Computing intersections, decomposing algebraic sets, the genus of a curve and parametrization of rational curves

Janko Böhm
University of Saarland

17.05.2004

Abstract

This is the manuscript for talks given in a seminar on computer aided geometric design at the University of Saarland. The aim of the talks was to introduce the basic concepts of algebraic geometry, the computational tools, i.e. resultants and Groebner bases, and their geometric applications.

Contents

1 Intersection computations

Considering the task of computing the intersection of $V(J_1), V(J_2) \subset \mathbb{A}^n(k)$, $J_1, J_2 \subset k[x_1, ..., x_n]$ we first recall that $V(J_1) \cap V(J_2)$ is again algebraic and we know how to describe it

$$V(J_1) \cap V(J_2) = V(J_1 + J_2)$$

and the generators of the ideal $J_1 + J_2$ are given by the union of the generators of J_1 and J_2. Do we have more information about the intersection?

1.1 The dimension theorem

Consider two affine linear subspaces $U, V \subset W$ of a vector space W of $\dim W = n$. Then

$$\dim U \cap V = \dim U + \dim V - \dim(U + V) \geq \dim U + \dim V - n$$

This also holds for linear subspaces in projective space $\mathbb{P}^n(k)$ and there is an analogous generalization to varieties. First note, that the intersection of two varieties can be reducible. We define the dimension $\dim X$ of $X = V(I) \subset \mathbb{A}^n(k)$ as the maximal d, such that the generic projection

$$\mathbb{A}^n(\bar{k}) \supset V(I) \xrightarrow{\pi} \mathbb{A}^d(\bar{k})$$

is finite (i.e. $\pi^{-1}(p)$ is a finite set of points $\forall p \in \mathbb{A}^d(\bar{k})$) and surjective. Then it holds:

Theorem 1 *Let $k = \bar{k}$. If $X, Y \subset \mathbb{A}^n(k)$ are varieties of $\dim X = r$ and $\dim Y = s$, then each irreducible component of $X \cap Y$ has dimension $\geq r + s - n$. If X and Y are in sufficiently general position to each other then equality holds.*

Note that in the projective setting $X, Y \subset \mathbb{P}^n(k)$ additionally we get, that $X \cap Y \neq \emptyset$ if $r + s - n \geq 0$ and $X \cap Y$ is connected if $r + s - n \geq 1$.

If the intersection is 0-dimensional i.e. a set of points (e.g., the intersection of two plane curves), then we can describe it by giving the coordinates of the points:

1.2 Describing sets of points

Given $J \subset k[x_1, ..., x_n]$ an ideal with $|V(J)| < \infty$, how to compute the points of $V(J)$ explicitely? The naive algorithm would be:

1. Project, e.g., compute $J \cap k[x_i] = \langle f_i \rangle$, which is generated by one element ($k[x_i]$ is a principal ideal domain). This can be done using Groebner bases or resultants.

2. Compute the finite sets $V(f_i)$.

3. Check, which points of $V(f_1) \times ... \times V(f_n)$ satisfy J.

but we can do better:

Definition 2 *A minimal Groebner basis $g_1, ..., g_r$ is called reduced, if for all i, j term of g_i is divisible by some $L(g_j)$ and the coefficient of all $L(g_j)$ is 1. The reduced Groebner basis is unique.*

Lemma 3 (Shape Lemma) *Given $J = \sqrt{J} \subset k[x_1, ..., x_n]$ with $V(J) = \{p_1, ..., p_r\}$ and $p_{i,n} \neq p_{j,n}$ for all $i \neq j$, then the reduced Groebner basis with respect to any monomial order with the property $x_n^a < x_i$ for all a and j (e.g., lex with $x_1 > ... > x_n$) has the shape*

$$x_1 - g_1(x_n), ..., x_{n-1} - g_{n-1}(x_n), g_n(x_n)$$

with g_n squarefree of degree $\deg g_n = r$ and $\deg g_i < \deg g_n$.

We skip the proof, as the idea is simple: All points project to different n-th coordinate values so the Groebner basis has to contain linear equations, which allow us to calculate the unique $1, ..., n-1$ coordinate values from the n coordinate value.

So we could solve g_n for the x_n-coordinates (e.g., numerically) and use the equations $1, ..., n-1$ to compute to coordinate values $1, ..., n-1$.

