On evaluation codes coming from a tower of function fields

Cícero Carvalho[a], María Chara[b,*], Luciane Quoos[c]

[a] *Universidade Federal de Uberlândia, Brazil*
[b] *Instituto de Matemática Aplicada del Litoral, FICH, (UNL-CONICET), Argentina*
[c] *Instituto de Matemática, Universidade Federal do Rio de Janeiro (UFRJ), Brazil*

Abstract

In this work we present the construction of evaluation codes defined from data coming from a tower of function fields. We use tools from from Gröbner basis theory to calculate the dimension and find a lower bound for the minimum distance of these codes.

Keywords: Towers of Function Fields, Codes, Gröbner basis
2010 MSC: 11G20, 94B05, 13P10

1. Introduction

Gröbner basis were introduced in 1965 by Bruno Buchberger in his Ph. D. thesis [4], to find a basis for the quotient ring $K[X_1, \ldots, X_n]/I$ as a K-vector space – here, I is an ideal of $K[X_1, \ldots, X_n]$. Since then, they have found a plethora of applications in commutative algebra and algebraic geometry. In this note we would like to show how to use them to find information on a given tower of function fields.

Let $\mathbb{F}_q$ be the finite field with q elements. A tower of function fields is a infinite chain of function fields of one variable $F_0 \subsetneqq F_1 \subsetneqq F_2 \subsetneqq \cdots$, defined over $\mathbb{F}_q$ (which we assume to be the full field of constants in the extension $F_i/\mathbb{F}_q$ for all $i \geq 0$), such that the extension F_{i+1}/F_i is finite and separable for all $i \geq 0$ and $g(F_i) \to \infty$ as $i \to \infty$, where $g(F_i)$ is the genus of the function field F_i. The systematic study of such towers was initiated by A. Garcia and H. Stichtenoth in mid 90's motivated by applications to coding theory. A common application of such study is to determine, for each $i \geq 0$ the number of rational places of

*Corresponding author
Email addresses: cicero@ufu.br (Cícero Carvalho), mchara@santafe-conicet.gov.ar (María Chara), luciane@im.ufrj.br (Luciane Quoos)

This work was partially done while the authors M. Chara and L. Quoos were visiting IMPA (Rio de Janeiro, Brazil) in Jan − Feb, 2013.
C. Carvalho was partially supported by CNPq and Fapemig (Proj. CEX APQ-01645-16)
M. Chara was partially supported by CONICET
L. Quoos was partially supported by CNPq (PDE grant number 200434/2015-2.)

F_i, and then apply Goppa's theory to produce codes, usually supported in one point (see e.g.[3, 10, 12]).

In our work we take another approach to produce codes from a tower of function fields. We work with recursive towers, meaning that $F_i = \mathbb{F}_q(x_0, \ldots, x_i)$ for $i \geq 0$ (hence $F_i = F_{i-1}(x_i)$ for $i > 0$) and there exists an irreducible polynomial in two variables $h \in \mathbb{F}_q[X, Y]$ such that $h(x_{i-1}, x_i) = 0$ for all $i > 0$. The ideal $I_i \subset \mathbb{F}_q[X_0, \ldots, X_i]$ generated by $h(X_0, X_1), \ldots, h(X_{i-1}, X_i)$ defines an affine curve $\mathcal{X}_i \subset \mathbb{A}^{i+1}(\mathbb{F}_q)$ for each $i > 0$. Fixing a non-negative integer d we produce an "affine variety code" (a type of code introduced by Fitzgerald and Lax in [8]) in the following way.

