Dihedral Codes with Prescribed Minimum Distance

Martino Borello, Abdelillah Jamous

Dihedral codes with prescribed minimum distance

Martino Borello[1] and Abdelillah Jamous[2]

[1] Université Paris 8, Laboratoire de Géométrie, Analyse et Applications, LAGA, Université Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France
[2] Faculty of Mathematics, University of Sciences and Technology Houari Boumediene, Algiers, Algeria

Abstract. Dihedral codes, particular cases of quasi-cyclic codes, have a nice algebraic structure which allows to store them efficiently. In this paper, we investigate it and prove some lower bounds on their dimension and minimum distance, in analogy with the theory of BCH codes. This allows us to construct dihedral codes with prescribed minimum distance. In the binary case, we present some examples of optimal dihedral codes obtained by this construction.

Keywords: Group Algebras · Dihedral codes · BCH bound.

1 Introduction

Block codes were invented in the forties to correct errors in the communication through noisy channels (see [18] for more details), and they are used nowadays in different areas of information security. Originally, they were thought just as subsets of (code)words of n letters chosen in an alphabet K, which are far enough apart from each other with respect to the Hamming distance. However, they usually need to have more algebraic structure to be stored efficiently. By considering *linear codes* of length n over a finite field K, that is subspaces of the vector space K^n, we have a compact description given, for example, by the *parity check matrix*, which is a matrix H such that $c \in \mathcal{C}$ if and only if $cH = 0$. Such a description reduces exponentially the size of the data to be stored with respect to general block codes. However, this reduction reveals to be insufficient in the context of code-based cryptography ([20,24] and many others), where the public key is related to the parity check matrix of a code of large length and dimension. The size of the public key constitutes one of the main practical disadvantages in the use of code-based cryptography and many efforts have been done to reduce it by preserving the security of the system. One option may be to use codes with symmetries, like cyclic or quasi-cyclic codes (see for example [3]). However, since decoding of general quasi-cyclic codes is difficult, the algebraic structure that one needs to add may also reveal to be a weakness of the system (see for example [14]).

A natural generalisation of cyclic codes is given by the family of group codes: a linear code $\mathcal{C}$ is called a *G-code* (or a group code) if $\mathcal{C}$ is a right (or left) ideal

in the group algebra $KG = \{a = \sum_{g \in G} a_g g \mid a_g \in G\}$ where G is a finite group. Reed Muller codes over prime fields $\mathbb{F}_p$ are group codes for an elementary abelian p-group G [4,10], and there are many other remarkable optimal codes which have been detected as group codes [5,12,15,21]. If G is cyclic, then all right (or left) ideals of KG afford only one check equation (and then only a few data have to be stored). In the case G is a general finite group there are only particular right (or left) ideals which satisfy this property, called *checkable* codes [19]. In [6] it is proved that such codes are the duals of principal ideals and group algebras KG for which all right (or left) ideals are checkable (or equivalently principal), called *code-checkable group algebras*, are characterised: KG is a code-checkable group algebra if and only if G is p-nilpotent with a cyclic Sylow p-subgroup, where p is the characteristic of K. This is a consequence of an early result by Passman ([25, Theorem 4.1]). Checkable codes are asymptotically good [2,7] and many optimal codes are checkable [6, Remark 2.9]. This seems to suggest that the family of checkable codes is worth further investigation. In particular, it is desirable to prove some bounds on the dimension and minimum distance for checkable codes and to introduce families of checkable or principal codes with prescribed minimum distance (in analogy with BCH codes).

To our knowledge, there are very few results concerning the parameters of group codes, both for general and particular groups. In [13], an algorithm for computing the dimension of general group codes is given. In a very recent paper [11], several relations and bounds for the dimension of principal ideals in group algebras are determined by analysing minimal polynomials of regular representations. The concatenated structure of dihedral codes is investigated in [9]. However, we are not aware of results which allow to construct group codes with a prescribed minimum distance or explicit lower bounds on both dimension and minimum distance, even in the easiest case of dihedral codes. This paper wants to be a first contribution in this direction. In §2 we will recall some results of the theory of quasi-cyclic codes. In §3 we will recall the definition of dihedral codes, present some results about their algebraic structure, make some remarks about the dual codes, prove a BCH bound for principal dihedral codes, propose a definition of principal BCH-dihedral codes, consider the particular case of binary dihedral codes and give some construction of optimal codes. Finally, in §4 we will present some open problems. In particular, an efficient decoding algorithm would be a necessary prerequisite for applications in cryptography.

2 Quasi-cyclic codes

We recall in this section some definitions and known results about quasi-cyclic codes. As we will see in the next section, dihedral codes, as all group codes, form a subfamily of quasi-cyclic codes.

Let q be a power of a prime and $\mathbb{F}_q$ the finite field with q elements. Let $n \in \mathbb{N}$. The symmetric group S_n acts on the vector space $\mathbb{F}_q^n$ as follows:

$$v^\sigma := (v_{\sigma^{-1}(1)}, v_{\sigma^{-1}(2)}, \dots, v_{\sigma^{-1}(n)})$$

for $v := (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$ and $\sigma \in S_n$. For a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$, the set of permutations such that $\mathcal{C}^\sigma := \{c^\sigma \mid c \in \mathcal{C}\}$ is equal to $\mathcal{C}$ is a group which is called the *permutation automorphism group* of $\mathcal{C}$ and which is denoted by $\mathrm{PAut}(\mathcal{C})$.

