On Weierstrass semigroups and one-point algebraic geometry codes

J.I. Farrán *

Departamento de Matemática Aplicada a la Ingeniería
E.T.S. Ingenieros Industriales – Universidad de Valladolid
Paseo del Cauce s/n - 47011 Valladolid – SPAIN
e-mail: ignfar@eis.uva.es

Abstract. We present two different algorithms to compute the Weierstrass semigroup at a point P together with functions for each value in this semigroup from a plane model of the curve. The first one works in a quite general situation and it is founded on the Brill-Noether algorithm. The second method works in the case of P being the only point at infinity of the plane model, what is very usual in practice, and it is based on the Abhyankar-Moh theorem, the theory of approximate roots and an integral basis for the affine algebra of the curve. This last way is simpler and has an additional advantage: one can easily compute the Feng-Rao distances for the corresponding array of one-point algebraic geometry codes, this thing be done by means of the Apéry set of the Weierstrass semigroup. Everything can be applied to the problem of decoding such codes by using the majority scheme of Feng and Rao.
Key words – algebraic curves, singular plane models, Brill-Noether algorithm, integral basis algorithm, Weierstrass semigroups, Apéry set, approximate roots, Abhyankar-Moh theorem, algebraic geometry codes and Feng-Rao distance.

1 Introduction

Feng and Rao introduced in [8] a majority scheme for the so called *one-point algebraic geometry codes*, what gives nowadays the most efficient decoding algorithm for algebraic geometry codes. Moreover, this procedure corrects up to half the so called *Feng-Rao designed minimum distance*, that is a lower bound for the minimum distance of these codes which is better that the *Goppa designed minimum distance*.

However, this idea is not new, since Goppa himself suggested in [10] that one can use the Weierstrass semigroup at the point P in order to obtain a lower bound of the Goppa distance for the one-point code $C_\Omega(D, mP)$. This was explicitly stated for example in [9]. Since, by definition, the Feng-Rao distance is closely related to the Weierstrass semigroup, one can look for lower bounds for such distance by using properties of this semigroup. In addition, and from "decoding

* Partially supported by DIGICYT PB94-1111-C02-01

reasons", the knowledge of the corresponding rational functions associated to the semigroup is also desirable.

More precisely, let $\tilde{\chi}$ be a non-singular projective algebraic curve defined over a finite field $\mathbb{F}$ such that $\tilde{\chi}$ is irreducible over $\overline{\mathbb{F}}$. In order to define the so called algebraic geometry codes (AG codes in short), take $\mathbb{F}$-rational points $P_1, \ldots, P_n$ on the curve and a $\mathbb{F}$-rational divisor G having disjoint support with the divisor $D \doteq P_1 + \ldots + P_n$, and then consider the linear well-defined maps

$$\begin{array}{c} ev_D \ : \ \mathcal{L}(G) \longrightarrow \mathbb{F}^n \\ f \mapsto (f(P_1), \ldots, f(P_n)) \end{array}$$

$$\begin{array}{c} res_D \ : \ \Omega(G-D) \longrightarrow \mathbb{F}^n \\ \omega \mapsto (res_{P_1}(\omega), \ldots, res_{P_n}(\omega)) \end{array}$$

where the $\mathbb{F}$-vector spaces of finite dimension

$$\mathcal{L}(H) \doteq \{f \in \mathbb{F}(\tilde{\chi}) \mid (f) + H \geq 0\} \cup \{0\}$$

$$\Omega(H) \doteq \{\omega \in \Omega(\tilde{\chi}) \mid (\omega) \geq H\} \cup \{0\}$$

are defined for any $\mathbb{F}$-rational divisor H on $\tilde{\chi}$. Thus one defines the linear codes

$$C_L \equiv C_L(D,G) \doteq Im(ev_D)$$

$$C_\Omega \equiv C_\Omega(D,G) \doteq Im(res_D)$$

The above constructed codes have asymptotically excellent parameters, namely they are the only known family of codes whose parameters are asymptotically better than the Varshamov-Gilbert bound, provided that q is a square and $q \geq 49$ (see [19]), and this is the main reason to study such codes. The length of both codes is obviously n, and one has $(C_\Omega) = C_L^\perp$ by the *residues theorem*. On the other hand, given D and G as above there exists a differential form ω such that $C_L(D,G) = C_\Omega(D, D-G+(\omega))$ and thus it suffices to deal with the codes of type C_Ω.

Thus, denote by $k = k(C)$ and $d = d(C)$ respectively the dimension over $\mathbb{F}$ and the minimum distance of the linear code $C = C_\Omega(D,G)$, $d(C)$ being the minimum value of non-zero entries of a non-zero vector of C. If $2g-2 < deg\, G < n$, the Riemann-Roch formula gives the estimates

$$\begin{cases} k = n - deg\, G + g - 1 \\ d \geq deg\, G + 2 - 2g \doteq d^* \end{cases}$$

where d^* is called Goppa distance of C (see [20] for further details).