Example 4 *Take the equations*

$$f_1 = x^3 - y^2$$
$$f_2 = x^3 - z$$
$$f_3 = xy - 1$$

A reduced Groebner basis of $I = \langle f_1, f_2, f_3 \rangle$ with respect to lex with $x > y > z$ is given by

$$x - z^2, y - z^3, z^5 - 1$$

Hence get the points $(\zeta^2, \zeta^3, \zeta)$ with a fifth root of unity ζ (so over $\mathbb{R}$ just $(1,1,1)$).

See Maple for plot.

1.3 Intersection of two varieties

Suppose we are given two plane curves C_1 and C_2 and want to compute the intersection. By the theorem of Bezout, we expect the intersection $C_1 \cap C_2$ to consist of $d_1 d_2$ points counted with multiplicity. In $\mathbb{P}^n$ with $n \geq 3$ we do not expect C_1 and C_2 to meet, but nevertheless it can happen due to the special nature of C_1 and C_2 with respect to each other. We assume, that C_1 and C_2 do not have a component in common and hence meet in points.

We already treated the question, how to describe ideals of points, so if $C_1 = V(J_1)$ and $C_2 = V(J_2)$ are given implicitely, consider $J = J_1 + J_2$ in the above discussion.

If one or both curves are given parametrically, then we can compute an implicit description for them. But if one of the curves is given parametrically, we should of course take advantage of this:

Lemma 5 *For curves C_1 and C_2 with $C_1 = image(\varphi)$ with $\varphi : \mathbb{A}^1(k) \to \mathbb{A}^n(k)$ polynomial and $C_2 = V(J_2)$ with $J_2 = \langle f_1, ..., f_r \rangle \in k[x_1, ..., x_n]$ it holds: There is an $f \in k[t]$ with $\langle f_1 \circ \varphi, ..., f_r \circ \varphi \rangle = \langle f \rangle$ by Euclidian algorithm and*

$$C_1 \cap C_2 = \varphi(V(f))$$

In $\mathbb{A}^3(k)$ we expect a surface S and a curve C to meet in points. If C and S are given implicitely, we are again in the case of describing a zero dimensional ideal, and otherwise we can implicitize them. If the curve is given parametrically, then we can deal with this completely analogous to the curve-curve case.

Example 6 *Consider the cubic surface*

$$S = V(xz(x+z) - y(2-2x-2y-2z)(-y+2-2x-2z)) \subset \mathbb{A}^3$$

and the curve $C = image(\varphi)$ with $\varphi(t) = \left(3t, -2t, 2 + t^3 + \frac{21}{8}t^2 + \frac{5}{4}t\right)$ we get the equation

$$S \cap C = \varphi\left(V\left(\frac{1}{64}t(8t+5)(t+2)\left(88t^4 + 231t^3 + 374t^2 + 224t + 128\right)\right)\right)$$

so we get 3 real intersection points. See Maple for the plot.

Given two surfaces $S_1 = V(J_1), S_2 = V(J_2) \subset \mathbb{A}^3(k)$ by the affine dimension theorem, we expect the intersection to be a curve.

Example 7 *The curve* $C = V(y^2 - x^3, z - x^2)$ *is the intersection of the two surfaces* $V(y^2 - x^3)$ *and* $V(z - x^2)$.

Example 8 *The intersection of the* 2 *surfaces*

$$X_1 = V\left(x^2 - y^2 z\right)$$
$$X_2 = V(z - 1)$$

decomposes into a union of two lines:

$$X_1 \cap X_2 = V(x - y, z - 1) \cup V(x + y, z - 1)$$

See Maple for the plot.

This naturately poses two questions, we will consider in what follows: How to describe curves parametrically (if possible) and how to deal with reducible varieties (this of course one can also apply to a set of points).

2 Decomposing algebraic sets

Definition 9 $\emptyset \neq S \subset k^n$ *is called irreducible, if it is not the union of two proper subvarieties, i.e.*

$$S \neq S_1 \cup S_2 \text{ for all varieties } S_1, S_2 \subsetneqq S$$

So the question arises, how to describe this in terms of ideals.

Recall that an ideal is called prime ideal, if $f \cdot g \in I$ then $f \in I$ or $g \in I$.

