Self-dual doubly-even 2-quasi-cyclic transitive codes are asymptotically good

Conchita Martínez-Pérez
Departamento de Matemáticas
Universidad de Zaragoza,
50009 Zaragoza
email: conmar@unizar.es

Wolfgang Willems
Institut für Algebra und Geometrie
Fakultät für Mathematik
Otto-von-Guericke-Universität
39016 Magdeburg
email: wolfgang.willems@mathematik.uni-magdeburg.de

Abstract. We prove that the class of binary self-dual doubly-even 2-quasi-cyclic transitive codes is asymptotically good. The proof is based on a result of Helmut Hasse on the density of primes which satisfy suitable conditions.

Index Terms: Asymptotically good codes, doubly-even codes, self-dual codes, transitive codes, 2-quasi-cyclic codes

MSC 2000: 94B05, 94B15, 94B65, 20C20, 11B05

1 Introduction

It is a long standing question whether the class of cyclic codes is asymptotically good (see for instance [11]). However, it has been known for more than 30 years that the class of quasi-cyclic codes, even the class of 2-quasi-cyclic codes, is asymptotically good ([2], [7]) and the class of self-dual codes [9] as well. In 2003, Ling and Solé proved that there are long binary quasi-cyclic self-dual codes which meet the Gilbert-Varshamov bound. In their construction they use $\frac{n}{3}$-quasi-cyclic codes of length n. Under the condition that there are infinitely many primes p for which 2 is primitive Dey [3] proved that the same holds true for a class of self-dual quasi-cyclic codes which lie between 2-quasi-cyclic and $\frac{n}{3}$-quasi-cyclic codes. More precisely, he constructs sequences of self-dual $2p$-quasi-cyclic and doubly-even $8p$-quasi-cyclic codes of length $2p^2$ respectively $8p^2$ which meet the Gilbert-Varshamov bound. On the other hand transitive Codes, i.e., codes for which the automorphism group acts transitively on the positions, achieve the Tsfasman-Vlăduţ-Zink bound, a result proved by Stichtenoth [12] in 2005. The main tool in his proof is a new asymptotically optimal tower $E_0 \subseteq E_1 \subseteq \ldots$ of function fields E_i where all extensions E_i/E_0 are

Galois. Surprisingly, using group theoretical methods and probabilistic arguments, Bazzi and Mitter [1] recently proved that even the class of 2-quasi-cyclic transitive codes is asymptotically good. The codes which Bazzi and Mitter consider are ideals in group algebras over dihedral groups. Note that such group algebras split into a direct sum of two cyclic group algebras which are fliped by an involution. Thus the class of codes which they consider is a class of 2-quasi-cyclic transitive codes which, in some sense, is the closest to the class of cyclic codes for which the problem of the asymptotic behaviour is still open.

In this note we prove

Theorem 1.1 *The class of binary self-dual doubly-even* 2*-quasi-cyclic transitive codes is asymptotically good.*

Note that this is slightly stronger than the result in [1]. In the proof we also use dihedral groups. However, and that is rather surprising, our proof runs more smoothly than that of Bazzi-Mitter. The reason is due to the fact that the particular 2-quasi-cyclic self-dual codes which we are going to study are automatically invariant under dihedral groups.

2 Self-dual 2-quasi-cyclic codes

A linear code is called *l-quasi-cyclic* if it is invariant under T^l where T denotes the cyclic shift. In this sense cyclic codes are 1-quasi-cyclic codes. Note that an l-quasi-cyclic code can be considered as a submodule of a direct sum of l copies of a group algebra KG where G is a cyclic group. Self-duality is then naturally defined via the Euclidean inner product $\langle \cdot\,, \cdot\rangle$ on each of the copies of KG which are assumed to be pairwise orthogonal to each other. Furthermore, we deal only with binary codes, i.e., the underlying field K is always $\mathbb{F}_2$.

Let $^{-}\colon \mathbb{F}_2G \to \mathbb{F}_2G$ denote the algebra antiautomorphism defined by the map $g \mapsto \bar{g} = g^{-1}$ for $g \in G$. To be brief we write $R = \mathbb{F}_2G$ where G is always a finite group and we denote by $U(R)$ the subgroup of units in R.

Lemma 2.1 *For $a, b \in R$ we put*

$$C_{a,b} = \{(fa, fb) \mid f \in R\}.$$

a) If G is a cyclic group then $C_{a,b}$ is a 2-quasi-cyclic code.

b) $C_{a,b} \subseteq C_{a,b}^{\perp}$ if and only if $a\bar{a} = b\bar{b}$.

c) $a\bar{a} = b\bar{b} \in U(R)$ if and only if $C_{a,b} = C_{a,b}^{\perp}$.

d) Let $a\bar{a} = b\bar{b} \in U(R)$, hence $C_{a,b} = C_{a,b}^{\perp}$. Then $C_{a,b}$ is doubly-even if and only if

$$\mathrm{wt}(a) + \mathrm{wt}(b) \equiv \bmod 4.$$

Proof. a) This is clear since Ra and Rb define cyclic codes of length $|G|$.
b) First assume that $a\bar{a} = b\bar{b}$. Then, for any $f, g \in R$, we have

$$\begin{aligned}\langle (fa, fb), (ga, gb)\rangle &= \langle fa, ga\rangle + \langle fb, gb\rangle \\ &= \langle \bar{g}f, a\bar{a}\rangle + \langle \bar{g}f, b\bar{b}\rangle \\ &= \langle \bar{g}f, a\bar{a} + b\bar{b}\rangle \ = 0,\end{aligned}$$

hence $C_{a,b} \subseteq C_{a,b}^{\perp}$.

