Manuscript submitted to
AIMS' Journals May 2016, 10(2): 229-254.
doi:10.3934/amc.2016003

ON THE IDEAL ASSOCIATED TO A LINEAR CODE

Irene Márquez-Corbella

INRIA Paris-Rocquencourt, SECRET Project-Team
78153 Le Chesnay Cedex, France.

Edgar Martínez-Moro

Mathematics Institute (IMUVa), University of Valladolid, Castilla, Spain.
Vernon Wilson Chair, Eastern Kentucky University.

Emilio Suárez-Canedo

Departament d'Enginyeria de la Informació i de les Comunicacions.
Universitat Autònoma de Barcelona (UAB)

(Communicated by the associate editor name)

Abstract. This article aims to explore the bridge between the algebraic structure of a linear code and the complete decoding process. To this end, we associate a specific binomial ideal $I_+(\mathcal{C})$ to an arbitrary linear code. The binomials involved in the reduced Gröbner basis of such an ideal relative to a degree-compatible ordering induce a uniquely defined test-set for the code, and this allows the description of a Hamming metric decoding procedure. Moreover, the binomials involved in the Graver basis of $I_+(\mathcal{C})$ provide a universal test-set which turns out to be a set containing the set of codewords of minimal support of the code.

1. Introduction.

In this paper, we associate a binomial ideal $I_+(\mathcal{C})$ to an arbitrary linear code $\mathcal{C}$ over any finite field $\mathbb{F}_q$. Several papers have been already devoted to the idea of associating the structure of a polynomial ideal to a linear code and thus, relate the reduction process on the first structure to the challenge of complete decoding on the second one. See [5, 16] and the references therein. Unfortunately, so far, this approach has not yet been applied succesfully to the non-binary case. Recently, some of these techniques were also studied by Aliasgari et al. [1] for non-binary group block codes, but the developed decoding algorithm was for the G-norm and not for the Hamming metric, recall that the G-norm is equivalent to the Hamming distance for $q = 2,\ 3$.

Therefore, the main achievement of this article has been to find the right structure that allows us to perform a complete decoding method as a reduction procedure for monomials in a polynomial ring. The decoding procedure presented here is a complete decoding algorithm that is, the procedure always provides the closest codeword to the received vector. Indeed we are ensured that it will retrieve the

2010 *Mathematics Subject Classification.* Primary: 94B05, 13P25; Secondary: 13P10.

Key words and phrases. Gröbner bases, Graver bases, Minimal support codewords.

The first two authors are partially supported by Spanish MICINN under project MTM2007-64704. The research of the first author is also supported by the FSMP postdoctoral program. The second author is also supported under project MTM2010-21580-C02-02 by Spanish MINCINN.

original sent codeword if the number of errors is smaller or equal to the error-correcting capability of the code.

First, in Section 2 we prove that $I_+(\mathcal{C})$ is finitely generated and the generators are provided by a basis of $\mathcal{C}$ and the binomials attached to the additive table of the base field $\mathbb{F}_q$. Or equivalently, $I_+(\mathcal{C})$ is generated by the binomials given by the $\mathbb{F}_q$-kernel of an explicit matrix. Note that this approach is a non-trivial extension of that of [14] to solve linear integer programming problems with modulo arithmetic conditions, that is, related with matrices over any ring of integers $\mathbb{Z}_s$.

Then, in Section 3, we show that a reduced Gröbner basis $\mathcal{G}$ of $I_+(\mathcal{C})$ relative to a degree-compatible ordering give us a complete decoding algorithm. The proposed procedure has some resemblance with the two gradient descent decoding algorithms known for binary codes [15, 2], note that both algorithms were unified in [6]. In our method, the test-set of $\mathcal{C}$ is replaced by $\mathcal{G}$ and addition is substituted for the reduction induced by $\mathcal{G}$. However, the idea behind our algorithm can be stated without the use of Gröbner basis theory as a *step by step decoding* [18] algorithm, which is a classical but very useful technique.

Next, in Section 4 we discuss an alternative for the computation of $\mathcal{G}$. A brief description of this technique as well as a complexity estimation can be found here. We can not expect that the algorithm runs in polynomial time since the complete decoding algorithm for general linear codes is an NP-hard problem [4], even if preprocessing is allowed (see [7]). However, the proposed algorithm is better suited for our case than the standard Buchberger's algorithm.

In Section 5, we consider the Graver basis associated to $I_+(\mathcal{C})$ which turns out to contain the set of codewords of minimal support of $\mathcal{C}$. The interest of this set is due to its relationship with the complete decoding problem and its applications in cryptography.

Finally, in Section 6 we apply the above approach to other classes of codes such as modular codes, codes defined over multiple alphabets or additive codes. The set of codewords of minimal support for modular codes has already been discussed in [16, 17] and in [1], where similar ideas are treated for a metric different from the Hamming.

1.1. **Preliminaries.** We begin with an introduction of basic definitions and some known results from coding theory over finite fields. By $\mathbb{K}$, $\mathbb{Z}$, $\mathbb{Z}_s$, $\mathbb{F}_q$ and $\mathbb{F}_q^*$, where q is a prime power, we denote an arbitrary finite field, the ring of integers, the ring of integers modulo s, any representation of a finite field with q elements, and the multiplicative group of nonzero elements of $\mathbb{F}_q$, respectively. For every finite field $\mathbb{F}_q$ the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic. A generator of the cyclic group $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$. Therefore, $\mathbb{F}_q$ consists of 0 and all powers from 1 to $q-1$ of that primitive element (see for instance [19]).

An $[n, k]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional subspace of $\mathbb{F}_q^n$. We define a *generator matrix* of $\mathcal{C}$ to be a $k \times n$ matrix G whose row vectors span $\mathcal{C}$, while a *parity check matrix* of $\mathcal{C}$ is an $(n-k) \times n$ matrix H whose null space is $\mathcal{C}$. We denote by $d_H(\cdot, \cdot)$ and $\mathrm{w}_H(\cdot)$ the *Hamming distance* and the *Hamming weight* on $\mathbb{F}_q^n$, respectively. We write d for the minimum distance of a linear code $\mathcal{C}$ and this is equal to its minimum weight. This parameter determines the error-correction capability of $\mathcal{C}$ which is given by $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, where $\lfloor x \rfloor$ is the largest integer at most x.

Remark 1. Let t be the error-correction capability of an $[n,k,d]$ code $\mathcal{C}$ over $\mathbb{F}_q$. Then, $d = 2t+1$ if d is odd and $d = 2t+2$ if d is even.

For a word $\mathbf{x} \in \mathbb{F}_q^n$, its support, denoted by $\mathrm{supp}(\mathbf{x})$, is defined as the set of nonzero coordinate positions, i.e., $\mathrm{supp}(\mathbf{x}) = \{i \mid x_i \neq 0\}$.

The *Voronoi region* of a codeword $\mathbf{c} \in \mathcal{C}$, denoted by $\mathrm{D}(\mathbf{c})$, is defined as:

$$\mathrm{D}(\mathbf{c}) = \left\{\mathbf{y} \in \mathbb{F}_q^n \mid d_H(\mathbf{y},\mathbf{c}) \leq d_H(\mathbf{y},\mathbf{c}') \text{ for all } \mathbf{c}' \in \mathcal{C} \setminus \{\mathbf{c}\}\right\}.$$

The union of all Voronoi regions of $\mathcal{C}$ is equal to $\mathbb{F}_q^n$. However, some points of $\mathbb{F}_q^n$ may be contained in several regions. Moreover, note that the Voronoi region of the all-zero codeword $\mathrm{D}(\mathbf{0})$ coincides with the set of coset leaders of $\mathcal{C}$.

A *test-set* $\mathcal{T}_\mathcal{C}$ for $\mathcal{C}$ is a set of codewords such that for every word $\mathbf{y} \in \mathbb{F}_q^n$, either $\mathbf{y}$ lies in the Voronoi region $\mathrm{D}(\mathbf{0})$, or there exists an element $\mathbf{t} \in \mathcal{T}_\mathcal{C}$ such that $\mathrm{w}_H(\mathbf{y}-\mathbf{t}) < \mathrm{w}_H(\mathbf{y})$.

Recall that the general principle of Gradient Descend Decoding algorithms (GDDA) is to use a certain set of codewords $\mathcal{T}_\mathcal{C}$ (namely test-set, formally described above) which has been precomputed and stored in memory in advance. Then the algorithm can be accomplished by recursively inspecting the test-set for the existence of an adequate element which is subtracted from the current vector. The following algorithm describes a gradient-like decoding algorithm for binary codes, this algorithm (for the binary case) appears in [3].

The following version of the GDD algorithm allows to reduce the size of the test-set for the q-ary case since once a vector is stored we can omit its multiples.

Algorithm 1: Gradient-like decoding

Data: The received word $\mathbf{y} \in \mathbb{F}_q^n$

Result: A codeword $\mathbf{c} \in \mathcal{C}$ that minimized the Hamming distance $d_H(\mathbf{c},\mathbf{y})$

Set $\mathbf{c} = \mathbf{0}$; **while** $\mathbf{y} \notin D(\mathbf{0})$ **do**

  Look for $\mathbf{z} \in \mathcal{T}_\mathcal{C}$ such that $\mathrm{w}_H(\mathbf{y} - \lambda\mathbf{z}) < \mathrm{w}_H(\mathbf{y})$ with $\lambda \in \mathbb{F}_q$;

  $\mathbf{y} \longleftarrow \mathbf{y} - \mathbf{z}$;

  $\mathbf{c} \longleftarrow \mathbf{c} + \mathbf{z}$

end while

Return $\mathbf{c} = \mathbf{y}$

In order to achieve complete decoding over a linear code $\mathcal{C}$ the aim of this article is to use a Gradient-like decoding method with the minimal test-set provided by a reduced Gröbner basis $\mathcal{G}$ of the ideal associated to the code $I_+(\mathcal{C})$ with respect to a degree compatible ordering. As we will see, we do not need to store all the binomials of such Gröbner basis but the codewords associated to the so-called *minimal test-set*.

A non-zero codeword $\mathbf{m}$ in $\mathcal{C}$ is said to be a *minimal support codeword* if there are no other codewords $\mathbf{c} \in \mathcal{C}$ such that $\mathrm{supp}(\mathbf{c}) \subset \mathrm{supp}(\mathbf{m})$. We denote by $\mathcal{M}_\mathcal{C}$ the set of codewords of minimal support of $\mathcal{C}$.

2. **The ideal associated to a linear code.** In this section we associate a binomial ideal to an arbitrary linear code provided by the rows of a generator matrix and the relations given by the additive table of the defining field.

Let $\mathbf{X}$ denote n vector variables $X_1, \ldots, X_n$ such that each variable X_i can be decomposed into $q-1$ components $x_{i,1}, \ldots, x_{i,q-1}$ with $i = 1, \ldots, n$. A monomial in $\mathbf{X}$ is a product of the form:

$$\mathbf{X}^{\mathbf{u}} = X_1^{\mathbf{u}_1} \cdots X_n^{\mathbf{u}_n} = \underbrace{\left(x_{1,1}^{u_{1,1}} \cdots x_{1,q-1}^{u_{1,q-1}}\right)}_{X_1^{\mathbf{u}_1}} \cdots \underbrace{\left(x_{n,1}^{u_{n,1}} \cdots x_{n,q-1}^{u_{n,q-1}}\right)}_{X_n^{\mathbf{u}_n}},$$

where $\mathbf{u} \in \mathbb{Z}_{\geq 0}^{n(q-1)}$. The total degree of $\mathbf{X}^{\mathbf{u}}$ is the sum $\deg(\mathbf{X}^{\mathbf{u}}) = \sum_{i=1}^{n} \sum_{j=1}^{q-1} u_{i,j}$. When $\mathbf{u} = (0, \ldots, 0)$, note that $\mathbf{X}^{\mathbf{u}} = 1$. Then the polynomial ring $\mathbb{K}[\mathbf{X}]$ is the set of all polynomials in $\mathbf{X}$ with coefficients in $\mathbb{K}$.

Let α be a primitive element of $\mathbb{F}_q$. We define by $\mathcal{R}_{X_i}$ the set of all the binomials on the variable X_i associated to the relations given by the additive table of the field $\mathbb{F}_q = \left\langle \alpha^j \mid j = 1, \ldots, q-1 \right\rangle \cup \{0\}$, i.e.,

$$\mathcal{R}_{X_i} = \left\{ \ \{x_{i,u}x_{i,v} - x_{i,w} \mid \alpha^u + \alpha^v = \alpha^w\} \quad \bigcup \quad \{x_{i,u}x_{i,v} - 1 \mid \alpha^u + \alpha^v = 0\} \ \right\},$$

with $i = 1, \ldots, n$. There are $\binom{q}{2}$ different binomials in $\mathcal{R}_{X_i}$.

We define $\mathcal{R}_{\mathbf{X}}$ as the following binomial ideal in $\mathbb{K}[\mathbf{X}]$: $\mathcal{R}_{\mathbf{X}} = \langle \cup_{i=1}^{n} \mathcal{R}_{X_i} \rangle$.

We will use the following characteristic crossing functions. These applications aim at describing a one-to-one correspondence between the finite field $\mathbb{F}_q$ with q elements and the standard basis of $\mathbb{Z}^{q-1}$, denoted as $E_q = \{\mathbf{e}_1, \ldots, \mathbf{e}_{q-1}\}$ where $\mathbf{e}_i$ is the unit vector with a 1 in the i-th coordinate and 0's elsewhere.

$$\Delta : \ \mathbb{F}_q \longrightarrow E_q \cup \{\mathbf{0}\} \subseteq \mathbb{Z}^{q-1} \qquad \text{and} \qquad \nabla : \ E_q \cup \{\mathbf{0}\} \longrightarrow \mathbb{F}_q$$

1. The map Δ replaces the element $\mathbf{a} = \alpha^i \in \mathbb{F}_q$ by the vector $\mathbf{e}_i$ and $0 \in \mathbb{F}_q$ by the zero vector $\mathbf{0} \in \mathbb{Z}^{q-1}$.
2. The map ∇ recovers the element $\alpha^j \in \mathbb{F}_q$ from the unit vector $\mathbf{e}_j$ and the zero element $0 \in \mathbb{F}_q$ from the zero vector $\mathbf{0} \in \mathbb{Z}^{q-1}$.

These maps will be used with matrices and vectors acting coordinate-wise. Although Δ is not a linear function. Note that we have

$$\mathbf{X}^{\Delta\mathbf{a}} \cdot \mathbf{X}^{\Delta\mathbf{b}} = \mathbf{X}^{\Delta\mathbf{a}+\Delta\mathbf{b}} = \mathbf{X}^{\Delta(\mathbf{a}+\mathbf{b})} \mod \mathcal{R}_{\mathbf{X}} \text{ for all } \mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n.$$

That is, the characteristic crossing functions induce the following maps:

$$\begin{array}{rcccccc} \tilde{\Delta} : & \mathbb{F}_q^n & \xrightarrow{\Delta} & (E_q \cup \{\mathbf{0}\})^n & \longrightarrow & \mathbb{K}[\mathbf{X}]/\mathcal{R}_{\mathbf{X}} \\ & \mathbf{a} & \longmapsto & \Delta\mathbf{a} & \longmapsto & \mathbf{X}^{\Delta\mathbf{a}} \end{array}$$

and

$$\begin{array}{rcccccc} \tilde{\nabla} : & \mathbb{K}[\mathbf{X}]/\mathcal{R}_{\mathbf{X}} & \longrightarrow & (E_q \cup \{\mathbf{0}\})^n & \xrightarrow{\nabla} & \mathbb{K}[\mathbf{X}] \\ & \mathbf{X}^{\mathbf{u}} & \longmapsto & \mathbf{u} & \longmapsto & \nabla\mathbf{u} \end{array}$$

Remark 2. Take into account that $\mathbb{F}_q$ contains $\phi(q-1)$ primitive elements, where ϕ is the Euler function (or equivalently, the number of integers less than and relative prime to $q-1$). Every primitive element of $\mathbb{F}_q$ can serve as a defining element of the characteristic crossing functions. But they will lead to different permutations of the components of the vector variable X_i.

Definition 2.1. The monomial $\mathbf{X}^{\mathbf{a}}$ is said to be in *standard form* if the exponents of each variable $x_{i,j}$ is 0 or 1, and two variables $x_{i,j}$ and $x_{i,l}$ do not appear in the same monomial. Therefore, a monomial is in standard form if it can be written as $\prod_{i=1}^{n} x_{i,j_i}$. Note that, any monomial modulo the additive relations $\{\mathcal{R}_{X_i}\}_{i=1,\ldots,n}$ is in standard form. Or equivalently, $\mathbf{X}^{\mathbf{a}}$ is in standard form if and only if there exists $\mathbf{b} \in \mathbb{F}_q^n$ such that $\mathbf{X}^{\mathbf{a}} = \mathbf{X}^{\Delta\mathbf{b}}$.