Let $i > 0$ and let $\{P_1, \ldots, P_m\}$ be pairwise distinct $\mathbb{F}_q$ rational points on the curve $\mathcal{X}_i$. Set

$$\widetilde{I}_i = I_i + \langle X_0^q - X_0, \ldots, X_i^q - X_i \rangle,$$

in [8, Section 1] (see also [5, Prop. 3.7]) it is shown that the evaluation morphism

$$\begin{array}{rcl} \varphi : \mathbb{F}_q[X_0, \ldots, X_i]/\widetilde{I}_i & \longrightarrow & \mathbb{F}_q^m \\ f + \widetilde{I}_i & \longmapsto & (f(P_1), \ldots, f(P_m)). \end{array}$$

is an isomorphism of $\mathbb{F}_q$ vector spaces, in particular $\widetilde{I}_i$ is the set of all polynomials in $\mathbb{F}_q[X_0, \ldots, X_i]$ vanishing on all points of $\mathcal{X}_i$. For an integer $d \geq 0$ let

$$L_i(d) := \{f + \widetilde{I}_i \mid f = 0 \text{ or } \deg(f) \leq d\},$$

clearly $L_i(d)$ is an $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q[X_0, \ldots, X_i]/\widetilde{I}_i$.

Definition 1.1. The image $\varphi(L_i(d)) =: C_i(d)$ is called the Reed-Muller type code of order d associated to I_i.

In what follows we want to determine the parameters of $C_i(d)$, for all $i > 0$ and all $d \geq 0$. We will do this by using tools coming from Gröbner bases theory. We use specially results on the so called footprint of an ideal. In the next section we present the concept of footprint and some basic results that will be needed throughout the paper. In Section 3 we work with a specific tower and show how to use Gröbner basis techniques to find the number of points of the affine curve $\mathcal{X}_i$, for $i \geq 0$, which is the length of code defined above. The same techniques are used to calculate the dimension of the code and obtain a lower bound for its minimum distance.

2. Tools from Gröbner bases theory

Let K be a field and let $\preceq$ be a monomial order defined on the set $\mathcal{M}$ of monomials of the polynomial ring $K[X_1, \ldots, X_n]$, i.e. $\preceq$ is a total order on $\mathcal{M}$, $1 \preceq M$ for any monomial M, and if $M_1 \preceq M_2$ then $MM_1 \preceq MM_2$ for all $M \in \mathcal{M}$. The largest monomial in a non-zero polynomial f is called the *leading monomial* of f and is denoted by $\mathrm{lm}(f)$.

Definition 2.1. Let I be an ideal of $K[X_1, \ldots, X_n]$. 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 $\mathrm{lm}(f)$ is a multiple of $\mathrm{lm}(g_i)$ for some $i \in \{1, \ldots, s\}$.

In [4] Buchberger proved that any ideal has a Gröbner basis (with respect to fixed monomial order) presenting what is now called Buchberger's algorithm, which starts from any given basis of the ideal and enlarges it to produce a Gröbner basis. It is not difficult to prove, using the division algorithm in $K[X_1, \ldots, X_n]$, that if $\{g_1, \ldots, g_s\}$ is a Gröbner basis for I then $I = \langle g_1, \ldots, g_s \rangle$. An important related concept is that of the footprint, which we now present.

Definition 2.2. Let I be an ideal of $K[X_1, \ldots, X_n]$. The *footprint* of I (w.r.t. $\preceq$) is the set $\Delta(I)$ of monomials which do not appear as leading monomial of any non-zero polynomial of I.

Again, using the division algorithm in $K[X_1, \ldots, X_n]$, one may prove the following result (see e.g. [5, Prop. 2.12]).

Proposition 2.3. Let $I \subset K[X_1, \ldots, X_n]$ 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 $\mathrm{lm}(g_i)$ for all $i = 1, \ldots, s$.

The following result was proved by Buchberger in his thesis, and is one of the main properties of the footprint (see e.g. [2, Prop. 6.52]).

Theorem 2.4. Let I be an ideal of $K[X_1, \ldots, X_n]$ and let $\Delta(I)$ be its footprint with respect to some fixed monomial order. Then the set $\{M + I \mid M \in \Delta(I)\}$ is a basis for $K[X_1, \ldots, X_n]/I$ as a K-vector space.

