Effective construction of algebraic geometry codes

G. Hache, Dominique Le Brigand

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Effective Construction of Algebraic Geometry Codes

Gaétan HACHÉ
Dominique Le BRIGAND

N° 2267
Mai 1994

PROGRAMME 2

Effective Construction of Algebraic Geometry Codes

Construction Effective des Codes Géométriques

Gaétan Haché* and Dominique Le Brigand†

ABSTRACT We intend to show that algebraic geometry codes (AG-codes, introduced by Goppa in 1977 [5]) can be constructed easily using blowing-up theory. This work is based on a paper by Le Brigand and Risler [12]. Given a plane curve, we desingularize the curve by means of blowing-up, and then using the desingularisation trees and the monoidal transformations associated to the blowing-up morphisms, we compute the adjoint divisor of the curve. Finaly we show how to use the algorithm of Brill-Noether to compute a basis of the vector space associated to a divisor of the curve. Two examples of constructions of AG-codes are given at the end.

RESUME Nous voulons montrer que les codes géométriques (introduits par Goppa en 1977 [5]) peuvent être construits sans trop de difficulté en utilisant la théorie des éclatements de points. Ce travail est essentiellement basé sur l'article de Le Brigand et Risler [12]. Etant donnée une courbe plane, on procède à une désingularisation de la courbe par éclatements des points singuliers et ensuite, en utilisant les arbres de désingularisations et les transformations monoïdales associées aux morphismes d'éclatements de points, on calcule le diviseur d'adjonction de la courbe. Finalement on montre comment utiliser l'algorithme de Brill-Noether pour obtenir une base de l'espace vectoriel associé à un diviseur de la courbe. Deux exemples de constructions de codes géométriques sont donnés à la fin.

*Projet CODES, INRIA-Rocquencourt, Domaine de Voluceau - BP 105, 78153 Le Chesnay Cedex, France. Email: gaetan.hache@inria.fr

†Université Pierre et Marie Curie, Paris VI, France. Chercheur extérieur au projet CODES. Email: dominique.lebrigand@inria.fr

1 Introduction

The opinion that algebraic geometry language makes algebraic geometry codes (AG-codes) construction very difficult seems to be widely spread in coding theory community. It seems that computing with a plane curve having non ordinary singular points is not well known. We would like to show that it is easy to compute the genus of any singular plane curve, to find a basis of the k-vector space $\mathcal{L}(D)$, where D is any divisor on the smooth model of such a curve (even if the support of D contains places above a singular point) and to evaluate functions of the function field at any rational point of the smooth model. We need all this in the construction of an algebraic geometry code. We propose an effective method using blowing-up theory; of course, there are other methods (see [16, 1, 13]), but we think that this one is computationally easy even if it may require field extensions. The algorithms have been implemented in Axiom, but we do not want to discuss here their complexity. This paper is mostly based on [12]. It is organized as follows. Section 2 fixes the notations and definitions of algebraic geometry codes. In Section 3, we recall the blowing-up theory, which leads to the desingularization of any plane curve. In Section 4, we give the construction of a basis for the k-vector space $\mathcal{L}(D)$ associated to a divisor D. Section 5 precises some algorithms we need for the construction of AG-codes. Finally, in Section 6, we give examples of codes using two different curves.

2 Preliminaries - Notations

One can find basic facts concerning algebraic curves in [15] or [14, (Appendix B)] where the function fields point of view is treated. We will use generally the same notations as [14]. Let k be the finite field $\mathbb{F}_q$, $\overline{k}$ its algebraic closure, C an affine curve defined and absolutely irreducible over k, P a rational point of C. We can suppose without loss of generality that $P = (0,0)$ in the affine coordinates (x,y) and $f(x,y) = 0$ is the equation of C. The affine coordinate ring of C is the integral domain

$$\Gamma(C) = k[x,y]/\langle f \rangle \ .$$

Its function field $k(C)$ is the quotient field of $\Gamma(C)$, that is

$$k(C) = \{\ g/h \mid g,\ h \in \Gamma(C),\ h \neq 0\ \}\ .$$

Now, let $\mathcal{X}$ be a smooth projective curve defined and absolutely irreducible over k. If $\mathcal{C}$ is a projective plane model of $\mathcal{X}$ with equation $F = 0$, where $F \in k[X,Y,Z]$ is an absolutely irreducible form, then its homogeneous coordinate ring is

$$\Gamma(\mathcal{C}) = k[X,Y,Z]/\langle F \rangle \ .$$

For $G \in k[X,Y,Z]$ a form, we denote by $\overline{G}$ its residual image in $\Gamma(\mathcal{C})$. The function field K/k of $\mathcal{X}$ is k-isomorphic to $k(\mathcal{C})/k$ where

$$k(\mathcal{C}) = \left\{\ \overline{G}/\overline{H} \mid G,\ H \in k[X,Y,Z],\ \text{forms of equal degree}\ ,\ \overline{H} \neq 0\ \right\}\ .$$

We identify K/k with $k(\mathcal{C})/k$. Suppose that $P = (0 : 0 : 1)$ in homogeneous coordinates $(X : Y : Z)$ and set $f(x,y) = F(x,y,1) = 0$. Then $f = 0$ is the equation of the affine part C_P of $\mathcal{C}$ at P and $k(\mathcal{C})$ is naturally isomorphic to $k(C_P)$. The local ring of $\mathcal{C}$ at P is

$$\mathcal{O}_P(\mathcal{C}) = \{\, g/h \mid g,h \in \Gamma(C_P),\ h(P) \neq 0 \,\}$$

and its unique maximal ideal is

$$\mathcal{M}_P(\mathcal{C}) = \{\, g/h \in \mathcal{O}_P(\mathcal{C}) \mid g(P) = 0 \,\} .$$

$\mathcal{O}_P(\mathcal{C})$ is a discrete valuation ring if and only if P is a simple point of $\mathcal{C}$. Let Q be any k-rational point of $k(\mathcal{C})$; assume for instance that Q is in the affine open set defined by $Z \neq 0$ and let $G \in k[X,Y,Z]$ be a form of degree d. We associate to G the element of $\mathcal{O}_Q(\mathcal{C})$

$$\overline{G}^Q = \overline{G}/\overline{Z}^d . \tag{1}$$

More generally, a **place** $\wp$ of K/k is the maximal ideal of some discrete valuation ring $\mathcal{O}_\wp$ of the function field K/k. The valuation in $\mathcal{O}_\wp$ will be denoted by $\mathbf{ord}_\wp$. Any element $t \in \wp$ such that $\wp = \langle t \rangle$ is called **a local parameter at** $\wp$ and $\mathbf{ord}_\wp(t) = 1$. If $\wp$ is a place of degree one, we will say that $\wp$ is **a k-rational point of** $\mathcal{X}$. In particular, to any simple k-rational point P of the plane model $\mathcal{C}$, corresponds a unique place $\wp$ of degree one of K/k and we will identify P with $\wp$. If P is a k-rational singular point of $\mathcal{C}$, then there is a finite number of places $\wp$ of K/k such that

$$\mathcal{O}_P(\mathcal{C}) \subset \mathcal{O}_\wp ;$$

we say that $\wp$ is **above** P and write $\wp \succ P$. Note that a place $\wp$ above a k-rational singular point is not necessarily of degree one. If $\deg \wp = r$, denoting by k_r the extension of k of degree r, we have $\wp = Q_1 + \cdots + Q_r$ where each Q_i is a place [1] of $\overline{k}(\mathcal{C})/\overline{k}$ and $Q_1, \ldots, Q_r$ are conjugated over k by $\mathcal{G}al(\overline{k}/k)$. In fact the places Q_i, $i = 1, \ldots, r$, can be considered as places of degree one of $k_r(\mathcal{C})/k_r$. If $u \in k(\mathcal{C})$, we denote also by u its image in $k_r(\mathcal{C})$ by the canonical embedding of $k(\mathcal{C})$ in $k_r(\mathcal{C})$ and we have

$$\mathbf{ord}_\wp(u) = \mathbf{ord}_{Q_i}(u) \ , \forall i = 1, \ldots, r .$$

Conversely, if Q is any place of $\overline{k}(\mathcal{C})/\overline{k}$, it belongs to a unique place $\wp$ of K; suppose again that $\deg \wp = r$ and let σ be a generator of $\mathcal{G}al(k_r/k)$. Then $i_Q = r$ is the smallest positive integer such that $Q^{\sigma^{i_Q}} = Q$ and we have

$$\wp = \sum_{j=0}^{i_Q - 1} Q^{\sigma^j} .$$

Let k' be any extension of k (or k itself) and let $\wp$ be a place of $k'(\mathcal{C})/k'$; for brevity, we shall refer to $\wp$ as a place of $k'(\mathcal{C})$. Likewise, if D is a divisor of $k'(\mathcal{C})/k'$, we shall say that D is a k'-rational divisor of $k'(\mathcal{C})$.
Finally, let us recall the definitions of algebraic geometry codes (cf. [15, p.266-]).

[1] Note that all the places of $\overline{k}(\mathcal{C})/\overline{k}$ are of degree one.

Definition 2.1 *Let $\mathcal{X}$ be a smooth projective curve defined and absolutely irreducible over the finite field $k = \mathbb{F}_q$. We denote by K/k its function field and let $\mathcal{P}$ and D be divisors of K/k with disjoint supports and*

$$\mathcal{P} = P_1 + \cdots + P_n$$

where P_i, $i = 1, \ldots, n$, are distinct k-rational points of $\mathcal{X}$. The **algebraic geometry code** *$C_L(\mathcal{X}, \mathcal{P}, D)$ is the image of the k-linear map*

$$ev_{\mathcal{P}} \ : \ \mathcal{L}(D) \longrightarrow k^n$$

such that

$$ev_{\mathcal{P}}(u) = (u(P_1), \ldots, u(P_n)) \ .$$

The code $C_L(\mathcal{X}, \mathcal{P}, D)$ has lenght n, dimension $\ell(D) - \ell(D - \mathcal{P})$ ($\ell(D)$ if $\deg D < n$) and minimum distance d such that $d \geq n - \deg D$; $d^* = n - \deg D$ is the **designed distance** of the code C_L. A generator matrix for $C_L(\mathcal{X}, \mathcal{P}, D)$ can be obtained knowing a basis for $\mathcal{L}(D)$ and a procedure for the evaluation of functions at the rational points P_i.
There is another construction of algebraic geometry codes

Definition 2.2 *Let $\mathcal{X}$ be a smooth projective curve defined and absolutely irreducible over the finite field $k = \mathbb{F}_q$. We denote by K/k its function field and let $\mathcal{P}$ and D be divisors of K/k with disjoint supports and*

$$\mathcal{P} = P_1 + \cdots + P_n$$

where P_i, $i = 1, \ldots, n$, are distinct k-rational points of $\mathcal{X}$. The **algebraic geometry code** *$C_\Omega(\mathcal{X}, \mathcal{P}, D)$ is the image of the k-linear map*

$$res_{\mathcal{P}} \ : \ \Omega(\mathcal{P} - D) \longrightarrow k^n$$

such that

$$res_{\mathcal{P}}(\omega) = (res_{P_1}(\omega), \ldots, res_{P_n}(\omega)) \ .$$

The codes $C_L(\mathcal{X}, \mathcal{P}, D)$ and $C_\Omega(\mathcal{X}, \mathcal{P}, D)$ are dual to each other; so a generator matrix for one of them gives a parity check matrix for the other. Finally, we recall that construction of bases for k-vector spaces $\mathcal{L}(G)$, where G is any divisor, is essential for presently existing decoding algorithms of algebraic geometry codes.

