a'}) + \sigma(bee^{\overline{b'}} \overline{b'}) = \sigma(aee^{\overline{a'}}) + \sigma(bee^{\overline{b'}}) = 0$

(3). This follows from (2) immediately.

Note that, for $e \in \widehat{E}$, FGe is an algebra (with identity e) and $(FGe)^2$ is an FGe-module, and Lemma 3.1 implies that the restriction to $(FGe)^2$ of the inner product of $(FG)^2$ is non-degenerate.

For the decomposition of $C \leq (FG)^2$ in Eq.(3.1), the component eC for $e \in \widehat{E}$ is an FGe-submodule of $(FGe)^2$.

Corollary 3.2. Let $C \leq (FG)^2$ be as in Eq.(3.1). Then the orthogonal submodule C^{\perp} has a direct decomposition:

$$C^{\perp} = (e_0 C)^{\perp_0} \oplus (e_1 C)^{\perp_1} \oplus \dots \oplus (e_r C)^{\perp_r} \oplus (\widehat{e}_{r+1} C)^{\perp_{r+1}} \oplus \dots \oplus (\widehat{e}_{r+s} C)^{\perp_{r+s}},$$

where $(e_i C)^{\perp_i}$ for $i = 0, 1, \cdots, r$ denotes the orthogonal FGe_i-submodule in $(FGe_i)^2$, and $(\hat{e}_{r+j}C)^{\perp_{r+j}}$ for $j = 1, \cdots, s$ denotes the orthogonal $FG\hat{e}_{r+j}$ -submodule in $(FG\hat{e}_{r+j})^2$.

Proof. By Lemma 3.1(2), the right hand side of the wanted equality is contained in the left hand side. By computing the dimensions of the two sides of the wanted equality, we obtain that the wanted equality does hold.

Corollary 3.3. Let $C \leq (FG)^2$ be as above. Then C is self-orthogonal if and only if eC is self-orthogonal in $(FGe)^2$ for any $e \in \widehat{E}$.

In general, a 2-quasi-FG code may not be generated by one element. For our purpose, in the following we consider the 2-quasi-FG codes generated by one element. For any $(a, b) \in (FG)^2$, let

$$C_{a,b} = \{ (ua, ub) \, | \, u \in FG \}$$
(3.2)

be the FG-submodule of $(FG)^2$ generated by (a, b).

Lemma 3.4. As FG-modules, $C_{a,b} \cong FG/\operatorname{Ann}_{FG}(a,b)$, where $\operatorname{Ann}_{FG}(a,b) = \{u \mid u \in FG, ua = 0 = ub\}$ denotes the annihilator of $\{a,b\}$ in FG. In particular, dim $C_{a,b} \leq n$.

Proof. By the construction of $C_{a,b}$, there is a surjective FG-module homomorphism from FG to $C_{a,b}$, mapping u to (ua, ub) for any $u \in FG$. It is easy to check that the kernel is just $\operatorname{Ann}_{FG}(a, b)$. Then we have $FG/\operatorname{Ann}_{FG}(a, b) \cong C_{a,b}$.

If one of a and b is invertible, then $\operatorname{Ann}_{FG}(a,b) = 0$, hence dim $C_{a,b} = n$ obviously. Without loss of generality, we assume that $a \in (FG)^{\times}$ is a unit, then $(a,b) = a(1,a^{-1}b) \in C_{1,a^{-1}b}$ and $C_{a,b} = C_{1,a^{-1}b}$.

Definition 3.5. For any $b \in FG$, we call $C_{1,b} = \{(u, ub) | u \in FG\} \leq (FG)^2$ a 2-quasi-FG code of type I, or a 2-quasi-abelian code of type I.

Remark 3.6. List the elements of G as

$$G = \{x_0 = 1, x_1, \cdots, x_{n-1}\}.$$
(3.3)

Any $a = \sum_{j=0}^{n-1} a_j x_j \in FG$ corresponds to a sequence $(a_0, a_1, \dots, a_{n-1}) \in F^n$. Thus, as a linear code, $C_{1,b}$ is an *F*-subspace of $(FG)^2$ with basis as follows:

$$(1,b), (x_1,x_1b), \cdots, (x_{n-1},x_{n-1}b).$$
 (3.4)

Of course, 1 corresponds to the sequence $(1, 0, \dots, 0) \in F^n$. Set $b = \sum_{j=0}^{n-1} b_j x_j$, i.e., b corresponds to the sequence $(b_0, b_1, \dots, b_{n-1}) \in F^n$. Any $x_i \in G$ provides a Cayley permutation ρ_i :

$$x_i \longmapsto \rho_i = \begin{pmatrix} 0 & 1 & \cdots & j & \cdots & n-1 \\ 0' & 1' & \cdots & j' & \cdots & (n-1)' \end{pmatrix},$$
(3.5)

where $x_{j'} = x_i x_j$ for $j = 0, 1, \dots, n-1$; in particular, 0' = i because $x_i x_0 = x_i$. The map $x_i \mapsto \rho_i$ is said to be the *Cayley representation* of the group *G*, e.g., see [2, pp. 28]. Clearly, ρ_0 is the identity permutation. Then

$$x_i b = \sum_{j=0}^{n-1} b_j x_i x_j = \sum_{j=0}^{n-1} b_j x_{j'};$$

i.e., $x_i b$ corresponds to the sequence obtained by ρ_i -permuting on the sequence $(b_0, b_1, \dots, b_{n-1})$. Let B be the $n \times n$ matrix whose *i*'th row is obtained by ρ_i -permuting on $(b_0, b_1, \dots, b_{n-1}) \in F^n$. By I we denote the identity matrix.

Lemma 3.7. Keep the notation in Remark 3.6. Then a linear code C of length 2n and dimension n has a generating matrix (I B) if and only if $C = C_{1,b}$.

Proof. Assume that $C = C_{1,b}$. By the above analysis, (x_i, x_ib) in Eq.(3.4) corresponds to the *i*'th row of the matrix (I B). So C is a [2n, n] linear code having (I B) as a generating matrix.

Conversely, assume that C is a [2n, n] linear code having $(I \ B)$ as a generating matrix. The *i*'th row of the matrix $(I \ B)$ corresponds to the element $(x_i, x_i b) \in (FG)^2$. Thus C can be regarded as an F-subspace of $(FG)^2$ with basis Eq.(3.4); hence $C = C_{1,b}$.

Example 3.8. A typical example is to take $G = \{1, x, x^2, \dots, x^{n-1}\}$ to be a cyclic group of order n. Then ρ_1 is just the cyclic permutation, $\rho_i = \rho_1^i$, and B is just the usual circulant matrix with first row $(b_0, b_1, \dots, b_{n-1})$. The code $C_{1,b}$ with generating matrix (I B) is said to be a *double circulant code* in literature, e.g., see [1, 16].

