Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences (ÖAW)

Sparse Parametrization of Plane Curves

T. Beck, J. Schicho

RICAM-Report 2005-08

SPARSE PARAMETRIZATION OF PLANE CURVES

TOBIAS BECK AND JOSEF SCHICHO

Abstract. We present a new method for the rational parametrization of plane algebraic curves. The algorithm exploits the shape of the Newton polygon of the defining implicit equation and is based on methods of toric geometry.

Contents

Date: June 6, 2005.

The authors were supported by the FWF (Austrian Science Fund) in the frame of the research projects SFB 1303 and P15551.

1. Introduction

Given a bivariate polynomial $f \in \mathbb{K}[x, y]$ over some field $\mathbb{K}$ we will describe a method to find a proper parametrization of the curve defined implicitly by f. That is we will find $(X(t), Y(t)) \in \mathbb{K}(t)$ s.t. $f(X(t), Y(t)) = 0$ and $(X(t), Y(t))$ induces a birational morphism from the curve to the affine line. This is the problem of finding a rational parametrization, a well-studied subject in algebraic geometry. There are already several algorithms, e.g. [10] and [14]. But up to now these methods do not take into account whether the defining equation is sparse or not. We will present an algorithm which exploits the shape of the Newton polygon of the defining polynomial by embedding the curve in a well-chosen complete surface. In this article we do not care for the involved extensions of the coefficient field and therefore assume that $\mathbb{K}$ is algebraically closed.

This article is organized as follows. In section 2 we recall some basic constructions of toric geometry. In particular we show how to embed a curve into a suitable complete toric surface. In section 3 we show how to compute the genus of the curve in this setting and how to find a linear system of rational functions on the curve that allows to find a parametrization. We state the main theorem which proves the algorithm to be correct. Finally we give a coarse description of the algorithm in pseudo-code and an example. The last section is devoted to a different proof of correctness using sheaf theoretical and cohomological arguments.

The reason for giving two different proofs is a historical one. When constructing the algorithm, we were looking for a suitable vector space of rational functions for the parametrization map. We found it by computing the first cohomology of certain sheaves of rational functions. Afterwards it turned out that more elementary arguments (using only the notion of divisors) can also be used to prove correctness of the algorithm. So in one sense the second proof is redundant. We decided to keep it nevertheless in the hope that it provides additional insight. When not seen in another context, the fact that a certain vector space has exactly the right dimension looks like a nice coincidence.

2. Preliminaries on Toric Varieties

Let $\mathbb{K}$ be an algebraically closed field. We are going to parametrize (if possible) a plane curve F' that is given by an absolutely irreducible polynomial $f \in \mathbb{K}[x, y]$ on the torus $T := (\mathbb{K}^*)^2$. Actually we will study a curve F which is the Zariski closure of F' in a complete surface containing the torus, i.e. $F \cap T = F'$. We will first show how to realize this surface and then recall some basic definitions and propositions. A good introduction to toric varieties can be found in [2].

2.1. **Embedding the curve into a complete toric surface.**

Parametrization by rational functions is a "global problem". In order to apply some theorems of global content we have to embed T in a complete surface. One possible complete surface, which is often used in this context, is the projective plane $\mathbb{P}^2_{\mathbb{K}}$. We will choose a complete toric surface instead, whose construction is guided by the shape of the Newton polygon of f. In fact also $\mathbb{P}^2_{\mathbb{K}}$ is a complete toric surface and corresponds to the Newton polygon of a dense polynomial f.

The Newton polygon $\Pi(f) \subset \mathbb{R}^2$ is defined as the convex hull of all lattice points $(r, s) \in \mathrm{Supp}(f)$ (i.e. all $(r, s) \in \mathbb{Z}^2$ s.t. $x^r y^s$ appears with a non-zero coefficient in f). For instance, if f is dense of total degree d then the Newton polygon is equal

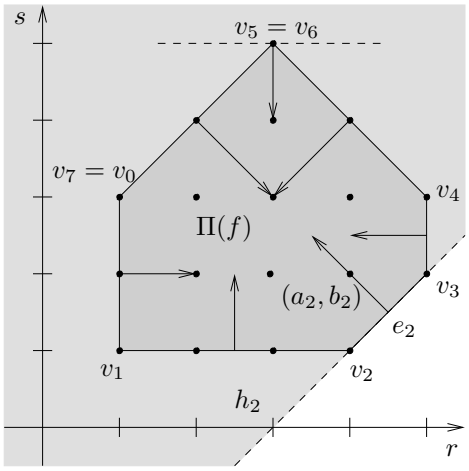


FIGURE 1. Newton polygon
Newton polygon $\Pi(f)$ with $n = 7$ vertices v_i. We emphasize edge e_2 and show its normal vector $(a_2, b_2) = (-1, 1)$ and the support half plane h_2. Here we would get $c_2 = -3$. The procedure of lemma 1 inserts an extra normal vector and thus we have the "double" vertex $v_5 = v_6$.

to the triangle with vertices $(0, 0)$, $(d, 0)$ and $(0, d)$. A sample Newton polygon is illustrated in figure 1. Throughout this article we will *always* implicitly assume that $\Pi(f)$ is non-degenerate; if f is irreducible and $\Pi(f)$ is a line segment or a point then the support of f has cardinality at most 2 and the parametrization problem is trivial.

For any pair of relatively prime $a, b \in \mathbb{Z}$, let $c(a, b) \in \mathbb{Z}$ be the minimum value of $ar + bs$, where $(r, s) \in \Pi(f)$. Then $\Pi(f)$ is a finite intersection of say n support half planes

$$h_i := \{(r, s) \in \mathbb{R}^2 \mid a_i r + b_i s \geq c_i\} \text{ where } c_i := c(a_i, b_i).$$

We assume that the (a_i, b_i) are arranged cyclically, i.e. $a_{i-1}b_i - a_i b_{i-1} > 0$ (setting $a_0 := a_n$ and $b_0 := b_n$). We also give names to the edges and the vertices of intersection

$$e_i := \{(r, s) \in \mathbb{R}^2 \mid a_i r + b_i s = c_i\} \text{ and } v_i := e_i \cap e_{i-1}.$$

Note that the set of half planes is not uniquely defined, there may be redundant half planes where the edge meets $\Pi(f)$ in one vertex (in this case, some of the vertices v_i will coincide).

Lemma 1. *We can assume that* $a_{i-1}b_i - a_i b_{i-1} = 1$ *for* $1 < i \leq n$.

Proof. The values $a_{i-1}b_i - a_i b_{i-1}$ are invariant under unimodular transformations (i.e. linear transformations by an integral matrix with determinant 1). Assume that $a_{i_0-1}b_{i_0} - a_{i_0}b_{i_0-1} > 1$ for some i_0. By a suitable unimodular transformation we may assume $(a_{i_0}, b_{i_0}) = (0, 1)$. It follows that $a_{i_0-1} > 1$.

We insert a new index, for simplicity say $i_0 - \frac{1}{2}$, set $a_{i_0-\frac{1}{2}} := 1$ and determine $b_{i_0-\frac{1}{2}}$ by integer division s.t. $0 \leq a_{i_0-1}b_{i_0-\frac{1}{2}} - b_{i_0-1} < a_{i_0-1}$. It follows

$$\begin{array}{rcllcl} a_{i_0-\frac{1}{2}}b_{i_0} - a_{i_0}b_{i_0-\frac{1}{2}} & = & 1 \cdot 1 - 0 \cdot b_{i_0-\frac{1}{2}} & = & 1 & \text{and} \\ a_{i_0-1}b_{i_0-\frac{1}{2}} - a_{i_0-\frac{1}{2}}b_{i_0-1} & = & a_{i_0-1}b_{i_0-\frac{1}{2}} - 1 \cdot b_{i_0-1} & < & a_{i_0-1} & \\ & = & a_{i_0-1} \cdot 1 - 0 \cdot b_{i_0-1} & = & a_{i_0-1}b_{i_0} - a_{i_0}b_{i_0-1}. & \end{array}$$

By inserting the additional support half plane with normal vector $(a_{i_0-\frac{1}{2}}, b_{i_0-\frac{1}{2}})$ and support line through the vertex v_{i_0}, we "substitute" the value $a_{i_0-1}b_{i_0} - a_{i_0}b_{i_0-1}$ by the smaller value $a_{i_0-1}b_{i_0-\frac{1}{2}} - a_{i_0-\frac{1}{2}}b_{i_0-1}$ and add $a_{i_0-\frac{1}{2}}b_{i_0} - a_{i_0}b_{i_0-\frac{1}{2}} = 1$ to the list. All other values stay fixed. Repeating this process the statement in the proposition can be achieved. □

Now we construct the toric surface. Let $1 \leq i \leq n$ and set $\tilde{U}_i := \mathbb{A}^2_{\mathbb{K}}$ (again identifying $\tilde{U}_0$ and $\tilde{U}_n$) with coordinates u_i and v_i. We denote the coordinate axes by $L_i := \{(u_i, v_i) \in \tilde{U}_i \mid u_i = 0\}$ and $R_i := \{(u_i, v_i) \in \tilde{U}_i \mid v_i = 0\}$ and define an open embedding of the torus

$$\phi_i : T \to \mathbb{A}^2_{\mathbb{K}} : (x, y) \mapsto (u_i, v_i) = (x^{b_i}y^{-a_i}, x^{-b_{i-1}}y^{a_{i-1}}).$$