Moreover, if we multiply standard monomials with disjoint support then, Δ provides linearity in $\mathbb{K}[\mathbf{X}]$, i.e. :

$$\mathbf{X}^{\Delta \mathbf{a}}\mathbf{X}^{\Delta \mathbf{b}} = \mathbf{X}^{\Delta(\mathbf{a}+\mathbf{b})} \text{ if } \operatorname{supp}(\mathbf{a}) \cap \operatorname{supp}(\mathbf{b}) = \emptyset$$

A polynomial $f \in \mathbb{K}[\mathbf{X}]$ is said to be in *standard form* if each monomial in its decomposition is in standard form.

Remark 3. The following property is crucial for the results achieved in this article:

$$\text{If } \mathbf{X}^{\mathbf{a}} \text{ is in standard form, then } \deg(\mathbf{X}^{\mathbf{a}}) = \mathrm{w}_H(\nabla \mathbf{a}).$$

Unless otherwise stated, we simply write $\mathcal{C}$ for an $[n,k]$ linear code defined over the finite field $\mathbb{F}_q$. We define the *ideal associated* to $\mathcal{C}$ as the binomial ideal:

$$I(\mathcal{C}) = \left\langle \left\{ \mathbf{X}^{\Delta \mathbf{a}} - \mathbf{X}^{\Delta \mathbf{b}} \mid \mathbf{a} - \mathbf{b} \in \mathcal{C} \right\} \right\rangle \subseteq \mathbb{K}[\mathbf{X}].$$

For a fuller discussion of this algebraic structure see [6, 5, 16] and the references therein.

Given the rows of a generator matrix of $\mathcal{C}$, labelled by $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{F}_q^n$, we define the following ideal:

$$I_+(\mathcal{C}) \quad = \quad \left\langle \ \left\{ \mathbf{X}^{\Delta(\alpha^j \mathbf{w}_i)} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \quad \bigcup \quad \left\{ \mathcal{R}_{X_i} \right\}_{i=1,\ldots,n} \ \right\rangle \subseteq \mathbb{K}[\mathbf{X}].$$

Remark 4. Note that we encode all the information of our ideal in the exponents, thus we can always take $\mathbb{K} = \mathbb{F}_2$.

Lemma 2.2. *Let $f(\mathbf{X}) \in \mathbb{K}[\mathbf{X}]$. Then,*

$$f(\mathbf{X}) \in \mathcal{R}_{\mathbf{X}} \quad \textit{if and only if} \quad \begin{array}{l} f(\mathbf{X}) = \sum_{i \in I} \left(\mathbf{X}^{\Delta \mathbf{a}_i} \mathbf{X}^{\Delta \mathbf{b}_i} - \mathbf{X}^{\Delta \mathbf{c}_i} \right) \\ \textit{with } \mathbf{a}_i + \mathbf{b}_i - \mathbf{c}_i = \mathbf{0} \textit{ in } \mathbb{F}_q^n \ , \ \forall i \in I \end{array}$$

Proof. Let $f(\mathbf{X}) \in \mathcal{R}_{\mathbf{X}}$. Thus, $f(\mathbf{X})$ can be written as a finite linear combination of elements in the set of generators of $\mathcal{R}_{\mathbf{X}}$ with coefficients in $\mathbb{K} = \mathbb{F}_2$, i.e.

$$f(\mathbf{X}) = \sum_{j=1}^{n} \sum_{l \in L_j} r_{jl}$$

where $\{r_{jl} \mid l \in L_j\}$ is a subset of generators of $\mathcal{R}_{X_j}$ for all $j = 1, \ldots, n$. Following the definition of $\mathcal{R}_{X_j}$, the binomials r_{jl} can take two different forms:

1. $r_{jl} = x_{ju}x_{jv} - x_{jw}$ with $\alpha^u + \alpha^v = \alpha^w$ in $\mathbb{F}_q$. Or equivalently,
$$r_{jl} = X_j^{\Delta \alpha^u} X_j^{\Delta \alpha^v} - X_j^{\Delta \alpha^w} = \mathbf{X}^{\Delta \alpha^u \mathbf{e}_j} \mathbf{X}^{\Delta \alpha^v \mathbf{e}_j} - \mathbf{X}^{\Delta \alpha^w \mathbf{e}_j}$$
2. $r_{jl} = x_{ju}x_{jv} - 1$ with $\alpha^u + \alpha^v = 0$ in $\mathbb{F}_q$. Or equivalently,
$$r_{jl} = X_j^{\Delta \alpha^u} X_j^{\Delta \alpha^v} - 1 = \mathbf{X}^{\Delta \alpha^u \mathbf{e}_j} \mathbf{X}^{\Delta \alpha^v \mathbf{e}_j} - 1$$

Hence, $f(\mathbf{X}) = \sum_{i \in I} \mathbf{X}^{\Delta \mathbf{a}_i} \mathbf{X}^{\Delta \mathbf{b}_i} - \mathbf{X}^{\Delta \mathbf{c}_i}$ with $\mathbf{a}_i + \mathbf{b}_i - \mathbf{c}_i = \alpha^u \mathbf{e}_i + \alpha^v \mathbf{e}_i - \alpha^w \mathbf{e}_i = \mathbf{0}$ in $\mathbb{F}_q^n$ for certain indices u, v, w, where $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ denotes the standard basis of $\mathbb{F}_q^n$.

To show the converse it suffices to show that each binomial $\mathbf{X}^{\Delta \mathbf{a}_j} \mathbf{X}^{\Delta \mathbf{b}_j} - \mathbf{X}^{\Delta \mathbf{c}_j}$ in the decomposition of $f(\mathbf{X})$ belongs to $\mathcal{R}_{\mathbf{X}}$ with

$$\mathbf{a}_j + \mathbf{b}_j - \mathbf{c}_j = (a_{j,1}, \ldots, a_{j,n}) + (b_{j,1}, \ldots, b_{j,n}) - (c_{j,1}, \ldots, c_{j,n}) = \mathbf{0} \text{ in } \mathbb{F}_q^n \text{ for all } j \in I$$

We have that:

$$\begin{aligned}
\mathbf{X}^{\Delta\mathbf{a}_j}\mathbf{X}^{\Delta\mathbf{b}_j}-\mathbf{X}^{\Delta\mathbf{c}_j} &= \prod_{i=1}^{n} X_i^{\Delta a_{j,i}}X_i^{\Delta b_{j,i}}-\prod_{i=1}^{n} X_i^{\Delta c_{j,i}}\\
= \underbrace{\left(X_1^{\Delta a_{j,1}}X_1^{\Delta b_{j,1}}-X_1^{\Delta c_{j,1}}\right)}_{\mathcal{R}_{X_1}}\prod_{i=2}^{n} X_i^{\Delta a_{j,i}}X_i^{\Delta b_{j,i}} &+ X_1^{\Delta c_{j,1}}\left(\prod_{i=2}^{n} X_i^{\Delta a_{j,i}}X_i^{\Delta b_{j,i}}-\prod_{i=2}^{n} X_i^{\Delta c_{j,i}}\right)\\
&= \cdots = \underbrace{\left(X_1^{\Delta a_{j,1}}X_1^{\Delta b_{j,1}}-X_1^{\Delta c_{j,1}}\right)}_{\mathcal{R}_{X_1}}\prod_{i=2}^{n} X_i^{\Delta a_{j,i}}X_i^{\Delta b_{j,i}}\\
&+ \underbrace{\left(X_2^{\Delta a_{j,2}}X_2^{\Delta b_{j,2}}-X_1^{\Delta c_{j,2}}\right)}_{\mathcal{R}_{X_2}}X_1^{\Delta c_{j,1}}\prod_{i=3}^{n} X_i^{\Delta a_{j,i}}X_i^{\Delta b_{j,i}}\\
&+\dots+\underbrace{\left(X_n^{\Delta a_{j,n}}X_n^{\Delta b_{j,n}}-X_n^{\Delta c_{j,n}}\right)}_{\mathcal{R}_{X_n}}\prod_{i=1}^{n-1} X_i^{\Delta c_{j,i}}
\end{aligned}$$

Thus, $\mathbf{X}^{\Delta\mathbf{a}_j}\mathbf{X}^{\Delta\mathbf{b}_j}-\mathbf{X}^{\Delta\mathbf{c}_j}\in\mathcal{R}_{\mathbf{X}}$ for all $j\in I$. □

Theorem 2.3. *$I(\mathcal{C})=I_+(\mathcal{C})$.*

Proof. It is clear that $I_+(\mathcal{C})\subseteq I(\mathcal{C})$ since all binomials in the generating set of $I_+(\mathcal{C})$ belong to $I(\mathcal{C})$. Indeed:

- $\mathbf{X}^{\Delta\alpha^j\mathbf{w}_i}-1\in I(\mathcal{C})$ since $\alpha^j\mathbf{w}_i\in\mathcal{C}$ for all $i=1,\dots,k$ and $j=1,\dots,q-1$.
- The set of binomials of $\mathcal{R}_{X_i}$ are elements of $I(\mathcal{C})$ for all $i=1,\dots,n$ since each binomial represents the zero codeword by Lemma 2.2.

To show the converse it suffices to show that each binomial $\mathbf{X}^{\Delta\mathbf{a}}-\mathbf{X}^{\Delta\mathbf{b}}$ of $I(\mathcal{C})$ belongs to $I_+(\mathcal{C})$. By the definition of $I(\mathcal{C})$ we have that $\mathbf{a}-\mathbf{b}\in\mathcal{C}$. Hence

$$\mathbf{a}-\mathbf{b}=\lambda_1\mathbf{w}_1+\cdots+\lambda_k\mathbf{w}_k \text{ with } \lambda_1,\dots,\lambda_k\in\mathbb{F}_q.$$

Note that, if the binomials $\mathbf{z}_1-1$ and $\mathbf{z}_2-1$ belong to the ideal $I_+(\mathcal{C})$ then $\mathbf{z}_1\mathbf{z}_2-1=(\mathbf{z}_1-1)\mathbf{z}_2+(\mathbf{z}_2-1)$ also belongs to $I_+(\mathcal{C})$. On account of the previous line, we have:

$$\begin{aligned}
\mathbf{X}^{\Delta(\mathbf{a}-\mathbf{b})}-1 &= \left(\mathbf{X}^{\Delta\lambda_1\mathbf{w}_1}-1\right)\prod_{i=2}^{k}\mathbf{X}^{\Delta\lambda_i\mathbf{w}_i}+\left(\prod_{i=2}^{k}\mathbf{X}^{\Delta\lambda_i\mathbf{w}_i}-1\right) \mod \mathcal{R}_{\mathbf{X}}\\
&= \left(\mathbf{X}^{\Delta\lambda_1\mathbf{w}_1}-1\right)\prod_{i=2}^{k}\mathbf{X}^{\Delta\lambda_i\mathbf{w}_i}+\left(\mathbf{X}^{\Delta\lambda_2\mathbf{w}_2}-1\right)\prod_{i=3}^{k}\mathbf{X}^{\Delta\lambda_i\mathbf{w}_i}+\cdots+\\
&+ \left(\mathbf{X}^{\Delta\lambda_{k-1}\mathbf{w}_{k-1}}-1\right)\mathbf{X}^{\Delta\lambda_k\mathbf{w}_k}+\left(\mathbf{X}^{\Delta\lambda_k\mathbf{w}_k}-1\right) \mod \mathcal{R}_{\mathbf{X}}.
\end{aligned}$$

The last equation forces that

$$\mathbf{X}^{\Delta(\mathbf{a}-\mathbf{b})}-1\in\left\langle \left\{\mathbf{X}^{\Delta\alpha^j\mathbf{w}_i}-1\right\}_{\substack{i=1,\dots,k\\ j=1,\dots,q-1}} \cup \mathcal{R}_{\mathbf{X}}\right\rangle.$$

We have actually proved that $\mathbf{X}^{\Delta\mathbf{a}}-\mathbf{X}^{\Delta\mathbf{b}}\in I_+(\mathcal{C})$ since

$$\mathbf{X}^{\Delta\mathbf{a}}-\mathbf{X}^{\Delta\mathbf{b}}=\left(\mathbf{X}^{\Delta(\mathbf{a}-\mathbf{b})}-1\right)\mathbf{X}^{\Delta\mathbf{b}} \mod \mathcal{R}_{\mathbf{X}},$$

which completes the proof. □

Example 1. *Let us consider the* $[7,2]$ *linear code* $\mathcal{C}$ *over* $\mathbb{F}_3$ *with generator matrix*

$$G = \begin{pmatrix} 1 & 0 & 1 & 2 & 1 & 1 & 1 \\ 0 & 1 & 2 & 2 & 1 & 0 & 2 \end{pmatrix} \in \mathbb{F}_3^{2\times 7},$$

where the primitive element $\alpha = 2$ *generates the finite field* $\mathbb{F}_3 = \{0, \alpha = 2, \alpha^2 = 1\}$ *which gives us the following additive table:*

T_+	α	α^2
α	α^2	0
α^2	0	α

Or equivalently, $\{\ \alpha+\alpha=\alpha^2, \quad \alpha^2+\alpha=0, \quad \alpha^2+\alpha^2=\alpha\ \}$. *Therefore, we obtain the following binomials associated to the previous rules:*

$$\mathcal{R}_{X_i} = \{\ x_{i,1}^2 - x_{i,2}, \quad x_{i,1}x_{i,2} - 1, \quad x_{i,2}^2 - x_{i,1}\ \} \text{ with } i = 1,\ldots,7.$$

Let us label the rows of G *by* $\mathbf{w}_1$ *and* $\mathbf{w}_2$. *By Theorem 2.3, the ideal associated to the linear code* $\mathcal{C}$ *may be defined as the following binomial ideal:*

$$\begin{aligned} I_+(\mathcal{C}) &= \left\langle \left\{ \mathbf{X}^{\Delta\alpha^j\mathbf{w}_i} - 1 \right\}_{\substack{i=1,2\\ j=1,2}} \bigcup \ \{\mathcal{R}_{X_i}\}_{i=1,\ldots,7} \right\rangle \\ &= \left\langle \left\{ \begin{array}{r} x_{1,2}x_{3,2}x_{4,1}x_{5,2}x_{6,2}x_{7,2} - 1, \\ x_{1,1}x_{3,1}x_{4,2}x_{5,1}x_{6,1}x_{7,1} - 1, \\ x_{2,2}x_{3,1}x_{4,1}x_{5,2}x_{7,1} - 1, \\ x_{2,1}x_{3,2}x_{4,2}x_{5,1}x_{7,2} - 1 \end{array} \right\} \bigcup \ \{\mathcal{R}_{X_i}\}_{i=1,\ldots,7} \right\rangle. \end{aligned}$$

Remark 5. Let $B \in \mathbb{F}_q^{m\times n}$ be a matrix, $B^\perp$ be the matrix whose rows generate the null-space of B and $\{\mathbf{w}_1,\ldots,\mathbf{w}_k\}$ be a set of generators of the row space of the matrix B. We can define the following binomial ideal:

$$I(B) = \left\langle \left\{ \mathbf{X}^{\Delta\mathbf{a}} - \mathbf{X}^{\Delta\mathbf{b}} \mid B^\perp(\mathbf{a}-\mathbf{b})^T = \mathbf{0} \right\} \right\rangle.$$

Therefore, the construction presented above for linear codes can be generalized for any matrix defined over an arbitrary finite field, i.e. we have actually proved that $I(B) = I_+(\mathcal{C}) = I(\mathcal{C})$. Thus, the definition of $I_+(\mathcal{C})$ is in fact independent of the choice of the matrix B and just depends on the subspace $\mathcal{C}$, i.e. the subspace generated by the row-vectors of B.

Let B be a $m \times n$ matrix defined over $\mathbb{F}_q$ and let B_i denote the i-th column of the matrix B. Let $\mathbf{X}$ denote n vector variables $X_1,\ldots,X_n$ such that $X_i = (x_{i,1},\ldots,x_{i,q-1})$ for $1 \le i \le n$ and $\mathbf{Y}$ denote m vector variables $Y_1,\ldots,Y_m$ such that $Y_j = (y_{j,1},\ldots,y_{j,q-1})$ for $1 \le j \le m$. Let $\mathcal{R}_{Y_j} \subseteq \mathbb{K}[Y_j]$ be the binomial ideal consisting of all the binomials on the variables $Y_j = (y_{j,1},\ldots,y_{j,q-1})$ associated to the relations given by the additive table of the field $\mathbb{F}_q = \langle \alpha^j \mid j = 1,\ldots,q-1\rangle \cup \{0\}$ with $1 \le j \le m$, we define $\mathcal{R}_{\mathbf{Y}} = \langle \cup_{i=1}^m \mathcal{R}_{Y_i} \rangle \subseteq \mathbb{K}[\mathbf{Y}]$.