In the next section we will deal with ideals which have a finite number of monomials in the footprint, i.e. ideals I such that the dimension, as a K-vector space, of $K[X_1, \ldots, X_n]/I$ is finite. These are called zero-dimensional ideals, see e.g. [2, Section 6.3] for properties of these ideals. The next result shows that if the footprint of an ideal is a finite set then the set of common zeros of the polynomials in the ideal (i.e. the affine variety $V_K(I)$ associated to I) also has a finite number of elements.

Proposition 2.5. Let I be an ideal of $K[X_1, \ldots, X_n]$, let $V_K(I)$ be the affine variety associated to I and and let $\Delta(I)$ be its footprint with respect to some fixed monomial order. If $\Delta(I)$ is a finite set then $V_K(I)$ is a finite set and $\#(V_K(I)) \leq \#(\Delta(I))$.

Proof. Let $P_1, \ldots, P_m$ be distinct points of $V_K(I)$ and consider the evaluation morphism $\varphi : K[X_1, \ldots, X_n]/I \to K^m$ given by $\varphi(f + I) = (f(P_1), \ldots, f(P_m))$. Working with the entries of $P_1, \ldots, P_m$ it is not difficult to find polynomials $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ such that $f_i(P_j) = \delta_{ij}$ for all $i, j \in \{1, \ldots, m\}$. Hence ϕ is a surjective K-linear transformation and we have

$$m \leq \dim_K(K[X_1, \ldots, X_n]/I) = \#(\Delta(I)),$$

which concludes the proof. □

In [2, Theorem 8.32] we find the following more refined result, which we will need.

Theorem 2.6. Let K be a field and let $I \subseteq K[X_1, \ldots, X_n]$ be an ideal. Assume that $\Delta(I)$ is a finite set, and let L be an algebraically closed extension field of K. Then the number of zeros of I in L^n is less than or equal to $\#(\Delta(I))$. If K is perfect and I is a radical ideal, then equality holds.

3. The number of points in curves associated to a function field tower

In this section we use the footprints of some specific ideals to obtain lower bounds for the number of points in curves defined by ideals associated to the function fields in a tower.

Proposition 3.1. Let $\mathbb{F}_q$ be a finite field with q elements, let $I \subseteq \mathbb{F}_q[X_1, \ldots, X_n]$ be an ideal and consider $\widetilde{I} = I + \langle X_1^q - X_1, \ldots, X_n^q - X_n \rangle$. Let $\preceq$ be any monomial ordering on $\mathcal{M}$ and let $\mathbb{V}_{\mathbb{F}_q}(I)$ denote the affine variety associated to I. Then the footprint $\Delta(\widetilde{I})$ is finite and $\#(\mathbb{V}_{\mathbb{F}_q}(I)) = \#(\Delta(\widetilde{I}))$.

Proof. Let $i \in \{1, \ldots n\}$. From the definition of monomial order we get that $\mathrm{lm}(X_i^q - X_i) = X_i^q$ and from the definition of Gröbner basis we get that some polynomial of such a basis must have $X_i^{\alpha_i}$ as leading monomial, with $1 \leq \alpha_i \leq q$ for all $i = 1, \ldots, n$. This shows that $\Delta(\widetilde{I})$ is finite (and has at most $\alpha_1 . \cdots . \alpha_n$ elements). Moreover $\widetilde{I}$ is a radical ideal because for each $i \in \{1, \ldots, n\}$, it contains a polynomial in X_i which has only simple roots (see [2, Lemma 8.13]). Let L be an algebraic closure of $\mathbb{F}_q$. From Theorem 2.6 we get that the number of zeros of $\widetilde{I}$ in L^n is equal to $\#(\Delta(\widetilde{I}))$ and from the definition of $\widetilde{I}$ we see that this number of zeros is also equal to $\#(\mathbb{V}_{\mathbb{F}_q}(I))$. □

In the following theorem we compute the number of points in a family of algebraic curves defined by a recursive tower of functions fields considered in [6, Proposition 4.1].