3 Blowing-up

The blowing-up theory is developed in many books, see for instance [7, 15]. The universal domain k is usually supposed to be an algebraically closed field. In [6, 8] k is an arbitrary field. The blowing-up process gives key informations concerning the smooth model of a given singular plane curve and its function field.

3.1 Definitions

Definition 3.1 *([7, p.28])* **Blowing-up a point in the affine space.** *Let k be any field and let P be the point $P = (0,0)$ in $\mathbb{A}^2(k)$. We consider the sub-variety W_1 of $\mathbb{A}^2 \times \mathbb{P}^1$ defined by*

$$W_1 = \left\{ (x,y) \times (x_1 : y_1) \in \mathbb{A}^2 \times \mathbb{P}^1 \mid xy_1 - yx_1 = 0 \right\}$$

where $(x_1 : y_1)$ are the homogeneous coordinates in $\mathbb{P}^1$. Then **the blowing-up π of P in** $\mathbb{A}^2$ *is the restriction to W_1 of the canonical projection from $\mathbb{A}^2 \times \mathbb{P}^1$ to $\mathbb{A}^2$.*

Properties of π.

1. W_1 is a smooth, irreducible surface defined over k.
2. If Q is any point in $\mathbb{A}^2(\overline{k})$ distinct from P, then $\pi^{-1}(Q)$ reduces to a single point; more precisely if $Q = (a,b) \neq (0,0)$ then
   (a) $\pi^{-1}(Q) = \{(a,b) \times (1 : b/a)\}$, if $a \neq 0$;
   (b) $\pi^{-1}(Q) = \{(a,b) \times (a/b : 1)\}$, if $b \neq 0$.
   (c) If Q is k-rational ($Q \in \mathbb{A}^2(k)$), then so is $\pi^{-1}(Q)$. More generally, there exists an isomorphism
   $$W_1 \setminus \pi^{-1}(P) \longrightarrow \mathbb{A}^2 \setminus \{P\}$$
   defined over k.
3. $\pi^{-1}(P)$ is isomorphic to $\mathbb{P}^1$; the points of $\pi^{-1}(P)$ are in one-to-one correspondence with the lines in $\mathbb{A}^2(\overline{k})$ passing by P.

One may generalize the definition of blowing-up as follows. Let S be a smooth projective surface defined over k and having the property that each point Q of S has an open neighbourhood U_Q isomorphic to $\mathbb{A}^2$. Let P be a k-rational point of S. Then there exists a unique smooth projective surface S_1 defined over k with the same property as S and there is a morphism

$$\pi : S_1 \to S$$

such that $S_1 \setminus \pi^{-1}(P)$ is isomorphic to $S \setminus \{P\}$ and $\pi^{-1}(P)$ is isomorphic to $\mathbb{P}^1$. If $P = (0,0)$ in the local coordinates of U_P, then the restriction of π above U_P coincides with the morphism considered in the preceding definition. The morphism π is **the blowing-up of P in S.**

3.2 Desingularization of a plane projective curve

Let $S_0 = \mathbb{P}^2(k)$, let C be a projective plane curve defined and absolutely irreducible over k and let P be a k-rational singular point of C.

Definitions 3.1 *Let π be the blowing-up morphism of P in S_0.*

- **The total transform** *of C by π is the inverse image of C by π.*
- **The strict transform** C_1 *of C by π is the closure of $\pi^{-1}(C \setminus \{P\})$ in S_1; $C_1 = \overline{\pi^{-1}(C \setminus \{P\})}$.*
- **The exceptional line** *is $\mathcal{E}_1 = \pi^{-1}(P)$.*
- **The infinitely near points of P by π** *are the common points of $\mathcal{E}_1$ and C_1.*

Using the properties of π, we have that $C_1 \setminus \pi^{-1}(P)$ is isomorphic to $C \setminus \{P\}$. The curves C and C_1 are birationally equivalent and π induces a k-isomorphism from $k(C)$ to $k(C_1)$. The point P is blown up into a projective line $\mathcal{E}_1$. We will show later that the number of infinitely near points equals the number of distinct tangents to C at P. Notice that these points may belong to a finite extension of k. The singular points of C_1 are

1. the singular points of $C \setminus \{P\}$, if any, using the identification of $C_1 \setminus \pi^{-1}(P)$ with $C \setminus \{P\}$,
2. eventually, the infinitely near points of P by π.

If Q is a singular point of C_1 we blow up Q. We may have to consider a finite extension k' of k if Q is not k-rational. After a finite number of blowing-ups we will obtain a smooth curve. We have the following result:

Theorem 3.1 *Let C_0 be a singular projective plane curve defined and absolutely irreducible over k; we set $S_0 = \mathbb{P}^2(k)$. Then, eventually over a finite algebraic extension k' of k, there exist smooth projective surfaces S_i $(i = 1, \ldots, n)$ defined over k' and a finite sequence of morphisms*

$$S_n \xrightarrow{\pi_n} S_{n-1} \xrightarrow{\pi_{n-1}} \cdots \xrightarrow{\pi_2} S_1 \xrightarrow{\pi_1} S_0$$

where, for $i = 1, \ldots, n$, π_i is the blowing-up of a k'-rational point P_{i-1} of S_{i-1} and if we denote by C_i the strict transform C_{i-1}, P_{i-1} is a singular point of C_{i-1}. The last strict transform C_n is a smooth curve defined over k' which is birationally equivalent to C_0; it is the smooth model $\mathcal{X}$ of C and we say that C has a desingularization over k'.

Let us see now precisely what we have to do in order to blow up a point P of a plane curve (P singular or not).

1. *Local equation of the curve at P.* Let $C : \{F = 0\}$ be a projective plane curve defined over k and let P be a k-rational point of C. Up to a linear change of projective coordinates $(X : Y : Z)$, we can have $P = (0 : 0 : 1)$; so $x = X/Z$ et $y = Y/Z$ are local coordinates at P in the affine open set defined by $Z \neq 0$ and the affine equation of C at P is

   $$f(x, y) = F(x, y, 1) = 0.$$

   We can write

   $$f(x, y) = f_r(x, y) + f_{r+1}(x, y) + \cdots + f_n(x, y)$$

where the f_i's are homogeneous forms of degree i; f_r is the **initial form of** f, $r = \mathrm{m}_P(\mathcal{C}) = \mathrm{m}_P(F) \geq 1$ is the **multiplicity of the point** P. P is singular (resp. simple) if and only if $r > 1$ (resp. $r = 1$). The factorization of f_r in $\overline{k}[x, y]$ is

$$f_r(x, y) = \prod_{i=1}^{s} L_i(x, y)^{n_i} \tag{2}$$

with $L_i(x, y) = a_i x + b_i y$ and $\sum_{i=1}^{s} n_i = r$. The curve $\mathcal{C}$ has s distinct tangents at P whose equations are $L_i = 0$, $i = 1, \ldots, s$.

2. *Strict transform of the curve by the blowing-up of* P. The equation in W_1 of the total transform of $\mathcal{C}$ by π is

$$\begin{cases} f(x, y) &= 0 \\ xy_1 - yx_1 &= 0 . \end{cases}$$

$\mathbb{P}^1$ is covered by two open sets: one is defined by $x_1 \neq 0$, the other by $y_1 \neq 0$. So W_1 is covered by two open sets isomorphic to $\mathbb{A}^2$

(a) the first one, denoted by U_x, corresponds to $x_1 = 1$. Identifying U_x with $\mathbb{A}^2$, we have that (x, y_1) are local coordinates in U_x and the restriction π_x of π to U_x is given by

$$\pi_x(x, y_1) = (x, xy_1) ; \tag{3}$$

(b) the second one, denoted by U_y, corresponds to $y_1 = 1$. Identifying U_y with $\mathbb{A}^2$, we have that (x_1, y) are local coordinates in U_y and the restriction π_y of π to U_y is given by

$$\pi_y(x_1, y) = (x_1 y, y) . \tag{4}$$

The equation in U_x of the total transform of $\mathcal{C}$ is

$$0 = f(x, xy_1) = x^r f_x(x, y_1) \tag{5}$$

where f_x is a polynomial in $k[x, y_1]$ such that $f_x(0, y_1) \neq 0$. We obtain two curves. One of them corresponds to $x = 0$; this is the local equation in U_x of the exceptional line $\mathcal{E}_1$. The other is defined by $f_x(x, y_1) = 0$; this is the local equation in U_x of the strict transform $\mathcal{C}_1$. The coordinates of the common points of $\mathcal{C}_1$ and $\mathcal{E}_1$ in U_x are $(0, \alpha)$, where α is a root of

$$f_x(0, T) = \prod_{i=1}^{s} (a_i + b_i T)^{n_i} = 0 ,$$

so α is the slope of a tangent to the curve at P. The number of these points is equal to the number of tangents which are distinct from $x = 0$.

The equation in U_y of the total transform is

$$0 = f(yx_1, y) = y^r f_y(x_1, y)$$

where f_y is a polynomial in $k[x_1, y]$ such that $f_y(x_1, 0) \neq 0$. We obtain two curves defined respectively by $y = 0$, the local equation of the exceptional line, and $f_y(x_1, y) =$

0, the local equation of the strict transform. The coordinates of the common points of $\mathcal{C}_1$ and $\mathcal{E}_1$ in U_y are $(\beta, 0)$, where β is a root of

$$f_y(T,0) = \prod_{i=1}^{s} (a_i T + b_i)^{n_i} = 0 .$$

The number of these points equals the number of tangents which are distinct from $y = 0$. We eventually recover the points corresponding to the tangents such that $b_i \neq 0$ and a new point $Q_0 = (0,0)$ if $\{x = 0\}$ is a tangent. If $\{x = 0\}$ is not tangent to the curve at P, we obtain all the infinitely near points of P in the open set U_x defined by $x_1 = 1$. Otherwise the infinitely near points of P are

(a) all the points $Q = (0, \alpha)$ in U_x such that $f_x(0, \alpha) = 0$;

(b) the point $Q = (0,0)$ in U_y if $f_y(0,0) = 0$.