The above estimates only depend on the degree of G, assumed that $\tilde{\chi}$ and n are fixed. This leads us to consider the special case $G = mP$, P being a $\mathbb{F}$-rational point of the curve which is not in the support of the divisor D. In this case, the so called one-point AG codes $C_m \doteq C_\Omega(D, mP)$ can be decoded by the majority scheme of Feng and Rao, which yields so far the most efficient decoding algorithm for this kind of codes (see [8]).

In order to implement this decoding method, one has to fix for every non-negative integer i a function f_i in $\mathbb{F}(\tilde{\chi})$ with an only pole at P of order i for those values of i for which it is possible, i.e. for i in the Weierstrass semigroup $\Gamma = \Gamma_P$ of $\tilde{\chi}$ at P. For a received word $\mathbf{y} = \mathbf{c} + \mathbf{e}$, where $\mathbf{c} \in C_m$, one can consider the unidimensional and bidimensional syndromes respectively given by

$$s_i(\mathbf{y}) \doteq \sum_{k=1}^{n} e_k \, f_i(P_k)$$

$$s_{i,j}(\mathbf{y}) \doteq \sum_{k=1}^{n} e_k \, f_i(P_k) \, f_j(P_k)$$

Notice that the set $\{f_i \mid i \leq m, \;\; i \in \Gamma\}$ is actually a basis for $\mathcal{L}(mP)$ and hence

$$C_m = \{\mathbf{y} \in \mathbb{F}^n \mid s_i(\mathbf{y}) = 0 \;\text{ for }\; i \leq m\}$$

Thus we can calculate $s_i(\mathbf{y})$ for $i \leq m$ from the received word $\mathbf{y}$ as $s_i(\mathbf{y}) = \sum_{k=1}^{n} y_k \, f_i(P_k)$, and such syndromes are called *known*.

In fact, it is well-known that if one had a high enough number of syndromes $s_{i,j}(\mathbf{y})$ for $i + j > m$ we could know the emitted word $\mathbf{c}$, and all the above syndromes can be computed by a majority voting (see [8] and [17]). The complexity of this algorithm is lower than the usual algorithms for general AG codes, and moreover the Weierstrass semigroup at P gives an estimate for $d(C)$ which is better than the Goppa bound. Such bound is the so called Feng-Rao distance, defined by

$$\delta_{FR}(m) \doteq \min\{n_s \mid s \in \Gamma \;\text{ and }\; s \geq m\}$$

where $n_s \doteq \sharp\{(i,j) \in \Gamma \times \Gamma \mid i + j = s\}$ for every $s \in \Gamma$.

Apart from finding all the closed singular points and all the $\mathbb{F}$-rational points of χ, what can be done by means of Gröbner bases computation, and also apart from computing the order of a rational function at a rational point and evaluating such function at this point if possible, what can be done for instance from the resolution tree of a plane model of the curve at such point by successive blowing-ups (see [12]), the main problem in practice is the computation of Γ and the functions f_i achieving the values of the semigroup Γ in order to carry out the Feng-Rao procedure.

Our aim is just to solve this last problem from the knowledge of a (possibly singular) plane model for the smooth curve by using geometric techniques, that is, from a geometric point of view. More precisely, in section **2** we study a method based on the Brill-Noether algorithm, which works in a quite general situation, and in section **3** we study an alternative method for the case of P being the only point at infinity of the plane model, which is founded on the Abhyankar-Moh theorem. This second method is not so general but it is more simple, and has the advantage of computing the Feng-Rao distance in an effective way. We conclude the paper giving in section **4** two examples where we compare both methods.

2 Weierstrass semigroups and adjoints

For a given plane curve χ, the computation of a basis for $\mathcal{L}(G)$, G being a rational divisor over $\tilde{\chi}$, is reduced, by the Brill-Noether theorem, to compute bases for spaces of adjoints of a suitable degree n. In fact, Goppa himself already mentioned in [10] the Brill-Noether theory as a way to construct AG codes in general. This theory can be done effective from the desingularization of χ, lazy parametrizations of the rational branches at all the singular points of the plane curve and testing virtual passing conditions (see [6], or [11] for an alternative method).

Now, in order to compute the Weierstrass semigroup Γ_P at P and a rational function f_l with a unique pole at P of order l for any fixed $l \in \Gamma_P$, we need not actually carry out the whole mentioned algorithm until we get a basis of $\mathcal{L}(mP)$ for a suitable m, but we can determine such semigroup and those functions by using only a part of the steps of the algorithm, as you can see in [7]. However, since the explicit description of all the steps of this algorithm and their effective solution would take long, we will give a procedure which assumes such a basis has been previously computed.