Its isomorphic image is $T_i = \tilde{U}_i \setminus (L_i \cup R_i)$ and on T_i the morphism ϕ_i has the inverse

$$(u_i, v_i) \mapsto (x, y) = (u_i^{a_{i-1}}v_i^{a_i}, u_i^{b_{i-1}}v_i^{b_i}).$$

For $1 \leq i \leq n$ we define isomorphisms

$$\psi_{i-1,i} : \tilde{U}_{i-1} \setminus R_{i-1} \to \tilde{U}_i \setminus L_i : (u_{i-1}, v_{i-1}) \mapsto (u_i, v_i) = (u_{i-1}^{a_{i-2}b_i - a_ib_{i-2}}v_{i-1}, u_{i-1}^{-1})$$

with inverses

$$\psi_{i,i-1} := \psi_{i-1,i}^{-1} : (u_i, v_i) \mapsto (u_{i-1}, v_{i-1}) = (v_i^{-1}, u_iv_i^{a_{i-2}b_i - a_ib_{i-2}}).$$

For two non-neighboring indices i and j, we get isomorphisms $\psi_{i,j} := \phi_j \circ \phi_i^{-1} : T_i \to T_j$. The $\psi_{i,j}$ then satisfy the gluing conditions $\psi_{j,k} \circ \psi_{i,j} = \psi_{i,k}$ whenever both sides are defined. Hence they describe an abstract variety V, the toric surface defined by $\Pi(f)$.

Via the gluing construction, each $\tilde{U}_i$ corresponds to an isomorphic open subset $U_i \subset V$ which together cover V. For any index i the open subset $U_{i-1} \cap U_i$ corresponds to the two open subsets $\tilde{U}_{i-1} \setminus R_{i-1}$ and $\tilde{U}_i \setminus L_i$ that are isomorphic by $\psi_{i-1,i}$. The union of the sets corresponding to $R_{i-1} \subset \tilde{U}_{i-1}$ and $L_i \subset \tilde{U}_i$ is a curve in V isomorphic to $\mathbb{P}^1_{\mathbb{K}}$ which we call edge curve and denote by E_i. The curves E_{i-1} and E_i intersect transversally in a point $V_i \in U_i$, corresponding to $(0, 0) \in \tilde{U}_i$. For non-neighboring indices i and j the edge curves E_i and E_j are disjoint. The complement of the union of all edge curves is the torus T, which is also the intersection of all open sets U_i.

Now the curve F given by f is defined to be the Zariski closure of F' in V. We will see its local equations in the next section. For the rest of the article we fix f and the corresponding curve $F \subset V$, i.e. in particular the data a_i, b_i, c_i derived from its Newton polygon.

Remark 2. The proof of lemma 1 corresponds to the resolution procedure for toric surfaces. Being covered by affine planes $\mathbb{A}^2_{\mathbb{K}}$ the constructed toric surface is actually smooth. For the parametrization algorithm this is not strictly necessary (although

it may be useful). Also the theoretical arguments that follow do not really need a smooth surface. Everything would go through as well using affine toric charts. We use this construction mainly for simplifying notation.

2.2. **Toric invariant divisors.** Irreducible curves on V are also called prime (Weil) divisors. A general divisor D is defined to be a formal sum (i.e. a linear combination over $\mathbb{Z}$) of prime divisors. The set of divisors forms a free Abelian group $\mathrm{Div}(V)$. The edge curves E_i of the previous section are the special "toric invariant" prime divisors. Consequently a toric invariant divisor is a formal sum of the E_i. One associates to a rational function $g \in \mathbb{K}(x,y)$ its principal divisor (g). Roughly speaking g has poles and zeros on V along certain subvarieties of codimension one; then (g) is the divisor of zeros minus the divisor of poles (with multiplicities). For a detailed introduction to divisors we refer to [12]. Two divisors are called linearly equivalent iff they differ only by a principal divisor. The divisor class group is defined as the group of divisors modulo this equivalence.

The coordinate ring of the torus is $\mathbb{K}[x,y,x^{-1},y^{-1}]$ which is a unique factorization domain. Hence any divisor on the torus is a principal divisor and the class group is trivial. This implies that the class group of the surface V is generated by the toric invariant divisors E_i. We will now show how to find representants in terms of these divisors.

Lemma 3. *Let $g \in \mathbb{K}[x,y,x^{-1},y^{-1}]$. Then g defines a curve on the torus T. Let G be its closure in the surface V. Then the divisor G is linearly equivalent to $G_0 = \sum_{1\le i\le n} -\tilde{c}_i E_i$ where $\tilde{c}_i = \min_{(r,s)\in \mathrm{Supp}(g)}(a_i r + b_i s)$, more precisely $G = G_0 + (g)$.*

Proof. On the affine open subset U_i let

$$g_i(u_i,v_i) := u_i^{-\tilde{c}_{i-1}} v_i^{-\tilde{c}_i} g(u_i^{a_{i-1}} v_i^{a_i}, u_i^{b_{i-1}} v_i^{b_i}).$$

Then $g_i \in \mathbb{K}[u_i,v_i]$ is the local equation of G. Further g_i differs from $u_i^{-\tilde{c}_{i-1}} v_i^{-\tilde{c}_i}$ only by the rational function g which is the same on each affine open set. Together we see that $G = G_0 + (g)$. □

This result holds for any $g \in \mathbb{K}[x,y,x^{-1},y^{-1}]$ and of course in particular for $g = f$, $G = F$ and $\tilde{c}_i = c_i$ from section 2.1. From the proof we get the local equations of the curve F embedded in V

$$f_i(u_i,v_i) := u_i^{-c_{i-1}} v_i^{-c_i} f(u_i^{a_{i-1}} v_i^{a_i}, u_i^{b_{i-1}} v_i^{b_i}) \tag{1}$$

and a linearly equivalent divisor $F_0 := \sum_{1\le i\le n} -c_i E_i$. Note that the divisor G_0 in the proposition depends only on the support of g, so we define:

Definition 4. Given a lattice polygon $\Pi \in \mathbb{R}^2$. We define the associated divisor $\mathrm{div}(\Pi) := \sum_{1\le i\le n} -\tilde{c}_i E_i$ with $\tilde{c}_i = \min_{(r,s)\in\Pi}(a_i r + b_i s)$.

With this definition of course $\mathrm{div}(\Pi(g)) = G_0$. In the sequel we will mainly deal with toric invariant divisors.

2.3. **Linear systems of toric invariant divisors.** A divisor D is called effective (or greater or equal to 0) iff it is a non-negative sum of prime divisors. The linear system of rational functions associated to a divisor D is the vector space of rational functions $g \in \mathbb{K}(x,y)$ s.t. $D + (g)$ is effective. If D is in particular a toric invariant divisor, then (g) must not have any poles on the torus. Thus we define:

Definition 5. Given a toric invariant divisor $D \in \mathrm{Div}(V)$, we define the linear system $\tilde{\mathcal{L}}(D) := \{g \in \mathbb{K}[x, y, x^{-1}, y^{-1}] \mid (g) + D \geq 0\}$.

As a corollary to lemma 3 we see that if the divisor is given by a lattice polygon this linear system is non-empty and has a simple description.

Corollary 6. *Let $\Pi \in \mathbb{R}^2$ be a lattice polygon, let $D = \mathrm{div}(\Pi) = \sum_{1 \leq i \leq n} -\tilde{c}_i E_i$ and define $\overline{\Pi} := \bigcap_{1 \leq i \leq n} \{(r, s) \in \mathbb{R}^2 \mid a_i r + b_i s \geq \tilde{c}_i\}$. Then $\tilde{\mathcal{L}}(D) = \langle x^r y^s \rangle_{(r,s) \in \overline{\Pi}}$ as a $\mathbb{K}$-vector space.*

Here $\overline{\Pi}$ is the smallest polygon containing Π and given by an intersection of translates of the half planes h_i.

3. Sparse Parametrization

It is well-known that a curve is parametrizable iff it has genus 0. In this section we will first show how to compute the genus in our setting. Afterwards we give a linear system of rational functions that is used to find the parametrizing map. Finally we describe the algorithm and execute it on an example.

3.1. **The genus.** If the curve F was embedded in the projective plane $\mathbb{P}^2_{\mathbb{K}}$ and had total degree d , we would have the genus formula $g(C) = \frac{(d-1)(d-2)}{2} - \sum_{P \in C} \delta_P$. The number δ_P is a measure of singularity, which is defined as the dimension of the quotient of the integral closure of the local ring by the local ring at P (cf. [7, exercise IV.1.8]). For instance, if P is an ordinary singularity of multiplicity μ, i.e. a self-intersection point where μ branches meet transversally, then $\delta_P = \frac{\mu(\mu-1)}{2}$. In particular the sum may be restricted to range over all singular points $P \in C$. If $\Pi \subset \mathbb{R}^2$ is a bounded domain we denote by $\#(Pi) := |\Pi \cap \mathbb{Z}^2|$ the number of lattice points in Π. We also write Π° for the interior of a domain. In the toric situation the genus can be computed as follows:

Proposition 7. *The genus of F is equal to the number of interior lattice points of $\Pi(f)$ minus the sum of the δ-invariants of all points of F:*

$$\mathrm{g}(F) = \#(\Pi(f)^\circ) - \sum_{P \in F} \delta_P$$

(The sum actually ranges over the singular points of F only.)