Notice that if P is a simple point of $\mathcal{C}$, then there is a unique infinitely near point Q which is a simple point of $\mathcal{C}_1$. If P is k-rational, Q is also k-rational. Let Q be any point of $\mathcal{C}_1$ and let (u, v) be local coordinates in an affine open neighbourhood V of Q such that $Q = (0,0)$ and $g(u,v) = 0$ is the affine equation of $\mathcal{C}_1$. We can blow up the point Q the same way as before :

(a) if Q is an infinitely near point of P and $V = U_x$, then $(u,v) = (x, y_1 - \alpha)$, $g = f_x(x, y_1 - \alpha)$; if $V = U_y$, we have $(u,v) = (x_1, y)$ and $g = f_y(x_1, y)$;

(b) if Q corresponds to a point of $\mathcal{C}$ distinct from P by the isomorphism $\mathcal{C}_1 \setminus \pi^{-1}(P) \rightarrow \mathcal{C} \setminus \{P\}$, we blow up this point considered as a point of $\mathcal{C}$.

3. *Desingularization tree* (see [15, p.230]). Let $\mathcal{C}$ be a plane singular projective curve. We define **the desingularization tree** $\mathcal{T}$ of $\mathcal{C}$. Each singular point P of the curve is the **root of a sub-tree** $\mathcal{T}_P$ of $\mathcal{T}$ and P is characterized by its coordinates and the local equation of the curve at P. To each infinitely near point Q of P corresponds a branch; Q is **a node** of the sub-tree. To Q is attached informations concerning the open set U_x or U_y which contains it, the local coordinates at Q, functions of those at P, and the affine equation of the strict transform. The sub-tree $\mathcal{T}_P$ is constructed [2] recursively: if a node is a singular point of some curve $\mathcal{C}_i$, then it is the root of a sub-tree. A branch stops when we obtain a simple point, called **a leaf**, on the corresponding strict transform.

   In our implementation we make the computations in a field k big enough so that all the nodes of the tree are k-rational.

3.3 Monoidal transformation

Let P be any k-rational point of the curve $\mathcal{C}$ and let $f(x,y) = 0$ be the equation of $\mathcal{C}$ in an open affine neighbourhood of P such that $P = (0,0)$ (P is not necessarily a singular point of $\mathcal{C}$). Let $\mathcal{C}_1$ be the strict transform of the curve by the blowing-up of P. We have seen

[2] In Section 5.2 an algorithm is given.

that the function field $k(\mathcal{C})$ can be identified with the quotient field of $k[x,y]/\langle f\rangle$ and if f_x (resp. f_y) is the affine equation of $\mathcal{C}_1$ in U_x (resp. U_y), we can identify the function field $k(\mathcal{C}_1)$ with the quotient field of $k[x,y_1]/\langle f_x\rangle$ (resp. the quotient field of $k[x_1,y]/\langle f_y\rangle$). Using these identifications, we obtain the following k-isomorphisms

$$\begin{array}{rccc} \pi_x^* : & k(\mathcal{C}) & \longrightarrow & k(\mathcal{C}_1) \\ & g(x,y)/h(x,y) & \mapsto & g(x,xy_1)/h(x,xy_1) \end{array}$$

and

$$\begin{array}{rccc} \pi_y^* : & k(\mathcal{C}) & \longrightarrow & k(\mathcal{C}_1) \\ & g(x,y)/h(x,y) & \mapsto & g(yx_1,y)/h(yx_1,y)\,. \end{array}$$

We call π_x^* (resp. π_y^*) the **monoidal transformation** of the blowing-up of P with respect to U_x (resp. U_y). If Q is an infinitely near point of P, then

$$\pi_x^*(\mathcal{O}_P(\mathcal{C})) \subset \mathcal{O}_Q(\mathcal{C}_1)$$

and we have a similar result for π_y^*. Suppose now that $\mathcal{C}$ has a desingularization over k', P is a singular point and Q is a leaf of $\mathcal{T}_P$; then Q is a simple point of some strict transform, denoted by $\mathcal{C}_Q$, which can be considered as an affine curve when we restrict ourself to the open neighbourhood isomorphic to $\mathbb{A}^2$ containing Q. If $\pi_1, \pi_2, \ldots, \pi_s$ is the finite sequence of blowing-ups which leads from P to Q, we consider the k'-isomorphism

$$\pi_Q^* : k'(\mathcal{C}) \longrightarrow k'(\mathcal{C}_Q)$$

obtained by the composition of the monoidal transformations associated to π_i, $i = 1,\ldots,s$, with respect to the appropriate affine neighbourhoods. Then the leaves Q of the sub-tree $\mathcal{T}_P$ are in one-to-one correspondence with the places of $k'(\mathcal{C})$ lying over P and

$$\pi_Q^*(\mathcal{O}_P(\mathcal{C})) \subset \mathcal{O}_Q(\mathcal{C}_Q)\,.$$

Hence for any place $\wp$ above P there is a unique leaf Q such that

$$\pi_Q^*(\mathcal{O}_\wp) = \mathcal{O}_Q(\mathcal{C}_Q)\,;$$

for any $u \in k'(\mathcal{C})$ we have

$$\mathbf{ord}_\wp(u) = \mathbf{ord}_Q(\pi_Q^*(u))$$

and if $u \in \mathcal{O}_\wp$ then

$$u(\wp) = \pi_Q^*(u)(Q)\,.$$

3.4 The $\wp$-morphism

Let $\wp$ be any place of $\overline{k}(\mathcal{C})$ and k' a finite extension of k such that $\wp$ is place of degree one of $k'(\mathcal{C})$. If $\wp = P$ is a simple point of $\mathcal{C}$ we may define, by choosing an affine neighbourhood and up to a linear change of affine coordinates, an affine plane curve $C^\wp$ defined over k' and a birational morphism

$$\phi_\wp : C^\wp \longrightarrow \mathcal{C}$$

such that

$$\phi_{\wp}((0,0)) = P.$$

If $\wp$ is above a singular point P of C, then by blowing-ups and linear affine changes of coordinates we may also define an affine plane curve $C^{\wp}$ defined over k' and a birational morphism

$$\phi_{\wp} : C^{\wp} \longrightarrow C$$

such that

$$\phi_{\wp}((0,0)) = P.$$

In either case, we have a k'-isomorphism

$$\phi_{\wp}^* : k'(C) \longrightarrow k'(C^{\wp})$$

such that

$$\phi_{\wp}^*(\mathcal{O}_{\wp}) = \mathcal{O}_{(0,0)}(C^{\wp}).$$

We also have another useful property: since linear changes of affine coordinates and blowing-ups consist in linear and quadratic substitutions, we have for any form $G \in k'[X,Y,Z]$

$$\phi_{\wp}^*(\overline{G}^P) \in \Gamma(C^{\wp}) .$$

Hence, for the computation of the order or the evaluation of functions at places $\wp$ of $\overline{k}(C)$, it is sufficient to have algorithms defined at the simple point $(0,0)$ of the affine plane curve $C^{\wp}$. We call the morphism $\phi_{\wp}$ the **$\wp$-morphism.**

3.5 Genus of a plane curve

Let $\mathcal{T}$ be the desingularization tree of the plane curve $\mathcal{C} : \{F = 0\}$ and let m be the degree of F. Suppose that the tree consists of successive blowing-ups π_i, $i = 1, \ldots, n$, of n points $P_1, \ldots, P_n$, where, for $i = 1, \ldots, n$, P_i is a singular point of $\mathcal{C}_i$ of multiplicity r_i. We have the classical formula for the genus of the curve (see [15, p.229])

$$g = \frac{(m-1)(m-2)}{2} - \sum_{i=1}^{n} \frac{r_i(r_i-1)}{2} . \tag{6}$$

The preceding sum is taken over all the nodes of $\mathcal{T}$ including the singular points of the plane curve.

3.6 Additional remarks

Let k be the finite field $\mathbb{F}_q$ and $\mathcal{C}$ a projective plane curve defined and absolutely irreducible over k. We suppose that the singular points of $\mathcal{C}$ are rational over k; if not we replace k by a finite extension. Then the blowing-up of one of them, P, is defined on k and birational. The initial form f_r of the affine equation of $\mathcal{C}$ at P factors over $k[x,y]$. Let the factorization be

$$f_r = \prod_{j=1}^{t} p_j(x,y)^{m_j} ,$$

where p_j is an irreducible polynomial over k. We set $r_j = \deg p_j$ and denote by k_j the extension of k of degree r_j. Using similar notations as in (2) we have

$$f_r(x,y) = \prod_{j=1}^{t} \prod_{i=1}^{r_j} L_{i,j}(x,y)^{m_j} .$$

For any j, $j = 1,\ldots,t$, the slopes of the tangents $\{L_{i,j} = 0\}$, $i = 1,\ldots,r_j$ are conjugated over k and so are the corresponding infinitely near points $Q_{i,j}$. For a fixed j, we set $r = r_j$, $Q_i = Q_{i,j}$ $i = 1,\ldots,r$. Since the equation of the strict transform $\mathcal{C}_1$ is defined over k, if one of the Q_i is simple, so are the others; in that case, $\wp = \sum_{i=1}^{r} Q_i$ is a place of degree r of $k(\mathcal{C}_1)$. If one of the Q_i is singular, so are the others, of equal multiplicity. Further, the sub-trees corresponding to each Q_i are, in a sense, conjugated: this means that if σ is an element of $\mathcal{G}al(k_r/k)$ and $Q_i^{\sigma} = Q_l$, there is a canonical bijection between the sub-trees $\mathcal{T}_{Q_i}$ and $\mathcal{T}_{Q_l}$ which sends each node N of $\mathcal{T}_{Q_i}$ to N^{σ} which is a node of $\mathcal{T}_{Q_l}$. The local equation of the strict transform at N and N^{σ} are also conjugated by σ and N and N^{σ} have equal multiplicity on their respective strict transform. In fact, this is already true for the singular points of $\mathcal{C}$. If P is a singular point which is not k-rational and k_r is the least extension of k containing the coordinates of P, then, since the curve is defined over k, the conjugate points of P are singular points of the curve with the same multiplicity as P and their sub-trees are conjugated. For this reason we can say that, if the curve is defined over k, then its desingularization tree is globally rational over k.
In [7, p.163], the definition of a more general blowing-up is given. Theorically it allows to blow up at the same time a singular point and all its conjugates over k and so to stay in the base field k. But, at that moment, we cannot find an effective implementation of this theory.

4 Adjoint curve

The adjoint curves of an absolutely irreducible projective plane curve $\mathcal{C}$ play a crucial role in the determination of bases for vector spaces $\mathcal{L}(D)$, where D is any divisor of $k(\mathcal{C})$ (see [6, 12]). An adjoint curve of a plane curve $\mathcal{C}$ is a plane curve passing by the singular points of $\mathcal{C}$ with a "large enough" multiplicity.