We denote by $\mathbb{K}[\mathbf{X},\mathbf{Y}]_{\mathrm{STD}}$ the set of polynomials in $\mathbb{K}[\mathbf{X},\mathbf{Y}]$ in standard form, i.e. $f \in \mathbb{K}[\mathbf{X},\mathbf{Y}]_{\mathrm{STD}}$ if each monomial in its decomposition is in standard form.

The ring homomorphism

$$\Theta_B : \quad \mathbb{K}[\mathbf{X},\mathbf{Y}]_{\mathrm{STD}} \quad \longrightarrow \quad \mathbb{K}[\mathbf{Y}]$$

is then defined by $\Theta_B(\mathbf{X}^{\Delta\mathbf{a}}) = \mathbf{Y}^{\Delta(\mathbf{a}B^T)}$ for every $\mathbf{a} \in \mathbb{F}_q^n$, and $\Theta_B(\mathbf{Y}^{\Delta\mathbf{a}}) = \mathbf{Y}^{\Delta\mathbf{a}}$. Thus, $\Theta_B(x_{i,j}) = \Theta_B(X_i^{\Delta\alpha^j}) = \Theta_B(\mathbf{X}^{\Delta(\alpha^j\mathbf{e}_i)}) = \mathbf{Y}^{\Delta(\alpha^j B_i^T)}$ where $\{\mathbf{e}_1,\ldots,\mathbf{e}_n\}$ denotes the standard basis of $\mathbb{F}_q^n$.

More generally, for every polynomial $f = \sum c_{\mathbf{v}} \mathbf{X}^{\Delta \mathbf{v}_x} \mathbf{Y}^{\Delta \mathbf{v}_y} \in \mathbb{K}[\mathbf{X}, \mathbf{Y}]_{\mathrm{STD}}$ we have that

$$\Theta_B(f) = f(\Theta_B(\mathbf{X}), \mathbf{Y}) = \sum c_{\mathbf{v}} \Theta_B\left(\mathbf{X}^{\Delta \mathbf{v}_x}\right) \mathbf{Y}^{\Delta \mathbf{v}_y}$$

This function can be found in [9].

Remark 6. Note that the restriction of Θ_B to $\mathcal{R}_{\mathbf{X}}$ is the function defined by:

$$\Theta_B : \mathcal{R}_{\mathbf{X}} \longrightarrow \mathcal{R}_{\mathbf{Y}}$$

This assertion is a direct consequence of Lemma 2.2.

Lemma 2.4. *Let us consider the matrix $B \in \mathbb{F}_q^{m\times n}$ and the vectors $\mathbf{a} \in \mathbb{F}_q^n$ and $\mathbf{b} \in \mathbb{F}_q^m$. The equality $\mathbf{a}B^T = \mathbf{b}$ holds if and only if $\Theta_B\left(\mathbf{X}^{\Delta \mathbf{a}}\right) \equiv \mathbf{Y}^{\Delta \mathbf{b}} \mod \mathcal{R}_{\mathbf{Y}}$.*

Proof. This lemma is a straightforward consequence of Lemma 2.2. □

Another ideal associated to the matrix $B \in \mathbb{F}_q^{m\times n}$ is defined by

$$I_B = \left\langle \left\{\Theta_B(x_{i,j}) - x_{i,j}\right\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,q-1}} \bigcup \left\{\mathcal{R}_{Y_j}\right\}_{j=1,\ldots,m} \right\rangle \subseteq \mathbb{K}[\mathbf{X}, \mathbf{Y}].$$

Lemma 2.5. *For a given polynomial $f \in \mathbb{K}[\mathbf{X}, \mathbf{Y}]_{\mathrm{STD}}$.*

$$f \in I_B \quad \textit{if and only if} \quad \Theta_B(f) \equiv 0 \mod \mathcal{R}_{\mathbf{Y}}.$$

Proof. For each $j = 1, \ldots, m$ we have $\binom{q}{2}$ different binomials in $\mathcal{R}_{Y_j}$. We denote by $r_{j,l}(Y_j)$ the polynomial at position l with respect to certain order in $\mathcal{R}_{Y_j}$ with $j = 1, \ldots, m$.

Let $f \in I_B$, by representing f with the generators of I_B, we have that

$$f(\mathbf{X}, \mathbf{Y}) = \sum_{i=1}^{n}\sum_{j=1}^{q-1} \lambda_{i,j}\left(\Theta_B(x_{i,j}) - x_{i,j}\right) + \sum_{j=1}^{m}\sum_{l=1}^{\binom{q}{2}} \beta_{j,l} r_{j,l}(Y_j)$$

with $\{\lambda_{i,j}\}_{\substack{i=1,\ldots,n \\ j=1,\ldots,q-1}}$ and $\{\beta_{j,l}\}_{\substack{j=1,\ldots,m \\ l=1,\ldots,\binom{q}{2}}} \in \mathbb{K}[\mathbf{X}, \mathbf{Y}]$.

Then,

$$\begin{aligned} \Theta_B(f) &= f\left(\Theta_B(\mathbf{X}), \mathbf{Y}\right) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{q-1} \Theta_B(\lambda_{i,j})\left(\Theta_B(x_{i,j}) - \Theta_B(x_{i,j})\right) + \sum_{j=1}^{m}\sum_{l=1}^{\binom{q}{2}} \Theta_B(\beta_{j,l}) r_{j,l}(Y_j) \\ &= \sum_{j=1}^{m}\sum_{l=1}^{\binom{q}{2}} \Theta_B(\beta_{j,l}) r_{j,l}(Y_j) \equiv 0 \mod \mathcal{R}_{\mathbf{Y}}. \end{aligned}$$

To prove the converse, first note that given any vector $\mathbf{a} = (a_1, \ldots, a_n) = (\alpha^{j_1}, \ldots, \alpha^{j_n}) \in \mathbb{F}_q^n$ the monomial $\mathbf{X}^{\Delta \mathbf{a}}$ can be written as:

$$\begin{aligned} X_1^{\Delta a_1} \cdots X_n^{\Delta a_n} &= x_{1,j_1} \cdots x_{n,j_n} = \prod_{i=1}^{n}\left(\Theta_B(x_{i,j_i}) + (x_{i,j_i} - \Theta_B(x_{i,j_i}))\right) \\ &= \prod_{i=1}^{n} \Theta_B(x_{i,j_i}) + \sum_{i=1}^{n} C_{i,j}\left(x_{i,j_i} - \Theta_B(x_{i,j_i})\right) \\ &= \Theta_B(\mathbf{X}^{\Delta \mathbf{a}}) + \sum_{i=1}^{n} C_{i,j}\left(x_{i,j_i} - \Theta_B(x_{i,j_i})\right) \end{aligned}$$

for some $\{C_{i,j}\}_{\substack{i=1,\ldots,n\\ j=1,\ldots,q-1}} \in \mathbb{K}[\mathbf{X},\mathbf{Y}]$. Note that, for all polynomial $f \in \mathbb{K}[\mathbf{X},\mathbf{Y}]_{\mathrm{STD}}$ there exists polynomials $g_i(\mathbf{Y}), h(\mathbf{Y}) \in \mathbb{K}[\mathbf{Y}]_{\mathrm{STD}}$ and $f_i(\mathbf{X}) \in \mathbb{K}[\mathbf{X}]_{\mathrm{STD}}$ such that

$$f(\mathbf{X},\mathbf{Y}) = \sum_{i\in I} f_i(\mathbf{X})g_i(\mathbf{Y}) + h(\mathbf{Y})$$

We have already show that we can write each $f_i(\mathbf{X})$ as $f_i(\Theta_B(\mathbf{X}))+\hat{f}_i$ with $\hat{f}_i \in I_B$. Thus,

$$f(\mathbf{X},\mathbf{Y}) = \underbrace{\sum_{i\in I} f_i(\Theta_B(\mathbf{X}))g_i(\mathbf{Y}) + h(\mathbf{Y})}_{=\Theta_B(f)\in\mathcal{R}_{\mathbf{Y}}} + \underbrace{\sum_{i\in I} \hat{f}_i g_i(\mathbf{Y})}_{\in I_B} \in I_B$$

□

Remark 7. Lemmas 2.5 and 2.4 are technical findings valid for any matrix B. On the following theorem we applied the above lemmas to a matrix $A^{\perp}$ where A is a generator matrix of the linear code $\mathcal{C}$.

Let us recall a well-known property of binomials ideals:

Corollary 1. [10, Corollary 1.3] *If $I \subseteq \mathbb{K}[X_1,\ldots,X_n]$ is a binomial ideal, then the elimination ideal $I \cap \mathbb{K}[X_1,\ldots,X_r]$ is a binomial ideal for every $r \leq n$.*

The following result shows how the ideal associated to the code $\mathcal{C}$ can also be defined as the ideal associated to a parity check matrix of $\mathcal{C}$ and also as the kernel of a polynomial ring homomorphism. Note that the ideals $I(A)$ and I_A are independent of the matrix A, they just depend on the subspace generated by the row-vectors of matrix A.

Theorem 2.6. $I_+(\mathcal{C}) = I(A) = I_{A^{\perp}} \cap \mathbb{K}[\mathbf{X}]$.

Proof. To prove that $I_+(\mathcal{C}) \subseteq I_{A^{\perp}} \cap \mathbb{K}[\mathbf{X}]$ it suffices to observe the following:

- $\Theta_{A^{\perp}}\left(\mathbf{X}^{\Delta(\alpha^j\mathbf{w}_i)} - 1\right) = \mathbf{Y}^{\Delta(\alpha^j\mathbf{w}_i)(A^{\perp})^T} - 1$ is the zero binomial, since $A\cdot A^{\perp} = \mathbf{0}$, for $j \in \{1,\ldots,q-1\}$ and $i \in \{1,\ldots k\}$.
- By Remark 6 we have that $\Theta_{A^{\perp}}(\mathcal{R}_{\mathbf{X}}) \subseteq \mathcal{R}_{\mathbf{Y}}$.

Therefore, applying Lemma 2.5 we conclude that the set of generators of $I_+(\mathcal{C})$ belongs to $I_{A^{\perp}} \cap \mathbb{K}[\mathbf{X}]$.

Conversely, let $f = \mathbf{X}^{\Delta\mathbf{a}} - \mathbf{X}^{\Delta\mathbf{b}}$ be any binomial of $I_{A^{\perp}} \cap \mathbb{K}[\mathbf{X}]$ with $\mathbf{a},\mathbf{b} \in \mathbb{F}_q^n$. Note that Corollary 1 allows us taking f as a binomial. Lemma 2.5 implies that $\Theta_{A^{\perp}}(f) = \mathbf{Y}^{\Delta(A^{\perp}\mathbf{a}^T)^T} - \mathbf{Y}^{\Delta(A^{\perp}\mathbf{b}^T)^T} \equiv 0 \mod \mathcal{R}_{\mathbf{Y}}$. Hence, by Lemma 2.4 we have that $A^{\perp}\mathbf{a}^T = A^{\perp}\mathbf{b}^T$, thus by Theorem 2.3 $f \in I(A) = I_+(\mathcal{C})$. □

3. **Decoding linear codes using a reduced Gröbner basis.** In this section we prove that the reduced Gröbner basis for the ideal $I_+(\mathcal{C})$ w.r.t. a degree compatible ordering on $\mathbb{K}[\mathbf{X}]$ (see for example [8] for a definition of such orderings) provides an algebraic decoding algorithm associated to computing the reduction of a monomial modulo the binomial ideal $I_+(\mathcal{C})$.

If we fix a term order $\prec$ then the *leading term* of a polynomial f with respect to $\prec$, denoted by $\mathrm{LT}_{\prec}(f)$, is the largest monomial among all monomials which occurs with non-zero coefficient in the expansion of f. Let I be an ideal in $\mathbb{K}[\mathbf{X}]$, then the *initial ideal* $\mathrm{in}_{\prec}(I)$ is the monomial ideal generated by the leading term of all the polynomials in I, i.e. $\mathrm{in}_{\prec}(I) = \{\mathrm{LT}_{\prec}(f) \mid f \in I\}$. The monomials which do not lie in the ideal $\mathrm{in}_{\prec}(I)$ are called *canonical monomials*. The semigroup ideal generated by the leading terms of a set of polynomials $F \subseteq \mathbb{K}[\mathbf{X}]$ w.r.t. $\prec$ is denoted by $\mathrm{LT}_\prec(F)$.

Definition 3.1. An ordering $\prec$ on $\mathbb{K}[\mathbf{X}]$ is said to be *degree compatible* if

$$\deg(\mathbf{X}^{\mathbf{u}}) < \deg(\mathbf{X}^{\mathbf{v}}) \text{ implies that } \mathbf{X}^{\mathbf{u}} \prec \mathbf{X}^{\mathbf{v}}$$

for all monomials $\mathbf{X}^{\mathbf{u}}, \mathbf{X}^{\mathbf{v}} \in \mathbb{K}[\mathbf{X}]$.

Definition 3.2. A finite set of nonzero polynomials $\mathcal{G} = \{g_1, \ldots, g_m\}$ of the ideal I is a Gröbner basis with respect to the term order $\prec$ if the leading terms of the elements of $\mathcal{G}$ generate the initial ideal $in_\prec(I)$. Moreover $\mathcal{G}$ is reduced if

1. g_i are monic for all $i = 1, \ldots, m$.
2. If $i \neq j$ then none of the monomials appearing in the expansion of g_j is divisible by $\mathrm{LT}_\prec(g_i)$.

A well known result is that every non-zero ideal has a unique reduced Gröbner basis. Let $\mathcal{G}$ be a Gröbner basis for an ideal $I \subset \mathbb{K}[\mathbf{X}]$ and let $f \in \mathbb{K}[\mathbf{X}]$. Then there is a unique remainder r on the division of f by $\mathcal{G}$ called the *normal form* of f and denoted by $\mathrm{Red}(f, \mathcal{G})$. For a deeper discussion of Gröbner bases we refer the reader to [8, 20].

Throughout this section, let $\mathcal{G} = \{g_1, \ldots, g_s\}$ be the reduced Gröbner basis of the ideal $I_+(\mathcal{C})$ with respect to $\succ$, where we take $\succ$ to be any degree compatible ordering on $\mathbb{K}[\mathbf{X}]$ with $X_1 \prec \ldots \prec X_n$.

Let us present some elementary facts about Gröbner basis of binomials ideals.

Proposition 1. [10, Proposition 1.1] *Let $\prec$ be an ordering on $\mathbb{K}[\mathbf{X}]$, and let $I \subseteq \mathbb{K}[\mathbf{X}]$ be a binomial ideal:*

1. *The reduced Gröbner basis $\mathcal{G}$ of I with respect to $\prec$ consists of binomials.*
2. *The normal form with respecto to $\prec$ of any term modulo $\mathcal{G}$ is again a term.*

Lemma 3.3. *All the elements of $\mathcal{G} \setminus \mathcal{R}_{\mathbf{X}}$ are in standard form.*

Proof. Suppose, contrary to our claim, that there exists an element $g = \mathbf{X}^{\mathbf{g}^+} - \mathbf{X}^{\mathbf{g}^-}$ in $\mathcal{G} \setminus \mathcal{R}_{\mathbf{X}}$ such that $\mathbf{X}^{\mathbf{g}^+}$ and/or $\mathbf{X}^{\mathbf{g}^-}$ are not in standard form.

By definition, there exists i, j such that $\mathbf{X}^{\Delta\alpha^j \mathbf{w}_i} = \mathbf{X}^{\mathbf{g}^+}\mathbf{X}^{\mathbf{u}}$. Therefore, if $l \in \mathrm{supp}(\mathbf{X}^{\mathbf{g}^+})$, then $l \in \mathrm{supp}(\mathbf{X}^{\Delta\alpha^j \mathbf{w}_i})$. Or equivalently, $\mathbf{X}^{\mathbf{g}^+}$ is in standard form.

