Applications of results from commutative algebra to the study of certain evaluation codes

Cícero Carvalho

1. Introduction

This is the text of a short course given at the meeting CIMPA School on Algebraic Methods in Coding Theory, organized by CIMPA and USP - State University of Sao Paulo. Our aim with this course is to present tools and results from Gröbner basis theory which are suited to be used in some areas of coding theory, and then to use them to study the so-called affine cartesian codes.

The literature on the basics of Gröbner bases theory is numerous (we can cite [**1**], [**3**], [**16**] and [**9**], to name a few) so we decided not to present proofs of some of the more technical results in this theory. Thus, in section 2 we quickly introduce the basic facts of Gröbner bases theory, and we also present the definition and the properties of the so-called footprint of an ideal (also known as Gröbner escalier, see Definition 2.11). Section 3 starts with the definition of affine varieties, linear codes and affine variety codes, as introduced by Fitzgerald and Lax in [**11**]. We then introduce affine cartesian codes, a Reed-Muller type of code studied by López, Rentería-Márquez and Villareal in [**14**] (see Definition 3.9). These codes also appeared, independently, and in a generalized form, in a work by O. Geil and C. Thomsen (see [**13**]). It's in the determination of the parameters of these codes that we will show how to combine results from Gröbner basis theory and commutative algebra to obtain results in coding theory. In [**14**] the authors have already determined the parameters of affine cartesian codes, but our methods differ substantially from theirs. Here we make extensive use of the properties of

1991 *Mathematics Subject Classification.* Primary 14G50; Secondary 11T71, 13P25, 13D40, 94B27,94B60.

Key words and phrases. Evaluation codes, affine variety codes, affine cartesian codes, Gröbner basis, footprint of an ideal.

The author acknowledges and thanks the support from FAPEMIG, proc. CEX-APQ-01645-16.

the footprint which simplifies very much the calculation of those parameters. In the last section, we present some results about the second lowest Hamming weight of affine cartesian codes.

2. Prelminary results on Gröbner bases and the footprint of an ideal

As mentioned above, our methods involve the use of results from Gröbner basis theory, and in the present section we present a detailed account of these results.

Let k be a field and denote by $k[\boldsymbol{X}]$ the ring of polynomials $k[X_1, \ldots, X_n]$. A product like $aX_1^{\alpha_1}. \cdots .X_n^{\alpha_n}$, where $a \in k^*$ and $\alpha_1, \ldots, \alpha_n$ are nonnegative integers is called a *term*, while $X_1^{\alpha_1}. \cdots .X_n^{\alpha_n}$ is called a *monomial.* A monomial $X_1^{\alpha_1}. \cdots .X_n^{\alpha_n}$ will sometimes be denoted by $\boldsymbol{X}^{\boldsymbol{\alpha}}$ (or $\boldsymbol{X}^{\boldsymbol{\beta}}$, $\boldsymbol{X}^{\boldsymbol{\gamma}}$, etc) where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ and $\mathbb{N}_0$ is the set of nonnegative integers. We write $\mathcal{M}$ for the set of monomials of $k[\boldsymbol{X}]$. Given a polynomial $f \in k[\boldsymbol{X}]$ we say that a monomial M *appears in* f if the coefficient of M in f is nonzero.

Definition 2.1. A *monomial order* in $\mathcal{M}$ is a total order $\preceq$ defined on $\mathcal{M}$ such that:
i) if $\boldsymbol{X}^{\boldsymbol{\alpha}} \preceq \boldsymbol{X}^{\boldsymbol{\beta}}$ then $\boldsymbol{X}^{\boldsymbol{\alpha}+\boldsymbol{\gamma}} \preceq \boldsymbol{X}^{\boldsymbol{\beta}+\boldsymbol{\gamma}}$, for all $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma} \in \mathbb{N}_0^n$;
ii) any nonempty subset $\mathcal{A} \subset \mathcal{M}$ has a smallest element.

Examples 2.2.
i) The *lexicographic order* (with $X_n \preceq \cdots \preceq X_1$) is defined by setting $\boldsymbol{X}^{\boldsymbol{\alpha}} \preceq \boldsymbol{X}^{\boldsymbol{\beta}}$ if $\boldsymbol{\alpha} = \boldsymbol{\beta}$ or the first nonzero entry from the left to the right in $\boldsymbol{\beta} - \boldsymbol{\alpha}$ is positive. Thus we have $X_2^{1000} \preceq X_1$ and $X_1^2 X_3^{2012} \preceq X_1^2 X_2$.
ii) The *graded lexicographic order* (with $X_n \preceq \cdots \preceq X_1$) is defined by setting $\boldsymbol{X}^{\boldsymbol{\alpha}} \preceq \boldsymbol{X}^{\boldsymbol{\beta}}$ if $\boldsymbol{\alpha} = \boldsymbol{\beta}$ or $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ or if $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ then $\boldsymbol{X}^{\boldsymbol{\alpha}} \preceq_{\text{lex}} \boldsymbol{X}^{\boldsymbol{\beta}}$ where $\preceq_{\text{lex}}$ is the order defined in (i).
ii) The *graded reverse lexicographic order* is defined by setting $\boldsymbol{X}^{\boldsymbol{\alpha}} \preceq \boldsymbol{X}^{\boldsymbol{\beta}}$ if $\boldsymbol{\alpha} = \boldsymbol{\beta}$ or $\sum_{i=1}^n \alpha_i < \sum_{i=1}^n \beta_i$ or if $\sum_{i=1}^n \alpha_i = \sum_{i=1}^n \beta_i$ then the first nonzero entry from the right to the left in $\boldsymbol{\beta} - \boldsymbol{\alpha}$ is negative.

Definition 2.3. Let $f = \sum_{i=1}^m a_i M_m \in k[\boldsymbol{X}]$ be a nonzero polynomial, where $a_i \in k$, $a_i \neq 0$ and $M_i \in \mathcal{M}$ for all $i = 1, \ldots, m$, and let $\preceq$ be a monomial order defined on $\mathcal{M}$. Then the *leading monomial* of f (with respect to $\preceq$) is $M_\ell := \max\{M_i \mid i = 1, \ldots, m\}$, the *leading coefficient* of f (with respect to $\preceq$) is a_ℓ and the *leading term* of f (with respect to $\preceq$) is $a_\ell M_\ell$. We denote these elements by $M_\ell = \text{lm}(f)$, $a_\ell = \text{lc}(f)$ and $a_\ell M_\ell = \text{lt}(f)$.

Thus, for example, if $f(X_1, X_2, X_3) = 4X_1^3 X_2^4 + 5X_1 X_3^8 + 2 \in \mathbb{R}[X_1, X_2, X_3]$ and we endow the set of monomials with the lexicographic order then we get $\mathrm{lm}(f) = X_1^3X_2^4$ and $\mathrm{lt}(f) = 4X_1^3X_2^4$, while if we decide to use the graded lexicographic order we have $\mathrm{lm}(f) = X_1X_3^8$ and $\mathrm{lt}(f) = 5X_1X_3^8$.

An important procedure in Gröbner bases theory is the division of a polynomial by a list of nonzero polynomials.

Definition 2.4. To divide $f \in k[\boldsymbol{X}]$ by $\{g_1, \ldots, g_t\} \subset k[\boldsymbol{X}] \setminus \{0\}$, with respect to a monomial order $\preceq$, means to find quotients $q_1, \ldots, q_t$ and a remainder r in $k[\boldsymbol{X}]$ such that $f = q_1g_1 + \cdots + q_tg_t + r$, and either $r = 0$ or no monomial appearing in r is a multiple of $\mathrm{lm}(g_i)$, for all $i \in \{1, \ldots, t\}$.

In the literature on Gröbner bases cited at the introduction the reader will find a description of the usual algorithm used to determine the quotients and the remainder, as well as a proof that the algorithm in fact ends after a finite number of steps. Here we just describe the algorithm and show how it works in an example. The basic idea is the same that we are familiar with when dividing two polynomials of one variable: we will use the leading terms of $g_1, \ldots, g_t$ to "kill" the leading term of f and of subsequent polynomials that appear in intermediate steps of the division. The novelty here is that sometimes the leading term of an "intermediate polynomial" is not a multiple of any of $\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t)$ so we must move it to the remainder to go on with the division. We think the idea will become clear after the following example: we want to divide $f = X^2Y + XY^2 + Y^2 \in \mathbb{R}[X, Y]$ by $\{g_1 = XY - 1, g_2 = Y^2 - 1\} \subset \mathbb{R}[X, Y]$, and we endow the set of monomials of $\mathbb{R}[X, Y]$ with the lexicographic order (where $Y \preceq X$). We start by noting that $\mathrm{lm}(f) = X^2Y$ so it is a multiple of $\mathrm{lm}(g_1) = XY$, and from $\mathrm{lm}(f) = X.\mathrm{lm}(g_1)$ we start the division by writing $f = X.g_1 + X + XY^2 + Y^2$. Now we get that $\mathrm{lm}(X + XY^2 + Y^2) = X.Y^2$ so again it is a multiple of $\mathrm{lm}(g_1)$ and since $X.Y^2 = Y.\mathrm{lm}(g_1)$ we proceed with the division by writing $f = X.g_1 + Y.g_1 + X + Y + Y^2 = (X + Y).g_1 + X + Y + Y^2$. Observe now that $\mathrm{lm}(X + Y + Y^2) = X$ which is not a multiple of $\mathrm{lm}(g_1)$ or $\mathrm{lm}(g_2) = Y^2$, so we will consider X as part of the remainder. Thus $f = (X+Y).g_1+Y+Y^2+r_1$, where $r_1 = X$, and we proceed with the division by noting that $\mathrm{lm}(Y+Y^2) = Y^2$ is not a multiple of $\mathrm{lm}(g_1)$ but it is a multiple of $\mathrm{lm}(g_2)$, and from $Y^2 = 1.\mathrm{lm}(g_2)$ we get $f = (X+Y).g_1+1.g_2+Y+1+r_1$. Since the terms in $Y + 1$ are not a multiple either of $\mathrm{lm}(g_1)$ or of $\mathrm{lm}(g_2)$ we consider them as a part of the remainder. The figure below shows the calculation at its end.

$$
\begin{array}{r|ll|l}
 & X+Y, & 1 & \text{Remainder} \\
\cline{2-3}
X^2Y + XY^2 + Y^2 & XY-1, & Y^2-1 & X+Y+1 \\
-X^2Y + X & & & \\
\cline{1-1}
X + XY^2 + Y^2 & & & \\
-XY^2 + Y & & & \\
\cline{1-1}
X + Y + Y^2 & & & \\
-X & & & \\
\cline{1-1}
Y + Y^2 & & & \\
-Y^2 + 1 & & & \\
\cline{1-1}
Y + 1 & & & \\
-Y - 1 & & & \\
\cline{1-1}
0 & & &
\end{array}
$$

This finishes the division and we have $f = q_1g_1 + q_2g_2 + r$ with $q_1 = X + Y$, $q_2 = 1$ and $r = X + Y + 1$.

