A Note on the Theoretical Support to Compute Dimension in Abelian Codes

José Joaquín Bernal and Juan Jacobo Simón
Departamento de Matemáticas
Universidad de Murcia
Murcia, Spain
{josejoaquin.bernal, jsimon}@um.es

***Abstract*—In this note we give a theoretical support by means of quotient polynomial rings for the computation formulas of the dimension of abelian codes.**

***Index Terms*—Abelian codes, dimension.**

I. Introduction

As it is known, the computation of the dimension of abelian codes may be done by easy formulas expressed in terms of their defining sets (see Theorem 17 below).Those formulas was developed in the setting of group rings (see [8] for a nice exposition) and all proofs are written by means of character theory. This situation comes from the fact that the original frame of abelian codes were abelian group rings and group representations (see [5]).

Over time, more complicated computations and tools drove a number of theorists to consider abelian codes in the setting of quotient rings of polynomial rings. In this way, the theoretical support of some basic computations, as dimension in terms of defining sets, has not been updated, or has been only partially updated, as in [10].

Another way to find the dimension of an abelian code may be done by using Groebner basis, as in [7]. It may be done in terms of what is called the footprint of an ideal (see [4]). All computations and theoretical results are, by default, expressed in terms of polynomials; and, in contrast with the case of defining sets, all arguments are clearly known.

The aim of this note is to give a full theoretical support for the computation formulas to get the dimension of abelian codes. First, we will study the correspondence between abelian codes and their defining sets. Then we shall deduce the computation formulas in those terms. Then, we recall the definition and construction of footprints and see the computation formula that arises from them. Finally, we comment on some interactions between defining sets and footprints from Groebner basis.

II. Notation and basic definitions

Throughout this note, $\mathbb{F}$ will be a finite field with q elements, with q a power of a prime number, r_i will be positive integers, for $i \in \{1, \ldots, s\}$, and $n = r_1 \cdots r_s$. We denote by $\mathbb{Z}_{r_i}$ the ring of integers modulo r_i. We always write its elements as **canonical representatives**. When necessary, we write $\overline{a} \in \mathbb{Z}_k$ for any $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. For any commutative ring R and any subset $A \subseteq R$ we denote by $\langle A \rangle$ the ideal generated by A, as usual.

Support: Grant PID2020-113206GB-I00 funded by MICIU/ AEI/ 10.13039/501100011033 y Fundación Séneca de Murcia, project 22004/PI/22.

An **Abelian Code** of length $n = r_1 \ldots r_s$ is an ideal in the algebra $\mathbb{F}(r_1, \ldots, r_s) = \mathbb{F}[X_1, \ldots, X_s]/\langle X_1^{r_1} - 1, \ldots, X_s^{r_s} - 1 \rangle$ and we assume that this algebra is semisimple; that is, $\gcd(n, q) = 1$. For the sake of simplicity, we often refer to "Abelian Code" simply as "code". It is well-known (see, for example, [1]) that every finite semisimple commutative ring has a (unique) **complete set of primitive orthogonal idempotents** associated to its decomposition as finite product of simple rings.

Codewords are identified with polynomials. We denote the weight of a codeword c by $\omega(c)$. We set $\boldsymbol{\mathcal{I}} = \mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_s}$ and we write the elements $f \in \mathbb{F}(r_1, \ldots, r_s)$ as its canonical representatives; that is, $f = \sum a_m \boldsymbol{X}^m$, where $m = (m_1, \ldots, m_s) \in \boldsymbol{\mathcal{I}}$ and $\boldsymbol{X}^m = X_1^{m_1} \cdots X_s^{m_s}$. When necessary, for a polynomial $f \in \mathbb{F}[X_1, \ldots, X_s]$ we denote by $\overline{f}$ its image under the canonical projection onto $\mathbb{F}(r_1, \ldots, r_s)$.

For each $i \in \{1, \ldots, s\}$, we denote by R_{r_i} (resp. U_{r_i}) the set of all r_i-th roots of unity (resp. all r_i-th primitive roots of unity) and define $R = \prod_{i=1}^s R_{r_i}$ ($U = \prod_{i=1}^s U_{r_i}$). For $m = (m_1, \ldots, m_s) \in \boldsymbol{\mathcal{I}}$, we write $\boldsymbol{\alpha}^m = (\alpha_1^{m_1}, \ldots, \alpha_s^{m_s})$. Throughout this paper, we fix the notation $\mathbb{L}$ for an extension field, $\mathbb{L}|\mathbb{F}$, containing U_{r_i}, for all $i \in \{1, \ldots, s\}$.

For a canonical representative $f \in \mathbb{F}(r_1, \ldots, r_s)$ seen as polynomial $f = f(X_1, \ldots, X_s) \in \mathbb{F}[X_1, \ldots, X_s]$ and $\boldsymbol{\alpha} \in R$, we write $f(\boldsymbol{\alpha}) = f(\alpha_1, \ldots, \alpha_s)$.

III. Defining sets in Abelian Codes

The study of several important parameters of the Cyclic and Abelian Codes is carried out through their definition sets. For example, their minimum distance or dimension may be computed easily by means of them and it is also essential in all decoding techniques because they are needed to determine the correction capability and to form the syndrome values of error polynomials.

In this section we shall prove that every abelian code C in $\mathbb{F}(r_1, \ldots, r_s)$ is totally determined by its defining set (see definition below). We keep all notation above; in particular, we recall that $\mathbb{F}(r_1, \ldots, r_s)$ is a semisimple ring.