4.1 Adjunction divisor

In that Section we refer to [6] or [12] for the proofs. Let $\mathcal{C}$ be a curve defined over k which has a desingularization over a finite extension k' of k and let $\mathcal{T}$ be its desingularization tree. Suppose that this tree consists of successive blowing-ups π_i, $i = 1,\ldots,n$, of n k'-rational points $P_1,\ldots,P_n$, where, for $i = 1,\ldots,n$, P_i is a singular point of $\mathcal{C}_i$ ($\mathcal{C}_1 = \mathcal{C}$) of multiplicity r_i. Let E_i be the divisor of $k(\mathcal{C})$ associated to the exceptional line $\mathcal{E}_i$ of π_i: we call E_i **the exceptional divisor of** π_i. $\mathcal{E}_i$ cuts the strict transform $\mathcal{C}_i$ at the infinitely near points of P_i and so the support of E_i is equal to the set of leaves of the tree $\mathcal{T}_{P_i}$. It can be shown, see Lemma 5.1, that its degree is equal to r_i. Using the preceding notations, we have

Definitions 4.1 *Let $\mathcal{C} : \{F = 0\}$ be a projective plane curve defined and absolutely irreducible over a field k and let $\mathcal{T}$ be its desingularization tree defined over a finite extension k' of k.*

- *The divisor of $k'(\mathcal{C})$ defined by*

$$\mathcal{A} = \sum_{i=0}^{n} (r_i - 1)E_i$$

is **the adjunction divisor of** $\mathcal{C}$. *Using Section 3.6, it can be shown that $\mathcal{A}$ is in fact rational over k.*

- *Let $\mathcal{C}' : \{G = 0\}$ be a projective plane curve defined over k such that the form $G \in k[X, Y, Z]$ is not divisible by F. Then $\mathcal{C}'$ is* **an adjoint of** $\mathcal{C}$ *if*

$$(G) \geq \mathcal{A}\,.$$

If we consider the points P_i which belong to the sub-tree $\mathcal{T}_P$ corresponding to a singular point P of $\mathcal{C}$ and set

$$\mathcal{A}_P = \sum_{P_i \in \mathcal{T}_P} (r_i - 1)E_i$$

then $\mathcal{A}_P$ is called **the adjunction divisor of** $\mathcal{C}$ **at** P. If P is a simple point, then clearly $\mathcal{A}_P = 0$. Let G be a form not divisible by F and such that $(G)_P \geq \mathcal{A}_P$. We say that $\mathcal{C}' : \{G = 0\}$ is **an adjoint of** $\mathcal{C}$ **at** P. Using the fact that $\deg E_i = r_i$, we can rewrite formula (6): if $\deg F = m$, the genus of $\mathcal{C}$ is equal to

$$\begin{aligned} g &= \frac{(m-1)(m-2)}{2} - \sum_{P \in \mathcal{C}} \frac{\deg \mathcal{A}_P}{2} \\ &= \frac{(m-1)(m-2)}{2} - \frac{\deg \mathcal{A}}{2}\,. \end{aligned} \tag{7}$$

Finally let us recall the link between adjoint curves and special divisors. Let $\mathcal{C}' : \{G = 0\}$ be an adjoint curve of $\mathcal{C} : \{F = 0\}$, d (resp. m) the degree of G (resp. F); we set

$$\mathcal{R} = (G) - \mathcal{A}\,.$$

The divisor $\mathcal{R}$ is positive and k-rational. We say that $\mathcal{R}$ is the divisor cut out on $\mathcal{C}$ by the adjoint $\mathcal{C}'$ outside $\mathcal{A}$. The following result is well known (see [6, p. 437])

Theorem 4.1 *The adjoint curves of degree $d = m - 3$ cut out on $\mathcal{C}$ outside $\mathcal{A}$ the complete canonical series denoted by $\mathcal{K}$.*

This means that any special divisor $\mathcal{R}$ of $k(\mathcal{C})$ is such that

$$\mathcal{R} = (G) - \mathcal{A}\,,$$

where G is a form of degree $m - 3$.

4.2 Conductor

In this section we refer to [6, p. 430] or [15, p. 217-]. Let $\mathcal{C}$ be a projective plane curve defined and absolutely irreducible over a field k, P a k-rational point of $\mathcal{C}$, $\mathcal{O}_P$ the local ring at P, $\overline{\mathcal{O}}_P$ the integral closure of $\mathcal{O}_P$ in K.

Definition 4.1 *The* **conductor at P of the curve** *is the set*

$$\mathrm{c}_P = \left\{ u \in \mathcal{O}_P \mid u\,\overline{\mathcal{O}}_P \subset \mathcal{O}_P \right\} .$$

The conductor c_P is the largest ideal in $\mathcal{O}_P$ which is also an ideal in $\overline{\mathcal{O}}_P$. If P is a simple point, then

$$\overline{\mathcal{O}}_P = \mathcal{O}_P$$

so $\mathrm{c}_P = \mathcal{O}_P$. Associated to the conductor at P there are two integers n_P and δ_P which are important invariants of a singular point P.

1. **The integer n_P.** We set

$$n_P = dim_k\, \overline{\mathcal{O}}_P/_{\mathrm{c}_P} .$$

Since

$$\overline{\mathcal{O}}_P = \bigcap_{\wp \succ P} \mathcal{O}_\wp$$

and since c_P is an ideal of the semi-local ring $\overline{\mathcal{O}}_P$, for any place $\wp$ above P, the ideal generated by c_P in the discrete valuation ring $\mathcal{O}_\wp$ is a power of $\wp$

$$\mathrm{c}_P \mathcal{O}_\wp = \wp^{n_\wp}$$

and

$$n_P = \sum_{\wp \succ P} n_\wp \deg \wp .$$

The conductor at P is related to the divisor

$$A_P = \sum_{\wp \succ P} n_\wp \wp$$

in the following way

$$\mathrm{c}_P = \{ u \in \mathcal{O}_P \mid (u)_P \geq A_P \} .$$

Observe that $\deg A_P = n_P$ and if P is a simple point, then $n_P = 0$ and $A_P = 0$. In [15], $A = \sum_{P \in \mathcal{C}} A_P$ is called **the divisor of double points** of the curve. It can be shown that, since $\mathcal{C}$ is a plane curve, we have $A_P = \mathcal{A}_P$ for all P in $\mathcal{C}$ so $A = \mathcal{A}$ (see [6]). If u is a non zero element of K then $u = \overline{G}/\overline{H}$, where G and H are forms of equal degree and $\overline{H} \neq 0$. We have

$$u \in \mathrm{c}_P \iff (G)_P \geq (H)_P + A_P .$$

This implies that the plane curve with equation $G = 0$ is an adjoint of $\mathcal{C}$ at P.

2. **The integer δ_P.** The second integer associated to a point P of the curve is

$$\delta_P = dim_k\, \overline{\mathcal{O}}_P/\mathcal{O}_P\ ;$$

if P is a simple point, then $\delta_P = 0$ and this condition characterizes simple points. Since $\mathcal{C}$ is a plane curve, the integer δ_P is related to n_P by the equality

$$n_P = 2\delta_P\ .$$

If the equation of the plane curve $\mathcal{C}$ is a form of degree m, then the genus of the curve is given by (compare with (7))

$$g = \frac{(m-1)(m-2)}{2} - \sum_{P\in\mathcal{C}} \delta_P\ . \tag{8}$$

Further $\delta_P = \sum_{Q\in T_P} r_Q(r_Q-1)/2$ is the number of independent conditions that must be verified by a plane curve $\mathcal{C}'$ to be an adjoint of $\mathcal{C}$ at P.

4.3 Basis for $\mathcal{L}(D)$

The construction of a basis for $\mathcal{L}(D)$ is treated in [9] in the case where $\mathcal{C}$ has only ordinary singular points and in [12] for any singular curve. Following [12], we use the fundamental theorem of Max Noether:

Theorem 4.2 *Let $G=0$ be the equation of a plane curve not containing $\mathcal{C}:\{F=0\}$ as a component. Then, if $(H)\geq \mathcal{A}+(G)$, there exist forms A and B with coefficients in k such that*

$$H = AF + BG\ .$$

Theorem 4.3 *(see [12]) Let $\mathcal{C}:\{F=0\}$ be a projective plane curve defined and absolutely irreducible over k, $\mathcal{A}$ its adjunction divisor and D any positive divisor in K. If G_0 is a form in $k[X,Y,Z]$ of degree d such that $(G_0)\geq \mathcal{A}+D$, then*

$$\mathcal{L}(D) = \left\{ \overline{G}/\overline{G}_0 \mid G\in k[X,Y,Z],\ G \text{ is a form },\ \deg G = d,\ (G)\geq (G_0)-D \right\}\cup\{0\}\ .$$

So, the elements of $\mathcal{L}(D)$ are related to the adjoints of the curve. To obtain a basis for this k-vector space, we pick a form G_0 such that $(G_0)\geq \mathcal{A}+D$. Suppose that $\deg G_0 = d$ and

$$(G_0) = \mathcal{A}+D+R\ ;$$

then we search a basis for the k-vector space of the forms of degree d

$$G = \sum_{i+j+l=d} \lambda_{i,j,l}\, X^iY^jZ^l\ ,\ \lambda_{i,j,l}\in k$$

such that G is not divisible by the equation of $\mathcal{C}$ and $(G)\geq \mathcal{A}+R$.
Notice that if D is not positive, we can write

$$D = D_+ - D_-$$

where D_+ and D_- are positive divisors with disjoint supports. It follows that we can obtain a basis for $\mathcal{L}(D)$ in the following way:

Theorem 4.4 *If G_0 is a form in $k[X,Y,Z]$ of degree d such that $(G_0) \geq \mathcal{A} + D_+$, then*

$$\mathcal{L}(D) = \left\{ \overline{G}/\overline{G_0} \mid G \in k[X,Y,Z],\ G \text{ is a form},\ \deg G = d,\ (G) \geq (G_0) - D \right\} \cup \{0\} .$$

Proof: If $D_- = 0$, we recover the case D positive. Otherwise we set

$$(G_0) = \mathcal{A} + D_+ + R .$$

If $u = \overline{G}/\overline{G_0}$ where G is a form of degree d such that $(G) \geq (G_0) - D$, then

$$(u) = (G) - (G_0) \geq -D$$

and u is in $\mathcal{L}(D)$. Conversely, if u is a non zero element in $\mathcal{L}(D)$, then $(u) + D = D'$ is an positive divisor and

$$(u) + D_+ = D' + D_- ;$$

so D_+ and $D' + D_-$ are two positive equivalent divisors such that, if $u = \overline{H}/\overline{H'}$, with H and H' forms of equal degree, then

$$(H) + D_+ = (H') + D' + D_- .$$

Since we have

$$\begin{aligned} (G_0 H) &= (G_0) + (H) \\ &= \mathcal{A} + D_+ + R + (H) \\ &= \mathcal{A} + D' + D_- + R + (H') \geq \mathcal{A} + (H') \end{aligned}$$

we may apply Max Noether's Theorem to the form $G_0 H$ by which there exist forms A and G such that

$$G_0 H = AF + GH'$$

so $(u) = (H) - (H') = (G) - (G_0)$ and $u = \alpha \overline{G}/\overline{G_0}$, for some $\alpha \in k$. □
Finally, to obtain a basis for $\mathcal{L}(D)$, we must know

1. how to compute the divisor of a given form,
2. how to find a form of given degree whose divisor is greater than a given positive divisor.

