

Rational Parametrization

Summary. Chapter 4 is the central chapter of the book. In this chapter, we focus on rational or parametric curves, we study different problems related to this type of curves and we show how to algorithmically parametrize a rational curve. The chapter consists of three conceptual blocks. The first one (Sect. 4.1) is devoted to the notion of rational parametrization of a curve, and to the study of the class of rational curves, i.e., curves having a rational parametrization. In the second block of the chapter (Sects. 4.2–4.5), we assume that a rational parametrization of a curve is provided and we consider various problems related to such a rational parametrization. The material in this part of the chapter follows the ideas in [SeW01a]. In Sect. 4.2 the injectivity of the parametrization is studied, in Sect. 4.3 we analyze the number of times the points on the curve are traced via the parametrization, in Sect. 4.4 the inversion problem for proper parametrizations is studied, and in Sect. 4.5 the implicitization question is addressed. The third block of the chapter (Sects. 4.6–4.8) deals with the problem of algorithmically deciding whether a given curve is rational, and in the affirmative case, of actually computing a rational parametrization of the curve. The material in this part of the chapter follows the ideas in [SeW91], which are based on [AbB87a, AbB87b, AbB88, AbB89]. In Sect. 4.6 we study the simple case of curves parametrizable by lines, in Sect. 4.7 these ideas are extended to the general case, and in Sect. 4.8, once the theoretical and algorithmic ideas have been developed, we show how to carry out all these algorithms symbolically.

Alternatively, a parametrization algorithm can be constructed from methods in [VaH94]. Also, the reader interested in the parametrization problem for surfaces may see [Sch98a].

Throughout this chapter, unless explicitly stated otherwise, we use the following notation. K is an algebraically closed field of characteristic 0. We consider either affine or projective plane algebraic curves. In addition, if \mathcal{C} is

an affine rational curve, and $\mathcal{P}(t)$ is a rational affine parametrization of \mathcal{C} over K (see Definition 4.1), we write its components either as

$$\mathcal{P}(t) = \left(\frac{\chi_{11}(t)}{\chi_{12}(t)}, \frac{\chi_{21}(t)}{\chi_{22}(t)} \right),$$

where $\chi_{ij}(t) \in K[t]$ and $\gcd(\chi_{1i}, \chi_{2i}) = 1$, or as

$$\mathcal{P}(t) = (\chi_1(t), \chi_2(t)),$$

where $\chi_i(t) \in K(t)$. Similarly, rational projective parametrizations (see Definition 4.2) are expressed as

$$\mathcal{P}(t) = (\chi_1(t), \chi_2(t), \chi_3(t)),$$

where $\chi_i(t) \in K[t]$ and $\gcd(\chi_1, \chi_2, \chi_3) = 1$.

Furthermore, associated with a given parametrization $\mathcal{P}(t)$ we consider the polynomials

$$G_1^{\mathcal{P}}(s, t) = \chi_{11}(s)\chi_{12}(t) - \chi_{12}(s)\chi_{11}(t), \quad G_2^{\mathcal{P}}(s, t) = \chi_{21}(s)\chi_{22}(t) - \chi_{22}(s)\chi_{21}(t)$$

as well as the polynomials

$$H_1^{\mathcal{P}}(t, x) = x \cdot \chi_{12}(t) - \chi_{11}(t), \quad H_2^{\mathcal{P}}(t, y) = y \cdot \chi_{22}(t) - \chi_{21}(t).$$

The polynomials $G_i^{\mathcal{P}}$ will play an important role in Sect. 4.3 in deciding whether a parametrization $\mathcal{P}(t)$ is proper by means of the tracing index; i.e., in studying whether the parametrization is injective for almost all parameter values. The polynomials $H_i^{\mathcal{P}}$ will be used in Sect. 4.5 for the implicitization problem.

4.1 Rational Curves and Parametrizations

Some plane algebraic curves can be expressed by means of rational parametrizations, i.e., pairs of univariate rational functions that, except for finitely many exceptions, represent all the points on the curve. For instance, the parabola $y = x^2$ can also be described as the set $\{(t, t^2) \mid t \in \mathbb{C}\}$; in this case, all affine points on the parabola are given by the parametrization (t, t^2) . Also, the tacnode curve (see Exercise 2.9 and Fig. 4.1) defined in $\mathbb{A}^2(\mathbb{C})$ by the polynomial

$$f(x, y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$$

can be represented, for instance, as

$$\left\{ \left(\frac{t^3 - 6t^2 + 9t - 2}{2t^4 - 16t^3 + 40t^2 - 32t + 9}, \frac{t^2 - 4t + 4}{2t^4 - 16t^3 + 40t^2 - 32t + 9} \right) \mid t \in \mathbb{C} \right\}.$$

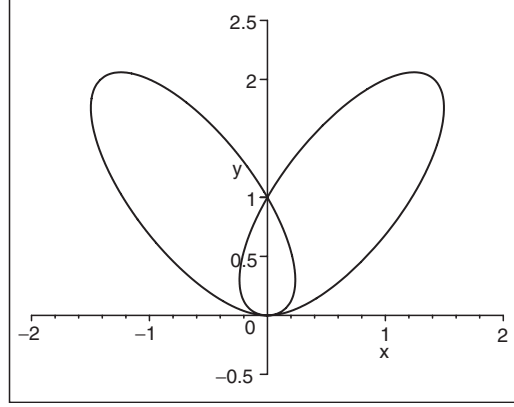


Fig. 4.1. Tacnode curve

In this case, all points on the tacnode are reachable by this pair of rational functions with the exception of the origin.

However, not all plane algebraic curves can be rationally parametrized, as we will see in Example 4.3. In this section, we introduce the notion of rational or parametrizable curves and in this whole chapter we study the main properties and characterizations of this type of curves. In fact, we will see that the rationality of curves can be characterized by means of the genus, and therefore the algorithmic methods described in Chap. 3 will be used.

Definition 4.1. *The affine curve \mathcal{C} in $\mathbb{A}^2(K)$ defined by the square-free polynomial $f(x, y)$ is rational (or parametrizable) if there are rational functions $\chi_1(t), \chi_2(t) \in K(t)$ such that*

- (1) *for almost all $t_0 \in K$ (i.e. for all but a finite number of exceptions) the point $(\chi_1(t_0), \chi_2(t_0))$ is on \mathcal{C} , and*
- (2) *for almost every point $(x_0, y_0) \in \mathcal{C}$ there is a $t_0 \in K$ such that $(x_0, y_0) = (\chi_1(t_0), \chi_2(t_0))$.*

In this case $(\chi_1(t), \chi_2(t))$ is called an affine rational parametrization of \mathcal{C} .