We recall the notion of cyclotomic coset. For any $\gamma \in \mathbb{N}$ the q^γ-cyclotomic coset of an integer a modulo r is the set

$$C_{(q^\gamma,r)}(a) = \left\{a \cdot q^{\gamma \cdot i} \mid i \in \mathbb{N}\right\} \subseteq \mathbb{Z}_r.$$

By elementary algebraic properties of polynomials over finite fields it is well-known that if $(a, \ldots, a_s)$ is a root of the polynomial $f \in \mathbb{F}[\boldsymbol{X}]$ then $(a_1^q, \ldots, a_s^q)$ is also a root of f. This property is the key of the extension of the notion of q-cyclotomic coset to several variables.

Definition 1. *In the setting described above, given an element $(a_1, \ldots, a_s) \in I$, we define its q-orbit modulo $(r_1, \ldots, r_s)$ as the subset $Q(a_1, \ldots, a_s) = \left\{\left(a_1 \cdot q^i, \ldots, a_s \cdot q^i\right) \mid i \in \mathbb{N}\right\} \subseteq \boldsymbol{\mathcal{I}}$.*

We also extend the notion of set of zeros for Cyclic Codes.

Definition 2. *Let $A \subset \mathbb{F}(r_1, \ldots, r_s)$. The set of zeros of A is $\mathcal{Z}(A) = \{\boldsymbol{\beta} \in R \mid f(\boldsymbol{\beta}) = 0,$ for all $f \in A\}$.*

Once one has fixed $\boldsymbol{\alpha} \in U$ one may define the following object.

Definition 3. *In the setting above, the defining set of A, with respect to $\boldsymbol{\alpha} \in U$ is $\mathcal{D}_{\boldsymbol{\alpha}}(A) = \{m \in \boldsymbol{\mathcal{I}} \mid \boldsymbol{\alpha}^m \in \mathcal{Z}(A)\}$.*

Remark 4. Let C be a code in $\mathbb{F}(r_1, \ldots, r_s)$ and $\boldsymbol{\alpha} \in U$. From Definition 1 we have immediately that the defining set $\mathcal{D}_{\boldsymbol{\alpha}}(C)$ is a disjoint union of q-orbits.

Now we shall prove that there is a one to one correspondence between Abelian Codes and the sets of q-orbits.

Lemma 5 (See [9])**.** *Let $f \in \mathbb{F}(r_1, \ldots, r_s)$ be an arbitrary element and consider $\boldsymbol{\alpha} \in U$. If $f(\boldsymbol{\alpha}^m) = 0$ for all $m \in \boldsymbol{\mathcal{I}}$ then $f = 0$ in $\mathbb{F}[\boldsymbol{X}]$.*

Proof. We set $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s)$ and we proceed by induction on s:

For $s = 1$ is obvious by classical arguments on degrees of polynomials in one variable. Suppose the result is true for $s-1$ and we have to see for s.

Let $f(\boldsymbol{X}) = \sum_{j=0}^{r_s-1} f_j(X_1, \ldots, X_{s-1}) X_s^j$ be such that $f(\boldsymbol{\alpha}^m) = 0$ for all $m \in \boldsymbol{\mathcal{I}}$. If for each $m \in \boldsymbol{\mathcal{I}}$ we set $f_{\alpha_1^{m_1}, \ldots, \alpha_{s-1}^{m_s-1}} = \sum_{j=0}^{r_s-1} f_j(\alpha_1^{m_1}, \ldots, \alpha_{s-1}^{m_s-1}) X_s^j$, we see that it has the roots $\alpha_s^0, \ldots, \alpha_s^{r_s-1}$ (r_s-roots) and it has degree at most $r_s - 1$; so that $f_{\alpha_1^{m_1}, \ldots, \alpha_{s-1}^{m_s-1}} = 0$. This means that $f_j(X_1, \ldots, X_{s-1})$ vanishes in $\boldsymbol{\alpha}^m$ for all $j = 0, \ldots, s-1$. Hence, by induction hypothesis, $f_j(X_1, \ldots, X_{s-1}) = 0$ and then $f(\boldsymbol{X}) = \sum_{j=0}^{r_s-1} 0 \cdot X_s^j = 0$. □

We denote by $\mathcal{Q}$ the collection of all subsets of $\boldsymbol{\mathcal{I}}$ that are unions of q-orbits. We consider the usual partial ordering in $\mathcal{Q}$, given by set inclusion. Note that if $r_i \geq 2$ for all $i = 1, \ldots, s$ then $|\mathcal{Q}| \geq 3$, as $Q(0,0)$, $Q(1,0)$ and $Q(0,1)$ are disjoint sets.

First, we settle the correspondence $C \mapsto \mathcal{D}_{\boldsymbol{\alpha}}(C) \in \mathcal{Q}$. We begin by listing some properties that may be proved in a direct way.

Proposition 6. *Let C and D codes in $\mathbb{F}(r_1, \ldots, r_s)$, with defining sets $\mathcal{D}_{\boldsymbol{\alpha}}(C)$ and $\mathcal{D}_{\boldsymbol{\alpha}}(D)$, respectively. Then*

1) *If $C \subseteq D$ then $\mathcal{D}_{\boldsymbol{\alpha}}(D) \subseteq \mathcal{D}_{\boldsymbol{\alpha}}(C)$.*
2) *$\mathcal{D}_{\boldsymbol{\alpha}}(C + D) = \mathcal{D}_{\boldsymbol{\alpha}}(C) \cap \mathcal{D}_{\boldsymbol{\alpha}}(D)$.*

As a consequence we have the following corollary.

Corollary 7. *Let $e_1, \ldots, e_t$ be the complete set of primitive orthogonal idempotents of $\mathbb{F}(r_1, \ldots, r_s)$, and write $C = \sum_{k=1}^{l} Re_{i_k}$. Then $\mathcal{D}_{\boldsymbol{\alpha}}(C) = \cap_{k=1}^{l} \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_k})$*

Note that the intersection of all defining sets is $\cap_{k=1}^{n} \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_k}) = \emptyset$.