In this context, a remarkable transformation is the so-called *shift map*, that is

$$T_n : \mathbb{F}_q^n \to \mathbb{F}_q^n \qquad c \mapsto c^{(1\ \ldots\ n)} = (c_n, c_1, \ldots, c_{n-1}).$$

Linear codes which are invariant under the shift or its power are the so-called quasi-cyclic codes.

Definition 1. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear code. Suppose that $n = \ell m$, for some positive integers ℓ and m. The code $\mathcal{C}$ is* quasi-cyclic *of index ℓ if $T_n^\ell(\mathcal{C}) = \mathcal{C}$, that is if*

$$(1\ \ldots\ n)^\ell = \prod_{j=1}^{\ell} (j\ \ell + j\ 2\ell + j\ \ldots\ (m-1)\ell + j) \in \mathrm{PAut}(\mathcal{C}).$$

If $\ell = 1$, the code $\mathcal{C}$ is called cyclic.

Let $R := \mathbb{F}_q[x]/(x^m - 1)$. We may relabel the coordinates and consider the bijective $\mathbb{F}_q$-linear map

$$\varphi : \mathbb{F}_q^n = (\mathbb{F}_q^\ell)^m \to R^\ell \tag{1}$$

$$(c_{11}, \ldots, c_{1\ell}, \ldots, c_{m1}, \ldots, c_{m\ell}) \mapsto (c_{11} + \cdots + c_{m1}x^{m-1}, \ldots, c_{1\ell} + \cdots + c_{m\ell}x^{m-1}).$$

The image of a quasi-cyclic code in R^ℓ is an R-submodule. Actually, the multiplication by x corresponds to the ℓ-th power of the shift.

Remark 1. There is a one-to-one correspondence between the R-submodules of R^ℓ and left ideals of $\mathrm{Mat}_\ell(R)$ (which is isomorphic, as a ring, to $\mathrm{Mat}_\ell(\mathbb{F}_q)[x]/(x^m - 1)$). This is a particular case of the Morita equivalence for modules [23]. The explicit one-to-one map is given as follows: to any R-submodule N of R^ℓ we associate the left ideal $\mathcal{I}_N$ of $\mathrm{Mat}_\ell(R)$ composed by matrices whose rows are elements in N. As already observed in [1], since R is a commutative principal ideal ring, every R-submodule N of R^ℓ has at most ℓ generators, so that the left ideal $\mathcal{I}_N$ is principal (it suffices to consider the matrix whose rows are the generators and eventually some zeros). So there exists a generator of $\mathcal{I}_N$ which can be seen a polynomial in $\mathrm{Mat}_\ell(\mathbb{F}_q)[x]/(x^m - 1)$.

Let ℓ be a positive integer, and $\alpha \in \mathbb{F}_{q^\ell}$ be a primitive element of $\mathbb{F}_{q^\ell}/\mathbb{F}_q$. Recall that $\{1, \alpha, \ldots, \alpha^{\ell-1}\}$ is an $\mathbb{F}_q$-base of the vector space $\mathbb{F}_{q^\ell}$. The *folding* is the $\mathbb{F}_q$-linear map

$$\begin{aligned} \phi : \mathbb{F}_q^\ell &\to \mathbb{F}_{q^\ell} = \mathbb{F}_q[\alpha] \\ (a_1, \ldots, a_\ell) &\mapsto a_1 + a_2\alpha + \cdots + a_\ell\alpha^{\ell-1}. \end{aligned}$$

Definition 2. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n = (\mathbb{F}_q^\ell)^m$ be a linear code. The* folded code *of $\mathcal{C}$ is $\mathcal{C}' = \phi^m(\mathcal{C}) \subseteq (\mathbb{F}_{q^\ell})^m$. In this case, $\mathcal{C}$ is the* unfolded code *of $\mathcal{C}'$.*

Remark 2. Note that the folded code $\mathcal{C}'$ of a linear code $\mathcal{C}$ is an $\mathbb{F}_q$-linear code. Moreover, $\mathcal{C}$ is quasi-cyclic if and only if $\mathcal{C}'$ is invariant under the shift T_m.

In the next section we will use the above equivalence and the following definition many times.

Definition 3. *An $\mathbb{F}_q$-linear code $\mathcal{C} \subseteq (\mathbb{F}_{q^\ell})^m$ which is invariant under the shift T_m is called* $\mathbb{F}_q$-linear cyclic code.

Barbier *et al.* define in [1] the analogue of BCH codes in the quasi-cyclic case. They call them *quasi-BCH* codes. In [16], the algebraic structure of $\mathbb{F}_q$-linear cyclic codes over $\mathbb{F}_{q^\ell}$ is studied. In next section we will explore the same concepts in the context of dihedral codes.

