J. Algebra Comb. Discrete Appl.
5(2) • 71–83

Received: 18 October 2017
Accepted: 9 March 2018

Journal of Algebra Combinatorics Discrete Structures and Applications

The root diagram for one-point AG codes arising from certain curves with separated variables

Research Article

Federico Fornasiero, **Guilherme Tizziotti**

Abstract: Heegard, Little and Saints introduced in [8] an encoding algorithm for a class of AG codes via Gröbner basis more compact compared with the usual encoding via generator matrix. So, knowing that the main drawback of Gröbner basis is the high computational cost required for its calculation, in [12], the same authors introduced the concept of root diagram that allows the construction of an algorithm for computing a Gröbner basis with a lower complexity for one-point Hermitian codes. In [4], Farrán, Munuera, Tizziotti and Torres extended the results obtained in [12] for codes on norm-trace curves. In this work we generalize these results by constructing the root diagram for codes arising from certain curves with separated variables that has certain special automorphism and a Weierstrass semigroup generated by two elements. Such family of curves includes the norm-trace curve, among other curves with recent applications in coding theory.

2010 MSC: 11T71, 13P10

Keywords: AG codes, Gröbner basis, Root diagram

1. Introduction

In the early 1980s, V.D. Goppa constructed error-correcting codes using algebraic curves, the called *algebraic geometric codes* (AG codes), see [6] and [7]. The introduction of methods from algebraic geometry to construct good linear codes was one of the major developments in the theory of error-correcting codes. From that moment many studies and applications on this theory have emerged. In [8], Little, Saints and Heegard noted that any linear code with a nontrivial automorphism has the structure of a module over a polynomial ring and so that the theory of Gröbner bases for modules gives a compact description and implementation of a systematic encoder, which is similar to the usual one for cyclic codes. This encoding method is efficient and also interesting from a theoretical point of view. It is known that

Federico Fornasiero; Department of Mathematics, Universidade Federal de Pernambuco, Brazil (email: federico@dmat.ufpe.br).
Guilherme Tizziotti (Corresponding Author); Department of Mathematics, Universidade Federal de Uberlândia, Brazil (email: guilhermect@ufu.br).

http://dx.doi.org/10.13069/jacodesmath.423733 ISSN 2148-838X

the main drawback of Gröbner basis is the high computational cost required for its calculation. Indeed, it is well known that the complexity of computing a Gröbner basis is doubly exponential in general. But, in [12], using an appropriate automorphism of the Hermitian curve, Little et al. introduced the concept of *root diagram* that allows construction of an algorithm for computing a Gröbner basis with a lower complexity for one-point Hermitian codes. In other words, the root diagram is the key to the construction of the algorithm given in [12, Proposition 4.4]. In [4], the results of [12] were extended to codes arising from the norm-trace curve, which is a generalization of the Hermitian curve. In this work, using the same techniques used in [12] and [4], we will construct the root diagram for codes arising from certain curves, which we will denote by $\mathcal{X}^\star$, with separated variables that has certain special automorphism and a Weierstrass semigroup generated by two elements (see (1), (2) and (3) in Section 3). In addition to Hermitian and norm-trace curves, we have important examples of such curves $\mathcal{X}^\star$ with recent applications in coding theory, namely: the maximal curve with plane model $y^q + y = x^{q^r+1}$, see [11]; a quotient of the Hermitian curve with plane model $y^q + y = x^m$, see [13]; and curves on Kummer extensions, see [2].

This paper is organized as follows. In Section 2 we recall some background on Gröbner basis for modules, AG codes and root diagram. In Section 3 we present a way to construct the root diagram for one-point AG codes C arising from $\mathcal{X}^\star$. Finally, in Section 4 we present examples of those curves and the necessary information to construct the root diagram studied in the previous section.

2. Background

We will denote a finite field with q elements by $\mathbb{F}_q$. Let $\mathcal{X}$ be a projective, non-singular, geometrically irreducible algebraic curve of genus $g > 0$ over $\mathbb{F}_q$; throughout the paper we will refer to this simply as *curve*. If $\sharp\mathcal{X}(\mathbb{F}_q)$ is the number of $\mathbb{F}_q$-rational points on $\mathcal{X}$, then $\sharp\mathcal{X}(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$. This inequality is so-called *Hasse-Weil bound* and if $\sharp\mathcal{X}(\mathbb{F}_q) = q + 1 + 2g\sqrt{q}$ the curve $\mathcal{X}$ is called a *maximal curve*.

Let $\mathbb{F}_q(\mathcal{X})$ be the field of rational functions on $\mathcal{X}$. For a $\mathbb{F}_q$-rational point P on $\mathcal{X}$ let

$$H(P) := \{n \in \mathbb{N}_0 \ ; \ \exists f \in \mathbb{F}_q(\mathcal{X}) \text{ with } \mathrm{div}_\infty(f) = nP\},$$

where $\mathbb{N}_0$ is the set of nonnegative integers and $\mathrm{div}_\infty(f)$ denotes the divisor of poles of f. The set $H(P)$ is a numerical semigroup, called *Weierstrass semigroup* of $\mathcal{X}$ at P and its complement $G(P) = \mathbb{N}_0 \setminus H(P)$ is called *Weierstrass gap set* of P. As an important result, the cardinality of the set $G(P)$ is equal to genus g of $\mathcal{X}$, see Theorem 1.6.8 in [15].

2.1. Gröbner basis for $\mathbb{F}_q[t]$-modules

We will introduce some notations about Gröbner basis for $\mathbb{F}_q[t]$-modules that are needed later. For a complete treatment on this topic see [1] and [3]. A *monomial* $\mathbf{m}$ in the free $\mathbb{F}_q[t]$-module $\mathbb{F}_q[t]^r$ is an element of the form $\mathbf{m} = t^i\mathbf{e}_j$, where $i \geq 0$ and $\mathbf{e}_1, \ldots, \mathbf{e}_r$ is the standard basis of $\mathbb{F}_q[t]^r$. Fixed a monomial ordering, for all element $\mathbf{f} \in \mathbb{F}_q[t]^r$, with $\mathbf{f} \neq 0$, we may write $\mathbf{f} = a_1\mathbf{m}_1 + \cdots + a_\ell\mathbf{m}_\ell$, where, for $1 \leq i \leq \ell$, $0 \neq a_i \in \mathbb{F}_q$ and $\mathbf{m}_i$ is a monomial in $\mathbb{F}_q[t]^r$ satisfying $\mathbf{m}_1 > \mathbf{m}_2 > \ldots > \mathbf{m}_\ell$. The term $a_1\mathbf{m}_1$ is called *leading term* of $\mathbf{f}$ and denoted by $LT(\mathbf{f})$, the coefficient a_1 and the monomial $\mathbf{m}_1$ are called *leading coefficient*, $LC(\mathbf{f})$, and *leading monomial*, $LM(\mathbf{f})$, respectively. A *Gröbner basis* for a submodule $M \subseteq \mathbb{F}_q[t]^r$ is a set $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_s\}$ such that $\{LT(\mathbf{g}_1), \ldots, LT(\mathbf{g}_s)\}$ generates the submodule $LT(M)$ formed by the leading terms of all elements in M. The monomials in $LT(M)$ are called *nonstandard* while those in the complement of $LT(M)$ are the *standard monomials* for M. We recall that every submodule $M \subseteq \mathbb{F}_q[t]^n$ has a Gröbner basis $\mathcal{G}$, which induces a division algorithm: given $\mathbf{f} \in \mathbb{F}_q[t]^r$ there exist $\mathbf{a}_1, \ldots, \mathbf{a}_s, \mathbf{R}_\mathcal{G} \in \mathbb{F}_q[t]^r$ such that $\mathbf{f} = \mathbf{a}_1\mathbf{g}_1 + \ldots + \mathbf{a}s\mathbf{g}_s + \mathbf{R}_\mathcal{G}$ (see [1, Algorithm 1.5.1] or [3, Theorem 3]).