We will address these problems in the next Section.

5 Algorithmic part

Let $\mathcal{C}$ be a plane projective curve defined over $k = \mathbb{F}_q$ with equation $F(X,Y,Z) = 0$, $\mathcal{P}$ and D two k-rational divisors; in order to construct the code $C_L(\mathcal{X}, \mathcal{P}, D)$, where $\mathcal{X}$ is the smooth model of $\mathcal{C}$, we need

1. all the singular points and the k-rational points of $\mathcal{C}$;

2. the desingularization tree;

3. the adjunction divisor $\mathcal{A}$, a k-rational basis $\left\{u_1, u_2, \ldots, u_{\ell(D)}\right\}$ for $\mathcal{L}(D)$ and the values of u_i at the k-rational points P occuring in the support of $\mathcal{P}$.

   For this we need algorithms

   (a) to compute the divisor associated to a form;

   (b) to compute the order of a function u at a point P of the smooth model and $u(P)$ if it is defined;

   (c) to interpolate forms through k-rational divisors: that is to find all the forms G such that (G) is greater than a given k-rational divisor.

5.1 Finding singular and rational points

Let F_X, F_Y and F_Z be respectively the derivatives of F with respect to the variables X, Y and Z. Then

$$(a:b:c) \in \mathcal{C} \text{ is singular} \iff (\text{Sing}) \begin{cases} F(a,b,c) &= 0 \\ F_X(a,b,c) &= 0 \\ F_Y(a,b,c) &= 0 \\ F_Z(a,b,c) &= 0 \\ (a,b,c) &\neq (0,0,0)\,. \end{cases}$$

To solve (Sing) it is sufficient to solve the two following systems:

$$\begin{cases} F(a,b,1) &= 0 \\ F_X(a,b,1) &= 0 \\ F_Y(a,b,1) &= 0 \end{cases} \tag{9}$$

and

$$\begin{cases} F(a,1,0) &= 0 \\ F_X(a,1,0) &= 0 \\ F_Z(a,1,0) &= 0 \end{cases} \tag{10}$$

and finally test if $(1:0:0)$ is a singular point. For the last step we employ the following equivalence

$$(1:0:0) \in \mathcal{C} \text{ is singular} \iff \begin{cases} F(1,0,0) &= 0 \\ F_Y(1,0,0) &= 0 \\ F_Z(1,0,0) &= 0\,. \end{cases}$$

The algebraic systems (9) and (10) yield a finite number of solutions. Those of (10) may be found by computing the greatest common divisor

$$R(a) = \gcd\left\{F(a,1,0), F_X(a,1,0), F_Z(a,1,0)\right\}$$

and the roots of R yields the solutions. If R does not factor linearly over k then there are singular points over a finite extension of k. To find the solution of (9), the best method is

to compute a Gröbner basis of the ideal generated by the polynomials occuring in (9) (see [11]).
To find the rational points we use the same idea:

$$P=(a:b:c)\in\mathcal{C} \text{ is rational over } \mathbb{F}_q \iff (\text{Rat}) \begin{cases} F(a,b,c) &= 0 \\ a^q-a &= 0 \\ b^q-b &= 0 \\ c^q-c &= 0 \\ (a,b,c) &\neq (0,0,0)\,. \end{cases}$$

5.2 Computing the desingularization tree

Suppose that $\mathcal{C}$ has a desingularization over $k_r=\mathbb{F}_{q^r}$. Let $P=(a:b:1)$ be a k_r-rational singular point of $\mathcal{C}$. We compute the desingularization tree by taking advantage of the action of the Galois group $\mathcal{G}al(k_r/k)$, as described in Section 3.6. Instead of computing each desingularization tree for the conjugate points of P if any, we compute only one tree on which the nodes will have the necessary informations concerning the conjugate points. For this purpose we fix σ a generator of the Galois group $\mathcal{G}al(k_r/k)$ and we associate to a point $P=(a,b)\in\mathbb{A}^2(k_r)$ its orbit under the action of σ which will be represented by

$$\mathcal{OR}_P=\{0,1,2,\ldots,i_P-1\}\ ,$$

where i_P is the smallest positive integer such that $P^{\sigma^{i_P}}=P$. The nodes of a sub-tree of $\mathcal{T}_P$ will be represented by

$$[Q=(a',b'),\ f_Q=0,\ r_Q,\ \mathcal{E}_Q:\{l_Q=0\},\ \mathcal{OR}_Q]\,,$$

where, in the appropriate affine neighbourhood, $Q=(a',b')\in\mathbb{A}^2(k_r)$ is an infinitely near point of multiplicity r_Q on the strict transform with affine equation $f_Q=0$, $l_Q=0$ is the affine equation of the exceptional line and $\mathcal{OR}_Q$ is the orbit of Q. The root P of the desingularization tree $\mathcal{T}_P$ has the same representation but, since for P the exceptional line is not defined, we write

$$[P=(a,b),\ f_P=0,\ r_P,\ \mathcal{E}_P:\{\},\ \mathcal{OR}_P].$$

We have the following algorithm

Algorithm 5.1
Input: $(P=(a,b),\ f_P,\mathcal{E}_P)$
Output: *The desingularization tree of* P.
desingTree$(P=(a,b),\ f_P,\mathcal{E}_P)$

1. *Compute* $\mathcal{OR}_P$.
2. *Set* $f(x,y):=f_P(x+a,y+b)$*; take the affine change of coordinates so that the point* $P=(a,b)$ *is brought to the origin. Compute* r_P *which is the degree of the initial form of* f.

3. *If* $r_P = 1$ *then return the tree consisting of the single node*

$$[P = (a, b),\ f_P,\ 1,\ \mathcal{E}_P,\ \mathcal{OR}_P]\ ;$$

4. *otherwise, let* $f_x = 0$ *be the equation of the strict transform of* f *in* U_x.

5. *Factor* $f_x(0, T) = \prod_{j=1}^{t} p_j(T)^{m_i}$ *and set* s = *lowest common multiple of* $\deg p_j$, $j = 1, 2, \ldots t$. *If* $s \neq 1$ *this means that there are singular points nonrational over* k. *Restart with an extension of* k *of degree* s.

6. *Compute* $R = \{\alpha \mid f_x(0, \alpha) = 0\}$. *Initialize an empty set* **listOfSubTrees** *which at the end will contain all the sub-trees of* $\mathcal{T}_P$.

7. *While* R *is not empty repeat*

   (a) *Pick a root* $\alpha \in R$,

   (b) *compute* $\mathcal{T}_Q$ = **desingTree**$(Q(0, \alpha), f_x, \{x = 0\})$ *and add the result to* **ListOfSubTrees**,

   (c) *compute* $R = R \setminus \{\alpha^{q^i} \mid i \in \mathcal{OR}_Q\}$. *(On the node of* $\mathcal{T}_Q$ *we may retreive* $\mathcal{OR}_Q$*)*

8. *Test if* x *divides the minimal form of* f; *if so, then* $Q' = (0, 0)$ *is an infinitely near point in* U_y; *compute* $\mathcal{T}_{Q'}$ = **desingTree**$(Q', f_y, \{y = 0\})$ *where* $f_y = 0$ *is the equation of the strict transform in* U_y *and add the result in* **ListOfSubTrees**.

9. *Return*

$$\mathcal{T}_P = \{[P = (a, b),\ f_P,\ r,\ \mathcal{E}_P,\ \mathcal{OR}_P],\ \textbf{listOfSubTrees}\}\ .$$

We will see in the next Section how we can take advantage of the orbit assigned to each node.

5.3 Divisor associated to a form

Let $G \in k[X, Y, Z]$ be a form such that $\overline{G} \neq 0$ in $\Gamma(\mathcal{C})$. For any point $P \in \mathcal{C}$, we set $g = \overline{G}^P$ (see Section 2) and $(G)_P = \sum_{\wp > P} \mathbf{ord}_\wp(g)\, \wp$. Since $(G)_P$ depends only on g, we will sometimes set $(G)_P = (g)_P$. If $G(P) \neq 0$, that is if P is not a point of the curve $\mathcal{C}' : \{G = 0\}$, then $(G)_P = 0$. The divisor of G in $k(\mathcal{C})$ is equal to

$$(G) = \sum_{P \in \mathcal{C}} (G)_P = \sum_{P \in \mathcal{C} \cap \mathcal{C}'} (G)_P\ ;$$

its degree is equal to $\deg F \times \deg G$ by Bézout Theorem. Let us compute $(G)_P$ for all the common points P of $\mathcal{C}$ and $\mathcal{C}'$.

1. If P is a simple point of $\mathcal{C}$, we have

$$(G)_P = \mathbf{ord}_P(g)\, P\ .$$

2. If P is a singular point of $\mathcal{C}$, let π be its blowing-up morphism. For each infinitely near point Q of P ($\pi(Q) = P$), let π_Q^* be the monoidal transformation with respect to the neighbourhood (U_x or U_y) containing Q; let $L_Q = 0$ be the affine equation at Q of the exceptional line and g_Q (resp. l_Q) the residual image of the strict transform of G (resp. L_Q) in $\Gamma(\mathcal{C}_1)$. Then $(G)_P$ is defined in a recursive way by

$$\begin{aligned}
(G)_P = (g)_P &= \sum_{\pi(Q)=P} \left(\pi_Q^*(g)\right)_Q \\
&= \sum_{\pi(Q)=P} \left(l_Q^{\mathbf{m}_P(G)}\, g_Q\right)_Q \\
&= \mathbf{m}_P(G) \sum_{\pi(Q)=P} (l_Q)_Q + \sum_{\pi(Q)=P} (g_Q)_Q \\
(g)_P &= \mathbf{m}_P(G)\, E_P + \sum_{\pi(Q)=P} (g_Q)_Q \qquad (11)
\end{aligned}$$

where $E_P = \sum_{\pi(Q)=P} (l_Q)_Q$ is the exceptional divisor of π. To each singular infinitely near point Q of P we associate an exceptional divisor E_Q and if Q is simple, we set $E_Q = 0$.