We consider self-dual 2-quasi-FG codes of type I.

Lemma 3.9. For any $C_{a,b} \leq (FG)^2$ as in Eq.(3.2), the following three are equivalent to each other:

(1) $C_{a,b}$ is self-orthogonal;

- (2) $a\overline{a} + b\overline{b} = 0;$
- (3) the following two hold:
 - (3.i) $ae_i\overline{ae_i} + be_i\overline{be_i} = 0$, for $i = 0, 1, \cdots, r$; (3.ii) $a\widehat{e}_{r+j}\overline{a\widehat{e}_{r+j}} + b\widehat{e}_{r+j}\overline{b\widehat{e}_{r+j}} = 0$, for $j = 1, \cdots, s$.

Proof. (2) \Rightarrow (1) For any elements $u(a,b), u'(a,b) \in C_{(a,b)}$, the inner product

$$\left\langle u(a,b), u'(a,b) \right\rangle = \sigma(ua \cdot \overline{u'a}) + \sigma(ub \cdot \overline{u'b}) = \sigma\left(u\overline{u'}(a\overline{a} + b\overline{b})\right) = 0$$

(1) \Rightarrow (2). The proof is similar to [9, Lemma II.3]. Suppose $a\bar{a} + b\bar{b} = \sum_{x \in G} a_x x$ with a coefficient $a_{x_0} \neq 0$. Then the inner product of $(a, b) \in C_{a,b}$ and $x_0(a, b) \in C_{a,b}$ is

$$\langle (a,b), x_0(a,b) \rangle = \sigma \left(\overline{x_0}(a\overline{a} + b\overline{b}) \right) = \sigma \left(x_0^{-1} \cdot \sum_{x \in G} a_x x \right) = a_{x_0} \neq 0,$$

which contradicts to (1).

 $(2) \Leftrightarrow (3)$. Since

$$a = ae_0 + ae_1 + \dots + ae_r + a\hat{e}_{r+1} + \dots + a\hat{e}_{r+s},$$

$$b = be_0 + be_1 + \dots + be_r + b\hat{e}_{r+1} + \dots + b\hat{e}_{r+s},$$

then

$$\begin{aligned} a\overline{a} + b\overline{b} &= (ae_0\overline{ae_0} + be_0\overline{be_0}) + (ae_1\overline{ae_1} + be_1\overline{be_1}) + \dots + (ae_r\overline{ae_r} + be_r\overline{be_r}) \\ &+ (a\widehat{e}_{r+1}\overline{a\widehat{e}_{r+1}} + b\widehat{e}_{r+1}\overline{b\widehat{e}_{r+1}}) + \dots + (a\widehat{e}_{r+s}\overline{a\widehat{e}_{r+s}} + b\widehat{e}_{r+s}\overline{b\widehat{e}_{r+s}}). \end{aligned}$$

Hence, (2) and (3) are equivalent.

Corollary 3.10. Let $C_{1,b}$ be a 2-quasi-FG code of type I. The following are equivalent to each other:

- (1) $C_{1,b}$ is self-dual;
- (2) $b\overline{b} = -1;$
- (3) the following two hold:
 - (3.i) $be_i \overline{be_i} = -e_i$, for $i = 0, 1, \cdots, r$; (3.ii) $b\widehat{e}_{r+j}\overline{b\widehat{e}_{r+j}} = -\widehat{e}_{r+j}$, for $j = 1, \cdots, s$.

Proof. Since dim $C_{1,b} = n$ (Lemma 3.7), it follows from Lemma 3.9.

4 Self-dual 2-quasi-abelian codes of Type I

Keep the notation in Section 3. In the following we always denote

$$\mathcal{D} = \{ C_{1,b} \mid b \in FG, \ b\overline{b} = -1 \}, \tag{4.1}$$

which is the set of all self-dual 2-quasi-FG codes of type I, see Corollary 3.10. We always assume that δ is a real number such that $0 \leq \delta \leq 1 - q^{-1}$, and set

$$\mathcal{D}^{\leq \delta} = \left\{ C_{1,b} \, \big| \, C_{1,b} \in \mathcal{D}, \, \Delta(C_{1,b}) = \frac{\mathrm{w}(C_{1,b})}{2n} \leq \delta \right\}.$$
(4.2)

4.1 Counting $|\mathcal{D}|$

Theorem 4.1. Let the notation be as in Eq.(2.5), Eq.(2.9) and Eq.(2.10). Then

$$|\mathcal{D}| = \begin{cases} \prod_{i=1}^{r} (q^{n_i} + 1) \prod_{j=1}^{s} (q^{n_{r+j}} - 1), & q \text{ is even;} \\ 2 \prod_{i=1}^{r} (q^{n_i} + 1) \prod_{j=1}^{s} (q^{n_{r+j}} - 1), & q \equiv 1 \pmod{4}; \\ 0, & q \equiv -1 \pmod{4}. \end{cases}$$

Proof. The cardinality $|\mathcal{D}|$ is equal to the number of the choices of $b \in FG$ such that $b\overline{b} = -1$. Let

$$\begin{aligned} \mathfrak{T}_{i} &= \{\beta \mid \beta \in FGe_{i}, \ \beta\beta = -e_{i}\}, \quad i = 0, 1, \cdots, r;\\ \mathfrak{T}_{r+j} &= \{\beta \mid \beta \in FG\widehat{e}_{r+j}, \ \beta\overline{\beta} = -\widehat{e}_{r+j}\}, \quad j = 1, \cdots, s. \end{aligned}$$
(4.3)

By Corollary 3.10,

$$\left|\mathcal{D}\right| = \left|\mathcal{T}_{0}\right| \cdot \prod_{i=1}^{r} \left|\mathcal{T}_{i}\right| \cdot \prod_{j=1}^{s} \left|\mathcal{T}_{r+j}\right|$$

Thus the proof of the theorem will be completed by the following Lemma 4.2, Lemma 4.3 and Lemma 4.4.

Lemma 4.2. Let the notation be as in Eq.(4.3). Then

$$|\mathcal{T}_0| = \begin{cases} 1, & q \text{ is even}; \\ 2, & q \equiv 1 \pmod{4}; \\ 0, & q \equiv -1 \pmod{4} \end{cases}$$

Proof. Since $FGe_0 = Fe_0$ and $\overline{\beta} = \beta$ for all $\beta \in Fe_0$, $|\mathcal{T}_0|$ is equal to the number of the solutions in F of the equation $X^2 = -1$. Note that the unit group F^{\times} is a cyclic group of order q - 1.