3 Dihedral codes

Let $m \geq 3$ be an integer and

$$D_{2m} := \langle \alpha, \beta \mid \alpha^m = 1, \beta^2 = 1, \beta\alpha = \alpha^{m-1}\beta \rangle,$$

be the *dihedral group* of order $2m$. The *group algebra* $\mathbb{F}_q D_{2m}$ is the set

$$\mathbb{F}_q D_{2m} := \left\{ \sum_{\gamma \in D_{2m}} a_\gamma \gamma \;\middle|\; a_\gamma \in \mathbb{F}_q \right\},$$

which is vector space over $\mathbb{F}_q$ with canonical basis $\{\gamma\}_{\gamma \in D_{2m}}$. The operations of sum and multiplication by scalars are defined in the following natural way: for any $a_\gamma, b_\gamma \in \mathbb{F}_q$ and $c \in \mathbb{F}_q$

$$\sum_{\gamma \in D_{2m}} a_\gamma \gamma + \sum_{\gamma \in D_{2m}} b_\gamma \gamma = \sum_{\gamma \in D_{2m}} (a_\gamma + b_\gamma)\gamma,$$

$$c \cdot \left(\sum_{\gamma \in D_{2m}} a_\gamma \gamma \right) = \sum_{\gamma \in D_{2m}} c a_\gamma \gamma.$$

Moreover, $\mathbb{F}_q D_{2m}$ is an algebra with the product

$$\left(\sum_{\gamma \in D_{2m}} a_\gamma \gamma \right) \bullet \left(\sum_{\gamma \in D_{2m}} b_\gamma \gamma \right) = \sum_{\gamma \in D_{2m}} \left(\sum_{\mu\nu = \gamma} a_\mu b_\nu \right) \gamma.$$

Definition 4. *A* dihedral code*, or a D_{2m}-code, is a left ideal of $\mathbb{F}_q D_{2m}$.*

As observed in [8], a linear code of length $2m$ can be seen as a D_{2m}-code if and only if its automorphism group contains a subgroup isomorphic to D_{2m} all

of whose nontrivial elements act fixed point free on the coordinates $\{1, \dots, 2m\}$. In particular, if we consider the ordering

$$D_{2m} = \{\underbrace{1}_{b_1}, \underbrace{\beta}_{b_2}, \underbrace{\alpha}_{b_3}, \underbrace{\alpha\beta}_{b_4}, \underbrace{\alpha^2}_{b_5}, \underbrace{\alpha^2\beta}_{b_6}, \dots, \underbrace{\alpha^{m-1}}_{b_{2m-1}}, \underbrace{\alpha^{m-1}\beta}_{b_{2m}}\}, \tag{2}$$

and the $\mathbb{F}_q$-linear isomorphism between $\mathbb{F}_q^{2m}$ and $\mathbb{F}_q D_{2m}$ given by $e_i \mapsto b_i$ (where $\{e_i\}$ is the canonical basis of $\mathbb{F}_q^{2m}$), a linear code $\mathcal{C} \subseteq \mathbb{F}_q^{2m}$ is a D_{2m}-code if and only if

$$\alpha' := (1\ 3\ 5\ \dots\ 2m-1)(2\ 4\ 6\ \dots\ 2m)$$

and

$$\beta' := (1\ 2)(3\ 2m)(4\ 2m-1)(5\ 2m-2)\cdots(m+1\ m+2)$$

are in $\mathrm{PAut}(\mathcal{C})$. These elements correspond to the permutation representation of the left multiplication by α and by β respectively in $\mathbb{F}_q D_{2m}$. In particular, since $\alpha' = (1\ \dots\ 2m)^2$, a dihedral code is a quasi-cyclic code of index 2.

From now on, we will always consider the ordering (2) fixed and we will identify $\mathbb{F}_q^{2m}$ and $\mathbb{F}_q D_{2m}$.

3.1 Algebraic structure

Let $\mathcal{C}$ be a D_{2m}-code over $\mathbb{F}_q$. As we observed above, since $\mathcal{C}$ is a quasi-cyclic codes of index 2, $\mathcal{C}$ is a free left module of rank 2 over $R := \mathbb{F}_q[x]/(x^m - 1)$, which is a commutative principal ideal ring. As we have already seen in Remark 1, this means that $\mathcal{C}$ has at most two generators as a module over R. These are also two generators of $\mathcal{C}$ viewed as an ideal in $\mathbb{F}_q D_{2m}$. We have one generator of $\mathcal{C}$ as an ideal in $\mathrm{Mat}_2(\mathbb{F}_q)[x]/(x^m - 1)$, given by the polynomial with coefficients in the ring of matrices with first row given by the first generator and second row given by the second one. However, it may happen that $\mathcal{C}$ is not principal as an ideal in $\mathbb{F}_q D_{2m}$.

Remark 3. As observed in [6], an early result by Passman ([25, Theorem 4.1]) gives us that all D_{2m}-codes over a field $\mathbb{F}_q$ of characteristic p if and only if D_{2m} is p-nilpotent with a cyclic Sylow p-subgroup (we recall that a group G is p-nilpotent if it admits a normal subgroup N of order coprime with p and such that G/N is a p-group). This is the case if and only if p does not divide m. So

- if $(m, q) = 1$, all D_{2m}-codes over $\mathbb{F}_q$ are principal;
- otherwise, a D_{2m}-code over $\mathbb{F}_q$ is either principal or the sum of two principal ideals.