It is important to observe that from the division algorithm we get that if the remainder r is not zero then the leading monomial of r is less than or equal to the leading monomial of f.

Also, looking carefully at the algorithm we observe that we are taking into account the order in which the divisors $g_1, \ldots, g_t$ are written (in other words, we are actually dividing f by a sequence $(g_1, \ldots, g_t)$) and we may ask if a change in this order will produce a change in the quotients and the remainder. The answer to this question is yes, and one may check that applying the above procedure to divide $X^2Y + XY^2 + Y^2$ by $\{Y^2 - 1, XY - 1\}$ (taken in this order) we get $X^2Y + XY^2 + Y^2 = (X + 1)(Y^2 - 1) + X(XY - 1) + 2X + 1$.

We are now ready to introduce the concept of Gröbner basis. It first appeared in the thesis of the austrian mathematician Bruno Buchberger, published in 1965 (see [**4**]). His advisor, Wolfgang Gröbner, had proposed the following thesis problem: given an ideal $I \subset k[\boldsymbol{X}]$, find a basis for $k[\boldsymbol{X}]/I$ as a k-vector space. If $k[\boldsymbol{X}]$ is a ring of just one variable then the answer is well known: I is generated by a polynomial of a certain degree d (in the case where $I \neq 0$) and $\{1 + I, X + I, \ldots, X^{d-1} + I\}$ is a basis for $k[\boldsymbol{X}]/I$. In the case where $k[\boldsymbol{X}]$ is a ring of more than one variable the situation changes dramatically. From the Hilbert basis theorem, we know that I is generated by a finite number of polynomials, but I is not necessarily a principal ideal; furthermore the quotient ring $k[\boldsymbol{X}]/I$ may be an infinite dimensional k-vector space (e.g. take $I = (X) \subset k[X, Y]$). Buchberger's solution to this problem was to, having fixed a monomial order in $\mathcal{M}$, determine a special generating set for I whose main property is that the classes of the monomials which are not multiples of any of the leading monomials of the polynomials in this special basis form a basis for $k[\boldsymbol{X}]/I$ as a k-vector space. In 1976 (see

[**5**]) Buchberger decided to call this special basis for I a "Gröbner basis" as token of recognition of the influence of his advisor's ideas in his thesis work.

Definition 2.5. Let $I \subset k[\boldsymbol{X}]$ be a nonzero ideal and endow $\mathcal{M}$ with a monomial order $\preceq$. A set $\{g_1, \ldots, g_s\} \subset I$ is a *Gröbner basis* for I (with respect to $\preceq$) if for every $f \in I$, $f \neq 0$, we have that $\operatorname{lm}(f)$ is a multiple of $\operatorname{lm}(g_i)$ for some $i \in \{1, \ldots, s\}$.

Example 2.6. Let $I = (XY - 1, Y^2 - 1) \subset \mathbb{R}[X, Y]$ and consider the lexicographic order (with $Y \preceq X$) defined on the set of monomials of $\mathbb{R}[X, Y]$. Then $Y(XY - 1) - X(Y^2 - 1) = -Y + X \in I$ and $\operatorname{lm}(X - Y) = X$ is not a multiple of $\operatorname{lm}(XY - 1) = XY$ or $\operatorname{lm}(Y^2 - 1) = Y^2$, hence $\{XY - 1, Y^2 - 1\}$ is *not* a Gröbner basis for I.

We assume from now on that $\mathcal{M}$ is endowed with some fixed monomial order and that $I \neq (0)$. The following result shows that a Gröbner basis for I is indeed a basis for I, and that we may use it to decide if a given polynomial is in I.

Lemma 2.7. *Let $\{g_1, \ldots, g_s\} \subset I$ be a Gröbner basis for I, then $f \in I$ if and only if the remainder in the division of f by $\{g_1, \ldots, g_s\}$ is zero. As a consequence $I = (g_1, \ldots, g_s)$.*

Proof. The "if" part is trivial. On the other hand for $f \in I$ let $f = \sum_{i=1}^{s} q_i g_i + r$ be the division of f by $\{g_1, \ldots, g_s\}$. Then $r = f - \sum_{i=1}^{s} q_i g_i \in I$ hence we must have $r = 0$ otherwise r would be a nonzero polynomial in I whose leading monomial is not a multiple of $\operatorname{lm}(g_i)$ for any $i = 1, \ldots, s$, contradicting the fact that $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I. This shows that $I \subset (g_1, \ldots, g_s)$ and a fortiori $I = (g_1, \ldots, g_s)$. $\square$

An important property of a Gröbner basis is the following.

Proposition 2.8. *Let $\{g_1, \ldots, g_s\} \subset I$ be a Gröbner basis for I. In the division of $f \in k[\boldsymbol{X}]$ by $\{g_1, \ldots, g_s\}$ the remainder is always the same, regardless of the order that we choose for $g_1, \ldots, g_s$ in the division algorithm.*

Proof. Assume that $f = q_1 g_1 + \cdots + q_s g_s + r = \tilde{q}_1 g_1 + \cdots + \tilde{q}_s g_s + \tilde{r}$, where $q_i, \tilde{q}_i \in k[\boldsymbol{X}]$ for all $i = 1, \ldots, s$, $r, \tilde{r} \in k[\boldsymbol{X}]$ and no monomial appearing in r or $\tilde{r}$ is a multiple of $\operatorname{lm}(g_i)$ for all $i = 1, \ldots, s$. From $r - \tilde{r} = \sum_{i=1}^{s} (\tilde{q}_i - q_i) g_i \in I$ we must have $r - \tilde{r} = 0$ otherwise $r - \tilde{r}$ would be a nonzero polynomial in I whose leading monomial is not a multiple of $\operatorname{lm}(g_i)$ for any $i = 1, \ldots, s$, contradicting the fact that $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I. $\square$

The above results list some nice properties of Gröbner bases but so far it is not clear if every ideal $I \subset k[\boldsymbol{X}]$ admits such a basis. This is part of the main contribution of Buchberger in his thesis work. There he presents an algorithm that starting from any finite basis for I increases it, if necessary, in a sequence of steps until at some point the augmented basis is a Gröbner basis. We will present Buchberger's algorithm but we will not prove that indeed it produces a Gröbner basis after a finite number of steps, again we refer the reader to any of the books mentioned at the introduction.

The following is a key concept in Buchberger's algorithm.

Definition 2.9. Let $f, g \in k[\boldsymbol{X}] \setminus \{0\}$, with $\mathrm{lt}(f) = a\boldsymbol{X}^{\boldsymbol{\alpha}}$ and $\mathrm{lt}(g) = b\boldsymbol{X}^{\boldsymbol{\beta}}$. Let $\gamma_i = \max\{\alpha_i, \beta_i\}$, for $i = 1, \ldots, n$ and set $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_n) \in \mathbb{N}_0^n$. The *$S$-polynomial of f and g* is defined as $S(f, g) = (1/a)\boldsymbol{X}^{\boldsymbol{\gamma}-\boldsymbol{\alpha}} f - (1/b)\boldsymbol{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}} g$.

Observe that $\mathrm{lt}((1/a)\boldsymbol{X}^{\boldsymbol{\gamma}-\boldsymbol{\alpha}} f) = \boldsymbol{X}^{\boldsymbol{\gamma}} = \mathrm{lt}((1/b)\boldsymbol{X}^{\boldsymbol{\gamma}-\boldsymbol{\beta}} g)$. Buchberger proved that $\{g_1, \ldots, g_s\} \subset I$ is a Gröbner basis for I if and only if the remainder in the division of $S(g_i, g_j)$ by $\{g_1, \ldots, g_s\}$ is zero for all distinct $i, j \in \{1, \ldots, s\}$. He also proved that the following procedure may be used in an algorithm which produces a Gröbner basis for $I = (g_1, \ldots, g_s)$ in a finite number of steps: assume that for some pair of distinct integers $i, j \in \{1, \ldots, s\}$ the remainder $R_{i,j}$ in the division of $S(g_i, g_j)$ by $\{g_1, \ldots, g_s\}$ is not zero. Define $g_{s+1} = R_{i,j}$ and consider the set $\{g_1, \ldots, g_s, g_{s+1}\}$. Clearly $I = (g_1, \ldots, g_s, g_{s+1})$ because $g_{s+1} \in I$. If the remainder in the division of $S(g_i, g_j)$ by $\{g_1, \ldots, g_{s+1}\}$ is zero for all distinct $i, j \in \{1, \ldots, s+1\}$ then $\{g_1, \ldots, g_{s+1}\}$ is a Gröbner basis for I. If for some pair of distinct integers $i, j \in \{1, \ldots, s+1\}$ the remainder $R_{i,j}$ in the division of $S(g_i, g_j)$ by $\{g_1, \ldots, g_{s+1}\}$ is not zero then define $g_{s+2} = R_{i,j}$ and consider the set $\{g_1, \ldots, g_{s+2}\}$. Buchberger proved that after a finite number of steps this process will produce a set $\{g_1, \ldots, g_t\}$ which is a Gröbner basis for I.

