Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

On evaluation codes coming from a tower of function fields ☆

Cícero Carvalho [a,1], María Chara [b,2], Luciane Quoos [c,3]

[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

ARTICLE INFO

Article history:
Received 10 February 2017
Accepted 3 October 2017
Available online xxxx

MSC:
11G20
94B05
13P10

Keywords:
Towers of function fields
Codes
Gröbner basis

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 Gröbner basis theory to calculate the dimension and find a lower bound for the minimum distance of these codes.

1. Introduction

Gröbner bases were introduced in 1965 by Bruno Buchberger in his PhD thesis (Buchberger, 1965), 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

☆ This work was partially done while the authors M. Chara and L. Quoos were visiting IMPA (Rio de Janeiro, Brazil) in January–February, 2013.

E-mail addresses: cicero@ufu.br (C. Carvalho), mchara@santafe-conicet.gov.ar (M. Chara), luciane@im.ufrj.br (L. Quoos).

[1] C. Carvalho was partially supported by CNPq and Fapemig (Proj. CEX APQ-01645-16).
[2] M. Chara was partially supported by CONICET.
[3] L. Quoos was partially supported by CNPq (PDE grant number 200434/2015-2).

https://doi.org/10.1016/j.jsc.2017.11.008
0747-7171/

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 an 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 F_i, and then apply Goppa's theory to produce codes, usually supported in one point (see e.g. Blake et al., 1998; Hasegawa et al., 2006; Voss and Høholdt, 1997).

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, 1998) 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 Fitzgerald and Lax (1998, Section 1) (see also Carvalho, 2015, Prop. 3.7) it is shown that the evaluation morphism

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

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 $i \in \{1, \ldots, s\}$.

Please cite this article in press as: Carvalho, C., et al. On evaluation codes coming from a tower of function fields. J. Symb. Comput. (2017), https://doi.org/10.1016/j.jsc.2017.11.008