We will study then the algebraic structure of principal left ideals in $\mathbb{F}_q D_{2m}$, that is principal dihedral codes. Via the map φ defined as in (1), we can consider $\varphi(\mathcal{C})$ inside R^2. The automorphism α' corresponds to the multiplication by x in R^2, whereas the automorphism β' acts on R^2 as follows: for $(a(x), b(x)) \in R^2$,

$$(a(x), b(x))^{\beta'} = (b(x^{m-1}), a(x^{m-1})).$$

So, $\mathcal{C}$ is a D_{2m}-code if and only if $\varphi(\mathcal{C})$ is an R-submodule of R^2 invariant under the action of β', that is such that $(b(x^{m-1}), a(x^{m-1})) \in \varphi(\mathcal{C})$ for all $(a(x), b(x)) \in \varphi(\mathcal{C})$.

If $\mathcal{C}$ is principal, then $\varphi(\mathcal{C})$ is an R-submodule of R^2 generated, as a module, by

$$(a(x), b(x)) \quad \text{and} \quad (b(x^{m-1}), a(x^{m-1})).$$

Remark 4. We have already mentioned the Morita correspondence between R-submodules and left ideals in $\mathrm{Mat}_2(R) \cong \mathrm{Mat}_2(\mathbb{F}_q)[x]/(x^m-1)$. In this case, the left ideal $I_{\mathcal{C}} \subseteq \mathrm{Mat}_2(\mathbb{F}_q)[x]/(x^m-1)$ associated to $\mathcal{C}$ is the principal ideal

$$I_{\mathcal{C}} = \left\langle \begin{pmatrix} a_0 & b_0 \\ b_0 & a_0 \end{pmatrix} + \begin{pmatrix} a_1 & b_1 \\ b_{m-1} & a_{m-1} \end{pmatrix} x + \cdots + \begin{pmatrix} a_{m-1} & b_{m-1} \\ b_1 & a_1 \end{pmatrix} x^{m-1} \right\rangle,$$

where $a(x) := a_0 + a_1 x + \ldots + a_{m-1}x^{m-1}$ and $b(x) := b_0 + b_1 x + \ldots + b_{m-1}x^{m-1}$.

Considering the folding $(\mathbb{F}_q)^2 \to \mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$, we can see the two polynomials $a(x), b(x)$ as a unique polynomial over $\mathbb{F}_{q^2}$ as

$$p(x) := (a_0 + b_0\alpha) + (a_1 + b_1\alpha)x + \ldots + (a_{m-1} + b_{m-1}\alpha)x^{m-1}$$

so that a principal dihedral code can be seen as the sum of the two $\mathbb{F}_q$-linear cyclic codes over $\mathbb{F}_{q^2}$, that is the one generated by $p(x)$ and the one generated by $\overline{p}(x^{m-1})$, where

$$\overline{p}(x) := (b_0 + a_0\alpha) + (b_1 + a_1\alpha)x + \ldots + (b_{m-1} + a_{m-1}\alpha)x^{m-1}.$$

The $\mathbb{F}_q$-linear map $\tau := a + b\alpha \mapsto \overline{\tau} := b + a\alpha$ can be expressed by the following linearised polynomial:

$$\tau \mapsto L(\tau) := \left(\frac{1-\alpha^2}{\alpha^q - \alpha}\right)\tau^q + \left(\frac{\alpha^{q+1}-1}{\alpha^q-\alpha}\right)\tau.$$

so that, if

$$p(x) := \tau_0 + \tau_1 x + \ldots + \tau_{m-1}x^{m-1},$$

we have

$$\overline{p}(x) = \overline{\tau_0} + \overline{\tau_1}x + \ldots + \overline{\tau_{m-1}}x^{m-1} =$$
$$\left(\frac{1-\alpha^2}{\alpha^q - \alpha}\right) p(x^{1/q})^q + \left(\frac{\alpha^{q+1}-1}{\alpha^q-\alpha}\right) p(x).$$

Definition 5. *For a polynomial $r(x) \in \mathbb{F}_{q^2}[x]/(x^m-1)$, we denote by $\langle r(x)\rangle_{\mathbb{F}_q}$ the unfolded $\mathbb{F}_q$-linear cyclic code generated by $r(x)$, i.e. the unfolded of*

$$\{t(x)r(x) \in \mathbb{F}_{q^2}[x]/(x^m-1) \mid t(x) \in \mathbb{F}_q[x]\}.$$

We can resume all the discussion in the following.

Theorem 1. *Let $\mathbb{F}_{q^2} = \mathbb{F}_q[\alpha]$ and $\mathcal{C}$ be a principal D_{2m}-code over $\mathbb{F}_q$. It exists $p(x) \in \mathbb{F}_{q^2}[x]/(x^m - 1)$ such that*

$$\mathcal{C} = \langle p(x) \rangle_{\mathbb{F}_q} + \langle \overline{p}(x^{m-1}) \rangle_{\mathbb{F}_q},$$

where

$$\overline{p}(x^{m-1}) = \left(\frac{1-\alpha^2}{\alpha^q - \alpha}\right) p(x^{(m-1)/q})^q + \left(\frac{\alpha^{q+1}-1}{\alpha^q - \alpha}\right) p(x^{m-1}) \in \mathbb{F}_{q^2}[x]/(x^m - 1).$$

In particular, as we have already observed in Remark 3, all D_{2m}-codes over $\mathbb{F}_q$ are principal if $(m, q) = 1$ and they are a sum of at most two principal D_{2m}-codes otherwise.

