J. Symbolic Computation (1996) **11**, 1–000

Rational Parametrizations of Algebraic Curves using a Canonical Divisor

Mark van Hoeij
Department of mathematics
University of Nijmegen
6525 ED Nijmegen
The Netherlands
e-mail: hoeij@sci.kun.nl

(Received 30 September 1996)

For an algebraic curve $\mathbf{C}$ with genus 0 the vector space $\mathcal{L}(D)$ where D is a divisor of degree 2 gives rise to a bijective morphism g from $\mathbf{C}$ to a conic $\mathbf{C}_2$ in the projective plane. We present an algorithm that uses an integral basis for computing $\mathcal{L}(D)$ for a suitably chosen D. The advantage of an integral basis is that it contains all the necessary information about the singularities, so once the integral basis is known the $\mathcal{L}(D)$ algorithm does not need work with the singularities anymore. If the degree of $\mathbf{C}$ is odd, or more generally, if any odd degree rational divisor on $\mathbf{C}$ is known then we show how to construct a rational point on $\mathbf{C}_2$. In such cases a rational parametrization, which means defined without algebraic extensions, of $\mathbf{C}_2$ can be obtained. In the remaining cases a parametrization of $\mathbf{C}_2$ defined over a quadratic algebraic extension can be computed. A parametrization of $\mathbf{C}$ is obtained by composing the parametrization of $\mathbf{C}_2$ with the inverse of the morphism g.

1. Introduction and Outline

There exist several algorithms for computing parametrizations of algebraic curves $\mathbf{C}$ with genus $g(\mathbf{C}) = 0$. To parametrize a curve means to compute a birational equivalence of the curve with a projective line $\mathbf{P}^1$. This means computing an isomorphism between the function field of the curve $\mathbf{C}$ and the function field of the projective line. The algorithms in (Sendra and Winkler, 1991; 1993; 1994) and (Hilbert and Hurwitz, 1890) produce parametrizations using an algebraic extension of the constants of degree at most 2.

In (van Hoeij, ISSAC1994) an algorithm is given that, given a point on the curve, computes a parametrization. When a rational† point is given the algorithm performs well. But if no point is given this algorithm will choose a point, which can introduce a large (at most the degree of the curve) algebraic extension. Then the algorithm produces

† in this paper "rational" means: defined over the same constants field L over which the curve itself is defined. More precisely: invariant under the action the Galois group $\mathrm{Gal}(\overline{L}/L)$.

0747–7171/90/000000 + 00 \$03.00/0

a parametrization over this algebraic extension. The use of a possibly large algebraic extension is a disadvantage of this approach. Basically the method consists of computing a divisor D on the curve, consisting of only 1 point, and then computing $\mathcal{L}(D)$ using integral basis computation. The problem with the method is that the divisor D need not be rational, and the algebraic extension used to denote this divisor appears in the output as well.

The approach in this paper is to compute a vector space $\mathcal{L}(D)$ where now D is a rational divisor (note: this does not mean that the places in D are rational, only that D itself is invariant under the Galois group). We can take D equal to -1 times a canonical divisor. It follows from the Riemann-Roch theorem that the degree of D is $-1 \cdot (2g(\mathbf{C}) - 2) = 2$ and the dimension of $\mathcal{L}(D)$ is 3. The main new results in this paper consist of several tricks for computing a basis g_1, g_2, g_3 of $\mathcal{L}(D)$ in an efficient way. The map (g_1, g_2, g_3) from the curve $\mathbf{C}$ to the projective plane $\mathbf{P}^2$ is a bijective morphism from $\mathbf{C}$ to a conic $\mathbf{C}_2$ in $\mathbf{P}^2$. We can compute the inverse morphism, so a morphism from $\mathbf{C}_2$ to $\mathbf{C}$. Now a parametrization of $\mathbf{C}$ is found by computing a parametrization of $\mathbf{C}_2$, and composing it with the morphism from $\mathbf{C}_2$ to $\mathbf{C}$.

The problem that remains is to compute a parametrization of the conic $\mathbf{C}_2$, preferably a rational parametrization. Note that we can always find a point over an algebraic extension of degree ≤ 2 by intersecting $\mathbf{C}_2$ with a line. So we can always compute a parametrization using an algebraic extension of degree ≤ 2. It is known that if the degree of $\mathbf{C}$ is odd then $\mathbf{C}$ has a rational point. So in such cases it must be possible to construct a rational point on the conic $\mathbf{C}_2$. We use the following approach to find such a point. Construct (if possible) a rational divisor of odd degree on $\mathbf{C}$. This can be done if we can find a place on $\mathbf{C}$ that is defined over an algebraic extension of odd degree. For example if the degree of the curve is odd such a place can be found by intersecting the curve with a line. Or if one of the Puiseux series that were used in the integral basis algorithm is algebraic of odd degree. Then construct a rational divisor on $\mathbf{C}_2$ from this. After adding to this divisor a suitable multiple of the divisor consisting of the two points at infinity we obtain a divisor D_2 on $\mathbf{C}_2$ of degree 1. Then the quotient G_1/G_2, where G_1, G_2 is a basis of $\mathcal{L}(D_2)$, has one unique pole on $\mathbf{C}_2$. This will be a rational point P on the curve $\mathbf{C}_2$. We can use it to compute a rational parametrization of $\mathbf{C}_2$. By composing this with the morphism from $\mathbf{C}_2$ to $\mathbf{C}$ a rational parametrization of $\mathbf{C}$ is obtained. Or, instead of computing the inverse of the morphism (g_1, g_2, g_3) we can use the point P to construct a rational parameter (a parameter is generator of the function field of $\mathbf{C}$). This parameter is a bijective morphism from $\mathbf{C}$ to $\mathbf{P}^1$. A parametrization of $\mathbf{C}$ is then obtained by computing the inverse morphism from $\mathbf{P}^1$ to $\mathbf{C}$.

So for any odd degree curve we can compute a rational parametrization and for even degree curves a parametrization defined over a field extension of degree ≤ 2. The algorithm in this paper is implemented and is available via WWW from
`http://www-math.sci.kun.nl/math/compalg/IntBasis`
and by e-mail request. Note: the name of the IntBasis package has been changed. It is now called `algcurves` and will be included in the next version of Maple.

2. Preliminaries, notations and assumptions

In this paper the ground field is $\mathbb{Q}$. The algorithm works over other ground fields L of characteristic 0 as well, provided that one has the basic computer algebra tools for L like algorithms for solving linear equations and factoring polynomials over L.

In this section we list our notations and a number of facts about algebraic curves. For proofs and more facts see Chapter IV in (Hartshorne, 1977), or (Griffiths and Harris, 1978).

