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

Conchita Martínez-Pérez and Wolfgang Willems

***Abstract*— We prove that the class of binary self-dual doubly-even 2-quasi-cyclic transitive codes is asymptotically good. This improves a recent result [1] of Bazzi and Mitter. The proof is based on the study of a particular class of codes invariant under dihedral groups using a bend of representation theory and probabilistic arguments. The methods are closely related to those used in [1]. In order to complete the proof a number theoretical result of Hasse is needed.**

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

## I. Introduction

It is a long standing question whether the class of cyclic codes is asymptotically good (see for instance [13]). 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. Under the assumption that 2 is primitive for infinitely many primes (Artin's conjecture) Chen, Peterson and Weldon [2] proved already in 1969 that 2-quasi-cyclic codes meet the Gilbert-Varshamov bound. Some years later Kasami showed in [9] that 2-quasi-cyclic codes always meet a bound which is slightly weaker than the Gilbert-Varshamov bound. Just recently Gaborit and Zemor improved in [4] Kasami's result by showing that 2-quasi-cyclic codes even achieve a bound better than the Gilbert-Varshamov bound. Furthermore, by a result of MacWilliams, Sloane and Thompson [11] the class of self-dual codes is asymptotically good. 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 $n$. Assuming Artin's conjecture 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. 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 shown by Stichtenoth [16] 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 investigated 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 considered 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 asymptotic behaviour is still open.

In this note we prove

**Theorem I.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]. As in the paper of Bazzi and Mitter the codes we are going to consider are also ideals in group algebras over dihedral groups, hence automatically 2-quasi-cyclic and transitive.

For the basics on self-dual codes we refer to the article [14] of Rains and Sloane in the Handbook of Coding Theory or [7]. The background in representation theory of finite groups may be taken from chapter VII of [8]. An introduction to the density of sets of primes is given in chapter VI, section 4, of [15].

## II. 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

Conchita Martínez-Pérez is with the Departamento de Matematáticas, Universidad de Zaragoza, 50009 Zaragoza, Spain (e-mail: conmar@unizar.es)

Wolfgang Willems is with the Institut für Algebra und Geometrie, Fakultät für Mathematik, Otto-von-Guericke Universität, 39016 Magdeburg, Germany (e-mail: wolfgang.willems@mathematik.uni-magdeburg.de)

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 II.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*

$$\mathrm{wt}(a) + \mathrm{wt}(b) \equiv 0 \bmod 4.$$

*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 ([7], Theorem 1.4.8), the code $C_{a,b}$ is doubly-even if and only if 4 divides $\mathrm{wt}(a) + \mathrm{wt}(b)$. ∎

**Lemma II.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 $\mathrm{wt}(a) + \mathrm{wt}(b) \equiv 0 \bmod 4$. By Lemma II.1 d), the code $C_{a,b}$ is doubly-even. Thus, by Gleason's Theorem ([7], 9.2.2 or [17], 3.3.22), 8 divides the length of $C_{a,b}$. Hence 8 divides $2|G|$ or equivalently 4 divides $|G|$. ∎

**Lemma II.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 $R = \mathbb{F}_2G$ and consider the left action of $D$ on $\mathbb{F}_2D = R \oplus Rt = R \times R$. 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 $a\bar{a} = b\bar{b}$. ∎

In order to construct self-dual doubly-even codes $C_{a,b}$ we need $4 \mid |G|$, by Lemma II.1 and Lemma II.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 guarantees 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 $R = \mathbb{F}_2 G$ are exactly the simple modules for $\mathbb{F}_2 H$ since $T$ acts trivially on all simple $R$-modules (see [8], Chap. VII, Theorem 13.4). The condition $s(|H|)$ odd implies, by ([12] Theorem 3.3), that the trivial $\mathbb{F}_2 H$-module is the only simple $\mathbb{F}_2 H$-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 [8], 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 $\mathbb{F}_2 H$ with mutually orthogonal primitive idempotents $e_i$. The principal block of $\mathbb{F}_2 H$ is $\mathbb{F}_2 H e_0 = \mathbb{F}_2 e_0$ 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