We say that $(\chi_1(t), \chi_2(t))$ is in reduced form if the rational functions $\chi_1(t)$, and $\chi_2(t)$ are in reduced form; i.e., if for $i = 1, 2$ the gcd of the numerator and the denominator of χ_i is trivial.

Definition 4.2. *The projective curve \mathcal{C} in $\mathbb{P}^2(K)$ defined by the square-free homogeneous polynomial $F(x, y, z)$ is rational (or parametrizable) if there are polynomials $\chi_1(t), \chi_2(t), \chi_3(t) \in K[t]$, $\gcd(\chi_1, \chi_2, \chi_3) = 1$, such that*

- (1) *for almost all $t_0 \in K$ the point $(\chi_1(t_0) : \chi_2(t_0) : \chi_3(t_0))$ is on \mathcal{C} , and*
- (2) *for almost every point $(x_0 : y_0 : z_0) \in \mathcal{C}$ there is a $t_0 \in K$ such that $(x_0 : y_0 : z_0) = (\chi_1(t_0) : \chi_2(t_0) : \chi_3(t_0))$.*

In this case, $(\chi_1(t), \chi_2(t), \chi_3(t))$ is called a projective rational parametrization of \mathcal{C} .

- Remarks.** (1) By abuse of notation, we will sometimes refer to a projective parametrization as a triple of rational functions. Of course, we could always clear denominators and generate a polynomial projective parametrization.
- (2) In Sect. 2.5 we have introduced the notion of local parametrization of a curve over K , not necessarily rational. Rational parametrizations are also called *global parametrizations*, and can only be achieved for curves of genus 0 (see Theorem 4.11). On the other hand, since $K(t) \subset K((t))$, it is clear that any global parametrization is a local parametrization. Consider the global rational parametrization $\mathcal{P} = (\chi_1, \chi_2)$. W.l.o.g. (perhaps after a linear change of parameter) we may assume that $t = 0$ is not a root of the denominators. By interpreting the numerators and denominators of a global parametrization as formal power series, and inverting the denominators, we get exactly a local parametrization $\chi_1 = A(t), \chi_2 = B(t)$ with center $(\chi_1(0), \chi_2(0))$, as introduced in Sect. 2.5.
- (3) The notion of rational parametrization can be stated by means of rational maps. More precisely, let \mathcal{C} be a rational affine curve and $\mathcal{P}(t) \in K(t)^2$ a rational parametrization of \mathcal{C} . By Definition 4.1, the parametrization $\mathcal{P}(t)$ induces the rational map

$$\begin{aligned} \mathcal{P} : \mathbb{A}^1(K) &\longrightarrow \mathcal{C} \\ t &\longmapsto \mathcal{P}(t), \end{aligned}$$

and $\mathcal{P}(\mathbb{A}^1(K))$ is a dense (in the Zariski topology) subset of \mathcal{C} . Sometimes, by abuse of notation, we also call this rational map a rational parametrization of \mathcal{C} .

- (4) Every rational parametrization $\mathcal{P}(t)$ defines a monomorphism from the field of rational functions $K(\mathcal{C})$ to $K(t)$ as follows (see proof of Theorem 4.9):

$$\begin{aligned} \varphi : K(\mathcal{C}) &\longrightarrow K(t) \\ R(x, y) &\longmapsto R(\mathcal{P}(t)). \end{aligned} \quad \square$$

Example 4.3. An example of an irreducible curve which is not rational is the projective cubic \mathcal{C} , defined over \mathbb{C} , by $x^3 + y^3 = z^3$. Suppose that \mathcal{C} is rational, and let $(\chi_1(t), \chi_2(t), \chi_3(t))$ be a projective parametrization of \mathcal{C} . Observe that not all components of the parametrization can be constant. Then

$$\chi_1^3 + \chi_2^3 - \chi_3^3 = 0.$$

Differentiating this equation w.r.t. t we get

$$3 \cdot (\chi_1' \chi_1^2 + \chi_2' \chi_2^2 - \chi_3' \chi_3^2) = 0.$$

W.l.o.g. assume that χ_2 is not constant, so $\chi_2 \neq 0$ and $\chi'_2 \neq 0$. $\chi_1^2, \chi_2^2, \chi_3^2$ are a solution of the system of homogeneous linear equations with coefficient matrix

$$\begin{pmatrix} \chi_1 & \chi_2 & -\chi_3 \\ \chi'_1 & \chi'_2 & -\chi'_3 \end{pmatrix}.$$

By fundamental line operations we reduce this coefficient matrix to

$$\begin{pmatrix} \chi_2\chi'_1 - \chi'_2\chi_1 & 0 & \chi'_2\chi_3 - \chi_2\chi'_3 \\ 0 & \chi_2\chi'_1 - \chi'_2\chi_1 & \chi'_3\chi_1 - \chi_3\chi'_1 \end{pmatrix}.$$

So

$$(\chi_1^2 : \chi_2^2 : \chi_3^2) = (\chi_2\chi'_3 - \chi_3\chi'_2 : \chi_3\chi'_1 - \chi_1\chi'_3 : \chi_1\chi'_2 - \chi_2\chi'_1).$$

Since χ_1, χ_2, χ_3 are relatively prime, this proportionality implies

$$\chi_1^2 \mid (\chi_2\chi'_3 - \chi_3\chi'_2), \quad \chi_2^2 \mid (\chi_3\chi'_1 - \chi_1\chi'_3), \quad \chi_3^2 \mid (\chi_1\chi'_2 - \chi_2\chi'_1).$$

Suppose $\deg(\chi_1) \geq \deg(\chi_2), \deg(\chi_3)$. Then, we get that the first divisibility implies $2\deg(\chi_1) \leq \deg(\chi_2) + \deg(\chi_3) - 1$, a contradiction. Similarly, we see that $\deg(\chi_2) \geq \deg(\chi_1), \deg(\chi_3)$ and $\deg(\chi_3) \geq \deg(\chi_1), \deg(\chi_2)$ are impossible. Thus, there can be no parametrization of \mathcal{C} .

Definitions 4.1 and 4.2 are stated for general affine and projective curves, respectively. However, in the next theorem we show that only irreducible curves can be parametrizable.

Theorem 4.4. *Any rational curve is irreducible.*

Proof. We prove this for affine curves, the proof for projective curves is similar and is left to the reader. Let \mathcal{C} be a rational affine curve parametrized by a rational parametrization $\mathcal{P}(t)$. First observe that the ideal of \mathcal{C} consists of the polynomials vanishing at $\mathcal{P}(t)$, i.e.,

$$I(\mathcal{C}) = \{h \in K[x, y] \mid h(\mathcal{P}(t)) = 0\}.$$

Indeed, if $h \in I(\mathcal{C})$ then $h(P) = 0$ for all $P \in \mathcal{C}$. In particular h vanishes on all points of \mathcal{C} generated by the parametrization, and hence $h(\mathcal{P}(t)) = 0$. Conversely, let $h \in K[x, y]$ be such that $h(\mathcal{P}(t)) = 0$. Therefore, h vanishes on all points of the curve generated by $\mathcal{P}(t)$, i.e., on all points of \mathcal{C} with finitely many exceptions. So, since \mathcal{C} is the Zariski closure of the image of \mathcal{P} , it vanishes on \mathcal{C} , i.e., $h \in I(\mathcal{C})$ (see Appendix B).

