MATHEMATICS OF COMPUTATION
S 0025-5718(01)01390-4
Article electronically published on December 4, 2001

SYMBOLIC HAMBURGER-NOETHER EXPRESSIONS OF PLANE CURVES AND APPLICATIONS TO AG CODES

A. CAMPILLO AND J. I. FARRÁN

ABSTRACT. In this paper, we consider some practical applications of the symbolic Hamburger-Noether expressions for plane curves, which are introduced as a symbolic version of the so-called Hamburger-Noether expansions. More precisely, we give and develop in symbolic terms algorithms to compute the resolution tree of a plane curve (and the adjunction divisor, in particular), rational parametrizations for the branches of such a curve, special adjoints with assigned conditions (connected with different problems, like the so-called Brill-Noether algorithm), and the Weierstrass semigroup at P together with functions for each value in this semigroup, provided P is a rational branch of a singular plane model for the curve. Some other computational problems related to algebraic curves over perfect fields can be treated symbolically by means of such expressions, but we deal just with those connected with the effective construction and decoding of algebraic geometry codes.

1. Introduction

There are several classical problems in the theory of algebraic curves which are interesting from a computational point of view. This paper is basically addressed to solve, in a symbolic way, two of them which become fundamental in some practical applications, as for instance in the theory of algebraic geometry codes (AG codes in short). The first one is related to plane curves, and it consists of computing adjoints of fixed degree with extra passing conditions. The resolution of this problem requires in particular a good description of the desingularization process of the plane curve χ, and the computation of its *adjuntion divisor* $\mathcal{A}$ as a consequence. This is usually treated in the literature with the aid of blowing-ups and Puiseux expansions. Blowing-ups are classically used to describe the resolution of singularities, and Puiseux expansions (when available) are used in this context for finding local parametrizations for any branch of χ, which are needed to impose local conditions on polynomials for being adjoints with base conditions. The second problem is the computation of the Weierstrass semigroup of a smooth curve $\tilde{\chi}$ at a certain rational point P, together with a rational function $f_l \in \mathbb{F}(\tilde{\chi})$ regular outside P and achieving a pole at P of order l, for each l in this semigroup. We solve this second problem with the aid of the adjuntion theory for plane curves, so that we assume the knowledge of a singular plane birational model χ for the smooth curve $\tilde{\chi}$.

Received by the editor October 13, 1999 and, in revised form, December 26, 2000.
2000 *Mathematics Subject Classification.* Primary 14Q05; Secondary 11T71.
Key words and phrases. Algebraic curves, singular plane models, desingularization, symbolic Hamburger-Noether expressions, adjoints, virtual passing conditions, Weierstrass semigroups, AG codes.
Both authors are partially supported by DIGICYT PB97-0471.

The objective of this paper is to give a complete symbolic-computation treatment of these two basic problems. Our approach is based on very classical ideas. First, we consider Hamburger-Noether expansions from a symbolic viewpoint. More precisely, we introduce in Section 2 the so-called symbolic Hamburger-Noether expressions, which will provide us with both all the information on the desingularization process (this is detailed in Section 3) and (symbolic) parametrizations for all their branches. Hamburger-Noether expansions are developed in [1] for the case of irreducible curve singularities over algebraically closed fields. Here we will need not only the symbolic version but also the case of reduced plane curve singularities over perfect fields in general. In this way, we avoid the use of both blowing-ups and Puiseux expansions, and we explain the advantages of this fact in the practical applications.

In order to compute adjoints with extra passing conditions, we use in Section 4 the ideas of the so-called *principle of discharge* due to Enriques in [6] (see [4] and [22] for a modern treatment). The problem of computing Weierstrass semigroups is approached in Section 5 in similar terms, i.e., the adjuntion theory of plane curves can be applied to give an algorithm to compute this semigroups and the corresponding functions. In both problems, the solution becomes effective by using the symbolic Hamburger-Noether expressions. Thus, the algorithms that we present are derived from the properties of adjoint divisors and classical theories by Hamburger-Noether and Enriques. These algorithms have been implemented by Ch. Lossen (University of Kaiserslautern) and the second author (see [7]) in the computer algebra system SINGULAR [12], created by Greuel, Pfister and Schönemann.

All the results of this paper stand for (singular) plane curves defined over a perfect field $\mathbb{F}$ (for example, any field of characteristic zero, any field $\mathbb{F}$ of characteristic $p > 0$ such that $\{x^p \mid x \in \mathbb{F}\} = \mathbb{F}$ and, in particular, any finite field). This assumption is typical in algebraic geometry as well as in the theory of algebraic function fields, and it is essential in this paper since dropping this requirement would imply that most of the results are false, especially those related to any calculation in an extension of the ground field. For example, in order to compute spaces of adjoints with base conditions which are defined over $\mathbb{F}$, one would like that there exists a basis consisting only of adjoints defined over $\mathbb{F}$, and this is not true if $\mathbb{F}$ is not a perfect field. In the same way, Hamburger-Noether expansions are available only if the ground field is perfect.

For the particular case of finite fields, our results can be applied to the theory of algebraic geometry codes. These codes were introduced by Goppa in [9], and their construction from any smooth algebraic projective curve $\tilde{\chi}$ defined over a finite field $\mathbb{F}$ can be reduced to evaluating rational functions in vector spaces $\mathcal{L}(G)$ at certain rational points, G being a rational divisor over $\mathbb{F}$ (details are given in Section 6). Besides, with the motivation of the codes, some effective algorithms related to algebraic curves have been adapted for their practical use in coding theory. In this way, it is Goppa himself who first proposed in [10] the use of the Brill-Noether algorithm to construct AG codes, i.e., to compute a vector basis $\mathcal{L}(G)$. This algorithm computes such a basis in terms of adjoints of certain degree with concrete assigned conditions, which corresponds to our first basic problem. Since then, several other papers like [14], [15], [19] or [21] were published on the same subject.

On the other hand, good codes also need to have good decoding algorithms. Since the beginning of the 90's several decoding methods have been developed (see [18] for a survey on this matter). The most efficient one is based on the majority voting test of Feng and Rao (see [8]). This method requires the previous computation of the Weierstrass semigroup of $\tilde{\chi}$ at a certain rational point P, together with a rational function $f_l \in \mathbb{F}(\tilde{\chi})$ regular outside P and achieving a pole at P of order l, for each l in this semigroup (cf. Section 6), which corresponds to our second basic problem. We solve this problem in Section 5 in terms of plane curves.

2. Symbolic Hamburger-Noether expressions of plane curve singularities

In this section, we introduce the symbolic Hamburger-Noether expressions for plane curve singularities. For this, we fix in the sequel an arbitrary perfect field $\mathbb{F}$ and an absolutely irreducible projective algebraic plane curve χ defined over $\mathbb{F}$. For a closed point P of χ with local ring $R = \mathcal{O}_{\chi,P}$ we denote by a (rational over $\mathbb{F}$) branch of χ at P any maximal prime ideal of $\overline{R}$, where $\overline{R}$ denotes the semilocal ring given by the integral closure of R in its quotient field, i.e., the semilocal ring of the normalization of χ at the neighbourhood of P. The datum of such a maximal ideal is equivalent to giving a minimal prime ideal of $\widehat{R}$, the completion with respect to the maximal ideal of R (see [23] for the details). Rational branches can also be characterized in terms of parametrizations, as described below.

Assume that we have chosen an affine chart containing the point P, and let $A = \mathbb{F}[\mathrm{X}, \mathrm{Y}]/(f(\mathrm{X}, \mathrm{Y}))$ be the affine ring of coordinates, $f(\mathrm{X}, \mathrm{Y}) = 0$ being the affine equation of the curve in this chart. Regarding P as a nonzero prime ideal of A, one has $R = A_P$, where A_P is the localized ring of A at the prime ideal P, and there is a natural $\mathbb{F}$-algebra embedding $k(P) \hookrightarrow \widehat{R}$, $k(P)$ being the *residue field* of P (i.e., the quotient ring of R modulo its maximal ideal). For practical reasons, one can actually write $k(P) \cong K \doteq \mathbb{F}[\mathrm{Z}]/(Q(\mathrm{Z}))$ for an irreducible polynomial $Q \in \mathbb{F}[\mathrm{Z}]$, i.e., we can say that K is a *symbolic extension* of $\mathbb{F}$. Thus, by enlarging (if necessary) the field $\mathbb{F}$ by its extension K, and up to a translation in $K[\mathrm{X}, \mathrm{Y}]$, we can assume that P is the origin, the defining ideal of P being then (X, Y). After this initial enlarging, the branches that we will consider are rational over K, and K is again a perfect field. With this notation, one has $\widehat{R} \cong K[[\mathrm{X}, \mathrm{Y}]]/(f(\mathrm{X}, \mathrm{Y}))$, and hence there exists a natural morphism $K[[\mathrm{X}, \mathrm{Y}]] \to \widehat{R}$. This allows us to introduce the following

Definition 2.1. In the above conditions, a parametrization of χ at P related to the coordinates X, Y is a K-algebra morphism

$$\rho \ : \ K[[\mathrm{X}, \mathrm{Y}]] \to F[[t]]$$

continuous for the (X, Y)-adic and the t-adic topologies, such that $\mathrm{Im}(\rho) \not\subseteq F$ and $\rho(f) = 0$, where K is a symbolic extension of the base field $\mathbb{F}$ which is isomorphic to the residue field of P, F is a finite extension of K and t is an indeterminate. It is equivalent to giving formal series $x(t), y(t) \in F[[t]]$ with at least one nonidentically zero such that $f(x(t), y(t)) \equiv 0$.

One can associate to each parametrization ρ the rational branch given by the minimal prime ideal $\mathfrak{p} = \ker(\widehat{\rho})$, where $\widehat{\rho} \ : \ \widehat{R} \to F[[t]]$ is the natural morphism induced by ρ. Thus, we say that ρ is a parametrization of the rational branch given by $\mathfrak{p}$. If $\varphi \in K[[\mathrm{X}, \mathrm{Y}]]$ is a generator of $\ker(\rho)$ (this ideal is principal, according to Krull's theory), then φ is a factor of f seen as a power series in $K[[\mathrm{X}, \mathrm{Y}]]$. Thus, one can see that rational branches correspond one-to-one to irreducible factors of the power series $f(\mathrm{X},\mathrm{Y})$ in the ring $K[[\mathrm{X},\mathrm{Y}]]$, and such factors are uniquely determined up to a unit. The equality $\varphi(x(t),y(t))=0$ for a factor φ of f checks that the parametrization corresponds to the branch given by the factor φ.