Proof. Let $\tilde{F} \to F$ be the normalization of the curve. The genus of F can be defined as the arithmetic genus $\mathrm{g}_a(\tilde{F})$ of its normalization. It is known that $\mathrm{g}_a(\tilde{F}) = \mathrm{g}_a(F) - \sum_{P \in F} \delta_P$ (cf. [7, exercise IV.1.8]).

The fact that the arithmetic genus $\mathrm{g}_a(F)$ equals the number of interior lattice points of $\Pi(f)$ is a consequence of the adjunction formula (cf. [4, p. 91]). □

3.2. **The parametrizing linear system.** First we define a family of special divisors on V.

Definition 8. Choose $1 \leq m < n$ and let

$$c'_i = \begin{cases} c_i & \text{if } 1 \leq i \leq m \text{ and} \\ c_i + 1 & \text{else} \end{cases}$$

where the c_i originate from the lattice polygon $\Pi(f)$. We define $D_m := F_0 - \sum_{m+1 \leq i \leq n} E_i = \sum_{1 \leq i \leq n} -c'_i E_i \in \mathrm{Div}(V)$ and denote by $d_i := \#(e_i) - 1$ the number of lattice points on the edge i. Further we define the constant $\tilde{d}_m := \sum_{1 \leq i \leq m} d_i$.

From now on fix such an m. Note that we deliberately excluded $m = n$. Now we compute the intersection number $F_0 \cdot D_m$, i.e. the number of intersections of F_0 and D_m counting multiplicities.

Lemma 9. *If $\tilde{d}_m \geq 2$ then $F_0 \cdot D_m = 2\#(\Pi(f)^\circ) + \tilde{d}_m - 2$.*

Proof. Let $v_{i_0} = (r_{i_0}, s_{i_0})$ be the vertex of $\Pi(f)$ common to the edges e_{i_0-1} and e_{i_0}. The intersection number is invariant w.r.t. linear equivalence of divisors. Then

$$\begin{aligned}
F_0 \cdot E_{i_0} &= (F_0 + (x^{r_{i_0}} y^{s_{i_0}})) \cdot E_{i_0} \\
&= \left(\textstyle\sum_{1\leq i\leq n} -c_i E_i + \sum_{1\leq i\leq n}(a_i r_{i_0} + b_i s_{i_0})E_i\right) \cdot E_{i_0} \\
&= \textstyle\sum_{1\leq i\leq n}(-c_i + a_i r_{i_0} + b_i s_{i_0})E_i \cdot E_{i_0} \\
&\overset{1)}{=} (-c_{i_0-1} + a_{i_0-1} r_{i_0} + b_{i_0-1} s_{i_0})E_{i_0-1} \cdot E_{i_0} \\
&\quad + (-c_{i_0} + a_{i_0} r_{i_0} + b_{i_0} s_{i_0})E_{i_0} \cdot E_{i_0} \\
&\quad + (-c_{i_0+1} + a_{i_0+1} r_{i_0} + b_{i_0+1} s_{i_0})E_{i_0+1} \cdot E_{i_0} \\
&\overset{2)}{=} a_{i_0+1}(r_{i_0} - r_{i_0+1}) + b_{i_0+1}(s_{i_0} - s_{i_0+1}) \\
&= \langle (a_{i_0+1}, b_{i_0+1}), (r_{i_0} - r_{i_0+1}, s_{i_0} - s_{i_0+1}) \rangle
\end{aligned}$$

where 1) holds because E_i and E_{i_0} are disjoint for non-neighboring indices i and i_0 and 2) holds because of the choice of (r_{i_0}, s_{i_0}) and E_{i_0}, E_{i_0+1} intersecting transversally. Finally the vector $(r_{i_0} - r_{i_0+1}, s_{i_0} - s_{i_0+1})$ is equal to $d_{i_0}(-b_{i_0}, a_{i_0})$ (because $\gcd(a_{i_0}, b_{i_0}) = 1$). Computing the scalar product and applying the identity $a_{i_0} b_{i_0+1} - b_{i_0} a_{i_0+1} = 1$ yields $F \cdot E_{i_0} = d_{i_0}$.

Further we compute

$$\begin{aligned}
F_0 \cdot D_m &= F_0 \cdot F_0 - F_0 \cdot \textstyle\sum_{m+1\leq i\leq n} E_i \\
&\overset{1)}{=} 2Vol(\Gamma) - \textstyle\sum_{m+1\leq i\leq n} d_i \\
&\overset{2)}{=} \left(2\#(\Pi(f)^\circ) - 2 + \textstyle\sum_{1\leq i\leq n} d_i\right) - \textstyle\sum_{m+1\leq i\leq n} d_i \\
&= 2\#(\Pi(f)^\circ) + \tilde{d}_m - 2
\end{aligned}$$

where 1) follows from the self-intersection formula for toric invariant divisors and 2) from Pick's formula (cf. [4, pp. 111 and 113]). □

We can also determine the dimension of the associated linear system.

Lemma 10. *We have $\dim_{\mathbb{K}}(\tilde{\mathcal{L}}(D_m)) = \#(\Pi(f)^\circ) + \tilde{d}_m - 1$.*

Proof. The divisor D_m is associated to a lattice polygon $\overline{\Pi}$ which is obtained "by subtracting certain edges of $\Pi(f)$", compare figure 2. For the number of lattice points one verifies the formula

$$\#(\overline{\Pi}) = \#(\Pi(f)) - \left(\textstyle\sum_{m+1\leq i\leq n} d_i\right) - 1 = \#(\Pi(f)^\circ) + \tilde{d}_m - 1.$$

But $\overline{\Pi}$ is already given by an intersection of translates of the half planes h_i. The lemma now follows from corollary 6. □

We define a subspace of the linear system $\tilde{\mathcal{L}}(D_m)$ by adding linear constraints derived from conductor ideals. Afterwards we state and prove the main theorem.

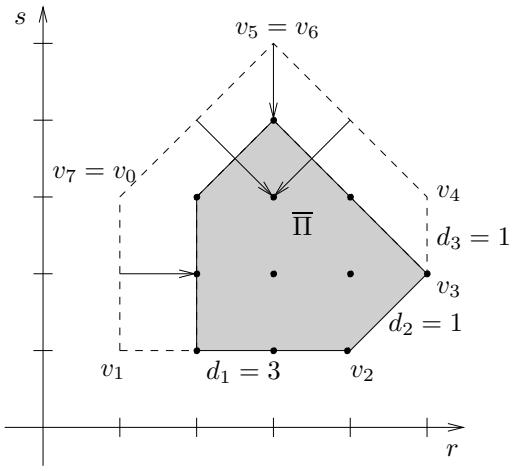


FIGURE 2. Dimension of the linear system
We illustrate the point counting argument of lemma 10. Let $m = 3$. The polygon $\overline{\Pi}$ corresponding to $\tilde{\mathcal{L}}(D_m)$ contains $d_1 + d_2 + d_3 - 1 = 4$ lattice points more than the interior of $\Pi(f)$.

Definition 11. Let R be a commutative ring and $\tilde{R}$ its integral closure. The set

$$\mathcal{C}(R) := \{r \in R \mid r\tilde{R} \subseteq R\}$$

is an ideal of both R and $\tilde{R}$. It is called the conductor (cf. [15, chapter V, §5]).

Definition 12. Let $g \in \tilde{\mathcal{L}}(D_m)$. For $1 \leq i \leq n$ let f_i and c_i be as in equation (1) and let

$$g_i(u_i, v_i) := u_i^{-c'_{i-1}} v_i^{-c'_i} g(u_i^{a_{i-1}} v_i^{a_i}, u_i^{b_{i-1}} v_i^{b_i})$$

with c'_i as in definition 8. We define the linear system of adjoint polynomials by $A_m := \{g \in \tilde{\mathcal{L}}(D_m) \mid g_i + \langle f_i \rangle \in \mathcal{C}(\mathbb{K}[u_i, v_i]/\langle f_i \rangle) \text{ for } 1 \leq i \leq n\}$.

There are other equivalent ways to define the adjoint system. For example if F has an ordinary singularity P of multiplicity μ then g (resp. one of the g_i) has to vanish on P with multiplicity at least $\mu - 1$. For more complicated singularities also infinitely close neighboring points have to be taken into account.

Theorem 13. *Assume $\tilde{d}_m \geq 2$. Let g be a* generic *polynomial in A_m and let $G \subset V$ be the Zariski closure of the curve defined by g on the torus. Then G and F have $\tilde{d}_m - 2$* free *intersections (i.e. intersections not determined by the linear constraints) and $\dim_{\mathbb{K}}(A_m) = \tilde{d}_m - 1$.*

Proof. For being adjoint to F the curve G has to pass through the singularities of F in a certain way and therefore has to meet additional linear constraints. In fact each singularity P poses δ_P constraints and gives rise to a local intersection of multiplicity $2\delta_P$ (cf. [5]).