In this work we will use the POT (position over term) ordering over $\mathbb{F}_q[t]^r$ which is defined as follows. Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_r\}$ be the standard basis in $\mathbb{F}_q[t]^r$, with $\mathbf{e}_1 > \ldots > \mathbf{e}_r$. The POT ordering on $\mathbb{F}_q[t]^r$ is defined

by

$$t^i\mathbf{e}_j > t^k\mathbf{e}_\ell$$

if $j < \ell$, or $j = \ell$ and $i > k$.

We say that $\mathbf{f} \in \mathbb{F}_q[t]^r$ is *reduced* with respect to a set $P = \{\mathbf{p}_1, \ldots, \mathbf{p}_l\}$ of non-zero elements in $\mathbb{F}_q[t]^r$ if $\mathbf{f} = \mathbf{0}$ or no monomial in $\mathbf{f}$ is divisible by a $LM(\mathbf{p}_i)$, $i = 1, \ldots, l$. A Gröbner basis $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_s\}$ is *reduced* if $\mathbf{g}_i$ is reduced with respect to $\mathcal{G} - \{\mathbf{g}_i\}$ and $LC(\mathbf{g}_i) = 1$ for all i, and *non-reduced* otherwise. Every submodule of $\mathbb{F}_q[t]^r$ has a unique reduced Gröbner basis (see [1], Theorem 3.5.22).

2.2. Linking AG codes and $\mathbb{F}_q[t]$-modules

Let $P_1, \ldots, P_n, Q_1, \ldots, Q_\ell$ be $n + \ell$ distinct $\mathbb{F}_q$-rational points on $\mathcal{X}$ and let $m_1, \ldots, m_\ell$ be integers. Consider the divisors $D = P_1 + \cdots + P_n$ and $G = m_1Q_1 + \cdots + m_\ell Q_\ell$. The *algebraic geometry code* (AG code) $C_{\mathcal{X}}(D, G)$ arising from the curve $\mathcal{X}$ is defined as

$$C_{\mathcal{X}}(D, G) := \{(f(P_1), \ldots, f(P_n)) \in \mathbb{F}_q^n : f \in \mathcal{L}(G)\}, \tag{1}$$

where $\mathcal{L}(G)$ is the space of rational functions f on $\mathcal{X}$ such that $f = 0$ or $\mathrm{div}(f) + G \geq 0$, where $\mathrm{div}(f)$ denote the (principal) divisor of the function $f \in \mathcal{L}(G)$. The number n is the length of $C_{\mathcal{X}}(D, G)$, and the dimension of $C_{\mathcal{X}}(D, G)$ is its dimension as an $\mathbb{F}_q$-vector space, which is generally denoted by $\dim(C_{\mathcal{X}}(D, \lambda P)) := k$. The elements in $C_{\mathcal{X}}(D, G)$ are called *codewords*. If $G = m_1Q_1$ the AG code $C_{\mathcal{X}}(D, m_1Q_1)$ is called *one-point AG code*. For more details about AG codes, see e.g. [10].

Let $\mathrm{Supp} = \{P_1, \ldots, P_n\}$ the support of the divisor D. Since $|\mathrm{Supp(D)}| = n$, we have that the permutation group $\mathcal{P}(\mathrm{Supp(D)})$ on $\mathrm{Supp(D)}$ is isomorphic to the symmetric group S_n, and each $\sigma \in \mathcal{P}(\mathrm{Supp(D)})$ induces a $\mathbb{F}_q$-linear mapping $\widehat{\sigma}$ of the code $C_{\mathcal{X}}(D, G)$ to $\mathbb{F}_q^n$ by setting

$$\widehat{\sigma}(f(P_1), \ldots, f(P_n)) := (f(\sigma(P_1)), \ldots, f(\sigma(P_n))).$$

The mapping $\widehat{\sigma}$ is an *automorphism* of the code $C_{\mathcal{X}}(D, G))$ if $\widehat{\sigma}(C_{\mathcal{X}}(D, G)) = C_{\mathcal{X}}(D, G)$.

In [7], Goppa already observed that the underlying algebraic curve induces automorphism of the associated AG codes as follows.

Proposition 2.1. *Let* $\mathrm{Aut}(\mathcal{X}) = \{\sigma : \mathcal{X} \to \mathcal{X} \ ; \ \sigma \text{ is birational }\}$ *be the automorphism group of* $\mathcal{X}$ *over* $\mathbb{F}_q$ *and, for divisors* D *and* G*, consider the subgroup*

$$\mathrm{Aut_{D,G}}(\mathcal{X}) = \{\sigma \in \mathrm{Aut}(\mathcal{X}) \ : \ \sigma(\mathrm{D}) = \mathrm{D} \text{ and } \sigma(\mathrm{G}) = \mathrm{G}\} .$$

Then, each $\sigma \in \mathrm{Aut_{D,G}}(\mathcal{X})$ *induces an automorphism of* $C_{\mathcal{X}}(D, G)$ *by*

$$\widehat{\sigma}(f(P_1), \ldots, f(P_n)) = (f(\sigma(P_1)), \ldots, f(\sigma(P_n))) .$$

Assume that $\mathcal{X}$ has a nontrivial automorphism $\sigma \in \mathrm{Aut_{D,G}}(\mathcal{X})$ and let H be the cyclic subgroup of $\mathrm{Aut}(\mathcal{X})$ generated by σ. Let $\mathrm{Supp}(D) = O_1 \cup \ldots \cup O_r$ be the decomposition of the support of D into disjoint orbits under the action of σ. Then, by Proposition 2.1, the entries of the codewords in $C_{\mathcal{X}}(D, G)$ will be cyclically permuted in several blocks by σ. We will denote $\sigma^0 = Id$, where Id is the identity automorphism, and, for a positive integer j, $\sigma^j = \underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{j}$. In this way, for each $i = 1, \ldots, r$, pick any one point $P_{i,0} \in O_i$ and enumerate the other points on O_i as $P_{i,j} = \sigma^j(P_{i,0})$, where j runs from 1 to $|O_i| - 1$. Using this fact, we get the following result.

Lemma 2.2. *Let* $C_{\mathcal{X}}(D, G)$ *be an AG code arising from* $\mathcal{X}$ *over* $\mathbb{F}_q$ *and let* $\sigma \in \mathrm{Aut_{D,G}}(\mathcal{X})$ *be a nontrivial automorphism. If* $\mathrm{Supp}(D) = O_1 \cup \ldots \cup O_r$ *is the decomposition of the support of* D *into disjoint orbits under the action of* σ*, then there is a one-to-one correspondence between* $C_{\mathcal{X}}(D, G)$ *and a submodule* $\overline{C}$ *of the free module* $\mathbb{F}_q[t]^r$*.*

Proof. Suppose that $\mathrm{Supp}(D) = O_1 \cup \ldots \cup O_r$ is the decomposition of the support of D into disjoint orbits under the action of σ. For each $i = 1, \ldots, r$, let $O_i = \{P_{i,0}, \ldots, P_{i,|O_i|-1}\}$, where $P_{i,j} = \sigma^j(P_{i,0})$ for each $j = 1, \ldots, |O_i| - 1$, and let $h_i(t) = \sum_{j=0}^{|O_i|-1} f(P_{i,j})t^j$.