We say that another parametrization $\sigma : K[[\mathrm{X},\mathrm{Y}]] \to F'[[u]]$ is derived from ρ, and it is denoted by $\sigma \succ \rho$, if there exists a formal series $t(u) \in F'[[u]]$ with positive order and a K-algebra continuous morphism $\beta : F[[t]] \to F'[[u]]$ with $\beta(t)=t(u)$, such that $\sigma = \beta \circ \rho$. One has that $\succ$ is a partial preorder, and we say that two parametrizations ρ and σ are equivalent if $\sigma \succ \rho$ and $\rho \succ \sigma$. Thus, a parametrization ρ is called *primitive* if it is minimal with respect to the partial preorder $\succ$. Primitive parametrizations corresponding to each branch are uniquely determined modulo equivalence, and moreover, the field extension $F|K$ in such parametrizations is also minimal (that is, $\rho(\mathrm{X})$ and $\rho(\mathrm{Y})$ are not both in $F'[[t]]$ for some field F' with $K \subseteq F' \subset F$ and $F' \neq F$). One actually has that rational branches at P are in bijection with equivalence classes of primitive parametrizations at P. Thus, we can call a *rational parametrization* to any equivalence class of primitive parametrizations, and it is easy to see that such a parametrization is "rational" in the usual sense that it is invariant under the action of the Galois group of the extension $\overline{K}|K$. In particular, there always exist rational parametrizations associated to the rational branches (details in [1]). By choosing a parametrization representing each rational branch, one obtains a choice which can be called the *standard set of rational parametrizations* at P, and our next aim is the effective computation of such a set by means of the so-called Hamburger-Noether expansions.

Although a general definition could be given for arbitrary singular curves, we are studying only the case of plane curves in order to get effective computations. Thus, let $\rho : K[[\mathrm{X},\mathrm{Y}]] \to F[[t]]$ be a parametrization of the plane curve χ defined at the point P, F being a finite extension of K and so of the base field $\mathbb{F}$. One can actually consider R (the local ring of χ at P) as a subring of $F[[t]]$, the images of X and Y being a minimal system of generators of the maximal ideal of R. With this notation we introduce the following

Definition 2.2. The *Hamburger-Noether expansion* of χ at P for the rational branch given by ρ is a finite sequence $\mathbb{D}$ of expressions in the variables $Z_{-1}, Z_0, \ldots, Z_r$ of the form

$$Z_{-1} = a_{0,1}Z_0 + a_{0,2}Z_0^2 + \ldots + a_{0,h_0}Z_0^{h_0} + Z_0^{h_0}Z_1,$$

$$Z_0 = a_{1,2}Z_1^2 + a_{1,3}Z_1^3 + \ldots + a_{1,h_1}Z_1^{h_1} + Z_1^{h_1}Z_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$Z_{r-2} = a_{r-1,2}Z_{r-1}^2 + a_{r-1,3}Z_{r-1}^3 + \ldots + a_{r-1,h_{r-1}}Z_{r-1}^{h_{r-1}} + Z_{r-1}^{h_{r-1}}Z_r,$$

$$Z_{r-1} = \sum_{i\geq 1} a_{r,i}Z_r^i,$$

where r is a nonnegative integer, $a_{j,i} \in F$, $a_{k,1}=0$ if $k>0$, h_j are positive integers and moreover

$$\varphi(Z_0(Z_r), Z_{-1}(Z_r)) = 0 \quad \text{in} \quad F[[Z_r]]$$

if $\varphi \in K[[\mathrm{X},\mathrm{Y}]]$ is a generator of the prime ideal $\ker(\rho)$.

The existence of such expansions and the finiteness of the number of lines is referred to [1] and [24]. In fact such an expansion $\mathbb{D}$ always gives a rational parametrization equivalent to ρ if we consider $\mathrm{X} \equiv \mathrm{Z}_0$ and $\mathrm{Y} \equiv \mathrm{Z}_{-1}$ as a function of the local parameter $s = Z_r$ by successive substitutions. Moreover, $\mathbb{D}$ depends only on the branch given by ρ and the choice of the parameters x, y in R given by the images of X, Y under ρ. Thus, for X and Y fixed the (finite) set of all the possible nonequivalent Hamburger-Noether expansions form a standard set of rational parametrizations of χ at P.

Remark 2.3. The role played by the Hamburger-Noether expansions in arbitrary characteristic is just the same as that classically played by the Puiseux expansions in characteristic 0, which are given by

$$X(t) = \alpha t^{\nu},$$

$$Y(t) = \sum_{i \geq \nu} \lambda_i t^i,$$

where $\alpha \in F^*$ and $\lambda_i \in F$. The main obstacles for using Puiseux expansions in both theoretical and algorithmic purposes are basically the following:

- They do not always exist in positive characteristic.
- When such expansions exist, the problem of making them primitive is not at all trivial (see [1] or [5]).
- The parameter t is not (in general) a rational function over the given curve.

Avoiding the above three obstacles is the main reason why we use Hamburger-Noether expansions instead of Puiseux expansions. Moreover, the procedure for computing the Hamburger-Noether expansions provides at the same time a description of the desingularization of a plane curve which is simpler than the usual presentation in terms of blowing-ups, as we will see in the next section.

Now, we show how to compute the Hamburger-Noether expansions without having, a priori, any local parametrization of the branch, but only with the aid of the Newton diagram of the local equation of χ at P. We will do it for the case of only one rational branch at P for the sake of simplicity, but the method also works for several branches (in the reduced case) because of the fact that the Newton polygon would be the collection of those of each branch joined together with increasing slope (see [24] for further details).

From now on we will assume without loss of generality that $K = \mathbb{F}$, so that the ground field will be denoted by $\mathbb{F}$. Let χ be given in affine coordinates by the local equation $f(\mathrm{X}, \mathrm{Y}) = \sum_{\alpha,\beta \geq 0} c_{\alpha\beta} \mathrm{X}^{\alpha} \mathrm{Y}^{\beta} = 0$, f being an irreducible polynomial in $\mathbb{F}[\mathrm{X}, \mathrm{Y}]$. Assume that we want to study the point $P = (0, 0)$ and that there is only one rational branch at the origin defined over $\mathbb{F}$. Implicitly, we are assuming for simplicity that the point is rational over $\mathbb{F}$, i.e., the residue field is $K = \mathbb{F}$, in order to be able to translate it to the origin, but this is not a serious restriction, since otherwise we can substitute for $\mathbb{F}$ an initial symbolic extension K of $\mathbb{F}$. Then we consider the Newton diagram of f

$$D(f) \doteq \{(\alpha, \beta) \mid c_{\alpha\beta} \neq 0\}$$

and we call the *Newton polygon* of f (at the origin) the set of all the bounded segments of the convex hull of $D(f) + \mathbb{R}_+^2$, and it will be denoted by $P(f)$.

Excluding the trivial cases where the curve is one of the coordinate axes, let l (respectively n) be the minimum integer such that $(l,0) \in D(f)$ (respectively $(0,n) \in D(f)$). We can obviously assume that $n \leq l$. In this case, the Newton polygon consists of just one segment with nonzero slope and extremes $(l,0)$ and $(0,n)$. If $\Delta = P(f)$ is the Newton polygon we can define

$$L(\mathrm{X},\mathrm{Y}) \doteq \sum_{(\alpha,\beta)\in\Delta} c_{\alpha\beta}\mathrm{X}^{\alpha}\mathrm{Y}^{\beta}.$$

One obviously has $L(\mathrm{X},\mathrm{Y}) = c\,D(\mathrm{X},\mathrm{Y})$ for some $c \in \mathbb{F}^*$ and some $D(\mathrm{X},\mathrm{Y})$ which is monic in Y and defined over $\mathbb{F}$. Moreover

$$D(\mathrm{X},\mathrm{Y}) = \prod_{j=1}^{d} (\mathrm{Y}^{n'} - \delta_j \mathrm{X}^{l'})^e$$

for some $\delta_j \in \overline{\mathbb{F}}^*$, where $ed = \gcd(l,n)$. Then the *characteristic polynomial* of Δ is given by

$$\Phi_{\Delta}(\lambda) \doteq \prod_{j=1}^{d} (\lambda - \delta_j).$$

It is an irreducible polynomial over $\mathbb{F}$ (that is, the δ_j are conjugate to each other by the Galois group over $\mathbb{F}$). Moreover, one has $l = l'ed$ and $n = n'ed$, being $\gcd(l',n') = 1$.

If we write $l = qn + h$ with $0 \leq h < n$, we find one of the following two cases:

Case 1. $h = 0$, which implies $ed = n$, $l' = q$ and $n' = 1$. Thus write

$$a_{0,1} = \ldots = a_{0,l'-1} = 0, \quad \text{and} \quad a_{0,l'} = \delta$$

δ being a symbolic root of $\Phi_{\Delta}(\lambda)$. We mean by a symbolic root of $\Phi_{\Delta}(\lambda)$ that one substitutes for $\mathbb{F}$ the field $\mathbb{F}_1 = \mathbb{F}[\lambda]/(\Phi_{\Delta}(\lambda))$ and one takes as δ the residual class of λ in this field. Then, we get that the first line of the Hamburger-Noether expansion starts with

$$Z_{-1} = a_{0,l'} Z_0^{l'} + \ldots .$$

Then we transform f by

$$T_1(f,\delta,l') = f(\mathrm{X}, \mathrm{Y} + \delta\,\mathrm{X}^{l'}) = f_1(\mathrm{X},\mathrm{Y})$$

getting f_1 with a segment of extremes $(l_1,0)$ and $(0,n)$ as the Newton polygon, $l_1 > l$, and we iterate the process, taking into account that f_1 has the coefficients in the field $\mathbb{F}_1 = \mathbb{F}[\lambda]/(\Phi_{\Delta}(\lambda))$ and that it is irreducible over such field (notice that this process terminates immediately if there is no point of the form $(l_1,0)$).