Definition 6. *We call the polynomial $p(x)$ a* generator *of the principal dihedral code.*

Corollary 1. *Let $\mathcal{C}$ be a principal D_{2m}-code over $\mathbb{F}_q$ generated by $p(x)$. Then*

$$\dim_{\mathbb{F}_q} \mathcal{C} \geq \max\{m - \deg p(x), m - \deg \overline{p}(x^{m-1})\}.$$

Proof. This follows from the fact that the vectors in $\mathbb{F}_q^{2m}$ corresponding to the polynomials

$$\{p(x), xp(x), \ldots, x^{m-\deg p(x)-1} p(x)\}$$

are linearly independent, and the same holds for the ones corresponding to

$$\{\overline{p}(x^{m-1}), x\overline{p}(x^{m-1}), \ldots, x^{m-\deg \overline{p}(x^{m-1})-1} \overline{p}(x^{m-1})\}.$$

Remark 5. For calculations, it may be interesting to have integer exponents. In case $(m, q) = 1$, we can take m' to be the inverse of m modulo q, so that $m'm - 1$ is divisible by q. Let $r := (m'm - 1)/q$. Then

$$\overline{p}(x^{m-1}) = \left(\frac{1-\alpha^2}{\alpha^q - \alpha}\right) p(x^r)^q + \left(\frac{\alpha^{q+1}-1}{\alpha^q - \alpha}\right) p(x^{m-1}).$$

3.2 Dual code

In analogy with the theory of cyclic and quasi-cyclic codes, it it interesting to investigate the dual codes of dihedral codes, which are still dihedral.

Proposition 1. *The dual code $\mathcal{C}^\perp$ of a dihedral code $\mathcal{C}$ is a dihedral code.*

Proof. This follows trivially from the fact that $\mathrm{PAut}(\mathcal{C}^\perp) = \mathrm{PAut}(\mathcal{C})$.

The dual of a principal dihedral code is not necessarily principal. But if $(m, q) = 1$, as we mentioned already, all dihedral codes are principal. So it makes sense to investigate the relation between the generator of a code and a generator of its dual.

Let $p(x)$ and $q(x)$ be two polynomial in $\mathbb{F}_{q^2}[x]/(x^m - 1)$ and let v and w the two vectors in $\mathbb{F}_q^{2m}$ corresponding to $p(x)$ and $q(x)$ respectively. We may define

$$\begin{aligned} * : \mathbb{F}_{q^2}[x]/(x^m - 1) \times \mathbb{F}_{q^2}[x]/(x^m - 1) &\to \mathbb{F}_q \\ (p(x), q(x)) &\mapsto p(x) * q(x) := \langle v, w \rangle \end{aligned}$$

Proposition 2. *Let $(m,q)=1$. If $\mathcal{C}$ is a principal D_{2m}-code generated by $p(x)$ and $\mathcal{C}^\perp$ is a principal D_{2m}-code generated by $q(x)$, then*

$$p(x)*q(x)=0,\ p(x)*\overline{q}(x^{m-1})=0,$$

$$\overline{p}(x^{m-1})*q(x)=0,\ \overline{p}(x^{m-1})*\overline{q}(x^{m-1})=0.$$

The same holds with all the shift of $p(x)$ and $\overline{p}(x^{m-1})$.

Proof. This is clear from the definition of $*$.

Remark 6. At least two questions stand open in this context: the conditions in Proposition 2 are only necessary. It would be very interesting to find sufficient conditions for a polynomial $q(x)$ to be a generator of the dual. We may add the orthogonality with all the shift of $p(x)$ and $\overline{p}(x^{m-1})$, but this would still be not enough. A polynomial $q(x)$ satisfying all these relations would generate a subcode of $\mathcal{C}^\perp$, but not necessarily the whole dual. In fact, there is an argument on the dimension missing. Secondly, it would be nice to give some relations with the usual product of polynomials (as in the cyclic codes case) and not with the $*$ product.

For dihedral codes over fields of characteristic 2, a nice relation holds.

Proposition 3. *If q is a power of 2, then $\langle\overline{p}(x^{m-1})\rangle_{\mathbb{F}_q}\subseteq\langle p(x)\rangle_{\mathbb{F}_q}^{\perp}$. In particular, the code generated by $p(x)$ is contained in $\langle p(x)\rangle_{\mathbb{F}_q}+\langle p(x)\rangle_{\mathbb{F}_q}^{\perp}$.*

Proof. Recall that if $p(x)$ corresponds to the vector

$$v=(a_0,b_0,a_1,b_1,\ldots,a_{m-1},b_{m-1}),$$

then $\overline{p}(x^{m-1})$ corresponds to the vector

$$w=(b_0,a_0,b_{m-1},a_{m-1},\ldots,b_1,a_1),$$

so that

$$\langle v,w\rangle=2(a_0b_0+a_1b_{m-1}+a_{m-1}b_1+\ldots)=0$$

in any field of characteristic 2. Clearly, the same argument applies to $x^ip(x)$.