- F is a homogeneous polynomial of degree n in $\mathbb{Q}[x, y, z]$ which is irreducible over $\overline{\mathbb{Q}}$. Then F defines an irreducible algebraic curve $\mathbf{C}(\mathbf{P}^2)$ in the projective plane $\mathbf{P}^2 = \mathbf{P}^2(\overline{\mathbb{Q}})$. $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$.
- $\overline{\mathbb{Q}}(\mathbf{C})$ is the function field of this curve. Denote $f = F_{z=1}$, i.e. f is F with $z = 1$ substituted. The function field $\overline{\mathbb{Q}}(\mathbf{C})$ can be identified with $\overline{\mathbb{Q}}(x)[y]/(f)$.
- A place P on the curve is a discrete valuation ring $\overline{\mathbb{Q}} \subset P \subset \overline{\mathbb{Q}}(\mathbf{C})$ such that $\overline{\mathbb{Q}}(\mathbf{C})$ is the fraction field of P. A place P corresponds to a discrete valuation
$$v_P : \overline{\mathbb{Q}}(\mathbf{C}) \to \mathbb{Z} \bigcup \{\infty\}.$$
The algebraic curve $\mathbf{C}$ is the set of all places P. Every place P of $\mathbf{C}$ contains a local ring of precisely one point on the curve $\mathbf{C}(\mathbf{P}^2)$. This defines a map
$$\mathbf{C} \to \mathbf{C}(\mathbf{P}^2) \subset \mathbf{P}^2. \tag{2.1}$$
The local ring of a point P is a place if and only if P is a regular point. So we can identify a regular point with a place. This way we can view $\mathbf{C}$ as the set $\mathbf{C}(\mathbf{P}^2)$ minus the set of singularities plus the set of places above the singularities.
- A non-constant morphism from a curve $\mathbf{C}_1$ to a curve $\mathbf{C}_2$ is a pair (m, g) such that $g : \overline{\mathbb{Q}}(\mathbf{C}_2) \to \overline{\mathbb{Q}}(\mathbf{C}_1)$ is a $\overline{\mathbb{Q}}$-homomorphism (hence an embedding) and $m : \mathbf{C}_1 \to \mathbf{C}_2$ is a map such that for any place $P \in \mathbf{C}_1$ we have $m(P) = \{h \in \overline{\mathbb{Q}}(\mathbf{C}_2) | g(h) \in P\}$, i.e. $m(P) = g^{-1}(P)$. The degree of this morphism is the degree of the field extension $g(\overline{\mathbb{Q}}(\mathbf{C}_2)) \subset \overline{\mathbb{Q}}(\mathbf{C}_1)$.
- For elements $g \in \overline{\mathbb{Q}}[x, y]$ denote $\deg(g)$ as the degree of g in x and y, i.e. the maximal $i + j$ for which the monomial $x^i y^j$ has a non-zero coefficient in g. Write $\deg_y(g)$ as the degree of g considered as a polynomial in y.
By abuse of notation we will consider the symbols x and y as variables but also as elements of the function field $\overline{\mathbb{Q}}(\mathbf{C}) = \overline{\mathbb{Q}}(x)[y]/(f)$. An element $h \in \overline{\mathbb{Q}}(x)[y]/(f)$ can be represented in a unique way as a polynomial in y of degree $< \deg_y(f)$ with coefficients in $\overline{\mathbb{Q}}(x)$. It can also be represented as h_1/h_2 where $h_1 \in \overline{\mathbb{Q}}[x, y]$ with $\deg_y(h_1) < \deg_y(f)$ and $h_2 \in \overline{\mathbb{Q}}[x]$.
- We assume that $\deg_y(f) = \deg(f) = n$. This is equivalent with the assumption that $(0, 1, 0)$ is not a point on the curve. It implies that y in $\overline{\mathbb{Q}}(\mathbf{C})$ is integral over $\overline{\mathbb{Q}}[x]$. "Integral over a ring R" means "root of a monic polynomial over R". Then the map
$$(x, y, z) \in \mathbf{C}(\mathbf{P}^2) \mapsto (x, z) \in \mathbf{P}^1 \tag{2.2}$$
is defined. Combined with (2.1) this gives a morphism from $\mathbf{C}$ to $\mathbf{P}^1$. This morphism corresponds to the embedding of the function field $\overline{\mathbb{Q}}(x)$ of $\mathbf{P}^1$ in the function field $\overline{\mathbb{Q}}(\mathbf{C})$ of $\mathbf{C}$. Denote e_P for a place P on $\mathbf{C}$ as the ramification index of this morphism.
A second assumption is that $F_{z=0,x=1} \in \mathbb{Q}[y]$ is square-free. This means that the points at infinity (the points on the line $z = 0$) are regular and are not ramified (i.e. have ramification index 1). The two assumptions can be satisfied by applying a linear transformation on x, y, z in F.
- $\overline{\mathbb{Q}}(\mathbf{C})$ can also be identified with the field $\overline{\mathbb{Q}}(z)[y]/(F_{x=1})$. We can write elements of $\overline{\mathbb{Q}}(\mathbf{C})$ as rational functions in x and y, but also as rational functions in z and y. A conversion from a function in x-y syntax to z-y syntax is done by first making the

function homogeneous (multiply all terms in the numerator and denominator by a suitable power of z such that the numerator and denominator become homogeneous polynomials of the same degree) and then substituting $x = 1$. The function $x^i y^j$ is, written in z-y syntax, equal to y^j/z^{i+j}.
In both syntaxes we always write elements of the function field as polynomials in y of degree $< n$, with rational functions in x or z as coefficients.

- A place is called finite if $v_P(x) \geq 0$ (in other words: $x \in P$) and infinite if $v_P(x) < 0$ (then $v_P(x) = -1$ because of the assumption that there are no ramification points at infinity). Denote $\mathbf{A} \subset \mathbf{C}$ as the set of finite places. This corresponds to the part of the curve on the affine plane $\mathbf{A}^2 = \{(x, y, 1) | x, y \in \overline{\mathbb{Q}}\} \subset \mathbf{P}^2$. Denote $\mathbf{B} \subset \mathbf{C}$ as the set of infinite places. This corresponds to the part of the curve on the line $z = 0$. Denote
$$O_{\mathbf{A}} = \bigcap_{P \in \mathbf{A}} P \quad \text{and} \quad O_{\mathbf{B}} = \bigcap_{P \in \mathbf{B}} P.$$
O_A is the set of functions with no poles on the affine part of the curve and O_B is the set of functions with no poles at infinity. So $O_A \bigcap O_B$ is the set of functions with no poles on the curve, hence equal to $\overline{\mathbb{Q}}$.
O_A is the integral closure of $\overline{\mathbb{Q}}[x]$ (this is the set of functions in the function field of $\mathbf{P}^1$ with no poles except at infinity) in the function field.
O_B is the integral closure of $\overline{\mathbb{Q}}[z]_{(z)}$ (this is the set of functions in the function field of $\mathbf{P}^1$ that have no pole at $z = 0$) in the function field.
- A divisor D is a formal $\mathbb{Z}$-linear combination of places
$$D = \sum_{P \in \mathbf{C}} n_P \cdot P$$
where $n_P \in \mathbb{Z}$ is zero in all but a finite number of places $P \in \mathbf{C}$. The set $\mathcal{L}(D)$ is defined as
$$\mathcal{L}(D) = \{g \in \overline{\mathbb{Q}}(\mathbf{C}) | v_P(g) + n_P \geq 0 \ \text{ for all } \ P \in \mathbf{C}\}.$$
This is a $\overline{\mathbb{Q}}$-vector space (note that $0 \in \mathcal{L}(D)$ because $v_P(0) = \infty$). The degree of the divisor D is defined as
$$\deg(D) = \sum_{P \in \mathbf{C}} n_P.$$
Assume that the genus $g(\mathbf{C})$ of the curve is 0. If $\deg(D) \geq 0$ then
$$\dim(\mathcal{L}(D)) = \deg(D) + 1$$
according to the Riemann-Roch theorem. Suppose g_1 and g_2 are non-zero elements of $\mathcal{L}(D)$ and $h = g_1/g_2$ is not a constant. Then the number of poles (which is also the number of roots) N, counted with multiplicity, of h is $\leq \deg(D)$. Then $\overline{\mathbb{Q}}(h) \subset \overline{\mathbb{Q}}(\mathbf{C})$ is a field extension of degree N. For generic elements g_1, g_2 this number N equals $\deg(D)$.
If the divisor D has degree 2 and g_1, g_2, g_3 is a basis of $\mathcal{L}(D)$ then the 6 products $g_i g_j$, $1 \leq i \leq j \leq 3$ span the vector space $\mathcal{L}(2D)$ of dimension 5 (proof: choose a place P. For divisors of the form $2P$ it is easy to see that the statement holds. Then it also holds for D by writing D as $2P$ plus the divisor of an element of the function field). So these products are linearly dependent and hence g_1, g_2, g_3 satisfy

a homogeneous polynomial relation $F_2(g_1, g_2, g_3) = 0$ of degree 2. Let $\mathbf{C}_2$ be the curve defined by F_2. Then the map

$$(g_1, g_2, g_3) : \mathbf{C} \to \mathbf{C}_2(\mathbf{P}^2) \subset \mathbf{P}^2 \tag{2.3}$$

defines a morphism from $\mathbf{C}$ to $\mathbf{C}_2$. The function field of the image of this morphism is $\overline{\mathbb{Q}}(g_1/g_3, g_2/g_3)$. The morphism corresponds to the embedding of this field in the function field $\overline{\mathbb{Q}}(\mathbf{C})$ of $\mathbf{C}$. It is bijective (i.e. it has degree 1) because

$$\overline{\mathbb{Q}}(\frac{g_1}{g_3}, \frac{g_2}{g_3}) = \overline{\mathbb{Q}}(\mathbf{C}). \tag{2.4}$$

To see that this equation holds note that $g_1/g_3, g_2/g_3, 1$ is a basis of $\mathcal{L}(P_1 + P_2)$ for some places P_1 and P_2 on $\mathbf{C}$. Choose a non-constant element $h \in \mathcal{L}(P_1)$. A function h with only 1 pole generates the function field, so $\overline{\mathbb{Q}}(\mathbf{C}) = \overline{\mathbb{Q}}(h)$. Now $\mathcal{L}(P_1) \subset \mathcal{L}(P_1 + P_2)$ so h is a $\overline{\mathbb{Q}}$-linear combination of $g_1/g_3, g_2/g_3, 1$ hence $\overline{\mathbb{Q}}(h) \subset \overline{\mathbb{Q}}(g_1/g_3, g_2/g_3)$. The fact that (g_1, g_2, g_3) is a bijective morphism from $\mathbf{C}$ to a curve in $\mathbf{P}^2$ of degree $\deg(D) = 2$ can also be found in (Hartshorne, 1977), Chapter IV, Example 3.3.2, page 309.