If q is even, then -1 = 1, q - 1 is odd, hence $|\mathcal{T}_0| = 1$.

Assume that q is odd. Then -1 is the unique element of order 2 in F^{\times} . Hence, $X^2 = -1$ has solutions if and only if F^{\times} has an element of order 4, i.e., 4 | q - 1. Thus, if 4 | q - 1 then $|\mathcal{T}_0| = 2$; otherwise $|\mathcal{T}_0| = 0$.

Lemma 4.3. Keep the notation in Eq.(4.3). If $1 \le i \le r$ then $|\mathfrak{T}_i| = q^{n_i} + 1$.

Proof. Since FGe_i is a finite field with $|FGe_i| = q^{2n_i}$, and e_i is the identity element of the field, then the unit group $(FGe_i)^{\times}$ is cyclic, and $|(FGe_i)^{\times}| = q^{2n_i} - 1 = (q^{n_i} + 1)(q^{n_i} - 1)$. Note that $\overline{e}_i = e_i$. Hence by Lemma 2.1(4), the "bar" map is a Galois automorphism of FGe_i of order 2. So, for any $\beta \in FGe_i$, $\overline{\beta} = \beta^{q^{n_i}}$. Then the equation $\beta\overline{\beta} = -e_i$ turns into:

$$\beta^{q^{n_i}+1} = -e_i. (4.4)$$

Case 1: q is even. The equation $X^{q^{n_i}+1} = 1$ has exactly $q^{n_i} + 1$ roots in the finite field FGe_i . The lemma holds.

Case 2: q is odd. Then $2 | (q^{n_i} - 1)$, the equation $X^{2(q^{n_i}+1)} = 1$ has exactly $2(q^{n_i} + 1)$ roots. Hence, $X^{q^{n_i}+1} = -1$ has exactly $q^{n_i} + 1$ roots in the finite field FGe_i .

Lemma 4.4. Keep the notation in Eq.(4.3). If $1 \le j \le s$ then $|\mathcal{T}_{r+j}| = q^{n_{r+j}} - 1$.

Proof. Write $\beta = \beta' + \beta''$ with $\beta' \in FGe_{r+j}$ and $\beta'' \in FG\overline{e}_{r+j}$. Then $\beta\overline{\beta} = -\widehat{e}_{r+j}$ for $\beta \in \mathfrak{T}_{r+j}$ is rewritten as

$$-e_{r+j} - \overline{e}_{r+j} = (\beta' + \beta'')\overline{(\beta' + \beta'')} = (\beta' + \beta'')\overline{(\beta' + \beta'')} = \beta'\overline{\beta''} + \overline{\beta'}\beta'',$$

which is equivalent to

$$\beta'\overline{\beta''} = -e_{r+j}$$
 (equivalently, $\overline{\beta'}\beta'' = -\overline{e}_{r+j}$). (4.5)

Take any $\beta' \in (FGe_{r+j})^{\times}$ there is a unique element $\gamma \in (FGe_{r+j})^{\times}$ such that $\beta'\gamma = -e_{r+j}$; and, there is a unique $\beta'' \in (FG\overline{e}_{r+j})^{\times}$ such that $\beta'' = \gamma$. Note that $|(FGe_{r+j})^{\times}| = q^{n_{r+j}} - 1$. In conclusion, there are exactly $q^{n_{r+j}} - 1$ elements $\beta = \beta' + \beta'' \in FG(e_{r+j} + \overline{e}_{r+j})$ such that $\beta\overline{\beta} = -e_{r+j} - \overline{e}_{r+j} = -\widehat{e}_{r+j}$.

Corollary 4.5. The following four are equivalent to each other:

- (1) The self-dual 2-quasi abelian codes exist.
- (2) The self-dual 2-quasi abelian codes of Type I exist.
- (3) -1 is a square element of F.
- (4) Either q is even, or 4 | q 1.

Proof. (3) \Leftrightarrow (4). Both (3) and (4) are equivalent to that the equation $X^2 = -1$ has solutions in F, see the proof of Lemma 4.2.

(1) \Rightarrow (4). Let $C \leq (FG)^2$ such that $C = C^{\perp}$. By Corollary 3.2,

$$e_0 C \oplus e_1 C \oplus \cdots \oplus e_r C \oplus \widehat{e}_{r+1} C \oplus \cdots \oplus \widehat{e}_{r+s} C = C = C^{\perp}$$
$$= (e_0 C)^{\perp_0} \oplus (e_1 C)^{\perp_1} \oplus \cdots \oplus (e_r C)^{\perp_r} \oplus (\widehat{e}_{r+1} C)^{\perp_{r+1}} \oplus \cdots \oplus (\widehat{e}_{r+s} C)^{\perp_{r+s}}.$$

In particular, $e_0 C = (e_0 C)^{\perp_0}$, which implies that there is a $\beta \in Fe_0$ such that $\beta \overline{\beta} = -e_0$; so $|\mathcal{T}_0| > 0$. By Lemma 4.2, (4) holds.

(4)
$$\Rightarrow$$
(2). By Theorem 4.1, $|\mathcal{D}| > 0$.
(2) \Rightarrow (1). Trivial.

4.2 Estimating $|\mathcal{D}^{\leq \delta}|$

Before going on, we list two lemmas which will be cited later. The following

$$h_q(\delta) = \delta \log_q(q-1) - \delta \log_q \delta - (1-\delta) \log_q(1-\delta), \quad \delta \in [0, 1-q^{-1}],$$
(4.6)

is the so-called *q*-entropy function, which is increasing and concave on the interval $[0, 1 - q^{-1}]$ with $h_q(0) = 0$ and $h_q(1 - q^{-1}) = 1$. For any subset $S \subseteq (FG)^2$, we denote $S^{\leq \delta} = \{(a, b) \mid (a, b) \in S, \frac{w(a, b)}{2n} \leq \delta\}.$

Lemma 4.6. If $A \leq FG$, then $A \times A \leq (FG)^2$ and $|(A \times A)^{\leq \delta}| \leq q^{h_q(\delta) \cdot \dim(A \times A)}$.

Proof. It follows from [8, Corollary 3.4 and Corollary 3.5].

Lemma 4.7. Let $q \ge 2, k_1, \dots, k_m$ be integers. If $k_i \ge \log_q m$ for $i = 1, \dots, m$, then

- (1) $(q^{k_1} 1) \cdots (q^{k_m} 1) \ge q^{k_1 + \dots + k_m 2};$
- (2) $(q^{k_1}+1)\cdots(q^{k_m}+1) \le q^{k_1+\cdots+k_m+2}$.

Proof. (1). Please see [9, Lemma 2.9].