Conversely, if $C_{a,b} \subseteq C_{a,b}^{\perp}$ then for any $x \in G$ we get

$$0 = \langle (xa, xb), (a, b) \rangle = \langle x, a\bar{a} \rangle + \langle x, b\bar{b} \rangle.$$

Thus the coefficient of x in $a\bar{a}$ coincides with that in $b\bar{b}$ which shows that $a\bar{a} = b\bar{b}$.
c) The assumption $a\bar{a} = b\bar{b} \in U(R)$ trivially implies that a and b are units in the ring R. Hence $R = Ra = Rb$ which proves that $\dim C_{a,b} = |G|$. Thus, by part b), the code $C_{a,b}$ is self-dual.

Conversely, if $C_{a,b} = C_{a,b}^{\perp}$ then $a\bar{a} = b\bar{b}$, by part b). Furthermore we have $\dim\, Ra = |G| = \dim\, R$ which is equivalent to $a \in U(R)$.
d) By part c), the code $C_{a,b}$ is self-dual. Moreover, $C_{a,b}$ has a generating set $\{(ga, gb) \mid g \in G\}$ in which all vectors have weight

$$\mathrm{wt}(ga, gb) = \mathrm{wt}(a, b) = \mathrm{wt}(a) + \mathrm{wt}(b).$$

Thus, by ([13], Satz 3.1.7), the code $C_{a,b}$ is doubly-even if and only if 4 divides $\mathrm{wt}(a) + \mathrm{wt}(b)$. □

Lemma 2.2 *There exist $a, b \in U(R)$ with $a\bar{a} = b\bar{b}$ and $4 \mid \mathrm{wt}(a) + \mathrm{wt}(b)$ if and only if $4 \mid |G|$.*

Proof. First suppose that $4 \mid |G|$. We put $c = \sum_{g \in G} g$ and $b = 1 + c$. Then $c^2 = 0$ and $c = \bar{c}$. Furthermore,

$$b\bar{b} = (1 + c)(1 + \bar{c}) = 1 + 2c + c^2 = 1.$$

In particular, $b \in U(R)$. Since $4 \mid |G|$ we have

$$\mathrm{wt}(b) = |G| - 1 \equiv -1 \bmod 4.$$

Thus $(1, b)$ satisfies the required conditions.

Conversely, suppose that there are $a, b \in U(R)$ which satisfy $a\bar{a} = b\bar{b}$ and $\mathrm{wt}(a) + \mathrm{wt}(b) \equiv \bmod 4$. By Lemma 2.1 d), the code $C_{a,b}$ is doubly-even. Thus, by Gleason's Theorem ([13], Korollar 3.3.22), 8 divides the length of $C_{a,b}$. Hence 8 divides $2|G|$ or equivalently 4 divides $|G|$. □

Lemma 2.3 *Let $D = G\langle t \rangle$ be a dihedral group where G is a cyclic normal subgroup of index 2 whose elements are all inverted by the involution t. Put $R = \mathbb{F}_2 G$ and consider the action of D on $\mathbb{F}_2 D = R \oplus Rt = R \times R$. If $a, b \in U(R)$ then $a\bar{a} = b\bar{b}$ if and only if $C_{a,b}$ is invariant under the dihedral group D.*
In particular, $C_{a,b}$ is a self-dual 2-quasi-cyclic transitive code.

Proof. Let $z = x + yt \in R \oplus Rt$ with $x, y \in R$. Then

$$tz = tx + tyt = \bar{x}t + \bar{y}.$$

This means that

$$t(x, y) = (\bar{y}, \bar{x}).$$

Thus $C_{a,b}$ is t-invariant if and only if $C_{a,b} = C_{\bar{b},\bar{a}}$. But note that $(a,b) \in C_{\bar{b},\bar{a}}$ if and only if for some $f \in R$,

$$a = f\bar{b} \quad \text{and} \quad b = f\bar{a}.$$

Since a and b are units this is equivalent to $a\bar{b}^{-1} = b\bar{a}^{-1}$ or $a\bar{a} = b\bar{b}$ which is satisfied by asumption. □

In order to construct self-dual doubly-even codes $C_{a,b}$ we need $4 \mid |G|$, by Lemma 2.1 and Lemma 2.2. In this case the group algebra $\mathbb{F}_2G$ is no longer semisimple and the structure becomes quite complicated in general. However, we are only interested in 2-quasi-cyclic codes. Thus we may assume that G is cyclic. This guaranties that we can easily deal with the modular group algebra $\mathbb{F}_2G$.