Theorem 3.2. Let $\mathcal{F} = (F_0, F_1, \ldots)$ be the tower of function fields over $\mathbb{F}_5$ defined by $F_0 = \mathbb{F}_5(x_0)$, where x_0 is a transcendental element over $\mathbb{F}_5$, and $F_i = F_{i-1}(x_i)$ satisfies

$$x_i^2 = \frac{x_{i-1}^2 - x_{i-1} + 1}{x_{i-1}}, \qquad \text{for } i > 0.$$

Let $h(X, Y) = XY^2 - X^2 + X - 1$,

$$I_i = \langle h(X_0, X_1), \ldots, h(X_{i-1}, X_i) \rangle \subset \mathbb{F}_5[X_0, \ldots, X_i].$$

and let $\mathcal{X}_i \subset \mathbb{A}^{i+1}(\mathbb{F}_5)$ be the curve defined by I_i, $i > 0$. Then the number of points of $\mathcal{X}_i$ is $N(\mathcal{X}_i) = 2^{i+1} + 2$, for all $i > 0$.

Proof. Let i be a positive integer and

$$I_i = \langle X_0X_1^2 - X_0^2 + X_0 - 1, \ldots, X_{i-1}X_i^2 - X_{i-1}^2 + X_{i-1} - 1\rangle.$$

As we mentioned in the introduction, from [8, Section 1] or [5, Prop. 3.7] we get that the ideal formed by the polynomials which vanish in all points of $\mathcal{X}_i$ is

$$\widetilde{I}_i = I_i + \langle X_0^q - X_0, \ldots, X_i^q - X_i\rangle.$$

It is easy to check that if $(a_0, \ldots, a_i) \in \mathcal{X}_i$ then $a_j \neq 0$ for all $j = 0, \ldots, i$, so we must have that

$$\langle X_0X_1^2 - X_0^2 + X_0 - 1, \ldots, X_{i-1}X_i^2 - X_{i-1}^2 + X_{i-1} - 1, X_0^4 - 1, \ldots, X_i^4 - 1\rangle \subset \widetilde{I}_i$$

and a fortiori we get

$$\widetilde{I}_i = \langle X_0X_1^2 - X_0^2 + X_0 - 1, \ldots, X_{i-1}X_i^2 - X_{i-1}^2 + X_{i-1} - 1, X_0^4 - 1, \ldots, X_i^4 - 1\rangle.$$

We want to show that

$$G_i = \{X_jX_i^2 - X_i^2 + X_j - 1 \mid j = 0, \ldots, i-1\} \cup \{X_j^2 - X_i^2 | j = 0, \ldots, i-1\} \cup \{X_i^4 - 1\}$$

is a Gröbner basis for $\widetilde{I}_i$ with respect to the graded lexicographic order $\succ$ in $\mathbb{F}_5[X_0, \ldots, X_i]$, where $X_0 \succ \cdots \succ X_i$; and we start by proving that the ideal $\langle G_i\rangle$ generated by G_i is equal to $\widetilde{I}_i$. Let $j \in \{0, \ldots, i-1\}$, then

$$X_jX_{j+1}^2 - X_j^2 + X_j - 1 = X_j(X_{j+1}^2 - X_i^2) - (X_j^2 - X_i^2) + X_jX_i^2 - X_i^2 + X_j - 1 \in \langle G_i\rangle,$$

and

$$X_j^4 - 1 = (X_j^2 + X_i^2)(X_j^2 - X_i^2) + X_i^4 - 1 \in \langle G_i\rangle,$$

so that $\widetilde{I}_i \subset \langle G_i\rangle$. On the other hand, for all $j \in \{0, \ldots, i-1\}$ we have