Now we shall prove injectivity. First we prove the following lemma whose proof is straightforward.

Lemma 8. *Let C be a code in $\mathbb{F}(r_1, \ldots, r_s)$ and $\boldsymbol{\alpha} \in U$. Consider the ideal (code)*

$$D = \{f \in \mathbb{F}(r_1, \ldots, r_s) \mid f(\boldsymbol{\alpha}^m) = 0, \text{ for all } m \in \mathcal{D}_{\boldsymbol{\alpha}}(C)\}.$$

Then $\mathcal{D}_{\boldsymbol{\alpha}}(C) = \mathcal{D}_{\boldsymbol{\alpha}}(D)$

Next lemma is crucial to prove injectivity.

Lemma 9. *Let $e \in \mathbb{F}(r_1, \ldots, r_s)$ be a primitive idempotent. Then $\mathcal{D}_{\boldsymbol{\alpha}}(Re)$ is maximal in $\mathcal{Q}$.*

Conversely, if $\boldsymbol{\mathcal{I}} \neq Q \in \mathcal{Q}$ is a maximal element, then $C = \{f \in \mathbb{F}(r_1, \ldots, r_s) \mid f(\boldsymbol{\alpha}^m) = 0,$ for all $m \in Q\}$ is an ideal such that $C = Re$ with e a primitive idempotent.

Proof. Let $e_1, \ldots, e_t$ be the complete set of orthogonal idempotents of the ring $\mathbb{F}(r_1, \ldots, r_s)$. Suppose that $\mathcal{D}_{\boldsymbol{\alpha}}(Re) \subseteq Q \subseteq \boldsymbol{\mathcal{I}}$. We set $C = \{f \in \mathbb{F}(r_1, \ldots, r_s) \mid f(\boldsymbol{\alpha}^m) = 0,$ for all $m \in Q\}$. Then $Q \subseteq \mathcal{D}_{\boldsymbol{\alpha}}(C)$, so that $\mathcal{D}_{\boldsymbol{\alpha}}(Re) \subseteq \mathcal{D}_{\boldsymbol{\alpha}}(C)$. We write $C = \sum_{k=1}^{l} Re_{i_k}$. By Corollary 7 one has that $\mathcal{D}_{\boldsymbol{\alpha}}(C) = \cap_{k=1}^{l} \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_k})$; from which $\mathcal{D}_{\boldsymbol{\alpha}}(Re) \subset \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_k})$ for $k = 1, \ldots l$. Now suppose that there is a primitive idempotent $e_{i_k} \neq e$. As they are primitive idempotents it must happen that $ee_{i_k} = 0$. Since $e_{i_k} \neq 0$, by Lemma 5, there exists $m \in \boldsymbol{\mathcal{I}}$ such that $m \notin \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_k})$, so that $e_{i_k}(\boldsymbol{\alpha}^m) \neq 0$ and $e(\boldsymbol{\alpha}^m) \neq 0$. A contradiction.

Conversely, suppose that Q is maximal in $\mathcal{Q}$. Then, there exists $a \in \boldsymbol{\mathcal{I}}$ such that $Q \cup Q(a) = \boldsymbol{\mathcal{I}}$. Now, as we have pointed out, it happens that $\cap_{k=1}^{t} \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_k}) = \emptyset$; so that there must exist a primitive idempotent, say $e = e_{i_k}$, such that $Q(a) \nsubseteq \mathcal{D}_{\boldsymbol{\alpha}}(Re)$ and by statement *(1)* of this lemma, we have $Q(a) \cup \mathcal{D}_{\boldsymbol{\alpha}}(Re) = \boldsymbol{\mathcal{I}}$. From here, $Q = \mathcal{D}_{\boldsymbol{\alpha}}(Re)$ and by Lemma 8, $\mathcal{D}_{\boldsymbol{\alpha}}(C) = \mathcal{D}_{\boldsymbol{\alpha}}(Re)$, so that $C \neq 0$. It remains to see that $C = Re$. Suppose that there exists $e' = e_{i_{k'}}$ with $k \neq k'$ such that $Re' \subset C$. Then $\mathcal{D}_{\boldsymbol{\alpha}}(Re') = \mathcal{D}_{\boldsymbol{\alpha}}(C)$, by maximality, and hence $\mathcal{D}_{\boldsymbol{\alpha}}(Re') = \mathcal{D}_{\boldsymbol{\alpha}}(Re)$, but $ee' = 0$. As in the proof of paragraph above, we get a contradiction. □

Now we are going to prove the injectivity of the correspondence $C \mapsto \mathcal{D}_{\boldsymbol{\alpha}}(C) \in \mathcal{Q}$. We begin by showing it for primitive idempotents.

Corollary 10. *Let $e, f \in \mathbb{F}(r_1, \ldots, r_s)$ be primitive idempotents. If $\mathcal{D}_{\boldsymbol{\alpha}}(Re) = \mathcal{D}_{\boldsymbol{\alpha}}(Rf)$ then $e = f$.*

Proof. By Lemma 9 one has that $Re = Rf$ and, as they are primitive idempotents then $e = f$. □

For a subset $Q \subset \boldsymbol{\mathcal{I}}$, we denote $\widehat{Q} = \boldsymbol{\mathcal{I}} \setminus Q$; that is, its complement in $\boldsymbol{\mathcal{I}}$. From results above it follows that if $e_1, \ldots, e_t$ is the complete set of primitive idempotents of $\mathbb{F}(r_1, \ldots, r_s)$ then it has exactly $m_1, \ldots, m_t$ representatives of all distinct q-orbits such that $\widehat{\mathcal{D}_{\boldsymbol{\alpha}}(Re_i)} = Q(m_i)$ by reordering adequately all indexes.