First of all, we need a bound $\tilde{l}$ for the values in Γ_P which will be used in the Feng and Rao procedure (see [8]). Then, assume that a basis $\{h_1, \ldots, h_s\}$ of $\mathcal{L}(\tilde{l}P)$ over $\mathbb{F}$ has been already computed, and that $\tilde{l}$ is not a gap. We give a triangulation method which works by induction on the dimension s as follows:

(1) Compute the pole orders $\{-\upsilon_P(h_i)\}$ at P, and assume that the functions $\{h_i\}$ are ordered so that these pole orders are increasing in i.

(2) At least the function h_s satisfies $-\upsilon_P(h_s) = \tilde{l}$ and we set $f_{\tilde{l}} \doteq h_s$. If any other h_j satisfies the same condition, there exists a non-zero constant λ_j in $\mathbb{F}$ such that $-\upsilon_P(h_j - \lambda_j h_s) < \tilde{l}$; then we change such functions h_j by $g_j \doteq h_j - \lambda_j h_s$ and set $g_k \doteq h_k$ for all the others. The result now is obviously another basis $\{g_1, \ldots, g_s\}$ of $\mathcal{L}(\tilde{l}P)$ over $\mathbb{F}$ but with only one function $g_s = f_{\tilde{l}}$ whose pole at P has maximum order $\tilde{l}$.

(3) Since the functions g_i are linear independent over $\mathbb{F}$ and $-\upsilon_P(g_i) < \tilde{l}$ for $i < s$, one has obtained a basis $\{g_1, \ldots, g_{s-1}\}$ of $\mathcal{L}(l'P)$ over $\mathbb{F}$, where l' denotes the largest non-gap such that $l' < \tilde{l}$. But now the dimension is $s-1$ and we can continue by induction.

The result of the above procedure is a function f_l for each non-gap $l \leq \tilde{l}$, and in fact it can be used to compute the Weierstrass semigroup up to an integer $\tilde{l}$, since the maximum gap l' such that $l' \leq \tilde{l}$ is just $\max\{-\upsilon_P(h_1), \ldots, -\upsilon_P(h_s)\}$, in the above notations, and so on by induction.

The limitation of this general method is just the computation of the Feng-Rao distance, what is in general a complex problem of arithmetic semigroups. If we compute an arbitrary generator system (for example, the set of all the primitive elements of Γ_P , which is always contained in the set of the fist $g+2$ non-gaps, as you can see in [16]), the problem is the effective description of the elements of Γ_P in terms of such generators, which is not even unique in general. As we

will see later, this problem becomes easier by considering special generators, but then we do not have in general a reasonable bound for the largest element in such system, unless the semigroup is a special one. This leads us to consider an alternative way to compute Weierstrass semigroups, when P is the only branch at infinity of a plane model, and where the Abhyankar-Moh theorem together with the theory of Apéry systems allows us to compute easily the Feng-Rao distance.

3 Weierstrass semigroups and approximate roots

Let $\tilde{\chi}$ be again a non-singular projective algebraic curve defined over a finite field $\mathbb{F}$ and which is absolutely irreducible. Let χ be now a plane model for $\tilde{\chi}$, and assume that the hypothesis

(H1) χ has a unique branch at infinity

is satisfied, i.e. there exist a birational morphism

$$n \,:\, \tilde{\chi} \to \chi \subseteq \mathbb{P}^2$$

and a line $L \subset \mathbb{P}^2$ defined over $\mathbb{F}$ such that $L \cap \chi$ consists of only one point P and $\tilde{\chi}$ has only one branch at P. Notice that both P and the branch at P are defined over the underlying finite field $\mathbb{F}$, since χ does. Thus there is only one point of $\tilde{\chi}$ over P, which will be denoted by $\overline{P}$.

Set $\tilde{\Upsilon} = \tilde{\chi} \setminus \{\overline{P}\}$ and $\Upsilon = \chi \setminus \{P\}$. One has the two following additive subsemigroups of $\mathbb{N}$:

$$\begin{aligned} \Gamma_P &\doteq \{-v_{\overline{P}}(f) \mid f \in \mathcal{O}_{\tilde{\chi}}(\tilde{\Upsilon})\} \\ S_P &\doteq \{-v_{\overline{P}}(f) \mid f \in \mathcal{O}_{\chi}(\Upsilon)\} \end{aligned}$$

Notice that Γ_P is just the Weierstrass semigroup of $\tilde{\chi}$ at $\overline{P}$ and it contains S_P , but they are different unless the curve χ is non-singular in the affine part. Moreover, $\mathbb{N} \setminus \Gamma_P$ has g elements, g being the genus of $\tilde{\chi}$, and $\Gamma_P \setminus S_P$, which is also finite, will be computed below.