(2). Assume that $k_1 \leq \cdots \leq k_m$. Since $\log_q m \leq k_1, \frac{m}{q^{k_1}} \leq 1$.

$$\frac{(q^{k_1}+1)\cdots(q^{k_m}+1)}{(q^{k_1})\cdots(q^{k_m})} = \left(1+\frac{1}{q^{k_1}}\right)\cdots\left(1+\frac{1}{q^{k_m}}\right) \le \left(1+\frac{1}{q^{k_1}}\right)^m \le \left(1+\frac{1}{q^{k_1}}\right)^{q^{k_1}}.$$

Since the sequence $(1 + \frac{1}{k})^k$ for $k = 1, 2, \cdots$ is increasing and bounded above by 3 and $3 < q^2$, we obtain the wanted inequality.

Recall that $\widehat{E} = \{e_0, e_1, \cdots, e_r, \widehat{e}_{r+1}, \cdots, \widehat{e}_{r+s}\}, \ \widehat{E}^{\dagger} = \widehat{E} - \{e_0\}, \text{ and for } e \in \widehat{E}^{\dagger}, \ n_e = \frac{1}{2} \dim FGe, \text{ see Eq.}(2.5), \text{ Eq.}(2.9) \text{ and Eq.}(2.10).$

For any $a \in FG$, we denote:

$$\widehat{E}_{a} = \left\{ e \mid e \in \widehat{E}, \ ea \neq 0 \right\}, \quad \widehat{E}_{a}^{\dagger} = \left\{ e \mid e \in \widehat{E}^{\dagger}, \ ea \neq 0 \right\};$$

$$L_{a} := \bigoplus_{e \in \widehat{E}_{a}^{\dagger}} FGe \leq FG, \quad \ell_{a} := \sum_{e \in \widehat{E}_{a}^{\dagger}} n_{e} \quad (\text{hence } \dim L_{a} = 2\ell_{a}).$$
(4.7)

Lemma 4.8. For $(a, d) \in (FG)^2$, let

$$\mathcal{D}_{(a,d)} = \{ C_{1,b} \,|\, C_{1,b} \in \mathcal{D}, (a,d) \in C_{1,b} \}.$$

If $\mathcal{D}_{(a,d)} \neq \emptyset$, then $\widehat{E}_a = \widehat{E}_d$ and

$$\left|\mathcal{D}_{(a,d)}\right| \le 2\prod_{e\in\widehat{E}^{\dagger}-\widehat{E}_{a}^{\dagger}}(q^{n_{e}}+1).$$

Proof. Assume that $C_{1,b} \in \mathcal{D}_{(a,d)}$, then $C_{(1,b)} \in \mathcal{D}$, i.e., $b\overline{b} = -1$ and (a,d) = u(1,b) for some $u \in FG$. Then a = u and d = ub = ab. Assume $b = \sum_{e \in \widehat{E}} \beta_e$ with $\beta_e \in FGe$. Then, for $e \in \widehat{E}$,

$$\beta_e \overline{\beta}_e = -e, \qquad ed = ea\beta_e. \tag{4.8}$$

Hence, $\beta_e \in (FGe)^{\times}$. So $ea \neq 0$ iff $ed = ea\beta_e \neq 0$. That is, $\widehat{E}_a = \widehat{E}_d$.

Note that there already exist such β_e 's satisfying Eq.(4.8) because $\mathcal{D}_{(a,d)} \neq \emptyset$. What we are computing is how many choices of them.

Case 1: $e = e_0$. We have seen from Lemma 4.2 that there are at most two choices of β_{e_0} .

Case 2: $e \in \widehat{E}_a^{\dagger}$. There are two subcases.

Subcase 2.1: $e = e_i$ for some $1 \le i \le r$. Then FGe_i is a field; and $ae_i \ne 0 \ne de_i$. So, $de_i = ae_i\beta_{e_i}$ implies that $\beta_{e_i} = (ae_i)^{-1}(de_i)$ is uniquely determined.

Subcase 2.2: $e = \hat{e}_{r+j} = e_{r+j} + \overline{e}_{r+j}$ for some $1 \leq j \leq s$. Then $\beta_{\hat{e}_{r+j}} = \beta' + \beta''$ with $\beta' \in (FGe_{r+j})^{\times}$ and $\beta'' \in (FG\overline{e}_{r+j})^{\times}$ such that $\beta'\overline{\beta''} = -e_{r+j}$, see Eq.(4.5). Since $\hat{e}_{r+j}a \neq 0$, $e_{r+j}a \neq 0$ or $\overline{e}_{r+j}a \neq 0$ (or both). Without loss of generality, assume that $e_{r+j}a \neq 0$. In FGe_{r+j} , by Eq.(4.8), $e_{r+j}d = e_{r+j}a\beta'$, hence $\beta' = (e_{r+j}a)^{-1}(e_{r+j}d)$ is uniquely determined. Consequently, $\beta'' = -\beta'^{-1}$ is also uniquely determined.

Combining the two subcases, we conclude that, if $e \in \widehat{E}_a^{\dagger}$, there is a unique $\beta_e \in FGe$ satisfying Eq.(4.8).

Case 3: $e \in \hat{E}^{\dagger} - \hat{E}_a^{\dagger}$. Then ae = 0 = de, hence the second equality of Eq.(4.8) always holds. Thus, there are $q^{n_e} + 1$ choices for β_e (see Lemma 4.3), or $q^{n_e} - 1$ choices for β_e (see Lemma 4.4).

Summarizing the above three cases, we get the inequalities of the lemma. \Box

Corollary 4.9. Keep the notation as above.

$$|\mathcal{D}_{(a,d)}| \le q^{\frac{n-1}{2}-\ell_a+3}.$$

Proof. By Eq.(2.10), $\frac{n-1}{2} = \sum_{e \in \widehat{E}^{\dagger}} n_e = \sum_{e \in \widehat{E}^{\dagger}_a} n_e + \sum_{e \in \widehat{E}^{\dagger}_a} -\widehat{E}^{\dagger}_a n_e$. By the above lemma and Lemma 4.7(2), we have: $|\mathcal{D}_{(a,d)}| \leq 2 \prod_{e \in \widehat{E}^{\dagger} - \widehat{E}^{\dagger}_a} (q^{n_e} + 1) \leq 2 \cdot q^2 \cdot q^{\sum_{e \in \widehat{E}^{\dagger} - \widehat{E}^{\dagger}_a} n_e} \leq q^3 \cdot q^{\frac{n-1}{2} - \ell_a}$.