If P is a singular point, $(G)_P$ is computed recursively following the branches of $\mathcal{T}_P$. To illustrate how to use the orbit of a node in $\mathcal{T}_P$ we have the following algorithm, in which the details have been left out:

Algorithm 5.2
Input: *(g, $\mathcal{T}_P$) where g is the affine residual image of a form G and $\mathcal{T}_P$ is the desingularization tree of P.*
Output: *The divisor $(G)_P$.*
localDivisor$(g, \mathcal{T}_P)$

1. *If P is a leaf then set $D = \mathbf{ord}_P(g)P$;*
2. *otherwise compute $D = \mathbf{m}_P(G)E_P + \sum_{\mathcal{T}_Q \in S} \mathbf{localDivisor}(g_Q, \mathcal{T}_Q)$ where S is the set of sub-trees of $\mathcal{T}_P$.*
3. *Return $\sum_{i \in \mathcal{OR}_P} D^{\sigma^i}$.*

Note that before using the algorithm **localDivisor** one must compute for each node the corresponding exceptional divisor. This is easily done with the following algorithm:

Algorithm 5.3
Input: *$\mathcal{T}_P$ the desingularization tree of P.*
Output: *$\mathcal{T}_P$ with attached to each node the corresponding exceptional divisor.*
desingTreeWithExceDiv$(\mathcal{T}_P)$

1. *If P is a leaf then attach to the node the divisor 0 and return $\mathcal{T}_P$;*

2. *otherwise let S be the set of sub-trees of $\mathcal{T}_P$ and recursively call the algorithm on the sub-trees;*

$$S' = \{\ \mathbf{desingTreeWithExceDiv}(\mathcal{T}_Q)\ \mid\ \mathcal{T}_Q \in S\ \}\ .$$

Compute the divisor $E_P = \sum_{T'_Q \in S'} \mathbf{localDivisor}(l_Q, T'_Q)$ and return the tree $\mathcal{T}_P$ with E_P attached to the node.

We are now able to prove the following lemma, which is used in Section 4.1:

Lemma 5.1 *Let P be a point of an affine curve C and let r_P be its multiplicity. Then the exceptional divisor E_P of the blowing-up of P is of degree r_P.*

Proof: Let $L = 0$ be the equation of a line passing by P but not tangent to C at P; then

$$\deg(L)_P = \mathbf{m}_P(C) \times \mathbf{m}_P(L) = r_P\ .$$

Further, the strict transform of $L = 0$ contains no infinitely near point of P. So $(L)_P = E_P$ and $\deg(E_P) = r_P$. □

Applying formula (11), the computation of the divisor $(G)_P$ reduces to the computation of the order of some functions at simple points corresponding to the leaves of $\mathcal{T}_P$. Since the leaves of the desingularization tree $\mathcal{T}_P$ are in one-to-one correspondence with the places of $\overline{k}(C)$ lying above P, we have to calculate the order of a function at a place of $\overline{k}(C)$.

5.4 Order of a function at a place

Let $\wp$ be a place of $\overline{k}(C)$ and k_r an extension of degree r of k such that $\wp$ is a place of degree one in $k_r(C)$. Let $u = \overline{G}/\overline{H} \in k_r(C)$. We have $\wp \succ P$ or $\wp = P$ for a unique k_r-rational point P of C. By the $\wp$-morphism (see Section 3.4)

$$\mathbf{ord}_\wp(u) = \mathbf{ord}_{(0,0)}(\phi^*_\wp(\overline{G}^P)) - \mathbf{ord}_{(0,0)}(\phi^*_\wp(\overline{H}^P))$$

and both $\phi^*_\wp(\overline{G}^P)$ and $\phi^*_\wp(\overline{H}^P)$ are in $\Gamma(C^\wp)$ where $C^\wp$ is an affine plane curve defined over k_r. The problem reduces to the following: compute $\mathbf{ord}_P(g)$ where $P = (0,0)$ is a simple point of an affine plane curve C defined over k_r and $g \in \Gamma(C)$. Let (x, y) be the affine coordinates, $f(x, y) = 0$ the equation of C and $G(x, y) \in k_r[x, y]$ be a representative of g. If $G(0,0) \neq 0$ then of course $\mathbf{ord}_P(g) = 0$; otherwise suppose that $\{x = 0\}$ is not the tangent to C at P. Then the initial form of C at P is $f_1 = ax - by$, with $b \neq 0$; we set $\alpha = a/b$. Let π be the blowing-up of P. On the exceptional line $\mathcal{E} : \{x = 0\}$ there is a unique infinitely near point $Q = (0, \alpha) \in U_x$ which is k_r-rational. We have

$$\mathbf{ord}_P(g) = \mathbf{ord}_Q \pi^*_x(g)\ .$$

Let C_Q be the strict transform of C and let $f_x = 0$ be its equation in U_x. Since $\{x = 0\}$ is not the tangent to C at P, $\mathcal{E}$ is not tangent to C_Q at Q. Without ambiguity we denote also by x the residual image of x in $k_r[x, y_1]/\langle f_x \rangle$. Then x is a local parameter at Q and $\mathbf{ord}_Q(x) = 1$. If g_Q is the residual image in $k_r[x, y_1]/\langle f_x \rangle$ of the strict transform G_Q of G, we have (see (5) in Section 3.2)

$$\pi^*_x(g) = x^{\mathbf{m}_P(G)}\, g_Q\ , \tag{12}$$

so

$$\mathbf{ord}_P(g) = \mathbf{m}_P(G) + \mathbf{ord}_Q(g_Q)\,.$$

If $\mathbf{m}_Q(G_Q) = 0$ we have $\mathbf{ord}_Q(g_Q) = 0$ and we are finished, otherwise we blow up the point Q. Clearly a finite number of blowing-ups gives the value of $\mathbf{ord}_P(g)$.

5.5 Evaluation of a function at a rational place

Let φ be a place of $k(C)$ of degree one. Like for the computing of the order we need only to consider $u(P)$, where $P = (0,0)$ is a simple point of an affine plane curve C and $u = g(x,y)/h(x,y)$ where g and h are respectively the residual images in $\Gamma(C)$ of some $G,\ H \in k[x,y]$. One of the following three cases occurs:

1. if $\mathbf{m}_P(H) = 0$, $u(P) = G(0,0)/H(0,0)$;
2. if $\mathbf{m}_P(G) = 0$ and $\mathbf{m}_P(H) > 0$, u is not defined at P;
3. if $\mathbf{m}_P(G) > 0$ and $\mathbf{m}_P(H) > 0$, we do not know yet if P is a pole of u or not.

To deal with the third case, we use the same idea as before. We blow up P and, considering the unique infinitely near point Q, we have (see (12))

$$\pi_Q^*(u) = \frac{x^{\mathbf{m}_P(G)}\, g_Q}{x^{\mathbf{m}_P(H)}\, h_Q}\,.$$

1. If $\mathbf{m}_P(G) \geq \mathbf{m}_P(H)$, then

$$\pi_Q^*(u) = \frac{x^{(\mathbf{m}_P(G)-\mathbf{m}_P(H))}\, g_Q}{h_Q}\,.$$

Since $\mathbf{ord}_P(g) = \mathbf{m}_P(G) + \mathbf{ord}_Q(g_Q)$, $\mathbf{ord}_P(h) = \mathbf{m}_P(H) + \mathbf{ord}_Q(h_Q)$ and $\mathbf{m}_P(G) > 0$, $\mathbf{m}_P(H) > 0$ we have

$$\begin{cases} \mathbf{ord}_P(g) & > & \mathbf{ord}_Q(x^{(\mathbf{m}_P(G)-\mathbf{m}_P(H))}\, g_Q) \\ \mathbf{ord}_P(h) & > & \mathbf{ord}_Q(h_Q)\,. \end{cases}$$

2. If $\mathbf{m}_P(G) < \mathbf{m}_P(H)$, then

$$\pi_Q^*(u) = \frac{g_Q}{x^{(\mathbf{m}_P(H)-\mathbf{m}_P(G))}\, h_Q}$$

and

$$\begin{cases} \mathbf{ord}_P(g) & > & \mathbf{ord}_Q(g_Q) \\ \mathbf{ord}_P(h) & > & \mathbf{ord}_Q(x^{(\mathbf{m}_P(H)-\mathbf{m}_P(G))}\, h_Q)\,. \end{cases}$$

Thus, after a finite number of blowing-ups we recover one of the first two cases.

5.6 Interpolating forms through divisors

Let D be a k-rational effective divisor of $k(\mathcal{C})$; we want to find all the forms $G \in k[X,Y,Z]$ of a fixed degree d such that $(G) \geq D$. Assume that

$$D = \sum_{i=1}^{m} n_i Q_i$$

where the Q_i are places of $k(\mathcal{C})$. Set $r_i = \deg Q_i$ and write (see Section 2)

$$Q_i = \sum_{j=1}^{r_i} \wp_{i,j} ,$$

where $\wp_{i,j}$ are places of degree one of $k_{r_i}(\mathcal{C})$. If we fix $\wp_i = \wp_{i,1}$ and let σ_i be a generator of the Galois group $\mathcal{G}al(k_{r_i}/k)$, we can also write

$$Q_i = \sum_{j=0}^{r_i-1} \wp_i^{\sigma_i{}^j} ,$$

so

$$D = \sum_{i=1}^{m} n_i \sum_{j=0}^{r_i-1} \wp_i^{\sigma_i{}^j} .$$

Then

$$(G) \geq D \iff \mathbf{ord}_{\wp_i}(\overline{G}^{P_i}) \geq n_i, \quad i = 1,2,\ldots,m$$

where $P_i \in \mathcal{C}$ is the unique k_{r_i}-rational point such that either $\wp_i \succ P_i$ or $\wp_i = P_i$. Let $\wp$ be any one of those places $\wp_i$, r its degree and P the corresponding point P_i. We consider the affine plane curve $C^{\wp}$ (see Section 3.4) with affine coordinates (x,y). We suppose that $\{x = 0\}$ is not the tangent line of $C^{\wp}$ at $(0,0)$. Then $C^{\wp}$ has a parametrization in $(0,0)$ [3]

$$\begin{cases} x(t) &= t \\ y(t) &= \sum_{e=1}^{\infty} a_e t^e , \ a_e \in k_r . \end{cases}$$

Notice that if $\wp'$ is conjugated with $\wp$ over k, then the parametrizations of $C^{\wp}$ and $C^{\wp'}$ are conjugated over k.