Theorem 10 S *is irreducible iff* $I(S)$ *is prime.*

Proof. Suppose $I(S)$ is prime, but S is reducible with $S = S_1 \cup S_2$. There is a $p \in S_2$ and $f \in I(S_1)$ with $f(p) \neq 0$. Otherwise $I(S_1) \subset I(S_2)$ so $S_1 = S$. Symmetrically there is a $q \in S_1$ and $g \in I(S_2)$ with $g(q) \neq 0$. Hence $f \cdot g \in I(S)$ and $f, g \notin I(S)$.

Consider our example with the 4 points:

Example 11 $\langle x^2 - 1, y^2 - 4 \rangle = \langle x-1, y-2 \rangle \cap \langle x-1, y+2 \rangle \cap \langle x+1, y-2 \rangle \cap \langle x+1, y+2 \rangle$*, the intersection of* 4 *maximal ideals.*

Recall, that an ideal $I \subsetneqq R$ is called maximal, if for all ideals J with $I \subset J \subset R$ holds $I = J$ or $J = R$. (Exercise: prove that a maximal ideal is prime). If $k = \overline{k}$ the maximal ideals correspond to the points.

Example 12 $\langle x^2 - x, xy \rangle = \langle x \rangle \cap \langle x-1, y \rangle$*, the intersection of a prime ideal and a maximal ideal.*

(Exercise: Prove the equalities).

Since any algebraic set can be written as union of irreducible ones (varieties), and any such is given by a prime ideal, one could expect that any ideal is the intersection of prime ideals. The example $\langle x^2 \rangle$ shows that this is false. What is true is the following:

Recall, that an ideal $J \subset R$ is called irreducible, if for all ideals $J \subset J_i$ we have $J \neq J_1 \cap J_2$. Futhermore recall, that a ring is called Noetherian, if the following equivalent conditions hold:

1. every ideal is finitely generated

2. R contains no infinitely properly ascending chain of ideals

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq ...$$

3. Any nonempty set of ideals in R has a maximal element.

The Hilbert basis theorem states, that the polynomial ring $k[x_1, ..., x_n]$ is Noetherian.

Lemma 13 *In a Noetherian ring any ideal is the finite intersection of irreducible ideals.*

Proof. Let M be the set of ideals, which cannot be written as a finite intersection of irreducible ideals. M has a maximal element J, since the ring is Noetherian. J is not irreducible, i.e. $J = J_1 \cap J_2$. Since J was maximal, J_1 and J_2 are finite intersections of irreducibles and so is also J.

Example 14 *In the following example the vanishing locus consists of* 2 *points*

$$\left\langle x^2\left(x-1\right),y\right\rangle = \left\langle x-1,y\right\rangle \cap \left\langle x^2,y\right\rangle$$

both ideals are irreducible, but $\left\langle x^2,y\right\rangle$ *is not prime.*

If we pass to the radical, then our above suspection becomes true:

Theorem 15 *For any ideal* J *the radical* $\sqrt{J}$ *is a finite intersection of prime ideals.*

Example 16 *In the above example*

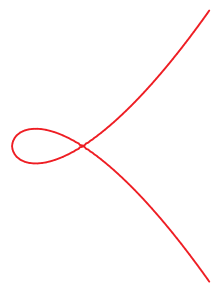
$$\left\langle x\left(x-1\right),y\right\rangle = \sqrt{\left\langle x^2\left(x-1\right),y\right\rangle} = \left\langle x-1,y\right\rangle \cap \left\langle x,y\right\rangle$$

3 The genus of a curve

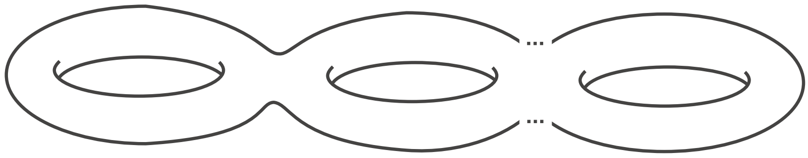
Consider an irreducible curve $C \subset \mathbb{P}^n(\mathbb{C})$ i.e. a variety of dimension 1. Given such a C, e.g., obtained as the intersection of some other varieties, from the computational point of view, it would be great to have a description by a parametrization. Does every curve have a rational parametrization? The answer is no, and the reason is the following:

3.1 Topological definition

Any curve $C \subset \mathbb{P}^n(\mathbb{C})$ is of complex dimension 1 and hence of real dimension 2, i.e. it is a real surface. At almost all points of C we can parametrize C locally by an open neighbourhood in $\mathbb{C}$. The set of points, where this is not possible, we call $\operatorname{Sing} C$, the singularities of C, e.g., think of



$C - \operatorname{Sing} C$ (as an orientable topological manifold) is homeomorphic (i.e. can be transformed continuously) to a manifold with a certain number of holes (also zero holes i.e. a shere)



(minus some points, which correspond to the singularities).