Case 2. $h > 0$; in this case, the first line of the Hamburger-Noether expansion is just

$$Z_{-1} = Z_0^q Z_1.$$

Now, since the polynomial $U(f,l,n) = f(\mathrm{Y}, \mathrm{X}\,\mathrm{Y}^q)$ is divisible by Y^{nq}, we can transform f by

$$T(f,l,n) = \frac{f(\mathrm{Y},\mathrm{X}\,\mathrm{Y}^q)}{\mathrm{Y}^{nq}} = f_1(\mathrm{X},\mathrm{Y}).$$

Thus the obtained Newton polygon Δ_1 has $(n,0)$ and $(0,h)$ as extremes, $h < n$, and its characteristic polynomial is $\Phi_{\Delta_1}(\lambda) = \lambda^e\,\Phi_{\Delta}(1/\lambda)$. Then we repeat the process, looking for the next line of the Hamburger-Noether expansion, identifying $T(f,l,n)\ \mathrm{X} \equiv \mathrm{Z}_1$ and $\mathrm{Y} \equiv \mathrm{Z}_0$.

If we find the case $h = 0$ consecutive times during the computation of the line $k+1$ of the Hamburger-Noether expansion, where $k \in \{0, 1, \dots, r-1\}$, we append the newly obtained result to the previous part of that line until we get the case $h > 0$, where we append the term $Z_k^q Z_{k+1}$ and change to the next line.

Hence, by applying a finite number of transformations of type T_1 or T, we get a trivial Newton polygon where either $\min(l,n) = 1$ or there is no point in the vertical axis, and the procedure stops. In this case one has all the lines of the Hamburger-Noether expansion except the last one. But then the equation $f(\mathrm{X},\mathrm{Y})$ is transformed into a polynomial $g(\mathrm{Z}_r, \mathrm{Z}_{r-1})$, g being defined over a field $\mathbb{F}'$ which is obtained by successive symbolic extensions of $\mathbb{F}$ and one has

$$\frac{\partial g}{\partial \mathrm{Z}_{r-1}}(0,0) \neq 0.$$

This means that one can obtain as many terms as needed of the last line of the Hamburger-Noether expansion from the polynomial $g(\mathrm{Z}_r, \mathrm{Z}_{r-1})$ as an implicit function (that is, by indeterminate coefficients), since this line represents Z_{r-1} as a formal series in the variable Z_r. Thus, we do not need in practice the data given by the (infinite) series of the last line of the Hamburger-Noether expansion, but only the (finite) data of the implicit equation g, which contains the same information. This data is what we call a *symbolic Hamburger-Noether expression*, that is

$$Z_{-1} = a_{0,1}Z_0 + a_{0,2}Z_0^2 + \ldots + a_{0,h_0}Z_0^{h_0} + Z_0^{h_0}Z_1,$$

$$Z_0 = a_{1,2}Z_1^2 + a_{1,3}Z_1^3 + \ldots + a_{1,h_1}Z_1^{h_1} + Z_1^{h_1}Z_2,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$Z_{r-2} = a_{r-1,2}Z_{r-1}^2 + a_{r-1,3}Z_{r-1}^3 + \ldots + a_{r-1,h_{r-1}}Z_{r-1}^{h_{r-1}} + Z_{r-1}^{h_{r-1}}Z_r,$$

$$g(Z_r, Z_{r-1}) = 0.$$

It can be computed in an effective way by the above method for every singular closed point of χ (initially written in a symbolic extension of the base field if such a point is not rational). Even more, we do all these computations in successive symbolic extensions of $\mathbb{F}$ instead of considering a sufficiently large extension of it, which in practice saves a lot of time. In summary, at the end of the above algorithm one obtains, even in positive characteristic, parametrizations which are rational, and such that the parameter $t = Z_r$ is a rational function over $\mathbb{F}[\mathrm{X},\mathrm{Y}]/(f)$.

In the case of several branches the characteristic polynomial is not irreducible and each branch corresponds to an irreducible factor of this polynomial and its corresponding symbolic root, proceeding as in the case of one branch with every factor in parallel. Hence, in the general case we have to add in each step of the previous algorithm a factorization procedure for the corresponding characteristic polynomial, which also has an effective solution. Each irreducible factor follows at least one of the rational branches, so that one has an algorithm in the form of a tree. Thus, the branches of the tree given by this algorithm correspond one-to-one to the branches of the curve at the point considered, and for each tree branch one has associated to it (as a byproduct of the algorithm) the symbolic Hamburger-Noether expression corresponding to the curve branch. The computation of Hamburger-Noether expansions is a known method and it has been implemented with the computer algebra system SINGULAR [12].

Remark 2.4. (i) The computation of the needed symbolic extensions of $\mathbb{F}$ requires factorization of polynomials in one variable, which has an effective solution in computational algebra.

(ii) In fact, we could apply the method to any computable perfect field $\mathbb{F}$, that is, when the operations in $\mathbb{F}$ are done in an effective way (for instance, when $\mathbb{F}$ is any field of algebraic numbers).

Example 2.5. Let χ be the projective plane curve over $\mathbb{F}_2$ given by

$$F(\mathrm{X},\mathrm{Y},\mathrm{Z}) = \mathrm{X}^{10} + \mathrm{Y}^8\mathrm{Z}^2 + \mathrm{X}^3\mathrm{Z}^7 + \mathrm{Y}\mathrm{Z}^9 = 0$$

with the only singular point $P = (0:1:0)$ which is rational over $\mathbb{F}_2$, being furthermore the unique point of χ at infinity. Take the local equation

$$f(\mathrm{X},\mathrm{Z}) = \mathrm{X}^{10} + \mathrm{X}^3\mathrm{Z}^7 + \mathrm{Z}^9 + \mathrm{Z}^2$$

of χ where P is the origin, and apply the Hamburger-Noether algorithm to this equation. With the above notation, one has $L(\mathrm{X},\mathrm{Z}) = \mathrm{Z}^2 + \mathrm{X}^{10} = (\mathrm{Z}+\mathrm{X}^5)^2$; thus $l = 10$, $l' = 5$, $n = e = 2$, $n' = d = 1$ and $q = 5$, in the case $h = 0$.

The characteristic polynomial is $\Phi(\lambda) = \lambda + 1$ and thus the symbolic root is just $\delta = 1$, i.e., we do not need to enlarge the base field $\mathbb{F}_2$. Hence, one has

$$a_{0,0} = \ldots = a_{0,4} = 0, \qquad a_{0,5} = 1$$

and we make the change

$$f_1(\mathrm{X},\mathrm{Z}) = f(\mathrm{X},\mathrm{Z}+\mathrm{X}^5) = \mathrm{Z}^2 + \mathrm{X}^{38} + \ldots$$

with $L(\mathrm{X},\mathrm{Z}) = (\mathrm{Z}+\mathrm{X}^{19})^2$ and thus $l = 38$, $l' = 19$, $n = e = 2$, $n' = d = 1$, $q = 19$ and again $h = 0$; one also has $\Phi(\lambda) = \lambda + 1$ and $\delta = 1$. Thus

$$a_{0,6} = \ldots = a_{0,18} = 0, \qquad a_{0,19} = 1$$

and we make the transform

$$f_2(\mathrm{X},\mathrm{Z}) = f_1(\mathrm{X},\mathrm{Z}+\mathrm{X}^{19}) = \mathrm{Z}^2 + \mathrm{X}^{45} + \ldots .$$

In this case, one has $L(\mathrm{X},\mathrm{Z}) = \mathrm{Z}^2 + \mathrm{X}^{45}$, obtaining $l = l' = 45$, $n = n' = 2$, $d = e = 1$ and $q = 22$, in the case $h = 1 > 0$ and we have to change the line in the Hamburger-Noether expansion without enlarging the base field. Now the transform to make is

$$f_3(\mathrm{X},\mathrm{Z}) = \frac{f_2(\mathrm{Z},\mathrm{X}\mathrm{Z}^{22})}{\mathrm{Z}^{44}} = \mathrm{Z} + \mathrm{X}^2 + \ldots$$

with the origin a nonsingular point of the new equation and the procedure ends with $r = 1$. Thus, the symbolic Hamburger-Noether expressions at P are

$$\left\{ \begin{array}{rcl} Z_{-1} & = & Z_0^5 + Z_0^{19} + Z_0^{22}Z_1, \\ g(Z_1,Z_0) & = & Z_1^9Z_0^{154} + Z_1^8Z_0^{151} + Z_1^8Z_0^{137} + Z_1Z_0^{130} + Z_0^{127} + Z_1^7Z_0^{113} \\ & & +Z_1^6Z_0^{110} + Z_0^{113} + Z_1^5Z_0^{107} + Z_1^4Z_0^{104} + Z_1^3Z_0^{101} + Z_1^6Z_0^{96} \\ & & +Z_1^2Z_0^{98} + Z_1Z_0^{95} + Z_1^4Z_0^{90} + Z_0^{92} + Z_1^2Z_0^{84} + Z_1^5Z_0^{79} \\ & & +Z_1^4Z_0^{76} + Z_0^{78} + Z_1Z_0^{67} + Z_1^4Z_0^{62} + Z_0^{64} + Z_0^{50} \\ & & +Z_1^3Z_0^{45} + Z_1^2Z_0^{42} + Z_1Z_0^{39} + Z_0^{36} + Z_1^2Z_0^{28} + Z_0^{22} \\ & & +Z_1Z_0^{18} + Z_0^{15} + Z_1Z_0^{11} + Z_0^8 + Z_1^2 + Z_0. \end{array} \right.$$

3. Normalization, resolution and adjunction via symbolic Hamburger-Noether expressions

The purpose of this section is the revision of some classical concepts taking into account the symbolic Hamburger-Noether expressions which have been introduced in the previous section. Thus, for a given plane curve χ one can consider its normalization, that is the proper birational morphism

$$\mathbf{n} : \tilde{\chi} \longrightarrow \chi,$$

where $\tilde{\chi}$ is the curve obtained by gluing together the affine charts given by the normalization of the affine graded $\mathbb{F}$-algebras A_U for all affine charts U of χ (see [17] for further details). The curve $\tilde{\chi}$ can be obtained as the blowing-up of the conductor, that is the sheaf of ideals locally given by

$$\mathcal{C}_\chi(U) \doteq \{f \in \overline{\mathcal{O}_\chi(U)} \mid f\,\overline{\mathcal{O}_\chi(U)} \subseteq \mathcal{O}_\chi(U)\}.$$