Proposition 11. *Let C and D be codes in $\mathbb{F}(r_1, \ldots, r_s)$. If $C \subsetneq D$ then $\mathcal{D}_{\boldsymbol{\alpha}}(D) \subsetneq \mathcal{D}_{\boldsymbol{\alpha}}(C)$.*

Proof. Let $e_1, \ldots, e_t$ be the complete set of primitive orthogonal idemptents of $\mathbb{F}(r_1, \ldots, r_s)$. Set $C = \sum_{j=1}^{k} Re_{i_j}$. By hypothesis, there is $f \in \{e_1, \ldots, e_t\}$ such that $f \in C \setminus D$. If we call $Q(m_f) = \widehat{\mathcal{D}_{\boldsymbol{\alpha}}(Rf)}$, then we have, by Corollary 10, that $Q(m_f) \subset \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_j})$ for $j = 1, \ldots, k$ and hence $Q(m_f) \subset \cap_{j=1}^{k} \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_j})$; but $Q(m_f) \not\subset \cap_{j=1}^{k} \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_j}) \cap \mathcal{D}_{\boldsymbol{\alpha}}(Rf)$, so that $\cap_{j=1}^{k} \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_j}) \cap \mathcal{D}_{\boldsymbol{\alpha}}(Rf) \subsetneq \cap_{j=1}^{k} \mathcal{D}_{\boldsymbol{\alpha}}(Re_{i_j})$. □

Now we prove the injectivity in the general case.

Corollary 12. *Let C and D be codes in $\mathbb{F}(r_1, \ldots, r_s)$. Then $C = D$ if and only if $\mathcal{D}_{\boldsymbol{\alpha}}(C) = \mathcal{D}_{\boldsymbol{\alpha}}(D)$.*

Proof. Necessity is trivial. Let us see sufficiency. Suppose we have $\mathcal{D}_{\boldsymbol{\alpha}}(C) = \mathcal{D}_{\boldsymbol{\alpha}}(D)$ and set $E = \{f \in \mathbb{F}(r_1, \ldots, r_s) \mid f(\boldsymbol{\alpha}^m) = 0, \text{ for all } m \in \mathcal{D}_{\boldsymbol{\alpha}}(C)\}$. Then $C, D \subseteq E$ and by Lemma 8 $\mathcal{D}_{\boldsymbol{\alpha}}(E) = \mathcal{D}_{\boldsymbol{\alpha}}(C) = \mathcal{D}_{\boldsymbol{\alpha}}(D)$. Finally, Proposition 11 tells us that $C = E = D$. □

Once injectivity has been proved, we are going to see that the correspondence $C \mapsto \mathcal{D}_{\boldsymbol{\alpha}}(C) \in \mathcal{Q}$ is onto. To do this, we have to prove that every element of $\mathcal{Q}$ is a defining set.

Proposition 13. *Let $Q \in \mathcal{Q}$ an arbitrary element. If $C = \{f \in \mathbb{F}(r_1, \ldots, r_s) \mid f(\boldsymbol{\alpha}^m) = 0, \text{ for all } m \in Q\}$ then $\mathcal{D}_{\boldsymbol{\alpha}}(C) = Q$.*

Proof. Clearly $Q \subseteq \mathcal{D}_{\boldsymbol{\alpha}}(C)$. Let $m_1, \ldots, m_k$ and $u_1, \ldots, u_l$ be representatives of the q-orbits modulo $(r_1, \ldots, r_s)$, such that $m_i \in Q$, for $i = \{1, \ldots, k\}$ and $u_j \notin Q$, for $j = \{1, \ldots, l\}$. Then $Q = \cap_{j=1}^{l} \widehat{Q_q(u_j)}$. By Lemma 9, each $\widehat{Q_q(u_j)} = \mathcal{D}_{\boldsymbol{\alpha}}(Re_j)$, with e_j primitive idempotent, for $j = 1, \ldots, l$. So, $\mathcal{D}_{\boldsymbol{\alpha}}(\sum_{j=1}^{l} Re_j) = \cap_{j=1}^{l} \mathcal{D}_{\boldsymbol{\alpha}}(Re_j) = \cap_{j=1}^{l} \widehat{Q_q(u_j)} = Q$. □

Theorem 14. *In the setting and notation of this section, there exists a bijective correspondence between the abelian codes of $\mathbb{F}(r_1, \ldots, r_s)$ and the elements of $\mathcal{Q}$, in the following way. For any code C in $\mathbb{F}(r_1, \ldots, r_s) = R$ and any $Q \in \mathcal{Q}$,*

$$\begin{array}{rcl} C & \longrightarrow & \mathcal{D}_{\boldsymbol{\alpha}}(C) \\ \{f \in R \mid f(\boldsymbol{\alpha}^m) = 0, \text{ for all } m \in Q\} & \longleftarrow & Q. \end{array}$$

Proof. Immediate from Corollary 12 and Proposition 13. □

IV. Computing dimension through defining sets and the DFT

We begin by comment on some well-known facts about tensor products and scalar extensions. Consider a field extension $\mathbb{L}|\mathbb{F}$. It is well-known (see [1, Exercise 19.3] or [11, Corollary 1.7.16]) that if V is an $\mathbb{F}$-vector space with basis $\{v_i\}_{i=1}^{s}$ then $\{1 \otimes v_i\}_{i=1}^{s}$ is a basis for the $\mathbb{L}$-vector space $\mathbb{L} \otimes_{\mathbb{F}} V$ and as a consequence $\dim_{\mathbb{F}} V = \dim_{\mathbb{L}}(\mathbb{L} \otimes V)$.