Definition 17 *We call this number of holes the genus $g(C)$ of C.*

Proposition 18 *$g(C)$ is a topological invariant and a birational invariant.*

We will see in a minute, that exactly the curves C with $g(C) = 0$ admit a birational parametrization

$$\varphi = (f_0 : f_1 : f_2) : \mathbb{P}^1(\mathbb{C}) \to C \subset \mathbb{P}^2(\mathbb{C})$$

(with $f_i \in \mathbb{C}[t]$ homogeneous of equal degree). We call these curves **rational**. The above propositon tells us, that any rational curve has $g(C) = 0$.

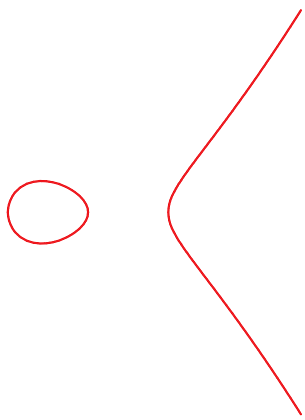
3.2 Smooth plane curves

Theorem 19 *Let $C = V(f) \subset \mathbb{P}^2(\mathbb{C})$, $f \in \mathbb{C}[x, y, z]$, $d = \deg f$ be a smooth curve, then the genus of C is*

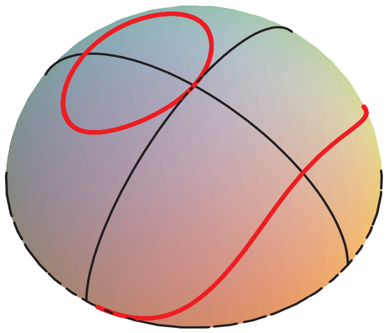
$$g(C) = \frac{(d-1)(d-2)}{2}$$

We check this in the example of the plane cubic:

Example 20 *Consider a nonsingular plane cubic, which after a linear coordinate change is given by $V(x(x+1)(x-\lambda) - y^2) \subset \mathbb{A}^2(\mathbb{C})$. The real picture in $\mathbb{A}^2(\mathbb{R})$ looks like*



In the projective point of view $C = V\left(x\left(x+z\right)\left(x-\lambda z\right)-y^2 z\right) \subset \mathbb{P}^2\left(\mathbb{C}\right)$ *and the real picture in* $\mathbb{P}^2\left(\mathbb{R}\right)$ *is*



Note, that C *is tangent of order* 3 *to the line at infinity. See Maple for the plot.*

Consider the map

$$f : C \longrightarrow \mathbb{P}^1\left(\mathbb{C}\right), \quad \left(x : y : z\right) \mapsto \left(x : z\right)$$

which is $2:1$ *as in affine coordinate* $z = 1$ *for any value* $x \neq 0, -1, \lambda$ *we get* 2 *values for* y*:*

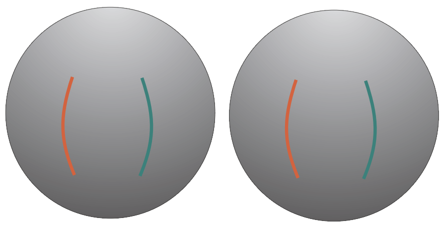
$$y = \pm\sqrt{x\left(x+1\right)\left(x-\lambda\right)}$$

and in affine coordinates $x = 1$ *for any value* $z \neq 0$ *we get* 2 *values for* y*:*

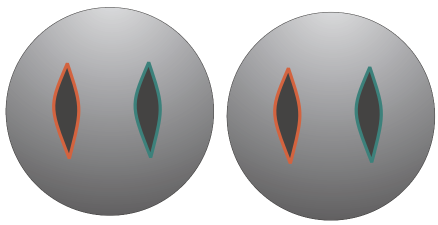
$$y = \pm\sqrt{\left(1+z\right)\left(1-\lambda z\right)\frac{1}{z}}$$

By stereographic projection $\mathbb{P}^1\left(\mathbb{C}\right)$ *is homeomorphic to the* 2 *sphere* $S^2 \subset \mathbb{R}^3$*.*