$$\begin{aligned} X_j^2 - X_{j+1}^2 = {} & (3X_jX_{j+1}^2 + 3X_j^2 + X_{j+1}^2 + 3X_j + 2)(X_jX_{j+1}^2 - X_j^2 + X_j - 1) \\ & + 3(X_j^4 - 1) - (3X_j^2 + X_j)(X_{j+1}^4 - 1) \end{aligned}$$

which implies that for all $j \in \{0, \ldots, i-1\}$ we have $X_j^2 - X_i^2 \in \widetilde{I}_i$. Also, for any $j \in \{0, \ldots, i-1\}$ we get

$$X_jX_i^2 - X_i^2 + X_j - 1 = X_jX_{j+1}^2 - X_j^2 + X_j - 1 - X_j(X_{j+1}^2 - X_i^2) + (X_j^2 - X_i^2) \in \widetilde{I}_i.$$

Hence $\langle G_i\rangle = \widetilde{I}_i$.

We will now prove that G_i is a Gröbner basis for $\widetilde{I}_i$, and we only need to calculate the S-polynomial of polynomials in G_i whose leading monomials are not coprime (see [7, Prop. 4, p. 104]). Let $r, s \in \{0, \ldots, i-1\}$ be distinct integers. The leading monomials of $X_rX_i^2 - X_i^2 + X_r - 1$ and $X_sX_i^2 - X_i^2 + X_s - 1$ are, respectively, $X_rX_i^2$ and $X_sX_i^2$. Hence they are not coprime, and

$$\begin{aligned} S(X_rX_i^2 - X_i^2 + X_r - 1, X_sX_i^2 - X_i^2 + X_s - 1) = {} & X_rX_i^2 - X_sX_i^2 + X_r - X_s = \\ & (X_rX_i^2 - X_i^2 + X_r - 1) - (X_sX_i^2 - X_i^2 + X_s - 1). \end{aligned}$$

Also for any $j \in \{0, \ldots, i-1\}$ we have

$$\begin{aligned} S(X_j X_i^2 - X_i^2 + X_j - 1, X_i^4 - 1) &= -X_i^4 + X_j X_i^2 - X_i^2 + X_j \\ &= (X_j X_i^2 - X_i^2 + X_j - 1) - (X_i^4 - 1) \end{aligned}$$

and

$$\begin{aligned} S(X_j X_i^2 - X_i^2 + X_j - 1, X_j^2 - X_i^2) &= X_i^4 - X_j X_i^2 + X_j^2 - X_j \\ &= (X_j^2 - X_i^2) + (X_i^4 - 1) \\ &\quad - (X_j X_i^2 - X_i^2 + X_j - 1). \end{aligned}$$

Thus all S-polynomials reduce to zero modulo G_i (see [7, Def. 1, page 103]) which concludes the proof that G_i is a Gröbner basis for $\widetilde{I}_i$ with respect to the order $\succ$ defined above. Thus the set of leading monomials of G_i is

$$\{X_j X_i^2, X_j^2 \,|\, j = 0, \ldots, i-1\} \cup \{X_i^4\},$$

and from Proposition 2.3 we get that

$$\Delta(\widetilde{I}_i) = \{X_0^{\alpha_0} X_1^{\alpha_1} \ldots X_i^{\alpha_i} \mid \alpha_j = 0, 1 \text{ for } j = 0, 1, \ldots, i\} \cup \{X_i^2, X_i^3\}.$$

Hence $\#(\Delta(\widetilde{I}_i)) = 2^{i+1} + 2$ and from the above proposition we get

$$N(\mathcal{X}_i) = 2^{i+1} + 2.$$

□

In the next result we calculate the parameters of the code $C_i(d)$ associated to the tower presented in Theorem 3.2.