In our setting, the set $\{\boldsymbol{X}^m\}_{m \in \boldsymbol{\mathcal{I}}}$ is a basis for the $\mathbb{F}$-vector space $\mathbb{F}(r_1, \ldots, r_s)$, so that $\{1 \otimes \boldsymbol{X}^m\}_{m \in \boldsymbol{\mathcal{I}}}$ is a basis for $\mathbb{L}$-vector space $\mathbb{L} \otimes_{\mathbb{F}} \mathbb{F}(r_1, \ldots, r_s)$. It is easy to check that the correspondence $1 \otimes \boldsymbol{X}^m \mapsto \boldsymbol{X}^m$ induces an isomorphism of $\mathbb{L}$-vector spaces $\mathbb{L} \otimes_{\mathbb{F}} \mathbb{F}(r_1, \ldots, r_s) \cong \mathbb{L}(r_1, \ldots, r_s)$. Moreover, in [11, Example 1.7.21.i], it is proved that it is, in fact, an isomorphism of $\mathbb{L}$-algebras.

Following the arguments above one may prove that for any ideal $J \leq \mathbb{F}(r_1, \ldots, r_s)$, it happens that $\dim_{\mathbb{F}} J = \dim_{\mathbb{L}}(\mathbb{L} \otimes_{\mathbb{F}} J)$. So, we have the following theorem.

Theorem 15. *Let $\mathbb{L}|\mathbb{F}$ be a field extension. Then $\mathbb{L} \otimes_{\mathbb{F}} \mathbb{F}(r_1, \ldots, r_s) \cong \mathbb{L}(r_1, \ldots, r_s)$ as algebras. Moreover, if J is a code in $\mathbb{F}(r_1, \ldots, r_s)$ then*

$$\dim_{\mathbb{F}}(J) = \dim_{\mathbb{L}}(\mathbb{L} \otimes_{\mathbb{F}} J).$$

Now we review the definition and basic properties of the discrete Fourier transform (DFT, for short) in the context of multivariate polynomials. The reader may see [5] for a presentation in the context of character theory.

Following the notation settled in Section II, let $f \in \mathbb{F}(r_1, \ldots, r_s)$ be an arbitrary element, that we consider as a polynomial. The DFT with respect to $\boldsymbol{\alpha} \in U$ is the polynomial $\varphi_{\boldsymbol{\alpha},f}(\boldsymbol{X}) = \sum_{m \in \boldsymbol{\mathcal{I}}} f(\boldsymbol{\alpha}^m) \boldsymbol{X}^m \in \mathbb{L}(r_1, \ldots, r_s)$.

We want to formalize this concept and view it as a map. The first important fact that we recall is that, for any $f \in \mathbb{F}(r_1, \ldots, r_s)$, its image verifies $\varphi_{\boldsymbol{\alpha},f}(\boldsymbol{X}) \in \mathbb{L}(r_1, \ldots, r_s)$; that is, it belongs to the polynomial factor ring over the extension field, $\mathbb{L}$. Now with respect to arithmetical properties, it is easy to check that, for $f, g \in \mathbb{F}(r_1, \ldots, r_s)$, we have $\varphi_{\boldsymbol{\alpha},f+g}(\boldsymbol{X}) = \varphi_{\boldsymbol{\alpha},f}(\boldsymbol{X}) + \varphi_{\boldsymbol{\alpha},g}(\boldsymbol{X})$; however, the DFT is not multiplicative with respect to the usual polynomial product. This is the reason for which it is considered another multiplication on the codomain. For $f, g \in \mathbb{L}(r_1, \ldots, r_s)$, with $f = \sum_{m \in \boldsymbol{\mathcal{I}}} f_m \boldsymbol{X}^m$ and $g = \sum_{m \in \boldsymbol{\mathcal{I}}} g_m \boldsymbol{X}^m$ we define $f \star g = \sum_{m \in \boldsymbol{\mathcal{I}}} f_m g_m \boldsymbol{X}^m$; that is, the product coeficient by coeficient or coordinatewise. We denote this algebra by $(\mathbb{L}^n, \star)$. Now, clearly $\varphi_{\boldsymbol{\alpha},f \star g}(\boldsymbol{X}) = \varphi_{\boldsymbol{\alpha},f}(\boldsymbol{X}) \star \varphi_{\boldsymbol{\alpha},g}(\boldsymbol{X})$.

One may prove that the DFT, viewed as $\varphi : \mathbb{L}(r_1, \ldots, r_s) \to (\mathbb{L}^n, \star)$ is an isomorphism of algebras with inverse $\varphi^{-1}_{\boldsymbol{\alpha},f}(\boldsymbol{X}) = \frac{1}{s} \sum_{m \in \boldsymbol{\mathcal{I}}} f(\boldsymbol{\alpha}^{-m}) \boldsymbol{X}^m$.

In the following lemma, we find three important facts on the DFT that are easy to check.

Lemma 16. *In the setting above, with $\varphi_{\boldsymbol{\alpha},-} : \mathbb{L}(r_1, \ldots, r_s) \to (\mathbb{L}^n, \star)$, let $e \in \mathbb{F}(r_1, \ldots, r_s)$ and $f \in (\mathbb{L}^n, \star)$ be idempotent elements in their respective algebras. Then*

1) *If $f = \sum_{m \in I} f_m \boldsymbol{X}^m$ then we must have $f_m \in \{0, 1\}$.*
2) *The support $\operatorname{supp}(\varphi_{\boldsymbol{\alpha},e}) = \boldsymbol{\mathcal{I}} \setminus \mathcal{D}_{\boldsymbol{\alpha}}(\mathbb{F}(r_1, \ldots, r_s)e)$.*

We are now ready to show the following easy formula to compute the dimension of abelian codes, expressed only in polynomial terms.