- Let K be the divisor of the differential dx, K is called a canonical divisor. From the assumption that there are no ramification points at infinity it follows that

$$K = (\sum_{P \in \mathbf{A}} (e_P - 1)P) - (2 \sum_{P \in \mathbf{B}} P).$$

Denote $D = -K$. The degree of a canonical divisor is $2g(\mathbf{C}) - 2 = -2$, so

$$\deg(D) = 2.$$

Denote "the divisor of the line at infinity"

$$D_\infty = \sum_{P \in \mathbf{B}} P$$

The elements of $\mathcal{L}(2D_\infty)$ have pole order ≤ 2 on $\mathbf{B}$, in other words: they are elements of $\frac{1}{z^2} O_{\mathbf{B}}$. Furthermore they have no poles on $\mathbf{A}$, which means that they are elements of $O_{\mathbf{A}}$ as well. Since $D \leq 2D_\infty$ we have

$$\mathcal{L}(D) \subset \mathcal{L}(2D_\infty) = O_A \bigcap \frac{1}{z^2} O_B.$$

We briefly summarize the assumptions that were done:

1 $F \in \mathbb{Q}[x, y, z]$ is a homogeneous polynomial of degree n.
2 The curve in $\mathbf{P}^2$ given by F is irreducible over $\overline{\mathbb{Q}}$ and has genus 0.
3 $f = F_{z=1}$ has degree n as a polynomial in y.
4 $F_{z=0,x=1} \in \mathbb{Q}[y]$ is square-free.

Assumptions 3 and 4 can be satisfied by applying a linear transformation on F.

3. Rational parametrization by a conic

The topic in this section is computing, for a given curve $\mathbf{C}$, a birational equivalence with a conic $\mathbf{C}_2$. The steps in the following algorithm are explained in sections 3.1, 3.2 and 3.3.

Algorithm Rational Parametrization by a conic
Input: $f \in \mathbb{Q}[x,y]$ such that f is irreducible in $\overline{\mathbb{Q}}[x,y]$ and has genus 0, and two variables s and t.
Output: A polynomial $f_2 \in \mathbb{Q}[s,t]$ of degree ≤ 2 and two elements $X(s,t)$ and $Y(s,t)$ of $\mathbb{Q}(s)[t]/(f_2)$ giving a bijective morphism from the curve $\mathbf{C}_2$ defined by f_2 to the curve $\mathbf{C}$ defined by f. In a number of cases a rational point P on $\mathbf{C}_2$ will be given in the output as well.

1 $n := \deg(f)$
2 **if** $n \neq \deg_y(f)$ **then** apply recursion on $f_{x=x+y}$ (f with $x+y$ substituted for x) **end if**
3 $F :=$ the homogeneous element of $\mathbb{Q}[x,y,z]$ of degree n for which $f = F_{z=1}$.
4 **if** $F_{z=0,x=1}$ is not square-free **then** apply recursion on $(F_{z=z+x})_{z=1}$ **end if**
5 Compute an integral basis (a basis of the $\overline{\mathbb{Q}}[x]$-module O_A) $b_0, \ldots, b_{n-1}$ of the form $b_i = b_{i,1}/b_{i,2}$ with $b_{i,2} \in \mathbb{Q}[x]$ monic and where $b_{i,1} \in \mathbb{Q}[x,y]$ is monic in y with $\deg_y(b_{i,1}) = i$.
6 **if** $(n-1)(n-2)/2 - \sum_i \deg(b_{i,2}) \neq 0$ **then exit** "the genus is not 0" **end if**
7 $d := b_{n-1,2}$
8 Compute a basis $1, R_0/d, \ldots, R_{n-1}/d$ of $\mathcal{L}(D_\infty)$.
9 $v := (1, R_0/d, \ldots, R_{n-1}/d, xR_0/d, \ldots, xR_{n-1}/d)$ is a basis for $\mathcal{L}(2D_\infty)$.
10 $a := \frac{dy}{dx} \in \mathbb{Q}(x)[y]/(f)$.
11 $v :=$ a basis for those elements g in the vector space spanned by v for which $ga \in O_A$.
12 $i := n$
13 **while** the number of elements in the basis v is > 3 **do**

(a) $i := i - 1$
(b) $a := \frac{db_i}{dx}$
(c) $v :=$ a basis for those elements g in the vector space spanned by v for which $ga \in O_A$.

end do
14 $g_i := d$ times the i-th element of v for $i = 1,2,3$.
15 $F_2(s,t,u) := \sum a_{jk} s^j t^k u^{2-j-k}$, $0 \leq j \leq 2$, $0 \leq k \leq 2-j$ where the a_{jk}, s, t and u are variables.
16 $i := 0$
17 **while** the number of variables a_{jk} in F_2 is more than 1 **do**

(a) $r :=$ the remainder of a division of $(F_2(g_1, g_2, g_3))_{x=i}$ by $f_{x=i}$
(b) Solve the system $\{\text{coefficient}(r,y,j) = 0 | j = 0, \ldots, n-1\}$ and substitute the solution into F_2.
(c) $i := i + 1$

end do
18 Substitute the value 1 for the one remaining variable a_{jk} in F_2.
19 **if** $\deg_s(F_2) = 1$ or $\deg_u(F_2) = 1$ **then** apply a permutation on s, t, u to obtain $\deg_t(F_2) = 1$ and apply the same permutation on g_1, g_2, g_3. **end if**
20 $f_2 := (F_2)_{u=1}$
21 Now $\frac{g_1}{g_3} \mapsto s$ and $\frac{g_2}{g_3} \mapsto t$ gives an isomorphism from $\overline{\mathbb{Q}}(x)[y]/(f) = \overline{\mathbb{Q}}(\frac{g_1}{g_3}, \frac{g_2}{g_3})$ to $\overline{\mathbb{Q}}(s)[t]/(f_2)$. Denote this isomorphism by Ψ.

22 **if** $\deg_t(f_2) = 1$ **then** s generates $\overline{\mathbb{Q}}(s)[t]/(f_2)$ so g_1/g_3 generates $\overline{\mathbb{Q}}(x)[y]/(f)$. Compute rational functions $X(s), Y(s) \in \mathbb{Q}(s)$ such that $x = X(g_1/g_3)$ and $y = Y(g_1/g_3)$ and go to step 30. **end if**

23 $P_s(X) :=$ the characteristic polynomial of $\Psi(x)$ over the field extension $\mathbb{Q}(s) \subset \mathbb{Q}(s)[t]/(f_2)$.

24 $P_t(X) :=$ the characteristic polynomial of $\Psi(x)$ over the field extension $\mathbb{Q}(t) \subset \mathbb{Q}(t)[s]/(f_2)$.

25 $P := P_s(X) - P_t(X)$.

26 $X(s,t) :=$ solve X in $\mathbb{Q}(s)[t]/(f_2)$ from the equation $P = 0$.

27 Repeat steps 23 to 26 with y instead of x and Y instead of X.

28 Check the result heuristically as follows: take a point s_0, t_0 on the curve $\mathbf{C}_2$, i.e. $f_2(s_0, t_0) = 0$, and check if $f(X(s_0,t_0), Y(s_0,t_0)) = 0$. Use modular arithmetic to speed up this check.

29 Try to find a rational point P on $\mathbf{C}_2$

(a) **if** f_2 has a rational point at ∞ **then** finding P is easy, go to step 30 **end if**

(b) **if** n is odd or during the Puiseux series computation that was done to compute the integral basis a Puiseux series was found that corresponds to a place that is algebraic over $\mathbb{Q}$ of odd degree **then**

i $P_1 :=$ a place on $\mathbf{C}$ which is algebraic of odd degree m over $\mathbb{Q}$.

ii $P_2 :=$ the point $(g_1(P_1), g_2(P_1), g_3(P_1)) \in \mathbf{P}^2$

iii **if** $m = 1$ **then** $P := P_2$, go to step 30 **end if**

iv $G := \sum a_{ij} s^i t^j$, $0 \le j \le 1$, $0 \le i \le (m+1)/2 - j$ where a_{ij} are variables.

v solve the system $\{G(P_2') = 0 | P_2' \in$ the set of conjugates of P_2 over $\mathbb{Q}\}$.

vi $G_1, G_2 :=$ a basis of solutions.

vii $P :=$ the pole of G_1/G_2.

end if

30 **exit** $X(s,t), Y(s,t), f_2$ and, if found, the point P.

If a rational point P on $\mathbf{C}_2$ is found then we can compute a rational parametrization of $\mathbf{C}_2$ and combine it with $(X(s,t), Y(s,t)) : \mathbf{C}_2 \to \mathbf{C}$ to find a rational parametrization of $\mathbf{C}$. If no rational point P is found then we take a point in a quadratic algebraic extension and find a parametrization of $\mathbf{C}_2$ (and hence of $\mathbf{C}$) over this extension.

3.1. The steps in the algorithm

Step 1 to 4. Note that the characteristic of the ground field should be 0, otherwise the recursion need not terminate. After step 4 the there are no singularities nor ramification points at infinity and $(0,1,0)$ is not a point on the curve.

Step 5, 6 and 7. We can compute elements $b_i \in \mathbb{Q}(x)[y]/(f)$ (a so-called integral basis, cf. (Trager, 1984; Ford, 1978; van Hoeij, JSC1994)) such that

$$O_{\mathbf{A}} = \overline{\mathbb{Q}}[x]b_0 + \cdots + \overline{\mathbb{Q}}[x]b_{n-1}.$$

Any integral basis can easily be transformed into a basis in the form that is specified in step 5. The algorithm in (van Hoeij, JSC1994) produces an integral basis that is already in this form. Furthermore the denominator d of the last basis element b_{n-1} is the least common multiple of all denominators in the integral basis. So

$$O_{\mathbf{A}} \subset \frac{1}{d}\mathbb{Q}[x,y]/(f). \tag{3.1}$$

Our integral basis algorithm uses Puiseux expansions, cf. (Duval, 1989). The Hurwitz theorem gives a formula for the genus of $\mathbf{C}$ in terms of the ramification indices e_P. This formula can be translated into a formula that is expressed in terms of Puiseux expansions, cf. section 3.1 in (van Hoeij, 1995). So, as a byproduct of our the integral basis algorithm, the value of $g(\mathbf{C})$ is obtained.