The number of free intersections of G and F is therefore equal to

$$\begin{aligned} & F_0 \cdot D_m - \left(\sum_{P\in F} 2\delta_P\right) \\ \overset{\text{lem. 9}}{=} \quad & 2\#(\Pi(f)^\circ) + \tilde{d}_m - 2 - 2\left(\sum_{P\in F}\delta_P\right) \\ = \quad & 2\underbrace{\left(\#(\Pi(f)^\circ) - \sum_{P\in F}\delta_P\right)}_{=0} + \tilde{d}_m - 2. \end{aligned}$$

It is not clear a priori that the linear conditions are linearly independent, but we can compute a lower bound for the dimension of the system:

$$\begin{aligned} \dim_{\mathbb{K}}(A_m) \quad \geq \quad & \dim_{\mathbb{K}}(\tilde{\mathcal{L}}(D_m)) - \left(\sum_{P\in F}\delta_P\right) \\ \overset{\text{lem. 10}}{=} \quad & \#(\Pi(f)^\circ) + \tilde{d}_m - 1 - \left(\sum_{P\in F}\delta_P\right) \\ = \quad & \underbrace{\left(\#(\Pi(f)^\circ) - \sum_{P\in F}\delta_P\right)}_{=0} + \tilde{d}_m - 1 \end{aligned}$$

In both cases we finally apply the genus formula of proposition 7.

The last inequality is actually an equality. Assume indirectly that $\dim_{\mathbb{K}}(A_m) \geq \tilde{d}_m$. In this case we could choose another set $\{P_j\}_{1\leq j\leq \tilde{d}_m-1} \subset F$ of $\tilde{d}_m - 1$ smooth points. Restricting the system A_m to a system $\tilde{A}_m$ by requiring that $g \in \tilde{A}_m$ (resp. the corresponding g_i) also has to vanish on each of the P_j, we get $\dim_{\mathbb{K}}(\tilde{A}_m) \geq 1$ and intersection number -1. We would have constructed a curve on V (different from F) with negative intersection number, a contradiction. For another argument we refer to remark 18. □

This result is the main ingredient of the sparse parametrization algorithm. Assume $\tilde{d}_m \geq 3$. Choosing $\tilde{d}_m - 3$ additional smooth points $\{P_j\}_{1\leq j\leq \tilde{d}_m-3} \subset F$ we restrict the system A_m to a system $\tilde{A}_m$ by requiring that $g \in \tilde{A}_m$ (resp. the corresponding g_i) also has to vanish on each of the P_j. We get $\dim_{\mathbb{K}}(\tilde{A}_m) = 2$ and the number of free intersections drops to 1. Now let $\{p, q\} \subset \tilde{A}_m$ be a basis, then F and the zero set of $p + tq$ have (for generic values of t) one intersection in the torus depending on t. The coordinates of this intersection point can be expressed as rational functions in t; this is the parametrization. It is birational by construction, the inverse is given by $t = -p/q$.

3.3. **The algorithm.** We give the coarse description of an algorithm (algorithm 1) that exploits theorem 13 to compute a parametrization.

The first step is to compute the representation of the objects, e.g. the integers a_i, b_i, c_i defining the morphisms ϕ_i and the polynomials f_i (see equation (1)). The algorithm contains several loops over finite sets of points. The involved computations always have to use these local representations.

Line 2 makes the algorithm more economic because $\tilde{d}_m - 3$ is the number of additional smooth points that have to be chosen later.

Then (lines 3 to 7) we compute the genus, applying proposition 7, in order to decide rationality and return FAIL if the curve is not parametrizable.

Now we compute the parametrizing linear system (lines 8 to 13). We start with $\tilde{\mathcal{L}}(D_m)$. In a real implementation this could mean, we make an indetermined Ansatz $g = \sum_{(r,s)} c_{(r,s)} x^r y^s$ for a polynomial in $\tilde{\mathcal{L}}(D_m)$, the sum ranging only over a finite number of indices, compare lemma 10 and figure 2.

Algorithm 1 *Parametrize*$(f : \mathbb{K}[x,y]) : \mathbb{K}(t)^2 \cup \{\text{FAIL}\}$

Input : an irreducible polynomial $f \in \mathbb{K}[x,y]$
Output : a proper parametrization $(X(t), Y(t)) \in \mathbb{K}(t)^2$ s.t. $f(X(t), Y(t)) = 0$ or FAIL if no such parametrization exists

Compute $\Pi(f)$ and determine the chart representation $F \subset V = \bigcup_{1 \le i \le n} U_i$;
Find m and renumber indices s.t. $\tilde{d}_m - 2$ is minimally positive;
$\delta := 0$;
for $P \in \mathrm{Sing}(F)$ **do**
    $\delta := \delta + \delta_P$;
if $\#(\Pi(f)^\circ) - \delta \neq 0$ **then**
    return FAIL;
$S := \tilde{\mathcal{L}}(D_m)$;
for $P \in \mathrm{Sing}(F)$ **do**
    Add to S the adjoint conditions imposed by P;
Choose a set $\{P_j\}_{1 \le j \le \tilde{d}_m - 3}$ of smooth points on F;
for $1 \le j \le \tilde{d}_m - 3$ **do**
    Add to S the vanishing condition imposed by P_j;
return *Findmap*(f, S);

In order to add to S the adjoint conditions, one could compute the Puiseux expansions of the curve branches at the singular points, substitute those expansions into g (or one of the g_i respectively, see definition 12) and extract the linear constraints by enforcing the result to vanish with a certain minimum order. In positive characteristic, when Puiseux expansions are generally not available, the adjoint conditions can be determined using Hamburger-Noether expansions (see [1]). Another method would be to compute (locally) the conductor ideal (see [9]), reduce g (resp. g_i) w.r.t. this ideal and extract the linear constraints by enforcing ideal membership. In order to add to S the vanishing conditions for the smooth points, one simply substitutes the coordinates of a P_j into g (resp. g_i) and equates to zero.

In the final step we call a procedure *Findmap* to actually compute the parametrizing map. It could for example choose a basis $\{p, q\} \subset S$ and then solve the zero-dimensional system $f = p + tq = 0$ in $\mathbb{K}(t)[x,y]$ for $(x,y) \notin \mathbb{K}^2$ (using Gröbner bases or resultants).

Remark 14. As mentioned before it is not strictly necessary to carry out the resolution process of lemma 1. But if one does, one can compute locally using bivariate polynomial representations. In this setting some computer algebra systems (e.g. `Singular` [6] and `Maple`) provide functions to compute the delta invariants, certain series expansions of plane curves, etc. They can be used to determine the adjoint conditions.

3.4. **An example.** Consider the curve F defined by the polynomial

$$f := -27y^{21} + 8x^2y^{18} + 13x^3y^{16} - 8x^5y^{13} - 4x^4y^{14} + 4x^7y^{10} - 20x^6y^{11} - 8x^8y^8 + 8x^{10}y^5 + 4x^9y^6 + 8x^{11}y^3 + 4x^{13} \in \mathbb{Q}[x,y]$$

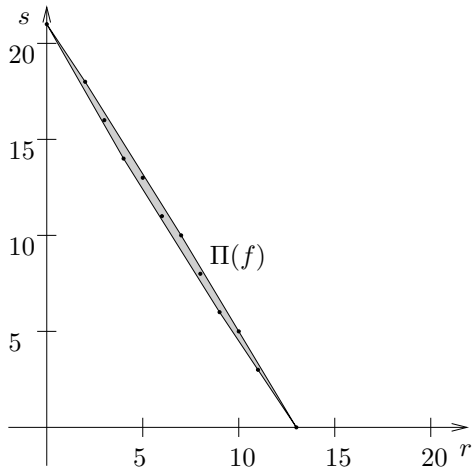


FIGURE 3. Newton polygon of f
The Newton polygon $\Pi(f)$ of the example is very "slim". Its only interior points are $(3,16)$, $(5,13)$, $(6,11)$ and $(8,8)$.

on the torus. Its Newton polygon $\Pi(f)$ has 6 vertices. We represent it as the intersection of $n = 8$ half planes h_i which are governed by the following data:

$$\begin{array}{llll}
v_1 = (13,0), & (a_1,b_1) = (-5,-3), & c_1 = -65, & d_1 = 2 \\
v_2 = (7,10), & (a_2,b_2) = (-8,-5), & c_2 = -106, & d_2 = 1 \\
v_3 = (2,18), & (a_3,b_3) = (-3,-2), & c_3 = -42, & d_3 = 1 \\
v_4 = (0,21), & (a_4,b_4) = (2,1), & c_4 = 21, & d_4 = 0 \\
v_5 = (0,21), & (a_5,b_5) = (7,4), & c_5 = 84, & d_5 = 1 \\
v_6 = (4,14), & (a_6,b_6) = (5,3), & c_6 = 62, & d_6 = 0 \\
v_7 = (4,14), & (a_7,b_7) = (8,5), & c_7 = 102, & d_7 = 1 \\
v_8 = (9,6), & (a_8,b_8) = (3,2), & c_8 = 39, & d_8 = 2
\end{array}$$

The half planes h_4 and h_6 have been introduced in order to fulfill the condition $a_{i-1}b_i - a_ib_{i-1} = 1$, although it will turn out that they do not really play a role here. By doing so, we added the vertices $v_4 = v_5$, $v_6 = v_7$ and the edges e_4, e_6 of length $d_4 = d_6 = 0$. From the Newton polygon (see figure 3) we see that $\#(\Pi(f)^\circ) = 4$.