Finally, in order to prove that \mathcal{C} is irreducible, we prove that $I(\mathcal{C})$ is prime (see Appendix B). Let $h_1 \cdot h_2 \in I(\mathcal{C})$. Then $h_1(\mathcal{P}(t)) \cdot h_2(\mathcal{P}(t)) = 0$. Thus, either $h_1(\mathcal{P}(t)) = 0$ or $h_2(\mathcal{P}(t)) = 0$. Therefore, either $h_1 \in I(\mathcal{C})$ or $h_2 \in I(\mathcal{C})$. \square

The rationality of a curve does not depend on its embedding into an affine or projective plane. So, in the sequel, we may choose freely between projective and affine situations, whatever we find more convenient.

Lemma 4.5. *Let \mathcal{C} be an irreducible affine curve and \mathcal{C}^* its corresponding projective curve. Then \mathcal{C} is rational if and only if \mathcal{C}^* is rational. Furthermore, a parametrization of \mathcal{C} can be computed from a parametrization of \mathcal{C}^* and vice versa.*

Proof. Let

$$(\chi_1(t), \chi_2(t), \chi_3(t))$$

be a parametrization of \mathcal{C}^* . Observe that $\chi_3(t) \neq 0$, since the curve \mathcal{C}^* can have only finitely many points at infinity. Hence,

$$\left(\frac{\chi_1(t)}{\chi_3(t)}, \frac{\chi_2(t)}{\chi_3(t)} \right)$$

is a parametrization of the affine curve \mathcal{C} .

Conversely, a rational parametrization of \mathcal{C} can always be extended to a parametrization of \mathcal{C}^* by normalizing the z -coordinate to 1 and clearing denominators. \square

Definition 4.1 clearly implies that associated with any rational plane curve there is a pair of univariate rational functions over K , not both simultaneously constant, which is a parametrization of the curve. The converse is also true. That is, associated with any pair of univariate rational functions over K , not both simultaneously constant, there is a rational plane curve \mathcal{C} such that the image of the parametrization is dense in \mathcal{C} . The implicit equation of this curve \mathcal{C} is directly related to a resultant. In the following lemma we state this property. Later, in Sect. 4.5, we give a geometric interpretation to the integer r that appears in Lemma 4.6, proving that it counts the number of times the curve is traced when one gives values to the parameter of the parametrization.

Lemma 4.6. *Let \mathcal{C} be an affine rational curve over K , $f(x, y)$ its the defining polynomial, and*

$$\mathcal{P}(t) = (\chi_1(t), \chi_2(t))$$

a rational parametrization of \mathcal{C} . Then, there exists $r \in \mathbb{N}$ such that

$$\text{res}_t(H_1^{\mathcal{P}}(t, x), H_2^{\mathcal{P}}(t, y)) = (f(x, y))^r.$$

Proof. Let $\chi_i(t) = \frac{\chi_{i1}(t)}{\chi_{i2}(t)}$, and let

$$h(x, y) = \text{res}_t(H_1^{\mathcal{P}}(t, x), H_2^{\mathcal{P}}(t, y)).$$

First we observe that $H_1^{\mathcal{P}}$ and $H_2^{\mathcal{P}}$ are irreducible, because $\chi_1(t)$ and $\chi_2(t)$ are in reduced form. Hence $H_1^{\mathcal{P}}$ and $H_2^{\mathcal{P}}$ do not have common factors. Therefore, $h(x, y)$ is not the zero polynomial. Furthermore, h cannot be a constant

polynomial either. Indeed: let $t_0 \in K$ be such that $\chi_{12}(t_0)\chi_{22}(t_0) \neq 0$. Then $H_1^{\mathcal{P}}(t_0, \mathcal{P}(t_0)) = H_2^{\mathcal{P}}(t_0, \mathcal{P}(t_0)) = 0$. So $h(\mathcal{P}(t_0)) = 0$, and since h is not the zero polynomial it cannot be constant.

Now, we consider the square-free part $h'(x, y)$ of $h(x, y)$ and the plane curve \mathcal{C} defined by $h'(x, y)$ over K . Let us see that $\mathcal{P}(t)$ parametrizes \mathcal{C} . For this purpose, we check the conditions introduced in Definition 4.1.

1. Let $t_0 \in K$ be such that $\chi_{12}(t_0)\chi_{22}(t_0) \neq 0$. Reasoning as above, we see that $h(\mathcal{P}(t_0)) = 0$. So $h'(\mathcal{P}(t_0)) = 0$, and hence $\mathcal{P}(t_0)$ is on \mathcal{C} .
2. Let c_1, c_2 be the leading coefficients of $H_1^{\mathcal{P}}, H_2^{\mathcal{P}}$ w.r.t. t , respectively. Note that $c_1 \in K[x], c_2 \in K[y]$ are of degree at most 1. For every (x_0, y_0) on \mathcal{C} such that $c_1(x_0) \neq 0$ or $c_2(y_0) \neq 0$ (note that there is at most one point in K^2 where c_1 and c_2 vanish simultaneously), we have $h(x_0, y_0) = 0$. Thus, since h is a resultant, there exists $t_0 \in K$ such that $H_1^{\mathcal{P}}(t_0, x_0) = H_2^{\mathcal{P}}(t_0, y_0) = 0$. Also, observe that $\chi_{12}(t_0) \neq 0$ since otherwise the first component of the parametrization would not be in reduced form. Similarly, $\chi_{22}(t_0) \neq 0$. Thus, $(x_0, y_0) = \mathcal{P}(t_0)$. Therefore, almost all points on \mathcal{C} are generated by $\mathcal{P}(t)$.

Now by Theorem 4.4 it follows that $h'(x, y)$ is irreducible. Therefore, there exists $r \in \mathbb{N}$ such that $h(x, y) = (h'(x, y))^r$. \square

Sometimes it is useful to apply equivalent characterizations of the concept of rationality. In Theorems 4.7, 4.9, 4.10, and 4.11 some such equivalent characterizations are established.