To be more precise, let G be a cyclic group for the rest of this section. Let T denote the Sylow 2-subgroup of G and let H be the subgroup of G consisting of all elements of odd order. Thus $2 \nmid |H|$, $G = TH$ and $T \cap H = \langle 1 \rangle$. Furthermore, we always assume that $s(|H|)$ is odd where, for $m \in \mathbb{N}$ odd, $s(m)$ is defined as the smallest positive integer such that

$$m \mid 2^{s(m)} - 1.$$

Note that the simple modules for $R = \mathbb{F}_2G$ are exactly the simple modules for $\mathbb{F}_2H$ since T acts trivially on all simple R-modules (see [6], Chap. VII, Theorem 13.4). The condition $s(|H|)$ odd implies, by ([10] Theorem 3.3), that the trivial $\mathbb{F}_2H$-module is the only simple $\mathbb{F}_2H$-module V (or R-module) which is self-dual in the sense of representation theory, i.e., $V \cong V^* = \mathrm{Hom}(V, \mathbb{F}_2)$ (see [6], Chap. VII, section 8). This means, if we put $e_0 = \sum_{h \in H} h$, then we have a decomposition

$$1 = e_0 + \sum_{i=1}^{s} (e_i + \bar{e}_i)$$

in the algebra $\mathbb{F}_2H$ with mutually orthogonal primitive idempotents e_i. The principal block of $\mathbb{F}_2H$ is $\mathbb{F}_2He_0 = \mathbb{F}_2e_0$ and $\bar{e}_i$ defines the block dual to the block associated to e_i.

From this we get the decomposition

$$R = Re_0 \perp (Re_1 \oplus R\bar{e}_1) \perp \ldots \perp (Re_s \oplus R\bar{e}_s)$$

for the group algebra R where each module Re_i is uniserial of Loewy length $2^t = |T|$, i.e., there exists a unique composition series

$$P_i = Re_i = P_iJ^0 > P_iJ > \ldots > P_iJ^{2^t-1} > P_iJ^{2^t} = 0$$

where J denotes the Jacobson radical of R and for all k the factor module $P_iJ^k/P_iJ^{k+1} \cong V_i$ is the simple R-module, say of dimension l_i, corresponding to e_i (see [6], Chap. VII, section 10 and Theorem 14.9). In particular, if I is a submodule of P_i then $I = P_iJ^k$ for some k, hence $\dim I = (2^t - k)l_i$. Note that $R\bar{e}_i$ has the same structure as Re_i with V_i replaced by the dual module V_i^*. Moreover, since P_i is a local algebra

$$U(P_i) = P_i \setminus P_iJ$$

is the group of units in P_i.

Note in addition that $Re_0 = \mathbb{F}_2 T e_0$ and that for each $a \in R$ there is a unique $y \in \mathbb{F}_2 T$ with $ae_0 = ye_0$.

Lemma 2.4 *With the notation of the preceding section we have.*

a) $|U(P_i)| = 2^{(2^t-1)l_i}(2^{l_i}-1)$.

b) If $f, r \in P_i$ *and* $\dim Rf = \alpha l_i$ *then*

$$|\{a_i \in U(P_i) \mid a_i f = r\}| \leq \begin{cases} 2^{(2^t-\alpha)l_i} & \text{if } f \neq 0 \\ 2^{(2^t-1)l_i}(2^{l_i}-1) & \text{if } f = 0. \end{cases}$$

Proof. a) This is clear.
b) For $f = 0$ the bound is trivial. Thus we may suppose that $f \neq 0$. Since Rf is a submodule of P_i of dimension αl_i we have $Rf = P_i J^{2^t-\alpha}$. If $a_i, b_i \in P_i$ with $a_i f = b_i f = r$ then $(a_i - b_i)f = 0$. Therefore $a_i - b_i$ can be chosen as any element in the kernel of the map $P_i \to P_i$ defined by $a \mapsto af$. Counting dimensions we see that this kernel is exactly $P_i J^\alpha$ from which the assertion follows. $\square$

The next lemma which we freely use in the sequel is well-known.

Lemma 2.5 *If* C *is a binary code and* $c, c' \in C$ *then*

$$\mathrm{wt}(c+c') = \begin{cases} \mathrm{wt}(c) + \mathrm{wt}(c') \mod 4 & \text{if } \langle c, c' \rangle = 0 \\ \mathrm{wt}(c) + \mathrm{wt}(c') - 2 \mod 4 & \text{if } \langle c, c' \rangle = 1. \end{cases}$$

Lemma 2.6 *If* $b \in U(R)$ *with* $b\bar{b} = 1$ *then there is a unique* $y \in \mathbb{F}_2 T$ *which satisfies the following three conditions.*

(i) $be_0 = ye_0$.

(ii) $y\bar{y} = 1$.

(iii) $\mathrm{wt}(b) \equiv \mathrm{wt}(y) \mod 4$.

Proof. The assumption $b\bar{b} = 1$ implies the existence of a unique $y \in \mathbb{F}_2 T$ with $be_0 = ye_0$ and $y\bar{y} = 1$. Thus it remains to show that part *(iii)* holds true. Clearly,

$$b = be_0 + \sum_{i=1}^{s} b(e_i + \bar{e}_i).$$

We put $b_i = b(e_i + \bar{e}_i)$ for $i = 1, \ldots, s$. Note that

$$\langle be_i, b\bar{e}_i \rangle = \langle \bar{b}be_i, \bar{e}_i \rangle = \langle e_i, \bar{e}_i \rangle = \langle e_i^2, 1 \rangle = \langle e_i, 1 \rangle = 1$$

since $\langle e_i, 1 \rangle$ is the dimension of the simple $\mathbb{F}_2 H$-module corresponding to e_i which is odd since $s(|H|)$ is assumed to be odd. Thus, by Lemma 2.5,

$$\mathrm{wt}(b_i) = \mathrm{wt}(be_i + b\bar{e}_i) \equiv \mathrm{wt}(be_i) + \mathrm{wt}(b\bar{e}_i) - 2 \mod 4.$$