Nevertheless, it is better in practice to look at $\tilde{\chi}$ as successive blowing-ups of all the closed points of χ which are singular until we get a curve without singular points, since this approach can be explicitly described by equations. In each of those blowing-ups one has as a result the corresponding *strict transform* χ_i for $i \geq 0$ (starting from $\chi_0 = \chi$), defined as usual (see for example [15] or [17]). This process can be represented by a combinatorial object called the *resolution forest* $\mathcal{T}_\chi$, consisting of one *weighted oriented tree* for each singular closed point of χ, and which is constructed as follows:

1) The vertices represent the successive points which are obtained by blowing-up singular points of the successive strict transforms χ_i of χ until one gets a nonsingular point at the end of each branch of the process. Two such vertices p and q of one tree corresponding to the points P and Q are connected by an edge from p to q if Q is one of the points obtained by blowing-up P.
2) On each edge $\overrightarrow{pq}$ of the forest we put a weight $\rho_{pq} \doteq [k(Q) : k(P)]$, where $k(P)$ and $k(Q)$ are the corresponding residue fields of the local rings $\mathcal{O}_{\chi_i,P}$ and $\mathcal{O}_{\chi_{i+1},Q}$.
3) If p is the root of the tree corresponding to the singular point P of χ, then we put on p an initial weight $[k(P) : \mathbb{F}]$. On all the other vertices of the forest we can assign two alternative weights which are equivalent if we know the weights on the edges. In both cases one assigns to p a weight for each branch of the tree passing through p, where by a branch we denote any upper extremal point of the forest, and we say that a branch q passes through p when there is an oriented path from p to q in $\mathcal{T}_\chi$. Notice that such branches are in bijection with the rational branches at P of the corresponding curve obtained by blowing-up P, and also with the closed points over P of the normalization. The two alternative weights on p for each q are the following:
   (I) The *multiplicity* at P of the rational branch $\mathfrak{q}$ corresponding to q computed in the corresponding curve χ_P obtained by blowing-up χ, that is the multiplicity $e_{p,q}$ of the noetherian ring $\widehat{\mathcal{O}}_{\chi_P,P}/\mathfrak{q}$ of dimension 1 (denoting here by $\mathfrak{q}$ the corresponding minimal prime ideal of $\widehat{\mathcal{O}}_{\chi_P,P}$).
   (II) The *order* at P of the rational branch $\mathfrak{q}$, that is the number $m_{p,q} \doteq \min\{v_Q(f) | f \in \mathfrak{m}_{\chi_P,P}\}$, where $\mathfrak{m}_{\chi_P,P}$ is the maximal ideal of the local ring $\mathcal{O}_{\chi_P,P}$ and v_Q denotes the normalized valuation (that is, with $\mathbb{Z}$ as group of values) corresponding to Q regarded as a point of $\tilde{\chi}$. The

equivalence between both weights is given by the formula

$$m_{p,q}\,[k(Q):k(P)] = e_{p,q}.$$

Notice that the order is actually the multiplicity of each of the conjugate geometric branches lying over P, considering χ to be defined over the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$. By substituting $\overline{\mathbb{F}}$ for $\mathbb{F}$ one obtains another combinatorial object which is much more complex than the one described above and that has all weights on the edges equal to 1 and hence $m_{p,q} = e_{p,q}$. This object can be easily reconstructed from the rational object $\mathcal{T}_\chi$ and it does not show properly the structure of χ over $\mathbb{F}$; thus $\mathcal{T}_\chi$ is a more precise invariant of the normalization.

We will show now that from the computation of symbolic Hamburger-Noether expressions one gets, as a by-product, the desingularization of the curve (see [1] for more details). In fact, for simplicity consider again the case of only one rational branch. Let $f \in \mathbb{F}[\mathrm{X},\mathrm{Y}]$ be a local equation of χ at P, supposed rational and $P=(0,0)$ in the affine coordinates X,Y (otherwise we consider an initial symbolic extension K instead of $\mathbb{F}$). If we write $l = qn+h$ as in the previous section, then the first q *infinitely near* points $P = P_0, P_1, \ldots, P_{q-1}$ are rational over $\mathbb{F}$, with $P_i = (0,0)$, for $0 \le i \le q-1$, in the local affine coordinates $\{\mathrm{X}, \frac{\mathrm{Y}}{\mathrm{X}^i}\}$ at P_i.

If $h=0$, then P_q has the symbolic field $\mathbb{F}_1 = \mathbb{F}[\lambda]/(\Phi_\Delta(\lambda))$ as residue field, with $P_q = (0,0)$ in the local affine coordinates related to $\mathbb{F}_1$ given by $\{\mathrm{X}, \frac{\mathrm{Y}}{\mathrm{X}^q} - \delta\}$, δ being a symbolic root of the characteristic polynomial $\Phi_\Delta(\lambda)$.

If $h>0$, then the new coordinates are $\{\mathrm{Z}_1, \mathrm{Z}_0\}$, P_q is rational over $\mathbb{F}$ and $P_q = (0,0)$ in these coordinates, and $\mathrm{Z}_1 = 0$ is the exceptional divisor instead of $\mathrm{Z}_0 = 0$. Anyway, by doing the above changes of variables successively one easily gets the corresponding total, strict or virtual transform of any divisor.

With this notation, the edges $\overrightarrow{p_{i-1}p_i}$ of the resolution forest $\mathcal{T}_\chi$, p_j corresponding to P_j, have weight 1 either if $i<q$ or if $i=q$ and $h>0$, and weight d if $i=q$ and $h=0$. The value $e\cdot n'$ in each step is just the order of that branch at $P_0,\ldots,P_{q-1}$, and $n = d\cdot e\cdot n'$ is the multiplicity. The weights at P_q appear in the next step of the algorithm, where P_q plays the role of $P_0 = P$, and so on.

When one gets the trivial polygon by iterating this method, one obtains all the infinitely near points with all the weights of the combinatorial object $\mathcal{T}_\chi$. When the procedure ends, one has the coordinates $\{\mathrm{Z}_r, \mathrm{Z}_{r-1}\}$ and the local equation $g(\mathrm{Z}_r, \mathrm{Z}_{r-1})$, satisfying $\frac{\partial g}{\partial \mathrm{Z}_{r-1}}(0,0) \neq 0$. Doing s additional transformations of type T_1 one obtains the embedded resolution, with Z_r^s the initial form of $g(\mathrm{Z}_r, \mathrm{Z}_{r-1})$.

In the case of several branches, the resolution can be obtained taking into account that there are as many irreducible factors of the characteristic polynomial as infinitely near points in the exceptional divisor, and the corresponding symbolic roots yield suitable local coordinates for such points, that is, everything can be done, branch by branch, with an algorithm in the form of a tree.

Example 3.1. In Example 2.5, one obtains the resolution tree of χ at P as the sequence of points

$$P \equiv p_0 \to p_1 \to \ldots \to p_{21} \to p_{22} \equiv q$$

corresponding to rational points of multiplicity $e_{p_i,q} = 2$ if $i = 0, \ldots, 21$, and $e_{p_{22},q} = 1$, the weights of all the edges being 1 as the initial weight, since we have never enlarged the base field.

Remark 3.2. The above example shows how the computation of the symbolic Hamburger-Noether expressions to obtain the desingularization of a plane curve is simpler (in terms of effectiveness) than using just successive blowing-ups. In fact, the Hamburger-Noether method requires in this case just 3 transformations, compared to 22 blowing-ups. In general, each transformation in the Hamburger-Noether algorithm is equivalent to a sequence of blowing-ups, so that the number of polynomial transformations on the equation of the curve is smaller, and so the final complexity. In other words, sometimes one needs several blowing-ups in order to get something essentially new in the desingularization process, whereas in the Hamburger-Noether case something essential changes at every step of the algorithm, and so symbolic Hamburger-Noether expressions give a way to be more precise and effective in dealing with the resolution process of a plane curve. Besides, the Hamburger-Noether method gives an automatic way to select convenient coordinates at all the infinitely near points, which become good for further computations.

On the other hand, the additional work to obtain the desingularization tree from the Hamburger-Noether algorithm is not very hard, since it basically consists of reading the arithmetic data which have been already computed in the intermediate steps. The only important work would be the computation of all the intermediate strict transforms, when one essentially repeats all the sequence of blowing-ups, but in most of the applications one needs just the combinatorial process of the resolution and the final data of the process (i.e., those concerning the branches of the tree), and these data are essentially contained in the symbolic Hamburger-Noether expressions together with the resolution tree $\mathcal{T}_\chi$.

Finally, from a theoretical point of view, the Hamburger-Noether algorithm provides at the same time the desingularization tree and primitive parametrizations for the obtained rational branches. Such parametrizations are not intrinsically obtained from the blowing-up process.

Some useful information which one can derive from $\mathcal{T}_\chi$ is the adjunction divisor $\mathcal{A}$ of the singular plane curve χ, and hence the so-called adjoint divisors. The adjunction divisor of χ is nothing but the effective divisor given by the conductor ideal $\mathcal{C}_\chi$ on $\tilde{\chi}$ (notice that $\tilde{\chi}$ is the blowing-up of $\mathcal{C}_\chi$). It can be computed from the resolution forest as follows.

Let $q_1, \ldots, q_l$ be the branches of $\mathcal{T}_\chi$, and let $Q_1, \ldots, Q_l$ be the corresponding points of $\tilde{\chi}$, by identifying $\tilde{\chi}$ with χ_N. For each vertex $p \in \mathcal{T}_\chi$ set

$$e_p = \sum_{j=1}^{l} e_{p,q_j}$$

with the convention that $e_{p,q_j} = 0$ if the branch q_j does not pass through the vertex p. Then, the adjunction divisor is given by

$$\mathcal{A} = \sum_{j=1}^{l} \left(\sum_{p \in \mathcal{T}_\chi} m_{p,q_j} (e_p - 1) \right) Q_j .$$

In the sequel, we will denote $d_Q \doteq d_q \doteq \sum_{p\in\mathcal{T}_\chi} m_{p,q}(e_p-1)$. One has

$$\deg\,\mathcal{A} = \sum_{p\in\mathcal{T}_\chi} e_p(e_p-1)\deg\,P$$

since $\deg\,Q_j = \deg\,P\cdot[k(Q_j):k(P)]$ and $e_{p,q_j} = m_{p,q_j}\cdot[k(Q_j):k(P)]$ for p in the branch q_j.