It is known by [3] that

$$\min\left\{\dim FGe \mid e \in E - \{e_0\}\right\} = \mu_q(n), \tag{4.9}$$

where $\mu_q(n)$ is the minimal size of non-trivial q-cyclotomic cosets on \mathbb{Z}_n . For $e \in \hat{E}^{\dagger}$, by Lemma 2.1, dim(FGe) is even and dim $(FGe) \ge \mu_q(n)$.

For an integer ℓ with $\mu_q(n) \leq 2\ell \leq n-1$, we denote

 $\Omega_{2\ell} = \{ J \le FG \mid J \text{ is a direct sum of some of } (FGe) \text{'s for } e \in \widehat{E}^{\dagger}, \dim J = 2\ell \}.$ (4.10)

Lemma 4.10. $|\Omega_{2\ell}| \le |\widehat{E}^{\dagger}|^{2\ell/\mu_q(n)} \le n^{2\ell/\mu_q(n)}$.

Proof. For $J \in \Omega_{2\ell}$, dim $J = 2\ell$ and J is a direct sum of some of (FGe)'s for $e \in \widehat{E}^{\dagger}$. Since dim $FGe = 2n_e \ge \mu_q(n)$, the number of the direct summands in J is at most $2\ell/\mu_q(n)$. And, since $|\widehat{E}^{\dagger}| = r + s \le n - 1$, the number of the choices of each direct summand of J is at most r + s.

For $J \in \Omega_{2\ell}$, we denote (where ℓ_a and L_a are defined in Eq.(4.7))

$$\begin{split} \tilde{J} &= FGe_0 + J \ \text{ (hence } \dim \tilde{J} = 2\ell + 1); \\ \tilde{J}^* &= \big\{ a \, \big| \, a \in \tilde{J}, \ L_a = J \ \text{(equivalently, } \ell_a = \ell) \big\}. \end{split}$$

Lemma 4.11. $\mathcal{D}^{\leq \delta} = \bigcup_{\ell = \frac{1}{2}\mu_q(n)}^{(n-1)/2} \bigcup_{J \in \Omega_{2\ell}} \bigcup_{(a,d) \in (\tilde{J}^* \times \tilde{J}^*)^{\leq \delta}} \mathcal{D}_{(a,d)}.$

Proof. If $(a,d) \in (\tilde{J}^* \times \tilde{J}^*)^{\leq \delta}$, then $0 < \frac{w(a,d)}{2n} \leq \delta$. For any $C_{1,b} \in \mathcal{D}_{(a,d)}$, we have $C_{1,b} \in \mathcal{D}$ and $\frac{w(C_{1,b})}{2n} \leq \delta$, i.e., $C_{1,b} \in \mathcal{D}^{\leq \delta}$. Hence $\mathcal{D}_{(a,d)} \subseteq \mathcal{D}^{\leq \delta}$.

Let $C_{1,b} \in \mathbb{D}^{\leq \delta}$. There is $0 \neq (a,d) \in (FG)^2$ such that

$$(a,d) \in C_{1,b}$$
 and $0 < w(a,d) \le 2\delta n$.

Then $C_{1,b} \in \mathcal{D}_{(a,d)}$ and $\widehat{E}_a^{\dagger} \neq \emptyset$ (otherwise $(a,d) = (\alpha e_0, \alpha' e_0)$ with $0 \neq \alpha \in F$ and $0 \neq \alpha' \in F$, hence $w(a,d) = 2n > 2\delta n$). By Lemma 4.8, $\widehat{E}_d^{\dagger} = \widehat{E}_a^{\dagger}$. Then $(a,d) \in \widetilde{J}^* \times \widetilde{J}^*$ with $J = L_a \in \Omega_{2\ell_a}$. Thus, the left hand side of the equality in the lemma is contained in the right hand side.

Lemma 4.12. Let $\frac{1}{2}\mu_q(n) \leq \ell \leq \frac{n-1}{2}$ and $J \in \Omega_{2\ell}$. Then

$$\left|\bigcup_{(a,d)\in(\tilde{J}^*\times\tilde{J}^*)^{\leq\delta}}\mathfrak{D}_{(a,d)}\right|\leq q^{\frac{n-1}{2}+4\ell\left(h_q(\delta)-\frac{1}{4}\right)+2h_q(\delta)+3}.$$

Proof. Since dim $(\tilde{J} \times \tilde{J}) = 2(2\ell + 1) = 4\ell + 2$, by Lemma 4.6 we have

 $\left| (\tilde{J} \times \tilde{J})^{\leq \delta} \right| \leq q^{(4\ell+2)h_q(\delta)}.$

For $(a,d) \in (\tilde{J}^* \times \tilde{J}^*)^{\leq \delta}$, $\ell_a = \ell$ and $\left| \mathcal{D}_{(a,d)} \right| \leq q^{\frac{n-1}{2}-\ell+3}$ (see Corollary 4.9). So

$$\begin{split} \left| \bigcup_{(a,d)\in(\tilde{J}^*\times\tilde{J}^*)^{\leq\delta}} \mathcal{D}_{(a,d)} \right| &\leq \sum_{(a,d)\in(\tilde{J}^*\times\tilde{J}^*)^{\leq\delta}} \left| \mathcal{D}_{(a,d)} \right| \\ &\leq \sum_{(a,d)\in(\tilde{J}^*\times\tilde{J}^*)^{\leq\delta}} q^{\frac{n-1}{2}-\ell+3} \leq \sum_{(a,d)\in(\tilde{J}\times\tilde{J})^{\leq\delta}} q^{\frac{n-1}{2}-\ell+3} \\ &= \left| (\tilde{J}\times\tilde{J})^{\leq\delta} \right| \cdot q^{\frac{n-1}{2}-\ell+3} \leq q^{(4\ell+2)h_q(\delta)} \cdot q^{\frac{n-1}{2}-\ell+3} \\ &= q^{\frac{n-1}{2}+4\ell(h_q(\delta)-\frac{1}{4})+2h_q(\delta)+3}. \end{split}$$

We are done.