Moreover, since b is a unit in R we have $Rbe_i = Re_i$. Thus the code Re_i has a basis consisting of elements of weight $\mathrm{wt}(e_i)$ and also a basis consisting of elements of weight $\mathrm{wt}(be_i)$. As $Re_i \subseteq (Re_i)^\perp$ for $i \geq 1$, we get

$$\mathrm{wt}(be_i) \equiv \mathrm{wt}(e_i) \mod 4,$$

hence

$$\mathrm{wt}(b_i) \equiv -2 \bmod 4,$$

for all $i \geq 1$. According to Lemma 2.5 we obtain the congruence

$$\mathrm{wt}(b) \equiv \mathrm{wt}(be_0) - 2s \mod 4.$$

Replacing b by y says

$$\mathrm{wt}(y) \equiv \mathrm{wt}(ye_0) - 2s \mod 4$$

which shows that $\mathrm{wt}(b) \equiv \mathrm{wt}(y) \mod 4$ since $be_0 = ye_0$. □

Definition 2.7 We put

$$\Omega = \{(a, b) \mid a, b \in U(R),\ a\bar{a} = b\bar{b},\ \mathrm{wt}(a) + \mathrm{wt}(b) \equiv 0 \bmod 4\}.$$

and

$$\omega_0 = |\{(y_1, y_2) \mid y_1, y_2 \in U(\mathbb{F}_2 T),\ y_1\bar{y}_1 = y_2\bar{y}_2,\ \mathrm{wt}(y_1) + \mathrm{wt}(y_2) \equiv 0 \bmod 4\}|.$$

Lemma 2.8 *The size of* Ω *is*

$$|\Omega| = \omega_0 \prod_{i=1}^{s} 2^{3l_i 2^t} \left(\frac{2^{l_i} - 1}{2^{l_i}}\right)^3.$$

Proof. For units a, b with $a\bar{a} = b\bar{b}$ consider the unique units $y_1, y_2 \in \mathbb{F}_2 T$ with $ae_0 = y_1 e_0$ and $be_0 = y_2 e_0$. Then $y_1\bar{y}_1 = y_2\bar{y}_2$ and in addition, by Lemma 2.6, $\mathrm{wt}(a^{-1}b) \equiv \mathrm{wt}(y_1^{-1}y_2) \bmod 4$. Since $C_{a,b} = C_{1,a^{-1}b}$ and $C_{y_1,y_2} = C_{1,y_1^{-1}y_2}$ we have $\mathrm{wt}(a) + \mathrm{wt}(b) \equiv 0 \bmod 4$ if and only if $\mathrm{wt}(y_1^{-1}y_2) \equiv \mathrm{wt}(a^{-1}b) \equiv -1 \bmod 4$ and this happens if and only if $\mathrm{wt}(y_1) + wt(y_2) \equiv 0 \bmod 4$.

Next observe that each $a \in R$ has a decomposition

$$a = ae_0 + \sum_{i=1}^{s}(ae_i + a\bar{e}_i),$$

and $a \in U(R)$ if and only if all summands ae_i and $a\bar{e}_i$ are units in Re_i resp. $R\bar{e}_i$. To define any $a \in U(R)$ we can choose arbitrary units $ae_i \in Re_i$ and $a\bar{e}_i \in R\bar{e}_i$, or equivalently

$$ae_i,\ \bar{a}e_i = \overline{a\bar{e}_i}.$$

The equation $a\bar{a} = b\bar{b}$ for $a, b \in U(R)$ implies

$$(*) \qquad (ae_i)(\bar{a}e_i) = (be_i)(\bar{b}e_i).$$

Thus, to satisfy the equation $a\bar{a} = b\bar{b}$ we may choose for $i \geq 1$ arbitrary units

$$ae_i,\ \bar{a}e_i, be_i \in Re_i$$

and $\bar{b}e_i$ is then determined by $(*)$.

This shows that

$$|\Omega| = \omega_0 \prod_{i=1}^{s} |U(Re_i)|^3.$$

Applying Lemma 2.4 a) we obtain

$$|\Omega| = \omega_0 \prod_{i=1}^{s} 2^{3l_i(2^t-1)}(2^{l_i}-1)^3 = \omega_0 \prod_{i=1}^{s} 2^{3l_i 2^t}(\frac{2^{l_i}-1}{2^{l_i}})^3.$$

$\square$

Lemma 2.9 *Let $f \in R$ with* $\dim fR = l$ *and let $r_1, r_2 \in Rf$ be fixed. If the dimensions of all simple non-trivial R-modules are large enough and if $(a,b) \in \Omega$ is chosen randomly then the probability* $\Pr_{(a,b)\in\Omega}(fa = r_1, fb = r_2)$ *that $fa = r_1$ and $fb = r_2$ is bounded by*

$$\Pr_{(a,b)\in\Omega}(fa = r_1, fb = r_2) \leq \frac{2^{2^{t+1}}}{2^{5l/4}}$$

Proof. We consider the decomposition

$$Rf = Rfe_0 \oplus \oplus_{i=1}^{s}(Rfe_i \oplus Rf\bar{e}_i).$$

If $\alpha_i = \dim Rfe_i$ for $i = 0, \ldots s$ and $\beta_i = \dim Rf\bar{e}_i$ for $i = 1, \ldots, s$ then