Remark 7. In many examples, we get the equality $\langle\overline{p}(x^{m-1})\rangle_{\mathbb{F}_q}=\langle p(x)\rangle_{\mathbb{F}_q}^{\perp}$. However, we could not find a general property of $p(x)$ which guarantees it. Again, there is an argument on the dimension missing.

3.3 Minimum distance bounds

Let t be the order of q^2 modulo m, and let ω be a primitive m-th root of unity in $\mathbb{F}_{q^{2t}}$. If $\delta-1$ consecutive powers of ω are roots of both $p(x)$ and $\overline{p}(x^{m-1})$, then a BCH bound can be proved for the code generated by $p(x)$ and $\overline{p}(x^{m-1})$.

Theorem 2 (BCH bound for principal dihedral codes). *If $\delta - 1$ consecutive powers of ω are roots of both $p(x)$ and $\overline{p}(x^{m-1})$, then the dihedral code $\mathcal{C}$ generated by $p(x)$ has minimum distance at least δ.*

Proof. A codeword $c(x)$ of the folded $\mathcal{C} \subseteq \mathbb{F}_{q^2}^m$ is of the form

$$c(x) = t_1(x)p(x) + t_2(x)\overline{p}(x^{m-1}),$$

for $t_1(x), t_2(x) \in \mathbb{F}_q[x]$. As $\delta - 1$ consecutive powers of ω are roots of both $p(x)$ and $\overline{p}(x^{m-1})$, we have $c(x) = c'(x)g(x)$ where $c'(x) \in \mathbb{F}_{q^2}[x]$ and

$$g(x) = \mathrm{lcm}\{M_{\omega^b}(x), M_{\omega^{b+1}}(x), \ldots, M_{\omega^{b+\delta-2}}(x)\},$$

where $M_{\omega^i}(x)$ is the minimal polynomial of ω^i over $\mathbb{F}_{q^2}$. It follows that the folded $\mathcal{C}$ is a subcode of the BCH code genereted by $g(x)$, which has minimum distance at least δ by the classical BCH bound. Since a nonzero coordinate in a codeword of the folded $\mathcal{C}$ corresponds to at least a nonzero coordinate of the unfolded codeword in $\mathcal{C}$, the minimum distance of $\mathcal{C}$ is at least δ.

Let us consider the case $(m, q) = 1$ and let r be defined as in Remark 5. For many applications, it is suitable to consider codes with a prescribed minimum distance. This can be achieved by imposing that $\delta - 1$ consecutive powers of ω, say $\omega^b, \omega^{b+1}, \ldots, \omega^{b+\delta-2}$, together with their inverse and their r-th powers, are roots of $p(x)$, which guarantees that the code generated has minimum distance at least δ.

Definition 7. *Let $(m, q) = 1$. A dihedral code $\mathcal{C} \subseteq \mathbb{F}_q^{2m}$ is a* BCH-dihedral code *of prescribed minimum distance δ if it exists an integer b such that its generator is*

$$p(x) = \mathrm{lcm} \left\{ \begin{array}{c} M_{\omega^b}(x), M_{\omega^{b+1}}(x), \ldots, M_{\omega^{b+\delta-2}}(x) \\ M_{\omega^{-b}}(x), M_{\omega^{-b-1}}(x), \ldots, M_{\omega^{-b-\delta+2}}(x) \\ M_{\omega^{br}}(x), M_{\omega^{br+r}}(x), \ldots, M_{\omega^{br+\delta r-2r}}(x) \end{array} \right\}$$

where $r = (m'm - 1)/q$, with m' being the inverse of m modulo q, and $M_{\omega^i}(x)$ is the minimal polynomial of ω^i over $\mathbb{F}_{q^2}$.

Remark 8. The definition above guarantees to have minimum distance at least δ. Anyway, it may probably be improved by analysing the relations between the cyclotomic cosets of the different roots. This reveals to be simpler in the binary case, that we will consider in the next subsection.

3.4 Binary case

Let us consider now D_{2m}-codes over $\mathbb{F}_2$, with $m \geq 3$ odd. The binary case is particularly interesting, since $\alpha^{2+1} - 1 = 0$. In this case

$$\overline{p}(x^{m-1}) = \alpha p(x^{(m-1)/2})^2,$$

so that if $Z(p)$ is the set of zeros of $p(x)$, then $Z(p)^{2/(m-1)}$ is the set of zeros of $\overline{p}(x^{m-1})$. In this case, we are considering $p(x)$ and $\overline{p}(x^{m-1})$ as polynomials in $\mathbb{F}_4[x]$ and not in the quotient ring.