Example 2.10. We saw in Example 2.6 that $\{XY - 1, Y^2 - 1\}$ is not a Gröbner basis for $I = (XY - 1, Y^2 - 1) \subset \mathbb{R}[X, Y]$ with respect to the lexicographic order where $Y \preceq X$. Let's apply Buchberger algorithm to find a Gröbner basis for I. Let $g_1 = XY - 1$ and $g_2 = Y^2 - 1$, then $S(g_1, g_2) = Yg_1 - Xg_2 = X - Y$ and the remainder in the division of $S(g_1, g_2)$ by $\{g_1, g_2\}$ is clearly $X - Y$. So let $g_3 = X - Y$ and consider the set (which generates I) $\{XY - 1, Y^2 - 1, X - Y\}$. Now the reminder in the division of $S(g_1, g_2)$ by $\{XY - 1, Y^2 - 1, X - Y\}$ is zero. One may also easily check that the remainder in the division of $S(g_1, g_3) = Y^2 - 1$ and $S(g_2, g_3) = Y^3 - X$ by $\{XY - 1, Y^2 - 1, X - Y\}$ is zero, so $\{XY - 1, Y^2 - 1, X - Y\}$ is a Gröbner basis for I (with respect to $\preceq$).

We introduce now the concept that solves Buchberger's thesis problem.

DEFINITION 2.11. Let $I \subset k[\boldsymbol{X}]$ be an ideal. The *footprint* of I (with respect to a fixed monomial order in $\mathcal{M}$) is the set

$$\Delta(I) = \{M \in \mathcal{M} \mid M \text{ is not the leading monomial of any polynomial in } I\}$$

The footprint of an ideal I has a close relationship with a Gröbner basis for I (both being defined with respect to the same monomial order in $\mathcal{M}$).

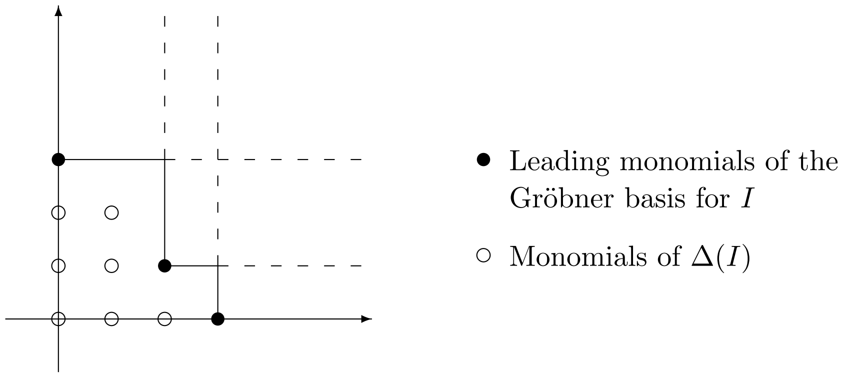
PROPOSITION 2.12. *Let $I \subset k[\boldsymbol{X}]$ be an ideal and let $\{g_1, \ldots, g_s\}$ be a Gröbner basis for I. Then a monomial M is in $\Delta(I)$ if and only if M is not a multiple of $lm(g_i)$ for all $i = 1, \ldots, s$.*

PROOF. The "only if" part is obvious from the definition of $\Delta(I)$. On the other hand, from the definition of Gröbner basis we know that if M is not a multiple of $\operatorname{lm}(g_i)$ for all $i = 1, \ldots, s$ then M is not the leading monomial of any polynomial in I. □

The above proof is very straightforward and uses the definition of $\Delta(I)$ in one direction and the defintion of Gröbner basis in the other. This hints that the concepts of Gröbner basis and footprint may be equivalent, and indeed they are in the following sense. Having defined what is a Gröbner basis for an ideal I we can define the footprint of I using the statement of the above proposition. On the other hand we can start with Definition 2.11 and then define a Gröbner basis for I as being a set $\{g_1, \ldots, g_s\} \subset I$ such that the set of monomials which are multiples of $\operatorname{lm}(g_i)$ for some $i \in \{1, \ldots, s\}$ is exactly $\mathcal{M} \setminus \Delta(I)$. Then one can prove that such a set $\{g_1, \ldots, g_s\}$ indeed exists and satisfies the condition in definition 2.5 (we do this in the Appendix).

In the following example we show how to use the above result to obtain a graphical representation of the footprint.

EXAMPLE 2.13. Let $I = (X^3 - X, Y^3 - Y, X^2Y - Y) \subset \mathbb{R}[X, Y]$, and endow $\mathcal{M}$ with the lexicographic order, where $Y \preceq X$. It is not difficult to check that $\{X^3 - X, Y^3 - Y, X^2Y - Y\}$ is a Gröbner basis for I. We have $\operatorname{lm}(X^3 - X) = X^3$, $\operatorname{lm}(Y^3 - Y) = Y^3$, $\operatorname{lm}(X^2Y - Y) = X^2Y$, and we apply the above proposition to determine $\Delta(I)$. It is easy to "see" the footprint of I in the figure below, where we represent a monomial $X^\alpha Y^\beta$ by the pair of nonnegative integers (α, β).



In fact, the points $(3,0)$, $(0,3)$ and $(2,1)$ correspond to the leading monomials of the Gröbner basis and from them it is easy to determine the monomials which are multiples of at least one of these leading monomials (thus determining the set of monomials which are the leading monomials of the polynomials in I). From this set and the above result we get that $\Delta(I) = \{1, X, X^2, Y, XY, Y^2, XY^2\}$.

We now present the solution to Buchberger's thesis problem, which will be very useful in the next section.

THEOREM 2.14. *Let $I \subset k[\boldsymbol{X}]$. Then*

$$\mathcal{B} := \{M + I \mid M \in \Delta(I)\}$$

is a basis for $k[\boldsymbol{X}]/I$ as a k-vector space.

PROOF. Let $\mathcal{G}$ be a Gröbner basis for I with respect to the same monomial order used to determine $\Delta(I)$, and let $f \in k[\boldsymbol{X}]$. Dividing f by $\mathcal{G}$ we get that the remainder is of the form $r = \sum_{i=1}^{t} a_i M_i$ where $a_i \in k[\boldsymbol{X}]$ and $M_i \in \Delta(I)$ for all $i = 1, \ldots, t$. Since $f + I = r + I$ we get that $\mathcal{B}$ generates $k[\boldsymbol{X}]/I$ as a k-vector space. Now assume that $\sum_{i=1}^{\ell} b_i(M_i + I) = 0 + I$, where $b_i \in k$ and $M_i \in \Delta(I)$ for all $i = 1, \ldots, \ell$. Then $\sum_{i=1}^{\ell} b_i M_i \in I$ so we must have $b_i = 0$ for all $i = 1, \ldots, \ell$, otherwise $\sum_{i=1}^{\ell} b_i M_i$ would be a nonzero element of I whose leading monomial is not a leading monomial of a polynomial in I. This shows that $\mathcal{B}$ is a linearly independent set over k. $\square$

EXAMPLE 2.15. We continue with the setup of Example 2.13. From the above result we get that $\mathbb{R}[X, Y]/I$ is an $\mathbb{R}$-vector space of dimension 7 and $\{1 + I, X + I, X^2 + I, Y + I, XY + I, Y^2 + I, XY^2 + I\}$ is a basis for this vector space.

We end this section with a remark that we will need in what follows. Let $I \subset k[\boldsymbol{X}]$ be an ideal and let $\{f_1, \ldots, f_t\}$ be a basis for I. We will denote by $\Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$ the set

$$\Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t)) := \{M \in \mathcal{M} \mid M \text{ is not a multiple of } f_i \text{ for all } i = 1, \ldots, t\}.$$

REMARK 2.16. Observe that $\Delta(I) \subset \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$. Actually, from Proposition 2.12 we get that $\Delta(I) = \Delta(\mathrm{lm}(f_1), \ldots, \mathrm{lm}(f_t))$ if and only if $\{f_1, \ldots, f_t\}$ is a Gröbner basis for I.

3. Affine varieties and affine cartesian codes

We start this section by presenting a key concept in algebraic geometry, the one which starts the interaction between algebra and geometry.

DEFINITION 3.1. Let $I \subset k[\boldsymbol{X}]$ be an ideal. The *(affine) variety* associated to I is the set

$$V(I) = \{(a_1, \ldots, a_n) \in k^n \mid f(a_1, \ldots, a_n) = 0 \text{ for all } f \in I\}.$$

It is easy to see that if $I = (g_1, \ldots, g_t)$ then $(a_1, \ldots, a_n) \in V(I)$ if and only if $g_i(a_1, \ldots, a_n) = 0$ for all $i = 1, \ldots, t$.

Given $V = V(I)$ we may ask for the set of all polynomials which vanish on V. It is easy to see that this set is an ideal of $k[\boldsymbol{X}]$ which contains I, and it is known as the *ideal of the variety* V and denoted by $\mathcal{I}(V)$. A famous theorem by Hilbert states that if k is algebraically closed then $\mathcal{I}(V(I)) = \sqrt{I}$, where $\sqrt{I} := \{f \in k[\boldsymbol{X}] \mid f^m \in I \text{ for some } m \in \mathbb{N}\}$ is the ideal known as the *radical of* I, see e.g. [**9**, p. 173].

A variety $V(I)$ may have infinitely many points (e.g. take $I = (Y - X^2) \subset \mathbb{R}[X, Y]$) or a finite number of points (e.g. take $I = (X^2 - 1, Y^2 - 1) \subset \mathbb{R}[X, Y]$). To prove an important relationship between the variety of I and the footprint of I when $\Delta(I)$ is finite we will need the following auxiliary result.