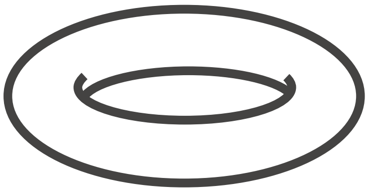
If we cut $\mathbb{P}^1\left(\mathbb{C}\right) \simeq S^2$ *along the paths from* $\left(0:1\right)$ *to* $\left(-1:1\right)$ *and from* $\left(\lambda:1\right)$ *to* $\left(1:0\right)$ *and* C *along the preimages then* C *falls apart into two pieces*



each of them homeomorphic to S^2 *with two openings*

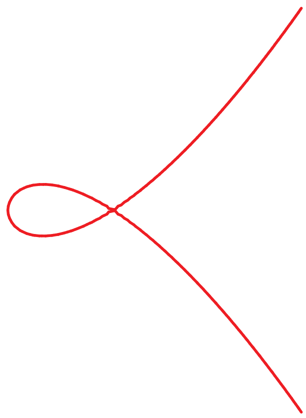


So C is homeomorphic to the union of these two pieces with the red and the green curve identified, hence C is homeomorphic to a torus



i.e. $g(C) = 1 = \frac{2 \cdot 1}{2}$ *as predicted by the above theorem.*

Note that there is one exception: If $\lambda = 0$ then C is singular



the two paths join together and C becomes homeomorphic to S^2, so has $g(C) = 0$.

This naturately raises the question, how to compute the genus of a singular plane curve:

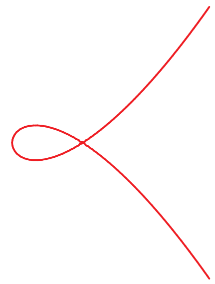
3.3 Singular plane curves and space curves

Another reason, why we should consider singular curves lies in the fact, that projections of smooth space curves with $g(C) = 0$ to the plane happen to be singular (we will soon see why).

Example 21 *Consider the curve $C = image(\varphi)$, $\varphi : \mathbb{A}^1(k) \rightarrow \mathbb{A}^3(k)$, $\varphi(t) = (t, t^2, t^3)$ and the projection $\pi(C)$ given by*

$$\pi : \mathbb{A}^3(k) \rightarrow \mathbb{A}^2(k), \ \pi(x, y, z) = (y, x - z)$$

so $\pi(C) = V(u^3 - 2u^2 + u - v^2)$ *and again looks like:*



See Maple for the twisted cubic projections.
A singular point of this type is called an ordinary double point (or a node).

In general it holds:

Theorem 22 *Any smooth space curve* C' *can be birationally projected to the plane, to give a curve* C *with at most ordinary double points.*

For example a generic projection will do. By considering the inverse of the projection C' has a parametrization, iff C has one.

Given a plane curve we can compute the genus from the number of nodes:

Theorem 23 *Given an irreducible curve* $C = V(f)$, $f \in k[x, y]$, $d = \deg f$ *with* δ *ordinary double points, the genus* $g(C)$ *is*

$$g(C) = \frac{(d-1)(d-2)}{2} - \delta$$

In particular, we note, that the only irreducible nonsingular rational plane curves are the lines and conics.

4 Parametrization of rational curves

So let´s now consider the question of parametrizing plane curves.

Theorem 24 *An irreducible plane curve* $C \subset \mathbb{P}^2(\mathbb{C})$ *is rational, iff* $g(C) = 0$.

The idea of the proof in the case of C having only δ double points is as follows:

Let $I(C) = \langle f \rangle$, $f \in k[x, y, z]$ homogeneous of degree $d = \deg f$ with $g(C) = 0$, so $\delta = \frac{(d-1)(d-2)}{2}$. Consider the projective space of homogeneous polynomials of degree $d-1$ and in there the linear subspace L of those polynomials, which pass through all δ double points and through $2d-3$ further smooth points of C (L is called a linear system, and the common zeroes the base points of L. Note, that if two curves vanish on the base points, then also any linear combination of them vanishes). As passing through a point gives 1 linear condition to these polynomials, we get

$$\dim L \geq \left(\frac{d\,(d+1)}{2} - 1\right) - \delta - (2d-3) = 1$$

Suppose $\dim L \geq 2$ then we have 3 linearly independent homogeneous polynomials $\varphi_0, \varphi_1, \varphi_2$ so for any two points $p, q \in C \backslash V(L)$