Theorem 3.3. For $i \geq 1$, let $\mathcal{F}$ and I_i be as in Theorem 3.2. Let d be a non-negative integer and $C_i(d)$ be the Reed-Muller type code of order d associated to I_i. Then the length of $C_i(d)$ is $2^{i+1} + 2$, and the dimension of $C_i(d)$ is:

$$\dim C_i(d) = \begin{cases} 1 & \text{if } d = 0; \\ i + 2 & \text{if } d = 1; \\ 3 + \dfrac{i(i+3)}{2} & \text{if } d = 2; \\ 3 + \binom{i+1}{1} + \cdots + \binom{i+1}{d} & \text{if } 3 \leq d \leq i+1 \text{ and } i \geq 2; \\ 2^{i+1} + 2 & \text{if } d \geq i+1 \text{ and } i \geq 2, \text{ or} \\ & \quad d \geq 3 \text{ and } i = 1. \end{cases}$$

As for the minimum distance $\delta_i(d)$ of $C_i(d)$ we have that $\delta_i(0) = 2^{i+1} + 2$, $\delta_i(d) = 1$, if $i \geq 2$ and $d \geq i+1$, or $i = 1$ and $d \geq 3$, and $\delta_i(d) \geq 2^{i+1-d}$ if $4 \leq d \leq i+1$.

Proof. Recall that the evaluation homomorphism

$$\varphi : \mathbb{F}_5[X_0, \ldots, X_n]/\widetilde{I}_i \to \mathbb{F}_5^{2^{i+1}+2}$$

is an isomorphism and that the classes of the monomials in

$$\Delta(\widetilde{I}_i) = \{X_0^{\alpha_0} X_1^{\alpha_1} \ldots X_i^{\alpha_i} \mid \alpha_j = 0, 1 \text{ for } j = 0, 1, \ldots, i\} \cup \{X_i^2, X_i^3\},$$

form a basis for the quotient $\mathbb{F}_5[X_0, \ldots, X_i]/\widetilde{I}_i$. Hence, if $i \geq 2$ and $d \geq i+1$, or $i = 1$ and $d \geq 3$, then the classes of all monomials in $\Delta(\widetilde{I}_i)$ are in $L_i(d)$ so $C_i(d) = \mathbb{F}_5^{2^{i+1}+2}$, $\dim C_i(d) = 2^{i+1} + 2$ and $\delta_i(d) = 1$.

If $d = 0$ clearly $\dim C_i(0) = 1$ and hence $\delta_i(0) = 2^{i+1}+2$. On the other hand the elements of $\Delta(\widetilde{I}_i)$ with degree up to 1 are $\{1, X_0, \ldots, X_i\}$ so $\dim C_i(1) = i+2$, and the number of elements in $\Delta(\widetilde{I}_i)$ of degree up to 2 is

$$\dim C_i(2) = i + 2 + \binom{i+1}{2} + 1 = 3 + \frac{i(i+3)}{2}.$$

If $i \geq 2$ and $3 \leq d \leq i+1$, then counting the number of monomials in $\Delta(\widetilde{I}_i)$ with degree at most d we get

$$\dim C_i(d) = 1 + \binom{i+1}{1} + \cdots + \binom{i+1}{d} + 2.$$

Now we want to determine a lower bound for the minimum distance of $C_i(d)$ when $4 \leq d \leq i+1$. Thus let $f \in \mathbb{F}_5[X_0, \ldots, X_i]$ be a polynomial of degree $d' \leq d$ and let $P_1, \ldots, P_{2^{i+1}+2}$ be the points of $\mathcal{X}_i$, we want to find an upper bound the number of zero entries in $\varphi(f + \widetilde{I}_i) = (f(P_1), \ldots, f(P_{2^{i+1}+2}))$. Clearly, if $g = (X_0 - 1)^{d-d'} f$ then $\varphi(g + \widetilde{I}_i)$ has at least as many zero entries than $\varphi(f + \widetilde{I}_i)$, so we may assume that the degree of f is d. Also, since the classes of the monomials in $\Delta(\widetilde{I}_i)$ form a basis for the quotient $\mathbb{F}_5[X_0, \ldots, X_i]/\widetilde{I}_i$, we may assume that f is an $\mathbb{F}_5$-linear combination of monomials in $\Delta(\widetilde{I}_i)$ having degree at most d. The number of zero entries in $\varphi(f + \widetilde{I}_i)$ is equal to the number of points in the variety $V(J_i)$ where $J_i = \widetilde{I}_i + \langle f \rangle$, and from Proposition 2.5 we have $\#(V(J_i)) \leq \#(\Delta(J_i))$. From the definition of footprint we get that an upper bound for $\#(\Delta(J_i))$ is the number of monomials in $\mathbb{F}_5[X_0, \ldots, X_i]$ which are not multiples of any of the leading monomials of the generators of $\widetilde{I}_i$ or f, and this set is equal to the set of monomials in $\Delta(\widetilde{I}_i)$ which are not multiples of the leading monomial of f, i.e.