Theorem 4.7. *An irreducible curve \mathcal{C} , defined by $f(x, y)$, is rational if and only if there exist rational functions $\chi_1(t), \chi_2(t) \in K(t)$, not both constant, such that $f(\chi_1(t), \chi_2(t)) = 0$. In this case, $(\chi_1(t), \chi_2(t))$ is a rational parametrization of \mathcal{C} .*

Proof. Let \mathcal{C} be rational. So there exist rational functions $\chi_1, \chi_2 \in K(t)$ satisfying conditions (1) and (2) in Definition 4.1. Obviously not both rational functions χ_i are constant, and clearly $f(\chi_1(t), \chi_2(t)) = 0$.

Conversely, let $\chi_1, \chi_2 \in K(t)$, not both constant, be such that $f(\chi_1(t), \chi_2(t))$ is identically zero. Let \mathcal{D} be the irreducible plane curve defined by $(\chi_1(t), \chi_2(t))$ (see Lemma 4.6). Then \mathcal{C} and \mathcal{D} are both irreducible, because of Theorem 4.4, and have infinitely many points in common. Thus, by Bézout's Theorem (Theorem 2.48) one concludes that $\mathcal{C} = \mathcal{D}$. Hence, $(\chi_1(t), \chi_2(t))$ is a parametrization of \mathcal{C} . \square

An alternative characterization of rationality in terms of field theory is given in Theorem 4.9. This theorem can be seen as the geometric version of Lüroth's Theorem. Lüroth's Theorem appears in basic text books on algebra such as [Jac74], [Jac80], or [VaW70]. Here we do not give a proof of this result.

Theorem 4.8 (Lüroth's Theorem). *Let \mathbb{L} be a field (not necessarily algebraically closed), t a transcendental element over \mathbb{L} . If \mathbb{K} is a subfield of $\mathbb{L}(t)$ strictly containing \mathbb{L} , then \mathbb{K} is \mathbb{L} -isomorphic to $\mathbb{L}(t)$.*

Theorem 4.9. *An irreducible affine curve \mathcal{C} is rational if and only if the field of rational functions on \mathcal{C} , i.e. $K(\mathcal{C})$, is isomorphic to $K(t)$ (t a transcendental element).*

Proof. Let $f(x, y)$ be the defining polynomial of \mathcal{C} , and let $\mathcal{P}(t)$ be a parametrization of \mathcal{C} . We consider the map

$$\begin{aligned}\varphi_{\mathcal{P}} : K(\mathcal{C}) &\longrightarrow K(t) \\ R(x, y) &\longmapsto R(\mathcal{P}(t)).\end{aligned}$$

First we observe that $\varphi_{\mathcal{P}}$ is well-defined. Let $\frac{p_1}{q_1}, \frac{p_2}{q_2}$, where $p_i, q_i \in K[x, y]$, be two different expressions of the same element in $K(\mathcal{C})$. Then f divides $p_1q_2 - q_1p_2$. In addition, by Theorem 4.7, $f(\mathcal{P}(t))$ is identically zero, and therefore $p_1(\mathcal{P}(t))q_2(\mathcal{P}(t)) - q_1(\mathcal{P}(t))p_2(\mathcal{P}(t))$ is also identically zero. Furthermore, since $q_1 \neq 0$ in $K(\mathcal{C})$, we have $q_1(\mathcal{P}(t)) \neq 0$. Similarly $q_2(\mathcal{P}(t)) \neq 0$. Therefore, $\varphi_{\mathcal{P}}(\frac{p_1}{q_1}) = \varphi_{\mathcal{P}}(\frac{p_2}{q_2})$.

Now, since $\varphi_{\mathcal{P}}$ is not the zero homomorphism, the map $\varphi_{\mathcal{P}}$ defines an isomorphism of $K(\mathcal{C})$ onto a subfield of $K(t)$ that properly contains K . Thus, by Lüroth's Theorem, this subfield, and $K(\mathcal{C})$ itself, must be isomorphic to $K(t)$.

Conversely, let $\psi : K(\mathcal{C}) \rightarrow K(t)$ be an isomorphism and $\chi_1(t) = \psi(x), \chi_2(t) = \psi(y)$. Clearly, since the image of ψ is $K(t)$, χ_1 and χ_2 cannot both be constant. Furthermore

$$f(\chi_1(t), \chi_2(t)) = f(\psi(x), \psi(y)) = \psi(f(x, y)) = 0.$$

Hence, by Theorem 4.7, the pair $(\chi_1(t), \chi_2(t))$ is a rational parametrization of \mathcal{C} . \square

Remarks. From the proof of Theorem 4.9 we see that every parametrization $\mathcal{P}(t)$ induces a monomorphism $\varphi_{\mathcal{P}}$ from $K(\mathcal{C})$ to $K(t)$. We will refer to $\varphi_{\mathcal{P}}$ as the *monomorphism induced by $\mathcal{P}(t)$* .

In the following theorem we see how rationality can also be established by means of rational maps.

Theorem 4.10. *An affine algebraic curve \mathcal{C} is rational if and only if it is birationally equivalent to K (i.e., the affine line $\mathbb{A}^1(K)$).*

Proof. By Theorem 2.38 one has that \mathcal{C} is birationally equivalent to K if and only if $K(\mathcal{C})$ is isomorphic to $K(t)$. Thus, by Theorem 4.9 we get the desired result. \square

The following theorem states that only curves of genus 0 can be rational. In fact, all irreducible conics are rational, and an irreducible cubic is rational if and only if it has a double point.

Theorem 4.11. *If an algebraic curve \mathcal{C} is rational then $\text{genus}(\mathcal{C}) = 0$.*

Proof. By the remark after Definition 3.4 the genus is invariant under birational maps. Hence the result follows from Theorem 4.10. \square

In Sect. 4.7 (see Theorem 4.63) we will demonstrate that also the converse is true, namely that every curve of genus 0 is rational.

4.2 Proper Parametrizations

Although the implicit representation for a plane curve is unique, up to multiplication by nonzero constants, there exist infinitely many different parametrizations of the same rational curve. For instance, for every $i \in \mathbb{N}$, (t^i, t^{2i}) parametrizes the parabola $y = x^2$. Obviously (t, t^2) is the parametrization of lowest degree in this family and it generates every point on the parabola only once. Such parametrizations are called proper parametrizations (see Definition 4.12).

The parametrization algorithms presented in this book always output proper parametrizations. Furthermore, there are algorithms for determining whether a given parametrization of a plane curve is proper, and if that is not the case, for transforming it to a proper one. In Sect. 6.1 we will describe these methods.

In this section, we introduce the notion of proper parametrization and we study some of their main properties. For this purpose, in the following we assume that \mathcal{C} is an affine rational plane curve, and $\mathcal{P}(t)$ is an affine rational parametrization of \mathcal{C} .