Now assume that $\mathbf{X}^{\mathbf{g}^-}$ is not in standard form. That is,

$$\mathbf{X}^{\mathbf{g}^-} = \mathbf{X}^{\mathbf{v}} x_{i,j_1} x_{i,j_2} \text{ with } x_{i,j_1} x_{i,j_2} - x_{i,j_3} \in \mathcal{R}_{X_i} \text{ for some index } j_3.$$

We distinguish two cases:

- $x_{i,j_1} x_{i,j_2} - x_{i,j_3} \in \mathcal{G}$, which contradicts the fact that $\mathcal{G}$ is reduced.
- $x_{i,j_1} x_{i,j_2} - x_{i,j_3} \notin \mathcal{G}$. Then we deduce that there exists $\hat{g} \neq g$ such that $x_{i,j_1} x_{i,j_2}$ is divisible by $\mathrm{LT}_\prec(\hat{g})$, or equivalently, $\mathbf{X}^{\mathbf{g}^-}$ is divisible by $\mathrm{LT}_\prec(\hat{g})$, again a contradiction.

□

By the above Lemma, we know that all the elements of $\mathcal{G} \setminus \mathcal{R}_{\mathbf{X}}$ are in standard form so, for all $g_i \in \mathcal{G} \setminus \mathcal{R}_{\mathbf{X}}$ with $i = 1, \ldots, s$, we define

$$g_i = \mathbf{X}^{\Delta \mathbf{g}_i^+} - \mathbf{X}^{\Delta \mathbf{g}_i^-} \quad \text{with} \quad \mathbf{X}^{\Delta \mathbf{g}_i^+} \succ \mathbf{X}^{\Delta \mathbf{g}_i^-} \quad \text{and} \quad \mathbf{g}_i^+ - \mathbf{g}_i^- \in \mathcal{C}.$$

Remark 8. From the fact that $\mathcal{G}$ is a Gröbner basis for $I_+(\mathcal{C})$, then we can deduce that $\mathbf{X}^{\Delta \mathbf{c}_1} - \mathbf{X}^{\Delta \mathbf{c}_2} \in \langle \mathcal{G} \rangle$ if and only if $\mathbf{c}_1 - \mathbf{c}_2 \in \mathcal{C}$.

Theorem 3.4. *Let t be the error-correction capability of $\mathcal{C}$. If $\deg\left(\mathrm{Red}_{\prec}(\mathbf{X}^{\Delta\mathbf{a}},\mathcal{G})\right) \leq t$, then the vector $\mathbf{e}\in\mathbb{F}_q^n$ verifying that $\mathbf{X}^{\Delta\mathbf{e}} = \mathrm{Red}_{\prec}(\mathbf{X}^{\Delta\mathbf{a}},\mathcal{G})$ is the error vector corresponding to the received word $\mathbf{a}\in\mathbb{F}_q^n$. In other words, $\mathbf{c}=\mathbf{a}-\mathbf{e}\in\mathcal{C}$ is the closest codeword to $\mathbf{a}\in\mathbb{F}_q^n$. Otherwise $\mathbf{a}$ contains more than t errors.*

Proof. Following the definition of *"reduction of a polynomial with respect to $\mathcal{G}$"*; since $\mathbf{X}^{\Delta\mathbf{e}} = \mathrm{Red}_{\prec}(\mathbf{X}^{\Delta\mathbf{a}},\mathcal{G})$ there exists polynomials $f_1,\ldots,f_s\in\mathbb{K}[\mathbf{X}]$ such that

$$\mathbf{X}^{\Delta\mathbf{a}} = f_1g_1+\cdots+f_sg_s+\mathbf{X}^{\Delta\mathbf{e}}, \text{ or equivalently } \mathbf{X}^{\Delta\mathbf{a}}-\mathbf{X}^{\Delta\mathbf{e}}\in\langle\mathcal{G}\rangle. \tag{1}$$

Remark 8 now leads to $\mathbf{a}-\mathbf{e}\in\mathcal{C}$.

Assume that there exists $\mathbf{e}_2\in\mathbb{F}_q^n$ such that $\mathbf{a}-\mathbf{e}_2\in\mathcal{C}$ and $\mathrm{w}_H(\mathbf{e}_2)<\mathrm{w}_H(\mathbf{e})$; i.e. the total degree of $\mathbf{X}^{\Delta\mathbf{e}_2}$ is strictly smaller than the total degree of $\mathbf{X}^{\Delta\mathbf{e}}$, $\deg\left(\mathbf{X}^{\Delta\mathbf{e}_2}\right)<\deg\left(\mathbf{X}^{\Delta\mathbf{e}}\right)$. Then, by Lemma 8, there exists $\hat{f}_1,\ldots,\hat{f}_s\in\mathbb{K}[\mathbf{X}]$ such that $\mathbf{X}^{\Delta\mathbf{a}}=\hat{f}_1g_1+\cdots+\hat{f}_sg_s+\mathbf{X}^{\Delta\mathbf{e}_2}$, which contradicts the uniqueness of the normal form.

We have actually proved that the exponent of the normal form of $\mathbf{X}^{\Delta\mathbf{a}}$ is in the Voronoi region of $\mathbf{0}$. Therefore the normal form of $\mathbf{X}^{\Delta\mathbf{a}}$ is the unique solution for the system (1) if $\deg(\mathbf{X}^{\Delta\mathbf{e}})\leq t$. Otherwise $\mathbf{a}$ contains more than t errors. □

Remark 9. Take notice that we are implicitly assuming that $\mathrm{Red}_{\prec}(\mathbf{X}^{\Delta\mathbf{a}},\mathcal{G})$ is a monomial in standard form which is the case. Indeed, we have shown in Lemma 3.3 that all the elements of $\mathcal{G}\setminus\mathcal{R}_{\mathbf{X}}$ are in standard form. Thus, even if $\mathcal{R}_{\mathbf{X}}\not\subset\mathcal{G}$ then, the normal form of any monomial in standard form modulo $\mathcal{G}$ is again a monomial in standard form.

The following results shows that one of the elements in $\mathcal{G}$ provides the error-correction bound of $\mathcal{C}$.

Proposition 2. *Let t be the error-correction capability of $\mathcal{C}$, then*

$$\begin{aligned} t &= \min\left\{\mathrm{w}_H(\mathbf{g}_i^+)\mid g_i\in\mathcal{G}\setminus\{\mathcal{R}_{\mathbf{X}}\}\right\}-1\\ &= \min\left\{\deg(g_i)\mid g_i\in\mathcal{G}\setminus\{\mathcal{R}_{\mathbf{X}}\}\right\}-1. \end{aligned}$$

Proof. This proposition is analogous to [5, Theorem 3]. Let $\mathbf{c}$ be a minimum weight nonzero codeword of $\mathcal{C}$, i.e. $\mathrm{w}_H(\mathbf{c})=d$, where d is the minimum distance of $\mathcal{C}$. Let $\mathbf{X}^{\Delta\mathbf{c}_1}$ and $\mathbf{X}^{\Delta\mathbf{c}_2}$ be two monomials in $\mathbb{K}[\mathbf{X}]$ such that $\mathbf{X}^{\Delta\mathbf{c}}=\mathbf{X}^{\Delta\mathbf{c}_1}\mathbf{X}^{\Delta\mathbf{c}_2}$, $\mathrm{supp}(\mathbf{c}_1)\cap\mathrm{supp}(\mathbf{c}_2)=\emptyset$ and $\mathrm{w}_H(\mathbf{c}_1)=t+1$, that is to say $\mathbf{X}^{\Delta\mathbf{c}_1}\succ\mathbf{X}^{\Delta\mathbf{c}_2}$.

Then $\mathbf{X}^{\Delta\mathbf{c}_1}\mathbf{X}^{\Delta\mathbf{c}_2}-1\in I_+(\mathcal{C})$, or equivalently $\mathbf{X}^{\Delta\mathbf{c}_1}-\mathbf{X}^{\Delta-\mathbf{c}_2}\in I_+(\mathcal{C})$. Note that $\mathrm{w}_H(\mathbf{c}_2)=\mathrm{w}_H(-\mathbf{c}_2)$, thus $\mathbf{X}^{\Delta\mathbf{c}_1}\succ\mathbf{X}^{\Delta-\mathbf{c}_2}$. Therefore, we get that $\mathbf{X}^{\Delta\mathbf{c}_1}$ belongs to the initial ideal $\mathrm{in}(I_+(\mathcal{C}))$, so there must exists an index $i\in\{1,\ldots,s\}$ such that the leading term of $g_i\in\mathcal{G}$ divides $\mathbf{X}^{\Delta\mathbf{c}_1}$, and thus, $\mathrm{w}_H(\mathbf{g}_i^+)\leq\mathrm{w}_H(\mathbf{c}_1)=t+1$.

Now suppose that there exists $g_j\in\mathcal{G}\setminus\{\mathcal{R}_{X_l}\}_{l=1,\ldots,n}$ with $j\in\{1,\ldots,s\}$ such that $\mathrm{w}_H(\mathbf{g}_j^+)\leq t$. By definition, $\mathbf{g}_j^+-\mathbf{g}_j^-\in\mathcal{C}\setminus\{\mathbf{0}\}$, but

$$\mathrm{w}_H(\mathbf{g}_j^+-\mathbf{g}_j^-)\leq\mathrm{w}_H(\mathbf{g}_j^+)+\mathrm{w}_H(\mathbf{g}_j^-)\leq 2t<d,$$

which contradicts the definition of minimum distance of $\mathcal{C}$.

Therefore,

$$t<\min\left\{\mathrm{w}_H(\mathbf{g}_j^+)\mid g_j\in\mathcal{G}\setminus\{\mathcal{R}_{X_l}\}_{l=1,\ldots,n}\right\}\leq\mathrm{w}_H(\mathbf{g}_i^+)\leq t+1,$$

which provides the result. □

Proposition 3. $\mathrm{w}_H(\mathbf{g}_i^+)-\mathrm{w}_H(\mathbf{g}_i^-)\leq 1$ *for all* $i\in\{1,\ldots,s\}$.

Proof. Without loss of generality we assume that $i = 1$. We can distinguish two cases:

- The case when $\mathrm{supp}(\mathbf{g}_1^+) \cap \mathrm{supp}(\mathbf{g}_1^-) = \emptyset$.

  Let $\mathrm{w}_H(\mathbf{g}_1^+ - \mathbf{g}_1^-) = d_1$ and $t_1 = \lfloor \frac{d_1 - 1}{2} \rfloor$. Then we will show that either $\mathrm{w}_H(\mathbf{g}_1^+) = t_1$ or $\mathrm{w}_H(\mathbf{g}_1^+) = t_1 + 1$.

  Obviously $\mathrm{w}_H(\mathbf{g}_1^+) > t_1$, otherwise $\mathrm{w}_H\left(\mathbf{g}_1^+ - \mathbf{g}_1^-\right) \leq 2t_1 < d_1$. Now suppose $\mathrm{w}_H(\mathbf{g}_1^+) > t_1 + 1$. Let $x_{i,j}$ be any variable that belongs to the support of $\mathbf{X}^{\Delta \mathbf{g}_1^+}$, i.e. $\mathbf{X}^{\Delta \mathbf{g}_1^+} = x_{i,j}\mathbf{X}^{\Delta \mathbf{w}}$ with $\mathrm{w}_H(\mathbf{w}) + 1 = \mathrm{w}_H(\mathbf{g}_1^+)$. Then, there exists an index $l \in \{1, \ldots, q-1\}$ such that $x_{i,j}x_{i,l} - 1 \in \mathcal{R}_{X_i}$. Therefore, $x_{i,l}\left(\mathbf{X}^{\Delta \mathbf{g}_1^+} - \mathbf{X}^{\Delta \mathbf{g}_1^-}\right) \equiv \mathbf{X}^{\Delta \mathbf{w}} - x_{i,l}\mathbf{X}^{\Delta \mathbf{g}_1^-} \mod \mathcal{R}_{\mathbf{X}}$. Observe that

$$\mathrm{w}_H(\mathbf{g}_1^-) + 1 = d_1 - \mathrm{w}_H(\mathbf{g}_1^+) + 1 < t_1 + 1 \quad \text{and} \quad \mathrm{w}_H(\mathbf{w}) = \mathrm{w}_H(\mathbf{g}_1^+) - 1 > t_1.$$

  As a consequence, $\mathbf{X}^{\Delta \mathbf{w}} \succ x_{i,l}\mathbf{X}^{\Delta \mathbf{g}_1^-}$ and thus $\mathbf{X}^{\Delta \mathbf{w}} \in \mathrm{LT}(\mathcal{G} \setminus \{g_1\})$, which contradicts the fact that $\mathcal{G}$ is reduced.

  Therefore $\mathrm{w}_H(\mathbf{g}_1^+) = t_1 + 1$ and $\mathrm{w}_H(\mathbf{g}_1^-) = t_1 + 1$ if d_1 is even and $\mathrm{w}_H(\mathbf{g}_1^-) = t_1$, otherwise. In both cases we have that $\mathrm{w}_H(\mathbf{g}_1^+) - \mathrm{w}_H(\mathbf{g}_1^-) \leq 1$.

- A similar argument applies to the case $i \in \mathrm{supp}(\mathbf{g}_1^+) \cap \mathrm{supp}(\mathbf{g}_1^-)$.

  In other words, $g_1 = \mathbf{X}^{\mathbf{g}_1^+} - \mathbf{X}^{\Delta \mathbf{g}_1^-} = x_{i,j}\mathbf{X}^{\Delta \mathbf{a}} - x_{i,l}\mathbf{X}^{\Delta \mathbf{b}}$. There exists an integer $m \in \{1, \ldots, q-1\}$ such that $x_{i,j}x_{i,m} - 1$ and $x_{i,l}x_{i,m} - x_{i,v}$ belongs to $\mathcal{R}_{X_i}$. Thus $x_{i,m}g_1 \equiv \mathbf{X}^{\Delta \mathbf{a}} - x_{i,v}\mathbf{X}^{\Delta \mathbf{b}} \mod \mathcal{R}_{\mathbf{X}}$. Suppose that $\mathbf{X}^{\Delta \mathbf{a}} \succ x_{i,v}\mathbf{X}^{\Delta \mathbf{b}}$, then $\mathbf{X}^{\Delta \mathbf{a}} \in \mathrm{LT}(\mathcal{G} \setminus \{g_1\})$, is a contradiction. Therefore, $\mathrm{w}_H(\mathbf{b}) + 1 \geq \mathrm{w}_H(\mathbf{a})$ which establishes the desired formula.

  Note that it may happen that $l = j$. In this case we would have that $\mathrm{w}_H(\mathbf{b}) \geq \mathrm{w}_H(\mathbf{a})$, i.e. $\mathrm{w}_H(\mathbf{g}_i^-) \geq \mathrm{w}_H(\mathbf{g}_i^+)$ which is impossible except for the case of equality.

□

Definition 3.5. Let $\mathcal{G}$ be the reduced Gröbner basis of the ideal $I(\mathcal{C})$ w.r.t. a degree compatible ordering $\prec$ in $\mathbb{K}[\mathbf{X}]$. We define *"the reduction process $\rightarrow$"* of any monomial $\mathbf{X}^{\mathbf{w}} \in \mathbf{X}$ using $\mathcal{G}$ as:

1. Reduce $\mathbf{X}^{\mathbf{w}}$ to its standard form $\mathbf{X}^{\mathbf{w}'}$ using the relations $\mathcal{R}_{\mathbf{X}}$.
2. Reduce $\mathbf{X}^{\mathbf{w}'}$ w.r.t. $\mathcal{G} \setminus \mathcal{R}_{\mathbf{X}}$ by the usual one step reduction.

This reduction process is well defined since it is confluent and noetherian i.e.: if $\mathbf{X}^{\mathbf{w}} \in \mathbf{X}$ is an arbitrary term. Then:

i) The reduction process $\rightarrow$ is noetherian.
ii) If $\mathbf{X}^{\mathbf{w}} \rightarrow \mathbf{X}^{\mathbf{w}_1}$, $\mathbf{X}^{\mathbf{w}} \rightarrow \mathbf{X}^{\mathbf{w}_2}$ and $\mathbf{X}^{\mathbf{w}_1}$, $\mathbf{X}^{\mathbf{w}_2}$ are irreducible monomials modulo $\rightarrow$, then $\mathbf{X}^{\mathbf{w}_1} = \mathbf{X}^{\mathbf{w}_2}$.

Remark 10. The irreducible element corresponding to $\mathbf{X}^{\mathbf{w}}$ coincides with the *normal form* of $\mathbf{X}^{\mathbf{w}}$ w.r.t. $\mathcal{G}$, denoted by $\mathrm{Red}(\mathbf{X}^{\mathbf{w}}, \mathcal{G})$. The above theorem states that $\mathrm{Red}(\mathbf{X}^{\mathbf{w}}, \mathcal{G})$ is unique and computable by a typical Buchberger's reduction process.