Theorem 4.13. Assume that $\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{2\mu_q(n)} > 0$. Then

$$\left| \mathcal{D}^{\leq \delta} \right| \leq q^{\frac{n-1}{2} - 2\mu_q(n) \left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\mu_q(n)}\right) + 4}.$$

Proof. Denote $\mu = \mu_q(n)$. By Lemma 4.11, Lemma 4.12 and Lemma 4.10,

$$\begin{aligned} |\mathcal{D}^{\leq \delta}| &\leq \sum_{\ell=\frac{1}{2}\mu}^{\frac{n-1}{2}} \sum_{J\in\Omega_{2\ell}} q^{\frac{n-1}{2}+4\ell \left(h_q(\delta)-\frac{1}{4}\right)+2h_q(\delta)+3} \\ &\leq \sum_{\ell=\frac{1}{2}\mu}^{\frac{n-1}{2}} n^{2\ell/\mu} \cdot q^{\frac{n-1}{2}+4\ell \left(h_q(\delta)-\frac{1}{4}\right)+2h_q(\delta)+3} \\ &= \sum_{\ell=\frac{1}{2}\mu}^{\frac{n-1}{2}} q^{\frac{n-1}{2}-4\ell \left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{2\mu}\right)+2h_q(\delta)+3}. \end{aligned}$$

Since $2\ell \ge \mu$ and $\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{2\mu} > 0$ (hence $2h_q(\delta) \le 1$),

$$\begin{aligned} |\mathcal{D}^{\leq \delta}| &\leq \sum_{\ell=\frac{1}{2}\mu}^{\frac{n-1}{2}} q^{\frac{n-1}{2}-2\mu\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{2\mu}\right)+1+3} \\ &\leq n \cdot q^{\frac{n-1}{2}-2\mu\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{2\mu}\right)+4} \\ &= q^{\frac{n-1}{2}-2\mu\left(\frac{1}{4}-h_q(\delta)-\frac{\log_q n}{\mu}\right)+4}. \end{aligned}$$

We are done.

4.3 Asymptotic goodness

Theorem 4.14. Assume that *q* is even or 4 | (q-1), and $\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{2\mu_q(n)} > 0$. Then

$$|\mathcal{D}^{\leq \delta}|/|\mathcal{D}| \leq q^{-2\mu_q(n)\left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\mu_q(n)}\right) + 6}.$$

 $\mathit{Proof.}\,$ By Theorem 4.1 and Lemma 4.7 ,

$$|\mathcal{D}| \ge \prod_{e \in \widehat{E}^{\dagger}} (q^{n_e} - 1) \ge q^{\sum_{e \in \widehat{E}^{\dagger}} n_e - 2} = q^{\frac{n-1}{2} - 2}.$$

By Theorem 4.13,

$$\begin{aligned} |\mathcal{D}^{\leq \delta}| / |\mathcal{D}| &\leq q^{\frac{n-1}{2} - 2\mu_q(n) \left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\mu_q(n)}\right) + 4} / q^{\frac{n-1}{2} - 2} \\ &= q^{-2\mu_q(n) \left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\mu_q(n)}\right) + 6}. \end{aligned}$$

We are done.

Lemma 4.15 ([9, Lemma 2.6]). There are infinitely many positive odd integers n_1, n_2, \cdots coprime to q such that $\lim_{i \to \infty} \frac{\log_q n_i}{\mu_q(n_i)} = 0$; in particular, $\mu_q(n_i) \to \infty$.

Remark 4.16. By [9, Lemma 2.6], there are infinitely many primes p_1, p_2, \cdots such that $\lim_{i\to\infty} \frac{\log_q p_i}{\mu_q(p_i)} = 0$. We just remark that the n_i 's in the lemma are not necessarily primes (which implies that the abelian groups G_i of order n_i are not necessarily cyclic). Because: by [3], for any integer m > 1 coprime to q,

 $\mu_q(m) = \min \{ \mu_q(p) \mid p \text{ runs over the prime divisors of } m \};$

therefore, if we take, for example, $n_i = p_i^2$, we still have $\lim_{i \to \infty} \frac{\log_q n_i}{\mu_q(n_i)} = 0$.

Theorem 4.17. Let n_1, n_2, \cdots be as in Lemma 4.15. Let G_i be any abelian group of order n_i for $i = 1, 2, \cdots$. If q is even or $q \equiv 1 \pmod{4}$, then there exist self-dual 2-quasi-FG_i codes C_i of type I, $i = 1, 2, \cdots$, such that the code sequence C_1, C_2, \cdots is asymptotically good.

Proof. Let \mathcal{D}_i be the set of all self-dual 2-quasi- FG_i codes of type I, let $\mathcal{D}_i^{\leq \delta}$ be as in Eq.(4.2). By the property of $h_q(\delta)$ in Eq.(4.6), we can take $\delta \in (0, 1-q^{-1})$ satisfying that $0 < h_q(\delta) < \frac{1}{4}$. Since $\lim_{i \to \infty} \frac{\log_q n_i}{\mu_q(n_i)} = 0$, we can further assume that $\frac{1}{4} - h_q(\delta) - \frac{\log_q n_i}{\mu_q(n_i)} > \varepsilon > 0$ for a positive real number ε . Since $\mu_q(n_i) \to \infty$, by Theorem 4.14 we have

$$\lim_{i \to \infty} \left| \mathcal{D}_i^{\leq \delta} \right| / \left| \mathcal{D}_i \right| \leq \lim_{i \to \infty} q^{-2\mu_q(n_i) \left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n_i}{\mu_q(n_i)} \right) + 6} = 0.$$

Thus we can take $C_i \in \mathcal{D}_i - \mathcal{D}_i^{\leq \delta}$ for $i = 1, 2, \cdots$. The self-dual 2-quasi- FG_i codes C_i of type I satisfy the following:

- the length $2n_i$ of C_i is going to ∞ ;
- the rate $R(C_i) = \frac{1}{2}$ for $i = 1, 2, \cdots$;
- the relative minimum distance $\Delta(C_i) > \delta$ for $i = 1, 2, \cdots$.

That is, the sequence of codes C_1, C_2, \cdots is asymptotically good.

5 Self-orthogonal 2-quasi-abelian codes

Keep the notation in Sections 2-4.

The existence of self-dual 2-quasi-FG codes (i.e., the self-orthogonal 2-quasi-FG codes of dimension n) is conditional, see Corollary 4.5. However, in the following we show that the self-orthogonal 2-quasi-FG codes of dimension n-1 always exist, and they are asymptotically good.

As exhibited in the proof of Theorem 4.1, the existence of self-dual 2-quasi-FG codes depends only on the computation in the e_0 -component (Lemma 4.2). Similarly to Eq.(2.9), by removing the e_0 -component we set

$$1^{\dagger} = 1 - e_0, \quad \text{i.e.,} \quad 1^{\dagger} = e_1 + \dots + e_r + \widehat{e}_{r+1} + \dots + \widehat{e}_{r+s};$$

$$FG^{\dagger} = FG \cdot 1^{\dagger} = \bigoplus_{e \in \widehat{F}^{\dagger}} FGe.$$

Then the e_0 -component of any $b^{\dagger} \in FG^{\dagger}$ vanishes, i.e., $e_0b^{\dagger} = 0$ and $b^{\dagger} = 1^{\dagger}b^{\dagger}$.