The r-tuples $(h_1(t), \ldots, h_r(t))$ can be seen also as an element of the $\mathbb{F}_q[t]$-module $A = \bigoplus_{i=1}^{r} \mathbb{F}_q[t]/\langle t^{|O_i|} - 1\rangle$. So, the collection $\tilde{C}$ of r-tuples obtained from all $f \in \mathcal{L}(G)$ is closed under sum and multiplication by t. Define $\overline{C} := \pi^{-1}(\tilde{C})$, where π is the natural projection from $\mathbb{F}_q[t]^r$ onto $\bigoplus_{i=1}^{r} \mathbb{F}_q[t]/\langle t^{|O_i|} - 1\rangle$. Thus, we get a one-to-one correspondence between $C_{\mathcal{X}}(D, G)$ and $\overline{C} \leq \mathbb{F}_q[t]^r$. □

By the previous lemma, an AG code $C_{\mathcal{X}}(D, G)$ can be identified with a submodule $\overline{C} \leq \mathbb{F}_q[t]^r$ and thus the standard theory of Gröbner basis for modules may be applied.

Suppose that $C_{\mathcal{X}}(D, G)$ has length n and dimension k. A Gröbner basis $\mathcal{G} = \{\mathbf{g}^{(1)}, \ldots, \mathbf{g}^{(r)}\}$ for $\overline{C} \leq \mathbb{F}_q[t]^r$ with exactly r elements allows us to obtain a systematic encoding of C. Since $\{LT(\mathbf{g}^{(1)}), \ldots, LT(\mathbf{g}^{(r)})\}$ generates $LT(\overline{C})$, it follows that the nonstandard monomials appearing in the r-tuples $(h_1(t), \ldots, h_r(t))$ can be obtained from the $\mathbf{g}^{(i)}$'s. By ordering these monomials in decreasing order we obtain the so-called *information positions* of $(h_1(t), \ldots, h_r(t))$, which are the first k monomials $\mathbf{m}_l = t^{i_l}\mathbf{e}_{j_l}$, $l = 1, \ldots, k$. Let $VC(h_1(t), \ldots, h_r(t))$ be the vector of coefficients of the terms of $(h_1(t), \ldots, h_r(t))$ listed in the POT order. We have the following systematic encoding algorithm:

Algorithm 2.3.
Input: *A Gröbner basis* $\mathcal{G}$, *monomials* $\{\mathbf{m}_1, \ldots, \mathbf{m}_k\}$ *and* $\mathbf{w} = (w_1, \ldots, w_k) \in \mathbb{F}_q^k$.
Output: $c(\mathbf{w}) \in C = C(\mathcal{X}, D, G)$.
1. *Set* $f := w_1\mathbf{m}_1 + \cdots + w_k\mathbf{m}_k$.
2. *Compute* $f = \mathbf{a}_1\mathbf{g}^{(1)} + \ldots + \mathbf{a}_r\mathbf{g}^{(r)} + \mathbf{R}_{\mathcal{G}}$.
3. *Return* $c(\mathbf{w}) := VC(f - \mathbf{R}_{\mathcal{G}})$.

This method is more compact compared with the usual encoding via generator matrix. The total amount of computation is roughly the same and the amount of necessary stored data is lower in this method, of order $r(n-k)$ against $k(n-k)$ when encoding via generator matrix. More details about this encoding algorithm can be found in [8].

2.3. The root diagram

Consider the one-point AG code $C = C_{\mathcal{X}}(D, \lambda P)$ and suppose that $\mathcal{X}$ has an automorphism σ fixing the divisors D and $G = \lambda P$. Suppose also that the order of σ is a factor of $q-1$. Let $\overline{C}$ be the submodule of $\mathbb{F}_q[t]^r$ associated to C by the automorphism σ. Using the POT ordering we can get a Gröbner basis $\mathcal{G} = \{\mathbf{g}_1, \ldots, \mathbf{g}_r\}$ for $\overline{C}$ such that $\mathbf{g}_i = (0, \ldots, 0, g_i^{(i)}(t), g_i^{(i+1)}(t), \ldots, g_i^{(r)}(t))$, for all $i = 1, \ldots, r$, see [[8], Proposition II.B.4].

Note that, if $\deg(g_i^{(i)}(t)) = d_i$, then $g_i^{(i)}(t)$ has d_i distinct roots in $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. In fact, let $\mathbf{q}_i = (t^{|O_i|} - 1)\mathbf{e}_i$. Note that $\mathbf{q}_i \in \pi^{-1}(0, \ldots, 0)$ and we have that $\mathbf{q}_i \in \overline{C}$. Since $|O_i|$ divides the order of σ, it follows that $t^{|O_i|} - 1$ divides $t^{q-1} - 1 = \prod_{a \in \mathbb{F}_q^*}(t - a)$. Now, $LT(\mathbf{g}^{(i)}) = g_i^{(i)}(t)$ divides $LT(\mathbf{q}_i) = t^{|O_i|} - 1$, and the claim follows from the fact that $t^{q-1} - 1$ has $q - 1$ distinct roots in $\mathbb{F}_q$.

For $i = 1, \ldots, r$, let $\mathcal{R}_i \subseteq \mathbb{F}_q^*$ be the set of roots of $t^{|O_i|} - 1$. By a *root diagram* $\mathcal{D}_C$ for the code C, we mean a table with r rows. For each i, the boxes on the i-th row correspond to the elements of $\mathcal{R}_i$. We mark the roots of $g_i^{(i)}(t)$ on the i-th row with a X in the corresponding box.

By Proposition II.C.1 in [8], there is a $\mathbb{F}_q$-basis for C in one-to-one correspondence with the nonstandard monomials in $\overline{C}$. That is, terms of the form $t^\ell\mathbf{e}_j$ appearing as leading terms of some element of $\overline{C}$, with $\ell \leq |O_j| - 1$. Now, if there are m_j empty boxes on row j of the root diagram, then $g_j^{(i)}(t)$ has $|O_j| - m_j$ roots and $LT(\mathbf{g}^{(j)}) = t^{|O_j|-m_j}$. So, we obtain m_j nonstandard monomials $t^\ell\mathbf{e}_j$. This fact gives us the following important result.

Proposition 2.4. ([12], Proposition 2.3) *The dimension of the code C is equal to the number of empty boxes in the root diagram $\mathcal{D}_C$.*

3. The root diagram for certain one-point AG codes

Let $\mathcal{X}^\star$ be the curve defined over $\mathbb{F}_q$ by affine equation $f(y) = g(x)$ and that has the following conditions:

1. $f(T), g(T) \in \mathbb{F}_q[T]$, $\deg(f) = a$ and $\deg(g) = b$, with $gcd(a, b) = 1$;
2. there exists a point P on $\mathcal{X}^\star$ such that $\mathrm{div}_\infty(x) = aP$, $\mathrm{div}_\infty(y) = bP$, and $H(P) = \langle a, b\rangle$;
3. there exists $\sigma \in \mathrm{Aut}_{\mathrm{D,G}}(\mathcal{X}^\star)$, where $G = \lambda P$ for some positive integer λ, given by $\sigma(x) = \alpha x$ and $\sigma(y) = \alpha^t y$, for some positive integer t and some $\alpha \in \mathbb{F}_q^*$.