Example 2. *Continuing with Example 1, note that the code has Hamming distance 5 so it corrects up to 2 errors. A reduced Gröbner basis $\mathcal{G}$ for the ideal $I_+(\mathcal{C})$ w.r.t. the* `degrevlex` *order with*

$$\underbrace{x_{1,1} < x_{1,2}}_{X_1} < \underbrace{x_{2,1} < x_{2,2}}_{X_2} < \cdots < \underbrace{x_{7,1} < x_{7,2}}_{X_7}$$

has 193 elements. It is easy to check that the binomial $G_1 = x_{3,1}x_{6,2}x_{7,1} - x_{1,1}x_{2,2}$ and all the generators of the ideal $\mathcal{R}_{\mathbf{X}}$ are elements of the reduced Gröbner basis.

Let us take the codeword $\mathbf{c} = (1,2,2,0,0,1,2)$ and add the error vector $\mathbf{e} = (2,2,0,0,0,0,0)$. Then the received word is $\mathbf{y} = (0,1,2,0,0,1,2) = \mathbf{c}+\mathbf{e}$ which corresponds to the monomial $w = x_{2,2}x_{3,1}x_{6,2}x_{7,1}$. Let us reduce w using $\mathcal{G}$:

$$w = x_{2,2}x_{3,1}x_{6,2}x_{7,1} \xrightarrow{G_1 = x_{3,1}x_{6,2}x_{7,1} - x_{1,1}x_{2,2}} x_{1,1}x_{2,2}x_{2,2} \xrightarrow{x_{2,2}^2 - x_{2,1} \in \mathcal{R}_{X_2}} x_{1,1}x_{2,1}.$$

The normal form of w modulo $\mathcal{G}$ is $x_{1,1}x_{2,1}$ which has weight 2, then $(2,2,0,0,0,0,0)$ is the error vector corresponding to w and the closest codeword is $x_{1,2}x_{2,1}x_{3,2}x_{6,2}x_{7,1}$, i.e. $\mathbf{c} = \mathbf{y}+\mathbf{e}$.

Remark 11. In [16] the authors describe another set of generators of the ideal $I(\mathcal{C})$ when $\mathcal{C}$ is a modular code, i.e. codes defined over $\mathbb{Z}_m$. In particular for codes over $\mathbb{F}_q$ with q prime, but not for the case p^r since $\mathbb{F}_{p^r} \ncong \mathbb{Z}_{p^r}$. In this article the ideal, denoted by $I_m(\mathcal{C})$, is defined by the rows of a generating matrix of the code and the modular relations of $\mathbb{Z}_m$. However, for $m \neq 2$ such ideal does not allow complete decoding since the reduction does not provide the minimum Hamming weight representative in the coset. In the following lines we give an example of what is discussed in this note.

Example 3. *Continuing with the Example 1, now suppose that we consider our code as a linear code over the alphabet $\mathbb{Z}_3 \cong \mathbb{F}_3$. Then we can define the ideal associated with $\mathcal{C}$ as the ideal generated by the following set of binomials (see* [16, Theorem 3.2] *for the definition of this ideal and the references given there)*

$$I_m(\mathcal{C}) = \left\langle \left\{ \begin{array}{c} y_1y_3y_4^2y_5y_6y_7 - 1, \\ y_2y_3^2y_4^2y_5y_7^2 - 1 \end{array} \right\} \bigcup \left\{ y_i^3 - 1 \right\}_{i=1,\ldots,7} \right\rangle \subseteq \mathbb{K}[y_1,\ldots,y_7].$$

If we compute a reduced Gröbner basis $\mathcal{G}$ of $I_m(\mathcal{C})$ w.r.t. a `degrevlex` *ordering with $y_1 < y_2 < \cdots < y_7$ we obtain 62 binomials. The elements*

$$G_1 = y_3^2y_6y_7^2 - y_1^2y_2 \quad \text{and} \quad G_2 = y_1^2y_2^2 - y_4y_5^2y_6$$

are elements of the reduced Gröbner basis.

Similarly to Example 2, let us take the codeword $\mathbf{c} = (1,2,2,0,0,1,2)$ and add the error $\mathbf{e} = (2,2,0,0,0,0,0)$. Then the received word is $\mathbf{y} = (0,1,2,0,0,1,2) = \mathbf{c}+\mathbf{e}$ which corresponds to the monomial $w = y_2y_3^2y_6y_7^2$. Let us reduce w using $\mathcal{G}$:

$$w = y_2y_3^2y_6y_7^2 \xrightarrow{G_1 = y_3^2y_6y_7^2 - y_1^2y_2} y_1^2y_2^2 \xrightarrow{G_2 = y_1^2y_2^2 - y_4y_5^2y_6} y_4y_5^2y_6.$$

The normal form of w modulo $\mathcal{G}$ is $y_4y_5^2y_6$ which does not correspond to the error vector.

Proposition 4. *The set $\mathcal{T} = \left\{ \mathbf{g}_i^+ - \mathbf{g}_i^- \mid i = 1,\ldots,s \right\}$ is a test-set for $\mathcal{C}$.*

Proof. Let $\mathbf{a} \in \mathbb{F}_q^n$ and suppose that $\mathbf{a} \notin D(\mathbf{0})$. According to Theorem 3.4 there exists $\mathbf{e} \in \mathbb{F}_q^n$ such that

$$\mathrm{Red}_{\prec}(\mathbf{X}^{\Delta\mathbf{a}}, \mathcal{G}) = \mathbf{X}^{\Delta\mathbf{e}} \text{ where } \mathrm{w}_H(\mathbf{e}) < \mathrm{w}_H(\mathbf{a}). \tag{2}$$

We now apply *"the reduction process $\rightarrow$"*. As $\mathbf{X}^{\Delta\mathbf{a}} - \mathbf{X}^{\Delta\mathbf{e}} \in I_+(\mathcal{C})$ with $\mathbf{X}^{\Delta\mathbf{a}} \succ \mathbf{X}^{\Delta\mathbf{e}}$, then $\mathbf{X}^{\Delta\mathbf{a}}$ is a multiple of $\mathrm{LT}_{\prec}(g_i)$ for some $i = 1,\ldots,s$. Or equivalently $\mathrm{supp}\left(\Delta\mathbf{g}_i^+\right) \subseteq \mathrm{supp}\left(\Delta\mathbf{a}\right)$, i.e. $\mathrm{w}_H(\mathbf{a} - \mathbf{g}_i^+) = \mathbf{w}_H(\mathbf{a}) - \mathbf{w}_H(\mathbf{g}_i^+)$. And consequently,

$$\mathrm{w}_H(\mathbf{a} - \left(\mathbf{g}_i^+ - \mathbf{g}_i^-\right)) \leq \mathrm{w}_H(\mathbf{a}) - \mathbf{w}_H(\mathbf{g}_i^+) + \mathrm{w}_H(\mathbf{g}_i^-) \leq \mathbf{w}_H(\mathbf{a}).$$

Note that the second inequality is due to the fact that $\mathbf{X}^{\Delta \mathbf{g}_i^+} \succ \mathbf{X}^{\Delta \mathbf{g}_i^-}$. Note that we have actually proved that $\mathbf{X}^{\Delta \mathbf{a}} \longrightarrow \mathbf{X}^{\Delta \mathbf{a} - (\mathbf{g}_i^+ - \mathbf{g}_i^-)}$. Repeated applications of *"the reduction process →"* enables us to arrive to $\mathbf{X}^{\Delta \mathbf{e}}$.

In case of equality of the above equation, it means that we have not chosen the right binomial $g_i \in \mathcal{G}$. Note that by Equation 2 there must exists an element $g_j \in \mathcal{G}$ such that $\mathrm{w}_H(\mathbf{a}) > \mathrm{w}_H(\mathbf{a} - \mathbf{g}_j^+ + \mathbf{g}_j^-)$. □

4. **FGLM technique to compute a Gröbner basis.** The aptly-named FGLM algorithm was developed by Faugère, Gianni, Lazard and Mora in [11]. This algorithm which only applies to zero-dimensional ideals allows to take a Gröbner basis from a relative easy calculations and convert it to the reduced Gröbner basis for the same ideal with respect to another monomial ordering.

In this section we present an algorithm to compute a reduced Gröbner basis of the ideal $I_+(\mathcal{C})$ which is associated to a linear code $\mathcal{C}$ defined over the finite field $\mathbb{F}_q$. This algorithm goes back to the work of Faugère et al. [11] and generalizes that of [5, 12, 13].

Throughout this section we require some theory of Gröbner Bases for submodules $M \subseteq \mathbb{K}[\mathbf{X}]^r$. We define a term $\mathbf{t}$ in $\mathbb{K}[\mathbf{X}]^r$ as an element of the form $\mathbf{t} = \mathbf{X}^{\mathbf{v}} \mathbf{e}_i$ where $\{\mathbf{e}_i\}_{i=1,\ldots,r}$ denote a standard basis of $\mathbb{K}^r$. A term ordering $\prec$ on $\mathbb{K}[\mathbf{X}]^r$ is a total well-ordering such that if $\mathbf{t}_1 \prec \mathbf{t}_2$ then $\mathbf{X}^{\mathbf{u}}\mathbf{t}_1 \prec \mathbf{X}^{\mathbf{u}}\mathbf{t}_2$ for every pair of terms $\mathbf{t}_1, \mathbf{t}_2 \in \mathbb{K}[\mathbf{X}]^r$ and every monomial $\mathbf{X}^{\mathbf{u}} \in \mathbb{K}[\mathbf{X}]$. Let $\prec$ be any monomial order on $\mathbb{K}[\mathbf{X}]$ the following term orderings are natural extensions of $\prec$ on $\mathbb{K}[\mathbf{X}]^r$:

- *Term-over-position* order (TOP order) first compares the monomials by $\prec$ and then the position within the vectors in $\mathbb{K}[\mathbf{X}]^r$. That is to say,
$$\mathbf{X}^\alpha \mathbf{e}_i \prec_{\mathrm{TOP}} \mathbf{X}^\beta \mathbf{e}_j \iff \mathbf{X}^\alpha \prec \mathbf{X}^\beta \quad \text{or} \quad \mathbf{X}^\alpha = \mathbf{X}^\beta \text{ and } i < j \ .$$
- *Position-over-term* order (POT order) which gives priority to the position of the vector in $\mathbb{K}[\mathbf{X}]^r$. In other words,
$$\mathbf{X}^\alpha \mathbf{e}_i \prec_{\mathrm{POT}} \mathbf{X}^\beta \mathbf{e}_j \iff i < j \quad \text{or} \quad i = j \text{ and } \mathbf{X}^\alpha \prec \mathbf{X}^\beta \ .$$

Definition 4.1. Let R be a commutative ring. Given a finitely generated R-module M and a set $z_1, \ldots, z_n$ of generators, a *syzygy* of M is an element $(g_1, \ldots, g_n) \in R^n$ for which $g_1 z_1 + \cdots + g_n z_n = 0$. The set of all syzygies relative to the given generating set is a submodule of R^n, called the module of syzygies.

If we fix a generator matrix $G \in \mathbb{F}_q^{k \times n}$ of $\mathcal{C}$ whose rows are labelled by $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ and we consider the following set of binomials:
$$F = \left\{ f_{i,j} = \mathbf{X}^{\Delta \alpha^j \mathbf{w}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \subseteq \mathbb{K}[\mathbf{X}].$$
Then, by Theorem 2.3, the set $F \cup \{\mathcal{R}_{X_i}\}_{i=1,\ldots,n}$ generates the ideal $I_+(\mathcal{C})$.

Let $r = k(q-1)+1$. Let M be the syzygy module in $\mathbb{K}[\mathbf{X}]^r$ with generating set
$$\hat{F} = \{-1, f_{1,1}, \ldots, f_{1,q-1}, \ldots, f_{k,1}, \ldots, f_{k,q-1}\},$$
where the binomials $\{\mathcal{R}_{X_i}\}_{i=1,\ldots,n}$ are considered implicit on the operations. Note that each syzygy corresponds to a solution of the following equation:
$$-\beta_0 + \sum_{i=1}^{k} \sum_{j=1}^{q-1} \beta_{(i-1)(q-1)+j} f_{i,j} = 0 \ \text{ with } \beta_l \in \mathbb{K}[\mathbf{X}] \text{ for } l = 1, \ldots, k(q-1).$$

Hence, the first component of any syzygy of the module M indicates an element of the ideal generated by F.

The outline of the proposed algorithm consist of three main parts:

1. **Initialization:** Take a Gröbner basis, namely $\mathcal{G}_1$, of the submodule $M \subseteq \mathbb{K}[\mathbf{X}]^r$ and choose a term ordering $\prec_2$ on $\mathbb{K}[\mathbf{X}]$. The set $\mathcal{G}_2$ is initially empty but will become the reduced Gröbner basis of M w.r.t. a TOP ordering induced by $\prec_2$.

   Remark 12. Consider the set $\mathcal{G}_1 = \left\{g_{ij} = \mathbf{e}_1 f_{i,j} + \mathbf{e}_{(i-1)(q-1)+j+1}\right\}$ where $\mathbf{e}_l$ denotes the unit vector of length r with a one in the l-th position. We claim that $\mathcal{G}_1$ is a basis for M.

   Moreover, $\mathcal{G}_1$ is a Gröbner basis of M relative to a POT ordering $\prec_{\mathbf{w}}$ induced by an ordering $\prec$ in $\mathbb{K}[\mathbf{X}]$ and the weight vector

   $$\mathbf{w} = (1, \mathrm{LT}_{\prec}(f_{1,1}), \ldots, \mathrm{LT}_{\prec}(f_{k,q-1})).$$

   Note that the leading term of g_{ij} with respect to $\prec_{\mathbf{w}}$ is $\mathbf{e}_{(i-1)(q-1)+j+1}$.

2. **Main Loop:** Use the FGLM algorithm running through the terms of $\mathbb{K}[\mathbf{X}]^r$ using a TOP ordering induced by $\prec_2$ to get the Gröbner basis $\mathcal{G}_2$ of M relative to the new ordering.

   Remark 13. It is immediate that the normal form with respect to $\mathcal{G}_1$ of any element is zero except in the first component, that is to say, the linear combinations that Fitzpatrick's algorithm [12] look for, take place in this component.

3. **Conclusion:** It is easily seen that the first component of the elements of $\mathcal{G}_2$ forms a Gröbner basis of $I_+(\mathcal{C})$ w.r.t. $\prec_2$.

Three structures are used in the algorithm:

- The list `List` whose elements are of the specific type $\mathbf{v} = (\mathbf{v}[1], \mathbf{v}[2])$ where $\mathbf{v}[2]$ represents an element in $\mathbb{K}[\mathbf{X}]$ which can be expressed as

  $$\mathbf{v}[2] = \mathbf{v}[1] + \sum_{i=1}^{k} \sum_{j=1}^{q-1} \lambda_{(i-1)(q-1)+j} f_{i,j} \text{ with } \lambda_1, \ldots, \lambda_{r-1} \in \mathbb{K}[\mathbf{X}].$$

  Thus, the coefficient vector $(\mathbf{v}[1], \lambda_1, \ldots, \lambda_{r-1}) \in \mathbb{K}[\mathbf{X}]^r$ is the associated vector of $\mathbf{v}[2]$ on the module M. And $\mathbf{v}[1]$ represents the first component of such vector.
- The list G_T which ends up being a reduced Gröbner basis of $I_+(\mathcal{C})$ w.r.t. a degree compatible ordering $\prec_T$.
- The list $\mathcal{N}$ of terms that are reduced with respect to G_T, i.e. the set of standard monomials.

We also require the following subroutines:

- `InsertNexts(w, List)` inserts the product $\mathtt{w}x$ for $x \in \mathbf{X}$ in `List` and removes the duplicates, where the binomials of $\{\mathcal{R}_{X_i}\}_{i=1,\ldots,n}$ are considered as implicit in the computation. Then the elements of `List` are sorted by increasing order w.r.t. $\prec_T$ in the first component of the pairs and in case of equality by comparing the second component. Recall that

  $$\mathbf{X} = \{X_1, \ldots, X_n\} = \{x_{1,1}, \ldots, x_{1,q-1}, \ldots, x_{n,1}, \ldots, x_{n,q-1}\}.$$
- `NextTerm(List)` removes the first element from the list `List` and returns it.
- `Member(v,[`$\mathbf{v}_1, \ldots, \mathbf{v}_r$`])` returns j if $\mathtt{v} = \mathbf{v}_j$ or `false` otherwise.

Remark 14. Note that the computation of $\mathbf{X}^{\mathbf{a}} x_{i,j}$ modulo the ideal $\mathcal{R}_{\mathbf{X}}$, with $\mathbf{a} \in \mathbb{Z}^{n(q-1)}$, acts like the operation $\nabla \mathbf{a} + \alpha^j \mathbf{e}_i$ in the finite field $\mathbb{F}_q^n$ where $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ denotes a standard basis of $\mathbb{F}_q^n$.