$$l = \alpha_0 + \sum_{i=1}^{s}(\alpha_i + \beta_i)l_i$$

where $l_i = \dim Re_i = \dim R\bar{e}_i$ for $i = 1, \ldots, s$. In order to get all elements $a, b \in U(R)$ with $a\bar{a} = b\bar{b}$ we may choose for $i = 1, \ldots, s$ three of the four elements $ae_i, a\bar{e}_i, be_i, \bar{b}e_i$ and the remaining is then determined by

$$(ae_i)(a\bar{e}_i) = (be_i)(b\bar{e}_i).$$

In order to bound the number of possibilities for $fa = r_1$ and $fb = r_2$ we choose the units ae_i, be_i arbitrarily, and then $a\bar{e}_i$ or $b\bar{e}_i$. In the latter case we choose exactly that one for which the number of possible choices such that $fa\bar{e}_i = r_1\bar{e}_i$ resp. $fb\bar{e}_i = r_2\bar{e}_i$ is smallest. Finally, we put

$$\epsilon_i = \begin{cases} 3 & \text{if } \alpha_i = \beta_i = 0 \\ 0 & \text{if } \alpha_i \neq 0 \neq \beta_i \\ 1 & \text{otherwise} \end{cases}$$

and $\gamma_i = \max\{\alpha_i, \beta_i\}$. Then, by Lemma 2.4, we get the following upper bound for the possibilities of $ae_i, a\bar{e}_i, be_i, b\bar{e}_i$ $(i \geq 1)$, namely

$$2^{(2^t-\alpha_i)l_i}2^{(2^t-\beta_i)l_i}2^{(2^t-\gamma_i)l_i}\left(\frac{2^{l_i}-1}{2^{l_i}}\right)^{\epsilon_i} = 2^{(-\alpha_i-\beta_i)l_i}2^{-\gamma_i l_i}2^{3l_i 2^t}\left(\frac{2^{l_i}-1}{2^{l_i}}\right)^{\epsilon_i}.$$

Remember, by the beginning of the proof of Lemma 2.8, that for $a\bar{a} = b\bar{b} \in U(R)$ the condition $\mathrm{wt}(a) + \mathrm{wt}(b) \equiv 0 \bmod 4$ is equivalent to the condition $\mathrm{wt}(y_1) + \mathrm{wt}(y_2) \equiv 0 \bmod 4$ where $ae_0 = y_1e_0$, $be_0 = y_2e_0$ and $y_1, y_2 \in \mathbb{F}_2T$ unique. Furthermore, the possibilities of choices $(y_1, y_2) \in U(\mathbb{F}_2T) \times U(\mathbb{F}_2T)$ with

$$y_1\bar{y}_1 = y_2\bar{y}_2 \text{ and } \mathrm{wt}(y_1) + \mathrm{wt}(y_2) \equiv 0 \bmod 4$$

was defined as ω_0 in Definition 2.7.
Since $\sum_{i=1}^s (\alpha_i+\beta_i) l_i = l-\alpha_0$ and $2\sum_{i=1}^s \gamma_i l_i \ge l-\alpha_0$ we have

$$|\{(a,b)\in\Omega \mid fa=r_1,\ fb=r_2\}| \le \\ \omega_0 2^{-l+\alpha_0-l/2+\alpha/2} \prod_{i=1}^s 2^{3l_i 2^t} \left(\frac{2^{l_i}-1}{2^{l_i}}\right)^{\epsilon_i}.$$

Finally, taking Lemma 2.8 into acount for $|\Omega|$, we obtain

$$\begin{aligned} \Pr_{(a,b)\in\Omega}(fa=r_1, fb=r_2) &\le 2^{-3l/2+3\alpha_0/2} \prod_{i=1}^s \left(\frac{2^{l_i}}{2^{l_i}-1}\right)^{3-\epsilon_i} \\ &\le 2^{-3l/2+3\cdot 2^t/2} 2^{l/4} = \frac{2^{2^{t+1}}}{2^{5l/4}}. \end{aligned}$$

For the last inequality observe that, if all l_i are large enough, then $\frac{2^{l_i}}{2^{l_i}-1} \le 2^{1/8}$ for all i and $\sum_{i=1}^s (3-\epsilon_i) \le 2l$. □

3 The density of some set of primes

Let $\mathbb{P}$ denote the set of all primes. For a subset $\mathcal{P}$ of $\mathbb{P}$ there are two notions of density, namely

$$\delta_{Dir}(\mathcal{P}) = \lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{P}} p^{-s}}{\sum_{p\in\mathbb{P}} p^{-s}},$$

the so-called *Dirichlet density*, and

$$\delta_{nat}(\mathcal{P}) = \lim_{x\to\infty} \frac{|\{p\le x \mid p\in P\}|}{|\{p\le x \mid p\in\mathbb{P}\}|},$$

the so-called *natural density*. Both limits do not exist in general, but if the natural density exists for $\mathcal{P}$ then the Dirichlet density exists for $\mathcal{P}$ and both coincide. (Examples show that the converse is wrong.)