Now if we want to give the definition of what an adjoint divisor is, we need first some notation. Let P be a closed point of the curve χ embedded in $\mathcal{S}=\mathbb{P}^2$ and consider the domains $R=\mathcal{O}_{\chi,P}$ and $\mathcal{O}=\mathcal{O}_{\mathcal{S},P}$. Thus, the conductor

$$\mathcal{C}_P = \mathcal{C}_{\overline{R}/R} \doteq \{z\in\overline{R} \mid z\,\overline{R}\subseteq R\}$$

is by definition an ideal in R and $\overline{R}$ at the same time. As an ideal of R, there exists another ideal $\mathfrak{A}_P$ containing the kernel of the natural morphism $\mathcal{O}\to R$ such that $\mathfrak{A}_P$ is applied onto $\mathcal{C}_P$ by this morphism. The ideal $\mathfrak{A}_P$ is called the ideal of *germs of adjoints* of χ at P over $\mathbb{F}$. In a global situation, the ideal of adjoints $\mathfrak{A}$ is defined as a sheaf of ideals of $\mathcal{O}_\mathcal{S}$ over $\mathcal{S}$ whose stalk at P is either $\mathfrak{A}_P$ when $P\in\chi$, or $\mathcal{O}_{\mathcal{S},P}$ otherwise. In other words, $\mathfrak{A}$ is the preimage of the conductor sheaf $\mathcal{C}_\chi$ under the natural morphism $\mathcal{O}_\mathcal{S}\to\mathcal{O}_\chi$. In fact, for $P\in\chi$ one has $\mathfrak{A}_P=\mathcal{O}_{\mathcal{S},P}$ if and only if P is nonsingular; hence $\mathfrak{A}$ has a finite support and can be given by the finite set of data $\{\mathfrak{A}_P \mid P\in\mathrm{Sing}\,(\chi)\}$.

On the other hand, with the above notation and following [3], for $P\in\mathcal{S}$ and $h\in\mathcal{O}_{\mathcal{S},P}$ with $e_P(h)\ge e_p-1$ given, denote by $H=\mathrm{div}(h)$ the divisor defined by h on the surface $\mathcal{S}$, and consider $\pi_P^*H=\mathrm{div}(\pi_P^*h)=(e_p-1)\,E_P+\tilde{H}$, where π_P denotes the blowing-up at P and E_P the exceptional divisor of π_P . Then $\tilde{H}$ is called the *virtual transform* of H (with respect to P and the weight e_p), and the multiplicity $\mu_q(h)\doteq e_q(\tilde{H})$ (for q proximate to p, that is, the corresponding point Q is in the strict transform of the exceptional divisor created in the blowing-up of the point P) is called the *virtual multiplicity* of h at q related to e_p-1. By induction, if one substitutes for the surface $\mathcal{S}$ the corresponding one at the inductive step, and by taking the successive virtual transforms related to the values e_r-1, one has in a similar way the concept of virtual multiplicity at any q in $\mathcal{T}_\chi$, where we take in successive steps the virtual multiplicity $\mu_r(h)$ instead of the value $e_p(h)$ taken in the first step. Then, one has

$$\mathfrak{A}_P = \{h\in\mathcal{O}_{\mathcal{S},P} \mid \mu_q(h)\ge e_q-1\ \ \forall q\ge p,\ \ q\in\mathcal{T}_\chi\}.$$

As a consequence, for an $\mathbb{F}$-rational divisor D on the surface $\mathcal{S}$ one has the following four equivalent ways of saying that D is an adjoint divisor:

(i) Adjoint by branches: if the intersection multiplicity of D and χ at every rational branch q of χ is at least the coefficient d_q that appears in the adjunction divisor $\mathcal{A}_\chi$.
(ii) Divisorial adjoint: if $\mathbf{N}^*D\ge\mathcal{A}$, where $\mathbf{N}=i\circ\mathbf{n}$, $\mathbf{n}$ the normalization of χ and i the embedding of χ in $\mathcal{S}$.
(iii) Arithmetic adjoint: if the local equation of D at every point $P\in\chi$ is in $\mathfrak{A}_P$.
(iv) Geometric adjoint: if the virtual multiplicity of D at every infinitely near point corresponding to $\mathcal{T}_\chi$ is greater than or equal to the effective multiplicity of the strict transform of χ at this point minus one.

Adjoints are useful for many purposes. One of them is to describe the vector space of finite dimension

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

for an arbitrary $\mathbb{F}$-rational divisor G on $\tilde{\chi}$, as derived from the classical Brill-Noether theorem. Assume that χ is given by the homogeneous polynomial $F \in \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2]$. Take a divisor G on $\tilde{\chi}$ that is rational over $\mathbb{F}$ and consider a form $H_0 \in \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2]$ of degree n, with $n \in \mathbb{N} \setminus \{0\}$, defined over $\mathbb{F}$, not divisible by F and satisfying

$$\mathbf{N}^* H_0 \geq G + \mathcal{A}.$$

Then, the *Brill-Noether theorem* states that

$$\mathcal{L}(G) = \{\frac{h}{h_0} \mid H \in \mathcal{F}_n, \ \ H \notin F \cdot \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2] \text{ and } \mathbf{N}^* H + G \geq \mathbf{N}^* H_0\} \cup \{0\},$$

where $h, h_0 \in \mathbb{F}(\chi)$ denote respectively the rational functions H, H_0 restricted on χ, and $\mathcal{F}_n \subset \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2]$ denotes the set of forms of degree n.

This result allows us to compute a basis of $\mathcal{L}(G)$ over $\mathbb{F}$ by means of an effective algorithm (see [15] for more details). Apart from the computation of $\mathcal{A}$, which can be done with the aid of the Hamburger-Noether algorithm, the main problem to solve in order to carry out the algorithm is the computation of a vector space of the form

$$\mathfrak{A}(R, n) \doteq \{H \in \mathcal{F}_n \ : \ F | H \text{ or } \mathbf{N}^* H \geq \mathcal{A} + R\} \cup \{0\},$$

where $R \geq 0$ is any rational divisor. This is just a problem of computing adjoints with passing conditions which will be studied in the next section, where the Hamburger-Noether expressions will again play an important role.

4. Computing adjoints with base conditions

We show in this section how to impose on a form H of given degree n to be an adjoint of the curve χ with extra passing conditions, these conditions given by a divisor R which is $\mathbb{F}$-rational and effective. This is what we call *adjoints with base conditions*, and it is founded on the classical ideas of Enriques [6] of testing passing conditions. This can be applied in particular to the computation of a vector basis of $\mathcal{L}(G)$ with the aid of the Brill-Noether algorithm.

In practice we know the polynomial $F(\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2) \in \mathbb{F}[\mathrm{X}_0, \mathrm{X}_1, \mathrm{X}_2]$ defining the absolutely irreducible curve χ in the projective plane, and we have the data of a divisor R that is effective and rational over $\mathbb{F}$, involving a finite number of rational branches of χ and their corresponding coefficients. We must first take a value of n such that there exists an adjoint of degree n which is not a multiple of the equation F of χ and satisfying

$$\mathbf{N}^* H_0 \geq \mathcal{A} + G,$$

that is, such that the vector space

$$\mathfrak{A}(R, n) \doteq \{H \in \mathcal{F}_n \ : \ F | H \text{ or } \mathbf{N}^* H \geq \mathcal{A} + R\} \cup \{0\}$$

is nonempty. You can find in [13] a bound for such an n.

In order to imposed the base condition, there are two ways to proceed. For the first one, assume that from the symbolic Hamburger-Noether expressions we have computed by lazy evaluation the rational parametrizations $(X(Z_r), Y(Z_r))$ given by the corresponding Hamburger-Noether expansions at every branch involved in the support of the adjunction divisor $\mathcal{A}$ and R.

The *Dedekind formula* allows us to find the coefficient d_q of $\mathcal{A}$ at the rational branch q, which is given by

$$d_q = \mathrm{ord}_t \left(\frac{f_Y(X(t),Y(t))}{X'(t)} \right) = \mathrm{ord}_t \left(\frac{f_X(X(t),Y(t))}{Y'(t)} \right)$$

$(X(t),Y(t))$ a rational parametrization of q (notice that either $X'(t) \neq 0$ or $Y'(t) \neq 0$). The algorithm to compute the symbolic Hamburger-Noether expressions provides us with as many terms of such a parametrization as we need to obtain the above orders in t, by successive substitution and lazy evaluation.

Now we consider the coefficient r_q of R at q, and thus the local condition at q imposed on H by the inequality $\mathbf{N}^* H \geq \mathcal{A} + R$ is given by

$$\mathrm{ord}_t\, h(X(t),Y(t)) \geq d_q + r_q,$$

h the local affine equation of H in terms of the coordinates X, Y at the corresponding point P. Again a suitable number of steps of the lazy evaluation suffices to describe the first $d_q + r_q$ monomials of the Taylor expansion of $h(X(t),Y(t))$ as a function of the indeterminate coefficients of H, whose vanishing gives the required linear conditions, taking all the possible branches q in the support of $\mathcal{A}$ and R.

The second way is just the imposition of *virtual passing conditions* through the infinitely near points of the *configuration* of resolution $\mathfrak{C}_\chi$ with virtual multiplicities $e_p - 1$, what also yields linear conditions on H. The resolution configuration $\mathfrak{C}_\chi$ stands here for the set of points P (at the successive blowing-ups) corresponding to the vertices $p \in \mathcal{T}_\chi$. Notice that from the symbolic Hamburger-Noether expressions one can derive not only the total information of $\mathfrak{C}_\chi$ but also the information on bigger configurations $\mathfrak{D}$ obtained by adding to $\mathfrak{C}_\chi$ finitely many points with multiplicity 1 at the end of every branch of $\mathcal{T}_\chi$. Furthermore, the algorithm to compute the symbolic Hamburger-Noether expressions also gives us the weights for the resolution tree and local coordinates at every infinitely near point, as we have seen in the previous section. On the other hand, we say that a homogeneous polynomial H passes (virtually) through a configuration $\mathfrak{D}$ of infinitely near points of χ with virtual multiplicities $\{\mu_P \mid P \in \mathfrak{D}\}$ if the virtual multiplicity of H at every point P of $\mathfrak{D}$ (as defined in Section 3) is greater than or equal to μ_P, generalizing the concept of geometric adjoint given in the section above.