LEMMA 3.2. *Let $I \subset k[\boldsymbol{X}]$ be an ideal and let $P_1, \ldots, P_r$ be distinct points of $V(I)$. Then there exist polynomials $p_1, \ldots, p_r \in k[\boldsymbol{X}]$ such that $p_i(P_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, r\}$.*

PROOF. Let $P_i = (a_{i1}, \ldots, a_{in}) \in k^n$ where $i = 1, \ldots, r$, we will show how to obtain p_1 as in the lemma. Since all points are distinct, for $i \in \{2, \ldots, r\}$ there exists $j_i \in \{1, \ldots, n\}$ such that $a_{1j_i} \neq a_{ij_i}$. Let $h_i = (X_{j_i} - a_{ij_i})/(a_{1j_i} - a_{ij_i})$, then $h_i(P_1) = 1$ and $h_i(P_i) = 0$ for all $i = 2, \ldots, r$ so taking $p_1 = \prod_{i=2}^{r} h_i$ we get $p_1(P_1) = 1$ and $p_1(P_i) = 0$ for all $i = 2, \ldots, r$. In the same way we obtain $p_2, \ldots, p_r$ as in the lemma. $\square$

PROPOSITION 3.3. *Let $I \subset k[\boldsymbol{X}]$ be an ideal such that $\Delta(I)$ is a finite set. Then $V(I)$ is also a finite set and $\#(V(I)) \leq \#(\Delta(I))$.*

Proof. Let $P_1, \ldots, P_r$ be distinct elements of $V(I)$, we will find a set in $k[\boldsymbol{X}]/I$ which is linearly independent and has r elements. This will prove the proposition because as we saw $\#(\Delta(I))$ is the dimension of $k[\boldsymbol{X}]/I$ as a k-vector space. From the above Lemma we know that there exist $p_1, \ldots, p_r \in k[\boldsymbol{X}]$ such that $p_i(P_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, r\}$. Assume that $\sum_{i=1}^r a_i(p_i + I) = 0 + I$ where $a_1, \ldots, a_r \in k$, then $\sum_{i=1}^r a_i p_i \in I$ hence $\sum_{i=1}^r a_i p_i(P_j) = 0$, i.e. $a_j = 0$ for all $j \in \{1, \ldots, r\}$. Thus $\{p_1 + I, \ldots, p_r + I\}$ is a linearly independent set in $k[\boldsymbol{X}]/I$, which completes the proof. □

Actually, one can prove a more refined result (see [**3**, Thm. 8.32]). Recall that an ideal I is said to be a *radical ideal* if $I = \sqrt{I}$.

Theorem 3.4. *Let $I \subset k[\boldsymbol{X}]$ be an ideal such that $\Delta(I)$ is a finite set and let L be an algebraically closed extension of k. Then $V_L(I) := \{(a_1, \ldots, a_n) \in L^n \mid f(a_1, \ldots, a_n) = 0$ for all $f \in I\}$ is a finite set and $\#(V_L(I)) \leq \#(\Delta(I))$. Moreover, if k is a perfect field (e.g. a finite field or a field of characteristic zero) and I is a radical ideal then $\#(V_L(I)) = \#(\Delta(I))$.*

Now we want to apply the above facts to the study of error correcting codes, so we will quickly recall the definitions of a linear code, defined over a finite field $\mathbb{F}_q$ with q elements, and its main parameters.

Definition 3.5. A *(linear) code* $\mathcal{C}$ defined over the alphabet $\mathbb{F}_q$ and of length n is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q^n$. The elements of $\mathcal{C}$ are sometimes called *codewords*.

Let $\boldsymbol{a} = (a_1, \ldots, a_n), \boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$, the Hamming distance between $\boldsymbol{a}$ and $\boldsymbol{b}$ is defined as $d(\boldsymbol{a}, \boldsymbol{b}) = \#\{i \mid a_i \neq b_i, \text{ where } i \in \{1, \ldots, n\}\}$. If $\mathcal{C} \subset \mathbb{F}_q^n$ is a code and $\boldsymbol{a}, \boldsymbol{b} \in \mathcal{C}$ then $\boldsymbol{a} - \boldsymbol{b} \in \mathcal{C}$ and $d(\boldsymbol{a}, \boldsymbol{b}) = d(\boldsymbol{a} - \boldsymbol{b}, \boldsymbol{0})$ where $\boldsymbol{0}$ is the zero vector in $\mathbb{F}_q^n$.

Definition 3.6. Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a code. The *minimum distance* of $\mathcal{C}$ is the positive integer defined as $d_{\min}(\mathcal{C}) = \min\{d(\boldsymbol{a}, \boldsymbol{b}) \mid \boldsymbol{a}, \boldsymbol{b} \in \mathcal{C}, \boldsymbol{a} \neq \boldsymbol{b}\}$ (hence $d_{\min}(\mathcal{C}) = \min\{d(\boldsymbol{a}, \boldsymbol{0}) \mid \boldsymbol{a} \in \mathcal{C}, \boldsymbol{a} \neq \boldsymbol{0}\}$).

It is not difficult to show that d has indeed the properties of a distance function. The importance of the minimum distance lies in its relation to the error correction capacity of the code. Assume that a sender transmits an n-tuple $\boldsymbol{a}$ of the code $\mathcal{C}$ to a receiver through a channel (e.g. as in the communication between two computers or a mobile phone and a nearby antenna). Usually the channel "has noise" i.e. it changes some of the entries in the original n-tuple. Suppose that the channel changes at most t entries, with $t \leq (d_{\min}(\mathcal{C}) - 1)/2$. The receiver knows the code and thus will see, if $\boldsymbol{a}$ has been changed, that the received word $\boldsymbol{a}'$ is not a codeword (and in fact it is not because $0 < d(\boldsymbol{a}, \boldsymbol{a}') \leq t < d_{\min}(\mathcal{C})$) and moreover one can show that among all codewords only $\boldsymbol{a}$ satisfies $d(\boldsymbol{a}, \boldsymbol{a}') \leq t$ so the receiver can determine that the codeword which was sent is $\boldsymbol{a}$. The importance of the dimension $k(\mathcal{C})$ of a code is that it is a measure of how much information the code can carry, since the number of codewords will then be q^k. The importance of the length n of the code is that the longer the code is the more energy one must spend to transmit each codeword. The relative parameters $k(\mathcal{C})/n$ and $d_{\min}(\mathcal{C})/n$ are key concepts which appear in the analysis of the performance of a code, playing also an important role when one wishes to compare distinct codes. The ideal code would have a large dimension, a large minimum distance and a short length, but these requirements can't be met at the same time. In fact a basic relation between these parameters is the so-called Singleton inequality which states that $k(\mathcal{C}) + d_{\min}(\mathcal{C}) \leq n + 1$ (see e.g. [**15**, p. 33]).

In 1998 Fitzgerald and Lax proposed the following construction of linear codes. Let $I = (g_1, \ldots, g_t) \subset \mathbb{F}_q[\mathbf{X}]$ and set $I_q = (g_1, \ldots, g_t, X_1^q - X_1, \ldots, X_n^q - X_n)$. Recall that $\prod_{a \in \mathbb{F}_q}(X - a) = X^q - X$ so that $V(I) = V(I_q)$. From now on we will always be considering the graded lexicographic order in $\mathcal{M} \subset \mathbb{F}_q[\mathbf{X}]$. From Remark 2.16 we get that $\#(\Delta(I_q)) \leq \#(\Delta(\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_t), X_1^q, \ldots, X_n^q)) \leq q^n$ so from Proposition 3.3 we get that $\#(V(I_q)) \leq \#(\Delta(I_q))$. Let $V(I_q) = \{P_1, \ldots, P_m\}$ and let φ be the map

$$\begin{array}{rcl} \varphi : \mathbb{F}_q[\mathbf{X}]/I_q & \longrightarrow & \mathbb{F}_q^m \\ f + I_q & \longmapsto & (f(P_1), \ldots, f(P_m)). \end{array}$$

PROPOSITION 3.7. *The map φ is an isomorphism of $\mathbb{F}_q$-vector spaces.*

PROOF. It is clear that φ is a linear transformation. From $X_i^q - X_i \in I_q$ for all $i = 1, \ldots, n$ we get that I_q is a radical ideal (because it contains a univariate square-free polynomial in each variable - see e.g. [**3**, Prop. 8.14]), and also for any algebraically closed extension L of $\mathbb{F}_q$ we have $V_L(I_q) = V_{\mathbb{F}_q}(I_q)$, thus from Theorems 2.14 and 3.4 we get that $\dim \mathbb{F}_q[\mathbf{X}]/I_q = \#(\Delta(I_q)) = m$. From Lemma 3.2 we know that there are polynomials $p_1, \ldots, p_m \in \mathbb{F}_q[\mathbf{X}]$ such that $p_i(P_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, m\}$, thus $\varphi(p_i + I_q) = \boldsymbol{e}_i$, where $\boldsymbol{e}_i$ is the i-th vector in the canonical basis for $\mathbb{F}_q^m$, for all $i \in \{1, \ldots, m\}$. This proves that φ is surjective and a fortiori an isomorphism. $\square$

The following concept was introduced by Fitzgerald and Lax in [**11**].

DEFINITION 3.8. Let $L \subset \mathbb{F}_q[\mathbf{X}]/I_q$ be an $\mathbb{F}_q$-subvector space of $\mathbb{F}_q[\mathbf{X}]/I_q$. The image $\varphi(L) =: C(L)$ is called the *affine variety code* associated to L.

In [**11**] the authors prove that every $\mathbb{F}_q$-linear code is equal to $C(L)$ for some suitably chosen n, I and L.

We want to present results about a particular type of affine variety codes that was introduced recently by H. López, C. Rentería-Marquez and R. Villareal in [**14**], and independently, and in a generalized form, by O. Geil and C. Thomsen (see [**13**]). Let $A_1, \ldots, A_n$ be nonempty sets of $\mathbb{F}_q$ and let $X := A_1 \times \cdots \times A_n$. Let $f_i := \prod_{c \in A_i}(X_i - c)$ for all $i \in \{1, \ldots, n\}$ and let $I := (f_1, \ldots, f_n)$, clearly $V(I) = X$. As above we set $I_q = (f_1, \ldots, f_n, X_1^q - X_1, \ldots, X_n^q - X_n)$ and observe that in this case $I_q = I$ because f_i is a factor of $X_i^q - X_i$ for all $i = 1, \ldots, n$. Consider, for all integers $d \geq 0$, the $\mathbb{F}_q$-subvector space of $\mathbb{F}_q[\mathbf{X}]/I$ given by

$$L_d := \{p + I \mid p = 0 \text{ or} \deg(p) \leq d\}$$

where $\deg(p)$ is the total degree of the polynomial $p \in \mathbb{F}_q[\mathbf{X}]$.