Now let $r:\mathbb{N}\to\mathbb{R}$ be a non-decreasing function with $r(n) \ll \sqrt{\frac{n}{\log n}}$, i.e.,

$$\frac{r(n)}{\sqrt{\frac{n}{\log n}}} \to 0 \quad \text{for } n\to\infty.$$

We put

$$\mathcal{B} = \{p \mid 2\ne p\in\mathbb{P}, s(p) < r(p)\} \qquad (\textit{bad primes})$$

and

$$\mathcal{G} = \{p \mid 2\ne p\in\mathbb{P}, s(p) \ge r(p)\} \qquad (\textit{good primes}).$$

Lemma 3.1 *We have*

$$\delta_{Dir}(\mathcal{B}) = 0.$$

Proof. Clearly, $p \in \mathcal{B}$ if and only if there are integers a and k with $0 < a < r(p)$ such that $2^a - 1 = pk$. Thus, if we put

$$\mathcal{B}_n = \{p \in \mathcal{B} \mid p \leq n\},$$

we obtain (as in Lemma 2.6 of [1])

$$\begin{aligned} |\mathcal{B}_n| &\leq |\{(a,k) \mid 0 < a < r(n) \text{ and } (2^a - 1)/k \text{ is a prime}\}| \\ &\leq r(n)\log(2^{r(n)} - 1) \\ &\leq r(n)^2 \\ &\ll n/\log n. \end{aligned}$$

By the Prime Number Theorem (see for instance [4]), we therefore get immediately $\delta_{nat}(\mathcal{B}) = 0$, hence $\delta_{Dir}(\mathcal{B}) = 0$. □

Next we divide $\mathbb{P} \setminus \{2\}$ into two other disjoint sets, namely

$$\Sigma = \{p \mid 2 \neq p \in \mathbb{P},\ s(p) \text{ even}\}$$

and

$$\Lambda = \{p \mid 2 \neq p \in \mathbb{P},\ s(p) \text{ odd}\}.$$

By a theorem of Hasse [5], we have $\delta_{Dir}(\Lambda) = 7/24$. This holds also true if we take only primes in $\mathcal{G}$ as we show in the next result.

Lemma 3.2 *We have*

$$\delta_{Dir}(\Lambda \cap \mathcal{G}) = 7/24.$$

In particular, there exists an infinite sequence of primes p with $s(p)$ odd and $r(p) \leq s(p)$.

Proof. By Lemma 3.1, we know that

$$\delta_{Dir}(\Lambda \cap \mathcal{B}) \leq \delta_{Dir}(\mathcal{B}) = 0.$$

Thus, together with Hasse's result, we obtain

$$\delta_{Dir}(\Lambda \cap \mathcal{G}) = \delta_{Dir}(\Lambda \cap \mathcal{G}) + \delta_{Dir}(\Lambda \cap \mathcal{B}) = \delta_{Dir}(\Lambda) = 7/24.$$

□

4 The asymptotic of self-dual doubly-even 2-quasi-cyclic codes

Throughout this section let $G = G_n$ be a cyclic group of order $n = 2^t m$ where $2 \nmid m$ and $s(m)$ is odd. Let $R = \mathbb{F}_2 G_n$ and let $U(R)$ denote the group of units in R.

Definition 4.1

a) We define

$$l(n) = l(m) = \min\{\dim M \mid M \text{ a simple non-trivial } R\text{-module}\}.$$

Note that $l(m) = \min\{s(p) \mid p \text{ a prime, } p \mid m\}$. In particular, $l(p) = s(p)$ for any odd prime p.

b) We put

$$D_l = \{a \mid a \in R,\ \dim Ra = l\}.$$

c) For any ideal I in R and $w \in \mathbb{N}_0$ we define

$$I^{(w)} = \{a \mid a \in I,\ \mathrm{wt}(a) = w\}.$$

d) If the underlaying group of $C_{a,b}$ in Lemma 2.1 is the cyclic group G_n we write $C_{a,b}^{(n)}$ for $C_{a,b}$ to indicate the cyclic group of order n.

Lemma 4.2 *With the notation as above we have.*

a) For any l, the size of D_l is bounded by

$$|D_l| \leq 2^{t(l/l(m)+1)+l} m^{l/l(m)}.$$

b) For any ideal I in R of dimension l we have

$$|I^{(w)}| \leq 2^{lH(w/m)}$$

where $H(x)$ denotes the binary entropy function, i.e.,

$$H(x) = -x \log_2 x - (1-x)\log_2(1-x) \quad (0 \leq x \leq 1).$$

Proof. a) Clearly $|D_l| \leq 2^l |I(l)|$ where

$$I(l) = \{I \mid I \text{ is a submodule of } R \text{ of dimension } l\}.$$

Now, let I be such a submodule of dimenson l. Remember that

$$R = Re_0 \oplus (Re_1 \oplus R\bar{e}_1) \oplus \ldots \oplus (Re_s \oplus R\bar{e}_s).$$

Thus we can write

$$I = Ie_0 \oplus (Ie_1 \oplus I\bar{e}_1) \oplus \ldots \oplus (Ie_s \oplus I\bar{e}_s)$$

where Ie_i is uniquely determined by its dimension since Re_i is uniserial. In other words, Ie_i is uniquely determined by the multiplicity of the simple module V_i in Ie_i as a composition factor. Therefore, if $l_i = \dim V_i$, then $|I(l)|$ is the number of solutions

$$l = \alpha_0 + l_1(\alpha_1 + \beta_1) + \ldots + l_s(\alpha_s + \beta_s)$$

with $0 \leq \alpha_i, \beta_i \leq 2^t$. If we have chosen α_0 the number of the remaining non-trivial modules is bounded by

$$(l - \alpha_0)/l(m) \leq l/l(m).$$

We may choose each non-trivial simple module at most 2^t times. Obviously, there are $2s \leq m$ non-trivial simple modules. Thus the number of choices is bounded by $2^t m$. This shows that

$$|I(l)| \leq 2^t (2^t m)^{l/l(m)},$$

hence

$$|D_l| \leq 2^{t+l} (2^t m)^{l/l(m)}.$$

b) This was already proved in [1]. $\square$

In order to prove that the class of binary self-dual doubly-even 2-quasi-cyclic codes is asymptotically good we first show a more general result. With suitable modifications its proof follows closely the ideas of the proof of Theorem 2.1 in [1].