Algorithm 2: Adapted FGLM algorithm for $I_+(\mathcal{C})$

Data: The rows $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{F}_q^n$ of a generator matrix of an $[n, k]$ linear code $\mathcal{C}$ defined over $\mathbb{F}_q$ and a degree compatible ordering $\prec_T$ on $\mathbb{K}[\mathbf{X}]$.
Result: A reduced Gröbner basis G_T of the ideal $I_+(\mathcal{C})$ w.r.t. $\prec_T$.

$\texttt{List} \longleftarrow \left[(1,1), \left\{ (1, \mathbf{X}^{\Delta \alpha^j \mathbf{w}_i}) \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \right]$;
$G_T \longleftarrow \emptyset$; $\mathcal{N} \longleftarrow \emptyset$; $r \longleftarrow 0$;
while $\texttt{List} \neq \emptyset$ **do**
  $\mathbf{w} \longleftarrow \texttt{NextTerm}(\texttt{List})$;
  if $\mathbf{w}[1] \notin \mathrm{LT}_{\prec_T}(G_T)$ **then**
    $j = \texttt{Member}(\mathbf{w}[2], [\mathbf{v}_1[2], \ldots, \mathbf{v}_r[2]])$;
    if $j \neq \texttt{false}$ **then**
      $G_T \longleftarrow G_T \cup \{\mathbf{w}[1] - \mathbf{v}_j[1]\}$;
    else
      $r \longleftarrow r + 1$;
      $\mathbf{v}_r \longleftarrow \mathbf{w}$;
      $\mathcal{N} \longleftarrow \mathcal{N} \cup \{\mathbf{v}_r[1]\}$;
      $\texttt{List} = \texttt{InsertNexts}(\mathbf{w}, \texttt{List})$;
    end if
  end if
end while

Theorem 4.2. *Algorithm 2 computes a reduced Gröbner basis of the ideal associated to a given linear code $\mathcal{C}$ of parameters $[n, k]$ defined over $\mathbb{F}_q$.*

Proof. The proof of the algorithm is an extension of that in [12, Algorithm2.1] and therefore, is also a generalization of the FGLM algorithm [11]. Let $G \in \mathbb{F}_q^{k \times n}$ be a generator matrix of $\mathcal{C}$. We label the rows of G by $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\} \subseteq \mathbb{F}_q^n$.

By Theorem 2.3 the ideal associated to the linear code $\mathcal{C}$ may be defined as the following binomial ideal:

$$\begin{aligned} I_+(\mathcal{C}) &= \left\langle \left\{ \mathbf{X}^{\Delta \alpha^j \mathbf{w}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \left\{ \mathcal{R}_{X_i} \right\}_{i=1,\ldots,n} \right\rangle \\ &= \left\langle \left\{ f_{i,j} \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \left\{ \mathcal{R}_{X_i} \right\}_{i=1,\ldots,n} \right\rangle. \end{aligned}$$

We first show that G_T is a subset of binomials of the ideal $I_+(\mathcal{C})$. The proof is based on the following observation: $\mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}} \in G_T$ if and only if it corresponds to the first component of a syzygy in the module M. In other words,

$$\mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}} \equiv \sum_{i=1}^{k} \sum_{j=1}^{q-1} \lambda_{(i-1)(q-1)+j} f_{i,j} \mod \mathcal{R}_{\mathbf{X}} \text{ with } \lambda_1, \ldots, \lambda_{r-1} \in \mathbb{K}[\mathbf{X}],$$

or equivalently, $\mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}} \in I_+(\mathcal{C})$.

Moreover, we claim that the initial ideal of $I_+(\mathcal{C})$ w.r.t. $\prec_T$ is generated by the leading terms of polynomials in G_T. Indeed, by Theorem 2.3, any binomial $f(\mathbf{X})$ of $I_+(\mathcal{C})$ can be written uniquely as a linear combination of elements in the generator set $F = \{f_{i,j}\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}}$ modulo the ideal $\mathcal{R}_{\mathbf{X}}$, i.e.

$$f(\mathbf{X}) = \sum_{i=1}^{k}\sum_{j=1}^{q-1} \lambda_{(i-1)(q-1)+j} f_{i,j} \mod \mathcal{R}_{\mathbf{X}} \text{ with } \lambda_1, \ldots, \lambda_{r-1} \in \mathbb{K}[\mathbf{X}].$$

Therefore, $\mathrm{LT}_{\prec_T}(f(\mathbf{X}))$ is a multiple of the leading term of an element of F that appears on its decomposition. But $\mathrm{LT}_{\prec_T}(f_{i,j}(\mathbf{X}))$ cannot be in $\mathcal{N}$ for all $i = 1, \ldots, k$ and $j = 1, \ldots, q-1$. To see this, note that the first element introduced in the set $\mathcal{N}$ is always 1 and

$$1 = \mathbf{X}^{\Delta\alpha^j \mathbf{w}_i} - f_{i,j} \text{ i.e. } \mathrm{Red}_{\prec_T}\left(\mathbf{X}^{\Delta\alpha^j \mathbf{w}_i}, F\right) = 1,$$

which implies that $\mathbf{X}^{\Delta\alpha^j \mathbf{w}_i} - 1 \in G_T$.

By definition, G_T is reduced since we only consider on the algorithm terms which are not divisible by any leading term of the Gröbner basis.

Finally, since $I_+(\mathcal{C})$ has finite dimension, then the number of terms in $\mathcal{N}$ is bounded. Note that at each iteration of the main loop either the size of `List` decreases or the size of $\mathcal{N}$ increases, thus there are only a finite number of iterations. This completes the proof of the algorithm. □

Remark 15. Recall that the dimension of the quotient vector space $\mathbb{F}_q^n/\mathcal{C}$ is $n-k$. Moreover, if $\mathcal{C}$ can correct up to t errors, then every word $\mathbf{e}$ of weight $\mathrm{w}_H(\mathbf{e}) \leq t$ is the unique coset leader (vectors of minimal weight in their cosets) of its coset modulo $\mathcal{C}$. In other words, all monomials of degree less than t modulo the ideal $\mathcal{R}_{\mathbf{X}}$ should be standard monomials for G_T.

Note that the writing rules given by the ideal $\mathcal{R}_{\mathbf{X}}$ implies that "the exponent of each variable $x_{i,j}$ is 0 or 1" and "two different variables $x_{i,j}$ and $x_{i,l}$ can not appear in a monomial". Thus, the number of standard monomials of a t-error correcting code is at least

$$M = \sum_{l=1}^{t} (q-1)^l \binom{n}{l}. \tag{3}$$

Accordingly, if $q^{n-k} = M$, then all cosets have a unique coset leader of weight smaller or equal to t. Codes that achieve this equality are the so-called *perfect codes*. Also for perfect codes, their Voronoi regions are disjoints. Otherwise, there must appear some cosets leaders of weight at most $\rho(\mathcal{C})$, where $\rho(\mathcal{C})$ denotes the covering radius of $\mathcal{C}$, but never as the unique leader, or equivalently there exists standard monomials of degree up to $\rho(\mathcal{C})$. Recall that $\rho(\mathcal{C})$ coincide with the largest weight among all the cosets leaders of $\mathcal{C}$, so $\rho(\mathcal{C}) = t$ if $\mathcal{C}$ is a perfect code.

By Proposition 3 in the worst case, a minimal generator of the initial ideal $\mathrm{in}_<(I_+(\mathcal{C}))$ has degree $\rho(\mathcal{C})+1$ where $<$ is a degree compatible ordering.

Theorem 4.3. *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$ of length n and covering radius $\rho(\mathcal{C})$. If the basis field operations need an unit time, then Algorithm 2 needs a total time of $\mathcal{O}\left(Dn^2(q-1)\log(q)\right)$, where*

$$D = \sum_{i=1}^{\rho(\mathcal{C})+1} (q-1)^i \binom{n}{i}.$$

Proof. The main time of the algorithm is devoted to the management of `InsertNexts`. In each main loop iteration this function first introduces $n(q-1)$ new elements to the list `List`, then compares all the elements and finally eliminates redundancy.

Note that comparing two monomials in $\mathbb{K}[\mathbf{X}]$ is equivalent to comparing vectors in $\mathbb{F}_q^n$, thus we need $\mathcal{O}(n\log(q))$ field operations.

At iteration i, after inserting the new elements in the list `List` we would have at most D_i elements where

$$D_i = \underbrace{(q-1)k}_{\substack{\text{Elements that}\\ \text{initialized } \texttt{List}}} + \underbrace{i\,(n(q-1))-i}_{\substack{\text{At each iteration}\\ \text{the first element is removed}\\ \text{and we add n(q-1)new elements}}}.$$

By Remark 15 we have an upper bound D for the number of times that `InsertNexts` should be called. This gives a total time of

$$\mathcal{O}\left(n\log(q)\left((q-1)k + D\left(n(q-1)\right)-D\right)\right) \sim \mathcal{O}\left(Dn^2(q-1)\log(q)\right).$$

□

Algorithm 3: Algorithm for computing a minimal Gröbner test-set for $\mathcal{C}$

Data: The rows $\{\mathbf{w}_1,\ldots,\mathbf{w}_k\} \subseteq \mathbb{F}_q^n$ of a generator matrix of the code $\mathcal{C}$ and a degree compatible ordering $\prec_T$ on $\mathbb{K}[\mathbf{X}]$.

Result: A minimal Gröbner test-set $\mathcal{T}$ for $\mathcal{C}$.

// For each binomial $\mathbf{g} = \mathbf{X}^{\mathbf{a}} - \mathbf{X}^{\mathbf{b}}$ we define $\overline{\mathbf{g}} := \nabla\mathbf{a} - \nabla\mathbf{b} \in \mathbb{F}_q^n$

// Add the following lines after Step 7 of Algorithm 2.

```
g ⟵ w[1] − v_j[1];
if supp(ḡ) ⊅ supp(ḡ_i) for all g_i ∈ G_T \ {g} then
  | T ⟵ T ∪ {ḡ}
end if
```

By Proposition 4, the set of codewords related with the exponents of a reduced Gröbner basis of the ideal associated with a linear code $\mathcal{C}$ with respect to a degree compatible ordering induces a test-set $\mathcal{T}$ for $\mathcal{C}$. However, not all the codewords of this test-set are codewords of minimal support, i.e. this set is somehow redundant. We can reduce the number of codewords to the set $\mathcal{T}\cap\mathcal{M}_{\mathcal{C}}$, which is still a test-set for the code $\mathcal{C}$, using Algorithm 3. Moreover, once a vector is stored we can omit its multiples as proposed Algorithm 1. The obtained test-set is called a *minimal Gröbner test-set*.

On the following example we compared the cost storage of the proposed GDDA with Complete Syndrome Decoding.

Example 4. *Consider $\mathcal{C}$ an $[9,3,3]$ ternary code with generator matrix*

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 0 \end{pmatrix} \in \mathbb{F}_3^{3\times 9}$$

This code has $3^3 = 27$ codewords. If we compute a reduced Gröbner basis $\mathcal{G}$ of $I_+(\mathcal{C})$ we obtained a test-set consisting of 24 codewords. But for decoding we just need a minimal test-set (we can eliminate those elements which are multiples and those *codewords which are not of minimal support). That is, if we apply **GDDA** we just need to save in memory 12 elements:*

$(1,2,1,1,1,2,0,0,2)$	$(0,1,2,2,2,2,0,2,1)$	$(1,1,2,2,2,0,0,1,1)$
$(0,1,1,1,0,0,2,1,1)$	$(0,0,1,1,2,2,1,1,0)$	$(0,1,0,0,1,1,1,0,1)$
$(1,2,0,0,2,0,2,2,2)$	$(1,1,0,0,1,2,1,2,1)$	$(2,0,0,0,0,2,0,1,0)$
$(1,1,1,1,0,1,2,0,1)$	$(1,0,1,1,2,0,1,0,0)$	

*But if we apply **Complete Syndrome Decoding** we need to store* $\frac{q^{n-k}-1}{(q-1)} = 364$ *coset leaders (we use here the same trick, neither the zero vector nor the multiples of a coset leader are stored).*

Our experimental results are in good agreement with the following conjecture.

Conjecture 1. *Given an* $[n,k]$ *linear code* $\mathcal{C}$ *over* $\mathbb{F}_q$*. Let* $\mathcal{T}_\mathcal{G}$ *be a test-set for* $\mathcal{C}$ *induced by a reduced Gröbner basis* $\mathcal{G}$ *of the ideal* $I(\mathcal{C})$ *w.r.t. a degree compatible ordering. Then,*

$$|T_\mathcal{G}| < \frac{q^{n-k}-1}{(q-1)}$$

That is, the cost storage of GDDA is smaller than Complete Syndrome Decoding.

5. **Set of codewords of minimal support.** We define the *Universal Gröbner basis* of $I_+(\mathcal{C})$, denoted by $\mathcal{U}_\mathcal{C}$, to be the union of all reduced Gröbner Bases $\mathcal{G}_\prec$ of $I_+(\mathcal{C})$ as $\prec$ runs over all terms orders of $\mathbb{K}[\mathbf{X}]$. A binomial $\mathbf{X}^{\mathbf{u}_1} - \mathbf{X}^{\mathbf{u}_2}$ in $I_+(\mathcal{C})$ is called *primitive* if there exists no other binomial $\mathbf{X}^{\mathbf{v}_1} - \mathbf{X}^{\mathbf{v}_2} \in I_+(\mathcal{C})$ such that $\mathbf{X}^{\mathbf{v}_1}$ divides $\mathbf{X}^{\mathbf{u}_1}$ and $\mathbf{X}^{\mathbf{v}_2}$ divides $\mathbf{X}^{\mathbf{u}_2}$.

Lemma 5.1. *Every binomial in* $\mathcal{U}_\mathcal{C}$ *is primitive.*

Proof. It is a straightforward generalization of [20, Lemma 4.6]. Let us fix an arbitrary term ordering $\prec$ in $\mathbb{K}[\mathbf{X}]$, and let $\mathcal{G}_\prec$ be the reduced Gröbner basis of $I_+(\mathcal{C})$ w.r.t. $\prec$. By definition, for any binomial $\mathbf{X}^{\mathbf{u}_1} - \mathbf{X}^{\mathbf{u}_2}$ in $\mathcal{G}_\prec$ with $\mathbf{X}^{\mathbf{u}_1} \succ \mathbf{X}^{\mathbf{u}_2}$, $\mathbf{X}^{\mathbf{u}_1}$ is a minimal generator of the initial ideal $\mathrm{in}_\prec(I_+(\mathcal{C}))$ and $\mathbf{X}^{\mathbf{u}_2}$ is a canonical monomial. Now suppose that $\mathbf{X}^{\mathbf{u}_1} - \mathbf{X}^{\mathbf{u}_2}$ is not primitive, or equivalently there exists another binomial $\mathbf{X}^{\mathbf{v}_1} - \mathbf{X}^{\mathbf{v}_2}$ in $I_+(\mathcal{C})$ such that $\mathbf{X}^{\mathbf{v}_1}$ divides $\mathbf{X}^{\mathbf{u}_1}$ and $\mathbf{X}^{\mathbf{v}_2}$ divides $\mathbf{X}^{\mathbf{u}_2}$. We distinguish two cases:

- If $\mathbf{X}^{\mathbf{v}_1} \succ \mathbf{X}^{\mathbf{v}_2}$, then $\mathbf{X}^{\mathbf{u}_1}$ is not a minimal generator of the initial ideal $\mathrm{in}_\prec(I_+(\mathcal{C}))$.
- If $\mathbf{X}^{\mathbf{v}_1} \prec \mathbf{X}^{\mathbf{v}_2}$, then $\mathbf{X}^{\mathbf{u}_2}$ is not in canonical form.

Both cases contradicts our assumption. □

We call the set of all primitive binomials of $I_+(\mathcal{C})$ the *Graver basis* of $I_+(\mathcal{C})$ and denote it by $\mathrm{Gr}_\mathcal{C}$.

Corollary 2. $\mathcal{U}_\mathcal{C} \subseteq \mathrm{Gr}_\mathcal{C}$.

Proof. The result is a direct consequence of Lemma 5.1. □

The following theorem suggests an algorithm for computing the Graver basis of the ideal $I_+(\mathcal{C})$. For this purpose we describe the Lawrence lifting of the ideal $I_+(\mathcal{C})$.