The total number of imposed linear conditions is

$$\sum_{P \in \mathfrak{C}_\chi} \frac{e_p\,(e_p - 1)}{2} \deg\, P = \frac{1}{2} \deg\, \mathcal{A}$$

since the condition $\mu_p(h) \geq e_p - 1$ is equivalent to the vanishing of $\dfrac{e_p - 1}{2} e_p$ coefficients, which yields this number of conditions over a field isomorphic to the residue field $k(P)$, and thus $\dfrac{1}{2} e_p\,(e_p - 1)\,\deg\, P$ conditions over the base field $\mathbb{F}$. Moreover, such conditions are linear independent whenever $n \geq m - 3$, because of the *Noether adjunction theorem*, which is referred to the Section 5, and the virtual transform $\tilde{H}$ of H can be computed from the symbolic Hamburger-Noether expressions. Note that the first $e_p - 1$ terms of the Taylor expansion of $\tilde{H}(X(t),Y(t))$ vanish.

Now we must add to $\mathbf{N}^* H \geq \mathcal{A}$ the conditions given by R. If supp R does not contain any singular point (that is, the adjoint defined by H_0 passes through $\mathfrak{C}_\chi$

with actual multiplicities $e_p - 1$), then the condition $\mathbf{N}^*H \geq \mathcal{A} + R$ is equivalent to $\mathbf{N}^*H \geq \mathcal{A}$ and $\mathbf{N}^*H \geq R$ at the same time, and thus the method is just the same as before. This situation can be assumed if n is large enough, by a theorem of Serre about the vanishing of the cohomology, but in practice the estimate of such values of n is very hard and we will give an alternative method to proceed.

Denote by r_q the coefficient of R at the rational branch q, with $r_q \geq 0$ by assumption. We will show that $\mathbf{N}^*H \geq \mathcal{A} + R$ can also be described with virtual passing conditions on H. In fact, consider the configuration $\mathfrak{C}_\chi^{+,R}$ given by adding to $\mathfrak{C}_\chi$ the first r_q points of multiplicity 1 in the sequence of infinitely near points corresponding to the branch q, for all q in the support of R.

Recall that the condition $\mathbf{N}^*H \geq \mathcal{A} + R$ can be written in terms of the local conditions

$$(*) \qquad \mathrm{ord}_t\, h(X_q(t), Y_q(t)) \geq d_q + r_q$$

for each rational branch q in $\mathfrak{C}_\chi^{+,R}$, with $(X_q(t), Y_q(t))$ a rational parametrization corresponding to q. From the inequalities $(*)$ one gets the following result.

Proposition 4.1. *Under the above conditions, the inequality $\mathbf{N}^*H \geq \mathcal{A} + R$ is equivalent to the condition that the hypersurface defined by H passes through the points of $\mathfrak{C}_\chi^{+,R}$ with virtual multiplicities $e_p - 1$ if $p \in \mathfrak{C}_\chi$ and 1 if $p \in \mathfrak{C}_\chi^{+,R} \setminus \mathfrak{C}_\chi$.*

Proof. If $\mathbf{N}^*H \geq \mathcal{A} + R$, then $\mathbf{N}^*H \geq \mathcal{A}$, since $R \geq 0$. Thus, from the definition of $\mathcal{A}$ one obtains that H passes through the points $p \in \mathfrak{C}_\chi$ with virtual multiplicities $e_p - 1$. On the other hand, the formula $(*)$ shows that the virtual transform of H at the first point of multiplicity 1 corresponding to the branch q has intersection multiplicity at least r_q with the strict transform of this branch; hence, H passes through the last r_q points of $\mathfrak{C}_\chi^{+,R} \setminus \mathfrak{C}_\chi$ corresponding to q with virtual multiplicity 1.

Conversely, if H passes through the points of $\mathfrak{C}_\chi^{+,R}$ with the above virtual multiplicities, then $(*)$ is satisfied for any branch q in $\mathfrak{C}_\chi^{+,R}$. □

Remark 4.2. The above result is considered in [3] for the case $r_q = e_{\mathrm{N}(q),q} - 1$ studying the behaviour of the polar curve of a plane curve in characteristic 0. We have proved that in fact the result is also true in any characteristic and for arbitrary values of r_q whenever $r_q \geq 0$. Notice that (in total) one considers a number of linear conditions equal to $\frac{1}{2}\deg \mathcal{A} + \deg R$, but they may not be linearly independent.

Remark 4.3. The theory of Enriques on plane curves with assigned singularities or, in more modern terms, the theory of Zariski-Lipman on complete ideals, allows us to substitute the weights $e_p - 1$ in $\mathfrak{C}_\chi$ and 1 in $\mathfrak{C}_\chi^{+,R} \setminus \mathfrak{C}_\chi$ by other weights $\overline{e_p}$ over $\mathfrak{C}_\chi^{+,R}$ satisfying the so-called proximity inequalities, that is

$$\overline{e_p} \geq \sum_{r \to p} \overline{e_r} \qquad \forall p \in \mathfrak{C}_\chi^{+,R}.$$

This substitution can be done by means of a combinatorial algorithm known as the principle of discharge (see for instance [3]). This algorithm is combinatorial in the sense that one can describe it just in terms of the embedded resolution forest associated to the configuration $\mathfrak{C}_\chi^{+,R}$.

Remark 4.4. Notice that the r_q added points of multiplicity 1 in each branch q can be deduced in practice from the symbolic Hamburger-Noether expressions computing the first r_q terms of the Taylor expansion of the implicit function given by the polynomial $g(Z_r, Z_{r-1})$. As a consequence, everything in the current section can be carried out with the aid of the Hamburger-Noether algorithm given in the previous sections, instead of using the theory of blowing-ups, as usually.

5. Computing Weierstrass semigroups

In this section we show how to compute, for a given rational point P of the smooth curve $\tilde{\chi}$, the Weierstrass semigroup Γ_P consisting of the Weierstrass nongaps at P, together with a function f_l with a unique pole at P of order l, for each $l \in \Gamma_P$. As a motivation, this problem is closely related to the decoding procedure of Feng and Rao for algebraic-geometric codes (see [8]). The proposed problem can be easily solved under special conditions with the aid of the theory of approximate roots (see [2]), but the method that we propose here works in a quite general situation and it is based on the theory of adjoints. For this, we make use of the classical adjunction theorem.

Denote by $\mathcal{A}_n$ the set of adjoints of degree n of the curve χ embedded in $\mathbb{P}^2$ and denote $\mathbf{N} = i \circ \mathbf{n}$, $\mathbf{n}$ the normalization of χ and i the embedding of χ in $\mathbb{P}^2$. For every $D \in \mathcal{A}_n$ one can consider its *pull-back*, which is given by $\mathbf{N}^* D = \mathcal{A} + D'$ for certain D'. The *adjunction theorem*, due to Noether, says that if $n + 3 \geq \deg\,\chi$, the divisors $D' = \mathbf{N}^* D - \mathcal{A}$ for $D \in \mathcal{A}_n$ are exactly those in the complete linear system $|K_{\tilde{\chi}} + (n - m + 3)\, L|$, $K_{\tilde{\chi}}$ a canonical divisor on $\tilde{\chi}$, L the hyperplane section divisor and $m = \deg\,\chi$ (see [11] for details).

This result means that local adjunction conditions are linearly independent if imposed on divisors of large enough degree, and this independence is in fact global, that is, when imposed on all the points of χ at the same time. In particular, if $n = m - 3$, one obtains the following result.

Proposition 5.1. *For $n = m - 3$ one has an $\mathbb{F}$-isomorphism of complete linear systems*

$$\mathcal{A}_n \to |K_{\tilde{\chi}}|, \qquad D \mapsto \mathbf{N}^* D - \mathcal{A}.$$

Notice that this map is injective since $n < m$, and the dimension over $\mathbb{F}$ of the vector space of forms of dimension $m-3$ in three variables equals the arithmetic genus $p_a(\chi)$. But now the total number of linearly independent adjunction conditions is $\frac{1}{2}\deg\,\mathcal{A}$, and thus the formula of the geometric genus $g(\chi) = p_a(\chi) - \frac{1}{2}\deg\,\mathcal{A}$ can be seen as a problem of virtual conditions through the configuration of resolution $\mathfrak{C}_\chi$.

In this situation, assume that $G = lP$, where l is a nonnegative integer and P is a rational point of $\tilde{\chi}$, that is, a rational branch defined over $\mathbb{F}$ at a certain point of the curve χ. Then the Riemann-Roch formula can be applied to the divisors lP and $(l-1)\,P$, what yields the equality

$$(\ell(lP) - \ell((l-1)\,P)) - (i(lP) - i((l-1)\,P)) = 1,$$

with $0 \leq \ell(lP) - \ell((l-1)\,P) \leq 1$ and $-1 \leq i(lP) - i((l-1)\,P) \leq 0$. Therefore one has $l \notin \Gamma_P$ if and only if $l \geq 1$ and there exists a differential form which is regular on $\tilde{\chi}$ and with a zero at P of order $l-1$. Notice that $l \in \Gamma_P$ if $l \geq 2g$. From these remarks and Proposition 5.1 one can easily prove the following

Proposition 5.2. *Let $l \in \mathbb{Z}$ such that $1 \leq l \leq 2g-2$. Then:*

(a) *$l \notin \Gamma_P$ if and only if there exists a homogeneous polynomial H_0 of degree $m-3$ with $\mathbf{N}^* H_0 \geq \mathcal{A} + (l-1)P$ such that P is not in the support of the effective divisor $\mathbf{N}^* H_0 - \mathcal{A} - (l-1)P$.*

(b) *There exists $l' \geq l$ with $l' \notin \Gamma_P$ if and only if there exists a homogeneous polynomial H_0 of degree $m-3$ such that $\mathbf{N}^* H_0 \geq \mathcal{A} + (l-1)P$.*

As a consequence, the following result provides us with an effective method to do the preprocessing of one-point AG codes with the aid of plane models of curves, and it works in a quite general situation.