Theorem 4.3 *Let (n) be a sequence of positive integers where $n = m2^t$ with $s(m)$ odd, (m) strictly increasing and $l(m) \gg \log m$. Furthermore assume that for all n the 2-part of n is bounded by $2 \leq t \leq c$. We put $R_n = \mathbb{F}_2 G_n$ and choose for each n at random a pair (a, b) in*

$$\Omega = \{(a, b) \in U(R_n) \times U(R_n) \mid a\bar{a} = b\bar{b},\ \mathrm{wt}(a) + \mathrm{wt}(b) \equiv 0 \bmod 4\}.$$

Then:

a) Each code $C_{a,b}^{(n)}$ is self-dual doubly-even 2-quasi-cyclic and transitive.

b) There exists a $\delta > 0$ such that the codes in the sequence $C_{a,b}^{(n)}$ have relative minimum distance

$$\frac{\mathrm{d}(C_{a,b}^{(n)})}{2n} \geq \delta$$

with a high probability that approaches 1 if $n \to \infty$.

Proof. Part a) follows imediately by the results of section 2. Thus it remains to prove b). To do so we fix some n and some small $\delta > 0$.

Let $R = \mathbb{F}_2 G_n$ and let $C_{a,b} = C_{a,b}^{(n)}$ for some $a, b \in \Omega$. Let P denote the probability that $\mathrm{d}(C_{a,b}) < 2n\delta$. Furthermore, for $f \in R$, let $E(f, a, b)$ be the event that

$$\mathrm{wt}(fa, fb) = \mathrm{wt}(fa) + \mathrm{wt}(fb) < 2n\delta \text{ and } (fa, fb) \neq (0, 0).$$

Let H_n resp. T_n be the subgroup of elements of odd order resp. the 2-Sylow subgroup of G_n and let $e_0 = \sum_{h \in H_n} h$. First we consider the case when $f \in Re_0$. Then $fa = y_1 e_0$ and $fb = y_2 e_0$ with $y_1, y_2 \in \mathbb{F}_2 T$. Thus $\mathrm{wt}(fa) = m\mathrm{wt}(y_1)$ and $\mathrm{wt}(fb) = m\mathrm{wt}(y_2)$. Therefore

$$\mathrm{wt}(fa, fb) = m(\mathrm{wt}(y_1) + \mathrm{wt}(y_2)) < 2n\delta = 2 \cdot 2^t m\delta$$

if and only if

$$\mathrm{wt}(y_1, y_2) = \mathrm{wt}(y_1) + \mathrm{wt}(y_2) < 2^{t+1}\delta.$$

This means that if we take $\delta < 2^{-c-1}$ then, for $f \in Re_0$, we get

$$\mathrm{Pr}_{(a,b) \in \Omega}(E(f, a, b)) = 0.$$

So we have

$$\begin{aligned}
P &\le \textstyle\sum_{f\notin Re_0} \Pr_{(a,b)\in\Omega}(E(f,a,b)) \\
&\le \textstyle\sum_{l=l(m)}^{n} |D_l| \max_{f\in D_l} \Pr_{(a,b)\in\Omega}(E(f,a,b)) \\
&\le \textstyle\sum_{l=l(m)}^{n} 2^{c(l/l(m)+1)+l} m^{l/l(m)} \max_{f\in D_l} \Pr_{(a,b)\in\Omega}(E(f,a,b)),
\end{aligned}$$

by Lemma 4.2 a).

Thus it remains to bound $\Pr_{(a,b)\in\Omega}(E(f,a,b))$. Here we get

$$\begin{aligned}
&\Pr_{(a,b)\in\Omega}(E(f,a,b)) \\
&\le \sum_{\substack{r_1,r_2\in fR \\ 0\le \mathrm{wt}(r_1)+\mathrm{wt}(r_2)<2n\delta}} \Pr_{(a,b)\in\Omega}(fa=r_1, fb=r_2) \\
&\le \max_{\substack{r_1,r_2\in fR \\ 0\le \mathrm{wt}(r_1)+\mathrm{wt}(r_2)<2n\delta}} \Pr_{(a,b)\in\Omega}(fa=r_1, fb=r_2) \sum_{\substack{w_1,w_2\ge 0 \\ w_1+w_2<2\delta n}} |I^{(w_1)}||I^{(w_2)}| \\
&\le \frac{2^{2^{c+1}}}{2^{5l/4}} \sum_{\substack{w_1,w_2\ge 0 \\ w_1+w_2<2\delta n}} |I^{(w_1)}||I^{(w_2)}| \qquad \text{(by Lemma 2.9)} \\
&\le \frac{2^{2^{c+1}}}{2^{5l/4}} \sum_{\substack{w_1,w_2\ge 0 \\ w_1+w_2<2\delta n}} 2^{l[H(w_1/n)+H(w_2/n)]} \qquad \text{(by Lemma 4.2)} \\
&\le \frac{2^{2^{c+1}}}{2^{5l/4}} \sum_{\substack{w_1,w_2\ge 0 \\ w_1+w_2<2\delta n}} 2^{2lH(\delta)} \qquad \text{(since } H \text{ is convex)} \\
&\le \frac{2^{2^{c+1}}}{2^{5l/4}} (2n\delta)^2 2^{2lH(\delta)}
\end{aligned}$$