The genus can also be computed from the integral basis itself, as follows. One has

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P \in \mathbf{C}(\mathbf{P}^2)} \delta_P.$$

Here the number δ_P for a point P is defined as the codimension of the local ring at P in the intersection of the places at P, cf. exercise 1.8 on page 298 in (Hartshorne, 1977). The points P at infinity are regular points, which implies $\delta_P = 0$. The sum of the δ_P for the finite points $P \in \mathbf{A}^2$ on the curve equals the codimension of $\overline{\mathbb{Q}}[x,y]$ (which is the intersection of the local rings for all finite points) in $O_{\mathbf{A}}$ (which is the intersection of the finite places). The integral basis explicitly gives $O_{\mathbf{A}}$ and so this codimension can be computed from the integral basis. Our integral basis algorithm produces a basis for which the numerators are monic polynomials in y with degrees $0, 1, \ldots, n-1$ and the denominators are polynomials in x. Then this codimension is the sum of the degrees of the denominators in this integral basis. The genus is $(n-1)(n-2)/2$ minus this sum.

Step 8 to 14. See section 3.2 for step 8 and 9, and section 3.3 for step 10 to 13. As was explained in section 2, equation (2.3), the map (g_1, g_2, g_3) defines a bijective morphism to a conic in $\mathbf{P}^2$. In step 14 we multiply by d to eliminate the denominators, cf. equation (3.1). So $g_1, g_2, g_3 \in \mathbb{Q}[x,y]$.

Step 15 to 20. About the notation: In step 17b the expression "coefficient(r, y, j)" stands for the coefficient of y^j in r where r is viewed as a polynomial in y. Solving the system of linear equations means to express as many as possible variables a_{jk} as linear expressions in the other variables $a_{j'k'}$. So when substituting the solution into F_2 a maximal number of variables a_{jk} is eliminated from F_2.

The 6 products $g_i g_j$, $1 \le i \le j \le 3$ span a vector space of dimension 5. So, up to a constant factor, there is precisely 1 linear relation. Hence F_2 is unique up to a constant factor. The condition on F_2 is that $F_2(g_1, g_2, g_3)$ is 0 in $\overline{\mathbb{Q}}(x)[y]/(f)$. So the necessary and sufficient condition on the variables a_{jk} is that the remainder of $F_2(g_1, g_2, g_3)$ after a division by f is 0. Instead of computing this remainder, we compute a smaller expression namely this remainder with a value substituted for x. This speeds up the computation but it does not need to give sufficient linear conditions on the variables a_{jk}. So we need to substitute several values for x until F_2 is determined up to a constant factor, i.e. until only 1 variable a_{jk} remains. Then we can substitute an arbitrary non-zero value for this variable. Now we substitute $u = 1$ in F_2 and find the function field $\overline{\mathbb{Q}}(g_1/g_3, g_2/g_3) \simeq \overline{\mathbb{Q}}(s)[t]/(f_2)$ of the curve $\mathbf{C}_2$.

Step 21 to 27. g_1/g_3 and g_2/g_3 generate the function field, cf. equation (2.4) in section 2, and satisfy the equation f_2. So Ψ is an isomorphism. At this point we only know the images of the generators g_1/g_3 and g_2/g_3 under Ψ but not the images of x and y. These images are computed as follows. We may assume that s does not generate the function field $\mathbb{Q}(s)[t]/(f_2)$, because if it does then $\deg_t(f_2) = 1$ and we can apply step 22 below. Furthermore we may assume that t does not generate $\mathbb{Q}(s)[t]/(f_2)$ because this situation is reduced in step 19 to the case where s generates the function field. So we can assume that $\mathbb{Q}(s) \subset \mathbb{Q}(s)[t]/(f_2)$ is a field extension of degree 2. The characteristic polynomial $P_s(X) \in \mathbb{Q}(s)[X]$ of $\Psi(x)$ over this field extension is a monic polynomial in X of degree 2 for which $P_s(\Psi(x)) = 0$. Similarly $P_t(X)$ is a monic polynomial in X of degree 2 and $P_t(\Psi(x)) = 0$. Then $P = P_s(X) - P_t(X)$ has degree 1 in X and so X can be solved from P by performing a division in $\mathbb{Q}(s)[t]/(f_2)$. This way $X(s,t) = \Psi(x) \in \mathbb{Q}(s)[t]/(f_2)$ is obtained.

The remaining question is how to compute $P_s(X)$ in step 23. Ψ is an isomorphism. Hence the characteristic polynomial $P_s(X)$ of $\Psi(x)$ over $\mathbb{Q}(\Psi(g_1/g_3)) = \mathbb{Q}(s)$ is the image under Ψ of the characteristic polynomial of x over $\mathbb{Q}(g_1/g_3)$.

Computing $P_s(X)$ is the same problem as computing the characteristic polynomial of x over $\theta(x_0)$ in section 4.1 in (van Hoeij, 1995). $P_s(X)$ can be obtained from

$$r = \mathrm{Res}_y(sg_3 - g_1, f)$$

(replace x by X in r). To speed up the computation of this resultant r we first substitute a generic value i (preferably a small integer to keep the expressions small) for x. This way $r_{x=i}$ is obtained. $P_s(X)$ can be constructed by computing $r_{x=i}$ for 5 different generic i, cf. (van Hoeij, 1995).

Step 22. This is more or less the same as step 23 above, except this time we need to compute only 3 different $r_{x=i}$ (where r is the resultant of $sg_3 - g_1$ and f) instead of 5. This step is explained in more detail in (van Hoeij, ISSAC1994).

Step 28. To be sure that the result is correct we should test if $f(X(s,t), Y(s,t))$ is 0 in $\mathbb{Q}(s)[t]/(f_2)$. However, this can be a lengthy computation. So instead of doing a complete check we check the result for only 1 point on $\mathbf{C}_2$. This is still useful for debugging the implementation, and by applying modular arithmetic this test will not take much time.

Step 29. If n is odd then we can choose a generic integer i, intersect the curve with the line $x = i$ and find n regular points on the curve. Since the number of points is odd, one of these points must be defined over an algebraic extension of odd degree over $\mathbb{Q}$. Take such a point $P_1 = (x_0, y_0, 1) \in \mathbf{P}^2$ and compute $P_2 = (g_1(P_1), g_2(P_1), g_3(P_1))$ on $\mathbf{C}_2$.

Suppose n is even and suppose we found the following Puiseux expansion during the integral basis computation

$$x = \alpha, \qquad \alpha = \alpha_1 + \alpha_2 t^r \quad \text{and} \quad y = \beta \in \overline{\mathbb{Q}}((t))$$

where $\alpha_1, \alpha_2 \in \overline{\mathbb{Q}}$, $r \in \mathbb{N}$ is the ramification index, t is a local parameter. Suppose that α_1, α_2 is algebraic of odd degree over $\mathbb{Q}$ and β is algebraic of odd degree (note that a Puiseux expansion with this property need not exist) over $\mathbb{Q}(\alpha_1, \alpha_2)((t))$. A Puiseux expansion corresponds to a place P_1 on $\mathbf{C}$. We want to evaluate (g_1, g_2, g_3) at this place to obtain a point P_2 on $\mathbf{C}_2$.

On a computer $(g_i)_{x=\alpha, y=\beta} \in \overline{\mathbb{Q}}((t))$, $1 \leq i \leq 3$ can be evaluated only up to a finite accuracy a, i.e. these expressions are computed modulo t^a. The algorithm must evaluate the $(g_i)_{x=\alpha,y=\beta}$ with an increasing accuracy a until at least one of the g_i is non-zero modulo t^a. Then divide the g_i by a suitable power of t such that $(g_1, g_2, g_3)_{x=\alpha,y=\beta}$ with $t = 0$ substituted is non-zero. Then the point P_2 on $\mathbf{C}_2$ is determined. Since Ψ is a rational (i.e. defined over $\mathbb{Q}$) bijection between $\mathbf{C}$ and $\mathbf{C}_2$ the conjugates of the point

P_2 over $\mathbb{Q}$ correspond to the conjugates of the place P_1 over $\mathbb{Q}$. Hence the number of conjugates of P_2 is odd, so P_2 is defined over an algebraic extension of $\mathbb{Q}$ of odd degree.