$$\#(\Delta(J_i)) \leq \#(\{M \in \Delta(\widetilde{I}_i) \mid \mathrm{lm}(f) \nmid M\}).$$

Since $\#(\Delta(\widetilde{I}_i)) = 2^{i+1} + 2$ we get

$$\#(\{M \in \Delta(\widetilde{I}_i) \mid \mathrm{lm}(f) \nmid M\}) = 2^{i+1} + 2 - \#(\{M \in \Delta(\widetilde{I}_i) \mid \mathrm{lm}(f) \mid M\})$$

so we look for the set of monomials in $\Delta(\widetilde{I}_i)$ which are multiple of $\mathrm{lm}(f)$. If $4 \leq \deg(f) \leq i+1$ then the leading monomial of f is a product of d distinct

elements in the set $\{X_0, \ldots, X_i\}$ (recall that f is an $\mathbb{F}_5$-linear combination of monomials in $\Delta(\widetilde{I}_i)$), so

$$\#(\{M \in \Delta(\widetilde{I}_i) \mid \mathrm{lm}(f) \mid M\}) = 1 + \binom{i+1-d}{1} + \cdots + \binom{i+1-d}{i+1-d} = 2^{i+1-d}.$$

Denoting the number of non-zero entries in $\varphi(f + \widetilde{I}_i)$ by $w_i(f)$ and collecting the above results, we get

$$\begin{aligned} w_i(f) &= 2^{i+1} + 2 - \#(V(J_i)) \geq 2^{i+1} + 2 - \#(\Delta(J_i)) \\ &\geq 2^{i+1} + 2 - \#(\{M \in \Delta(\widetilde{I}_i) \mid \mathrm{lm}(f) \nmid M\}) \\ &= 2^{i+1} + 2 - (2^{i+1} + 2 - 2^{i+1-d}) = 2^{i+1-d} \end{aligned}$$

which proves that $\delta_i(d) \geq 2^{i+1-d}$ for the case where $4 \leq d \leq i+1$. □

A similar reasoning to find a lower bound for the minimum distance has already been used in [9]. Also, in [1] we find Gröbner basis methods applied to the determination of lower bounds for the generalized Hamming weights.

The generalized Reed-Muller code $\mathrm{GRM}(d, n)$, in n variables and order d defined over $\mathbb{F}_q$, is obtained by evaluating all polynomials of degree up to d (together with the zero polynomial) in all points of $\mathbb{A}^n(\mathbb{F}_q)$, so it is a code of length $q^n - 1$. Formulas for its dimension and minimum distance are well known (see e.g. [11, Thm. 15.1.201] or [5, Thm. 3.14, Thm. 3.16]), and to compare the codes constructed above to the generalized Reed-Muller codes defined over $\mathbb{F}_5$ we choose codes with approximately the same dimension and compare the relative parameters.

Code	dimension	length	minimum distance	dim./len.	min. dist./len.
$C_{11}(6)$	2512	4098	≥ 64	0,612	$\geq 0,0156$
$\mathrm{GRM}(8,6)$	2499	15624	624	0,159	0,04
$C_{10}(5)$	1026	2050	≥ 64	0,501	$\geq 0,0312$
$\mathrm{GRM}(8,5)$	1007	3124	124	0,3223	0,04
$C_{11}(8)$	3799	4098	≥ 16	0,927	$\geq 0,004$
$\mathrm{GRM}(9,6)$	3745	15624	499	0,239	0,032

We see that the codes we constructed pack more information in a shorter length than the generalized Reed-Muller codes, and as a consequence have a lesser number for the relative minimum distance.