For this example the half planes have already been arranged s.t. by setting $m := 2$ we get the optimal value $\tilde{d}_m = 3$. Consequently we will not have to choose any smooth points to get additional linear constraints later on.

The curve F is (by our construction) embedded in a toric surface $V = \bigcup_{1\le i\le 8} U_i$. We compute the representation of F in local coordinates using equation (1):

$$\begin{aligned}
f_1 \;=\; & -27v_1^2u_1^3 - 4v_1^3u_1 + 13v_1^2u_1^2 + 8v_1u_1^3 - 20v_1^2u_1 \\
& - 8v_1u_1^2 + 4v_1^2 - 8v_1u_1 + 4u_1^2 + 8v_1 + 8u_1 + 4
\end{aligned}$$

$$\begin{aligned}
f_2 &= -4v_2^4u_2^3 + 4v_2^4u_2^2 - 20v_2^3u_2^2 + 8v_2^3u_2 + 13v_2^2u_2^2 \\
&\quad - 8v_2^2u_2 - 27v_2u_2^2 + 4v_2^2 - 8v_2u_2 + 8v_2 + 8u_2 + 4 \\
f_3 &= 4v_3^3u_3^4 + 8v_3^3u_3^3 - 4v_3^2u_3^4 + 4v_3^3u_3^2 - 20v_3^2u_3^3 \\
&\quad - 8v_3^2u_3^2 + 8v_3^2u_3 + 13v_3u_3^2 - 8v_3u_3 + 4v_3 - 27u_3 + 8 \\
f_4 &= 4v_4^5u_4^3 + 8v_4^4u_4^3 + 8v_4^4u_4^2 + 4v_4^3u_4^3 - 8v_4^3u_4^2 \\
&\quad + 4v_4^3u_4 - 20v_4^2u_4^2 - 8v_4^2u_4 - 4v_4u_4^2 + 13v_4u_4 + 8v_4 - 27 \\
f_5 &= 4v_5^7u_5^5 + 8v_5^6u_5^4 + 8v_5^5u_5^4 + 4v_5^5u_5^3 - 8v_5^4u_5^3 \\
&\quad + 4v_5^3u_5^3 - 8v_5^3u_5^2 - 20v_5^2u_5^2 + 8v_5^2u_5 + 13v_5u_5 - 4u_5 - 27 \\
f_6 &= 4v_6^3u_6^7 + 8v_6^3u_6^6 + 4v_6^3u_6^5 + 8v_6^2u_6^5 - 8v_6^2u_6^4 \\
&\quad - 8v_6^2u_6^3 + 8v_6^2u_6^2 + 4v_6u_6^3 - 20v_6u_6^2 + 13v_6u_6 - 27v_6 - 4 \\
f_7 &= 4v_7^4u_7^3 + 8v_7^4u_7^2 + 8v_7^3u_7^3 - 8v_7^3u_7^2 + 4v_7^2u_7^3 \\
&\quad - 27v_7^3u_7 - 8v_7^2u_7^2 + 13v_7^2u_7 + 8v_7u^2 - 20v_7u_7 + 4u_7 - 4 \\
f_8 &= 8v_8^3u_8^4 - 27v_8^3u_8^3 + 4v_8^2u_8^4 - 8v_8^2u_8^3 + 13v_8^2u_8^2 \\
&\quad + 8v_8u_8^3 - 8v_8u_8^2 - 20v_8u_8 + 4u_8^2 - 4v_8 + 8u_8 + 4
\end{aligned}$$

It turns out that F has a singular point P on the toric invariant divisor E_1. It shows up in the open subsets U_1 and U_2 and has coordinates $(u_1, v_1) = (-1, 0)$, $(u_2, v_2) = (0, -1)$ respectively. Another singular point $Q \in E_8$ is lying in U_1 and U_8 with coordinates $(u_1, v_1) = (0, -1)$ and $(u_8, v_8) = (-1, 0)$. The curves $F \cap U_i$ for $i \in \{3, 4, 5, 6, 7\}$ are smooth. Hence all the information on the singularities can be gathered in U_1. For this purpose we compute the Puiseux expansions at the points P and Q:

$$\begin{aligned}
\sigma_P(\alpha) &= -\tfrac{1}{4}(u_1+1) + \alpha(u_1+1)^2 + (\tfrac{435}{608}\alpha - \tfrac{51}{2432})(u_1+1)^3 \dots \\
\sigma_Q(\alpha) &= -1 - \tfrac{5}{2}u_1 + \beta u_1^2 + (\tfrac{21}{4}\beta + \tfrac{195}{16})u_1^3 \dots
\end{aligned}$$

Here α denotes a root of $1024\alpha^2+516\alpha+63$ and β denotes a root of $16\beta^2+24\beta-45$. Taking conjugates into account we have two curve branches through each of the singular points.

From these expansions one can compute amongst others the δ-invariants $\delta_P = \delta_Q = 2$ (for details we refer to [13]). We compute the genus $\mathrm{g}(F) = \#(\Pi(f)^\circ) - \delta_P - \delta_Q = 4 - 2 - 2 = 0$, i.e. the curve F is indeed parametrizable.

Now we make an indetermined Ansatz for a polynomial in $\tilde{\mathcal{L}}(D_m)$. The support of such a polynomial has to lie within $\Pi(f)$ but not on the edges e_i for $i \in \{3, \dots, 8\}$.

$$g := c_1x^3y^{16} + c_2x^5y^{13} + c_3x^7y^{10} + c_4x^6y^{11} + c_5x^8y^8 + c_6x^{10}y^5$$

For obvious reasons, we only have to compute the local representation in U_1 (see definition 12):

$$g_1 = c_1v_1^2u_1 + c_4v_1^2 + c_2v_1u_1 + c_5v_1 + c_3u_1 + c_6$$

In order to be adjoint $g_1(\sigma_P)$ has to vanish with order at least 2 around $u_1 = -1$ and $g_1(\sigma_Q)$ has to vanish with order at least 2 around $u_1 = 0$ (again see [13]). Executing the substitutions and equating lowest terms to 0 one gets the linear constraints $\frac{1}{4}c_2 + c_3 - \frac{1}{4}c_5 = 0$, $-c_3 - c_6 = 0$ (from P) and $c_4 - c_5 + c_6 = 0$, $c_1 - c_2 + c_3 + 5c_4 - \frac{5}{2}c_5 = 0$ (from Q). We solve this system w.r.t. parameters c_3, c_4 and substitute the result into g to get a polynomial $\tilde{g} \in A_m$ (for any concrete

value of c_3 and c_4).

$$\tilde{g} = (-\tfrac{3}{2}x^3y^{16} - 3x^5y^{13} + x^7y^{10} + x^8y^8 + x^{10}y^5)c_3 \\ + (-\tfrac{3}{2}x^3y^{16} + x^5y^{13} + x^6y^{11} + x^8y^8)c_4$$

As a final step we solve the system $\{f = 0, \tilde{g} = 0, c_3 = 1, c_4 = t\}$ for x and y in $\mathbb{Q}(t)$. It has two distinct solutions. One is $(x, y) = (0, 0)$ which corresponds to the two singular points P and Q, the other one yields the parametrization:

$$X(t) = \frac{-256(2t^2 + 4t - 1)^3(t + 1)^7t^8}{(-1 + 8t)^3(2t^2 + 7t - 1)^5}$$
$$Y(t) = \frac{-32t^5(2t^2 + 4t - 1)^2(t + 1)^4}{(-1 + 8t)^2(2t^2 + 7t - 1)^3}$$

For illustrative purposes assume we had chosen $m := 3$ non-optimal (or we were in a situation where a choice s.t. $\tilde{d}_m = 3$ is not possible). We would get the following indetermined Ansatz for a polynomial in $\tilde{\mathcal{L}}(D_m)$:

$$g := c_0x^2y^{18} + c_1x^3y^{16} + c_2x^5y^{13} + c_3x^7y^{10} + c_4x^6y^{11} + c_5x^8y^8 + c_6x^{10}y^5$$

We compute the local representations in U_1 and U_5.

$$g_1 = c_1v_1^2u_1 + c_0v_1u_1^2 + c_4v_1^2 + c_2v_1u_1 + c_5v_1 + c_3u_1 + c_6$$
$$g_5 = c_6v_5^5u_5^3 + c_3v_5^4u_5^2 + c_5v_5^3u_5^2 + c_2v_5^2u_5 + c_4v_5u_5 + c_0v_5 + c_1$$

Proceeding as before, i.e. substituting the Puiseux expansions at the singular points P and Q in U_1 into g_1 we get the linear constraints $-\frac{1}{4}c_0 + \frac{1}{4}c_2 + c_3 - \frac{1}{4}c_5 = 0$, $-c_3 + c_6 = 0$, $c_4 - c_5 + c_6 = 0$ and $c_1 - c_2 + c_3 + 5c_4 - \frac{5}{2}c_5 = 0$. Now we have to choose an additional smooth point on F, e.g. $(u_5, v_5) = (-\frac{27}{4}, 0)$ in U_5. Plugging these coordinates into g_5 and equating the result to zero we get $c_1 = 0$. We again solve the system and substitute into g.