The system of equations in step 29b5 can be solved over $\mathbb{Q}$ as follows. Suppose P_2 is defined over $\mathbb{Q}(\alpha)$ where $\alpha \in \overline{\mathbb{Q}}$ is algebraic of odd degree m over $\mathbb{Q}$. Write the equation $G(P_2) = 0$ in the form $e_0\alpha^0 + \cdots + e_{m-1}\alpha^{m-1} = 0$ where $e_0, \ldots, e_{m-1}$ are $\mathbb{Q}$-linear expressions the a_{ij}. The system in step 29b5 is formed by this linear equation and all its conjugates over $\mathbb{Q}$. This system is equivalent with $e_0 = e_1 = \cdots = e_{m-1} = 0$. The reason is that the transition matrix (this is a Vandermonde matrix) between these two systems of linear equations is invertible. So we have a system of equations over $\mathbb{Q}$. Hence we can find a rational basis G_1, G_2 of solutions. Now G_1, G_2 have pole orders $\leq (m+1)/2$ at the two points at infinity, and have m roots on $\mathbf{C}_2$ in common, hence G_1/G_2 has only one pole P on $\mathbf{C}_2$. Because G_1/G_2 is rational the conjugates of P must be poles of G_1/G_2 as well, hence equal to P. So P is invariant under conjugation, in other words P is a rational point.

3.2. Step 8 and 9: The points at infinity

$$O_{\mathbf{A}} = \overline{\mathbb{Q}}[x]b_0 + \cdots + \overline{\mathbb{Q}}[x]b_{n-1} \subset \frac{1}{d}\overline{\mathbb{Q}}[x,y]$$

$O_{\mathbf{B}}$ is the set of functions g in $\overline{\mathbb{Q}}(z)[y]/(F_{x=1})$ that have no poles in $\mathbf{B}$. It is the integral closure of $\overline{\mathbb{Q}}[z]_{(z)}$ (this is the set of all rational functions with no pole at $z = 0$) in the function field $\overline{\mathbb{Q}}(z)[y]/(F_{x=1})$. Like for $O_{\mathbf{A}}$ we can compute an integral basis for $O_{\mathbf{B}}$. However, because of our assumption that $F_{z=0,x=1}$ is square-free it follows that z does not divide the discriminant of $F_{x=1}$. A necessary condition (see for example (Trager, 1984; Ford, 1978; van Hoeij, JSC1994)) for having a non-trivial integral basis at $z = 0$ is that z^2 divides the discriminant (a necessary and sufficient condition is that there are singularities on the line $z = 0$). So the integral basis is trivial, which means

$$O_{\mathbf{B}} = \overline{\mathbb{Q}}[z]_{(z)}y^0 + \ldots + \overline{\mathbb{Q}}[z]_{(z)}y^{n-1}.$$

In x-y syntax this means that

$$\frac{g}{h} \in O_{\mathbf{B}} \iff \deg(g) \leq \deg(h)$$

for elements $g \in \overline{\mathbb{Q}}[x,y]$ and $h \in \overline{\mathbb{Q}}[x]$ with $\deg_y(g) < n$.

The divisor D_∞ is the sum of the points

$$(1, \alpha, 0) \in \mathbf{P}^2(\overline{\mathbb{Q}})$$

for which α is a root of the polynomial $F_{z=0,x=1} \in \mathbb{Q}[y]$. Because of the assumption that $F_{z=0,x=1}$ is square-free there are n such points, $\deg(D_\infty) = \deg(F_{z=0,x=1}) = n$. By the Riemann-Roch theorem and the fact that the genus is 0 the dimension of $\mathcal{L}(D_\infty)$ is $\deg(D_\infty) + 1 = n + 1$. The set of functions with at most a pole of order one at the infinite places is $\frac{1}{z}O_{\mathbf{B}}$ so

$$\mathcal{L}(D_\infty) = O_{\mathbf{A}} \bigcap \frac{1}{z}O_{\mathbf{B}}.$$

The inclusion map

$$\mathcal{L}(D_\infty) \subset \frac{1}{z}O_{\mathbf{B}}$$

is injective. By taking the quotient of these vector spaces and the vector space $O_{\mathbf{B}}$ we obtain an injective map (note that $\mathcal{L}(D_\infty) \bigcap O_{\mathbf{B}} = \overline{\mathbb{Q}}$)

$$\text{"mod } O_{\mathbf{B}}\text{"} : \mathcal{L}(D_\infty)/\overline{\mathbb{Q}} \to (\frac{1}{z} O_{\mathbf{B}})/O_{\mathbf{B}}.$$

The right hand side has the following basis (as $\overline{\mathbb{Q}}$ vector space)

$$\frac{y^0}{z}, \ldots, \frac{y^{n-1}}{z}.$$

The left hand side has dimension n as well. Hence this map is bijective and so there must exist elements $Q_i \in \mathcal{L}(D_\infty)$ (which are determined modulo $\overline{\mathbb{Q}}$) such that Q_i is y^i/z modulo $O_{\mathbf{B}}$. Now $1, Q_0, ..Q_{n-1}$ are linearly independent elements of $\mathcal{L}(D_\infty)$ and hence this forms a basis. Then

$$1, Q_0, ..Q_{n-1}, xQ_0, \ldots, xQ_{n-1}$$

is a basis for $\mathcal{L}(2 \cdot D_\infty)$.

$Q_i \in O_{\mathbf{A}} \subset \frac{1}{d}\overline{\mathbb{Q}}[x, y]$ so we can write

$$Q_i = \frac{R_i}{d}$$

where $R_i \in \overline{\mathbb{Q}}[x, y]$ with $\deg_y(R_i) < n$. Since Q_i is determined up to constants, R_i is determined up to constants times d hence R_i is uniquely determined if we add the condition that the coefficient of $x^{\deg(d)}y^0$ in R_i is zero. Since conjugates of $R_i \in \overline{\mathbb{Q}}[x, y]$ over $\mathbb{Q}$ satisfy the same conditions and R_i is uniquely determined by these conditions it follows that R_i is invariant under conjugation and hence

$$R_i \in \mathbb{Q}[x, y].$$

Write R_i as a polynomial in y with coefficients R_{ij} in $\mathbb{Q}[x]$

$$R_i = \sum_{j=0}^{n-1} R_{ij} y^j.$$

The fact that $Q_i \in \frac{1}{z} O_{\mathbf{B}}$ means in x-y syntax that

$$\deg(R_i) - \deg(d) \leq 1$$

so

$$\deg(R_{ij}) \leq 1 + \deg(d) - j. \tag{3.2}$$

The fact that Q_i mod $O_{\mathbf{B}}$ is y^i/z means in x-y syntax that (assume d is monic now) the coefficient of $x^{1+\deg(d)-j}$ in R_{ij} is 1 if $i = j$ and 0 otherwise. So the coefficients in $\mathbb{Q}$ of the monomials $x^p y^q$ of R_i are known for all $p + q > \deg(d)$ and for $(p, q) = (\deg(d), 0)$ (this coefficient was chosen to be 0 to make Q_i uniquely determined).

We can compute the R_i with the following "algorithm". Because $Q_i \in O_{\mathbf{A}}$ there must exist polynomials a_{ij} in x such that $Q_i = \sum_j a_{ij} b_j$ hence

$$R_i = \sum_{j=0}^{n-1} a_{ij} B_j \tag{3.3}$$

where $B_j = db_j \in \mathbb{Q}[x, y]$. First consider the coefficient of y^{n-1} in this expression. Note that on the right hand side this coefficient only depends on $a_{i,n-1}$. Since we have a bound on $\deg(R_{i,n-1})$ we have a bound on $\deg(a_{i,n-1})$ as well. So we can write $a_{i,n-1}$ as a polynomial in x with undetermined constant coefficients. Then by taking the coefficient of y^{n-2} in equation (3.3) and applying (3.2) a bound on the degree of $a_{i,n-2}$ can be obtained. Again write $a_{i,n-2}$ with undetermined coefficients. Note that we know certain coefficients of R_i, namely the coefficients of the monomials with degree $> \deg(d)$ and the coefficient of $x^{\deg(d)}y^0$. This implies a set S of linear conditions on the coefficients of $a_{i,n-2}$ and $a_{i,n-1}$. Solving S decreases the number of indeterminates in $a_{i,n-2}$ and $a_{i,n-1}$. Then we can proceed in the same way with $a_{i,n-3}$, compute a bound for the degree, write it with undetermined coefficients, compute linear equations, solve, reduce the number of indeterminates, etcetera. When finally we end with $a_{i,0}$ the linear equations must uniquely determine all the a_{ij} because R_i is uniquely determined by its properties and any solution of these linear equations will give rise to a R_i with the same properties.

In our implementation we use a small modification of this algorithm. Instead of computing $R_0, R_1, \ldots, R_{n-1}$ we compute all R_i at the same time by computing R where

$$R = \sum_{i=0}^{n-1} c_i R_i$$

and where the c_i are variables. Write

$$R = \sum_{i=0}^{n-1} \sum_{j=0}^{d_i} \alpha_{ij} x^j B_i.$$

Here the d_i are not a priori known, these are computed during the algorithm. Only $d_{n-1} = 1 + \deg(d) - (n-1)$ is known a priori. Now we search for the coefficients

$$\alpha_{ij} \in \mathbb{Q}c_0 + \ldots + \mathbb{Q}c_{n-1}.$$

With this modification the following algorithm is obtained.