Definition 4.12. *An affine parametrization $\mathcal{P}(t)$ of a rational curve \mathcal{C} is proper if the map*

$$\begin{array}{ccc} \mathcal{P} : \mathbb{A}^1(K) & \longrightarrow & \mathcal{C} \\ t & \longmapsto & \mathcal{P}(t) \end{array}$$

is birational, or equivalently, if almost every point on \mathcal{C} is generated by exactly one value of the parameter t .

We define the inversion of a proper parametrization $\mathcal{P}(t)$ as the inverse rational mapping of \mathcal{P} , and we denote it by \mathcal{P}^{-1} .

Lemma 4.13. *Every rational curve can be properly parametrized.*

Proof. From Theorem 4.10 one deduces that every rational curve \mathcal{C} is birationally equivalent to $\mathbb{A}^1(K)$. Therefore, every rational curve can be properly parametrized. \square

The notion of properness can also be stated algebraically in terms of fields of rational functions. From Theorem 2.38 we deduce that a rational

parametrization $\mathcal{P}(t)$ is proper if and only if the induced monomorphism $\varphi_{\mathcal{P}}$ (see Remark to Theorem 4.9)

$$\begin{aligned}\varphi_{\mathcal{P}} : K(\mathcal{C}) &\longrightarrow K(t) \\ R(x, y) &\longmapsto R(\mathcal{P}(t)).\end{aligned}$$

is an isomorphism. Therefore, $\mathcal{P}(t)$ is proper if and only if the mapping $\varphi_{\mathcal{P}}$ is surjective, that is, if and only if $\varphi_{\mathcal{P}}(K(\mathcal{C})) = K(\mathcal{P}(t)) = K(t)$. More precisely, we have the following theorem.

Theorem 4.14. *Let $\mathcal{P}(t)$ be a rational parametrization of a plane curve \mathcal{C} . Then, the following statements are equivalent:*

- (1) $\mathcal{P}(t)$ is proper.
- (2) The monomorphism $\varphi_{\mathcal{P}}$ induced by \mathcal{P} is an isomorphism.
- (3) $K(\mathcal{P}(t)) = K(t)$.

Remarks. We have introduced the notion of properness for affine parametrizations. For projective parametrizations the notion of properness can be introduced in a similar way by requiring the rational map, associated with the projective parametrization, to be birational. Moreover, if \mathcal{C} is an irreducible affine curve and \mathcal{C}^* is its projective closure, then $K(\mathcal{C}) = K(\mathcal{C}^*)$. Thus, taking into account Theorem 4.14 one has that the properness of affine and projective parametrizations are equivalent.

Now, we characterize proper parametrizations by means of the degree of the corresponding rational curve. To state this result, we first introduce the notion of degree of a parametrization.

Definition 4.15. *Let $\chi(t) \in K(t)$ be a rational function in reduced form. If $\chi(t)$ is not zero, the degree of $\chi(t)$ is the maximum of the degrees of the numerator and denominator of $\chi(t)$. If $\chi(t)$ is zero, we define its degree to be -1 . We denote the degree of $\chi(t)$ as $\deg(\chi(t))$. Rational functions of degree 1 are called linear.*

Obviously the degree is multiplicative with respect to the composition of rational functions. Furthermore, invertible rational functions are exactly the linear rational functions (see Exercise 4.1).

Definition 4.16. *We define the degree of an affine rational parametrization $\mathcal{P}(t) = (\chi_1(t), \chi_2(t))$ as the maximum of the degrees of its rational components; i.e.*

$$\deg(\mathcal{P}(t)) = \max \{ \deg(\chi_1(t)), \deg(\chi_2(t)) \}.$$

We start this study with a lemma that shows how proper and improper parametrizations of an affine plane curve are related.

Lemma 4.17. *Let $\mathcal{P}(t)$ be a proper parametrization of an affine rational curve \mathcal{C} , and let $\mathcal{P}'(t)$ be any other rational parametrization of \mathcal{C} .*

- (1) *There exists a nonconstant rational function $R(t) \in K(t)$ such that $\mathcal{P}'(t) = \mathcal{P}(R(t))$.*
(2) *$\mathcal{P}'(t)$ is proper if and only if there exists a linear rational function $L(t) \in K(t)$ such that $\mathcal{P}'(t) = \mathcal{P}(L(t))$.*

Proof. (1) We consider the following diagram:

$$\begin{array}{ccc}
 \mathbb{A}^1(K) & \xrightarrow{\mathcal{P}} & \mathcal{C} \subset \mathbb{A}^2(K) \\
 & \nwarrow \mathcal{P}^{-1} \circ \mathcal{P}' & \uparrow \mathcal{P}' \\
 & & \mathbb{A}^1(K)
 \end{array}$$

Then, since \mathcal{P} is a birational mapping, it is clear that $R(t) = \mathcal{P}^{-1}(\mathcal{P}'(t)) \in K(t)$.

(2) If $\mathcal{P}'(t)$ is proper, then from the diagram above we see that $\varphi := \mathcal{P}^{-1} \circ \mathcal{P}'$ is a birational mapping from $\mathbb{A}^1(K)$ onto $\mathbb{A}^1(K)$. Hence, by Theorem 2.38 one has that φ induces an automorphism $\tilde{\varphi}$ of $K(t)$ defined as:

$$\begin{aligned}
 \tilde{\varphi} : K(t) &\longrightarrow K(t) \\
 t &\longmapsto \varphi(t).
 \end{aligned}$$

Therefore, since K -automorphisms of $K(t)$ are the invertible rational functions (see e.g., [VaW70]), we see that $\tilde{\varphi}$ is our linear rational function.

Conversely, let ψ be the birational mapping from $\mathbb{A}^1(K)$ onto $\mathbb{A}^1(K)$ defined by the linear rational function $L(t) \in K(t)$. Then, it is clear that $\mathcal{P}' = \mathcal{P} \circ \psi : \mathbb{A}^1(K) \rightarrow \mathcal{C}$ is a birational mapping, and therefore $\mathcal{P}'(t)$ is proper. \square

Lemma 4.17 seems to suggest that a parametrization of prime degree is proper. But in fact, this is not true, as can easily be seen from the parametrization (t^2, t^2) of a line. Exercise 4.2 asks whether the line is the only curve for which primality of a parametrization does not imply properness.

Proper parametrizations can always be normalized such that in every component of the parametrization the degrees of the numerator and denominator agree. This will be useful later.

Lemma 4.18. *Every rational curve \mathcal{C} has a proper parametrization $\mathcal{P}(t) = (\chi_1(t), \chi_2(t))$ such that if $\chi_i(t)$ is nonzero, then $\deg(\chi_{i1}) = \deg(\chi_{i2})$.*

Proof. By Lemma 4.13 we know that \mathcal{C} has a proper rational parametrization, say $\mathcal{P}'(t)$. Note that if the i -th component of a parametrization is zero, then it is zero for every parametrization. Let us assume w.l.o.g that χ_1 is nonzero.