$$\tilde{g} = (-4x^5y^{13} - x^6y^{11} + x^7y^{10} + x^{10}y^5)c_6 \\ + (x^2y^{18} + \tfrac{5}{3}x^5y^{13} + \tfrac{2}{3}x^6y^{11} + \tfrac{2}{3}x^8y^8)c_0$$

Now in the same way as above we arrive at the following parametrization:

$$X(t) = \frac{(135 - 108t + 20t^2)^3(14t - 27)^7(-3 + 2t)^8}{429981696(16t^2 - 18t - 27)^5(t - 2)^8t^3}$$
$$Y(t) = \frac{-(135 - 108t + 20t^2)^2(14t - 27)^4(-3 + 2t)^5}{248832t^2(16t^2 - 18t - 27)^3(t - 2)^5}$$

Remark 15. A conventional algorithm based on an embedding of the curve in the projective plane $\mathbb{P}^2_{\mathbb{Q}}$ has to work very hard on that example. The corresponding complete curve would have again two singular points, but now the δ-invariants are 119 and 71. These complicated singularities show up only because the structure of the Newton polygon is not taken into account. Proceeding in this setting like we did, the involved linear systems are found as subspaces of a vector space of dimension greater than 200. The excellent Maple implementation of a parametrization algorithm produced around 40 DIN A4 pages of output. (Of course we admit that the chosen example is especially well-fit for our method.)

4. Another Proof of Correctness

This section is devoted to another proof of correctness using sheaf theoretical and cohomological arguments. Also theorem 13 could be deduced from what follows. From now on let $\tilde{F}$ be the normalization of F. We are in the following situation

$$\tilde{F} \overset{\pi}{\twoheadrightarrow} F \overset{\iota}{\hookrightarrow} V$$

and assume that F is parametrizable, i.e. $\mathrm{g}(\tilde{F}) = \mathrm{g}(F) = 0$.

4.1. **Some exact sequences.** The curve F is a closed subscheme of V. Let $\mathcal{I}(F)$ denote its ideal sheaf. We have an exact sequence of sheaves on V:

$$0 \to \mathcal{I}(F) \to \mathcal{O}_V \overset{\iota^\#}{\to} \iota_*(\mathcal{O}_F) \to 0$$

Now we define the conductor ideal sheaf on F, $\tilde{F}$ and V. Let $\mathcal{C}_F$ denote the sheaf defined by $U \mapsto \mathcal{C}(\mathcal{O}_F(U))$ (see definition 11) and $\mathcal{C}_{\tilde{F}} := \pi^*(\mathcal{C}_F)$. Observe that $\pi_*(\mathcal{C}_{\tilde{F}}) \cong (\mathcal{C}_F)$ because the conductor is an ideal sheaf on both F and $\tilde{F}$. Since $\mathcal{C}_F$ is a subsheaf of $\mathcal{O}_F$ trivially $\iota_*(\mathcal{C}_F)$ is a subsheaf of $\iota_*(\mathcal{O}_F)$. Now we define the conductor sheaf $\mathcal{C}_V$ on the surface by $\mathcal{C}_V(U) := (\iota^\#)^{-1}(\iota_*(\mathcal{C}_F)(U))$ for all open $U \subseteq V$. Clearly $\mathcal{C}_V$ is a subsheaf of $\mathcal{O}_V$ containing $ker(\iota^\#)$ and the restriction of $\iota^\#$ is still surjective. Thus we have an exact sequence

$$0 \to \mathcal{I}(F) \to \mathcal{C}_V \to \iota_*(\mathcal{C}_F) \to 0.$$

The invertible sheaf $\mathcal{L}(D)$ associated to a Weil divisor D on the smooth variety V is a subsheaf of the sheaf of rational functions $\mathcal{K}_V$ defined locally by

$$\mathcal{L}(D)(U) = \{g \in \mathcal{K}_V(U) \mid (g) + D\,|_U \geq 0\}$$

for all open $U \subseteq V$. This is a sheafified version of the definition 5. In fact $\tilde{\mathcal{L}}(D) = \Gamma(V, \mathcal{L}(D))$. Tensoring with invertible sheaves is exact so we get the exact sequence

$$0 \to \mathcal{I}(F) \otimes \mathcal{L}(D_m) \to \mathcal{C}_V \otimes \mathcal{L}(D_m) \to \iota_*(\mathcal{C}_F) \otimes \mathcal{L}(D_m) \to 0.$$

Now we define the following sheaf on $\tilde{F}$:

$$\mathcal{J} := \mathcal{C}_{\tilde{F}} \otimes (\iota \circ \pi)^*(\mathcal{L}(D_m))$$

Applying the projection formula (cf. [7, exercise II.5.1]) we see that

$$\begin{aligned}(\iota \circ \pi)_*(\mathcal{J}) &= (\iota \circ \pi)_*(\mathcal{C}_{\tilde{F}} \otimes (\iota \circ \pi)^*(\mathcal{L}(D_m))) \\ &\cong (\iota \circ \pi)_*(\mathcal{C}_{\tilde{F}}) \otimes \mathcal{L}(D_m) \\ &\cong \iota_*(\mathcal{C}_F) \otimes \mathcal{L}(D_m).\end{aligned}$$

Since $\mathcal{I}(F) = \mathcal{L}(-F) \cong \mathcal{L}(-F_0)$ we have $\mathcal{I}(F) \otimes \mathcal{L}(D_m) \cong \mathcal{L}(\widetilde{D_m})$ with $\widetilde{D_m} := D_m - F_0 = -\sum_{m+1 \leq j \leq n} E_j$. Putting things together, we get

$$0 \to \mathcal{L}(\widetilde{D_m}) \to \mathcal{C}_V \otimes \mathcal{L}(D_m) \to (\iota \circ \pi)_*(\mathcal{J}) \to 0. \tag{2}$$

Finally the global sections functor is left-exact which yields

$$0 \to \Gamma(V, \mathcal{L}(\widetilde{D_m})) \to \Gamma(V, \mathcal{C}_V \otimes \mathcal{L}(D_m)) \to \Gamma(V, (\iota \circ \pi)_*(\mathcal{J})) = \Gamma(\tilde{F}, \mathcal{J}). \tag{3}$$

But $\widetilde{D_m}$ is the inverse of an effective divisor and consequently has no global sections, i.e. $\Gamma(V, \mathcal{L}(\widetilde{D_m})) = 0$. In other words:

$$\Gamma(V, \mathcal{C}_V \otimes \mathcal{L}(D_m)) \hookrightarrow \Gamma(\tilde{F}, \mathcal{J}) \tag{4}$$

The global sections $\Gamma(V, \mathcal{C}_V \otimes \mathcal{L}(D_m))$ are very suitable for computation. Indeed if we write $\mathcal{C}_V \otimes \mathcal{L}(D_m)$ as a sheaf of rational functions, we see that its global sections correspond exactly to the system A_m of definition 12. In fact the last map of sequence (3) is also surjective and thus (4) is an isomorphism. We postpone the cohomological proof of this statement to the last section. Instead we proceed now with a brief study of the sheaf $\mathcal{J}$ and interpret the isomorphism in the context of the parametrization problem.

4.2. **The sheaf on the normalized curve.** First we reinterpret lemma 9 in the context of sheaves. In general for any divisor $D \in \mathrm{Div}(V)$ it is true that $\deg((\iota \circ \pi)^*(\mathcal{L}(D))) = F \cdot D$. Then $F \cdot D_m = F_0 \cdot D_m$ implies the following corollary.

Corollary 16. $\deg((\iota \circ \pi)^*(\mathcal{L}(D_m))) = 2\#(\Pi(f)^\circ) + \tilde{d}_m - 2$.

Proposition 17. *If* $\sum_{1 \le j \le m} d_j \ge 2$ *then* $\deg(\mathcal{J}) = \tilde{d}_m - 2$.