We observe that if the order of α is equal to $\mathrm{ord}(\alpha) := \nu$, then, by the definition of σ, it follows that the order of σ is equal to ν which divides $q - 1$.

We can ask if curves with such conditions do exist or if there are a large number of them. By [15, Prop. 6.4.1] and [9, Lemma 12.2 and Th. 12.9], we have that the curves defined over a finite field $\mathbb{F}_{q^s}$ by the affine equation $y^{q^n} + y = x^m$, with $\gcd(q, m) = 1$, are examples of curves that satisfy the above conditions if $m(q^n - 1)$ divides $q^s - 1$. We note that it is hard to study automorphisms of curves in general, especially without giving the equation that defines it. In particular, with the results on automorphisms known to date, we can not present general examples of curves satisfying the above conditions. For a study on automorphism of algebraic curves we refer the reader to [9, Ch. 11 and 12], particularly in the Section 12.1 results on automorphisms of curves given by separated polynomials can be found.

Let $D = P_1 + \ldots + P_n$, with $P_i \neq P$ for all $i = 1, \ldots, n$, a divisor on $\mathcal{X}^\star$ and let $\mathrm{Supp}(D) = O_1 \cup \ldots \cup O_r \cup O_{r+1} \cup \ldots \cup O_{r+s}$ be the decomposition of the support of D into disjoint orbits under the action of σ. In this section we will describe the root diagram for one-point AG codes $C_{\mathcal{X}^\star}(D, \lambda P)$.

Note that, by definition of σ, if $Q = (0, \eta) \in O_i$, for some $\eta \in \mathbb{F}_q$, then $O_i = \{(0, \eta), (0, \alpha^t\eta), \ldots, (0, \alpha^{t.t_i}\eta)\}$, where t_i is the smallest nonnegative integer such that $\alpha^{t.(t_i+1)} = 1$. Analogously, if $Q = (\omega, 0) \in O_i$, for some $\omega \in \mathbb{F}_q$, then $O_i = \{(\omega, 0), (\alpha\omega, 0), \ldots, (\alpha^{\nu-1}\omega, 0)\}$. Let $O_{r+1}, \ldots, O_{r+s}$ be the orbits that contains $\mathbb{F}_q$-rational points on $\mathcal{X}^\star$ of the form $(0, \eta)$ or $(\omega, 0)$. We will work with the first r rows of the root diagram $\mathcal{D}_C$ for the code $C_{\mathcal{X}^\star}(D, \lambda P)$, the results for the last s rows are similar can be obtained in particular cases. For each $i = 1, \ldots, r$, suppose that $O_i = \{P_{i,0}, P_{i,1}, \ldots, P_{i,|O_i|-1}\}$, where $P_{i,0} = (x_i, y_i)$, with $x_i \neq 0$ and $y_i \neq 0$, and $P_{i,j} = \sigma^j(P_{i,0}) = (\alpha^j x_i, \alpha^{jt} y_i)$. So, from the definition of σ it follows that $|O_1| = \ldots = |O_r| = \mathrm{ord}(\alpha) = \nu$.

Associated with the decomposition of the support of D into disjoint orbits under the action of σ as above, let us assume the following conditions:

(I) for each $i = 1, \ldots, r$, there exists a polynomial $M_i(y)$ such that the orbit O_i is the intersection of $\mathrm{Supp}(D)$ with the curve $M_i(y) = 0$ and, for all i, $M_i(y)$ is a non-zero constant when restricted to each of the orbits O_k, $k \neq i$;

(II) for each $1 \leq i \leq r$ and $0 \leq j \leq |O_i| - 1 = \nu - 1$, there exists a polynomial $B_{i,j}(x, y)$ such that $B_{i,j}(x, y)$ vanishes at each point of O_i except $P_{i,j}$.

In the Proposition 3.3 and the Theorem 3.4 below, the reader will see that the existence of these polynomials is fundamental to obtain the root diagram for one-point AG codes $C_{\mathcal{X}^\star}(D, \lambda P)$.

Let κ be the smallest positive integer such that $\alpha^{\kappa t} = 1$. The next result gives us a way to get $M_i(y)$.

Proposition 3.1. *Let κ, O_i and $P_{i,j} = \sigma^j(P_{i,0}) = (\alpha^j x_i, \alpha^{jt} y_i)$ be as above. If*

$$(*) \quad \alpha^{\ell t} y_i \neq \alpha^{\ell t} y_k, \text{ for all } \ell = 0, 1, \ldots, \kappa - 1 \text{ and } k \neq i,$$

then $M_i(y) = \prod_{\ell=0}^{\kappa-1}(y - \alpha^{\ell t}y_i)$ *satisfies the condition (I) above.*

Proof. By the definition of κ, it follows that the orbit O_i is the intersection of $\mathrm{Supp}(D)$ with the curve $M_i(y) = 0$. The condition $(*)$ implies that $M_i(y)$ is a non-zero constant when restricted to each of the orbits O_k, $k \neq i$. □

Note that the condition $(*)$, which is the key to getting a polynomial $M_i(y)$ as in (I), depends on the decomposition of the support of D and the coordinates of the points on such support.

We obtain $B_{i,j}(x, y)$ in a similar way by using a solution of an interpolation problem.

Lemma 3.2. *For* $i = 1, \ldots, r$ *and* $j = 0, \ldots, |O_i| - 1$, *let* $M_i(y)$ *and* $B_{i,j}(x, y)$ *be as (I) and (II) above. Then,* $div_\infty(M_i) = (\rho_1 b)P$ *and* $div_\infty(B_{i,j}) = (\rho_2 a + \rho_3 b)P$, *where* ρ_1, ρ_2 *and* ρ_3 *are nonnegative integers.*

Proof. We have that $\mathrm{div}_\infty(\mathrm{x}) = \mathrm{aP}$ and $\mathrm{div}_\infty(y) = bP$. Then, the result follows from the fact that $M_i(y)$ and $B_{i,j}(x, y)$ are polynomials. □

Let ρ_1, ρ_2 and ρ_3 be as the previous lemma. So, for $\lambda \leq (\rho_2 a + \rho_3 b) + r(\rho_1 b)$, we can get the following information about the root diagram $\mathcal{D}_C$.

Proposition 3.3. *Let* $C_{\mathcal{X}^\star}(D, \lambda P)$ *and* σ *be as above. Let* $\mathcal{D}_C$ *be the root diagram for* $C_{\mathcal{X}^\star}(D, \lambda P)$. *Fix* i, $1 \leq i \leq r$, *and let* ρ_1, ρ_2 *and* ρ_3 *be as above.*

1. *If* $\lambda \geq (i-1)(\rho_1 b)$, *then the* i*-th row of* $\mathcal{D}_C$ *is not full, in the sense that not every box in the* i*-th row are marked with* X*;*
2. *If* $\lambda \geq (\rho_2 a + \rho_3 b) + (i-1)(\rho_1 b)$, *then the row is empty, in the sense that none of the boxes in the* i*-th row is marked with* X.

Proof. Let $\overline{C} \leq \mathbb{F}_q[t]^r$ be the submodule associated to $C_{\mathcal{X}^\star}(D, \lambda P)$, where $D = P_1 + \ldots + P_n$ and $P_i \neq P$ for all $i = 1, \ldots, n$.