The first question to solve is the description of the semigroup S_P . In order to do that, we state the Abhyankar-Moh theorem, where the hypothesis

(H2) *char* $\mathbb{F}$ does not divide either $deg\,\chi$ or $e_P(\chi)$

is assumed. This result provides us with a set of generators for S_P with nice arithmetic properties (see [1] or [15]).

Theorem 3.1 (Abhyankar-Moh) *Assumed that (H1) and (H2) are satisfied by χ, then there exist an integer h and a sequence of integers $\delta_0, \ldots, \delta_h \in S_P$ which generate S_P such that:*

(I) *$d_{h+1} = 1$ and $n_i > 1$ for $2 \leq i \leq h$, where $d_i \doteq g\,c\,d\ (\delta_0, \ldots, \delta_{i-1})$ for $1 \leq i \leq h+1$ and $n_i \doteq d_i/d_{i+1}$ for $1 \leq i \leq h$.*

(II) *$n_i\delta_i$ is in the semigroup generated by $\delta_0, \ldots, \delta_{i-1}$ for $1 \leq i \leq h$.*
(III) *$n_i\delta_i > \delta_{i+1}$ for $1 \leq i \leq h-1$.*

Such semigroups are a particular case of telescopic semigroups, and their main arithmetic property is that every $n \in S_P$ can be easily written in an unique way in the form

$$n = \sum_{i=0}^{h} \lambda_i \delta_i \qquad [\star]$$

with $\lambda_0 \geq 0$ and $0 \leq \lambda_i < n_i$ for $1 \leq i \leq h$ (see [14] or [15]). Apéry in [4] and Angermüller in [3] worked with a slightly different semigroup, that is the semigroup of values of a branch. The type of semigroup in this case is very similar to the given by the Abhyankar-Moh theorem, but with the property

$$(\mathbf{III})^* \ n_i\delta_i < \delta_{i+1} \text{ for } 1 \leq i \leq h-1$$

instead of **(III)**.

Now we will say how to obtain these generators of S_P in a constructive way together with functions in $B \doteq \mathcal{O}_\chi(\Upsilon)$ having poles of order equal to those generators (and hence one will have functions in B with poles of order any element in S_P by using the arithmetic properties of such generators). For it, we need first the concept of approximate root.

Definition 3.2 *Let S be a ring, $G \in S[\mathrm{Y}]$ a monic polynomial of degree e and $F \in S[\mathrm{Y}]$ a monic polynomial of degree n with $e|n$. Then G will be called an approximate b-th root of F if $deg\,(F - G^b) < n - e = e\,(b-1)$.*

Now the main remark is that for every monic polynomial $F \in S[\mathrm{Y}]$ of degree n and for every b divisor of n which is a unit in S, there exists a unique approximate b-th root of F, and it can be computed very efficiently (see [7]).

Thus, let the affine plane model of the curve given by the equation

$$F = F(\mathrm{X}, \mathrm{Y}) = \mathrm{Y}^m + a_1(\mathrm{X})\,\mathrm{Y}^{m-1} + \ldots + a_m(\mathrm{X})$$

and suppose that $char\,\mathbb{F}$ satisfies the assumption of the Abhyankar-Moh theorem. Up to a change of variables in the form $\mathrm{X}' = \mathrm{X} + \mathrm{Y}^n$, $\mathrm{Y}' = \mathrm{Y}$, we can actually assume that $char\,\mathbb{F}$ does not divide the total degree m of χ. On the other hand, denote the approximate d-th root of F with respect to the coefficient ring $S = \mathbb{F}[\mathrm{X}]$ by $app(d, F)$. Thus, the so called *algorithm of approximate roots* computes the generators given by the Abhyankar-Moh theorem as follows:

$$F_0 = \mathrm{X}\,,\ \delta_0 = d_1 = m\,,\ F_1 = \mathrm{Y}\,,\ \delta_1 = deg_{\mathrm{X}} Res_{\mathrm{Y}}(F, F_1)$$

$$n > 1 \ \Rightarrow \ \left[\begin{array}{l} d_n = g\,c\,d\,(\delta_0, \delta_1, \ldots, \delta_{n-1}) \\ F_n = app(d_n, F) \\ \delta_n = deg_{\mathrm{X}} Res_{\mathrm{Y}}(F, F_n) \end{array}\right.$$

The procedure stops at the first $h \geq 1$ with $d_{h+1} = d_{h+2}$, what happens just when $d_{h+1} = 1$, since the point at infinity is unibranch (see [2] and [7]).