Definition 5.2. We define the *Lawrence lifting* of the ideal $I_+(\mathcal{C})$ as the ideal

$$I_{\Lambda(\mathcal{C})} = \left\langle \left\{ \mathbf{X}^{\Delta \mathbf{w}_1}\mathbf{Z}^{\Delta \mathbf{w}_2} - \mathbf{X}^{\Delta \mathbf{w}_2}\mathbf{Z}^{\Delta \mathbf{w}_1} \mid \mathbf{w}_1 - \mathbf{w}_2 \in \mathcal{C} \right\} \right\rangle$$

in the polynomial ring $\mathbb{K}[\mathbf{X},\mathbf{Z}]$ where $\mathbf{X}$ and $\mathbf{Z}$ denote $n(q-1)$ variables each.

Theorem 5.3. *The Graver basis of $I_{\Lambda(\mathcal{C})}$ coincides with any reduced Gröbner basis of $I_{\Lambda(\mathcal{C})}$.*

Proof. The proof starts with the observation that a binomial $\mathbf{X}^{\Delta \mathbf{u}_1} - \mathbf{X}^{\Delta \mathbf{u}_2}$ is primitive in the ideal $I_+(\mathcal{C})$ if and only if the corresponding binomial $\mathbf{X}^{\Delta \mathbf{u}_1}\mathbf{Z}^{\Delta \mathbf{u}_2} - \mathbf{X}^{\Delta \mathbf{u}_2}\mathbf{Z}^{\Delta \mathbf{u}_1}$ in the lifting ideal $I_{\Lambda(\mathcal{C})}$ is primitive. Therefore, between the Graver basis of the ideals $I_+(\mathcal{C})$ and $I_{\Lambda(\mathcal{C})}$ there exists the following relation:

$$\mathrm{Gr}_{\Lambda(\mathcal{C})} = \left\{ \mathbf{X}^{\Delta \mathbf{u}_1}\mathbf{Z}^{\Delta \mathbf{u}_2} - \mathbf{X}^{\Delta \mathbf{u}_2}\mathbf{Z}^{\Delta \mathbf{u}_1} \mid \mathbf{X}^{\Delta \mathbf{u}_1} - \mathbf{X}^{\Delta \mathbf{u}_2} \in \mathrm{Gr}_{\mathcal{C}} \right\}.$$

Now, take any element $g = \mathbf{X}^{\Delta \mathbf{u}_1}\mathbf{Z}^{\Delta \mathbf{u}_2} - \mathbf{X}^{\Delta \mathbf{u}_2}\mathbf{Z}^{\Delta \mathbf{u}_1}$ in $\mathrm{Gr}_{\Lambda(\mathcal{C})}$. Let B be the set of all binomials in $I_{\Lambda(\mathcal{C})}$ except g and assume that B generates the ideal $I_{\Lambda(\mathcal{C})}$. Therefore g can be written as a linear combination of the elements of B. In other words, there exists a binomial $\mathbf{X}^{\Delta \mathbf{v}_1}\mathbf{Z}^{\Delta \mathbf{v}_2} - \mathbf{X}^{\Delta \mathbf{v}_2}\mathbf{Z}^{\Delta \mathbf{v}_1}$ in B such that one of its terms divides the leading term of g. Replacing $\mathbf{v} = (\mathbf{v}_1, \mathbf{v}_2)$ by $-\mathbf{v} = (-\mathbf{v}_1, -\mathbf{v}_2)$ in $\mathbb{F}_q^n$ if necessary, we may assume that $\mathbf{X}^{\Delta \mathbf{v}_1}\mathbf{Z}^{\Delta \mathbf{v}_2}$ divides $\mathbf{X}^{\Delta \mathbf{u}_1}\mathbf{Z}^{\Delta \mathbf{u}_2}$, contrary to the fact that $\mathbf{X}^{\Delta \mathbf{u}_1} - \mathbf{X}^{\Delta \mathbf{u}_2}$ is primitive in $I_+(\mathcal{C})$. So some non-zero scalar multiple of g must appear in any reduced Gröbner basis of $I_{\Lambda(\mathcal{C})}$ which is also a minimal generating set of $I_{\Lambda(\mathcal{C})}$. □

This theorem gives us an algorithm to compute a Graver basis of the ideal $I_+(\mathcal{C})$, exposed as Algorithm 4. Note that Step 3 of Algorithm 4 can be executed by applying Algorithm 2. Later in Theorem 5.4 we will give a set of generators of the lawrence lifting ideal $I_{\Lambda(\mathcal{C})}$ which will facilitate the implementation of this algorithm.

Algorithm 4: Algorithm for computing the Graver basis of $I_+(\mathcal{C})$

Data: An $[n,k]$ linear code $\mathcal{C}$ defined over $\mathbb{F}_q$.
Result: The Graver basis of the ideal $I_+(\mathcal{C})$, $\mathrm{Gr}_{\mathcal{C}}$.
1 Choose any term order $\prec$ on $\mathbb{K}[\mathbf{X}, \mathbf{Z}]$;
2 Compute the Lawrence lifting ideal $I_{\Lambda(\mathcal{C})}$;
3 Compute a reduced Gröbner basis of $I_{\Lambda(\mathcal{C})}$ w.r.t. $\prec$;
4 Substitute the variable $\mathbf{Z}$ by $\mathbf{1}$;

Here is another way of defining the ideal $I_{\Lambda(\mathcal{C})}$.

Theorem 5.4. *Let $\mathcal{C}$ be an $[n,k]$ linear code defined over $\mathbb{F}_q$ and $\{\mathbf{w}_1, \ldots, \mathbf{w}_k\}$ be the rows of a generator matrix of $\mathcal{C}$. We define the ideal:*

$$I_3 = \left\langle \left\{ \mathbf{X}^{\Delta \alpha^j \mathbf{w}_i} - \mathbf{Z}^{\Delta \alpha^j \mathbf{w}_i} \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \ \{\mathcal{R}_{X_i}, \ \mathcal{R}_{Z_i}\}_{i=1,\ldots,n} \right\rangle.$$

Then $I_{\Lambda(\mathcal{C})} = I_3$.

Proof. The following result may be proved in the same way as Theorem 2.3. It is easily seen that all the binomials of the generating set of I_3 belongs to $I_{\Lambda(\mathcal{C})}$. Indeed, the exponents of all the binomials of the sets $\mathcal{R}_{X_i}$ and $\mathcal{R}_{Z_i}$ correspond to the codeword $\mathbf{0} \in \mathcal{C}$.

Conversely, we need to show that each binomial $\mathbf{X}^{\Delta \mathbf{a}}\mathbf{Z}^{\Delta \mathbf{b}} - \mathbf{X}^{\Delta \mathbf{b}}\mathbf{Z}^{\Delta \mathbf{a}}$ in $I_{\Lambda(\mathcal{C})}$ belongs to I_3. Applying the definition of the ideal $I_{\Lambda(\mathcal{C})}$ we can rewrite $\mathbf{a} - \mathbf{b} \in \mathcal{C}$ as

$$\mathbf{a} - \mathbf{b} = \lambda_1 \mathbf{w}_1 + \cdots + \lambda_k \mathbf{w}_k \text{ with } \lambda_1, \ldots, \lambda_k \in \mathbb{F}_q.$$

We have that

$$\begin{aligned}
\mathbf{X}^{\Delta(\mathbf{a}-\mathbf{b})}\mathbf{Z}^{\Delta(\mathbf{b}-\mathbf{a})}-1 &= \left(\mathbf{X}^{\Delta\lambda_1\mathbf{w}_1}\mathbf{Z}^{\Delta-\lambda_1\mathbf{w}_1}-1\right)\prod_{i=2}^{k}\mathbf{X}^{\Delta\lambda_i\mathbf{w}_i}\mathbf{Z}^{\Delta-\lambda_i\mathbf{w}_i}\\
&+ \left(\prod_{i=2}^{k}\mathbf{X}^{\Delta\lambda_i\mathbf{w}_i}\mathbf{Z}^{\Delta-\lambda_i\mathbf{w}_i}-1\right) \mod \{\mathcal{R}_{\mathbf{X}},\mathcal{R}_{\mathbf{Z}}\}\\
&= \left(\mathbf{X}^{\Delta\lambda_1\mathbf{w}_1}\mathbf{Z}^{\Delta-\lambda_1\mathbf{w}_1}-1\right)\prod_{i=2}^{k}\mathbf{X}^{\Delta\lambda_i\mathbf{w}_i}\mathbf{Z}^{\Delta-\lambda_i\mathbf{w}_i}+\\
&+ \left(\mathbf{X}^{\Delta\lambda_2\mathbf{w}_2}\mathbf{Z}^{\Delta-\lambda_2\mathbf{w}_2}-1\right)\prod_{i=3}^{k}\mathbf{X}^{\Delta\lambda_i\mathbf{w}_i}\mathbf{Z}^{\Delta-\lambda_i\mathbf{w}_i}+\cdots+\\
&+ \left(\mathbf{X}^{\Delta\lambda_{k-1}\mathbf{w}_{k-1}}\mathbf{Z}^{\Delta-\lambda_{k-1}\mathbf{w}_{k-1}}-1\right)\mathbf{X}^{\Delta\lambda_k\mathbf{w}_k}\mathbf{Z}^{\Delta-\lambda_k\mathbf{w}_k}\\
&+ \left(\mathbf{X}^{\Delta\lambda_k\mathbf{w}_k}\mathbf{Z}^{\Delta-\lambda_k\mathbf{w}_k}-1\right) \mod \{\mathcal{R}_{\mathbf{X}},\mathcal{R}_{\mathbf{Z}}\}.
\end{aligned}$$

The last equation forces that

$$\mathbf{X}^{\Delta(\mathbf{a}-\mathbf{b})}\mathbf{Z}^{\Delta(\mathbf{b}-\mathbf{a})}-1 \in \left\langle \left\{\mathbf{X}^{\Delta\alpha^j\mathbf{w}_i}\mathbf{Z}^{\Delta-\alpha^j\mathbf{w}_i}-1\right\}_{\substack{i=1,\ldots,k\\ j=1,\ldots,q-1}} \cup \{\mathcal{R}_{\mathbf{X}},\mathcal{R}_{\mathbf{Z}}\}\right\rangle.$$

Note that we have actually proved that

$$\mathbf{X}^{\Delta\mathbf{a}}\mathbf{Z}^{\Delta\mathbf{b}}-\mathbf{X}^{\Delta\mathbf{b}}\mathbf{Z}^{\Delta\mathbf{a}} \mod \langle\mathcal{R}_{\mathbf{X}},\mathcal{R}_{\mathbf{Z}}\rangle = \left(\mathbf{X}^{\Delta(\mathbf{a}-\mathbf{b})}\mathbf{Z}^{\Delta(\mathbf{b}-\mathbf{a})}-1\right)\in I_3,$$

which completes the proof. □

The following result suggests an algorithm to compute the set $\mathcal{M}_{\mathcal{C}}$. Note that given the set $\mathcal{M}_{\mathcal{C}}$ we could deduce the minimum distance of $\mathcal{C}$.

Theorem 5.5. *The set of codewords of minimal support of the code $\mathcal{C}$ is a subset of the vectors related to the Graver basis of the ideal associated to $\mathcal{C}$.*

Proof. Let $\mathbf{m}\in\mathcal{M}_{\mathcal{C}}$. Suppose the theorem is false, then no binomial of type $\mathbf{X}^{\Delta\mathbf{a}}-\mathbf{X}^{\Delta\mathbf{b}}\in I_+(\mathcal{C})$ with $\mathbf{a}-\mathbf{b}=\mathbf{m}$ would be primitive.

We can always choose a binomial representation $\mathbf{X}^{\Delta\mathbf{a}}-\mathbf{X}^{\Delta\mathbf{b}}$ (among all the possible) such that the following condition hold, labelled as **necessary condition**:

- If $x_{i,r}\in\operatorname{supp}\left(\mathbf{X}^{\Delta\mathbf{a}}\right)$ and $x_{i,s}\in\operatorname{supp}\left(\mathbf{X}^{\Delta\mathbf{b}}\right)$, then $x_{i,r}x_{i,s}-1\notin\mathcal{R}_{X_i}$. Otherwise we take $x_{i,s}\left(\mathbf{X}^{\Delta\mathbf{a}}-\mathbf{X}^{\Delta\mathbf{b}}\right)\in I_+(\mathcal{C})$, with $i=1,\ldots,n$, instead.

Let $\mathbf{X}^{\Delta\mathbf{v}_1}-\mathbf{X}^{\Delta\mathbf{v}_2}$ be a primitive binomial of $I_+(\mathcal{C})$ such that $\mathbf{X}^{\Delta\mathbf{v}_1}$ divides $\mathbf{X}^{\Delta\mathbf{a}}$ and $\mathbf{X}^{\Delta\mathbf{v}_2}$ divides $\mathbf{X}^{\Delta\mathbf{b}}$, or equivalently,

$$\operatorname{supp}(\Delta\mathbf{v}_1)\subset\operatorname{supp}(\Delta\mathbf{a}) \quad \text{and} \quad \operatorname{supp}(\Delta\mathbf{v}_2)\subset\operatorname{supp}(\Delta\mathbf{b})$$

The **necessary conditions** defined above guarantee that if there exists a nonzero coordinate $i\in\operatorname{supp}(\mathbf{a})\cap\operatorname{supp}(\mathbf{b})$ then $i\in\operatorname{supp}(\mathbf{a}-\mathbf{b})$. Therefore, we found $\mathbf{v}_1-\mathbf{v}_2\in\mathcal{C}\setminus\{\mathbf{m}\}$ such that $\operatorname{supp}(\mathbf{v}_1-\mathbf{v}_2)\subset\operatorname{supp}(\mathbf{m})$, which contradicts the minimality of $\mathbf{m}$.

□

Remark 16. We could get rid of the leftover codewords from the set obtained by the above theorem using Algorithm 3.

Corollary 3. *The set of codewords of minimal support of any linear code $\mathcal{C}$ can be computed from the ideal*

$$I_3 = \left\langle \left\{ \mathbf{X}^{\Delta\alpha^j \mathbf{w}_i} - \mathbf{Z}^{\Delta\alpha^j \mathbf{w}_i} \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q-1}} \bigcup \ \{\mathcal{R}_{X_i},\ \mathcal{R}_{Z_i}\}_{i=1,\ldots,n} \right\rangle.$$

Proof. This result follows directly from Theorems 5.4 and 5.5. □

Algorithm 5 describes step by step how to compute the set of codewords of minimal support of a linear code. Note that Step 2 of Algorithm 5 can be executed by applying Algorithm 2. Moreover, Algorithm 5 performs an incremental technique thus we can stop before the end, obtaining a partial result as for example a minimal codeword (with weight the minimum distance of the code).

Algorithm 5: Algorithm for computing $\mathcal{M}_\mathcal{C}$

Data: An $[n, k]$ linear code $\mathcal{C}$ defined over $\mathbb{F}_q$.
Result: The set of codewords of minimal support of $\mathcal{C}$, $\mathcal{M}_\mathcal{C}$

1 Choose any term order $\prec$ on $\mathbb{K}[\mathbf{X}, \mathbf{Z}]$;
2 Compute a reduced Gröbner basis of I_3 (defined in Theorem 5.4) w.r.t. $\prec$;
// Recall that $I_3 = I_{\Lambda(\mathcal{C})}$, i.e. the Lawrence lifting ideal of $I_+(\mathcal{C})$. In other words, if we compute a reduced Gröbner basis of I_3 we are obtain the Graver basis of $I_+(\mathcal{C})$
3 Substitute the variable $\mathbf{Z}$ by $\mathbf{1}$;
4 Get rid of the leftover codewords using Algorithm 3.

In the following example we will see how to use Algorithm 5 to obtain the set of codewords of minimal support of a linear code.

Example 5. *Consider $\mathcal{C}$ the $[6, 3]$ ternary code with generator matrix*

$$G_\mathcal{C} = \begin{pmatrix} 1 & 0 & 0 & 2 & 2 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 2 & 1 \end{pmatrix} \in \mathbb{F}_3^{3\times 6}.$$

This code has $3^3 = 27$ codewords.