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

where $J$ denotes the Jacobson radical of $R$ and for all $k$ the factor module $P_i J^k / P_i J^{k+1} \cong V_i$ is the simple $R$-module, say of dimension $l_i$, corresponding to $e_i$ (see [8], Chap. VII, section 10 and Theorem 14.9). In particular, if $I$ is a submodule of $P_i$ then $I = P_i J^k$ 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,

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

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 II.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*

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

*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 $\alpha l_i$ we have $Rf = P_i J^{2^t - \alpha}$. If $a, b \in P_i$ with $af = bf = r$ then $(a - b)f = 0$. Therefore $a - b$ can be chosen as any element in the kernel of the map $P_i \to P_i$ defined by $c \mapsto cf$. Counting dimensions we see that this kernel is exactly $P_i J^\alpha$ from which the assertion follows. ∎

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

**Lemma II.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 II.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 II.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 $\mathrm{wt}(be_i)$. Next observe that for $i \geq 1$ and $r, r' \in R$ we have

$$\langle re_i, r' e_i \rangle = \langle re_i \bar{e}_i, r' \rangle = \langle 0, r' \rangle = 0$$

since $e_i \bar{e}_i = 0$. Hence $Re_i \subseteq (Re_i)^\perp$ for $i \geq 1$ and we get

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

Thus

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

for all $i \geq 1$. According to Lemma II.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 II.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

$$\omega = |\{(y_1,y_2) \mid y_1,y_2 \in U(\mathbb{F}_2T),\ y_1\bar{y}_1 = y_2\bar{y}_2,\ \mathrm{wt}(y_1)+\mathrm{wt}(y_2) \equiv 0 \bmod 4\}|.$$

**Lemma II.8** *The size of $\Omega$ is*

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

*Proof:* For units $a,b$ with $a\bar{a} = b\bar{b}$ consider the unique units $y_1, y_2 \in \mathbb{F}_2T$ with $ae_0 = y_1e_0$ and $be_0 = y_2e_0$. Then $y_1\bar{y}_1 = y_2\bar{y}_2$ and in addition, by Lemma II.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

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

Applying Lemma II.4 a) we obtain

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

■

**Lemma II.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

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

Let $l_i$ be the dimension of the simple module corresponding to $Re_i$. If $\alpha_i l_i = \dim Rfe_i$ and $\beta_i l_i = \dim Rf\bar{e}_i$ for $i = 1,\ldots,s$ then

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

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

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

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 II.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

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

Remember, by the beginning of the proof of Lemma II.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 $ae_0 = y_1e_0$, $be_0 = y_2e_0$ with unique $y_1, y_2 \in \mathbb{F}_2T$. Furthermore, the number of possible 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 $\omega$ in Definition II.7.

Since $\sum_{i=1}^{s}(\alpha_i+\beta_i)l_i = l-\alpha_0$ and $2\sum_{i=1}^{s}\gamma_i l_i \geq l-\alpha_0$ we have

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

Finally, taking Lemma II.8 into acount for $|\Omega|$, we obtain

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

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

## III. The asymptotic of self-dual doubly-even 2-quasi-cyclic codes

In this section we shall prove our main result Theorem I.1. Throughout let $G = G_n$ be a cyclic group of order $n = 4p$ where $p$ is an odd prime with $s(p)$ odd. Let $R = \mathbb{F}_2 G_n$ and let $U(R)$ denote the group of units in $R$. Note that $s(p)$ is the dimension of any non-trivial simple $R$-module.