As a consequence, the generators of S_P given by the Abhyankar-Moh theorem and the corresponding functions can be easily computed in terms of approximate roots of F and resultants of polynomials. In particular, we can compute a rational function with an only pole at P of order n for every $n \in S_P$. In fact, if $n = \sum_{i=0}^{h} \lambda_i \delta_i$ with $\lambda_0 \geq 0$ and $0 \leq \lambda_i < n_i$ for $1 \leq i \leq h$, then $f_n = \prod_{i=0}^{h} F_i^{\lambda_i}$ is the searched function, where F_i are the polynomials which are obtained in the algorithm of approximate roots. In particular, this also allows us to compute a basis of the space $\mathcal{L}(lP)$ for every $l \in \Gamma_P$.

Now the remaining part of the method is the computation of $\Gamma_P \setminus S_P$ with the corresponding functions, what can be done effective by means of the following

Lemma 3.3 *Let A and B be the respective affine coordinate $\mathbb{F}$-algebras of $\tilde{\Upsilon}$ and Υ, i.e. $A = \mathcal{O}_{\tilde{\chi}}(\tilde{\Upsilon})$ and $B = \mathcal{O}_{\chi}(\Upsilon)$; then one has:*

$$\sharp(\Gamma_P \setminus S_P) = dim_{\mathbb{F}}(A/B)$$

Proof:

Take a basis $\{h_1, \ldots, h_l\}$ of A/B over $\mathbb{F}$, which can be calculated either in algebraic terms with the aid of the *integral basis algorithm* (see [13] or [18]) or in geometric terms from the desingularization of the affine part of the curve χ. Now we will show a *triangulation procedure* to find the values in $\Gamma_P \setminus S_P$ as well as functions which provide these values.

Set $B^i \doteq B + \mathbb{F}h_1 + \ldots + \mathbb{F}h_i$, for $0 \leq i \leq l$; we will proceed by induction, so let $0 \leq i < l$ and suppose we have found functions $g_1, \ldots, g_i$ which are linearly independent over $\mathbb{F}$ with

$$\Gamma_P^i \doteq S_P \cup \{-v_{\overline{P}}(g_1), \ldots, -v_{\overline{P}}(g_i)\} \subseteq \Gamma_P$$
$$-v_{\overline{P}}(g_j) \notin \Gamma_P^{i-1}$$
$$B + \mathbb{F}g_1 + \ldots + \mathbb{F}g_i = B^i$$

Now look at h_{i+1}; if $-v_{\overline{P}}(h_{i+1}) \notin \Gamma_P^i$, then set $g_{i+1} = h_{i+1}$ and go on.
Otherwise, there exists $f \in B^i$ with

$$v_{\overline{P}}(h_{i+1}) = v_{\overline{P}}(f)$$
$$-v_{\overline{P}}(h_{i+1} - f) < -v_{\overline{P}}(h_{i+1})$$

Thus we can repeat the process with $h_{i+1} - f$ replacing to h_{i+1} ; since $h_{i+1} \notin B^i$, one obtains in a finite number of steps a function g_{i+1} such that

$$g_{i+1} \equiv h_{i+1} \pmod{B^i} \quad \text{and} \quad -v_{\overline{P}}(g_{i+1}) \notin \Gamma_P^i$$

At the end of the procedure l different elements in $\Gamma_P \setminus S_P$ will be added, and then $\sharp(\Gamma_P \setminus S_P) \geq dim_{\mathbb{F}}(A/B)$. The equality follows immediately from the formula $A = B^l = B + \mathbb{F}g_1 + \ldots + \mathbb{F}g_l$.

□

In order to complete this section, we show how to calculate the Feng-Rao distance from the above computations. First we have to present some basic tools for arbitrary semigroups.

Definition 3.4 *Let $S \subseteq \mathbb{N}$ a semigroup with $\sharp(\mathbb{N} \setminus S) < \infty$ and $0 \in S$; for $m \in S$ define*

$$\delta_{FR}(m) \doteq min\{N_s \mid s \geq m, \ \ s \in S\}$$

where $N_s \doteq \sharp\{(a,b) \in S^2 \mid a+b=s\}$ for every $s \in S$.

Definition 3.5 *Let $S \subseteq \mathbb{N}$ a semigroup with the same hypothesis as in the previous definition; for $n \in S \setminus \{0\}$ define the Apéry set of S related to n as the set whose elements are the numbers*

$$a_i \doteq min\{m \in S \mid m \equiv i \ (mod \ \ n)\}$$

for $0 \leq i \leq n-1$ [2].