Definition 3.9. The *affine cartesian code* $C(d)$ is the image $\varphi(L_d)$.

A very important instance of affine cartesian codes happens when we take $A_i = \mathbb{F}_q$ for all $i = 1, \ldots, n$. These are the so-called generalized Reed-Muller codes, a much studied example of linear codes.

In [**14**] the authors determine the parameters of these codes and we will also do this here, although most of the time we will not follow [**14**] but will use techniques involving the theory presented so far. Let $d_i := \#(A_i)$ for all $i = 1, \ldots, n$, then $V(I) = d_1. \cdots .d_n$ and this is the length of $C(d)$ for all $d \geq 0$. In [**14**] the authors prove that one may assume $2 \leq d_1 \leq \cdots \leq d_n$ without loss of generality (see [**14**, Prop. 3.2]).

Lemma 3.10. *$\{f_1, \ldots, f_n\}$ is a Gröbner basis for I.*

Proof. Clearly $\mathrm{lm}(f_i) = X_i^{d_i}$ for all $i = 1, \ldots, n$ so that

$$\Delta(I) \subset \{X_1^{\alpha_1}. \cdots .X_n^{\alpha_n} \mid 0 \leq \alpha_i < d_i \; \forall\, i = 1, \ldots, n\}.$$

From $\#(V(I)) = d_1. \ldots .d_n \leq \#(\Delta(I))) \leq d_1. \ldots .d_n$ we get in particular that $\#(\Delta(I)) = d_1. \ldots .d_n$. This shows that $B := \{f_1, \ldots, f_n\}$ is a Gröbner basis for I, otherwise from Buchberger's algorithm we would have to add to B a polynomial whose leading monomial is not a multiple of $X_i^{d_i}$ for all $i = 1, \ldots, n$ but this would imply $\#(\Delta(I)) < d_1. \ldots .d_n$, a contradiction. □

Lemma 3.11. *(cf.* [**14**, Lemma 2.3]*) The ideal of X is I.*

Proof. Clearly $I \subset \mathcal{I}(X)$ so that $\Delta(\mathcal{I}(X)) \subset \Delta(I)$. From Proposition 3.3 and the above Lemma we have $d_1. \cdots .d_n = \#(V(\mathcal{I}(X))) \leq \#(\Delta(\mathcal{I}(X))) \leq \#(\Delta(I)) = d_1. \cdots .d_n$ so $\Delta(\mathcal{I}(X)) = d_1. \cdots .d_n$. Since $\{f_1, \ldots, f_n\} \subset \mathcal{I}(X)$ as in the previous lemma we get that $\{f_1, \ldots, f_n\}$ is a (Gröbner) basis for $\mathcal{I}(X)$ and $\mathcal{I}(X) = I$. □

Now we want to calculate the dimension of $C(d)$. Since φ is an isomorphism and $C(d) = \varphi(L_d)$ we have that $\dim C(d) = \dim L_d$. Let $\Delta(I)_{\leq d} := \{M \in \Delta(I) \mid \deg(M) \leq d\}$.

PROPOSITION 3.12. *The set* $\{M + I \mid M \in \Delta(I)_{\leq d}\}$ *is a basis for* L_d.

PROOF. From Theorem 2.14 we know that $\{M + I \mid M \in \Delta(I)_{\leq d}\}$ is a linearly independent set, and clearly it is contained in L_d. Let $f \in \mathbb{F}_q[\mathbf{X}]$, $f \neq 0$ such that $\deg(f) \leq d$. Let r be the remainder in the division of f by $\{f_1, \ldots, f_n\}$. From the division algorithm, the fact that $\{f_1, \ldots, f_n\}$ is a Gröbner basis for I and Proposition 2.12 we get that r is a linear combination of monomials in $\Delta(I)_{\leq d}$, which ends the proof. $\square$

As a consequence of the above result we get the following result.

LEMMA 3.13. *(cf.* [**14**, Thm. 3.1]*) The dimension of* $C(d)$ *is* $\dim C(d) = \#(\Delta(I)_{\leq d})$*, in particular* $\dim C(d) = d_1 . \cdots . d_n$ *and* $d_{\min}(C(d)) = 1$ *for all* $d \geq \sum_{i=1}^{n}(d_i - 1)$.

PROOF. The first assertion is a consequence of the above Proposition and the fact that φ is an isomorphism. For the second and third, observe that since $\{f_1, \ldots, f_n\}$ is a Gröbner basis for I we have

$$\Delta(I) = \{X_1^{\alpha_1} . \cdots . X_n^{\alpha_n} \mid 0 \leq \alpha_i \leq d_i - 1 \; \forall\, i = 1, \ldots, n\}$$

thus $\Delta(I)_{\leq d} = \Delta(I)$ whenever $d \geq \sum_{i=1}^{n}(d_i - 1)$. The result now follows from $\#(\Delta(I)) = d_1 . \cdots . d_n$ and the fact that $\varphi(L(d)) = \mathbb{F}_q^{d_1 . \cdots . d_n}$. $\square$

THEOREM 3.14. *(cf.* [**14**, Thm. 3.1]*) The dimension of* $C(d)$ *for* $0 \leq d < \sum_{i=1}^{n}(d_i - 1)$ *is given by*

$$\begin{aligned} \dim(C(d)) = & \binom{n+d}{d} - \sum_{i=1}^{n} \binom{n+d-d_i}{d-d_i} + \cdots + \\ & (-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} \binom{n+d-d_{i_1} - \cdots - d_{i_j}}{d - d_{i_1} - \cdots - d_{i_j}} + \cdots + \\ & (-1)^n \binom{n+d-d_1-\cdots-d_n}{d-d_1-\cdots-d_n} \end{aligned}$$

where we set $\binom{a}{b} = 0$ *if* $b < 0$.

PROOF. According to the previous result the dimension of $C(d)$ is equal to the cardinality of $\Delta(I)_{\leq d}$, i.e. the number of monomials in $\Delta(I)$ of the form $X_1^{\alpha_1} . \cdots . X_n^{\alpha_n}$ with $0 \leq \sum_{i=1}^{n} \alpha_i \leq d$. Let

$$h(t) := (1 + t + \cdots + t^{d_1 - 1}) . \cdots . (1 + t + \cdots + t^{d_n - 1}),$$

it is easy to see that the coefficient of t^e in $h(t)$ is equal to the number of monomials in $\Delta(I)$ which have degree e, for all $e \in \{0, \ldots, \sum_{i=1}^n (d_i - 1)\}$. Thus one way to obtain what we want is to calculate the coefficients of $t^0, t, \ldots, t^d$ and then sum them up. A quicker way is to observe that there is a bijection between the sets $\Delta(I)_{\leq d}$ and

$$\square_d := \{X_0^{\alpha_0}.X_1^{\alpha_1}.\cdots.X_n^{\alpha_n} \in \mathbb{F}_q[X_0, X_1, \ldots, X_n] \mid \text{ with } \sum_{i=0}^n \alpha_i = d \text{ and } 0 \leq \alpha_i \leq d_i - 1 \ \forall i = 1, \ldots, n\}$$

given by $\beta : \Delta(I)_{\leq d} \to \square_d$ where $\beta(M) = X_0^d M(X_1/X_0, \ldots, X_n/X_0)$ and $\beta^{-1} : \square_d \to \Delta(I)_{\leq d}$ is given by $\beta^{-1}(N) = N(1, X_1, \ldots, X_n)$. Now consider

$$H(t) := (1 + t + t^2 + \cdots).(1 + t + \cdots + t^{d_1 - 1}).\cdots.(1 + t + \cdots + t^{d_n - 1}),$$

then the coefficient of t^d is the cardinality of $\square_d$. To calculate this coefficient we note that we may think of $H(t)$ as a real function of one variable t defined in a suitable neighborhood of 0, say $|t| < 1$. Then $1 + t + t^2 + \cdots = 1/(1 - t)$ so that

$$H(t) = \frac{1}{1-t}.\frac{1 - t^{d_1}}{1 - t}.\cdots.\frac{1 - t^{d_n}}{1 - t}$$

thus $H(t) = (1/(1-t)^{n+1}) \prod_{i=1}^n (1 - t^{d_i})$. Using that $1/(1-t)^{n+1} = \sum_{j=0}^\infty \binom{n+j}{j} t^j$ we get

$$H(t) = (\sum_{j=0}^\infty \binom{n+j}{j} t^j)(1 - \sum_{i=1}^n t^{d_i} + \sum_{1 \leq i_1 < i_2 \leq n} t^{d_{i_1} + d_{i_2}} + \cdots + (-1)^j \sum_{1 \leq i_1 < \cdots < i_j \leq n} t^{d_{i_1} + \cdots + d_{i_j}} + \cdots + (-1)^n t^{d_{i_1} + \cdots + d_{i_n}}).$$

The expression for $\dim C(d)$ in the statement of the theorem is the coefficient of t^d in $H(t)$ calculated using the above product. $\square$

To find the minimum distance of $C(d)$, for $0 \leq d < \sum_{i=1}^n (d_i - 1)$, we need the following auxiliary result.

LEMMA 3.15. *Let $0 < d_1 \leq \cdots \leq d_n$ and $s < \sum_{i=1}^n (d_i - 1)$ be integers. Let $m(\alpha_1, \ldots, \alpha_n) := \prod_{i=1}^n (d_i - \alpha_i)$, where $0 \leq \alpha_i < d_i$ is an integer for all $i = 1, \ldots, n$. Then*

$$\min\{m(\alpha_1, \ldots, \alpha_n) \mid \alpha_1 + \cdots + \alpha_n \leq s\} = (d_{k+1} - \ell) \prod_{i=k+2}^n d_i$$

where k and ℓ are uniquely defined by $s = \sum_{i=1}^{k}(d_i - 1) + \ell$ with $0 \leq \ell < d_{k+1} - 1$. Here, if $k + 1 = n$ then we understand that $\prod_{i=k+2}^{n} d_i = 1$, and if $s < d_1 - 1$ then we set $k = 0$ and $\ell = s$.