References

[1] H.E. Andersen, O. Geil, *Evaluation Codes from order domain Theory*, Finite Fields Appl. 14 (1) (2008), 92–123.

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

[3] I. Blake, C. Heegard, T. Høholdt, V. Wei, *Algebraic-geometry codes. Information theory: 1948–1998*, IEEE Trans. Inform. Theory 44(6) (1998), 2596–2618.

[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] C. Carvalho, *Gröbner bases methods in coding theory*, Contemp. Math. 642 (2015) 73–86.

[6] M. Chara, R. Toledano *Rational places in extensions and sequences of function fields of Kummer type*, J. of Pure and Applied Algebra, 215, (2011), 2603–2614

[7] D.A. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 3rd. ed. Springer, 2007.

[8] J. Fitzgerald, R.F. Lax, *Decoding affine variety codes using Göbner bases*, Des. Codes and Cryptogr. 13(2) (1998) 147–158.

[9] O. Geil, *Evaluation Codes from an Affine Variety Code Perspective*, in Advances in Algebraic Geometry Codes, ed. E.M.Moro, C. Munuera and DṘuano. World Scientific Publishing (Coding Theory and Cryptology, Vol. 5) 153–181, 2008

[10] T. Hasegawa, S. Kondo, H. Kurusu, *A sequence of one-point codes from a tower of function fields*, Des. Codes Cryptogr. 41(3) (2006), 251–267.

[11] G.L. Mullen, D. Panario, *Handbook of Finite Fields*, CRC Press, 2013.

[12] C. Voss, T. Høholdt, *An explicit construction of a sequence of codes attaining the Tsfasman-Vlăduţ-Zink bound: the first steps*, IEEE Trans. Inform. Theory 43(1) (1997), 128–135.

Cícero Carvalho majored in Physics (1980) and Mathematics (1981) from Universidade Federal do Rio de Janeiro, Brazil. He received his Ph.D. in Mathematics in 1994, from IMPA, at Rio de Janeiro. From 1996 to 1998 he was a postdoctoral researcher at Harvard University. Since 1986 he is with Universidade Federal de Uberlândia, in Brazil, where currently he is full professor. His research interests include the study of curves over finite fields and coding theory.

Figure 1: Cícero Carvalho

María Chara received a Ph.D. in Mathematics from Universidad Nacional del Litoral (UNL) in 2012, in Argentina. Since 2016 she is an Assistant Researcher of Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET) at Instituto de Matemática Aplicada del Litoral (IMAL). She has been teaching at Universidad Nacional del Litoral since 2011, where she is currently an Assistant Professor. Her research interests include algebraic function fields over finite fields, towers of function fields and algebraic geometric codes.

Figure 2: María Chara

Luciane Quoos received a B.Sc. in mathematics from Universidade Federal do Rio Grande do Sul in 1993, and her M.Sc. and Ph.D. in mathematics from Instituto Nacional de Matemática Pura e Aplicada (IMPA) in 1995 and 2000, respectively, both in Brazil. In 1998 she joined the Departamento de Matemática Pura at the Universidade Federal do Rio de Janeiro where she is currently an Associate Professor. During a nine month period, starting in August 2002, she held an ERCIM (European Research Consortium for Informatics and Mathematics)

postdoctoral fellowship at the Norwegian University of Science and Technology. In 2016 she spent her sabbatical at the Università degli Studi di Perugia, Italy. Her research interests include maximal curves and curves with many rational points over finite fields, Weierstrass semigroups, towers of function fields and algebraic geometric codes.

Figure 3: Luciane Quoos