Theorem 17. *Let $\boldsymbol{\alpha} \in U$ be fixed and let C an abelian code in $\mathbb{F}(r_1, \ldots, r_s)$. Then*

$$\dim_{\mathbb{F}}(C) = |\boldsymbol{\mathcal{I}} \setminus \mathcal{D}_{\boldsymbol{\alpha}}(C)| = n - |\mathcal{D}_{\boldsymbol{\alpha}}(C)|.$$

Proof. Let $e \in \mathbb{F}(r_1, \ldots, r_s)$ the generating idempotent of C. Then $C = \mathbb{F}(r_1, \ldots, r_s)e$, and clearly $\mathbb{L} \otimes_{\mathbb{F}} C = \mathbb{L}(r_1, \ldots, r_s)e$. By Theorem 15, $\dim_F(C) = \dim_{\mathbb{L}}(\mathbb{L}(r_1, \ldots, r_s)e)$. If we call K the ideal generated by $\varphi_{\boldsymbol{\alpha},e}$ in $(\mathbb{L}^n, \star)$ then, we see immediately from Lemma 16 that $\dim_{\mathbb{L}}(K) = |\operatorname{supp}(\varphi_{\boldsymbol{\alpha},e})|$.

Now, as the DFT is an isomorphism of algebras then $\dim_{\mathbb{L}}(\mathbb{L}(r_1, \ldots, r_s)e) = \dim_{\mathbb{L}}(K)$. Finally,

$$\begin{aligned} \dim_{\mathbb{F}}(C) &= \dim_{\mathbb{L}}(\mathbb{L}(r_1, \ldots, r_s)e) = \\ &= \dim_{\mathbb{L}}(K) = |\operatorname{supp}(\varphi_{\boldsymbol{\alpha},e})| = \\ &= |\boldsymbol{\mathcal{I}} \setminus \mathcal{D}_{\boldsymbol{\alpha}}(C)| = n - |\mathcal{D}_{\boldsymbol{\alpha}}(C)|. \end{aligned}$$

□

As a consequence, we may reformulate the computing of the dimension in terms of the DFT.

Corollary 18. *Let us fix an element $\boldsymbol{\alpha} \in U$ and let C be an abelian code in $\mathbb{F}(r_1, \ldots, r_s)$ with generating idempotent $e \in C$. Then $\dim_{\mathbb{F}}(C) = |\operatorname{supp}(\varphi_{\boldsymbol{\alpha},e})|$.*

An interesting consequence of the relationship between defining sets and the DFT is the following. Let $\boldsymbol{\alpha} \in U$ be fixed and let C an abelian code in $\mathbb{F}(r_1, \ldots, r_s)$ with defining set $\mathcal{D}_{\boldsymbol{\alpha}}(C)$. We may compute explicitly the generator idempotent of C, as $e = \frac{1}{s} \sum_{m \in \boldsymbol{\mathcal{I}} \setminus \mathcal{D}_{\boldsymbol{\alpha}}(C)} f(\boldsymbol{\alpha}^{-m}) \boldsymbol{X}^m$.

V. Computing dimension through Groebner basis

Groebner bases are an important tool in the study of abelian codes. As in the case of defining sets, essential aspects of such codes, as information sets, bounds for the minimum distance and coding or decoding techniques, may be study by means of Groebner bases and their footprints. The reader may see [6], [12] for more information.

In this section we see another interesting application of Groebner bases in the study of Abelian Codes. We shall show that, one may compute the dimension of any Abelian Code, C by means of the so-called footprint of C.

Let us recall some notation and results about Groebner bases. Essentially, we shall follow [7, Chapter 2] and [4]. So, we denote

$$\mathbb{Z}_{\geq 0}^s = \{(m_1, \ldots, m_s) \in \mathbb{Z}^s \mid m_i \geq 0, \ \forall\, i \in \{1, \ldots, s\}\}.$$

Definition 19. *Consider a monomial ordering $\leq_T$ for $\mathbb{Z}_{\geq 0}^s$ and an element $f \in \mathbb{F}[\boldsymbol{X}]$, that we write $f = \sum_{m \in \operatorname{supp}(f)} f_m \boldsymbol{X}^m$.*

1) *The leading exponent, or multidegree of f is $\operatorname{LP}(f) = \max_{\leq_T}\{m \in \mathbb{Z}_{\geq 0}^s \mid m \in \operatorname{supp}(f)\}$.*
2) *The leading term is $\operatorname{LT}(f) = f_{\operatorname{LP}(f)} \boldsymbol{X}^{\operatorname{LP}(f)}$.*
3) *For any subset $J \subset \mathbb{F}[\boldsymbol{X}]$ we define the set of leading terms as $\operatorname{LT}(J) = \{\operatorname{LT}(f) \mid f \in J\}$.*

From Dickson's lemma [7, Theorem 2.4.5], the Hilbert's basis theorem [7, Theorem 2.5.4] and other results one may deduce the existence and properties of Groebner basis.