**Definition III.1**

a) For $l \in \mathbb{N}_0$ we put

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

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

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

c) If the underlying group of $C_{a,b}$ in Lemma II.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 III.2** *With the notation as above we have.*

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

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

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

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

*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, as $s(p) = \dim V_i$ for $V_i$ non-trivial, $|I(l)|$ is the number of solutions

$$l = \alpha_0 + s(p)(\alpha_1+\beta_1) + \ldots + s(p)(\alpha_s+\beta_s)$$

with $0 \leq \alpha_i, \beta_i \leq 4$. If we have chosen $\alpha_0$ the number of the remaining non-trivial modules is bounded by

$$(l-\alpha_0)/s(p) \leq l/s(p).$$

We may choose each non-trivial simple module at most $4$ times. Obviously, there are $2s \leq p$ non-trivial simple modules. Thus the number of choices is bounded by $4p$. This shows that

$$|I(l)| \leq 2^2(2^2p)^{l/s(p)},$$

hence

$$|D_l| \leq 2^{2+l}(2^2p)^{l/s(p)}.$$

b) This was already proved in ([1], Lemma 2.2). ■

In order to prove that the class of binary self-dual doubly-even 2-quasi-cyclic and transitive codes is asymptotically good we use suitable modifications of ideas of the proof of Theorem 2.1 in [1].

**Theorem III.3** *Let $(n)$ be a sequence of positive integers where $n = 4p$ with $p$ an odd prime and $s(p)$ odd, $(p)$ strictly increasing and $s(p) \gg \log p$. 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 for $n$ large enough 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 immediately by the results of section 2. Thus it remains to prove b). To do so we fix some $n$ and some small $\delta > 0$.

As above we set $R = \mathbb{F}_2 G_n$ and $C_{a,b} = C_{a,b}^{(n)}$ 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

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

Finally, by $H_n$ resp. $T_n$ we denote the subgroup of elements of odd order, which is of order $p$, resp. the 2-Sylow subgroup of $G_n$, which has order 4. We put $e_0 = \sum_{h \in H_n} h$. First we consider the case that $f \in Re_0$. Then $fa = y_1 e_0$ and $fb = y_2 e_0$ with $y_1, y_2 \in \mathbb{F}_2 T$. Thus $\mathrm{wt}(fa) = p\mathrm{wt}(y_1)$ and $\mathrm{wt}(fb) = p\mathrm{wt}(y_2)$. Therefore

$$\mathrm{wt}(fa, fb) = p(\mathrm{wt}(y_1) + \mathrm{wt}(y_2)) < 2n\delta = 8p\delta$$

if and only if

$$\mathrm{wt}(y_1, y_2) = \mathrm{wt}(y_1) + \mathrm{wt}(y_2) < 8\delta.$$

This means that if we take $\delta < 2^{-3}$ then, for $f \in Re_0$, we get

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

So, by Lemma III.2 a), we have

$$\begin{aligned} P &\leq \textstyle\sum_{f \notin Re_0} \mathrm{Pr}_{(a,b)\in\Omega}(E(f,a,b)) \\ &\leq \textstyle\sum_{l=s(p)}^{n} |D_l| \max_{f\in D_l} \mathrm{Pr}_{(a,b)\in\Omega}(E(f,a,b)) \\ &\leq \textstyle\sum_{l=s(p)}^{n} 2^{2(l/s(p)+1)+l} p^{l/s(p)} M \end{aligned}$$

where $M = \max_{f\in D_l} \mathrm{Pr}_{(a,b)\in\Omega}(E(f,a,b))$.