By Lemma 4.17, any linear reparametrization of a proper parametrization is again proper. If 0 is a root of none of the numerator and denominator of $\chi_1(t)$, then $\mathcal{P}'(\frac{1}{t})$ is still proper and the requirement on the degree is fulfilled. If 0 is a root of any of the numerator or denominator of $\chi_1(t)$, we consider the proper parametrization $\mathcal{P}'(t+a)$, where a is not a root of any of the numerator and denominator. This a always exists since $\chi_1(t)$ is nonzero. Now, observe that the numerator and the denominator of the first component of $\mathcal{P}'(t+a)$ do not vanish at 0. Therefore, we can always reparametrize the initial proper parametrization into a proper one, for which the degree requirement holds. \square

Before we can characterize the properness of a parametrization via the degree of the curve, we first derive the following technical property.

Lemma 4.19. *Let $p(x), q(x) \in K[x]^*$ be relatively prime such that at least one of them is nonconstant. There exist only finitely many values $a \in K$ such that the polynomial $p(x) - aq(x)$ has multiple roots.*

Proof. Let us consider the polynomial $f(x, y) = p(x) - yq(x) \in K[x, y]$. Since $\gcd(p, q) = 1$ and $p(x), q(x)$ are nonzero, the polynomial f is irreducible. Now we study the existence of roots of the discriminant of f w.r.t. y . Let $g(x, y) = \frac{\partial f}{\partial y}$. Note that g is nonzero, since at least one of the two polynomials $p(x)$ and $q(x)$ is not constant. Since $\deg(g) < \deg(f)$ and f is irreducible, we get $\gcd(f, g) = 1$. So $\text{discr}_x(f) \neq 0$. Hence the result follows immediately. \square

Corollary 4.20. *Let $p(x), q(x) \in K[x]^*$ be relatively prime such that at least one of them is nonconstant, and let $R(y)$ be the resultant*

$$R(y) = \text{res}_x(p(x) - yq(x), p'(x) - yq'(x)).$$

Then, for all $b \in K$ such that $R(b) \neq 0$, the polynomial $p(x) - bq(x)$ is squarefree.

The next theorem characterizes the properness of a parametrization by means of the degree of the implicit equation of the curve.

Theorem 4.21. *Let \mathcal{C} be an affine rational curve defined over K with defining polynomial $f(x, y) \in K[x, y]$, and let $\mathcal{P}(t) = (\chi_1(t), \chi_2(t))$ be a parametrization of \mathcal{C} . Then $\mathcal{P}(t)$ is proper if and only if*

$$\deg(\mathcal{P}(t)) = \max\{\deg_x(f), \deg_y(f)\}.$$

Furthermore, if $\mathcal{P}(t)$ is proper and $\chi_1(t)$ is nonzero, then $\deg(\chi_1(t)) = \deg_y(f)$; similarly, if $\chi_2(t)$ is nonzero then $\deg(\chi_2(t)) = \deg_x(f)$.

Proof. First we prove the result for the special case of parametrizations having a constant component; i.e., for horizontal or vertical lines. Afterwards, we consider the general case. Let $\mathcal{P}(t)$ be a parametrization such that one of its

two components is constant, say $\mathcal{P}(t) = (\chi_1(t), \lambda)$ for some $\lambda \in K$. Then the curve \mathcal{C} is the line of equation $y = \lambda$. Hence, by Lemma 4.17 (2) and because (t, λ) parametrizes \mathcal{C} properly, we get that all proper parametrizations of \mathcal{C} are of the form $(\frac{at+b}{ct+d}, \lambda)$, where $a, b, c, d \in K$ and $ad - bc \neq 0$. Therefore, $\deg(\chi_1) = 1$, and the theorem clearly holds.

Now we consider the general case, i.e., \mathcal{C} is not a horizontal or vertical line. Let $\mathcal{P}(t)$ be proper and in reduced form, such that none of its components is constant. Then we prove that $\deg(\chi_2(t)) = \deg_x(f)$, and analogously one can prove that $\deg(\chi_1(t)) = \deg_y(f)$. From these relations we immediately get that $\deg(\mathcal{P}(t)) = \max\{\deg_x(f), \deg_y(f)\}$. Let $\chi_2(t) = \chi_{21}(t)/\chi_{22}(t)$. We define \mathcal{S} as the subset of K containing

- (a) all the second coordinates of those points on \mathcal{C} that are either not generated by $\mathcal{P}(t)$, or more than once by different values of t ,
- (b) those $b \in K$ such that the polynomial $\chi_{21}(t) - b\chi_{22}(t)$ has multiple roots,
- (c) $\text{lc}(\chi_{21})/\text{lc}(\chi_{22})$, where “lc” denotes the leading coefficient,
- (d) those $b \in K$ such that the polynomial $f(x, b)$ has multiple roots,
- (e) the roots of the leading coefficient of $f(x, y)$ w.r.t. x .

We claim that \mathcal{S} is finite. Indeed: Since $\mathcal{P}(t)$ is a proper parametrization, there are only finitely many values satisfying (a). According to Lemma 4.19 there are only finitely many field elements satisfying (b). The argument for (c) is trivial. An element $b \in K$ satisfies (d) if and only if b is the second coordinate of a singular point of \mathcal{C} or the line $y = b$ is tangent to the curve at some simple point (see Theorem 2.50(6)). By Theorem 2.10, \mathcal{C} has only finitely many singular points, and $y = b$ is tangent to \mathcal{C} at some point (a, b) if (a, b) is a solution of the system $\{f = 0, \frac{\partial f}{\partial x} = 0\}$. However, by Bézout’s Theorem (Theorem 2.48), this system has only finitely many solutions. So only finitely many field elements satisfy (d). Since the leading coefficient of $f(x, y)$ w.r.t. x is a nonzero univariate polynomial, only finitely many field elements satisfy (e). Therefore, \mathcal{S} is finite.

Now we take an element $b \in K \setminus \mathcal{S}$ and we consider the intersection of \mathcal{C} and the line of equation $y = b$. Because of condition (e) the degree of $f(x, b)$ is exactly $\deg_x(f(x, y))$, say $m := \deg_x(f(x, y))$. Furthermore, by (d), $f(x, b)$ has m different roots, say $\{r_1, \dots, r_m\}$. So, there are m different points on \mathcal{C} having b as a second coordinate, namely $\{(r_i, b)\}_{i=1, \dots, m}$, and they can be generated by $\mathcal{P}(t)$ because of (a).