Theorem 5.3. *Under the same assumptions as above, there exists an algorithm founded in the theory of adjoints for computing the Weierstrass semigroup Γ_P together with functions f_l with a pole at P of order l and regular on $\tilde{\chi} \setminus \{P\}$, for all $l \in \Gamma_P$.*

Proof. (I) *Computing the Weierstrass semigroup*: Taking $G = (l-1)P$ instead of the divisor R in Proposition 4.1 and using the configuration $\mathfrak{C}_\chi^{+,G}$ one can impose the linear conditions given by $\mathbf{N}^* H \geq \mathcal{A} + (l-1)P$ on forms H of degree $m-3$, which are equivalent to virtual passing conditions through $q \in \mathfrak{C}_\chi$ with multiplicities $e_q - 1$ and through $q \in \mathfrak{C}_\chi^{+,G} \setminus \mathfrak{C}_\chi$ with multiplicity 1.

Then for l increasing from $l = 0$ (always in Γ_P) one imposes successively the linear conditions given by $\mathbf{N}^* H \geq \mathcal{A} + lP$, adding one condition in each step. Thus, the added condition given by the new l is linearly independent of the previous conditions, by using Proposition 5.2, if and only if $l \notin \Gamma_P$. All the g gaps of Γ_P, and hence the semigroup itself, are computed in at most $2g$ steps.

(II) *Computing the functions f_l*: There are two ways to proceed. One way is to compute the functions f_l for all $l \leq \tilde{l}$, $\tilde{l}$ a given upper-bound. The other way is to compute first a generator system for the Weierstrass semigroup and then to give the functions only for all l in such a system, with $\tilde{l}$ the largest generator. For practical reasons, this generator system may be the Apéry system related to a certain nonzero element e of the semigroup (usually the minimum) and then it suffices to consider $\tilde{l} = c + e - 1$, where c is the conductor of the semigroup. Such a generator systems has many advantages for further arithmetic computations (see [2]). Anyway, the method described below, which is a suitable application of the Brill-Noether algorithm, works in both cases.

(i) Compute a homogeneous polynomial H_0 not divisible by F of large enough degree n satisfying $\mathbf{N}^* H_0 \geq \mathcal{A} + \tilde{l}P$.

(ii) For any $l \in \Gamma_P$ with $l \leq \tilde{l}$, define R_l as the effective divisor such that $\mathbf{N}^* H_0 = \mathcal{A} + lP + R_l$. One obviously has that $R_{l-1} = R_l + P$. Thus, for decreasing l we can impose the conditions $\mathbf{N}^* H \geq \mathcal{A} + R_l$ by means of Proposition 4.1 in order to find a homogeneous polynomial $H_l \in \mathfrak{A}(R_l, n)$ not satisfying the condition $\mathbf{N}^* H_l \geq \mathcal{A} + R_{l-1}$.

(iii) Thus, the function $f_l = H_l / H_0$ restricted to χ is regular on $\tilde{\chi} \setminus \{P\}$ and has a pole at P of order l. □

Example 5.4. 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 nonsingular. We are going to compute the Weierstrass semigroup at $P=(0:0:1)$ with the above method.

Since P is nonsingular one easily obtains by lazy evaluation a local parametrization of χ at P given by

$$\begin{cases} X(t)=t^3+t^{10}+\ldots, \\ Y(t)=t. \end{cases}$$

Notice that every plane curve is adjoint to χ, since $\mathcal{A}=0$. Thus, in order to get the gaps of Γ_P one uses adjoints of degree $m-3=1$, whose generic equation is given by $H(\mathrm{X},\mathrm{Y},\mathrm{Z})=a\mathrm{X}+b\mathrm{Y}+c\mathrm{Z}$. Then, by substituting the first terms of the local parametrization at P we get

$$h(X(t),Y(t))=c+bt+at^3+at^{10}+\ldots$$

and proceed as in Theorem 5.3:

- $l=1$ is obviously the first gap, since $g=3>0$, but anyway it can also be checked by the method, since $l=0$ imposes no condition whereas $l=1$ imposes the condition $\mathrm{ord}_t\, h(X(t),Y(t))\geq 1$, which is equivalent to $c=0$.
- For $l=2$, the inequality $\mathrm{ord}_t\, h(X(t),Y(t))\geq 2$ is equivalent to the conditions $c=b=0$, which are linearly independent of those imposed by $l=1$, and thus $l=2$ is a new Weierstrass gap.
- If $l=3$, then $\mathrm{ord}_t\, h(X(t),Y(t))\geq 3$ is again equivalent to $c=b=0$. Thus the new condition depends on the previous one and $3\in\Gamma_P$.
- At last, when $l=4$ the condition $\mathrm{ord}_t\, h(X(t),Y(t))\geq 4$ is equivalent to $c=b=a=0$. Then $l=4$ is the third gap of Γ_P and the procedure ends.

Thus the Weierstrass gaps are $l=1,2,4$ and the minimal generator system is then $\{3,5,7\}$. Notice that this semigroup is not symmetric, since the conductor is $C=5<6=2g$, and that this set of generators is actually the Apéry system related to $\ell=3$. We are now going to compute a function f_l for each of these three generators also with the method described above.

We first take $\tilde{l}=7$ and search for a form H_0 of degree $n=4$ not divisible by F such that $\mathbf{N}^*H_0\geq\mathcal{A}+7P=7P$. That is, taking H_0 as a generic form of degree 4 with coefficients as variables, the needed condition is equivalent to $\mathrm{ord}_t\, H_0(X(t),Y(t),1)\geq 7$, with $(X(t),Y(t))$ the above local parametrization. This can be easily tested with Singular and one gets for instance the form $H_0=\mathrm{X}^2\mathrm{YZ}$, which is not divisible by F.

Now in order to compute $\mathbf{N}^*H_0$ we use the symmetry of F with respect to the three variables to get local parametrizations at the points $Q_1=(1:0:0)$ and $Q_2=(0:1:0)$. Thus, one easily obtains

$$\mathbf{N}^*H_0=2\,\mathbf{N}^*(\mathrm{X})+\mathbf{N}^*(\mathrm{Y})+\mathbf{N}^*(\mathrm{Z})=7P+4Q_1+5Q_2.$$

Then, in order to get f_7 we compute $R_7=4Q_1+5Q_2$ and find with the above method a form H_7 of degree 4 not divisible by F such that $\mathbf{N}^*H_7\geq R_7$ but not satisfying $\mathbf{N}^*H_7\geq R_6=R_7+P$. This is equivalent to the condition $\mathbf{N}^*H_7\geq R_7$ together with the local condition at P given by

$$\mathrm{ord}_t\, H_7(X(t),Y(t),1)=0$$

obtaining for instance $H_7=\mathrm{Z}^4$ and hence $f_7=\dfrac{\mathrm{Z}^3}{\mathrm{X}^2\mathrm{Y}}$.

In a similar way one checks that $H_5 = \mathrm{Y}^2\mathrm{Z}^2$ satisfies $\mathbf{N}^* H_5 \geq R_5$ but not $\mathbf{N}^* H_5 \geq R_4$, obtaining $f_5 = \dfrac{\mathrm{YZ}}{\mathrm{X}^2}$, and $H_3 = \mathrm{XYZ}^2$ satisfies $\mathbf{N}^* H_3 \geq R_3$ but not $\mathbf{N}^* H_3 \geq R_2$, obtaining $f_3 = \dfrac{\mathrm{Z}}{\mathrm{X}}$. In particular, a basis of $\mathcal{L}(7P)$ over $\mathbb{F}_2$ is given by

$$\{1, \frac{\mathrm{Z}}{\mathrm{X}}, \frac{\mathrm{YZ}}{\mathrm{X}^2}, \frac{\mathrm{Z}^2}{\mathrm{X}^2}, \frac{\mathrm{Z}^3}{\mathrm{X}^2\mathrm{Y}}\}.$$

There is an alternative way to get the functions f_l from the Brill-Noether algorithm. Assume that a basis $\{h_1, \ldots, h_s\}$ of $\mathcal{L}(\tilde{l}P)$ over $\mathbb{F}$ has already been computed and that $\tilde{l}$ is not a gap. We propose a triangulation method which works by induction on the dimension s as follows:

(1) By computing first the pole orders $\{-v_P(h_i)\}$ at P, assume that the functions $\{h_i\}$ are ordered in such a way that these pole orders are increasing in i, and set $l' = -v_P(h_s)$; if $l' < \tilde{l}$, we can replace $\tilde{l}$ by l', since $\mathcal{L}(\tilde{l}P) = \mathcal{L}(l'P)$, and go on.

(2) At least the function h_s satisfies $-v_P(h_s) = \tilde{l}$ and we set $f_{\tilde{l}} \doteq h_s$. If any other h_j satisfies the same condition, there exists a nonzero constant λ_j in $\mathbb{F}$ such that $-v_P(h_j - \lambda_j h_s) < \tilde{l}$; 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 linearly independent over $\mathbb{F}$ and $-v_P(g_i) < \tilde{l}$ 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 nongap such that $l' < \tilde{l}$. But now the dimension is $s - 1$ and we can continue by induction.

The above procedure also provides us with a function f_l for each nongap $l \leq \tilde{l}$. In fact, it can be used to compute the Weierstrass semigroup up to an integer $\tilde{l}$, since the maximum nongap l' such that $l' \leq \tilde{l}$ is just $\max\{-v_P(h_1), \ldots, -v_P(h_s)\}$, in the above notation, and so on by induction.

Remark 5.5. Ch. Lossen and the second author have implemented a SINGULAR library called **`brnoeth.lib`** [7] to carry out the algorithms of this section by means of the symbolic Hamburger-Noether expressions. There you can find procedures to compute the adjunction divisor $\mathcal{A}$ of a plane curve, bases for $\mathcal{L}(G)$ and Weierstrass semigroups, together with applications to AG codes. This library is currently available with the SINGULAR distribution (from Release 2.0) via **`http://www.singular.uni-kl.de/`**.

6. Applications to AG codes

Let $\tilde{\chi}$ be a nonsingular 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 algebraic geometry codes, take $\mathbb{F}$-rational points $P_1, \ldots, P_n$ of the curve and an $\mathbb{F}$-rational divisor G (which can be assumed effective) having disjoint support with $D \doteq P_1 + \ldots + P_n$, and then consider the well-defined linear maps

$$\begin{array}{c} \mathrm{ev}_D \ : \ \mathcal{L}(G) \longrightarrow \mathbb{F}^n \\ f \mapsto (f(P_1), \ldots, f(P_n)) \end{array} \quad \text{and} \quad \begin{array}{c} \mathrm{res}_D \ : \ \Omega(G - D) \longrightarrow \mathbb{F}^n \\ \omega \mapsto (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega)). \end{array}$$

One defines the linear codes

$$C_L \equiv C_L(D,G) \doteq \mathrm{Im}(\mathrm{ev}_D), \quad C_\Omega \equiv C_\Omega(D,G) \doteq \mathrm{Im}(\mathrm{res}_D).$$

The length of both codes is obviously n, and one has $(C_\Omega) = C_L^\perp$ by the *residue 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.