Algorithm $\mathcal{L}(D_\infty)$
Input: $f \in \mathbb{Q}[x,y]$ satisfying the conditions in section 2.
Output: A basis for $\mathcal{L}(D_\infty)$

$n := \deg_y(f)$ (is assumed to be equal to $\deg(f)$)
$R := 0$
Let $b_i = B_i/d$, $i = 0, \ldots, n-1$ be the integral basis from step 5 in section 3.
for i **from** $n-1$ **down to** 0 **do**
  d_x:=$1 + \deg(d) - i$
  Introduce a new undetermined variable c_i
  C_R:=coefficient$(R, y, i) - c_i x^{d_x}$
  C_B:=coefficient(B_i, y, i)
  d_i:=$\deg(C_R) - \deg(C_B)$
  Introduce new variables $\alpha_{i,0}, \ldots, \alpha_{i,d_i}$.
  α_i:=$\alpha_{i,0}x^0 + \ldots + \alpha_{i,d_i}x^{d_i}$
  S:=$\{$coefficient$(C_R - \alpha_i C_B, x, j) = 0 | j \geq d_x\}$
  if $i = 0$ **then** S:=$S \bigcup \{\alpha_{i,0} = 0\}$ **end if**
  solve this set S in the variables $\alpha_{i',j}$ where $i' \geq i$ and $j \geq 0$

if there is no solution **then**
  exit with the message: "The genus is > 0, or f is reducible, or f has singularities at infinity"
end if
R:=substitute solution of S in $R - \alpha_i B_i$
Comment: Now the coefficient of $x^j y^i$ in R is c_i if $j = d_x$ and 0 if $j > d_x$.
end do
Now R_i is obtained by substituting $c_i = 1$ and $c_j = 0$ for $j \neq i$ in R.
Output:

$$1, \frac{R_0}{d}, \ldots, \frac{R_{n-1}}{d}.$$

Note that the equation $\alpha_{0,0} = 0$ that we add to S is not equivalent with the condition we posed that the coefficient of $x^{\deg(d)} y^0$ in R is zero. However, this condition $\alpha_{0,0} = 0$ serves the same purpose, which is to make R uniquely determined.

3.3. Step 10 to 13: The ramification points

For $a_1, \ldots, a_d \in \overline{\mathbb{Q}}(\mathbf{C})$ define

$$V_{a_1,\ldots,a_d} = \{g \in \mathcal{L}(2D_\infty) | g a_i \in O_{\mathbf{A}} \text{ for each } i\}.$$

Suppose that

$$\forall_{P \in \mathbf{A}} \forall_i \; v_P(a_i) \geq 1 - e_P \tag{3.4}$$

and

$$\forall_{P \in \mathbf{A}} \; [e_P > 1 \Longrightarrow (\exists_i \; v_P(a_i) = 1 - e_P)]. \tag{3.5}$$

For a list $a_1, \ldots, a_d$ with these properties (3.4) and (3.5) we have $g \in V_{a_1,\ldots,a_d}$ if and only if $g \in \mathcal{L}(2D_\infty)$ and $v_P(g) \geq e_P - 1$ for all $P \in \mathbf{A}$. So

$$V_{a_1,\ldots,a_d} = \mathcal{L}(D)$$

where D is the divisor $-K$ defined in section 2.

Lemma 3.1. *The list $a_i = \frac{db_i}{dx}$, $i = 1, \ldots, n-1$ has properties (3.4) and (3.5).*

Proof: Let $P \in \mathbf{A}$ and let t be a local parameter at P such that $x = \alpha_1 + \alpha_2 t^r$ with $\alpha_1, \alpha_2 \in \overline{\mathbb{Q}}$ and where $r = e_P \in \mathbb{N}$ is the ramification index. If $g \in O_{\mathbf{A}}$ then g can be written as

$$g = \sum_{i=0}^{\infty} g_i t^i$$

with $g_i \in \overline{\mathbb{Q}}$. Then

$$\frac{dg}{dx} = \frac{dg}{d(\alpha_1 + \alpha_2 t^r)} = \frac{dg}{\alpha_2 r t^{r-1} dt} = \frac{1}{\alpha_2 r t^{r-1}} \sum_{i=1}^{\infty} g_i i t^{i-1}.$$

So $v_P(\frac{dg}{dx}) \geq v_P(1/t^{r-1}) = 1 - e_P$ and we have equality if and only if $g_1 \neq 0$. Hence property (3.4) holds.

Now let $P \in \mathbf{A}$ with $e_P > 1$. By the Riemann-Roch theorem it is easy to show that there exists a $g \in O_{\mathbf{A}}$ with $v_P(g) = 1$. Then $v_P(\frac{dg}{dx}) = 1 - e_P$. Since $g \in O_{\mathbf{A}}$ we have

$$g = \sum_{i=0}^{n-1} c_i b_i$$

for some $c_i \in \overline{\mathbb{Q}}[x]$. Then $\frac{dg}{dx} = \sum_i (c_i \frac{db_i}{dx} + \frac{dc_i}{dx} b_i)$ has valuation $1 - e_P$. Hence for at least one i we have $v_P(c_i \frac{db_i}{dx} + \frac{dc_i}{dx} b_i) \leq 1 - e_P$. The valuations of c_i, $\frac{dc_i}{dx}$ and b_i are ≥ 0 hence $v_P(\frac{db_i}{dx}) \leq 1 - e_P$. So property (3.5) follows as well.

□

In the algorithm in step 10 and 13b we take the list $a_1 = \frac{dy}{dx}$ and $a_{i+1} = \frac{db_{n-i}}{dx}$ for $i > 0$. From the lemma it follows that this list $a_1, a_2, \ldots$ has properties (3.4) and (3.5). The expression v in step 11 and 13c is a basis for V_{a_1}, in the next step V_{a_1,a_2} etcetera. The reason for taking the a_i in this order is that this way often a sublist consisting of 1, sometimes 2 and very rarely more than 2 elements of this list will be sufficient. Having a sufficiently long sublist $a_1, \ldots, a_t$ of this list, i.e. a sublist that has properties (3.4) and (3.5), can be detected because then the dimension of $V_{a_1,\ldots,a_t}$ is 3. So we need not always treat the derivatives of all integral basis elements but we can stop when the number of elements in the basis v for $V_{a_1,\ldots,a_t}$ is 3. Then the list v is a basis for $\mathcal{L}(D)$.

The remaining question is how to do step 11 (and 13c which is the same). Given is an element $a \in \mathbb{Q}(x)[y]/(f)$ for which $v_P(a) \geq 1 - e_P$ for all finite places P. Furthermore is given a basis v of some vector space contained in $\mathcal{L}(2D_\infty)$. The problem now is to compute the subspace of elements g satisfying

$$ga \in O_A \tag{3.6}$$

First we want to find the ramification points. Let disc be the discriminant of f, i.e. the resultant of f and $\frac{df}{dy}$

$$\text{disc} = \text{Res}_y(f, \frac{df}{dy}) \in \mathbb{Q}[x].$$

$b_{0,2}, \ldots, b_{n-1,2} \in \mathbb{Q}[x]$ are the denominators of our integral basis $b_0, \ldots, b_{n-1}$. Let

$$d_r = \frac{\text{disc}}{(\prod_i b_{i,2})^2}.$$

From the following lemma it follows that d_r is a polynomial and that the roots of d_r are the x-coordinates of the ramification points.

Lemma 3.2. *For $\alpha \in \overline{\mathbb{Q}}$ denote M_α as the valuation of d_r in $\overline{\mathbb{Q}}((x - \alpha))$, i.e. M_α is the largest integer for which $d_r/(x - \alpha)^{M_\alpha} \in \overline{\mathbb{Q}}[[x - \alpha]]$. Then*

$$M_\alpha = \sum_P (e_P - 1)$$

where the sum is taken over all places on the line $x = \alpha$.

Since $e_P - 1 \geq 0$ it follows that $M_\alpha \geq 0$ for all $\alpha \in \overline{\mathbb{Q}}$ so d_r is a polynomial. M_α is the multiplicity of the factor $x - \alpha$ in d_r. From the Hurwitz theorem it follows that sum of the $e_P - 1$ for all finite P is $2n-2$ because there are no ramification points at infinity and $g=0$. So the degree of d_r is $2n-2$.