On the other hand, we consider the polynomial $M(t) = \chi_{21}(t) - b\chi_{22}(t)$. We note that $\deg_t(M) \geq m$, since every point (r_i, b) is generated by some value of the parameter t . But, since every point $(a, b) \in \mathcal{C}$ is generated exactly once by \mathcal{P} (see condition (a)) and M cannot have multiple roots, we get that $\deg_t(M) = m = \deg_x(f(x, y))$. Now, since b is not the quotient of the leading coefficients of χ_{21} and χ_{22} (because of (c)), we finally see that $\deg_x(f(x, y)) = \deg(M) = \max\{\deg(\chi_{21}), \deg(\chi_{22})\}$.

Conversely, let $\mathcal{P}(t)$ be a parametrization of \mathcal{C} such that $\deg(\mathcal{P}(t)) = \max\{\deg_x(f), \deg_y(f)\}$, and let $\mathcal{P}'(t)$ be any proper parametrization of \mathcal{C} .

Then, by Lemma 4.17(1), there exists $R(t) \in K(t)$ such that $\mathcal{P}'(R(t)) = \mathcal{P}(t)$. $\mathcal{P}'(t)$ is proper, so $\deg(\mathcal{P}'(t)) = \max\{\deg_x(f), \deg_y(f)\} = \deg(\mathcal{P}(t))$. Therefore, since the degree is multiplicative with respect to composition, $R(t)$ must be of degree 1, and hence invertible. Thus, by Lemma 4.17(2), $\mathcal{P}(t)$ is proper. \square

The next corollary follow from Theorem 4.21 and Lemma 4.17(1).

Corollary 4.22. *Let \mathcal{C} be a rational affine plane curve defined by $f(x, y) \in K[x, y]$. Then the degree of any rational parametrization of \mathcal{C} is a multiple of $\max\{\deg_x(f), \deg_y(f)\}$.*

Example 4.23. We consider the rational quintic \mathcal{C} defined by the polynomial $f(x, y) = y^5 + x^2y^3 - 3x^2y^2 + 3x^2y - x^2$. By Theorem 4.21, any proper rational parametrization of \mathcal{C} must have a first component of degree 5, and a second component of degree 2. It is easy to check that

$$\mathcal{P}(t) = \left(\frac{t^5}{t^2 + 1}, \frac{t^2}{t^2 + 1} \right)$$

properly parametrizes \mathcal{C} . Note that $f(\mathcal{P}(t)) = 0$.

For a generalization of the Theorem 4.21 to the surface case see [PDS05].

4.3 Tracing Index

In Sect. 2.2 we have introduced the notion of degree of a dominant rational map between varieties (i.e., irreducible algebraic sets). In this section, we investigate the degree of a special type of rational maps, namely those induced by rational parametrizations of curves. That is, if $\mathcal{P}(t)$ is an affine rational parametrization of \mathcal{C} , we study the degree of the dominant rational map $\mathcal{P} : \mathbb{A}(K) \rightarrow \mathcal{C} : t \mapsto \mathcal{P}(t)$. Later, in Sect. 4.5, we will see that the degree of the rational map induced by the parametrization plays a role in the implicitization problem.

In addition, we will work with the fibres of the map \mathcal{P} . We will denote by $\mathcal{F}_{\mathcal{P}}(P)$ the fibre of a point $P \in \mathcal{C}$; that is

$$\mathcal{F}_{\mathcal{P}}(P) = \mathcal{P}^{-1}(P) = \{t \in K \mid \mathcal{P}(t) = P\}.$$

In Theorem 2.43 we have seen that the degree of a dominant rational map between two varieties of the same dimension is the cardinality of the fiber of a generic element. Therefore, in the case of the mapping \mathcal{P} , this implies that almost all points of \mathcal{C} are generated via $\mathcal{P}(t)$ by the same number of parameter values, and this number is the degree. Thus, intuitively speaking, the degree measures the number of times the parametrization traces the curve when the parameter takes values in K . Taking into account this intuitive meaning of the notion of degree, we will also call the degree of the mapping \mathcal{P} the tracing index of $\mathcal{P}(t)$.

Definition 4.24. Let \mathcal{C} be an affine rational curve, and let $\mathcal{P}(t)$ be a rational parametrization of \mathcal{C} . Then the tracing index of $\mathcal{P}(t)$, denoted by $\text{index}(\mathcal{P}(t))$, is the degree of $\mathcal{P} : \mathbb{A}(K) \rightarrow \mathcal{C}$, $t \mapsto \mathcal{P}(t)$; i.e., $\text{index}(\mathcal{P}(t))$ is a natural number such that almost all points on \mathcal{C} are generated, via $\mathcal{P}(t)$, by exactly $\text{index}(\mathcal{P}(t))$ parameter values.

4.3.1 Computation of the Index of a Parametrization

Theorem 4.25. Let $\mathcal{P}(t)$ be a parametrization in reduced form. Then for almost all $\alpha \in K$ we have

$$\text{card}(\mathcal{F}_{\mathcal{P}}(\mathcal{P}(\alpha))) = \deg_t(\gcd(G_1^{\mathcal{P}}(\alpha, t), G_2^{\mathcal{P}}(\alpha, t))).$$

Proof. Let $\chi_i = \chi_{i1}/\chi_{i2}$, in reduced form, be the i -th component of $\mathcal{P}(t)$. Let S be the set of all $\alpha \in K$ such that either $\mathcal{P}(\alpha)$ is not defined or both polynomials $G_1^{\mathcal{P}}(\alpha, t)$ and $G_2^{\mathcal{P}}(\alpha, t)$ have multiple roots. First, we see that S is a finite set. Indeed: clearly there exist only finitely many values such that $\mathcal{P}(t)$ is not defined. Now, we assume w.l.o.g. that $\chi_1(t)$ is nonconstant. Let α be such that $\chi_{12}(\alpha)\chi_{22}(\alpha) \neq 0$. If $G_1^{\mathcal{P}}(\alpha, t)$ has multiple roots, then $H_1^{\mathcal{P}}(t, \chi_1(\alpha)) = 1/\chi_{12}(\alpha)G_1^{\mathcal{P}}(\alpha, t)$ also has multiple roots. But by Lemma 4.19 this can only happen for finitely many values of α . Therefore, S is finite.