$$\begin{pmatrix} \varphi_0(p) & \varphi_1(p) & \varphi_2(p) \\ \varphi_0(q) & \varphi_1(q) & \varphi_2(q) \end{pmatrix} \cdot a = 0$$

has a solution $a \neq 0$ hence $g = a_0\varphi_0 + a_1\varphi_1 + a_2\varphi_2 \neq 0$ and $g(p) = 0$ and $g(q) = 0$, which contradicts the theorem of Bezout saying that g can only have one additional intersection point:

$$d\,(d-1) = (2 \cdot \delta - 1 \cdot (2d-3)) + 1$$

So $\dim L = 1$, i.e. $L = \langle \varphi_0, \varphi_1 \rangle$.

Then

$$\varphi = (\varphi_0 : \varphi_1) : C \to \mathbb{P}^1(\mathbb{C})$$

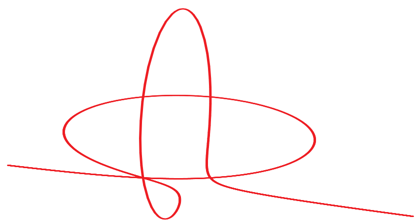
defines a birational map and the inverse is $\psi : \mathbb{P}^1(\mathbb{C}) \to C$ with $\psi(s:t)$ the additional intersection point of C with $V(s\varphi_0 + t\varphi_1)$.

Note, that we could also take linear systems of lower degree, if the dimension count allows this:

Example 25 *$C = V(f) \subset \mathbb{P}^2$ with*

$$\begin{aligned} f &= x^5 + 10x^4y + 20x^3y^2 + 130x^2y^3 - 20xy^4 + 20y^5 \\ &\quad - 2x^4z - 40x^3yz - 150x^2y^2z - 90xy^3z - 40y^4z \\ &\quad + x^3z^2 + 30x^2yz^2 + 110xy^2z^2 + 20y^3z^2 \end{aligned}$$

The affine real picture looks as follows:

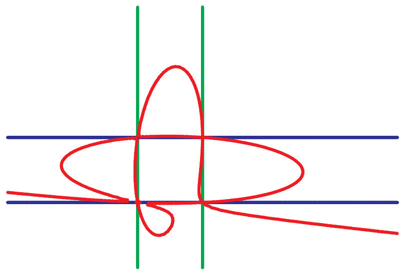


C has 3 double points $(1,0),(0,1),(1,1)$ and 1 triple point $(0,0)$.

Here we consider the linear system of quadrics

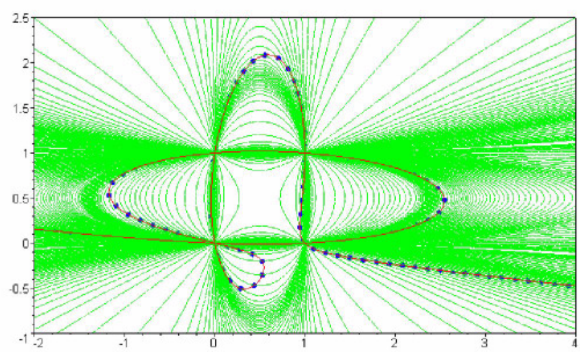
$$L = \langle y^2 - yz, x^2 - xz \rangle$$

through the 4 singularities, which is generated by the two reducible quadrics $y^2 - yz = y(y-z)$ and $x^2 - xz = x(x-z)$



By the theorem of Bezout each member of $L = \langle y^2 - yz, x^2 - xz \rangle$ has one additional intersection point, as

$$5 \cdot 2 = (3 \cdot 1 + 2 \cdot 3) + 1$$



(see Maple for the animation), so the above argument works and we compute the parametrization as follows.

We have to invert the rational map

$$\varphi : C \backslash Z \to \mathbb{P}^1, (x:y:z) \mapsto (y(y-z) : x(x-z))$$

with $Z = V(y(y-z), x(x-z))$ the four base points, where the map is not defined.