Now consider all the monomials $H_l \in k[X,Y,Z]$ of degree d ($l = 1,2,\ldots,s = (d+2)(d+1)/2$). Since $\phi_{\wp}^*(\overline{H}_l^P)$ is in $\Gamma(C^{\wp})$ we easily associate to H_l a local power series

$$\phi_{\wp}^*(\overline{H}_l^P)(x(t),y(t)) = \sum_{e=0}^{\infty} b_{l,e} t^e .$$

For any integer n we set

$$\Delta_{\wp}(H_l,n) = \sum_{e<n} b_{l,e} t^e .$$

Then clearly

$$\mathbf{ord}_{\wp}(\overline{H_l}^P) \geq n \iff \Delta_{\wp}(H_l,n) = 0 .$$

[3] It can be obtain using rational Puiseux expansions or Hamburger-Noether expansions (see [4, 2]).

Let $G \in k[X,Y,Z]$ be any form of degree d . We set

$$G = \sum_{l=1}^{s} \alpha_l H_l, \quad \alpha_l \in k \; ;$$

then

$$(G) \geq D \text{ or } \overline{G} = 0 \text{ in } \Gamma(\mathcal{C})$$

is equivalent to

$$(\alpha_1, \ldots, \alpha_s) \in k^s \text{ is a solution of } (\Delta_D) : \left\{ \sum_{l=1}^{s} \alpha_l \Delta_{\wp_i}(H_l, n_i) = 0, \quad i = 1, 2, \ldots, m \; . \right.$$

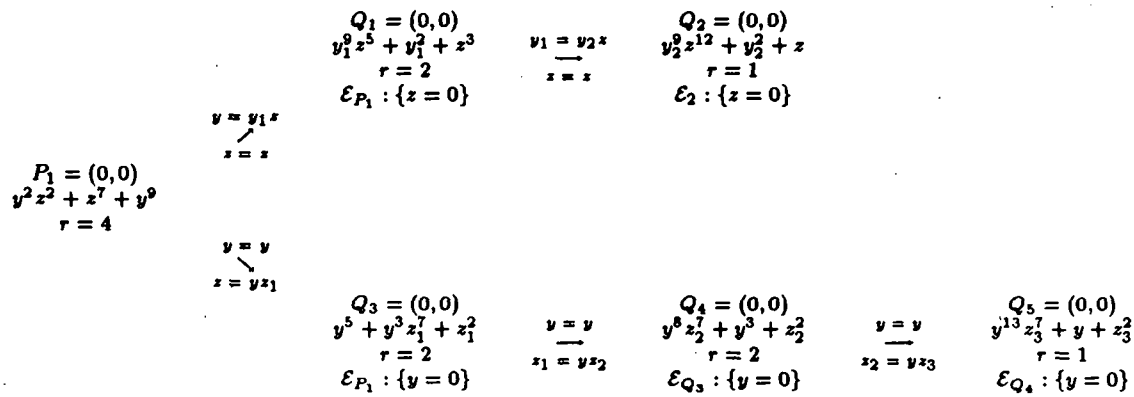
6 Examples

Example 6.1 Consider the plane projective curve $\mathcal{C}$ defined over $k = \mathbb{F}_2$ by the equation

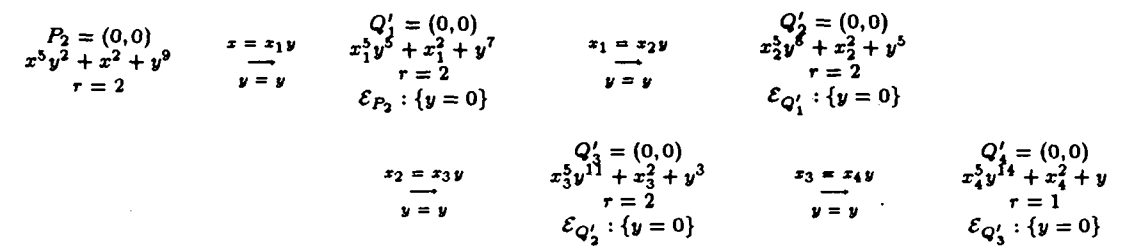
$$F = X^5Y^2Z^2 + X^2Z^7 + Y^9 = 0 \; ;$$

$\mathcal{C}$ has two singular points, $P_1 = (1:0:0)$ and $P_2 = (0:0:1)$, which are in fact the only rational points of $\mathcal{C}$ over k. The desingularization tree $\mathcal{T}$ is composed of two sub-trees, $\mathcal{T}_{P_1}$ and $\mathcal{T}_{P_2}$;

1. Sub-tree $\mathcal{T}_{P_1}$ (here $y = Y/X$ and $z = Z/X$)



2. Sub-tree $\mathcal{T}_{P_2}$ (here $x = X/Z$ and $y = Y/Z$)



We obtain three leaves Q_2, Q_5 and Q'_4 which are rational over k; so the smooth model of $\mathcal{C}$ has three k-rational points. The adjoint divisor is equal to

$$\mathcal{A} \;=\; 8Q_2 + 10Q_5 + 8Q'_4 \,.$$

Applying the genus formula (7), we have

$$g = \frac{(9-1)(9-2)}{2} - \frac{26}{2} = 15 \,.$$

Using the desingularization tree we find

$$\begin{cases} \mathbf{ord}_{Q_2}(\pi^*_{Q_2}(y)) &=& \mathbf{ord}_{Q_2}(y_2 z^2) &=& 5 \\ \mathbf{ord}_{Q_2}(\pi^*_{Q_2}(z)) &=& \mathbf{ord}_{Q_2}(z) &=& 2 \end{cases}$$

$$\begin{cases} \mathbf{ord}_{Q_5}(\pi^*_{Q_5}(y)) &=& \mathbf{ord}_{Q_5}(y) &=& 2 \\ \mathbf{ord}_{Q_5}(\pi^*_{Q_5}(z)) &=& \mathbf{ord}_{Q_5}(y^3 z_3) &=& 7 \end{cases}$$

$$\begin{cases} \mathbf{ord}_{Q'_4}(\pi^*_{Q'_4}(x)) &=& \mathbf{ord}_{Q'_4}(x_4 y^4) &=& 9 \\ \mathbf{ord}_{Q'_4}(\pi^*_{Q'_4}(y)) &=& \mathbf{ord}_{Q'_4}(y) &=& 2 \end{cases}$$

so we have

$$\begin{aligned} (X) &= 9Q'_4 \\ (Y) &= 5Q_2 + 2Q_5 + 2Q'_4 \\ (Z) &= 2Q_2 + 7Q_5 \,. \end{aligned}$$

Now, let $G_0 \in k[X,Y,Z]$ be a form of degree $d \geq 7$ such that [4]

$$(G_0) \geq \mathcal{A} \text{ and } \mathbf{supp}(G_0) \subseteq \mathbf{supp}\mathcal{A}$$

and consider the k-rational divisor

$$D = (G_0) - \mathcal{A} \,.$$

Then $\mathbf{supp}D \subseteq \mathbf{supp}\mathcal{A}$ and by Bézout theorem $\deg D = 9d - 26 > 2g - 2 = 28$; so the dimension of $\mathcal{L}(D)$ is

$$\ell(D) = \deg(D) - g + 1 = 9d - 26 - 15 + 1 = 9d - 40 \,.$$

To obtain a basis for $\mathcal{L}(D)$, we apply Theorem 4.3 and search forms G of degree d, not divisible by F and such that

$$(G) \geq (G_0) - D = \mathcal{A} \,.$$

[4]Such a form exists: for instance we could take $G_0 = Y^7$ and then $(G_0) = 35Q_2 + 14Q_5 + 14Q'_4$.

For this we consider the k-vector space V_d which has for basis all the monomials given by the following table

$X^iY^jZ^l,\ i+j+l=d$	Number of such monomials
$i \geq 0,\ j \geq 5,\ l \geq 0$	$(d-4)(d-3)/2$
$i \geq 0,\ j = 4,\ l \geq 1$	$d-4$
$i \geq 1,\ j = 3,\ l \geq 1$	$d-4$
$i \geq 1,\ j = 2,\ l \geq 1$	$d-3$
$i \geq 1,\ j = 1,\ l \geq 2$	$d-3$
$i \geq 1,\ j = 0,\ l \geq 4$	$d-4$

So we have

$$\dim_k V_d = (d-4)(d-2)/2 + 5d - 18\,.$$

Looking at the divisors $(X), (Y)$ and (Z), one can easily show that

$$G \in V_d \Rightarrow \overline{G} = 0 \text{ or } (G) \geq \mathcal{A}\,.$$

Consider the k-vector space

$$V'_d = \{\ G' \in k[X,Y,Z]\ \mid\ G' \text{ a form of degree d such that } F \text{ divides } G'\ \}\,.$$

Clearly, for $d = 7$ or $d = 8$, we have $\dim_k V'_d = 0$. Consider the case $d = 9$. Since all the monomials occuring in F belong to V_d, V'_d is a subspace of V_d. It follows easily that the same is true also for $d \geq 9$ and a basis for V'_d is $\{\ HF\ \mid\ H \in k[X,Y,Z]$ a monomial of degree $d-9\ \}$. Thus in any cases $(d \geq 7)$ we have

$$\dim_k V'_d = \frac{(d-7)(d-8)}{2}\,.$$

Hence

$$\dim_k V_d - \dim_k V'_d = (d-4)(d-2)/2 + 5d - 18 - (d-7)(d-8)/2 = 9d - 40 = \ell(D)$$

so that

$$\mathcal{L}(D) = \left\{\ \overline{G}/\overline{G}_0\ \mid\ G \in V_d \setminus V'_d\ \right\} \cup \{0\}\,.$$

Since the divisor D is rational over $\mathbb{F}_2$ we can use it to construct a code over any extension of $\mathbb{F}_2$. For instance, over $\mathbb{F}_{32}$ the curve $\mathcal{C}$ has 155 rational simple points so its smooth model has 158 rational points [5]. Since $\mathbf{supp}D \subseteq \mathbf{supp}\mathcal{A}$ we may take for divisor $\mathcal{P}$ the sum of the 155 rational simple points and for $d \geq 7$ and $9d - 40 < 155$ we may construct a class of codes with the following parameters

$$\begin{aligned} \text{lenght} &= 155 \\ \text{dimension} &= 9d - 40 \\ \text{designed distance} &= 155 - (9d - 26) = 181 - 9d\,. \end{aligned}$$

[5] In [10, ex. 6 p.815] it is said that the smooth model has 157 rational points over $\mathbb{F}_{32}$ and $g = 26$. In the same example, for the curve with equation $X^3YZ^{10} + X^{13}Z + Y^{14} = 0$ one can prove that the genus is in fact $g = 63$ and that there are 892 rational points on the smooth model over $\mathbb{F}_{2^7}$.

We summarize in the following table

d	dimension	designed distance
7	23	118
8	32	109
9	41	100
$\vdots$	$\vdots$	$\vdots$
20	140	1

Over $\mathbb{F}_{2^{10}}$ the curve $\mathcal{C}$ has 837 rational points, excluding the two singular points. With the same construction we obtain codes of length 837 with dimension and designed distance

d	dimension	designed distance
7	23	800
8	32	791
9	41	782
$\vdots$	$\vdots$	$\vdots$
95	815	8 .