Proof: Let P_∞ be a point at infinity and let p be a non-constant element of $\mathcal{L}(P_\infty)$. So p has only one pole with multiplicity 1, hence it is a parameter (a generator of the function field). So $\overline{\mathbb{Q}}(x)[y]/(f) = \overline{\mathbb{Q}}(p) = \overline{\mathbb{Q}}(x,p)$. Hence p is algebraic over $\overline{\mathbb{Q}}(x)$ of degree n. Let $g \in \overline{\mathbb{Q}}(x)[Z]$ be the minimum polynomial in the variable Z (g is monic in Z) of p over $\overline{\mathbb{Q}}(x)$. Since $p \in O_{\mathbf{A}}$ it follows that $g \in \overline{\mathbb{Q}}[x,Z]$. Since $x \in \overline{\mathbb{Q}}(p)$ it follows that $\deg_x(g) = 1$ hence there are no singularities on the curve given by g. Denote $d_g \in \overline{\mathbb{Q}}[x]$ as the discriminant of g with respect to Z. Let $z_1, \ldots, z_n \in \overline{\mathbb{Q}((x-\alpha))}$ be the roots of g in the algebraically closed field $\overline{\mathbb{Q}((x-\alpha))}$, so $g = \prod(Z - z_i)$. These z_i are Puiseux expansions. The discriminant d_g is the product of $z_i - z_j$ taken over all $i = 1, \ldots, n$ and $j \neq i$. Using the fact that there are no singularities it follows that the valuation (that is the smallest power of $x - \alpha$ with a non-zero coefficient) of $z_i - z_j$ is 0 if z_i and z_j correspond to different places, and the valuation is $1/e_P$ if z_i and z_j correspond to the same place P. The sum of the valuations of the $z_i - z_j$ is the valuation of the product d_g of the $z_i - z_j$. For each P there are $e_P(e_P - 1)$ pairs $i \neq j$ of Puiseux expansions that correspond to P hence the valuation of d_g is $\sum e_P(e_P-1)\cdot 1/e_P = \sum(e_P - 1)$ where the sum is taken over all places on the line $x = \alpha$. Now the lemma follows if we can prove that d_g/d_r is a constant.

Suppose L is a field, a and b are algebraic over L of degree n and $L(a) = L(b)$. Denote m_a and m_b as the minimum polynomials of a and b over L. We have two bases $a^0, \ldots, a^{n-1}$ and $b^0, \ldots, b^{n-1}$ for the L-vector space $L(a) = L(b)$. Let M be the transformation matrix between these two bases. Then the quotient of the discriminant of m_a and the discriminant of m_b is $(\det(M))^2$, cf. any introduction book on algebraic number theory. Apply this to $L = \overline{\mathbb{Q}}(x)$. Then to prove the lemma we need to show that the determinant of the transformation matrix between the bases $y^0, \ldots, y^{n-1}$ and $p^0, \ldots, p^{n-1}$ is a constant times $\prod_i b_{i,2}$.

Lemma 1 in (van Hoeij, 1995) says

$$\overline{\mathbb{Q}}[x]b_0 + \ldots + \overline{\mathbb{Q}}[x]b_{n-1} = O_{\mathbf{A}} = \overline{\mathbb{Q}}[x]p^0 + \ldots + \overline{\mathbb{Q}}[x]p^{n-1}$$

Hence the transformation matrix between $p^0, \ldots, p^{n-1}$ and $b_0, \ldots, b_{n-1}$ is invertible over $\overline{\mathbb{Q}}[x]$, and so the determinant of this matrix is a constant. The transformation matrix between $b_0, \ldots, b_{n-1}$ and $y^0, \ldots, y^{n-1}$ is on triangular form because $\deg_y(b_i) = i$. Furthermore the numerators of the b_i are monic in y hence the determinant of the transformation matrix is the product of the denominators of the b_i.

□

Now we continue with step 11. $v_P(a) \geq 1 - e_P \geq -M_\alpha e_P = -v_P(d_r)$ in a finite place P with x-coordinate α. So $v_P(d_r a) \geq 0$ for finite places P in other words $d_r a \in O_{\mathbf{A}}$. So we know a priori that $g d_r a \in O_{\mathbf{A}}$. Equation (3.6) is equivalent with

$$g d_r a \in d_r O_{\mathbf{A}} \tag{3.7}$$

in other words $g d_r a$ is zero in $O_{\mathbf{A}}$ modulo $d_r O_{\mathbf{A}}$. We have a $\overline{\mathbb{Q}}[x]$-basis

$$d_r b_0, \ldots, d_r b_{n-1}$$

for the $\overline{\mathbb{Q}}[x]$-module $d_r O_{\mathbf{A}}$. Like our integral basis this basis is in "triangular form", i.e. written as polynomials in y the degrees are 0 to $n-1$. This is convenient for computing in $O_{\mathbf{A}}$ modulo $d_r O_{\mathbf{A}}$. A basis for the elements g in the vector space spanned by

$$v = (v_1, \ldots, v_e)$$

that satisfy equation (3.7) is obtained as follows. Write $g = \sum_i g_i v_i$ where the g_i are variables. Then compute the remainder of $d_r g a$ modulo $d_r O_{\mathbf{A}}$ in the same way as in section 3.1 in (van Hoeij, ISSAC1994). Equating the remainder to zero gives the necessary and sufficient linear conditions on the g_i. Solving these equations gives the basis for the elements g with the property (3.6).

If $d_r = d_1 d_2$ with $\gcd(d_1, d_2) = 1$ then equation (3.7) is equivalent with $d_r g a$ is zero modulo $d_1 O_{\mathbf{A}}$ and zero modulo $d_2 O_{\mathbf{A}}$. Doing two computations modulo small polynomials, one modulo d_1 and one modulo d_2, is usually faster than one computation modulo a larger polynomial d_r. So a factorization of d_r can speed up the computation. We can take for example a square-free factorization. Or we can take d_1 to be the largest factor of d_r that has gcd 1 with the largest denominator d in the integral basis. Then we can first treat the ramification points from the factor d_1 as follows: Multiply ga by d_1, take the numerator (which is a polynomial in x and y with $\deg_y$ smaller than n) and equate the remainder of this numerator after a division by d_1 to 0. This gives the linear conditions on the variables g_i coming from the ramification points on d_1. Afterwards, the ramification points on d_1 need not be considered anymore. So then we can replace a by $d_1 a$. This makes the denominator of a smaller, which speeds up the computation.

4. Parametrization by a line

In some cases the algorithm in section 3 produces a parametrization by a line (in step 22), in the remaining cases the curve is parameterized by a conic. In these remaining cases a parametrization of $\mathbf{C}$ can be obtained in several ways. The approach in section 3 is to compute a point P on $\mathbf{C}_2$. P is algebraic of degree 2 over $\mathbb{Q}$ if step 29 fails and P is rational otherwise. Then we can use this point P to compute a parametrization of $\mathbf{C}_2$. Composition of this parametrization with the morphism from $\mathbf{C}_2$ to $\mathbf{C}$ gives a parametrization of $\mathbf{C}$.

A different way to use the point $P \in \mathbf{C}_2(\mathbf{P}^2)$ is to construct a parameter p on $\mathbf{C}$ from it. Write $P \in \mathbf{P}^2$ as (P_1, P_2, P_3). After applying a permutation on P_1, P_2, P_3 and the basis g_1, g_2, g_3 of $\mathcal{L}(D)$ we may assume $P_3 \neq 0$. Then $(P_3 s - P_1)/(P_3 t - P_2)$ has only one pole on $\mathbf{C}_2$ hence this is a parameter. So $p = (P_3 g_1 - P_1 g_3)/(P_3 g_2 - P_2 g_3)$ is a parameter on $\mathbf{C}$. Then we can apply step 22, with g_1, g_3 replaced by $P_3 g_1 - P_1 g_3, P_3 g_2 - P_2 g_3$ to find a parametrization of $\mathbf{C}$. So then steps 23 to 27 can be skipped. In the test examples that were done this approach is faster than the approach in section 3 if P is a rational point (3 resultant computations instead of 5), but slower if P is not rational.

4.1. An example

The following polynomial defines an algebraic curve with genus 0

$$f = y^4 + 8xy^3 - 17x^2y^2 - xy^2 + 8x^3y - 2x^2 + 5x^3 - 2x^4.$$

The integral basis is

$$b_0 = 1, \quad b_1 = y, \quad b_2 = \frac{y^2}{x}, \quad b_3 = \frac{y^3 + 9xy^2 - 9xy - x}{x(x-1)}.$$

Basis for $\mathcal{L}(D_\infty)$:

$$1,\quad x,\quad \frac{-xy+x^2y}{x(x-1)},\quad \frac{-y^2+xy^2}{x(x-1)},\quad \frac{-x-9xy+9y^2+y^3}{x(x-1)}.$$

Basis for $\mathcal{L}(D)$, multiplied by $d = x(x-1)$ to eliminate the denominators:

$$\begin{aligned}
g_1 &= 233y^3+1378xy^2+719x^2y^2-2066x^2y-31xy-1077x^3+618x^2+226x^4,\\
g_2 &= -103y^3+339xy^3+3158x^2y^2-1034xy^2+101xy-2225x^2y+560x^2-796x^3,\\
g_3 &= 110y^3+386x^2y^2+604xy^2-1310x^2y-19xy+339x^3y+284x^2-394x^3
\end{aligned}$$

Now $g_1, g_2, g_3 \in \mathbb{Q}(x)[y]/(f)$ satisfy a homogeneous quadratic relation $F_2(s,t,u)$. This relation can be computed quickly from the fact that $(g_1)_{x=2}, (g_2)_{x=2}, (g_3)_{x=2} \in \mathbb{Q}[y]/(f_{x=2})$ and $(g_1)_{x=3}, (g_2)_{x=3}, (g_3)_{x=3} \in \mathbb{Q}[y]/(f_{x=3})$ satisfy the same relation as well (we start with $x=2$ because the lines $x=0$ and $x=1$ contain singularities).

$$f_2(s,t) = (F_2)_{u=1} = 116t^2+1521st-2872t+2844s^2+11000-11151s$$

Now $f_2(g_1/g_3, g_2/g_3) = 0$ in $\mathbb{Q}(x)[y]/(f)$ and (g_1,g_2,g_3) is a bijective morphism from $\mathbf{C}$ to the curve $\mathbf{C}_2$ defined by f_2.