1. Suppose that $\lambda \geq (i-1)(\rho_1 b)$. By Lemma 3.2, the function

$$F_i(x, y) = M_1(x, y) \cdots M_{i-1}(x, y)$$

belongs to $L(\lambda P)$ and hence $(F_i(P_1), \ldots, F_i(P_n)) \in C_{\mathcal{X}^\star}(D, \lambda P)$. By computing $(F_i(P_1), \ldots, F_i(P_n))$, we observe that $\overline{C}$ contains an element of the form $(0, \ldots, 0, h_i(t), \ldots, h_r(t))$ with $i-1$ zeroes and $h_i(t) = \sum_{j=0}^{|O_i|-1} F_i(P_{i,j})t^j$. Since

$$F_i(P_{i,j}) = M_1(P_{i,j}) \cdots M_{i-1}(P_{i,j}) = \text{ constant } c \neq 0\,,$$

we have $h_i(t) = c.\sum_{j=0}^{|O_i|-1} t^j$ and thus $h(1) \neq 0$ as $|O_i|$ divides $q-1$. Therefore the i-th row of $\mathcal{D}_C$ is not full, since $g_i^{(i)}(t)$ divides $h_i(t)$.

2. Now, suppose $\lambda \geq (\rho_2 + \rho_3 b) + (i-1)(\rho_1 b)$. So, by Lemma 3.2, $G_i(x, y) = B_{i,0}(x, y)F_i(x, y) \in L(\lambda P)$ and $G_i(Q) = 0$ for $Q \in O_1 \cup O_2 \cup \ldots \cup O_{i-1}$. Moreover, $G_i(Q) = 0$ for all $Q \in O_i \setminus \{P_{i,0}\}$. Then the element of $\overline{C}$ corresponding to $(G_i(P_1), \ldots, G_i(P_n))$ verifies $h_1(t) = h_2(t) = \ldots = h_{i-1}(t) = 0$ and $h_i(t) = G_i(P_{i,0}) = c \neq 0$. Thus, $\overline{C}$ contains the element $(0, \ldots, 0, c, h_{i+1}(t), \ldots, h_r(t))$. So, the i-th row of $\mathcal{D}_C$ is empty.

□

Let N be the number of $\mathbb{F}_q$-rational points on $\mathcal{X}^\star$. By Riemann-Roch Theorem, it follows that if $\lambda < N$, then the dimension of the one-point AG code $C_{\mathcal{X}^\star}(D, \lambda P)$ is equal to the dimension of the Riemann-Roch space $L(\lambda P)$. In this case, we complete the information about the root diagram $\mathcal{D}_C$.

Theorem 3.4. *Let $\mathcal{D}_C$ be the root diagram for $C_{\mathcal{X}^\star}(D, \lambda P)$. If there is $i \in \{1, \ldots, r\}$ such that*

$$(i-1)(\rho_1 b) \leq \lambda < (\rho_2 a + \rho_3 b) + (i-1)(\rho_1 b),$$

then the i-th row of $\mathcal{D}_C$ is neither full, nor empty, and the complement of the set of roots marked on row i of the diagram is the set

$$E_i = \{\alpha^{-(\beta+\gamma b)} \in \mathbb{F}_q^* \mid 0 \leq \beta \leq b-1,\ 0 \leq \gamma \leq \rho_1 - 1,\ (i-1)(\rho_1 b) + \beta a + \gamma b \leq \lambda\}.$$

Proof. Let $\overline{C} \leq \mathbb{F}_q[t]^r$ be the submodule associated to $C_{\mathcal{X}^\star}(D, \lambda P)$. Let $D_i \subset \mathbb{F}_q^*$ be the set of non-marked boxes in row i, where $1 \leq i \leq r$. We will show that $D_i = E_i$. Let $F_i(y)$ be as in the previous proposition and consider $f_i(x,y) = F_i(y)x^\beta y^\gamma$. By Lemma 3.2 and the conditions over β and γ given in the definition of E_i, we have that $f_i(x,y) \in L(\lambda P)$. So, associated to $f_i(x,y)$ we get an element $h = (h_1(t), \ldots, h_r(t)) \in \overline{C}$. Since $F_i(Q) = 0$ for all $Q \in O_1 \cup \ldots \cup O_{i-1}$, it follows that $h_k(t) = 0$, for $k = 1, \ldots, i-1$. Let $P_{i,j} = \sigma(P_{i,0}) = (\alpha^j x_i, \alpha^{\ell j} y_i) \in O_i$. Thus, $f_i(P_{i,j}) = F_i(P_{i,j})\alpha^{j\beta} x_i^\beta \alpha^{\ell j \gamma} y_i^\gamma = F_i(P_{i,j}) x_i^\beta y_i^\gamma \alpha^{j(\beta+\ell\gamma)}$, for all $j = 0, 1, \ldots, |O_i| - 1$. Now, $F_i(P_{i,j})$, x_i^β and y_i^γ are all non-zero constants and independent of j. Taking $b_i = F_i(P_{i,j}) x_i^\beta y_i^\gamma \neq 0$, we have

$h_i(t) = \sum_{j=0}^{|O_i|-1} f_i(P_{i,j}) t^j = |O_i| \cdot b_i \sum_{j=0}^{|O_i|-1} (\alpha^{(\beta+\ell\gamma)} t)^j$ whose roots are all distinct from $\alpha^{-(\beta+\ell\gamma)}$. Consequently, $\alpha^{-(\beta+\ell\gamma)}$ is not a root of $g_i^{(i)}(t)$ and hence $E_i \subseteq D_i$.

By Proposition 2.4, $\dim(C_{\mathcal{X}^\star}(D, \lambda P)) = \sum \sharp D_i$. Since $H(P) = \langle a, b \rangle$ and $\lambda < N$, we have that $\dim(C_{\mathcal{X}^\star}(D, \lambda P)) = \sharp\{(\beta, \gamma) \in \mathbb{N}_0^2\ ;\ 0 \leq \beta \leq b-1$ and $\beta a + \gamma b \leq \lambda\}$.

Let $\widehat{E}_i = \{(\beta, \gamma) \in \mathbb{N}_0^2 \mid 0 \leq \beta \leq b-1, 0 \leq \gamma \leq \rho_1 - 1,\ (i-1)(\rho_1 b) + \beta a + \gamma b \leq \lambda\}$. Thus, $\sharp\{(\beta, \gamma) \in \mathbb{N}_0^2\ ;\ 0 \leq \beta \leq b-1$ and $\beta a + \gamma b \leq \lambda\} = \sum \sharp \widehat{E}_i$ and, since $\sum \sharp \widehat{E}_i = \sharp \sum E_i$, it follows that $\sum \sharp D_i = \sum \sharp E_i$. Therefore, $E_i = D_i$. □

Let $F_i(y)$ be as above. Then, we have that $F_i(Q) = c_i \in \mathbb{F}_q^*$, for all $Q \in O_i$. With the conditions of the above theorem, fix an index i, $1 \leq i \leq r$, where the row i of $\mathcal{D}_C$ is neither full, nor empty. Let $\alpha^{k_1}, \alpha^{k_2}, \ldots, \alpha^{k_\ell}$ be the roots marked on the row i and let $p(t) = \prod_{j=1}^{\ell}(t - \alpha^{k_j})$ be the unique monic polynomial of degree ℓ with these roots. Note that, including zeroes for powers of t higher than the number of roots, we can write $p(t) = \sum_{j=0}^{|O_i|-1} a_j t^j$, where $a_j = 0$ for $j > \ell$. Consider the function

$$f_i(x,y) = \frac{F_i(y)}{c_i} \left(\sum_{j=0}^{|O_i|-1} a_j \frac{B_{i,j}(x,y)}{B_{i,j}(P_{i,j})} \right)$$

Then, by the definition of $F_i(y)$ and $B_{i,j}(x,y)$, it is clear that $f_i(x,y) \in L(\lambda P)$ and its associated module element $\mathbf{h} \in \overline{C}$ has $i-1$ leading zero components and i-th component $h_i(t)$ equal to $p(t)$. Using this fact and the same procedures used in [12, Section 4, pp. 306] and [4, Section 4, pp. 60], namely

- `RootDiagram[i]`: returns a list of the roots corresponding to the marked boxes in line i of $\mathcal{D}_C$;
- `Boxes[i]`: the number of boxes in row i of $\mathcal{D}_C$, that is Boxes$[i] = |O_i|$;
- `Evaluate[i, point]`: a procedure which takes as input the coefficients $\{a_k\}$ of the unique monic polynomial over $\mathbb{F}_q$ having the marked elements on a row number i as roots and a point $P_{i,j}$ on O_i, and evaluates the function $f_i(x,y)$ as above at a *point* $P_{i,j}$;

we have the following algorithm, which is completely analogous to Proposition 4.4 in [12] and Algorithm 4.2 in [4].