Proof. Observe that the minimum must be attained when $\sum_{i=1}^{n} \alpha_i = s$, and the Lemma claims it is attained at the n-tuple $(d_1 - 1, \ldots, d_k - 1, \ell, 0, \ldots, 0)$. Thus let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ with $\sum_{i=1}^{n} \alpha_i = s$ and assume that $\alpha_{i_1} < d_{i_1} - 1$ for some $i_1 \in \{1, \ldots, k\}$. If there exists $i_2 \in \{k+1, \ldots, n\}$ such that $\alpha_{i_2} > 0$ and $\alpha_{i_1} + \alpha_{i_2} \leq d_{i_1} - 1$ then denoting by $\boldsymbol{\alpha}'$ the n-tuple obtained from $\boldsymbol{\alpha}$ by replacing α_{i_1} by $\alpha_{i_1} + \alpha_{i_2}$ and α_{i_2} by 0 we get that

$$m(\boldsymbol{\alpha}) - m(\boldsymbol{\alpha}') = (\alpha_{i_1}\alpha_{i_2} + (d_{i_2} - d_{i_1})\alpha_{i_2}). \prod_{\substack{i=1 \\ i \neq i_1, i_2}}^{n} (d_i - \alpha_i) \geq 0$$

so that $m(\boldsymbol{\alpha}) \geq m(\boldsymbol{\alpha}')$. If there exists $i_2 \in \{k+1, \ldots, n\}$ such that $\alpha_{i_2} > 0$ and $\alpha_{i_1} + \alpha_{i_2} > d_{i_1} - 1$ then denoting by $\boldsymbol{\alpha}''$ the n-tuple obtained from $\boldsymbol{\alpha}$ by replacing α_{i_1} by $d_{i_1} - 1$ and α_{i_2} by $\alpha_{i_2} - (d_{i_1} - 1 - \alpha_{i_1})$ we get that

$$m(\boldsymbol{\alpha}) - m(\boldsymbol{\alpha}'') = (d_{i_1} - 1 - \alpha_{i_1})(d_{i_2} - 1 - \alpha_{i_2}). \prod_{\substack{i=1 \\ i \neq i_1, i_2}}^{n} (d_i - \alpha_i) \geq 0$$

so that $m(\boldsymbol{\alpha}) \geq m(\boldsymbol{\alpha}'')$. This proves that if m attains its minimum at $\boldsymbol{\alpha}$ we may assume that $\alpha_i = d_i - 1$ for all $i = 1, \ldots, k$. In the same way we prove that we may also assume $\alpha_{k+1} = \ell$. $\square$

Theorem 3.16. *(cf. [**14**, Thm. 3.8]) Let $0 \leq d < \sum_{i=1}^{n}(d_i - 1)$, the minimum distance of $C(d)$ is $(d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$ where k and ℓ are uniquely defined by $d = \sum_{i=1}^{k}(d_i - 1) + \ell$ with $0 \leq \ell < d_{k+1} - 1$. As in the above result, if $k + 1 = n$ we understand that $\prod_{i=k+2}^{n} d_i = 1$, and if $d < d_1 - 1$ then we set $k = 0$ and $\ell = d$.*

Proof. Let $F \in L_d$ and let $J_F := (F, f_1, \ldots, f_n)$. Then the number of zeroes in the codeword $\varphi(F + I)$ is equal to $\#(V(J_F))$ so that the weight of this codeword is $w(\varphi(F + I)) = \prod_{i=1}^{n} d_i - \#(V(J_F))$. From Theorem 3.3 we get that $\#(V(J_F)) \leq \#(\Delta(J_F))$. Let $M := X_1^{\alpha_1}. \cdots .X_n^{\alpha_n}$ be the leading monomial of F, from Remark 2.16 we get that $\Delta(J_F) \subset \Delta(M, X_1^{d_1}, \ldots, X_n^{d_n})$ so that $\#(\Delta(J_F)) \leq \prod_{i=1}^{n} d_i - \prod_{i=1}^{n}(d_i - \alpha_i)$. Thus $w(\varphi(F+I)) \geq \prod_{i=1}^{n}(d_i - \alpha_i)$ and from the previous Lemma we have $w(\varphi(F + I)) \geq (d_{k+1} - \ell) \prod_{i=k+2}^{n} d_i$. To see that this bound is actually attained we write $A_i := \{a_{i1}, \ldots, a_{id_i}\}$ for $i = 1, \ldots, n$ and let $G(X_1, \ldots, X_n) = \left(\prod_{i=1}^{k} \prod_{j=1}^{d_i - 1}(X_i - a_{ij}) \right) \prod_{j=1}^{\ell}(X_{k+1} - a_{k+1\,j})$, then $\deg(G) = d$, G has

$\prod_{i=1}^n d_i - (d_{k+1} - \ell) \prod_{i=k+2}^n d_i$ zeroes in $A_1 \times \cdots \times A_n$ so $w(\varphi(G + I)) = (d_{k+1} - \ell) \prod_{i=k+2}^n d_i$. □

Comparing the above proof to the original one, presented in [**14**, Thm. 3.8], one sees that the footprint technique yields a substantial simplification in the proof. This technique had already been used in [**12**] to study higher Hamming weights of generalized Reed-Muller codes and was used in [**6**] to study higher Hamming weights of affine cartesian codes. We present the main results of [**6**] in the next section.

4. The second lowest Hamming weight of affine cartesian codes

LEMMA 4.1. *Let $2 \le s \le d_1 \le \cdots \le d_n$ be integers, with $n \ge 2$. Let $q(a_1, \ldots, a_n) = \prod_{i=1}^n (d_i - a_i)$ where $0 \le a_i < s$ is an integer for all $i = 1, \ldots, n$. Then*

$$\min\{q(a_1, \ldots, a_n) \mid a_1 + \cdots + a_n \le s\} = (d_1 - (s-1))(d_2 - 1) \prod_{i=3}^n d_i.$$

PROOF. As in the previous Lemma we observe that the minimum must be attained when $\sum_{i=1}^n a_i = s$. Thus, let $\boldsymbol{\alpha} = (a_1, \ldots, a_n)$, with $\sum_{i=1}^n a_i = s$ and assume that $a_1 < s - 1$. If there exists $i_2 \in \{2, \ldots, n\}$ such that $a_{i_2} > 0$ and $a_1 + a_{i_2} \le s - 1$ then denoting by $\boldsymbol{\alpha}'$ the n-tuple obtained from $\boldsymbol{\alpha}$ by replacing a_1 by $a_1 + a_{i_2}$ and a_{i_2} by 0, we get that

$$m(\boldsymbol{\alpha}) - m(\boldsymbol{\alpha}') = (a_1 a_{i_2} + (d_{i_2} - d_1) a_{i_2}) \prod_{\substack{i=2 \\ i \ne i_2}}^n (d_i - a_i) \ge 0$$

so $m(\boldsymbol{\alpha}) \ge m(\boldsymbol{\alpha}')$ and $m(\boldsymbol{\alpha}) > m(\boldsymbol{\alpha}')$ if $a_1 \ne 0$. If there exists $i_2 \in \{2, \ldots, n\}$ such that $a_1 + a_{i_2} > s - 1$ then we must have $a_1 > 0$ and $a_{i_2} = s - a_1$, denoting by $\boldsymbol{\alpha}''$ the n-tuple obtained from $\boldsymbol{\alpha}$ by replacing a_1 by $s - 1$ and a_{i_2} by 1 we get

$$m(\boldsymbol{\alpha}) - m(\boldsymbol{\alpha}'') = (d_{i_2} - d_1 + a_1 - 1)(s - a_1 - 1) \prod_{\substack{i=2 \\ i \ne i_2}}^n (d_i - a_i) \ge 0.$$

This shows that if q attains its minimum at $\boldsymbol{\alpha} = (a_1, \ldots, a_n)$ then we may assume that $a_1 = s - 1$ and now it is easy to check that we can also assume $a_2 = 1$. □

We will now determine the second Hamming weight of codes $C(d)$ for several particular cases of this code. We start with the case where all the sets in the cartesian product have the same cardinality a and $2 \le d < a$ (hence $a \ge 3$).