Denote by $k(C)$ and $d(C)$ the dimension over $\mathbb{F}$ and the minimum distance of the linear code C respectively, $d(C)$ the minimum number of nonzero entries of a nonzero vector of C. Goppa estimates for $k(C)$ and $d(C)$ are deduced from the Riemann-Roch formula as follows (see [25] for further details). If $2g-2 < \deg G < n$; then

$$(1) \quad \left[\begin{array}{lcl} k(C_L) & = & \deg G + 1 - g \\ d(C_L) & \geq & n - \deg G \end{array} \right. \qquad (2) \quad \left[\begin{array}{lcl} k(C_\Omega) & = & n - \deg G + g - 1 \\ d(C_\Omega) & \geq & \deg G + 2 - 2g. \end{array} \right.$$

With the assumption of having a (possibly singular) plane model χ of the curve $\tilde{\chi}$, the computational algorithms that are involved in the construction of AG codes can be basically reduced to the following:

(1) Find all the closed singular points and all the $\mathbb{F}$-rational points of χ, which can be done by means of Gröbner bases computation (see [15]).
(2) Compute the order of a function at a rational point P and evaluate the function at this point when possible, which can be done from lazy parametrizations for the rational branch corresponding to P. More precisely, if $\phi = G/H$ is a quotient of forms of the same degree in three variables and $(X(t):Y(t):Z(t))$ is the local parametrization obtained from the symbolic Hamburger-Noether expressions for the branch given by P, then doing the substitution

$$\phi(t) = \frac{G(X(t),Y(t),Z(t))}{h(X(t),Y(t),Z(t))} = \frac{a_r t^r + \dots}{b_s t^s + \dots},$$

the order is $r-s$, and if ϕ is well defined at P, then $\phi(P) = a_s/b_s$ (the point P is assumed to correspond to $t=0$).
(3) Find a basis for $\mathcal{L}(G)$ using the Brill-Noether algorithm, which can be done in terms of symbolic Hamburger-Noether expressions and computing adjoints with base conditions.

An interesting case is when $G = mP$, P an extra rational point of $\tilde{\chi}$. In this case the codes $C_m \doteq C_\Omega(D, mP)$ can be decoded by the majority scheme of the Feng and Rao algorithm, which is so far the most efficient method for the considered codes (see the details in [8]). In order to apply this decoding method, one has to fix for every nonnegative integer i a function f_i in $\mathbb{F}(\tilde{\chi})$ with only one pole at P of order i for those values of i for which it is possible, i.e., for the integers in the Weierstrass semigroup $\Gamma = \Gamma_P$ of $\tilde{\chi}$ at P. Afterwards, the key to the process is the computation of the bidimensional syndromes defined by

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

Therefore, in order to carry out this decoding algorithm, one must compute Γ and the functions f_i achieving the values of the semigroup Γ, and Section 5 just addressed solving this problem in terms of the theory of adjoints with the aid of symbolic Hamburger-Noether expressions.

Example 6.1. Let χ again be the curve given in Example 2.5 by the equation

$$F(\mathrm{X},\mathrm{Y},\mathrm{Z}) = \mathrm{X}^{10} + \mathrm{Y}^8\mathrm{Z}^2 + \mathrm{X}^3\mathrm{Z}^7 + \mathrm{Y}\mathrm{Z}^9 = 0$$

defined over $\mathbb{F}_2$ and whose genus is $g = 14$. This curve has 64 affine rational points over $\mathbb{F}_8$ (namely $P_1, \dots, P_{64}$) and only one point $P = (0:1:0)$ at infinity, which is the only singular point of χ and which was treated in the above example. Thus, if one takes an integer m with $26 < m < 64$, one can construct a code $C_m = C_\Omega(D, mP)$, where $D = P_1 + \ldots + P_{64}$, whose parameters are $[64, 77-m, \geq m-26]$. For example, if $m = 51$, then the dimension is $k = 26$ and C_{51} corrects any configuration of 12 errors. In order to construct such a code and to be able to decode by means of the Feng-Rao procedure, one first has to compute the Weierstrass semigroup at P and the corresponding functions.

By using the Singular library [7] mentioned above, we compute the Weierstrass semigroup up to the bound $\tilde{l} = 13$ by the triangulation method and obtain

$$\Gamma_P = \{0, 8, 10, 12, 13, \dots\}$$

and the corresponding functions

$$f_0 = 1, f_8 = \mathrm{X}, f_{10} = \mathrm{Y}, f_{12} = \mathrm{X}^5 + \mathrm{Y}^4,$$

$$f_{13} = \frac{\mathrm{X}^5\mathrm{Y}^4 + \mathrm{X}^4\mathrm{Y}^2 + \mathrm{X}^3 + \mathrm{Y}^8 + \mathrm{Y}}{\mathrm{X}^4} = \mathrm{X}\mathrm{Y}^4 + \mathrm{Y}^2 + \mathrm{X}^6, \dots.$$

In fact, this is enough to construct the whole Weierstrass semigroup and all the possibly needed functions, since the sequence $\{8, 12, 10, 13\}$ is telescopic and generates the semigroup (see [16] and [20]). Finally, by evaluating those functions at the points $P_1, \dots, P_{64}$ with the aid of local parametrizations, one easily obtains a parity check matrix for the code C_m .

References

1. A. Campillo, "Algebroid curves in positive characteristic", *Lecture Notes in Math.*, vol. 813, Springer-Verlag (1980). MR **82h:**14001
2. A. Campillo and J.I. Farrán, "Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models", *Finite Fields and their Applications* **6**, pp. 71-92 (2000). MR **2001a:**14026
3. E. Casas-Alvero, "Infinitely near imposed singularities and singularities of polar curves", *Math. Annalen* **287**, pp. 429-454 (1990). MR **91h:**14002
4. E. Casas-Alvero, "Singularities of plane curves", *London Math. Soc. Lecture Notes Series* **276**, Cambridge University Press (2000). CMP 2001:01
5. D. Duval, "Rational Puiseux expansions", *Comp. Math.* **70**, pp. 119-154 (1989). MR **90c:**14001
6. F. Enriques and O. Chisini, "Teoria geometrica delle equazioni e delle funzioni algebriche", Bologna (1918).
7. J.I. Farrán and Ch. Lossen, "`brnoeth.lib`", *A* Singular 2.0 *library for the Brill-Noether algorithm, Weierstrass semigroups and AG codes* (2001). Available via `http://www.singular.uni-kl.de/`.
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). MR **93m:**94031
9. V.D. Goppa, "Codes on algebraic curves", *Soviet. Math. Dokl.* **24** (1), pp. 170-172 (1981). MR **82k:**94017
10. V.D. Goppa, "Algebraic-geometric codes", *Math. USSR Izv.* **21**, pp. 75-91 (1983). MR **84g:**94011
11. D. Gorenstein, "An arithmetic theory of adjoint plane curves", *Trans. Amer. Math. Soc.* **72**, pp. 414-436 (1952). MR **14:**198h

12. G.-M. Greuel, G. Pfister and H. Schönemann, "SINGULAR 2.0", *A computer algebra system for polynomial computations*, Centre for Computer Algebra, University of Kaiserslautern (2001). Available via `http://www.singular.uni-kl.de/`.
13. G. Haché, "Construction effective des codes géométriques", *Ph.D. thesis*, Univ. Paris 6 (1996).
14. G. Haché, "Computation in algebraic function fields for effective construction of algebraic-geometric codes", *Lecture Notes in Computer Science* vol. 948, pp. 262-278 (1995). MR **98c**:94030
15. G. Haché and D. Le Brigand, "Effective construction of Algebraic Geometry codes", *IEEE Trans. Inform. Theory* **41**, pp. 1615-1628 (1995). MR **97g**:94037
16. J.P. Hansen and H. Stichtenoth, "Group codes on certain algebraic curves with many rational points", *AAECC* **1**, pp. 67-77 (1990). MR **96e**:94023
17. R. Hartshorne, "Algebraic Geometry", *Graduate Texts in Math.*, vol. 52, Springer-Verlag (1977). MR **57**:3116
18. T. Høholdt and R. Pellikaan, "On the decoding of algebraic-geometric codes", *IEEE Trans. Inform. Theory* **41**, pp. 1589-1614 (1995). MR **97a**:94008
19. M.D. Huang and D. Ierardi, "Efficient algorithms for Riemann-Roch problem and for addition in the jacobian of a curve", *Proceedings 32nd Annual Symposium on Foundations of Computer Sciences*, pp. 678-687, IEEE Comput. Soc. Press (1991).
20. 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). MR **97e**:94015
21. D. Le Brigand and J.J. Risler, "Algorithme de Brill-Noether et codes de Goppa", *Bull. Soc. Math. France* **116**, pp. 231-253 (1988). MR **89k**:14040
22. J. Lipman, "On complete ideals in regular local rings", *Algebraic Geometry and Commutative Algebra in honour of M. Nagata*, pp. 203-231 (1987). MR **90g**:14003
23. H. Matsumura, "Commutative ring theory", *Cambridge University Press*, Cambridge (1986). MR **88h**:13001
24. M. Rybowicz, "Sur le calcul des places et des anneaux d'entiers d'un corps de fonctions algébriques", *Ph.D. thesis*, Limoges (1990).
25. M.A. Tsfasman and S.G. Vlăduţ, "Algebraic-geometric codes", *Math. and its Appl.*, vol. 58, Kluwer Academic Pub., Amsterdam (1991). MR **93i**:94023

DEPARTAMENTO DE ALGEBRA, GEOMETRÍA Y TOPOLOGÍA, UNIVERSIDAD DE VALLADOLID, SPAIN
E-mail address: `campillo@agt.uva.es`

DEPARTAMENTO DE MATEMÁTICA APLICADA A LA INGENIERÍA, UNIVERSIDAD DE VALLADOLID, SPAIN
E-mail address: `ignfar@eis.uva.es`