Algorithm 3.5.

Input: the root diagram $\mathcal{D}_C$, the N $\mathbb{F}_q$-rational points $P_{i,j}$ of $\mathrm{Supp}(D) = O_1 \cup \ldots \cup O_r \cup O_{r+1} \cup O_{r+s}$.
Output: a non-reduced Gröbner basis $\mathcal{G} = \{\mathbf{g}^{(1)}, \mathbf{g}^{(2)}, \ldots, \mathbf{g}^{(r+s)}\}$ of $\overline{C}$.

$\mathcal{G} := \{\}$
for i from 1 to $r+s$ **do**
  if |RootDiagram[i]|< Boxes[i] **then**
    for k from 1 to $r+s$ **do**
      $g_k^{(i)} := 0$
      if $k \geq i$ **then**
        for j from 0 to Boxes[k] -1 **do**
          $g_k^{(i)} := g_k^{(i)} +$ Evaluate[i,$P_{k,j}$] $t^j \, \mathbf{e}_k$
        end for
      end if
    end for
  else
    $\mathbf{g}^{(i)} := (t^{\mathrm{Boxes}[i]} - 1)\, \mathbf{e}_i$
  end if
  $\mathcal{G} := \mathcal{G} \cup \{\mathbf{g}^{(i)}\}$
end for
return $\mathcal{G}$

Remark 3.6. *Note that this algorithm makes use only of interpolation and function evaluation problems. As studied in [12] and [4], it has a computational complexity much lower than the complexity of general Gröbner basis algorithms. In particular, it does not use divisions or reductions that would increase the complexity, as in the case of Buchberger's algorithm.*

4. Examples

4.1. The maximal curve $y^q + y = x^{q^r+1}$

Let $\mathcal{X}_{q,q^r+1}$ be the curve defined over $\mathbb{F}_{q^{2r}}$ by the affine equation

$$y^q + y = x^{q^r+1},$$

where q is a prime power and r an odd integer. Note that when $r = 1$ the curve is just the Hermitian curve. The curve $\mathcal{X}_{q,q^r+1}$ has genus $g = q^r(q-1)/2$, one single singular point $P_\infty = (0:1:0)$ at infinity and other q^{2r+1} $\mathbb{F}_{q^{2r}}$-rational points. Thus, this curve is a maximal curve over $\mathbb{F}_{q,q^r+1}$ because its number of $\mathbb{F}_{q^{2r}}$-rational points equals the upper Hasse-Weil bound, namely equals $q^{2r} + 1 + 2gq^r$. Furthermore, $H(P_\infty) = \langle q, q^r + 1\rangle$, see [14], and

$$\begin{array}{rccc} \sigma: & x & \mapsto & \alpha x \\ & y & \mapsto & \alpha^{q^r+1} y \end{array} \tag{2}$$

with $\alpha \in \mathbb{F}_{q^{2r}}^*$ such that $\alpha^{(q^r+1)(q-1)} = 1$, is an automorphism of $\mathcal{X}_{q,q^r+1}$, see [11]. Note that σ has order $(q^r+1)(q-1)$. So, the order of σ divides $q^{2r} - 1$.

Note that under the action of the automorphism σ above the q^{2r+1} $\mathbb{F}_{q^{2r}}$-rational points on $\mathcal{X}_{q,q^r+1}$ are disposed in $q(q^{r-1}+\cdots+q+1)+2$ orbits, where $q(q^{r-1}+\cdots+q+1)$ of them has length $(q^r+1)(q-1)$ and the remaining two orbits, one has length $q-1$ and the other has length 1. In fact, for the definition of the automorphism σ, it is clear that:

- $\sigma(0,0) = (0,0)$, and so we have a one orbit with a single point;

- all the $q-1$ $\mathbb{F}_{q^{2r}}$-rational points $(0,b)$, with $b \neq 0$, form an orbit with length $q-1$, since $\sigma(0,b) = (0, \alpha^{q^r+1}b)$ and $\alpha \in \mathbb{F}_{q^{2r}}^*$ is such that $\alpha^{(q^r+1)(q-1)} = 1$;
- the other $q^{2r+1} - q = q(q^r+1)(q^r-1)$ $\mathbb{F}_{q^{2r}}$-rational points $(x,y) \in \mathcal{X}_{q,q^r+1}$, with $x \neq 0$ and $y \neq 0$, are arranged in $q(q^{r-1} + \cdots + q + 1)$ orbits of length $(q^r+1)(q-1)$.

Let α be as in (2). Let $\mathbb{F}_{q^{2r}}^* = \langle a \rangle$ and $t \in \{0, 1, \ldots, q^{2r}-2\}$ be such that $\alpha = a^t$. So, given $P_{i,0} = (a^{t_i}, a^{l_i}) \in O_i$, the other points $P_{i,j}$ on O_i are $P_{i,j} = \sigma^j(P_{i,0}) = (a^{t_i+jk}, a^{l_i+jk(q^r+1)})$, with $j \in \{1, \ldots, (q^r+1)(q-1)-1\}$. Then, for $i = 1, \ldots, r$ and $j = 0, \ldots, (q^r+1)(q-1)-1$, we get

$$M_i(y) := \prod_{j=0}^{q-2}(y - a^{l_i+jk(q^r+1)}) = y^{q-1} - a^{l_i(q-1)}, \tag{3}$$

and

$$B_{i,j}(x,y); = \prod_{s=1}^{q-2}(y - a^{l_i+k(q^r+1)(j+s)}) \prod_{s=1}^{(q^r+1)-1}(x - a^{t_i+k(j+s)}). \tag{4}$$

Since $\mathrm{div}_\infty(x) = qP_\infty$ and $\mathrm{div}_\infty(y) = (q^r+1)P_\infty$, we have that

- $\mathrm{div}_\infty(M_i(y)) = (q-1)(q^r+1)P_\infty$; that is, $M_i(y) \in L((q-1)(q^r+1)P_\infty)$, for all $i = 1, \ldots, r$;
- $\mathrm{div}_\infty(B_{i,j}(x,y)) = ((q-2)(q^r+1) + q((q^r+1)-1))P_\infty$; that is, $B_{i,j} \in L(q.q^r + (q-2)(q^r+1))P_\infty)$, for all $1 \leq i \leq r$) e $0 \leq j \leq (q^r+1)(q-1)-1$.