Proof. We compute the degree of $\mathcal{J}$ using $\deg(\mathcal{C}_{\tilde{F}}) = -2\sum_{P \in F} \delta_P$ (cf. [5]), corollary 16 and applying the genus formula of proposition 7:

$$\begin{aligned} \deg(\mathcal{J}) &= \deg(\mathcal{C}_{\tilde{F}} \otimes (\iota \circ \pi)^*(\mathcal{L}(D_m))) \\ &= \deg(\mathcal{C}_{\tilde{F}}) + \deg((\iota \circ \pi)^*(\mathcal{L}(D_m))) \\ &= -2\textstyle\sum_{P \in F} \delta_P + 2\#(\Gamma(f)^\circ) + \tilde{d}_m - 2 \\ &= 2\left(\#(\Gamma(f)^\circ) - \textstyle\sum_{P \in F} \delta_P\right) + \tilde{d}_m - 2 \\ &= \tilde{d}_m - 2. \end{aligned}$$

□

Assume $\tilde{d}_m \ge 3$ and let $d := \tilde{d}_m - 2$. Since F is assumed parametrizable, its normalization $\tilde{F}$ is isomorphic to $\mathbb{P}^1_{\mathbb{K}}$. Assume we have homogeneous coordinates u, v on $\mathbb{P}^1_{\mathbb{K}}$. Let $P \in \mathrm{Div}(\mathbb{P}^1_{\mathbb{K}})$ be the prime divisor corresponding to $u = 0$. Any invertible sheaf of degree d on $\mathbb{P}^1_{\mathbb{K}}$ is isomorphic to $\mathcal{L}(dP)$. This sheaf is generated by its global sections $\Gamma(\mathbb{P}^1_{\mathbb{K}}, \mathcal{L}(dP)) = \langle v^d/u^d, v^{d-1}u/u^d, \ldots, u^d/u^d \rangle$. They constitute a closed immersion $\psi : \mathbb{P}^1_{\mathbb{K}} \to \mathbb{P}^d_{\mathbb{K}} : [u : v] \mapsto [v^d : v^{d-1}u : \cdots : u^d]$. In other words, a basis of the global section space $\Gamma(\tilde{F}, \mathcal{J})$ defines an isomorphism between $\tilde{F}$ and the rational normal curve in $\mathbb{P}^d_{\mathbb{K}}$.

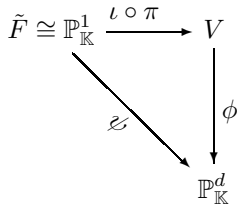
Remark 18. From this one could also get a slightly different proof of theorem 13 because $\deg(\mathcal{J})$ corresponds to the number of free intersections. The result on the dimension follows from the above arguments because $\dim_{\mathbb{K}}(A_m) = \dim_{\mathbb{K}}(\Gamma(V, \mathcal{C}_V \otimes \mathcal{L}(D_m))) = \dim(\Gamma(\tilde{F}, \mathcal{J})) = \deg(\mathcal{J}) + 1$.

4.3. **Reduction of the parametrization problem to rational normal curves.** Write $\mathcal{C}_V \otimes \mathcal{L}(D_m)$ as a sheaf of rational functions and identify $\mathcal{J}$ with $\mathcal{L}(dP)$ on $\mathbb{P}^1_{\mathbb{K}}$ as above. The functions in $\Gamma(V, \mathcal{C}_V \otimes \mathcal{L}(D_m))$ do not have a pole along F. The reader may check that isomorphism (4) is in fact given by the pullback $(\iota \circ \pi)^*$ of rational functions.

Now let $\{s_0, \ldots, s_d\} \subset \Gamma(V, \mathcal{C}_V \otimes \mathcal{L}(D_m)))$ be a basis s.t. $(\iota \circ \pi)^*(s_i) = v^{d-i}u^i/u^d$ and define a rational map by

$$\phi : T \to \mathbb{P}^d_{\mathbb{K}} : (x, y) \mapsto [s_0 : s_1 : \cdots : s_d]$$

on the torus. We find that it maps $\tilde{F}$ (and hence also F) birationally to the rational normal curve in $\mathbb{P}^d_{\mathbb{K}}$:



In the algorithm we finally choose a set of $\tilde{d}_m - 3 = d - 1$ smooth points and restrict the linear system using vanishing conditions imposed by these points. In our current setting this corresponds to choosing points on the rational normal curve and projecting until we reach the projective line $\mathbb{P}^1_{\mathbb{K}}$; the natural way to parametrize a rational normal curve.

4.4. **Vanishing of the first cohomology.** It remains to show that the last map of sequence (3) is surjective. We will use Čech cohomology w.r.t. the natural affine cover $\mathfrak{U} := \{U_i\}_{1 \le i \le n}$ to derive the desired result. From the short exact sequence (2) we get a long exact sequence

$$\begin{array}{rcccccc} 0 & \to & \Gamma(V, \mathcal{L}(\widetilde{D_m})) & \to & \Gamma(V, \mathcal{C}_V \otimes \mathcal{L}(D_m)) & \to & \Gamma(V, (\iota \circ \pi)_*(\mathcal{J})) \\ & \to & \check{\mathrm{H}}^1(\mathfrak{U}, \mathcal{L}(\widetilde{D_m})) & \to & \dots & & \end{array}$$

So we have to show that $\check{\mathrm{H}}^1(\mathfrak{U}, \mathcal{L}(\widetilde{D_m})) = 0$.

To define Čech cohomology we use the following set of half planes:

$$\bar{h}_i := \{(r,s) \in \mathbb{R}^2 \mid a_i r + b_i s \ge \Delta_i\} \text{ where } \Delta_i = \begin{cases} 0 & \text{for } 1 \le i \le m \text{ and} \\ 1 & \text{else} \end{cases}$$

Using the coordinate transformations of section 2 and these half planes one describes the needed sections of $\mathcal{L}(\widetilde{D_m})$ as $\mathbb{K}$-vector spaces:

$$\begin{aligned} \Gamma(U_i, \mathcal{L}(\widetilde{D_m})) &= \langle x^r y^s \rangle_{(r,s) \in \bar{h}_{i-1} \cap \bar{h}_i} \text{ for } 1 \le i \le n, \\ \Gamma(U_{i-1} \cap U_i, \mathcal{L}(\widetilde{D_m})) &= \langle x^r y^s \rangle_{(r,s) \in \bar{h}_i} \text{ for } 2 \le i \le n, \\ \Gamma(U_i \cap U_j, \mathcal{L}(\widetilde{D_m})) &= \langle x^r y^s \rangle_{(r,s) \in \mathbb{Z}^2} \text{ for } 1 \le i < j \le n \text{ and } j - i \ge 2, \\ \Gamma(U_i \cap U_j \cap U_k, \mathcal{L}(\widetilde{D_m})) &= \langle x^r y^s \rangle_{(r,s) \in \mathbb{Z}^2} \text{ for } 1 \le i < j < k \le n \end{aligned}$$

The first objects in the Čech complex are given by

$$\begin{aligned} \mathrm{C}^0(\mathfrak{U}, \mathcal{L}(\widetilde{D_m})) &= \prod_{1 \le i \le n} \Gamma(U_i, \mathcal{L}(\widetilde{D_m})), \\ \mathrm{C}^1(\mathfrak{U}, \mathcal{L}(\widetilde{D_m})) &= \prod_{1 \le i < j \le n} \Gamma(U_i \cap U_j, \mathcal{L}(\widetilde{D_m})), \\ \mathrm{C}^2(\mathfrak{U}, \mathcal{L}(\widetilde{D_m})) &= \prod_{1 \le i < j < k \le n} \Gamma(U_i \cap U_j \cap U_k, \mathcal{L}(\widetilde{D_m})) \end{aligned}$$

and the first maps by

$$\begin{aligned} d^0 &: (g_i)_i \mapsto (g_j - g_i)_{i<j}, \\ d^1 &: (g_{i,j})_{i<j} \mapsto (g_{j,k} - g_{i,k} + g_{j,k})_{i<j<k}. \end{aligned}$$

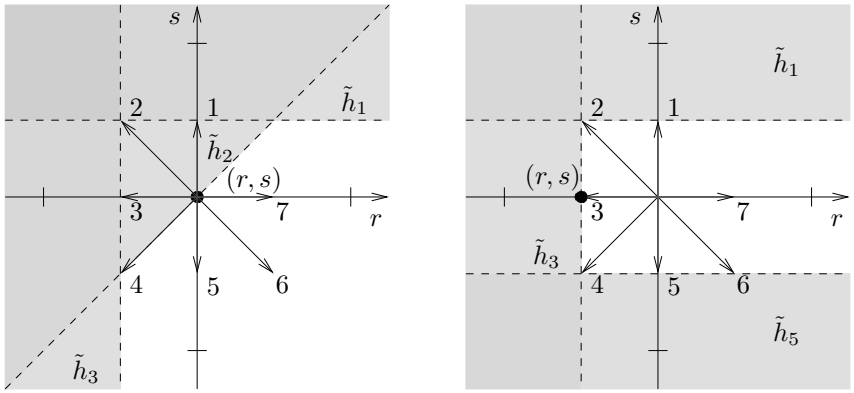


FIGURE 4. The half planes $\tilde{h}_i$
We illustrate the arguments of lemma 19.
Left: $l = 1$, $k = 3$, $j_0 = 2$ and $i_0 \in \{4, \dots, 7\}$. $(0, 1) = (a_1, b_1)$ and $(-1, 0) = (a_3, b_3)$ are linearly independent and we have the linear combination $(a_2, b_2) = (a_1, b_1) + (a_3, b_3)$.
Right: $l = 1$, $k = 5$, $j_0 = 3$ and $i_0 \in \{6, 7\}$. We have $(0, 1) = (a_1, b_1) = -(a_3, b_3)$ and $(r, s) = 1 \cdot (-b_1, a_1)$.

Since $\Pi(f)$ is a non-degenerate polygon the cone spanned by the set of normal vectors (a_i, b_i) must be the whole of $\mathbb{R}^2$. It can be shown that for each lattice point $(r, s) \in \mathbb{Z}^2$ there is at least one i s.t. $(r, s) \in \bar{h}_i$ and there is at least one i s.t. $(r, s) \notin \bar{h}_i$. Moreover each (r, s) separates the half planes into those containing the point and those not containing the point. It turns out that the half planes containing (r, s) have cyclically consecutive indices. This is equivalent to the following lemma.