Thus it remains to bound $M$. Here we get for $l$ fixed

$$\begin{aligned} &\mathrm{Pr}_{(a,b)\in\Omega}(E(f,a,b)) \\ &\leq \sum_{\substack{r_1,r_2 \in fR \\ \mathrm{wt}(r_1)+\mathrm{wt}(r_2)<2n\delta}} \mathrm{Pr}_{(a,b)\in\Omega}(fa = r_1, fb = r_2) \\ &\leq \max_{\substack{r_1,r_2 \in fR \\ \mathrm{wt}(r_1)+\mathrm{wt}(r_2)<2n\delta}} \mathrm{Pr}_{(a,b)\in\Omega}(fa = r_1, fb = r_2) \cdot \\ &\qquad \sum_{\substack{w_1,w_2 \geq 0 \\ w_1+w_2<2\delta n}} |I^{(w_1)}||I^{(w_2)}| \\ &\leq \tfrac{2^8}{2^{5l/4}} \sum_{\substack{w_1,w_2 \geq 0 \\ w_1+w_2<2\delta n}} |I^{(w_1)}||I^{(w_2)}| \quad \text{(by Lemma } II.9,\ t=2) \\ &\leq \tfrac{2^8}{2^{5l/4}} \sum_{\substack{w_1,w_2 \geq 0 \\ w_1+w_2<2\delta n}} 2^{l[H(w_1/p)+H(w_2/p)]} \text{ (by Lemma } III.2) \\ &\leq \tfrac{2^8}{2^{5l/4}} \sum_{\substack{w_1,w_2 \geq 0 \\ w_1+w_2<2\delta n}} 2^{2lH(\delta)} \qquad \text{(since } H \text{ is convex)} \\ &\leq \tfrac{2^8}{2^{5l/4}} (2n\delta)^2 2^{2lH(\delta)} \end{aligned}$$

Putting both parts together we obtain

$$\begin{aligned} P &\leq \textstyle\sum_{l=s(p)}^{n} 2^{2(l/s(p)+1)+l} p^{l/s(p)} \tfrac{2^8}{2^{5l/4}} (2n\delta)^2 2^{2lH(\delta)} \\ &= \delta^2 2^{12} \cdot \textstyle\sum_{l=s(p)}^{n} 2^{2l/s(p)+l} 2^{l/s(p)\log p} 2^{-5l/4} 2^{2\log n} 2^{2lH(\delta)} \\ &= \delta^2 2^{16} \cdot \textstyle\sum_{l=s(p)}^{n} 2^{2l/s(p)+l} 2^{l/s(p)\log p} 2^{-5l/4} 2^{2\log p} 2^{2lH(\delta)} \\ &= \delta^2 2^{16} \cdot \textstyle\sum_{l=s(p)}^{n} 2^{-2l[5/8-H(\delta)-\frac{\log p}{2s(p)}-\frac{2}{2s(p)}-\frac{1}{2}]+2\log p} \\ &= \delta^2 2^{16} \textstyle\sum_{l=s(p)}^{n} 2^{-2l[1/8-H(\delta)-\frac{\log p+2}{2s(p)}]+2\log p} \end{aligned}$$

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

$$1/8 - H(\delta) - \frac{\log p + 2}{2s(p)} > 0.$$

Under these assumptions we obtain

$$\begin{aligned} P &\leq \delta^2 2^{18} 2^{-2s(p)[1/8-H(\delta)-\frac{\log p+2}{2s(p)}]+3\log p} \\ &\leq \delta^2 2^{20} 2^{-2s(p)[1/8-H(\delta)]+4\log p} \end{aligned}$$

which tends to 0 for $p \to \infty$ since $s(p) \gg \log p$. ∎

**Remark III.4** For $n$ large enough the relative minimum distance $\delta$ given in Theorem III.3 has to satisfy $\delta < 1/8$ and $H(\delta) < 1/8$. Here we may choose $\delta = 0.017$.

**Proof of Theorem I.1**
According to Theorem III.3 we have to find a strictly increasing sequence $(p)$ of odd primes $p$ with $s(p)$ odd and $s(p) \gg \log p$. In the next section we prove the existence of such a sequence (see Proposition IV.3). Thus Theorem III.3 proves the existence of an asymptotically good sequence of binary self-dual doubly-even 2-quasicyclic and transitive codes.

## IV. The density of some set of primes

This section is devoted to the density of a particular set of primes. Our aim is to prove the existence of a sequence $(p)$ of primes $p$ where $s(p)$ is odd and $s(p)$ grows much faster than $\log p$ which completes the proof of the main result.