In the sequel, the index i will be considered as an element in $\mathbb{Z}/(n)$. Thus, one has a disjoint union

$$S = \bigcup_{i=0}^{n-1} (a_i + n\mathbb{N})$$

and therefore the set $\{a_1, \ldots, a_{n-1}, n\}$ is a generator system for the semigroup S, which is called the Apéry (generator) system of S related to n.

Moreover, if $i, j \in \mathbb{Z}/(n) \equiv \mathbb{Z}_n$ then $a_i + a_j = a_{i+j} + \alpha_{i,j} n$ with $\alpha_{i,j} \geq 0$, by definition of the Apéry set. With this notation, every $m \in S$ can be written in a unique way as $m = a_i + ln$, with $i \in \mathbb{Z}_n$ and $l \geq 0$; so we can associate to m two *coordinates* $(i,l) \in \mathbb{Z}_n \times \mathbb{N}$.

Apéry *relations* are very useful to compute N_m . In fact, for $0 \leq i \leq n-1$ and $h \geq 0$ one can define $B_i^{(h)} \doteq \sharp\{\alpha_{k,i-k} \leq h \mid k \in \mathbb{Z}_n\}$ and then one has the following result.

Proposition 3.6 $\quad N_m = B_i^{(0)} + B_i^{(1)} + \ldots + B_i^{(l)}$

Proof :

If $\alpha_{k,i-k} = h \leq l$, it has been considered $l-h+1$ times in the sets defining $B_i^{(h)}, B_i^{(h+1)}, \ldots, B_i^{(l)}$, but also the equality $l_1 + l_2 = l - \alpha_{k,i-k}$ holds for $l-h+1$ possible pairs l_1, l_2 .

□

Thus, N_m is *increasing in* l, and it suffices to calculate the *minimum in* i in order to obtain the corresponding Feng-Rao distance, according to the following result.

[2] We could actually remove $a_0 = 0$ since it does not add any information about S.

Theorem 3.7 *With the above notations, for each $j \in \mathbb{Z}_n$ take $m_j = a_j + t_j n$, where t_j is the minimum integer such that $t_j \geq max\left(\frac{a_i - a_j}{n} + l, 0\right)$. Then one has*

$$\delta_{FR}(m) = min\{N_{m_j} \mid j \in \mathbb{Z}_n\}$$

Proof :

The formula is quit clear if one realizes that m_j is the minimum element of S with first Apéry coordinate equal to j such that $m_j \geq m$, using the above remark on the number N_m .

□

Thus, computing the Feng-Rao distance is easy if we have the Apéry set related to an element of an arbitrary semigroup. This gives an effective algorithm to compute the Feng-Rao distance of a Weierstrass semigroup when computed by the method given in this section, because of the two following remarks:

(i) The Apéry set of the semigroup S_P related to $m = \delta_0 = deg\,\chi$ is just the set of all the elements of the form $\sum_{k=1}^{h} \lambda_k \delta_k$ with $0 \leq \lambda_k < n_k = d_k/d_{k+1}$ for $1 \leq k \leq h$, since using the property $[\star]$ one has that all these elements are different modulo m, minimum in S with this condition and the number of such elements is exactly m.

(ii) Now the Apéry set related to $m = deg\,\chi$ for the Weierstrass semigroup $\Gamma_P = S_P + b_1\mathbb{N} + \ldots + b_l\mathbb{N}$ where $l = dim_{\mathbb{F}}(A/B)$ and b_i being computed as in lemma 3.3 , and the corresponding Apéry relations, can be easily obtained from those of S_P in at most l steps, each of them involving only the elements $a_j + \lambda\, b_k$ with $0 \leq j \leq n-1$ and $0 \leq \lambda \leq n-1$.

4 Examples and conclusions

The choice of the method to use in order to compute a Weierstrass semigroup depends on the situation. More precisely, the Brill-Noether method works in a general situation, but the implementation is complicate and it does not give a nice description of the semigroup (namely, an Apéry system in order to calculate the Feng-Rao distance of certain one-point AG code). On the other hand, the Abhyankar-Moh method gives such a description of Γ_P and the algorithm works in a very simple way, but it requires some additional hypothesis on the plane model: it must have an only rational branch P at infinity which is defined over the base field $\mathbb{F}$ and the characteristic of $\mathbb{F}$ must not divide at the same time to the degree of the plane model and the multiplicity of P, what is not always fulfilled. If moreover the plane model has no other singular points at the affine part the curve, the algorithm of approximate roots directly yields the Weierstrass

semigroup, and then the algorithm can be very easily implemented (for instance, such a programme takes a few lines in AXIOM code). Anyway, the complement of this semigroup requires the previous computation of a certain integral basis, what is equivalent to the desingularization of the affine part of the plane model, but what follows from such basis by means of a simple triangulation procedure. We will briefly illustrate these ideas with two examples.