With the notations on the previous section we have that:

- $a = q$ and $b = q^r + 1$;
- $P = P_\infty$;
- $\mathrm{div}_\infty(x) = qP_\infty$ and $\mathrm{div}_\infty(y) = (q^r+1)P_\infty$;
- $H(P_\infty) = \langle q, q^r+1 \rangle$;
- $\rho_1 = q-1$, $\rho_2 = q^r$ and $\rho_3 = q-2$.

Thus, using the Proposition 3.3 and the Theorem 3.4, we can get the root diagram for one-point codes $C_{\mathcal{X}_{q,q^r+1}}(D, \lambda P_\infty)$ and then the Gröbner basis for the module $\overline{C}$ associated to $C_{\mathcal{X}_{q,q^r+1}}(D, \lambda P_\infty)$ by Algorithm 3.5.

Example 4.1. *Consider the curve $\mathcal{X}_{2,9} : y^2 + y = x^9$ over $\mathbb{F}_{64}$ and the code $C = C(\mathcal{X}_{2,9}, D, 20P_\infty)$, where D is the sum of the 128 $\mathbb{F}_{64}$-rational points distinct of $P_\infty = (0:1:0)$. Let α be a generator of $\mathbb{F}_{64}^*$. The automorphism $\sigma(x,y) = (\alpha^7 x, y)$ decomposes the points in Supp(D) into sixteen orbits, being fourteen of*

length 9 *and two of length* 1*:*

$$\begin{aligned}
O_1 &= \{P_{1,0} = (\alpha, \alpha^{18}), P_{1,1} = (\alpha^8, \alpha^{18}), \ldots, P_{1,8} = (\alpha^{57}, \alpha^{18})\},\\
O_2 &= \{P_{2,0} = (\alpha, \alpha^{54}), P_{2,1} = (\alpha^8, \alpha^{54}), \ldots, P_{2,8} = (\alpha^{57}, \alpha^{54})\},\\
O_3 &= \{P_{3,0} = (\alpha^2, \alpha^{36}), P_{3,1} = (\alpha^9, \alpha^{36}), \ldots, P_{3,8} = (\alpha^{58}, \alpha^{36})\},\\
O_4 &= \{P_{4,0} = (\alpha^2, \alpha^{45}), P_{4,1} = (\alpha^9, \alpha^{45}), \ldots, P_{4,8} = (\alpha^{58}, \alpha^{45})\},\\
O_5 &= \{P_{5,0} = (\alpha^3, \alpha^{31}), P_{5,1} = (\alpha^{10}, \alpha^{31}), \ldots, P_{5,8} = (\alpha^{59}, \alpha^{31})\},\\
O_6 &= \{P_{6,0} = (\alpha^3, \alpha^{59}), P_{6,1} = (\alpha^{10}, \alpha^{59}), \ldots, P_{6,8} = (\alpha^{59}, \alpha^{59})\},\\
O_7 &= \{P_{7,0} = (\alpha^4, \alpha^9), P_{7,1} = (\alpha^{11}, \alpha^9), \ldots, P_{7,8} = (\alpha^{60}, \alpha^9)\},\\
O_8 &= \{P_{8,0} = (\alpha^4, \alpha^{27}), P_{8,1} = (\alpha^{11}, \alpha^{27}), \ldots, P_{8,8} = (\alpha^{60}, \alpha^{27})\},\\
O_9 &= \{P_{9,0} = (\alpha^5, \alpha^{47}), P_{9,1} = (\alpha^{12}, \alpha^{47}), \ldots, P_{9,8} = (\alpha^{61}, \alpha^{47})\},\\
O_{10} &= \{P_{10,0} = (\alpha^5, \alpha^{61}), P_{10,1} = (\alpha^{12}, \alpha^{61}), \ldots, P_{10,8} = (\alpha^{61}, \alpha^{61})\},\\
O_{11} &= \{P_{11,0} = (\alpha^6, \alpha^{55}), P_{11,1} = (\alpha^{13}, \alpha^{55}), \ldots, P_{11,8} = (\alpha^{62}, \alpha^{55})\},\\
O_{12} &= \{P_{12,0} = (\alpha^6, \alpha^{62}), P_{12,1} = (\alpha^{13}, \alpha^{62}), \ldots, P_{12,8} = (\alpha^{62}, \alpha^{62})\},\\
O_{13} &= \{P_{13,0} = (\alpha^7, \alpha^{21}), P_{13,1} = (\alpha^{14}, \alpha^{21}), \ldots, P_{13,8} = (1, \alpha^{21})\},\\
O_{14} &= \{P_{14,0} = (\alpha^7, \alpha^{42}), P_{14,1} = (\alpha^{14}, \alpha^{42}), \ldots, P_{14,8} = (1, \alpha^{42})\},\\
O_{15} &= \{P_{15,0} = (0, 1)\},\\
O_{16} &= \{P_{16,0} = (0, 0)\}.
\end{aligned}$$

Since the set of roots of $t^9 - 1$ *in* $\mathbb{F}_{64}$ *is* $\{1, \alpha^7, \alpha^{14}, \alpha^{21}, \alpha^{28}, \alpha^{35}, \alpha^{42}, \alpha^{49}, \alpha^{56}\}$*, Proposition 3.3 and Theorem 3.4 (where* $a = 2$*,* $b = 9$*,* $\rho_1 = 1$*,* $\rho_2 = 8$*,* $\rho_3 = 0$ *and* $\lambda = 20$*) give the following root diagram.*

α^7	α^{14}	α^{21}	α^{28}	α^{35}	α^{42}	α^{49}	α^{56}	1
x	x	x						
x	x	x	x	x	x	x		
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x
								x
								x

4.2. A quotient of the Hermitian curve

Let $\mathcal{X}_{q,m}$ be the curve defined over $\mathbb{F}_{q^2}$ by the affine equation

$$y^q + y = x^m,$$

where q is a prime power and $m > 2$ is a divisor of $q+1$. This curve is a quotient of the Hermitian curve and has genus $g = (q-1)(m-1)/2$, a single point at infinity, denoted by P_∞, and other $q(1+m(q-1))$ $\mathbb{F}_{q^2}$-rational points. One may notice that $P_\infty = (0:1:0)$ if $m = q+1$, and $P_\infty = (1:0:0)$ if $m \neq q+1$. In [5], it is shown that $\mathcal{X}_{q,m}$ is a maximal curve and in [13], G. Matthews studied Weierstrass semigroup and algebraic codes arising from $\mathcal{X}_{q,m}$. In addition, we have that $H(P_\infty) = \langle m, q\rangle$, see [5, Theorem 3].

Let $\mathbb{F}_{q^2}^* = \langle\alpha\rangle$ and k such that $mk = q+1$. Then,

$$\begin{array}{rccl} \tau: & x & \to & \alpha^k x \\ & y & \to & \alpha^{q+1} y \end{array} \tag{5}$$

is an automorphism of $\mathcal{X}_{q,m}$ of order $m(q-1)$, which divides q^2-1.

It is not hard to see that under the action of the automorphism τ above the $q(1+m(q-1))$ $\mathbb{F}_{q^2}$-rational points on $\mathcal{X}_{q,m}$ are disposed in $q+2$ orbits, where q of them has length $m(q-1)$ and the remaining two orbits, one has length $q-1$ and the other has length 1.