Example 6.2 We construct an AG-code $C_L(\mathcal{X}, \mathcal{P}, D)$ where all the rational points of $\mathcal{X}$ appear in the support of $\mathcal{P}$. For that, as in [12, p. 248-] , we consider the projective plane curve $\mathcal{C}$ defined by the equation

$$F = X^5 + Y^2Z^3 + YZ^4 = 0 .$$

Over $k = \mathbb{F}_{16}$ this curve has 33 rational points with $P_1 = (0 : 1 : 0)$ as a unique singular point. The desingularization tree is (with $x = X/Y$ and $z = Z/Y$)

$$\begin{array}{c} P_1 = (0,0) \\ x^5 + z^3 + z^4 \\ r = 3 \end{array} \xrightarrow[z = xz_1]{x = x} \begin{array}{c} Q_1 = (0,0) \\ x^2 + xz_1^4 + z_1^3 \\ r = 2 \\ \mathcal{E}_1 : \{x = 0\} \end{array} \xrightarrow[z_1 = z_1]{x = x_1 z_1} \begin{array}{c} Q_2 = (0,0) \\ x_1^2 + x_1 z_1^3 + z_1 \\ r = 1 \\ \mathcal{E}_2 : \{z_1 = 0\} \end{array}$$

and the adjunction divisor is [6]

$$\mathcal{A} = 8Q_2 .$$

Let $\mathcal{P} = Q_2 + P_2 + P_3 + \cdots + P_{33}$ where, if β is a primitive root of $x^4 + x + 1$, we have

$$\begin{array}{lllllll} Q_2 & \succ & (0:1:0) & P_4 & = & (\beta : \beta : 1) & P_8 = (\beta^{13} : \beta : 1) \\ P_2 & = & (0:0:1) & P_5 & = & (\beta^4 : \beta : 1) & P_9 = (\beta^3 : \beta^5 : 1) \\ P_3 & = & (0:1:1) & P_6 & = & (\beta^7 : \beta : 1) & P_{10} = (\beta^9 : \beta^5 : 1) \\ & & & P_7 & = & (\beta^{10} : \beta : 1) & P_{11} = (1 : \beta^{10} : 1) \end{array}$$

and the conjugate points over $\mathbb{F}_2$ of $P_4, P_5, \ldots, P_{11}$. We need a k-rational divisor D with support disjoint from the support of $\mathcal{P}$. We consider the place α of $k(x)/k$ associated to the irreducible polynomial $(x^3 + x^2 + 1)$. Since $k(\mathcal{C}) = k(x, y)$, where $y^2 + y + x^5 = 0$, $k(\mathcal{C})/k$

[6] Note that there is a misprint in [12].

is an extension of degree 2 of $k(x)/k$ and there are two places $\wp_1$, $\wp_2$ of degree 3 in $k(C)/k$ dividing α. If a is a primitive root of x^3+x^2+1, then we have

$$\begin{aligned}\wp_1 &= (a:a^2:1)+(a^2:a^4:1)+(a^4:a:1) &&= P_1'+P_2'+P_3'\\ \wp_2 &= (a:a^3:1)+(a^2:a^6:1)+(a^4:a^5:1) &&= P_4'+P_5'+P_6'.\end{aligned}$$

We set

$$D=\wp_1+\wp_2$$

which, as requested, is a k-rational divisor with support disjoint from $\mathbf{supp}\,\mathcal{P}$. In fact, D is $\mathbb{F}_2$-rational so that $\mathcal{L}(D)$ has a $\mathbb{F}_2$-rational basis. According to Theorem 4.3 we need a form $G_0\in\mathbb{F}_2[X,Y,Z]$ such that

$$(G_0)\geq\mathcal{A}+D\,.$$

We use the method described in Section 5.6. The affine plane curve C^{Q_2} has for equation $x_1^2+x_1z_1^3+z_1=0$ and its parametrization at Q_2 is

$$Q_2:\begin{cases}x_1(t) &= t\\ z_1(t) &= t^2+t^7+\cdots\,.\end{cases}$$

On the affine part of C with $Z=1$ we find the following parametrizations at P_1' and P_4'

$$P_1':\begin{cases}x(t) &= a+t\\ y(t) &= a^2+a^4t+\cdots\end{cases}$$

$$P_4':\begin{cases}x(t) &= a+t\\ y(t) &= a^3+a^4t+\cdots\end{cases}$$

With the monomials of degree three, the linear system $\Delta_{\mathcal{A}+D}$ yields a unique solution

$$G_0=X^3+X^2Z+Z^3.$$

Indeed we have

$$(G_0)=9Q_2+D\,.$$

Next we look for the forms G of degree 3 such that

$$(G)\geq(G_0)-D=9Q_2.$$

Using the same method as before we have

$$\begin{aligned}(X) &= 3Q_2+P_2+P_3\\ (Y) &= 5P_2\\ (Z) &= 5Q_2\end{aligned}$$

and applying Theorem 4.3 it follows that a basis for $\mathcal{L}(D)$ is

$$\mathcal{B}=\left\{\overline{X^3}/\overline{G_0},\ \overline{X^2Z}/\overline{G_0},\ \overline{XZ^2}/\overline{G_0},\ \overline{YZ^2}/\overline{G_0},\ \overline{Z^3}/\overline{G_0}\right\}\,.$$

The code $C_L(\mathcal{X}, \mathcal{P}, D)$ has the following parameters

$$\begin{aligned} \text{lenght} &= 33 \\ \text{dimension} &= 5 \\ \text{designed distance} &= 27\,. \end{aligned}$$

To compute the generator matrix, we evaluate the elements of $\mathcal{B}$ at the points $Q_2, P_2, \ldots, P_{11}$

	Q_2	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}	P_{11}
$\overline{X^3}/\overline{G_0}$	1	0	0	β^5	β^5	β^4	β^{10}	β	β^{14}	β^7	1
$\overline{X^2Z}/\overline{G_0}$	0	0	0	β^4	β	β^{12}	1	β^3	β^{11}	β^{13}	1
$\overline{XZ^2}/\overline{G_0}$	0	0	0	β^3	β^{12}	β^5	β^5	β^5	β^8	β^4	1
$\overline{YZ^2}/\overline{G_0}$	0	0	1	β^3	β^9	β^{14}	β^{11}	β^8	β^{10}	1	β^{10}
$\overline{Z^3}/\overline{G_0}$	0	1	1	β^2	β^8	β^{13}	β^{10}	β^7	β^5	β^{10}	1

and add the 24 columns obtained respectively by conjugation over $\mathbb{F}_2$ of the columns corresponding to $P_4, \ldots, P_{11}$. Putting the generator matrix in its row echelon form one could easily see that the minimun distance is equal to the designed distance.
Since $\mathcal{C}$ is a hyperelliptic curve the dual code of $C_L(\mathcal{C}, \mathcal{P}, D)$, which is a $[33, 5, d^* = 4]$-code, can be decoded using [3].

7 Conclusion

Three main tasks have to be performed for the construction of an AG-code $C_L(\mathcal{X}, \mathcal{P}, D)$, given a plane model $\mathcal{C}$ of $\mathcal{X}$:

1. finding all the rational and singular points of $\mathcal{C}$,
2. computing the desingularization tree of $\mathcal{C}$,
3. interpolating forms through divisors,
4. solving linear system of equations.

Those four tasks must be done over finite fields. The following activities are involved

1. Gröbner basis computation,
2. operations on polynomials such as substitution of variables and factorization,
3. operations on series which are best done using lazy evaluation: this means that only the needed terms of the series are computed,
4. linear algebra computation.

All the above are implemented in most computer algebra systems. For our implementation we have chosen AXIOM. The reason for this choice is that AXIOM is object oriented. This allows clearer and easier programming and, most of all, it enables us to define the implementation over any finite field.

References

[1] M. Bronstein, M. Hassner, A. Vasquez and C.J. Williamson, *Algebraic algorithms for the construction of error correction codes on algebraic curves*, Proceedings of IEEE International Symposium on Information Theory, June 1991.

[2] A. Campillo, *Algebroid Curves in Positive Characteristic*, Lect. Notes in Math. 813, Springer-Verlag, 1980.

[3] I.M. Duursma, *Algebraic decoding using special divisors*, IEEE Trans. Info. Th., vol. 35, no 2, March 1993, 694-698.

[4] D. Duval, *Rational Puiseux Expansions*, Compositio Math. 70 (1989), 119-154.

[5] V.D. Goppa, *Codes associated with divisors*, Probl. Peredach. infor., 13(1):33-39, 1977.

[6] D. Gorenstein, *An arithmetic theory of adjoint plane curves*, Trans. Amer. Math. Soc. 72 (1952), 414-436.

[7] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag 1977.

[8] H. Hironaka, *On the arithmetic genera and the effective genera of algebraic curves*, Memoirs of the College of Sciences of Kyoto, Series A, 30, Math. 2 (1957),177-195.

[9] M.D. Huang and D. Ierardi, *Efficient algorithms for Riemann-Roch problem and for addition in the jacobian of a curve*, IEEE Trans. Info. Th., July 1991, 678-687.

[10] J. Justessen, K.J. Larsen, H.E. Jensen, A. Havemose and T. Hoholdt, *Construction and Decoding of a Class of Algebraic Geometry Codes*, IEEE Trans. Info. Th. 35, no 4, July 1989, 811-821.

[11] D. Lazard, *Solving zero-dimensional algebraic systems*, J. Symbolic Cumputation, 13, 1992.

[12] D. Le Brigand and J.J. Risler, *Algorithme de Brill-Noether et codes de Goppa*, Bull. Soc. math. France, 116 (1988), 231-253.

[13] D. Polemi, M. Hassner, O. Moreno and C.J. Williamson, *A computer algebra algorithm for the adjoint divisor*, Proceedings of IEEE International Symposium on Information Theory, January 1993.

[14] H. Stichtenoth, *Algebraic function fields and codes*, University Text, Springer-Verlag, 1993.

[15] M.Tsfasman and S. Vladut, *Algebraic-geometric codes*, Kluwer Academic Pub., Math. and its Appl. 58, 1991.

[16] A.T. Vasquez, *Rational desingularization of a curve defined over a finite field*, Number Theory, N. Y. Seminar 1989-1990, Springer-Verlag, 229-250.

Unité de recherche INRIA Rocquencourt
Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

Unité de recherche INRIA Lorraine - Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 Villers lès Nancy Cedex (France)
Unité de recherche INRIA Rennes - IRISA, Campus universitaire de Beaulieu 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 Grenoble Cedex 1 (France)
Unité de recherche INRIA Sophia Antipolis - 2004, route des Lucioles - B.P. 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 Le Chesnay Cedex (France)

ISSN 0249 - 6399