- *The zero codeword.*
- *16 codewords of minimal support. It is easy to check that if a codeword $\mathbf{c}$ is a minimal support codeword, then all its multiples are also codewords of minimal support. So these 16 codewords represent 8 different supports.*

1.	$(1,0,0,2,2,0)$	$(2,0,0,1,1,0)$	5.	$(1,0,1,0,1,1)$	$(2,0,2,0,2,2)$
2.	$(0,1,0,1,1,0)$	$(0,2,0,2,2,0)$	6.	$(2,0,1,2,0,1)$	$(1,0,2,1,0,2)$
3.	$(1,1,0,0,0,0)$	$(2,2,0,0,0,0)$	7.	$(0,1,1,2,0,1)$	$(0,2,2,1,0,2)$
4.	$(0,0,1,1,2,1)$	$(0,0,2,2,1,2)$	8.	$(0,2,1,0,1,1)$	$(0,1,2,0,2,2)$

- *Another 10 codewords which do not have minimal support.*

$(2,1,0,2,2,0)$	$(1,2,0,1,1,0)$	$(2,1,1,0,1,1)$	$(1,2,2,0,2,2)$
$(1,2,1,2,0,1)$	$(2,1,2,1,0,2)$		
$(2,2,1,1,2,1)$	$(1,1,2,2,1,2)$	$(1,1,1,1,2,1)$	$(2,2,2,2,1,2)$

Let $\alpha = 2$ be a primitive element of $\mathbb{F}_3$ and let us label the rows of G by $\mathbf{w}_1$, $\mathbf{w}_2$ and $\mathbf{w}_3$. By Theorem 2.3, the ideal associated to $\mathcal{C}$ may be defined as the following ideal:

$$\left\langle \left\{ \mathbf{X}^{\Delta(\alpha^j \mathbf{w}_i)} - 1 \right\}_{\substack{i=1,\ldots,3 \\ j=1,2}} \bigcup \; \{\mathcal{R}_{X_i}\}_{i=1,\ldots,6} \right\rangle,$$

where $\mathcal{R}_{X_i}$ consists of the following binomials

$$\mathcal{R}_{X_i} = \left\{ \; x_{i,1}^2 - x_{i,2}, \quad x_{i,1}x_{i,2} - 1, \quad x_{i,2}^2 - x_{i,1} \; \right\} \quad \text{with } i = 1, \ldots, 6.$$

If we compute a Gröbner basis of $I_+(\mathcal{C})$ w.r.t. a `degrev` *ordering we get 41 binomials representing the following set of 10 codewords:*

$$\begin{array}{llll} (0,2,2,1,0,2) & (0,1,1,2,0,1) & (0,1,2,0,2,2) & (0,2,1,0,1,1) \\ (0,2,0,2,2,0) & (0,1,0,1,1,0) & (0,0,2,2,1,2) & (0,0,1,1,2,1) \\ (2,2,0,0,0,0) & (1,1,0,0,0,0) & & \end{array}$$

From those 10 codewords we can remove vectors which are scalar multiples of another in the set, obtaining the following minimal test-set*:*

$$(1,1,0,0,0,0), (0,0,1,1,2,1), (0,1,0,1,1,0), (0,1,2,0,2,2), (0,1,1,2,0,1)$$

Again if we compare with Complete Syndrome Decoding (CSD) the cost storage of GDDA is much smaller. Indeed, for CSD we need to store $\frac{3^{n-k}-1}{2} = 13$ coset leaders.

Note that all nonzero codewords are codewords of minimal support but not all codewords of minimal support are represented in the above set.

Traditionally, if we compute a Graver basis of $I_+(\mathcal{C})$ we obtain 4212 binomials (following the techniques of [20]). However, Algorithm 5 returns directly the following set of codewords:

$$\begin{array}{llll} (2,1,2,1,0,2) & (1,2,1,2,0,1) & (1,2,2,0,2,2) & (2,1,1,0,1,1) \\ (1,0,2,1,0,2) & (2,0,1,2,0,1) & (2,0,2,0,2,2) & (1,0,1,0,1,1) \\ (0,2,2,1,0,2) & (0,1,1,2,0,1) & (0,1,2,0,2,2) & (0,2,1,0,1,1) \\ (0,0,2,2,1,2) & (0,0,1,1,2,1) & (2,1,0,2,2,0) & (1,2,0,1,1,0) \\ (2,0,0,1,1,0) & (1,0,0,2,2,0) & (0,1,0,1,1,0) & (0,2,0,2,2,0) \\ (1,1,0,0,0,0) & (2,2,0,0,0,0) & (0,0,0,0,0,0) & \end{array}$$

Observe that the set $\mathcal{M}_{\mathcal{C}}$ is contained in the previous set.

Conjecture 2. *Example 5 is just a toy example, but the difference between exhaustive search in the whole set of codewords and the set of codewords resulting from Algorithm 5 will be higher if $\mathcal{C}$ is chosen among a class of codes with a strong algebraic structure as for example: cyclic codes, Generalized Reed-Solomon codes ...*

6. **Applications to other types of codes.** We will show that the results presented on this article could be generalized to other classes of codes such as modular codes, codes defined over multiple alphabets or additive codes. Modular codes were already discussed in [16] but this new approach allows the computation of a test-set for decoding.

Other metrics could be more useful when dealing with group codes or codes over rings such as the Lee norm and G norm (see [1]) since they give us (via the Gray map isometry) nice descriptions of non-linear binary codes.

6.1. **Modular codes.** In [16] the authors were devoted to the study of modular codes $\mathcal{C}$ defined over the ring $\mathbb{Z}_s$. In other words, submodules of $(\mathbb{Z}_s^n, +)$. The important point in that article was the fact that a Graver basis of the lattice ideal associated with a modular code provides the set of codewords of minimal support of the code. Recall that the reduced Gröbner basis of the lattice ideal (defined as in [16]) does not allow decoding, see Example 5.

However, we can adapt the ideas presented above for linear codes to modular codes. We will use the following characteristic crossing functions.

$$\Delta_s: \quad \mathbb{Z}_s \longrightarrow E_s \cup \{\mathbf{0}\} \subseteq \mathbb{Z}^{s-1} \qquad \text{and} \qquad \nabla_s: \quad E_s \cup \{\mathbf{0}\} \longrightarrow \mathbb{Z}_s$$

These applications aim at describing a one-to-one correspondence between the ring $\mathbb{Z}_s$ and the standard basis of $\mathbb{Z}^{s-1}$, denoted as $E_s = \{\mathbf{e}_1, \ldots, \mathbf{e}_{s-1}\}$ where $\mathbf{e}_i$ denotes the unit vector with a 1 in the i-th coordinate and 0's elsewhere.

1. The map Δ_s replaces the element $i \in \mathbb{Z}_s$ by the vector $\mathbf{e}_i$ and $0 \in \mathbb{Z}_s$ by the zero vector $\mathbf{0} \in \mathbb{Z}^{s-1}$.
2. The map ∇ recovers the element $j \in \mathbb{Z}_s$ from the unit vector $\mathbf{e}_j$ and the zero element $0 \in \mathbb{Z}_s$ from the zero vector $\mathbf{0} \in \mathbb{Z}^{s-1}$.

Now let $\mathbf{X}$ denote n vector variables $X_1, \ldots, X_n$ such that each variable X_i can be decomposed into $s-1$ components $x_{i,1}, \ldots, x_{i,s-1}$ with $i = 1, \ldots, n$, representing the nonzero elements of $\mathbb{Z}_s$.

Remark 17. Note that the degree of a monomial of type $\mathbf{X}^{\Delta_s \mathbf{a}}$ with $\mathbf{a} \in \mathbb{Z}_s^n$ is defined as the weight of the vector $\mathbf{a}$.

Given the rows of a generator matrix of the modular code $\mathcal{C}$, labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k$ in $\mathbb{Z}_s^n$, we define the ideal associated to $\mathcal{C}$ as the binomial ideal

$$I_+(\mathcal{C}) = \left\langle \ \left\{\mathbf{X}^{\Delta_s \mathbf{w}_i} - 1\right\}_{i=1,\ldots,k} \ \bigcup \ \left\{\mathcal{R}_{X_i}\right\}_{i=1,\ldots,n} \ \right\rangle,$$

where $\mathcal{R}_{X_i}$ consists of all the binomials on the variable X_i associated to the relations given by the additive table of the ring $\mathbb{Z}_s$, i.e.

$$\mathcal{R}_{X_i} = \left\{ \begin{array}{c} \{x_{i,u}x_{i,v} - x_{i,w} \mid u + v \equiv w \mod s\} \\ \{x_{i,u}x_{i,v} - 1 \mid u + v \equiv 0 \mod s\} \end{array} \right\} \text{ with } i = 1, \ldots, n.$$

Remark 18. Note that the main difference of the set of generators describing the ideal associated with a modular code, respect to the set of generators of the ideal related with a $\mathbb{F}_q$-linear code, is its cardinality. That is, for linear codes we need to add all the multiples in $\mathbb{F}_q$ of each row $\mathbf{w}_i$, while for modular codes this is not necessary. Moreover, the previous result can be extended for codes over $\mathbb{F}_p$ with p prime since $\mathbb{F}_p \cong \mathbb{Z}_p$.

Taking into account the new definition of the ideal associated to a modular code we can apply all the results of this article to these types of codes. Therefore, now we are not only able to compute the set of codewords of minimal support of modular codes but also we provide a complete decoding algorithm for these codes.

6.2. **Multiple Alphabets.** Let $\mathcal{C}$ be a submodule of dimension k over the multiple alphabets $\mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_n}$. For simplicity of notation we write $\left\{\mathbf{e}_1^s, \ldots, \mathbf{e}_{s-1}^s\right\}$ for the canonical basis of $\mathbb{Z}^{s-1}$.

Let $\mathbf{X}$ stand for n vector variables $X_1, \ldots, X_n$ such that each variable X_i can be decomposed into $s_i - 1$ components $x_{i,1}, \ldots, x_{i,s_i-1}$ with $i = 1, \ldots, n$ representing the non zero element of $\mathbb{Z}_{s_i}$. Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_n}$. We will adopt the following notation:

$$\mathbf{X}^{\Delta \mathbf{a}} = X_1^{\Delta_{s_1} a_1} \cdots X_n^{\Delta_{s_n} a_n} = (x_{1,1} \cdots x_{1,s_1-1})^{\Delta_{s_1} a_1} \cdots (x_{n,1} \cdots x_{n,s_n-1})^{\Delta_{s_n} a_n}.$$

Similar to the modular case, given the rows of a generator matrix of $\mathcal{C}$, labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k$, we may define the ideal associated to $\mathcal{C}$ as the following binomial ideal:

$$I_+(\mathcal{C}) = \left\langle \ \left\{ \mathbf{X}^{\Delta \mathbf{w}_i} - 1 \right\}_{i=1,\ldots,k} \ \bigcup \ \left\{ \mathcal{R}_{X_i} \right\}_{i=1,\ldots,n} \ \right\rangle.$$

Remark 19. The main difference with the modular case is that the relations $\mathcal{R}_{X_i}$ could be different for each $i \in \{1, \ldots, n\}$.

With this new definition, all the results of this article are valid for these types of codes.

6.3. **Additive codes.** Let $\mathbb{F}_{q_1}$ be an algebraic extension of $\mathbb{F}_{q_2}$, i.e. $q_1 = p^{r_1}$ and $q_2 = p^{r_2}$ where p is a prime number and r_2 divides r_1. An $\mathbb{F}_{q_2}$-additive code $\mathcal{C}$ of parameters $[n, k]$ over $\mathbb{F}_{q_1}$ is an $\mathbb{F}_{q_2}$-linear subspace of $\mathbb{F}_{q_1}^n$.

In other words, given the rows of a generator matrix of $\mathcal{C}$ labelled by $\mathbf{w}_1, \ldots, \mathbf{w}_k \in \mathbb{F}_{q_1}^n$, the set of codewords of $\mathcal{C}$ may be defined as:

$$\left\{ \alpha_1 \mathbf{w}_1 + \cdots + \alpha_k \mathbf{w}_k \mid \alpha_i \in \mathbb{F}_{q_2} \text{ for } i = 1, \ldots, k \right\}.$$

Let α be a primitive element of $\mathbb{F}_{q_2}$. We check at once that the binomial ideal associated to $\mathcal{C}$ is defined by the following binomial ideal

$$I_+(\mathcal{C}) = \left\langle \ \left\{ \mathbf{X}^{\Delta \alpha^j \mathbf{w}_i} - 1 \right\}_{\substack{i=1,\ldots,k \\ j=1,\ldots,q_2-1}} \ \bigcup \ \left\{ \mathcal{R}_{X_i} \right\}_{i=1,\ldots,n} \ \right\rangle,$$

where $\mathcal{R}_{X_i}$ consist of all the binomials on the variable X_i associated to the relations given by the additive table of the field $\mathbb{F}_{q_1}$. Of course, the results obtained for $\mathbb{F}_q$-linear codes could be adapted to additive codes.

Conclusions. Complete decoding for an arbitrary linear code is proved to be NP-hard. That is, from a computational point of view, our description could not provide a polynomial time algorithm. However, we present a new complete decoding algorithm using the concept of Gröbner basis. This proposal was already presented for the binary case before but the generalization to the non-binary case was not possible with the previous approach.

It is outside the scope of this article but we are hopeful to achieve efficient methods using this approach for special types of codes like cyclic codes or some subclasses of cyclic codes such as Reed-Solomon codes and BCH codes since these codes have a rich algebraic structure and we can take advantage of existing efficient method to solve polynomial systems whose equations are left invariant by the action of a finite group.

We would like to notice that during the (Google Summer of code of 2013) the student Verónica Suaste (CIMAT, México) implemented Algorithm 2 and also a decoding algorithm using a minimal test-set for inclusion in Sage. The code is published at http://trac.sagemath.org/ticket/14973 and it will be included in next releases of Sage. Note that in the project conclusions, there are some examples in which the new decoding algorithm is faster than the classical syndrome decoding of Sage.

REFERENCES

[1] M. Aliasgari, M.R. Sadeghi, and D. Panario. Gröbner Bases for Lattices and an Algebraic Decoding Algorithm. *IEEE Transaction on Communications*, 61(4):1222–1230, 2013.

[2] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Trans. Inform. Theory*, 44(5):2010–2017, 1998.

[3] A. Barg. Complexity issues in coding theory. In *Handbook of coding theory, Vol. I, II*, pages 649–754. North-Holland, Amsterdam, 1998.

[4] E. R. Berlekamp, R. J. McEliece, and Henk C. A. Van Tilborg. On the inherent intractability of certain coding problems. *IEEE Trans. Inform. Theory*, IT-24(3):384–386, 1978.

[5] M. Borges-Quintana, M. A. Borges-Trenard, P. Fitzpatrick, and E. Martínez-Moro. Gröbner bases and combinatorics for binary codes. *Appl. Algebra Engrg. Comm. Comput.*, 19(5):393–411, 2008.

[6] M. Borges-Quintana, M.A. Borges-Trenard, I. Márquez-Corbella, and E. Martínez-Moro. An algebraic view to gradient descent decoding. In *IEEE Information Theory Workshop (ITW)*, pages 1 –4, 30 2010-sept. 3 2010.

[7] J. Bruck and M. Naor. The hardness of decoding linear codes with preprocessing. *IEEE Trans. Inform. Theory*, 36(2):381–385, 1990.

[8] D.A. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Number v. 10 in Undergraduate Texts in Mathematics. Springer, 2007.

[9] F. Di Biase and R. Urbanke. An Algorithm to Calculate the Kernel of Certain Polynomial Ring Homomorphisms. *Experimental Mathematics*, 4(3):227–234, 1995.

[10] D. Eisenbud and B. Sturmfels. Binomial ideals. *Duke Mathematical Journal*, 84(1):1–45, 1996.

[11] J. C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symbolic Comput.*, 16(4):329–344, 1993.

[12] P. Fitzpatrick. Solving a multivariable congruence by change of term order. *J. Symbolic Comput.*, 24(5):575–589, 1997.

[13] P. Fitzpatrick and J. Flynn. A Gröbner basis technique for Padé approximation. *J. Symbolic Comput.*, 13(2):133–138, 1992.

[14] D. Ikegami and Y. Kaji. Maximum Likelihood Decoding for Linear Block Codes using Grobner Bases. *IEICE Trans. Fund. Electron. Commun. Comput. Sci.*, E86-A(3):643–651, 2003.

[15] R. A. Liebler. Implementing gradient descent decoding. *Michigan Math. J.*, 58(1):285–291, 2009.

[16] I. Márquez-Corbella and E. Martínez-Moro. Algebraic structure of the minimal support codewords set of some linear codes. *Adv. Math. Commun.*, 5(2):233–244, 2011.

[17] I. Márquez-Corbella and E. Martínez-Moro. Decomposition of Modular Codes for Computing Test Sets and Graver Basis. *Mathematics in Computer Science*, 6:147–165, 2012.

[18] E. Prange. Step-by-step decoding in groups with weight function. part 1. Air Force Cambridge Research Labs Hanscom AFB MA, 1961.

[19] P. Samuel. *Algebraic Theory of Numbers: Translated from the French by Allan J. Silberger*. Dover Books on Mathematics. Dover Publications, 2013.

[20] B. Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.

Received xxxx 20xx; revised xxxx 20xx.

E-mail address: irene.marquez-corbella@inria.fr
E-mail address: edgar@maf.uva.es
E-mail address: emilio.suarez@deic.uab.cat