Definition 20. *Let $\leq_T$ be a monomial ordering for $\mathbb{Z}_{\geq 0}^s$ and let $\{0\} \neq J \leq \mathbb{F}[\boldsymbol{X}]$ an ideal. We say that the set $\{g_1, \ldots, g_t\}$ is a Groebner basis for J if*

$$\langle \operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t) \rangle = \langle \operatorname{LT}(J) \rangle.$$

By convention, $\langle \emptyset \rangle = \{0\}$ and so $\emptyset$ is a Groebner basis for $\{0\}$

Remark 21. *It is immediate to prove that, if $\mathcal{G} = \{g_1, \ldots, g_t\}$ is a Groebner basis for J then for all $f \in J$ there exists $g_i \in \mathcal{G}$ such that, its leading term divides to that of f; that is, $\operatorname{LT}(g_i) \mid \operatorname{LT}(f)$.*

From here we consider the following partial order in $\mathbb{Z}_{\leq 0}$.

Definition 22. *For any pair $m, m' \in \mathbb{Z}_{\geq 0}^s$ with $m = (m_1, \ldots, m_s)$ and $m' = (m'_1, \ldots, m'_s)$ we say that $m \preceq m'$ if $m_i \leq m'_i$ for each $i = 1, \ldots, s$.*

It is known that (see [7, Paragraph 2.6]), the division algorithm by elements of a Groebner basis has a good behavior. We summarize this in the next result.

Proposition 23. *Let $\mathcal{G} = \{g_1, \ldots, g_t\}$ be a Groebner basis for $J \leq \mathbb{F}[\boldsymbol{X}]$ and $f \in \mathbb{F}[\boldsymbol{X}]$, arbitrary. Then, there exists a unique division remainder, $r \in \mathbb{F}[\boldsymbol{X}]$ satisfying the following properties:*

1) *No term of r is greater than or equal to any of $\operatorname{LT}(g_1), \ldots, \operatorname{LT}(g_t)$.*
2) *$f = g + r$ with $g \in J$. In particular, $f \in J$ if and only if $r = 0$.*

Definition 24. *The remainder r is called the normal form of f.*

We say then that f is in normal form, with respect to $\mathcal{G}$, in case $f = r$.

So, the result above says that if $\mathcal{G} = \{g_1, \ldots, g_t\}$ is a Groebner basis for J then, for all $f \in J$ there exists $g_i \in \mathcal{G}$ such that $\operatorname{LT}(g_i) \preceq \operatorname{LT}(f)$.

Definition 25. *Let $J \leq \mathbb{F}[\boldsymbol{X}]$ an ideal with Groebner basis $\mathcal{G}$, such that all its elements are monic.*

1) *We say that $\mathcal{G}$ is minimal if, for all $g \in \mathcal{G}$ we have that $\operatorname{LT}(g) \notin \langle \operatorname{LT}(\mathcal{G}) \rangle$.*
2) *We say that $\mathcal{G}$ is reduced if for all $g \in \mathcal{G}$ no monomial of g belongs to $\langle \operatorname{LT}(\mathcal{G}) \setminus \{g\} \rangle$ (that is, the elements of $\mathcal{G}$ are in normal form).*

We know by [7, Theorem 2.7.5] that every nonzero ideal of $\mathbb{F}[\boldsymbol{X}]$ has a unique reduced Groebner basis.

A. Delta sets and the footprint of a code. Dimensions

Now we shall apply the results above to the computation of the dimension of Abelian Codes. Set q, s and $r_1, \ldots, r_s$, with $n = \prod_{i=1}^s r_i$, as above. We start with the following result from elementary algebra.

Consider the ideal $K = \langle X^{r_1} - 1, \ldots, X^{r_s} - 1\rangle$ and the quotient ring $\mathbb{F}[X_1, \ldots, X_s]/K = \mathbb{F}[\boldsymbol{X}]/K = \mathbb{F}(r_1, \ldots, r_s)$. Let $C \leq \mathbb{F}(r_1, \ldots, r_s)$ be a code. By the Correspodence Theorem, we know that there is a unique ideal $J \leq \mathbb{F}[\boldsymbol{X}]$ such that $K \subseteq J$ and that $J/K = C$. Now, by the Second Isomorphism Theorem,

$$\mathbb{F}[\boldsymbol{X}]/J \cong (\mathbb{F}[\boldsymbol{X}]/K) \,/\, (J/K) \cong \mathbb{F}(r_1, \ldots, r_s)/C$$

is an isomorphism of algebras; and so as $\mathbb{F}$-vector spaces we have that

$$\dim_{\mathbb{F}}(\mathbb{F}[\boldsymbol{X}]/J) = \dim_{\mathbb{F}}(\mathbb{F}(r_1, \ldots, r_s)/C) = n - \dim_{\mathbb{F}}(C). \tag{1}$$

Now, let $C \leq \mathbb{F}(r_1, \ldots, r_s)$ be a code and let $J \leq \mathbb{F}[\boldsymbol{X}]$ be the unique ideal such that $K \subseteq J$ and $J/K = C$. Fix a monomial ordering $\leq_T$. Let $\mathcal{G}_{\leq_T} = \mathcal{G} = \{g_1, \ldots, g_t\}$ a minimal Groebner basis for J. It is clear that, as $K \subset J$ there exists a subset $\{f_1, \ldots, f_s\} \subset \mathcal{G}$, such that $\mathrm{LP}(f_i)$ is such that, $\mathrm{LP}(f_i) \preceq (0, \ldots, 0, r_i, 0 \ldots, 0)$.

Following the notation, we define

$$A(\mathcal{G}) = \sum_{i=1}^{t} \mathrm{LP}(g_i) + \mathbb{Z}^s_{\geq 0}.$$

By the properties of minimal Groebner basis described above, we know that if $\mathcal{G}'$ is another minimal basis of J **under the same ordering** "$\leq_T$", then $A(\mathcal{G}) = A(\mathcal{G}')$. This uniqueness allows us to give the notion of the footprint.