Example 4.1 *Consider the affine plane curve* $F(\mathrm{X},\mathrm{Y}) = \mathrm{Y}^9 + \mathrm{Y}^8 + \mathrm{XY}^6 + \mathrm{X}^2\mathrm{Y}^3 + \mathrm{Y}^2 + \mathrm{X}^3$ *defined over* $\mathbb{F}_2$*, with only one branch at infinity* $P = (1:0:0)$*. The algorithm of approximate roots yields*

$$F_0 = \mathrm{X}\,,\ \delta_0 = d_1 = 9\,,\ F_1 = \mathrm{Y}$$

$$\delta_1 = deg_{\mathrm{X}} Res_{\mathrm{Y}}(F,\mathrm{Y}) = 3\,,\ d_2 = g\,c\,d\,(9,3) = 3$$

$$F_2 = app(3,F) = \mathrm{Y}^3 + \mathrm{Y}^2 + \mathrm{Y} + \mathrm{X} + 1$$

$$\delta_2 = deg_{\mathrm{X}} Res_{\mathrm{Y}}(F,F_2) = 8\,,\ d_3 = g\,c\,d\,(9,3,8) = 1$$

thus $h = 2$ *and* $S_P = \langle 9,3,8\rangle$*.*

On the other hand, according to the lemma 3.3, take a $\mathbb{F}_2$*-basis for* A/B

$$h_1 = \frac{\mathrm{Y}(1+\mathrm{Y}^6)}{\mathrm{X}+\mathrm{Y}^3} \quad h_2 = \frac{\mathrm{Y}(1+\mathrm{Y}^6)}{(\mathrm{X}+\mathrm{Y}^3)(\mathrm{Y}^2+\mathrm{Y}+1)}$$

$$h_3 = \frac{\mathrm{X}^2+\mathrm{Y}^6}{\mathrm{Y}^2+\mathrm{Y}+1} \quad h_4 = \frac{\mathrm{Y}^2(1+\mathrm{Y}^3)(\mathrm{Y}^2+\mathrm{Y}+1)}{\mathrm{X}+\mathrm{Y}^3}$$

The values at P *of this functions are* $-\upsilon_P(h_1) = 13 \notin S_P$*,* $-\upsilon_P(h_2) = 7 \notin \Gamma_P^1$*,* $-\upsilon_P(h_3) = 10 \notin \Gamma_P^2$ *and* $-\upsilon_P(h_4) = 13 \in \Gamma_P^3$*. Then change* h_4 *by*

$$g_4 = h_4 + h_1 = \frac{\mathrm{Y}(1+\mathrm{Y}^3)(\mathrm{Y}^2+\mathrm{Y}+1)}{\mathrm{X}+\mathrm{Y}^3}$$

and now $-\upsilon_P(g_4) = 10 \in \Gamma_P^3$*, so still one has to take the function*

$$g_4 = h_4 + h_1 + h_3 = \frac{\mathrm{Y}(1+\mathrm{Y}^3)(\mathrm{Y}^4+\mathrm{Y}^2+1) + (\mathrm{X}+\mathrm{Y}^3)^3}{(\mathrm{X}+\mathrm{Y}^3)(\mathrm{Y}^2+\mathrm{Y}+1)}$$

and now $-\upsilon_P(g_4) = 4 \notin \Gamma_P^3$*. Hence, the Weierstrass semigroup at* P *is*

$$\Gamma_P = \{0,3,\mathbf{4},6,\mathbf{7},8,9,\mathbf{10},11,12,\mathbf{13},14,\ldots\}$$

Unfortunately, there are examples where this method cannot be applied, and then the Brill-Noether method helps to compute Γ_P and the functions, even though it cannot compute in general the Feng-Rao distance.

Example 4.2 *Let χ be the Klein quartic over $\mathbb{F}_2$ given by the equation*

$$F(\mathrm{X},\mathrm{Y},\mathrm{Z}) = \mathrm{X}^3\mathrm{Y} + \mathrm{Y}^3\mathrm{Z} + \mathrm{Z}^3\mathrm{X} = 0$$

whose adjunction divisor is $\mathcal{A} = 0$, since χ is non-singular. We are going to compute now the Weierstrass semigroup at $P = (0:0:1)$, which is not the only one at infinity. Thus, by means of the Brill-Noether algorithm we compute a $\mathbb{F}_2$-basis of $\mathcal{L}(7P)$

$$\{h_1 = 1, h_2 = \frac{\mathrm{Z}}{\mathrm{Y}}, h_3 = \frac{\mathrm{Z}(\mathrm{Y}^2+\mathrm{YZ}+\mathrm{Z}^2)}{\mathrm{X}^2\mathrm{Y}}, h_4 = \frac{\mathrm{Z}^2(\mathrm{Y}+\mathrm{Z})}{\mathrm{X}^2\mathrm{Y}}, h_5 = \frac{\mathrm{Z}^3}{\mathrm{X}^2\mathrm{Y}}\}$$