We do the computation in the affine setting

$$\begin{aligned} &C_1 = V\left(f\left(x,y,1\right)\right) \subset \mathbb{A}^2 = \mathbb{P}^2 \backslash \left\{(x:y:0) \mid (x:y) \in \mathbb{P}^1\right\} \\ &\mathbb{A}^1 = \mathbb{P}^1 \backslash \left(1:0\right) \end{aligned}$$

where we already know, how to do this. Here φ *is given by*

$$\begin{aligned} \varphi_1 : C_1 \backslash Z_1 &\to \mathbb{A}^1 \\ (x,y) &\mapsto \frac{y\left(y-1\right)}{x\left(x-1\right)} \end{aligned}$$

with $Z_1 = V\left(y\left(y-1\right), x\left(x-1\right)\right)$ *and the ideal of the graph can be computed as*

$$I = \langle f\left(x,y,1\right), t \cdot x\left(x-1\right) - y\left(y-1\right), 1 - x\left(x-1\right)y\left(y-1\right)a\rangle \subset k\left[a,t,x,y\right]$$

where we added the helper variable a *and helper equation*

$$x\left(x-1\right)y\left(y-1\right)a = 1$$

to remove solutions (x,y,t) *lying over the base points* Z_1 *(where* φ_1 *is not defined).*

Computing a lex Groebner basis G *of*

$$I = \langle f\left(x,y,1\right), t \cdot x\left(x-1\right) - y\left(y-1\right), 1 - x\left(x-1\right)y\left(y-1\right)a\rangle \subset k\left[a,t,x,y\right]$$

with $a > t > x > y$ *we observe two things:*

1. $G \cap k\left[t\right] = \langle 0\rangle$ *so* $\overline{image\left(\varphi_1\right)} = \mathbb{A}^1$.
2. G *contains two equations linear in* x *and* y

$$\begin{aligned} \left(t^2 - t - \frac{1}{20}\right)x - \left(t^2 - \frac{13}{2}t - \frac{1}{2}\right)y = 0 \\ \left(\frac{161}{20}t + \frac{3}{8}\right)x + t^3y + 13t^2y + \frac{201}{4}ty + \frac{19}{5}y - t^3 - \frac{11}{2}t^2 - \frac{3}{2}t - \frac{1}{20} = 0 \end{aligned}$$

which we can solve for (x,y) *and get the parametrization*

$$\begin{aligned} x\left(t\right) &= \frac{t^5 + 12t^4 + \frac{151}{4}t^3 + \frac{251}{20}t^2 + \frac{43}{40}t + \frac{1}{40}}{t^5 + 12t^4 + \frac{181}{4}t^3 + \frac{28}{5}t^2 + \frac{3}{20}t - \frac{1}{400}} \\ y\left(t\right) &= \frac{t^5 + \frac{9}{2}t^4 - \frac{81}{20}t^3 - \frac{69}{40}t^2 - \frac{1}{8}t - \frac{1}{400}}{t^5 + 12t^4 + \frac{181}{4}t^3 + \frac{28}{5}t^2 + \frac{3}{20}t - \frac{1}{400}} \end{aligned}$$

In practice, if we are given a rational curve $C \subset \mathbb{P}^2(\mathbb{C})$ by an homogeneous equation $f \in \mathbb{Q}[x, y, z]$, we would like to have a parametrization of C by rational functions with coefficients in $\mathbb{Q}$. To use the proof of the theorem we could try to find points of C over $\mathbb{Q}$, which is nontrivial and not always possible. A solution to this problem is given by:

Theorem 26 *For an irreducible plane curve $C \subset \mathbb{P}^2\left(\overline{k}\right)$, $I(C) = \langle f \rangle$, $f \in k[x, y, z]$ with $g(C) = 0$ it holds:*

1. *If $\deg f$ is odd, then there is a birational map $\mathbb{P}^1\left(\overline{k}\right) \rightarrow C$ with coefficients in k.*

2. *If $\deg f$ is even, then there is a birational map $C_2 \rightarrow C$ with coefficients in k, where $C_2 = V(g) \subset \mathbb{P}^2\left(\overline{k}\right)$, $g \in k[x, y, z]$ is a plane conic. To parametrize C_2 we need a field extension of degree 2, iff C_2 does not contain a point over k.*

These maps can be computed algorithmically.

References

[1] Cox, Little, O´Shea: Ideals, Varieties, and Algorithms. UTM, Springer (1996).

[2] Decker, Schreyer: Varieties, Groebner Bases, and Algebraic Curves. Manuscript.

[3] Schenck: Computational Algebraic Geometry. LMSST 58, Cambridge University Press (2003).