Taking $r=q$ and the first r orbits given by points on $\mathcal{X}_{q,m}$ of the form $P=(a,b)$ with $a,b\neq 0$. So, for each $i=1,\ldots,r$, given $P_{i,0}=(\alpha^{\ell_i},\alpha^{t_i})\in O_i$, the other points $P_{i,j}$ on O_i are $P_{i,j}=\sigma^j(P_{i,0})=(\alpha^{\ell_i+jk},\alpha^{t_i+j(q+1)})$, with $j\in\{1,\ldots,m(q-1)-1\}$. That is,

$$O_i=\{P_{i,j}=(\alpha^{\ell_i+jk},\alpha^{t_i+j(q+1)})\ ;\ j=0,\ldots,m(q-1)-1\}.$$

Then, for $i=1,\ldots,r$ and $j=0,1,\ldots,m(q-1)-1$, we get

$$M_i(y)=\prod_{j=0}^{q-2}(y-\alpha^{t_i+j(q+1)})$$

and

$$B_{i,j}(x,y)=\prod_{s=0,s\neq j}^{q-2}(y-\alpha^{t_i+s(q+1)})\prod_{s=0,s\neq j}^{m(q-1)-1}(x-\alpha^{\ell_i+sk}).$$

So, since $\mathrm{div}_\infty(x)=qP_\infty$ and $\mathrm{div}_\infty(y)=mP_\infty$, it follows that

- $\mathrm{div}_\infty(M_i(y))=(q-1)mP_\infty$; that is, $M_i(y)\in L((q-1)mP_\infty)$, for all $i=1,\ldots,r$;
- $\mathrm{div}_\infty(B_{i,j}(x,y))=((q-2)m+(m-1)q)P_\infty$; that is, $B_{i,j}\in L((m-1)q+(q-2)m)P_\infty)$, for all $1\leq i\leq r$) and $0\leq j\leq m(q-1)-1$.

With the notations on the previous section we have that:

- $a=q$ and $b=m$;
- $P=P_\infty$;
- $(x)_\infty=qP_\infty$ and $(y)_\infty=mP_\infty$;
- $H(P_\infty)=\langle q,m\rangle$;
- $\rho_1=q-1$, $\rho_2=q-2$ and $\rho_3=m-1$.

Therefore, we can get the root diagram for one-point codes $C_{\mathcal{X}_{q,m}}(D,\lambda P_\infty)$ and then the Gröbner basis for the module $\overline{C}$ associated to $C_{\mathcal{X}_{q,m}}(D,\lambda P_\infty)$.

Example 4.2. *Consider the curve $\mathcal{X}^\star: y^5+y=x^3$ over $\mathbb{F}_{25}$ and the code $C=C_{\mathcal{X}^\star}(D,30P_\infty)$, where D is the sum of the 65 $\mathbb{F}_{25}$-rational points distinct of P_∞. Let α be a generator of $\mathbb{F}_{25}^*$. The automorphism $\tau(x,y)=(\alpha^2x,\alpha^6y)$ decomposes the points in Supp(D) into seven orbits, being five of length 12, one of*

length 4 *and one of length* 1*:*

$$\begin{aligned}
O_1 &= \{P_{1,0} = (1, \alpha), P_{1,1} = (\alpha^2, \alpha^7), \ldots, P_{1,11} = (\alpha^{22}, \alpha^{19})\},\\
O_2 &= \{P_{2,0} = (1, \alpha^{20}), P_{2,1} = (\alpha^2, \alpha^2), \ldots, P_{2,11} = (\alpha^{22}, \alpha^{14})\},\\
O_3 &= \{P_{3,0} = (1, \alpha^4), P_{3,1} = (\alpha^2, \alpha^{10}), \ldots, P_{3,11} = (\alpha^{22}, \alpha^{22})\},\\
O_4 &= \{P_{4,0} = (1, \alpha^5), P_{4,1} = (\alpha^2, \alpha^{11}), \ldots, P_{4,11} = (\alpha^{22}, \alpha^{23})\},\\
O_5 &= \{P_{5,0} = (1, \alpha^{18}), P_{5,1} = (\alpha^2, 1), \ldots, P_{5,11} = (\alpha^{22}, \alpha^{12})\},\\
O_6 &= \{P_{6,0} = (0, \alpha^3), P_{6,1} = (0, \alpha^9), P_{6,2} = (0, \alpha^{15}), P_{6,3} = (0, \alpha^{21})\},\\
O_7 &= \{P_{7,0} = (0, 0)\}.
\end{aligned}$$

Since the set of roots of $t^{12} - 1$ *and* $t^4 - 1$ *in* $\mathbb{F}_{25}$ *are* $\{1, \alpha^2, \alpha^4, \alpha^6, \ldots, \alpha^{22}\}$ *and* $\{1, \alpha^6, \alpha^{12}, \alpha^{18}\}$*, respectively. So, Proposition 3.3 and Theorem 3.4 (where* $a = 5$*,* $b = 3$*,* $\rho_1 = 4$*,* $\rho_2 = 3$*,* $\rho_3 = 2$ *and* $\lambda = 30$*) give the following root diagram.*

α^2	α^4	α^6	α^8	α^{10}	α^{12}	α^{14}	α^{16}	α^{18}	α^{20}	α^{22}	1
x											
x	x	x	x	x		x	x			x	
x	x	x	x	x	x	x	x	x	x	x	x
x	x	x	x	x	x	x	x	x	x	x	x
		x			x			x			x
											x

Acknowledgment: The authors would like to thank the anonymous referees for very useful comments and suggestions that improved the presentation of this work.

References

[1] W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Providence, RI: American Mathematical Society, 1994.
[2] A. S. Castellanos, A. M. Masuda, L. Quoos, One– and two–point codes over Kummer extensions, IEEE Trans. Inform. Theory 62(9) (2016) 4867–4872.
[3] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry, Springer, New York, 1998.
[4] J. I. Farrán, C. Munuera, G. Tizziotti, F. Torres, Gröbner basis for norm–trace codes, J. Symb. Comput. 48 (2013) 54–63.
[5] A. Garcia, P. Viana, Weierstrass points on certain non–classical curves, Arch. Math. 46(4) (1986) 315–322.
[6] V. D. Goppa, Codes on algebraic curves, Dokl. Akad. Nauk SSSR 259(6) (1981) 1289–1290.
[7] V. D. Goppa, Algebraic–geometric codes, Izv. Akad. Nauk SSSR Ser. Mat. 46(4) (1982) 762–781.
[8] C. Heegard, J. Little, K. Saints, Systematic encoding via Gröbner bases for a class of algebraic–geometric Goppa codes, IEEE Trans. Inform. Theory 41(6) (1995) 1752–1761.
[9] J. W. P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton University Press, Princeton, 2008.
[10] T. Høholdt, J. van Lint, R. Pellikaan, Algebraic geometry codes, in Handbook of Coding Theory, V. S. Pless, W. C. Huffman, R. A. Brualdi (Eds.), v. 1, Elsevier, Amsterdam, 1998, 871–961.
[11] S. Kondo, T. Katagiri, T. Ogihara, Automorphism groups of one–point codes from the curves $y^q + y = x^{q^r+1}$, IEEE Trans. Inform. Theory 47(6) (2001) 2573–2579.
[12] J. Little, K. Saints, C. Heegard, On the structure of Hermitian codes, J. Pure Appl. Algebra, 121(3) (1997) 293–314.
[13] G. L. Matthews, Weierstrass semigroups and codes from a quotient of the Hermitian curve, Des. Codes Cryptogr. 37(3) (2005) 473–492.

[14] A. Sepúlveda, G. Tizziotti, Weierstrass semigroup and codes over the curve $y^q + y = x^{q^r+1}$, Adv. Math. Commun. 8(1) (2014) 67–72.
[15] H. Stichtenoth, Algebraic Function Fields and Codes, Springer–Verlag, Berlin, 1993.