By using Hamburger-Noether expansions at P, one computes the pole order of these functions at such point

$$-v_P(h_1) = 0, -v_P(h_2) = 3, -v_P(h_3) = -v_P(h_4) = -v_P(h_5) = 7$$

Thus, we take $f_7 = h_5$ and replace $h_4 = h_4 + h_5 = \dfrac{\mathrm{Z}^2}{\mathrm{X}^2}$ and $h_3 = h_3 + h_5 = \dfrac{\mathrm{Z}(\mathrm{Y}+\mathrm{Z})}{\mathrm{X}^2}$. Now the pole orders are

$$-v_P(h_1) = 0, -v_P(h_2) = 3, -v_P(h_3) = -v_P(h_4) = 6$$

and then we take $f_6 = h_4$. Thus, by replacing $h_3 = h_3 + h_4 = \dfrac{\mathrm{YZ}}{\mathrm{X}^2}$ we obtain now three different pole orders

$$-v_P(h_1) = 0, -v_P(h_2) = 3, -v_P(h_3) = 5$$

and we can stop. In particular, we have computed the Weierstrass semigroup, since we know the three [3] *Weierstrass gaps $\{1, 2, 4\}$.*

References

1. S.S. Abhyankar, *Lectures on expansion techniques in Algebraic Geometry*, Tata Institute of Fundamental Research, Bombay (1977).
2. S.S. Abhyankar, *Irreducibility criterion for germs of analytic functions of two complex variables*, Advances in Mathematics **74**, pp. 190-257 (1989).
3. G. Angermüller, *Die Wertehalbgruppe einer ebenen irreduziblen algebroiden Kurve*, Math. Zeit. **153**, pp. 267-282 (1977).
4. R. Apéry, *Sur les branches superlinéaires des courbes algébriques*, C.R. Acad. Sciences Paris **222**, pp. 1198-1200 (1946).
5. A. Campillo and J. Castellanos, *Curve singularities*, Univ. Valladolid, preprint (1997).
6. A. Campillo and J.I. Farrán, *Construction of AG codes from symbolic Hamburger-Noether expressions of plane curves*, Univ. Valladolid, preprint (1998).

[3] Notice that the genus of χ is $g = 3$.

7. J.I. Farrán, *Construcción y decodificación de códigos álgebro-geométricos a partir de curvas planas: algoritmos y aplicaciones*, Ph.D. thesis, Univ. Valladolid (1997).
8. G.L. Feng and T.R.N. Rao, *Decoding algebraic-geometric codes up to the designed minimum distance*, IEEE Trans. Inform. Theory **39**, pp. 37-45 (1993).
9. A. García, S.J. Kim and R.F. Lax, *Consecutive Weierstrass gaps and minimum distance of Goppa*, J. Pure Appl. Algebra **84**, pp. 199-207 (1993).
10. V.D. Goppa *Geometry and codes*, Kluwer Academic Publishers (1988).
11. G. Haché, *Construction effective des codes géométriques*, Ph.D. thesis, Univ. Paris 6 (1996).
12. G. Haché and D. Le Brigand, *Effective construction of algebraic geometry codes*, IEEE Trans. Inform. Theory **41**, pp. 1615-1628 (1995).
13. M. van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*, Maple V Release 4 share library, preprint (1996).
14. C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inform. Theory **41**, pp. 1720-1732 (1995).
15. H. Pinkham, *Séminaire sur les singularités des surfaces (Demazure-Pinkham-Teissier)*, Cours donné au Centre de Math. de l'École Polytechnique (1977-1978).
16. S.C. Porter, B.-Z. Shen and R. Pellikaan, *On decoding geometric Goppa codes using an extra place*, IEEE Trans. Inform. Theory **38**, pp. 1663-1676 (1992).
17. S. Sakata, H.E. Jensen and T. Høholdt, *Generalized Berlekamp-Massey decoding of algebraic-geometric codes up to half the Feng-Rao bound*, IEEE Trans. Inform. Theory **41**, pp. 1762-1768 (1995).
18. B.M. Trager, *Integration of algebraic functions*, Ph.D. thesis, Dept. of EECS, Massachusetts Institute of Technology (1984).
19. M.A. Tsfasman, *Goppa codes that are better than Varshamov-Gilbert bound*, Prob. Peredachi Inform. **18**, pp. 3-6 (1982).
20. M.A. Tsfasman and S.G. Vlăduţ, *Algebraic-geometric codes*, Math. and its Appl., vol. 58, Kluwer Academic Pub., Amsterdam (1991).