We consider an m-th root of unity ω in $\mathbb{F}_{4^t}$, where t the order of 4 modulo m. The irreducible divisors of x^m-1 are associated to the cyclotomic cosets $C_i = \{i, 4i \bmod m, 4^2 i \bmod m, \ldots\}$ (this is classical in the theory of cyclic codes - see for example [18]): actually, if $M_{\omega^i}(x)$ is the polynomial associated to C_i (which is the minimal polynomial of ω^i), its zeros are $Z(M_{\omega^i}(x)) = \{\omega^j \mid j \in C_i\}$.

Proposition 4. *The following conditions are equivalent:*

a) $Z(M_{\omega^i})^{(m-1)/2} = Z(M_{\omega^i})$ *for all* $i \in \{0, \ldots, m-1\}$*;*
b) $\frac{m-1}{2} C_i = C_i$ *for all* $i \in \{0, \ldots, m-1\}$*;*
c) *it exists an integer* s *such that* $2^{2s+1} = -1 \bmod m$.

If m *is prime, then* a), b) *and* c) *are equivalent to*

d) $s_2(m) \equiv 2 \bmod 4$*, where* $s_2(m)$ *is the order of* 2 *modulo* m.

Proof. a)⇔b): if $Z(M_{\omega^i})^{(m-1)/2} = Z(M_{\omega^i})$, then it exists $j \in C_i$ such that $\omega^{i(m-1)/2} = \omega^j$, which means that the class C_i is sent to C_i by multiplying by $\frac{m-1}{2}$. The vice versa is trivial.
b)⇒c): since $\frac{m-1}{2} C_1 = C_1$, it exists s such that $\frac{m-1}{2} = 4^s \bmod m$. Then $2^{2s+1} = -1 \bmod m$.
c)⇒b): $2^{2s+1} = -1 \bmod m$ implies ($(m,2) = 1$ so that 2 is invertible) that $4^s = \frac{m-1}{2} \bmod m$. This means that for all $i \in \{0, \ldots, m-1\}$, we have $\frac{m-1}{2} i = 4^s i \in C_i$, which implies $\frac{m-1}{2} C_i = C_i$.
c)⇒d): Since $2^{4s+2} = 1 \bmod m$ and $2^{2s+1} = -1 \bmod m$, then $s_2(m)$ divides $2(2s+1)$ and $s_2(m)$ does not divide $2s+1$. So 2 divides $s_2(m)$. If 4 divides $s_2(m)$, then 4 divides $4s+2$, which is not true. So $s_2(m) \equiv 2 \bmod 4$.
d)⇒c): If $s_2(x) = 4s+2$, then 2^{2s+1} is a root of $x^2 - 1 \in \mathbb{F}_m[x]$, which has only two solutions. The only possible solution in this case is -1 (otherwise the order of 2 would be smaller than $4s+2$).

Remark 9. The set of primes $\mathcal{P} := \{m \mid s_2(m) \equiv 2 \bmod 4\} = \{3, 11, 19, 43, \ldots\}$ is infinite (its density in the set of primes is $7/24$ [22]).

Theorem 3. *If it exists an integer* s *such that* $2^{2s+1} = -1 \bmod m$ *(in particular if* m *is prime and* $s_2(m) \equiv 2 \bmod 4$*), then, for all integers* $\delta \geq 2$ *and* $b \geq 0$*, the binary* D_{2m}*-code generated by*

$$p(x) = \operatorname{lcm}\{M_{\omega^b}(x), M_{\omega^{b+1}}(x), \ldots, M_{\omega^{b+\delta-2}}(x)\}$$

is a principal BCH-dihedral code with minimum distance $d \geq \delta$ *and dimension* $k \geq m - \deg p(x)$.

Proof. It follows from the fact that, in this case, $p(x)$ divides $\overline{p}(x^{m-1})$: actually, all roots of $p(x)$ are roots of $\overline{p}(x^{m-1})$ (as polynomial in $\mathbb{F}_4[x]$) and $p(x)$ divides $x^m - 1$.

Remark 10. Theorem 3 allows to construct binary dihedral codes with prescribed minimum distance and with a lower bound on their dimensions. With MAGMA we did some calculations and we found some codes with the best-known minimum distance for their dimension (see [17]). For example:

- the D_{22}-code generated by

$$p(x) = x^5 + \alpha x^4 + x^3 + x^2 + \alpha^2 x + 1,$$

  which is a $[22, 12, 6]$ code;
- the D_{66}-code generated by

$$p(x) = x^{15} + \alpha x^{14} + x^{13} + x^{11} + x^{10} + \alpha^2 x^9 + \alpha^2 x^8 +$$

$$+\alpha x^7 + \alpha x^6 + x^5 + x^4 + x^2 + \alpha^2 x + 1,$$

  which is a $[66, 33, 12]$ code;
- the D_{86}-code generated by

$$p(x) = x^{21} + \alpha x^{20} + \alpha x^{18} + \alpha x^{17} + \alpha x^{16} + x^{15} + \alpha^2 x^{11} + \alpha x^{10} +$$

$$+x^6 + \alpha^2 x^5 + \alpha^2 x^4 + \alpha^2 x^3 + \alpha^2 x + 1,$$

  which is a $[86, 44, 15]$ code;
- the D_{86}-code generated by

$$p(x) = x^7 + x^6 + \alpha x^5 + \alpha^2 x^2 + x + 1.$$

  which is a $[86, 72, 5]$ code.