Lemma 5.1. For any $b^{\dagger} \in FG^{\dagger}$ with $b^{\dagger}\overline{b^{\dagger}} = -1^{\dagger}$, we have

$$C_{1^{\dagger},b^{\dagger}} = \{ (u1^{\dagger}, ub^{\dagger}) \mid u \in FG \}$$

is a self-orthogonal 2-quasi-FG code of dimension n-1.

Proof. By Lemma 3.9, $C_{1^{\dagger},b^{\dagger}}$ is self-orthogonal. Since $\operatorname{Ann}_{FG}(1^{\dagger},b^{\dagger}) = Fe_0$, by Lemma 3.4, $\dim C_{1^{\dagger},b^{\dagger}} = n-1$.

Similar to Eq.(4.1), we set

$$\mathcal{D}^{\dagger} = \left\{ C_{1^{\dagger}, b^{\dagger}} \, \middle| \, b^{\dagger} \in FG^{\dagger}, \, b^{\dagger}\overline{b^{\dagger}} = -1^{\dagger} \right\}.$$

$$(5.1)$$

And, similar to Eq.(4.2), we assume that $0 < \delta < 1 - q^{-1}$, and denote

$$(\mathcal{D}^{\dagger})^{\leq \delta} = \left\{ C_{1^{\dagger}, b^{\dagger}} \mid C_{1^{\dagger}, b^{\dagger}} \in \mathcal{D}^{\dagger}, \, \frac{\mathrm{w}(C_{1^{\dagger}, b^{\dagger}})}{2n} \leq \delta \right\}.$$
(5.2)

Theorem 5.2. $|\mathcal{D}^{\dagger}| = \prod_{i=1}^{r} (q^{n_i} + 1) \prod_{j=1}^{s} (q^{n_{r+j}} - 1).$

Proof. For $b^{\dagger} \in FG^{\dagger}$ such that $b^{\dagger}\overline{b^{\dagger}} = -1^{\dagger}$, the e_0 -components of both 1^{\dagger} and b^{\dagger} vanish. Thus $|\mathcal{D}^{\dagger}| = \prod_{k=1}^{r+s} |\mathfrak{T}_k|$, and the theorem follows from Lemma 4.3 and Lemma 4.4.

Remark 5.3. If $C_{1,b} \in \mathcal{D}$ and $b^{\dagger} = b - be_0$, then $b^{\dagger}\overline{b^{\dagger}} = -1^{\dagger}$ and $C_{1^{\dagger},b^{\dagger}} \in \mathcal{D}^{\dagger}$. In other words, $C_{1^{\dagger},b^{\dagger}}$ can be obtained by removing the e_0 -component of $C_{1,b}$. However, it may happen that $\mathcal{D} = \emptyset$, see Theorem 4.1. As a comparison, it is always true that $\mathcal{D}^{\dagger} \neq \emptyset$. We call $C_{1^{\dagger},b^{\dagger}} \in \mathcal{D}^{\dagger}$ a self-orthogonal 2-quasi-*FG* code of *type* I^{\dagger} .

For $(a,d) \in (FG)^2$, let $\mathcal{D}^{\dagger}_{(a,d)} = \{C_{1^{\dagger},b^{\dagger}} | C_{1^{\dagger},b^{\dagger}} \in \mathcal{D}^{\dagger}, (a,d) \in C_{1^{\dagger},b^{\dagger}}\}$. And, similar to Lemma 4.8, we have

Lemma 5.4. Let the notation be as above. If $\mathcal{D}^{\dagger}_{(a,d)} \neq \emptyset$, then $ae_0 = 0 = de_0$, $\widehat{E}^{\dagger}_a = \widehat{E}^{\dagger}_d$ and

$$\left|\mathcal{D}^{\dagger}_{(a,d)}\right| \leq \prod_{e \in \widehat{E}^{\dagger} - \widehat{E}^{\dagger}_{a}} (q^{n_{e}} + 1).$$

Proof. If $C_{1^{\dagger},b^{\dagger}} \in \mathcal{D}^{\dagger}$ and $(a,d) \in C_{1^{\dagger},b^{\dagger}}$, then there is a $u \in FG$ such that $a = u1^{\dagger}$ and $d = ub^{\dagger}$, hence $ae_0 = u1^{\dagger}e_0 = 0$, $de_0 = ub^{\dagger}e_0 = 0$, and $\widehat{E}_a^{\dagger} = \widehat{E}_d^{\dagger}$. Similar to the proof of Lemma 4.8, we can complete the proof (just note that Case 1 of the proof of Lemma 4.8 is no longer present here).

Similar to Corollary 4.9 and Lemma 4.11, we have

Corollary 5.5. $|\mathcal{D}^{\dagger}_{(a,d)}| \leq q^{\frac{n-1}{2}-\ell_a+2}.$

Lemma 5.6. $(\mathcal{D}^{\dagger})^{\leq \delta} = \bigcup_{\ell=\frac{1}{2}\mu_q(n)}^{(n-1)/2} \bigcup_{J \in \Omega_{2\ell}} \bigcup_{(a,d) \in (J^* \times J^*)^{\leq \delta}} \mathcal{D}^{\dagger}_{(a,d)}, \text{ where } J^* = \{a \mid a \in J, \ L_a = J\}.$

And Lemma 4.12 is revised as follows.

Lemma 5.7. Let $\frac{1}{2}\mu_q(n) \leq \ell \leq \frac{n-1}{2}$ and $J \in \Omega_{2\ell}$. Then

$$\left|\bigcup_{(a,d)\in (J^*\times J^*)\leq\delta} \mathcal{D}^{\dagger}_{(a,d)}\right| \leq q^{\frac{n-1}{2}+4\ell\left(h_q(\delta)-\frac{1}{4}\right)+2}.$$

Proof. It is similar to the computation in the proof of Lemma 4.12 (but \tilde{J} is replaced by J, etc.):

$$\begin{split} \left| \bigcup_{(a,d)\in(J^*\times J^*)\leq\delta} \mathcal{D}^{\dagger}_{(a,d)} \right| &\leq \sum_{(a,d)\in(J^*\times J^*)\leq\delta} \left| \mathcal{D}^{\dagger}_{(a,d)} \right| \\ &\leq \sum_{(a,d)\in(J^*\times J^*)\leq\delta} q^{\frac{n-1}{2}-\ell+2} \leq \sum_{(a,d)\in(J\times J)\leq\delta} q^{\frac{n-1}{2}-\ell+2} \\ &= \left| (J\times J)^{\leq\delta} \right| \cdot q^{\frac{n-1}{2}-\ell+2} \leq q^{4\ell h_q(\delta)} \cdot q^{\frac{n-1}{2}-\ell+2} \\ &= q^{\frac{n-1}{2}+4\ell} (h_q(\delta)-\frac{1}{4})+2, \end{split}$$

where the last second line follows from Lemma 4.6 and $\dim(J \times J) = 4\ell$.