Definition 26. *Let $\leq_T$ be a fixed monomial ordering and $C \leq \mathbb{F}(r_1, \ldots, r_s)$ be a code and let $J \leq \mathbb{F}[\boldsymbol{X}]$ be the unique ideal such that $K \subseteq J$ and $J/K = C$. We call the footprint of C the set*

$$\Delta(C) = \mathbb{Z}^s_{\geq 0} \setminus A(\mathcal{G}),$$

where $\mathcal{G}$ is any minimal Groebner basis for J.

Let us recall two elementary properties related to the results above. First, by definition of Groebner basis, we have that, for $f \in \mathbb{F}[\boldsymbol{X}]$, with normal form r_f it happens that if $f \notin J$ then $0 \neq \mathrm{LP}(r_f) \in \Delta(J)$. Second, by the uniqueness of the remainder we have that, for $f \in \mathbb{F}[\boldsymbol{X}]$, the correspondence $f \mapsto r_f$ is a $\mathbb{F}$-linear tranformation.

On the other hand, note that the footprint of any Abelian Code, C, is a finite set; in fact, $\Delta(C) \subseteq \boldsymbol{\mathcal{I}}$.

Theorem 27. *Let $\leq_T$ be a fixed monomial ordering and $C \leq \mathbb{F}(r_1, \ldots, r_s)$ be an Abelian Code with footprint $\Delta(C)$. Then by taking the canonical representatives, the set $\{\boldsymbol{X}^m \mid m \in \Delta(C)\}$ is a basis for $\mathbb{F}(r_1, \ldots, r_s)/C$.*

Hence, $\dim_{\mathbb{F}}(C) = n - |\Delta(C)|$.

Proof. First, note that, from the definition of minimal Groebner basis together with the fact that, for any $m \in \Delta(C)$, the normal form of the polynomial $\boldsymbol{X}^m$ is $r_{\boldsymbol{X}^m} = \boldsymbol{X}^m$. This means that the own $\boldsymbol{X}^m$ is a canonical representative. So, the set $\{\boldsymbol{X}^m \mid m \in \Delta(C)\}$ is a $\mathbb{F}$-basis for $\mathbb{F}[\boldsymbol{X}]/J$. Now, from the isomorphism in Equation (1) $\mathbb{F}[\boldsymbol{X}]/J \cong F(r_1, \ldots, r_s)$ the result follows immediately. The last part follws directly from the fact that the correspondence $f \mapsto r_f$ is $\mathbb{F}$-linear. □

Combining Theorem 17 and Theorem 27, above, we get the following corollary.

Corollary 28. *In the setting of Theorem 17 and Theorem 27 we have that $|\Delta(C)| = |\mathcal{D}_\alpha(C)|$.*

VI. Interactions between defining sets and footprints.

As we have commented above, some of the most important parameters, structure and coding-decoding techniques can be done by means of both defining sets through the discrete Fourier transform and the footprint through minimal Groebner basis.

In practice, the decision to use one tool or another, depends on the code construction; for instance, algebraic geometric codes make more use of footprints than general abelian codes.

We remark that in any case (if necessary) it is always possible to move from defining sets to footprints and vice versa. This transit can be done even avoiding the previous calculation of a minimal Groebner basis, as it is shown in [2].

We conclude by pointing out that there are frameworks in which all the tools that we have seen in this note must be combined to achieve a goal. Perhaps the most beautiful example of this is locator decoding (see [3], [13]). We need the defining set of the code to compute the syndrome values; then we implement the Berlekamp-Massey-Sakata algorithm to get a minimal Groebner basis of the locator ideal and finally we get the defining set of the locator ideal to get the error locations. By Corollary 28 we have that the number of errors occurred during transmission is exactly the cardinality of the footprint of the locator ideal.

References

[1] F. W. Anderson and K. R. Fuller, *Rings and Categories of Modules*, Springer-Verlag, Nueva York, 1974.

[2] J.J. Bernal and J.J. Simón, "Information sets in abelian codes: defining sets and Groebner basis", *Des. Codes Crypto.*, **70** (2014), 175–188

[3] J.J. Bernal and J.J. Simón, "A new approach to the Berlekamp-Massey-Sakata Algorithm. Improving Locator Decoding". *IEEE Transactions on Information Theory*, **67**(1) (2021), 268-281.

[4] R.E. Blahut, "Decoding of cyclic codes and codes on curves". In W.C. Huffman and V. Pless (Eds.), *Handbook of Coding Theory*. Vol. II, 1569-1633, 1998.

[5] P. Camion, *Abelian codes*. MRC Tech. Sum. Rep. no. 1059, Univ. of Wisconsin, Madison (1970).

[6] H. Chabanne, "Permutation decoding of abelian codes", *IEEE Trans. on Inform. Theory*, vol. 38, no. 6, pp. 1826-1829 (1992).

[7] D. Cox, J. Little, and D. O'Shea, *Ideals, varieties, and algorithms.* Springer: New York (1992).

[8] E. J. García Claro, *Dimensión de ideales an álgebras de grupo y códigos de grupo*, Tesis Doctoral, UAM-I, México, 2020.

[9] Sudhir R. Ghorpade, "A Note on Nullstellensatz over Finite Fields". *Contemporary Mathematics*, vol. 738, 2019.

[10] A. Poli and Ll. Huguet, *Error correcting codes*, Prentice Hall and Masson, 1992.

[11] L. H. Rowen, *Ring Theory*, Vol. 1, Academic Press, Boston, 1988.

[12] M. Sala, T. Mora, L. Perret et al. *Gröbner basis, Coding, and Cryptography*. Springer-Verlag, 2010.

[13] S. Sakata, The BMS Algorithm, *Gröbner basis, Coding, and Cryptography*. Springer-Verlag, 2010.