Lemma 19. *Let $J = \{l, \dots, j_0, \dots, k\} \subseteq \{1, \dots, n\}$ (with l, j_0, k pairwise distinct) be a set of cyclically consecutive indices and $(r, s) \in \mathbb{Z}^2$ a lattice point. If $(r, s) \notin \bar{h}_l \cup \bar{h}_k$ and $(r, s) \in \bar{h}_{j_0}$ then $(r, s) \notin \bar{h}_i$ for all $i \in \{1, \dots, n\} \setminus J$.*

Proof. If $J = \{1, \dots, n\}$ there is nothing to show. So let $J \neq \{1, \dots, n\}$, choose $i_0 \in \{1, \dots, n\} \setminus J$ and assume indirectly $(r, s) \in \bar{h}_{i_0}$. We distinguish two cases:

(1) If (a_l, b_l) and (a_k, b_k) are linearly independent (see figure 4, left) then they can be used to express either (a_{j_0}, b_{j_0}) or (a_{i_0}, b_{i_0}) as a positive linear combination. Assume w.l.o.g. $(a_{j_0}, b_{j_0}) = \alpha(a_l, b_l) + \beta(a_k, b_k)$ with $\alpha, \beta > 0$. Then

$$\Delta_{j_0} \leq a_{j_0} r + b_{j_0} s = \alpha \underbrace{(a_l r + b_l s)}_{<\Delta_l} + \beta \underbrace{(a_k r + b_k s)}_{<\Delta_k}.$$

This is possible only if $\Delta_{j_0} = 0$, $\Delta_l = \Delta_k = 1$ and $a_l r + b_l s = a_k r + b_k s = 0$, hence $(r, s) = 0$. Since also the set of indices i with Δ_i is cyclically consecutive this also implies $\Delta_{i_0} = 1$. Then $a_{i_0} r + b_{i_0} s = 0 < \Delta_{i_0}$ and hence $(r, s) \notin \bar{h}_{i_0}$, a contradiction.

(2) If $(a_l, b_l) = -(a_k, b_k)$ (see figure 4, right) then necessarily $\Delta_l = \Delta_k = 1$ and $(r, s) = \gamma(-b_l, a_l)$ with $\gamma \in \mathbb{Z}$. Then either $\Delta_{j_0} = 1$ or $\Delta_{i_0} = 1$ must hold. Assume w.l.o.g. $\Delta_{j_0} = 1$. Then $a_{j_0} r + b_{j_0} s \geq 1$ implies $\gamma \geq 1$ and $a_{i_0} r + b_{i_0} s \geq \Delta_{i_0}$ implies $\gamma \leq 0$, a contradiction. □

For an element $\underline{g} = (g_{l,k})_{l<k} \in \ker(d^1)$ we have $g_{l,k} = g_{l,i} + g_{i,k}$ for $l < i < k$. From this follows $g_{l,k} = \sum_{l<i\leq k} g_{i-1,i}$. Hence $\underline{g}$ is uniquely determined by $g_{i-1,i}$ for $1 < i \leq n$. Writing $g_{0,1} = g_{n,1} = -g_{1,n}$ we get in particular $\sum_{1\leq i\leq n} g_{i-1,i} = 0$. Because of the structure of the section spaces, we may describe C^0, d^0 etc. in an obvious way as direct sums with indices (r, s). We indicate this by subscripts, i.e. $\mathrm{C}^0_{(r,s)}$, $d^0_{(r,s)}$ etc.

Proposition 20. *The first cohomology of $\mathcal{L}(\widetilde{D_m})$ vanishes: $\check{\mathrm{H}}^1(\mathfrak{U}, \mathcal{L}(\widetilde{D_m})) = 0$.*

Proof. We have to show $\mathrm{im}(d^0) = \ker(d^1)$. For this we fix an arbitrary lattice point $(r, s) \in \mathbb{Z}^2$ and show $\mathrm{im}(d^0_{(r,s)}) = \ker(d^1_{(r,s)})$. Let $\underline{g} \in \ker(d^1_{(r,s)})$. Using lemma 19 we may assume w.l.o.g. that there is an $l < n$ s.t. $(r, s) \in \bar{h}_i$ for $1 \leq i \leq l$ but $(r, s) \notin \bar{h}_i$ for $l < i \leq n$.

We can find a $d^0_{(r,s)}$-preimage of $\underline{g}$ by setting $g_1 := 0$, $g_i := g_{i-1} + g_{i-1,i}$ for $1 < i \leq l$ and $g_i := 0$ for $l < i \leq n$. First observe that with this definition we really have $(g_i)_i \in \mathrm{C}^0_{(r,s)}(\mathfrak{U}, \mathcal{L}(\widetilde{D_m}))$ because $g_i \neq 0$ implies $(r, s) \in \bar{h}_{i-1} \cap \bar{h}_i$.

Now we check that $\underline{g} = d^0_{(r,s)}((g_i)_i)$: For $1 < i \leq l$ we get $g_{i-1,i} = g_i - g_{i-1}$ by definition. For $l + 1 < i \leq n$ we know that $(r, s) \notin \bar{h}_{i-1}$ and $(r, s) \notin \bar{h}_i$, i.e. $g_{i-1,i} = g_i = g_{i-1} = 0$, hence again $g_{i-1,i} = g_i - g_{i-1}$. This also implies

$$0 = \sum_{1\leq i\leq n} g_{i-1,i} = \sum_{1<i\leq l+1} g_{i-1,i} = \left(\sum_{1<i\leq l} g_i - g_{i-1}\right) + g_{l,l+1} = g_l + g_{l,l+1}$$

or equivalently $g_{l,l+1} = 0 - g_l = g_{l+1} - g_l$. □

5. Conclusion

We presented a method for the rational parametrization of plane algebraic curves (on the torus). The main idea was to embed the curve in a toric surface that is adapted to the shape of the Newton polygon. We showed one possible method to parametrize in this setting. But also other algorithms like [14] and [8] could possibly benefit from this approach.

Up to now sparsity of the defining equation is used as far as the Newton polygon is considerably smaller than a full triangle. Another sort of sparsity would be when the lattice spanned by the support of the equation is not the whole of $\mathbb{Z}^2$ but only a sublattice. We also think about studying that case.

In this article we have assumed an algebraically closed coefficient field. We have not taken into account the degree of the field extension needed to represent the parametrization when starting from a non-closed field. This has been addressed for example in [11]. The ideas should carry over to our situation. Parametrization of rational normal curves using a field extension of least possible degree can also be achieved using the Lie algebra method in [3].

References

[1] A. Campillo and J. I. Farrán. Symbolic Hamburger-Noether expressions of plane curves and applications to AG codes. *Math. Comp.*, 71(240):1759–1780 (electronic), 2002.

[2] David Cox. What is a toric variety? In *Topics in Algebraic Geometry and Geometric Modeling*, volume 334 of *Contemporary Mathematics*, pages 203–223. American Mathematical Society, Providence, Rhode Island, 2003. Workshop on Algebraic Geometry and Geometric Modeling (Vilnius, 2002).

[3] Willem A. de Graaf, Michael Harrison, Jana Pilnikova, and Josef Schicho. A Lie Algebra Method for Rational Parametrization of Severi-Brauer Surfaces. 2005. submitted for publication and electronically available at `http://arxiv.org/abs/math.AG/0501157`.

[4] William Fulton. *Introduction to toric varieties*, volume 131 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1993. The William H. Roever Lectures in Geometry.

[5] Daniel Gorenstein. An arithmetic theory of adjoint plane curves. *Trans. Amer. Math. Soc.*, 72:414–436, 1952.

[6] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 2.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2001. `http://www.singular.uni-kl.de`.

[7] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[8] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4):425–445, 2002.

[9] Michal Mňuk. An algebraic approach to computing adjoint curves. *J. Symbolic Comput.*, 23(2-3):229–240, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

[10] J. Rafael Sendra and Franz Winkler. Symbolic parametrization of curves. *J. Symbolic Comput.*, 12(6):607–631, 1991.

[11] J. Rafael Sendra and Franz Winkler. Parametrization of algebraic curves over optimal field extensions. *J. Symbolic Comput.*, 23(2-3):191–207, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

[12] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, second edition, 1994. Varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.

[13] Peter Stadelmeyer. On the Computational Complexity of Resolving Curve Singularities and Related Problems. Technical Report 00-31, RISC-Linz, A-4232 Hagenberg, December 2000. PhD Thesis.

[14] Mark van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *J. Symbolic Comput.*, 23(2-3):209–227, 1997. Parametric algebraic curves and applications (Albuquerque, NM, 1995).

[15] Oscar Zariski and Pierre Samuel. *Commutative algebra. Vol. I*. Springer-Verlag, New York, 1975. With the cooperation of I. S. Cohen, Corrected reprinting of the 1958 edition, Graduate Texts in Mathematics, No. 28.

JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS, ALTENBERGERSTRASSE 69, A–4040 LINZ, AUSTRIAN ACADEMY OF SCIENCES