The following Puiseux expansion at the singularity $(1,1,1)$

$$x = t+1,\quad y = t^0 + \frac{1}{2}t^1 + \cdots$$

is defined over $\mathbb{Q}$. The image of this place under (g_1,g_2,g_3) is the point $(26/5, -71/10, 1)$ on $\mathbf{C}_2$. This means that

$$p = \frac{(g_1 - \frac{26}{5}g_3)}{(g_2 + \frac{71}{10}g_3)}$$

generates the function field $\mathbb{Q}(x)[y]/(f)$. Expressing x as a rational function in p can be done by computing

$$r = \mathrm{Res}_y(s(g_2 + \frac{71}{10}g_3) - (g_1 - \frac{26}{5}g_3), f).$$

Now r is of the form a polynomial in x times $(14954139s^4+24828552s^3+15335676s^2+4170528s+420544)x+670761s^4+1385748s^3+1069524s^2+365472s+46656$. Solving x from this gives

$$X(s) = -\frac{670761s^4+1069524s^2+46656+365472s+1385748s^3}{14954139s^4+24828552s^3+15335676s^2+4170528s+420544}.$$

Note that in large examples (not in this example) the resultant computation can be costly. Then we first substitute a small integer i for x, so that $r_{x=i}$ is obtained. $X(s)$ can be reconstructed from a few such $r_{x=i}$. In a similar way we get

$$Y(s) = -\frac{2882061s^4+5389848s^3+3756924s^2+1157472s+133056}{14954139s^4+24828552s^3+15335676s^2+4170528s+420544}.$$

Now $(X(s), Y(s))$, $s \in \mathbf{P}^1$ parametrizes $\mathbf{C}$. The total computation time for this example is 6 seconds under Maple 5.3 for Linux on a Pentium 100.

We can simplify this parametrization as follows. The Puiseux expansions (these were needed for the integral basis algorithm) show that there are two rational places above $(0,0)$ and two rational places above $(1,1)$. So there are 4 rational values of $s \in \mathbf{P}^1$ for which $(X(s), Y(s)) \in \{(0,0),(1,1)\}$. Now we can write $s = (at+b)/(ct+d)$ and find equations for the following: $(X(s), Y(s)) = (0,0)$ for $t \in \{0,1\}$ and $(X(s), Y(s)) = (1,1)$ for $t = -1$. These equations have several solutions. We pick one of these solutions: $a = -\frac{12c}{19}, b = \frac{18c}{19}, d = -\frac{26c}{19}$. Then the following parametrization is obtained

$$\left(\frac{81\,t^2\,(t-1)^2}{101\,t^4 + 98\,t^3 - 339\,t^2 - 460\,t + 200}, -\frac{(9\,t-9)\,(t-5)\,(t+4)\,t}{101\,t^4 + 98\,t^3 - 339\,t^2 - 460\,t + 200}\right).$$

5. Discussion of the results

The main problem treated in this paper is the computation of $\mathcal{L}(D)$ where $D = -K$, for a curve with genus 0. It is known that for any divisor D it is possible to compute the vector space $\mathcal{L}(D)$. Computing this vector space can be reduced to computing and solving a (possibly large) system of linear equations. So our $\mathcal{L}(-K)$ could also be computed by a generic $\mathcal{L}(D)$ algorithm. The main result in this paper is a fast $\mathcal{L}(D)$ algorithm, specifically written for the case $D = -K$, $g = 0$. So it is more efficient and less general than a generic $\mathcal{L}(D)$ algorithm. To obtain an efficient algorithm we apply a divide and conquer approach, i.e. the problem is reduced to several smaller subproblems. The first subproblem is to compute $\mathcal{L}(D_\infty)$. For this subproblem we again apply a divide and conquer approach. To compute $\mathcal{L}(D_\infty)$ we need to solve linear equations. In section 3.2 the problem of solving one large system of equations is reduced to solving smaller systems, by first only considering the coefficient of y^{n-1}, then the coefficient of y^{n-2}, etc.

The next step is to treat the ramification points. Suppose for example that k is an irreducible factor of multiplicity 1 of the discriminant. Let $\alpha \in \overline{\mathbb{Q}}$ such that $k(\alpha) = 0$. In this situation there is one ramification point (α, β) on the line $x = \alpha$. One could make use of this point because the elements of $\mathcal{L}(-K)$ must have value 0 at this point. This gives necessary linear equations that can be computed by substituting the point (α, β) in the basis v in step 9. However, we found experimentally that this results in a large intermediate expression swell because β, expressed as an element of $\mathbb{Q}(\alpha)$, is usually a large expression. This severely limits the size of the curves that the algorithm can handle on a computer. The solution given in this paper to this problem is not to use the y-coordinate β of the ramification point, but instead to handle the ramification points using derivatives of integral elements (section 3.3).

The examples on the web-site show that our implementation can handle very large inputs on normal sized computers. Without the optimizations described above, our implementation would not be efficient enough to handle such large examples.

5.1. Remaining problems

The algorithm in this paper uses the fact that the curve is in some generic position ($\deg_y(f) = \deg(f)$ and no ramification points at infinity). This generic position can be achieved by a linear transformation. Such a transformation looks theoretically innocent, however, in concrete examples this can have a bad impact on the computation time. Indeed the implementation is often much slower on test examples which use a such a transformation than on examples which require no transformation. Applying such a linear transformation usually increases the size of f. But what is even worse is that useful properties that f may have could be erased in this way. An example of a useful property is that $\deg_y(f)$ is odd because then we can easily find a rational point on $\mathbf{C}_2$. Another useful property would be that $\deg_y(f)$ is small, i.e. smaller than $\deg(f)$, because this means: fewer elements in the integral basis, fewer ramification points, smaller resultants etcetera. It would be useful for these cases to modify (if possible) the method in such a way that these linear transformations are no longer needed.

The second problem is that the coefficients in the output of our algorithm are sometimes very large. One step in the algorithm is to compute a conic f_2 from a basis for the vector space $\mathcal{L}(D)$. Now the question is: Can one find a linear transformation on f_2 (on the vector space $\mathcal{L}(D)$ this means taking a different basis g_1, g_2, g_3) such that the coefficients in f_2 get smaller? A second question is the following: Given a point P on $\mathbf{C}_2$, find a different point which has "small" coefficients. These questions appear to be quite difficult in general. An answer to these two questions would improve the quality (i.e. reduce the size) of the output of the parametrization algorithm.

A different way to view this problem is the following: A morphism $(X(s,t), Y(s,t))$ from a conic to the curve $\mathbf{C}$ is computed in section 3. This allows us to compute points on $\mathbf{C}$. If we intersect $\mathbf{C}$ with a line we find a point with small coefficients in a large algebraic extension. If we compute a point by substituting a value in $(X(s,t), Y(s,t))$ then we find a point with large coefficients in a small (degree ≤ 2) algebraic extension. So there are points with small coefficients, and there are points over small algebraic extensions, but the problem is to find a point having both advantages at the same time. Such a point could then be used to compute a parametrization that has both advantages as well.

References

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

D. Duval, *Rational Puiseux expansions*, Compos. Math. 70, No. 2, 119-154 (1989).

D.J. Ford, *On the Computation of the Maximal Order in a Dedekind Domain*, Ph.D. thesis, Ohio State University, Dept. of Mathematics (1978).

P. Griffiths, J. Harris, *Principles of algebraic geometry*, Wiley-Interscience Series, (1978).

G. Haché, D. Le Brigand, *Effective Construction of Algebraic Geometry Codes* Rapport de recherche INRIA, No 2267 (1994).

R. Hartshorne, *Algebraic Geometry* Springer-Verlag (1977).

D. Hilbert, A. Hurwitz, *Ueber die Diophantischen Gleichungen vom Geschlecht Null*, Acta math 14, 217-224 (1890).

M. van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*, J. Symbolic Computation, 18, 353-363 (1994).

M. van Hoeij, *Computing parametrizations of rational algebraic curves*, ISSAC '94 Proceedings, 187-190 (1994).

M. van Hoeij, *An algorithm for computing the Weierstrass normal form*, ISSAC '95 Proceedings, 90-95 (1995).

J.R. Sendra, F. Winkler, *Determining Simple Points on Rational Algebraic Curves*, RISC-Linz Report Series No. 93-23 (1993).

J.R. Sendra, F. Winkler, *Optimal Parametrization of Algebraic Curves*, RISC-Linz Report Series No. 94-65 (1994).

J.R. Sendra, F. Winkler, *Symbolic parametrizations of curves*, J. Symbolic Computation 12, No. 6, 607-631 (1991).

B.M. Trager, *Integration of algebraic functions*, Ph.D. thesis, Dept. of EECS, Massachusetts Institute of Technology, (1984).

R.J. Walker, *Algebraic curves*, Princeton University Press, (1950).