Putting both parts together we obtain

$$\begin{aligned}
P &\le \textstyle\sum_{l=l(m)}^{n} 2^{c(l/l(m)+1)+l} m^{l/l(m)} \frac{2^{2^{c+1}}}{2^{5l/4}} (2n\delta)^2 2^{2lH(\delta)} \\
&= \delta^2 2^{2^{c+1}+c+2} \textstyle\sum_{l=l(m)}^{n} 2^{cl/l(m)+l} 2^{l/l(m)\log m} 2^{-5l/4} 2^{2\log n} 2^{2lH(\delta)} \\
&= \delta^2 2^{2^{c+1}+3c+2} \textstyle\sum_{l=l(m)}^{n} 2^{cl/l(m)+l} 2^{l/l(m)\log m} 2^{-5l/4} 2^{2\log m} 2^{2lH(\delta)} \\
&= \delta^2 2^{2^{c+1}+3c+2} \textstyle\sum_{l=l(m)}^{n} 2^{-2l[5/8-H(\delta)-\frac{\log m}{2l(m)}-\frac{c}{2l(m)}-\frac{1}{2}]+2\log m} \\
&= \delta^2 2^{2^{c+1}+3c+2} \textstyle\sum_{l=l(m)}^{n} 2^{-2l[1/8-H(\delta)-\frac{\log m+c}{2l(m)}]+2\log m}
\end{aligned}$$

Now we choose $0<\delta$ small enough and m large enough such that

$$1/8 - H(\delta) - \frac{\log m + c}{2l(m)} > 0.$$

Under these assumptions we obtain

$$\begin{aligned}
P &\le \delta^2 2^{2^{c+1}+4c+2} 2^{-2l(m)[1/8-H(\delta)-\frac{\log m+c}{2l(m)}]+3\log m} \\
&\le \delta^2 2^{2^{c+1}+5c+2} 2^{-2l(m)[1/8-H(\delta)]+4\log m}
\end{aligned}$$

which tends to 0 for $m \to \infty$ since $l(m) \gg \log m$. $\square$

Proof of Theorem 1.1
According to Theorem 4.3 we have to find a strictly increasing sequence of positive integers $(4m)$ with m odd, $s(m)$ odd and $l(m) \gg \log m$. For (m) we take the sequence (p) of primes we have found in Lemma 3.2. Then, obviously $l(p) = s(p)$ is odd. Furthermore, in Lemma 3.2, we may choose

$$r(n) = (\log n)^2 \ll \sqrt{n/\log n}.$$

Thus the sequence (p) satisfies

$$l(p) = s(p) \geq r(p) = (\log p)^2 \gg \log p$$

and we can apply Theorem 4.3 which proves the existence of an asymptotically good sequence of binary self-dual doubly-even 2-quasicyclic and transitive codes.

References

[1] L.M.J. Bazzi and S.K. Mitter. Some randomized code constructions from group actions. To appear *IEEE Trans. Inform. Theory.* `http://web.mit.edu/~mitter/www/publications/someconstructions.pdf`

[2] C.L. Chen, W.W. Peterson and E.J. Weldon. Some results on quasi-cyclic codes. *Inform. Contr.* **15**, pp. 407-423 (1969).

[3] B.K. Dey. On the existence of good self-dual quasi-cyclic codes. *IEEE Trans. Inform. Theory* **50**, pp. 1794-1798 (2004).

[4] G.H. Hardy and E.M. Wright. An Introduction to the Theory of Numbers. Oxford Science Publications, Fifth Edition 1994.

[5] H. Hasse. Über die Dichte der Primzahlen p, für die eine vorgegebene rationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod.p ist. *Math. Annalen* **166**, pp.19-23 (1966).

[6] B. Huppert and N. Blackburn. Finite Groups II. Springer Verlag 1982.

[7] T. Kasami. A Gilbert-Varshamov bound for quasi-cyclic codes of rate $\frac{1}{2}$. *IEEE Trans. Inform. Theory* **20**, p. 679 (1974).

[8] S. Ling and P. Solé. Good self-dual quasi-cyclic codes exist. *IEEE Trans. Inform. Theory* **49**, pp. 1052-1053 (2003).

[9] F.J.MacWilliams, N.J.A. Sloane and J.G. Thompson. Good self-dual codes exist. *Discrete Math.* **3**, pp. 153-162 (1972).

[10] C. Martínez-Pérez and W. Willems. Self-dual codes and modules for finite groups in characteristic two. *IEEE Trans. Inform. Theory* **50**, pp. 1798-1803 (2005).

[11] C. Martínez-Pérez and W. Willems. Is the class of cyclic codes asymptotically good? *IEEE Trans. Inform. Theory* **52**, pp. 696-700 (2006).

[12] H. Stichtenoth. Transitive and self-dual codes attaining the Tsfasman-Vladut-Zink bound. *IEEE Trans. Inform. Theory* **52**, pp. 2218-2224 (2006).

[13] W. Willems. Codierungstheorie, deGruyter, Berlin/New York 1999.