THEOREM 4.2. *Let $A_i \subset \mathbb{F}_q$ such that $\#(A_i) = a \geq 3$ for all $i = 1, \ldots, n$, with $n \geq 2$ and let $2 \leq d < a$. The second Hamming weight of $C(d)$ is $(a-(d-1))(a-1)a^{n-2}$.*

PROOF. We write $A_i = \{\boldsymbol{a}_{i1}, \ldots, \boldsymbol{a}_{ia}\}$ for all $i = 1, \ldots, n$, and let $1 \leq t < a$. Let $F \in \mathbb{F}_q[X_1, \ldots, X_n]$ be a polynomial of degree t and let $J_F = (F, f_1, \ldots, f_n)$. As in the proof of Theorem 3.16 we have that $w(\varphi(F+I)) = \prod_{i=1}^n d_i - \#(V_{\mathbb{F}_q}(J_F))$. Let $M := X_1^{a_1} \cdot \cdots \cdot X_n^{a_n}$ be the leading monomial of F (so that $\sum_{i=1}^n a_i = t$ because we are using the graded-lexicographic order). We deal first with the case where $t \geq 2$.
a) Assume that $a_i < t$ for all $i = 1, \ldots, n$. From

$$\#(V_{\mathbb{F}_q}(J_F)) \leq \#(\Delta(J_F)) \leq \#(\Delta(M, X_1^{d_1}, \ldots, X_n^{d_n})) = \prod_{i=1}^n d_i - \prod_{i=1}^n (d_i - a_i)$$

and Lemma 4.1 we get $w(\varphi(F+I)) \geq (d_1 - (t-1))(d_2 - 1)\prod_{i=3}^n d_i$. This bound is effectively attained, for example, when $F = \left(\prod_{i=1}^{t-1}(X_1 - \boldsymbol{a}_{1i})\right)(X_2 - \boldsymbol{a}_{21})$.
b) Assume now that $a_j = t$ for some $j \in \{1, \ldots, n\}$. If $\{F, f_1, \ldots, f_n\}$ is a Gröbner basis for J_F then $\#(\Delta(J_F)) = ta^{n-1}$ and $w(\varphi(F+I)) = a^n - ta^{n-1} = (a-t)a^{n-1}$; from Theorem 3.16 we get that this is the minimum distance of $C(t)$. If $\{F, f_1, \ldots, f_n\}$ is not a Gröbner basis for J_F then the S-polynomial $S(F, f_j) = X_j^{a-t}F - f_j$ must have a nonzero remainder R in the division by $\{F, f_1, \ldots, f_n\}$ (otherwise $\{F, f_1, \ldots, f_n\}$ would be a Gröbner basis because any other pair of distinct polynomials $\{g_1, g_2\}$ in $\{F, f_1, \ldots, f_n\}$ has leading monomials which are relatively prime - see [**9**, pags. 103 and 104]). Let $L := X_1^{b_1} \cdot \cdots \cdot X_n^{b_n}$ be the leading monomial of R, from the division algorithm we get $b_j < t$, $b_i < a$ for all $i \in \{1, \ldots, n\}$, $i \neq j$ and $\sum_{i=1}^n b_i \leq \deg(S(F, f_j)) \leq a$. Thus $J_F = (F, f_1, \ldots, f_n) = (R, F, f_1, \ldots, f_n)$ so that

$$\#(\Delta(J_F)) \leq \#(\Delta(L, X_j^t, X_1^a, \ldots, X_n^a)) = ta^{n-1} - (t - b_j)\prod_{i=1, i\neq j}^n (a - b_i)$$

Now we apply Lemma 3.15 with $d_1 = t$, $d_i = a$ for $i = 2, \ldots, n$ and $s = a$, and writing $a = (t-1) + (a-(t-1))$ we get that an upper bound for the number of zeroes of F in X is $ta^{n-1} - (t-1)a^{n-2}$ so the minimum distance of $\varphi(F+I)$ is lower bounded by $a^n - ta^{n-1} + (t-1)a^{n-2} = (a-1)(a-t+1)a^{n-2}$. This proves that for $2 \leq t < a$ the possible values for $w(F+I)$, where F is a polynomial of degree t are in the set $\{(a-t)a^{n-1}\} \cup \{w \in \mathbb{N} \mid w \geq (a-1)(a-t+1)a^{n-2}\}$ where $(a-t)a^{n-1}$ and $(a-1)(a-t+1)a^{n-2}$ are realized as weights.

In the case where $t = 1$ we have $M = X_j$ for some $j \in \{1, \dots, n\}$ so that $\#(\Delta(M, X_1^a, \dots, X_n^a) = a^n - (a-1)a^{n-1}$, thus $w(F + I) \geq (a-1)a^{n-1}$.

Now we put the above results together to calculate the second smallest weight of $C(d)$, where $2 \leq d < a$, and find that it is equal to $(a-1)(a-d+1)a^{n-2}$. This is because $(a-1)(a-d+1)a^{n-2} < (a-1)(a-t+1)a^{n-2}$ and $(a-1)(a-d+1)a^{n-2} < (a-t)a^{n-1}$ for all $1 \leq t < d$, and of course $(a-d)a^{n-1} < (a-1)(a-d+1)a^{n-2}$. □

Setting $a = q$ in the above theorem we get the values for the second Hamming weight of the generalized Reed-Muller codes when $2 \leq d < q$ (cf. [**12**]).

In the next theorem we treat the case where we have the cartesian product of two subsets of $\mathbb{F}_q$ with distinct cardinalities.

Theorem 4.3. *Let $A_1, A_2 \subset \mathbb{F}_q$ be such that $3 \leq \#(A_1) =: d_1 < d_2 := \#(A_2)$ and let $2 \leq d < d_1$. The second Hamming weight of $C(d)$ is $(d_1 - d + 1))(d_2 - 1)$.*

Proof. We follow the same procedure of the above proof, and although the beginning is similar the development is a bit more elaborate. We write $A_i = \{\boldsymbol{a}_{i1}, \dots, \boldsymbol{a}_{id_i}\}$ for $i = 1, 2$, and let $1 \leq t < d_1$. Let $F \in \mathbb{F}_q[X_1, X_2]$ be a polynomial of degree t and let $J_F = (F, f_1, f_2)$. Then $w(\varphi(F + I)) \geq d_1 d_2 - \#(\Delta(J_F))$. Let $M := X_1^{a_1}.X_2^{a_2}$ be the leading monomial of F (hence $a_1 + a_2 = t$). We deal first with the case where $t \geq 2$.

a) Assume that $a_i < t$ for $i = 1, 2$. From $\#(\Delta(J_F)) \leq \#(\Delta(M, X_1^{d_1}, X_2^{d_2})) = d_1 d_2 - \prod_{i=1}^2 (d_i - a_i)$ and Lemma 4.1 we get $w(\varphi(F + I)) \geq (d_1 - (t - 1))(d_2 - 1)$. This bound is effectively attained, for example, when $F = \left(\prod_{i=1}^{t-1}(X_1 - \boldsymbol{a}_{1i})\right)(X_2 - \boldsymbol{a}_{21})$.

b) Assume now that $a_j = t$ for $j = 1$ or $j = 2$. If $\{F, f_1, f_2\}$ is a Gröbner basis for J_F then $\#(\Delta(J_F)) = td_2$, if $a_1 = t$ or $\#(\Delta(J_F)) = td_1$, if $a_2 = t$ so that $w(\varphi(F + I)) \geq d_1 d_2 - td_2$ if $a_1 = t$ or $w(\varphi(F + I)) \geq d_1 d_2 - td_1$ if $a_2 = t$. According to Theorem 3.16 $(d_1 - t)d_2$ is the minimum distance of $C(t)$, and it is easy to check that $(d_2 - t)d_1$ is also realized as the weight of a codeword. We assume now that $\{F, f_1, f_2\}$ is not a Gröbner basis for J_F, and we treat separatedly the cases where $M = X_1^t$ and $M = X_2^t$.

When $M = X_1^t$ we must have that the S-polynomial $S(F, X_1) = X_1^{d_1 - t}F - X_1^{d_1}$ has a nonzero remainder in the division by $\{F, X_1^{d_1}, X_2^{d_2}\}$ (because X_1^t and $X_2^{d_2}$ are relatively prime), so let $L := X_1^{b_1} X_2^{b_2}$ be the leading monomial of this remainder. From the division algorithm we get $b_1 < t$, $b_2 < d_2$ and $b_1 + b_1 \leq d_1$. We have $\#(\Delta(J_F)) \leq \#(\Delta(L, M, X_1^{d_1}, X_2^{d_2})) = td_2 - (t - b_1)(d_2 - b_2)$ so $w(\varphi(F + I)) \geq d_1 d_2 - td_2 + (t - b_1)(d_2 - b_2)$. We now use Lemma

3.15 to find the minimum of $(t-b_1)(d_2-b_2)$, observing the restrictions on b_1 and b_2, and get $w(\varphi(F+I)) \geq d_1d_2-td_2+d_2-d_1+t-1 = (d_2-1)(d_1-t+1)$.

When $M = X_2^t$ we have that the S-polynomial $S(F, X_2) = X_2^{d_2-t}F - X_2^{d_2}$ has a nonzero remainder in the division by $\{F, X_1^{d_1}, X_2^{d_2}\}$ and again we denote by $L = X_1^{b_1}X_2^{b_2}$ the leading monomial of this remainder. From the division algorithm we get $b_1 < d_1$, $b_2 < t$ and $b_1 + b_2 \leq d_2$, but from $b_1 < d_1$ and $b_2 < t$ we also get $b_1+b_2 \leq d_1+t-2$, thus $b_1+b_2 \leq r := \min\{d_2, d_1+t-2\}$. As before we note that $\#(\Delta(J_F)) \leq \#(\Delta(L, M, X_1^{d_1}, X_2^{d_2})) = td_1-(d_1-b_1)(t-b_2)$ so that $w(\varphi(F+I)) \geq d_1d_2 - td_1 + (d_1-b_1)(t-b_2)$. Now we want to apply Lemma 3.15 to find the minimum of $(t-b_2)(d_1-b_1)$, observing the restrictions on b_1 and b_2. If $r = d_1+t-2$ then from $d_1+t-2 = (t-1)+(d_1-1)$ we get that the minimum is 1, hence $w(\varphi(F+I)) \geq d_1(d_2-t)+1$. If $r = d_2$ then $d_2 \leq d_1+t-2$ so $d_2-t+1 \leq d_1-1$, thus from $d_2 = (t-1)+d_2-t+1$ and Lemma 3.15 we get that the minimum is d_1-d_2+t-1, which implies that $w(\varphi(F+I)) \geq (d_1-1)(d_2-t+1)$.

This completes the analysis of the case where $t \geq 2$. In the case where $t = 1$ we have that either $w(\varphi(F+I)) \geq (d_1-1)d_2$ or $w(\varphi(F+I)) \geq d_1(d_2-1)$.

From what is done so far we get that if $2 \leq t < d_1$ then $w(\varphi(F+I)) \in \{(d_1-t)d_2\} \cup \{v \in \mathbb{N} \mid v \geq (d_2-1)(d_1-t+1)\}$ because $(d_2-1)(d_1-t+1) - d_1(d_2-t) = -(t-1)(d_2-d_1-1) \leq 0$ and $(d_2-1)(d_1-t+1)-(d_1-1)(d_2-t+1) = -(t-2)(d_2-d_1) \leq 0$.