Note that the dimension is always $2(m - \deg p(x))$.

4 Open problems

In the paper we defined dihedral codes with prescribed minimum distance and dimension. However, it would be interesting to prove better bounds on the dimension and to give a construction allowing to control it. In particular, an open problem is the following.

Problem 1. When does equality hold in Corollary 1? Can the bound be improved by adding some conditions on $p(x)$?

Related to that, there is also the problem of a canonical generator. Actually, in the theory of BCH codes we can read the dimension from the degree of the generator polynomial (the one of lowest degree). It does not seem to exist an analogue for dihedral codes. About dual codes, many questions stand open. The main one is about the relation between the generators of code. Another important problem, related to the use of dihedral codes in cryptography is the

following.

Problem 2. Is there any efficient decoding algorithm for dihedral codes, based on the algebraic structure proved in the paper?

Finally, it would be interesting to extend the results to other group codes, at least in the checkable case.

References

1. M. Barbier, C. Chabot and G. Quintin, *On quasi-cyclic codes as a generalization of cyclic codes*, Finite Fields Appl., 18(5), pp. 904-919, 2012.
2. L.M.J. Bazzi and S.K. Mitter, *Some randomized code constructions from group actions*, IEEE Trans. Inform. Theory 52, pp. 3210–3219, 2006.
3. T.P. Berger, P.L. Cayrel, P. Gaborit and A. Otmani, *Reducing key length of the McEliece cryptosystem*, In International Conference on Cryptology in Africa, Springer, Berlin, Heidelberg, pp. 77–97, 2009.
4. S.D. Berman, *On the theory of group codes*, Kibernetika 3, pp. 31–39, 1967.
5. F. Bernhardt, P. Landrock and O. Manz, *The extended Golay codes considered as ideals*, J. Comb. Theory, Series A 55, pp. 235–246, 1990.
6. M. Borello, J. de la Cruz and W. Willems, *On checkable codes in group algebras*, `arXiv: 1901.10979`, 2019.
7. M. Borello and W. Willems, *Group codes over fields are asymptotically good*, `arXiv: 1904.10885`, 2019.
8. M. Borello and W. Willems, *On the algebraic structure of quasi group codes*, `arXiv: 1912.09167`, 2019.
9. Y. Cao, Y. Cao and F.W. Fu, *Concatenated structure of left dihedral codes*, Finite Fields and Their Applications, 38, pp. 93–115, 2016.
10. P. Charpin, *Une généralisation de la construction de Berman des codes de Reed-Muller p-aire*, Comm. Algebra 16, pp. 2231–2246, 1988.
11. E.J.G. Claro and H.T. Recillas, *On the dimension of ideals in group algebras, and group codes*, `arXiv: 2002.06407`, 2020.
12. J.H. Conway, S.J. Lomonaco Jr and N.J.A. Sloane, *A* $[45, 13]$ *code with minimal distance 16*, Discrete Math. 83, pp. 213–217, 1990.
13. M. Elia and E. Gorla, *Computing the dimension of ideals in group algebras, with an application to coding theory*, `arXiv: 1403.7920`, 2019.
14. J.-C. Faugère, A. Otmani, L. Perret and J.-P. Tillich, *Algebraic cryptanalysis of McEliece variants with compact keys*, in: H. Gilbert (Ed.), Advances in Cryptology EUROCRYPT 2010, in: Lecture Notes in Comput. Sci., vol. 6110, Springer, Berlin, Heidelberg, pp. 279–298, 2010.
15. A. vom Felde, *A new presentation of Cheng-Sloane's* $[32, 17, 8]$*-code*, Arch. Math. 60, pp. 508–511, 1993.
16. C. Güneri, F. Özdemir and P. Solé, *On the additive cyclic structure of quasi-cyclic codes*, Discrete Mathematics, 341(10): pp. 2735–2741, 2018.
17. M. Grassl, Codetables, http://www.codetables.de/.
18. W. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge, U.K. Cambridge Univ. Press, 2003.
19. S. Jitman, S. Ling, H. Liu and X. Xie, *Checkable codes from group rings*, `arXiv: 1012.5498v1`, 2010.

20. R. J. McEliece, *A public-key cryptosystem based on algebraic coding theory*, DSN Progress Report 42–44, pp. 114–116, 1978.
21. I. McLoughlin and T. Hurley, *A group ring construction of the extended binary Golay code*, IEEE Trans. Inform. Theory 54, pp. 4381–4383, 2008.
22. P. Moree, *On the divisors of* $a^k + b^k$. Acta Arithmetica, 80(3), pp. 197–212, 1997.
23. K. Morita, *Duality for modules and its applications to the theory of rings with minimum condition*, Science Reports of the Tokyo Kyoiku Daigaku, Section A, 6(150), pp. 83-142, 1958.
24. H. Niederreiter, *Knapsack-type cryptosystems and algebraic coding theory*. Problems of Control and Information Theory. Problemy Upravlenija i Teorii Informacii 15, pp. 159–166, 1986.
25. D.S. Passman, *Observations on group rings*, Comm. Algebra 5, pp. 1119-1162, 1977.