Then, similar to Theorem 4.13 and Theorem 4.14, we can get the following results.

Theorem 5.8. Assume that $\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{2\mu_q(n)} > 0$. Then $|(\mathfrak{D}^{\dagger})^{\leq \delta}| \leq q^{\frac{n-1}{2} - 2\mu_q(n) \left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\mu_q(n)}\right) + 2}$.

Theorem 5.9. Assume that $\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{2\mu_q(n)} > 0$. Then

$$\left| (\mathcal{D}^{\dagger})^{\leq \delta} \right| / \left| \mathcal{D}^{\dagger} \right| \leq q^{-2\mu_q(n)\left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n}{\mu_q(n)}\right) + 4}.$$

Theorem 5.10. Let n_1, n_2, \cdots be odd positive integers coprime to q such that $\lim_{i\to\infty} \frac{\log_q n_i}{\mu_q(n_i)} = 0$. Let G_i be any abelian group of order n_i for $i = 1, 2, \cdots$. Then for $i = 1, 2, \cdots$ there exist self-orthogonal 2-quasi-FG_i codes C_i of type I^{\dagger} (hence $\dim C_i = n_i - 1$) such that the code sequence C_1, C_2, \cdots is asymptotically good.

Proof. Let \mathcal{D}_i^{\dagger} be the set of all self-orthogonal 2-quasi- FG_i codes of type I^{\dagger} . Take a real number $\delta \in (0, 1 - q^{-1})$ satisfying that $0 < h_q(\delta) < \frac{1}{4}$. We have

$$\lim_{i \to \infty} \left| (\mathcal{D}_i^{\dagger})^{\leq \delta} \right| / \left| \mathcal{D}_i^{\dagger} \right| \leq \lim_{i \to \infty} q^{-2\mu_q(n_i) \left(\frac{1}{4} - h_q(\delta) - \frac{\log_q n_i}{\mu_q(n_i)} \right) + 4} = 0.$$

Thus we can take $C_i \in \mathcal{D}_i^{\dagger} - (\mathcal{D}_i^{\dagger})^{\leq \delta}$ for $i = 1, 2, \cdots$. The self-orthogonal 2-quasi- FG_i codes C_i of type I^{\dagger} satisfy the following:

- the length $2n_i$ of C_i is going to ∞ ;
- the rate $\lim_{i \to \infty} R(C_i) = \frac{1}{2};$
- the relative minimum distance $\Delta(C_i) > \delta$ for $i = 1, 2, \cdots$.

That is, the sequence of codes C_1, C_2, \cdots is asymptotically good.

6 Conclusion

Let G be any abelian group of odd order n coprime to the cardinality q = |F|. We introduced the self-dual 2-quasi-FG codes of type I, and obtained the exact number of such codes. As a consequence, the self-dual 2-quasi-FG codes exist if and only if -1 is a square in F. We further estimated the number of the self-dual 2-quasi-FG codes of type I with small relative minimum distances. With the two numerical results we proved that the self-dual 2-quasi-FG codes are asymptotically good provided -1 is a square in F.

Moreover, we showed that the self-orthogonal 2-quasi-FG codes of dimension n-1 always exist. And, by the same method (with small revisions), we got two similar numerical results on such codes, and showed that the self-orthogonal 2-quasi-FG codes are asymptotically good.

References

- A. Alahmadi, F. Özdemir, P. Solé, "On self-dual double circulant codes", Des. Codes Cryptogr., vol. 86, pp. 1257-1265, 2018. [2, 3, 9]
- [2] J. L. Alperin, B. Bell, Groups and Representations, GTM 162, Springer-Verlag, 1995. [4, 9]
- [3] S. A. Aly, A. Klappenecker, P. K. Sarvepalli, "Duadic group algebra codes", ISIT 2007, pp. 2096-2100, 2007. [14, 17]
- [4] L. M. J. Bazzi, S. K. Mitter, "Some randomized code constructions from group actions", *IEEE Trans. Inform. Theory*, vol. 52, pp. 3210-3219, 2006.
 [3]
- [5] C. L. Chen, W. W. Peterson, E. J. Weldon, "Some results on quasi-cyclic codes", *Information and Control*, vol. 15, pp. 407-423, 1969. [2]
- [6] V. Chepyzhov, "New lower bounds for minimum distance of linear quasicyclic and almost linear quasi-cyclic codes", *Problem Peredachi Informatsii*, vol. 28, pp. 33-44, 1992. [2]
- B. K. Dey, "On existence of good self-dual quasi-cyclic codes", *IEEE Trans. Inform. Theory*, vol. 50, pp. 1794-1798, 2004. [2]
- [8] Yun Fan, Liren Lin, "Thresholds of random quasi-abelian codes", IEEE Trans. Inform. Theory, vol. 61, pp. 82-90, 2015. [13]
- [9] Yun Fan, Liren Lin, "Dihedral group codes over finite fields", *IEEE Trans. Inform. Theory*, vol. 67, pp. 5016-5025, 2021. [3, 4, 10, 13, 16, 17]
- [10] W. C. Huffman, V. Pless, Fundamentals of Error-Correcting Codes, Cambridge University Press, 2003. [2]

- [11] T. Kasami, "A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2", *IEEE Trans. Inform. Theory*, vol. 20, pp. 679, 1974. [2]
- [12] Liren Lin, "Random quasi-abelian codes and self-orthogonal negacyclic codes (in Chinese)", Ph.D. dissertation, Central China Normal Univ., Wuhan, China, 2014. [3]
- [13] S. Ling, P. Sole, "On the algebraic structure of quasi-cyclic codes II: Chain rings", Des. Codes Cryptogr., vol. 30, no. 1, pp.113-130, 2003. [2]
- [14] C. Martínez-Pérez, W. Willems, "Is the class of cyclic codes asymptotically good?" *IEEE Trans. Inform. Theory*, vol. 52, pp. 696-700, 2006. [2]
- [15] C. Martínez-Pérez, W. Willems, "Self-dual double-even 2-quasi-cyclic transitive codes are asymptotically good", *IEEE Trans. Inform. Theory*, vol. 53, pp. 4302-4308, 2007. [2]
- [16] C. Tjhai, M. Tomlinson, R. Horan, M. Ahmed, M. Ambroze, "Some results on the weight distributions of the binary double-circulant codes based on primes", DOI: 10.1109/ICCS.2006.301431, IEEE CCS, Singapore 2006. [3, 9]