Thus considering the weights $w(\varphi(F+I))$ for all polynomials F of degree less of equal than d (where $2 \leq d < d_1$) we get that the second smallest weight is $(d_2-1)(d_1-d+1)$, this is because $(d_2-1)(d_1-d+1) < (d_2-1)(d_1-t+1)$ and $(d_2-1)(d_1-d+1) < (d_1-t)d_2$ whenever $1 \leq t < d$, and $(d_1-d)d_2 < (d_2-1)(d_1-d+1)$. □

The following result deals with higher Hamming weights of the code $C(d)$.

Theorem 4.4. *Let $2 \leq d_1 \leq \cdots \leq d_n$ be integers, with $n \geq 2$, and let d be an integer such that $\sum_{i=1}^{n-1}(d_i-1) \leq d < \sum_{i=1}^{n}(d_i-1)$. Write $d = \sum_{i=1}^{n-1}(d_i-1)+\ell$, with $0 \leq \ell < d_n-1$. Then for $t \in \{1, \ldots, \ell+1\}$ the t-th weight of $C(d)$ is $d_n-\ell+(t-1)$.*

Proof. For $t \in \{1, \ldots, \ell+1\}$ we have $C(d-(t-1)) \subset C(d)$ so from Theorem 3.16 we get that in $C(d)$ there are words of weight $d_n-\ell, d_n-\ell+1, \ldots, d_n$, being $d_n-\ell$ the minimum distance of $C(d)$. This proves the theorem. □

We now put the last three results together to determine the second Hamming weight of $C(d)$, for all $d \geq 2$, in the case where we have the cartesian product of two sets containing at least three elements each.

COROLLARY 4.5. *Let $A_1, A_2 \subset \mathbb{F}_q$ be such that $3 \leq \#(A_1) =: d_1 \leq d_2 := \#(A_2)$ and let $2 \leq d$. Then second Hamming weight of $C(d)$ is equal to:*
i) $(d_1 - d + 1)(d_2 - 1)$ if $2 \leq d < d_1$;
ii) $d_1 + d_2 - d$ if $d_1 \leq d \leq d_1 + d_2 - 2$;
iii) 2 if $d_1 + d_2 - 2 < d$.

PROOF. Item (i) is a direct consequence of Theorems 4.2 and 4.3. Item (ii) is a consequence of the above theorem, because writing $d = (d_1 - 1) + \ell$ we get that the second weight is $d_2 - \ell + 1 = d_1 + d_2 - d$. Item (iii) comes from the fact that $C(d) = \mathbb{F}_q^m$ whenever $d \geq d_1 + d_2 - 2$ as observed just before Lemma 3.15 (this is also proved in [**14**]). $\square$

We remark that in the literature the second lowest Hamming weight is also called the next-to-minimal Hamming weight of a code. For the Reed-Muller codes, these weights have already been determined (see [**2**] and the references therein). In [**8**] most of the next-to-minimal weights of the affine cartesian are determined. The parameters of a projective version of the affine cartesian codes were recently determined by Carvalho, López and Neumann (see [**7**]).

Appendix A

Here we show how one may arrive at the concept of Gröbner basis starting from the definition of footprint of an ideal (see Definition 2.11). We endow the set of monomials of $\mathcal{M} \in k[\boldsymbol{X}]$ with a monomial order $\preceq$ and also with a partial order $\leq$ defined by: $\boldsymbol{X}^{\boldsymbol{\alpha}} \leq \boldsymbol{X}^{\boldsymbol{\beta}}$ if $\boldsymbol{X}^{\boldsymbol{\beta}}$ is a multiple of $\boldsymbol{X}^{\boldsymbol{\alpha}}$. Let $I \subset k[\boldsymbol{X}]$ be a nonzero ideal and let $\Delta(I)$ be the footprint of I with respect to $\preceq$. Let $\Gamma(I)$ be set of minimal elements of $\mathcal{M} \setminus \Delta(I)$ with respect to the partial order $\leq$ so that every monomial in $\mathcal{M} \setminus \Delta(I)$ is a multiple of some monomial in $\Gamma(I)$.

THEOREM A.1. *Let $(\Gamma(I))$ denote the ideal generated by the monomials in $\Gamma(I)$, then there exists a subset $\{M_1, \ldots, M_s\} \subset \Gamma(I)$ such that $(M_1, \ldots, M_s) = (\Gamma(I))$.*

PROOF. This is a consequence of the fact that $k[\boldsymbol{X}]$ is a noetherian ring, so every ideal is finitely generated and from the definition of $(\Gamma(I))$ the generators may be chosen among the elements of $\Gamma(I)$. $\square$

COROLLARY A.2. $\Gamma(I) = \{M_1, \ldots, M_s\}$.

PROOF. Let $M \in \Gamma(I) \subset (\Gamma(I))$, then $M = \sum_{i=1}^{s} p_i M_i$ where $p_i \in k[\boldsymbol{X}]$ for all $i = 1, \ldots, s$ and since M is a monomial it must be one of the monomials which appear in $p_j M_j$ for some $j \in \{1, \ldots, s\}$. Thus $M_j \leq M$ and since M is a minimal element with respect to $\leq$ we must have $M = M_j$. $\square$

DEFINITION A.3. Let $\mathcal{G}(I) \subset I$ be a set of polynomials $\{g_1, \ldots, g_s\}$ such that for every monomial $M \in \Gamma(I)$ there is exactly one polynomial in $\mathcal{G}(I)$ having M as leading monomial. Then $\mathcal{G}(I)$ is a *Gröbner basis* for I (with respect to $\preceq$).

The above theorem shows that there exists a Gröbner basis for any nonzero ideal of $k[\boldsymbol{X}]$, and the next result proves that this is the same concept defined in text (see Definition 2.5).

PROPOSITION A.4. *Let $\mathcal{G}(I)$ be a Gröbner basis for I. Then $\mathcal{G}(I)$ is a basis for the ideal I with the property that for any $f \in I$, $f \neq 0$ we have that $lm(f)$ is a multiple of $lm(g_i)$ for some $i \in \{1, \ldots, s\}$.*

PROOF. Let $\mathcal{G}(I) = \{g_1, \ldots, g_s\}$ and let $f \in I$. In the division of f by the elements of $\mathcal{G}(I)$ the remainder r is a sum of terms whose monomials are in $\Delta(I)$, and since $r \in I$ we must have $r = 0$, otherwise r would be a polynomial in I whose leading monomial is in $\Delta(I)$. This proves that $\mathcal{G}(I)$ is a basis for the ideal I. The last assertion is a consequence of the definition of $\Gamma(I)$ and the fact that $\Gamma(I) = \{\mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_s)\}$.. $\square$

Strictly speaking, since the leading monomials of the Gröbner basis $\mathcal{G}(I)$ defined above are not multiple one of another we have proved that from the footprint of I we may arrive at what is called in the literature a *minimal* Gröbner basis for I (provided that we choose $g_1, \ldots, g_s$ to be monic polynomials).

References

[1] W.W. Adams and P. Loustaunau, An Introduction to Grobner Bases, New York: AMS, 1994.

[2] S. Ballet and R. Rolland, "On low weight codewords of generalized affine and projective Reed-Muller codes," Des. Codes Cryptogr. **73**(2) (2014) 271–297.

[3] T. Becker and V. Weispfenning, Gröbner Bases - A computational approach to commutative algebra, Berlin, Germany: Springer Verlag, 1998, 2nd. pr.

[4] B. Buchberger, Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Mathematical Institute, University of Innsbruck, Austria. PhD Thesis. 1965. An English translation appeared in J. Symbolic Comput. 41 (2006) 475-511.

[5] B. Buchberger, A theoretical basis for the reduction of polynomials to canonical forms, SIGSAM Bull. (ACM Special Interest Group on Symbolic and Algebraic Manipulation) 10 (3), 19-29, (1976).

[6] C. Carvalho, "On the second Hamming weight of some Reed-Muller type codes," Finite Fields Appl. vol. 24, pp. 88-94, 2013.

[7] C. Carvalho, H. López and V.G.L. Neumann, "Projective Nested Cartesian Codes," Bull. Braz. Math. Soc. v. 48, pp. 283-302, 2017.

[8] C. Carvalho and V.G.L. Neumann, "On the next-to-minimal weight of affine cartesian codes," Finite Fields Appl. vol. 44, pp. 113-134, 2017.

[9] D. Cox, J. Little and D. O'Shea, Ideals, Varieties, and Algorithms, New York, NY: Springer, 3rd. ed., 2007.

[10] P. Delsarte, J. M. Goethals, and F. J. MacWilliams, "On generalized Reed-Muller codes and their relatives," Inform. Control, vol. 16, pp. 403-442, 1970.

[11] J. Fitzgerald and R.F. Lax, "Decoding affine variety codes using Göbner bases," Des. Codes and Cryptogr., vol. 13, pp. 147-158, 1998.

[12] O. Geil, "On the second weight of generalized Reed-Muller codes," Des. Codes Cryptogr., vol. 48, pp. 323-330, 2008.

[13] O. Geil and C. Thomsen, "Weighted Reed-Muller codes revisited," Des. Codes and Cryptogr., vol. 66, pp. 195-220, 2013.

[14] Hiram H. López, Carlos Rentería-Márquez and Rafael H. Villarreal, "Affine cartesian codes," Des. Codes Cryptogr., vol. 71, pp. 5-19, 2014.

[15] F.J. MacWilliams, and N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam, Netherlands: North-Holland, 1977.

[16] Teo Mora, Solving polynomial equation systems. II. Macaulay's paradigm and Gröbner technology. Encyclopedia of Mathematics and its Applications, 99. Cambridge University Press, Cambridge, 2005.

[17] A. Seidenberg, "Constructions in algebra," Trans. Amer. Math. Soc., vol. 197, pp. 273-313, 1974.

Faculdade de Matemática, Universidade Federal de Uberlândia, Av. J. N. Ávila 2121, 38.408-902 - Uberlândia - MG, Brazil.

E-mail address: `cicero@ufu.br`