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

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

and

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

**Lemma IV.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

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

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

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

By the Prime Number Theorem (see for instance [5]), 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 [6], 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 IV.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 $r(p) \le s(p)$.*

*Proof:* By Lemma IV.1, we know that

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

Thus, together with Hasse's result, we obtain

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

∎

**Proposition IV.3** *There exists a strictly increasing sequence $(p)$ of odd primes $p$ with $s(p)$ odd and $s(p) \gg \log p$.*

*Proof:* In Lemma IV.2 we may choose

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

Thus the sequence $(p)$ satisfies $s(p)$ odd and

$$s(p) \ge r(p) = (\log p)^2 \gg \log p.$$

∎

## REFERENCES


[1] L.M.J. BAZZI AND S.K. MITTER. Some randomized code constructions from group actions. *IEEE Trans. Inform. Theory* **52**, pp. 3210-3219 (2006).

[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] P. GABORIT AND G. ZEMOR. Asymptotic improvement of the Gilbert-Varshamov bound for binary linear codes. Proceed. ISIT 2006, Seattle, July 9-14, 287-291 (2006).

[5] G.H. HARDY AND E.M. WRIGHT. An Introduction to the Theory of Numbers. Oxford Science Publications, Fifth Edition 1994.

[6] 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).

[7] W.C. HUFFMANN AND V. PLESS. Fundamentals of error correcting codes. Cambridge University Press 2003.

[8] B. HUPPERT AND N. BLACKBURN. Finite Groups II. Springer Verlag, Berlin 1982.

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

[10] S. LING AND P. SOLÉ. Good self-dual quasi-cyclic codes exist. *IEEE Trans. Inform. Theory* **49**, pp. 1052-1053 (2003).

[11] F.J.MACWILLIAMS, N.J.A. SLOANE AND J.G. THOMPSON. Good self-dual codes exist. *Discrete Math.* **3**, pp. 153-162 (1972).

[12] 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).

[13] C. MARTÍNEZ-PÉREZ AND W. WILLEMS. Is the class of cyclic codes asymptotically good? *IEEE Trans. Inform. Theory* **52**, pp. 696-700 (2006).

[14] E.M. RAINS AND N.J.A. SLOANE. Self-dual codes. In: Handbook of Coding Theory, Vol. 1, Ed. V.S. Pless and W.C. Huffman, Elsevier, Amsterdam 1998.

[15] J.P. SERRE. A course in arithmetic. Springer Verlag, New York 1973.

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

[17] W. WILLEMS. Codierungstheorie, deGruyter, Berlin/New York 1999.


**Conchita Martínez-Pérez** Conchita Martínez-Pérez received the PhD degree in mathematics from the University of Zaragoza, Zaragoza, Spain, in 1999. Since 1995, she has been with the Department of Mathematics at the University of Zaragoza. At the beginning of 2000, she was with the Department of Mathematics, University of Magdeburg, Magdeburg, Germany, for four months, and from 2000 to 2001, she was with the Department of Mathematics, ETH, Zürich, Switzerland. Since 2004, she has been Professor at the University of Zaragoza. Her research areas of interest are algebraic coding theory, representation theory of finite groups, and cohomology of groups.

**Wolfgang Willems** Wolfgang Willems (M'00) received the Diploma in 1974 and the Ph.D. degree in 1977, both in mathematics, and from the Johannes-Gutenberg University, Mainz, Germany. From 1974 to 1998, he was mainly with the Department of Mathematics, the University of Mainz. He spent 1986-1987 and 1989-1991 as Visiting Professor at the University of Essen, Germany and the Institute of Experimental Mathematics, Essen. 1996 he was Acting Professor at the Otto-von-Guericke University, Magdeburg, Germany. Since 1998, he has been Professor for 'Pure Mathematics' at the University of Magdeburg. His primary research interests are algebraic coding theory and representation theory of finite groups.