Now, let $\alpha \in K \setminus S$. We observe that every element of the fibre $\mathcal{F}_{\mathcal{P}}(\mathcal{P}(\alpha))$ is a common root of $G_1^{\mathcal{P}}(\alpha, t)$ and $G_2^{\mathcal{P}}(\alpha, t)$. On the other hand, let β be a root of $\gcd(G_1^{\mathcal{P}}(\alpha, t), G_2^{\mathcal{P}}(\alpha, t))$. Note that $\gcd(G_1^{\mathcal{P}}(\alpha, t), G_2^{\mathcal{P}}(\alpha, t))$ is defined since not both components of $\mathcal{P}(t)$ are constant, and therefore at least one of the polynomials $G_i^{\mathcal{P}}(\alpha, t)$ is not zero. Let us assume that χ_1 is not constant. Then $\chi_{12}(\beta) \neq 0$, since otherwise $\chi_{12}(\alpha)\chi_{11}(\beta) = 0$. But $\chi_{12}(\alpha) \neq 0$ and hence $\chi_{11}(\beta) = 0$, which is impossible because $\gcd(\chi_{11}, \chi_{12}) = 1$. Similarly, if χ_2 is not constant, we get that $\chi_{22}(\beta) \neq 0$. Note that if some χ_i is constant the result is obtained trivially. Thus, $\beta \in \mathcal{F}_{\mathcal{P}}(\mathcal{P}(\alpha))$. Therefore, since $G_1^{\mathcal{P}}(\alpha, t)$ and $G_2^{\mathcal{P}}(\alpha, t)$ do not have multiple roots, the cardinality of the fibre is the degree of the gcd. \square

Theorem 4.25 implies that almost all points $(x_\alpha, y_\alpha) = \mathcal{P}(\alpha) \in \mathcal{C}$ are generated more than once if and only if $\deg_t(\gcd(G_1^{\mathcal{P}}(\alpha, t), G_2^{\mathcal{P}}(\alpha, t))) > 1$. In Lemma 4.27 we will see that the degree of this gcd is preserved under almost all specializations of the variable s . First we state the following result on gcds. Let φ_a denote the natural evaluation homomorphism of $K[x, y]$ into $K[y]$, i.e., for $a \in K$,

$$\begin{aligned} \varphi_a : K[x, y] &\longrightarrow K[y] \\ f(x, y) &\longmapsto f(a, y). \end{aligned}$$

Lemma 4.26. Let $f, g \in K[x, y]^*$, $f = \bar{f} \cdot \gcd(f, g)$, $g = \bar{g} \cdot \gcd(f, g)$. Let $a \in K$ be such that not both leading coefficients of f and g w.r.t. y vanish at a .

- (1) $\deg_y(\gcd(\varphi_a(f), \varphi_a(g))) \geq \deg_y(\varphi_a(\gcd(f, g))) = \deg_y(\gcd(f, g))$.
 (2) If the resultant w.r.t. y of \bar{f} and \bar{g} does not vanish at a , then

$$\gcd(\varphi_a(f), \varphi_a(g)) = \varphi_a(\gcd(f, g)).$$

Proof. Let $h = \gcd(f, g)$. Since not both leading coefficients (w.r.t. y) of f and g vanish under φ_a , also the leading coefficient of h cannot vanish under φ_a . So $\deg_y(\varphi_a(h)) = \deg_y(h)$. Furthermore, $\varphi_a(f) = \varphi_a(\bar{f})\varphi_a(h)$ and $\varphi_a(g) = \varphi_a(\bar{g})\varphi_a(h)$.

- (1) $\varphi_a(h)$ divides $\gcd(\varphi_a(f), \varphi_a(g))$, so

$$\deg_y(\gcd(\varphi_a(f), \varphi_a(g))) \geq \deg_y(\varphi_a(h)) = \deg_y(h).$$

- (2) We have

$$\gcd(\varphi_a(f), \varphi_a(g)) = \gcd(\varphi_a(\bar{f}), \varphi_a(\bar{g})) \cdot \varphi_a(h).$$

If $\gcd(\varphi_a(f), \varphi_a(g)) \neq \varphi_a(h)$, then $\gcd(\varphi_a(\bar{f}), \varphi_a(\bar{g})) \neq 1$. Hence, the resultant w.r.t. y of $\varphi_a(\bar{f}), \varphi_a(\bar{g})$ is zero. Therefore, since φ_a is a ring homomorphism, one obtains that

$$0 = \text{res}_y(\varphi_a(\bar{f}), \varphi_a(\bar{g})) = \varphi_a(\text{res}_y(\bar{f}, \bar{g})).$$

This, however, is excluded by the assumptions. \square

Lemma 4.27. *Let $\mathcal{P}(t)$ be a rational parametrization in reduced form. Then for almost all values $\alpha \in K$ of s we have*

$$\deg_t(\gcd(G_1^{\mathcal{P}}(s, t), G_2^{\mathcal{P}}(s, t))) = \deg_t(\gcd(G_1^{\mathcal{P}}(\alpha, t), G_2^{\mathcal{P}}(\alpha, t))).$$

Proof. We distinguish two cases. First, we assume that no component of $\mathcal{P}(t)$ is constant, so $G_1^{\mathcal{P}}(s, t)$ and $G_2^{\mathcal{P}}(s, t)$ cannot be zero. Thus, if $G = \gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}})$ and $G_1^{\mathcal{P}} = \overline{G_1^{\mathcal{P}}} \cdot G, G_2^{\mathcal{P}} = \overline{G_2^{\mathcal{P}}} \cdot G$, then $T(s) = \text{res}_t(\overline{G_1^{\mathcal{P}}}, \overline{G_2^{\mathcal{P}}}) \in K[s]$ is not identically zero. Therefore, $T(s)$ and the leading coefficients of $G_1^{\mathcal{P}}$ and $G_2^{\mathcal{P}}$, w.r.t. t , can only vanish at finitely many values. From Lemma 4.26 (2) we get $\varphi_\alpha(\gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}})) = \gcd(\varphi_\alpha(G_1^{\mathcal{P}}), \varphi_\alpha(G_2^{\mathcal{P}}))$ for almost all $\alpha \in K$.

Second, if any component of the parametrization $\mathcal{P}(t)$ is constant, we obviously have $\varphi_\alpha(\gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}})) = \gcd(\varphi_\alpha(G_1^{\mathcal{P}}), \varphi_\alpha(G_2^{\mathcal{P}}))$.

So, for almost all $\alpha \in K$,

$$\deg_t(\gcd(\varphi_\alpha(G_1^{\mathcal{P}}), \varphi_\alpha(G_2^{\mathcal{P}}))) = \deg_t(\varphi_\alpha(\gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}}))) \leq \deg_t(\gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}})).$$

On the other hand, by Lemma 4.26 (1), for almost all $\alpha \in K$,

$$\deg_t(\gcd(\varphi_\alpha(G_1^{\mathcal{P}}), \varphi_\alpha(G_2^{\mathcal{P}}))) \geq \deg_t(\gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}})).$$

Thus, for almost all $\alpha \in K$, $\deg_t(\gcd(\varphi_\alpha(G_1^{\mathcal{P}}), \varphi_\alpha(G_2^{\mathcal{P}}))) = \deg_t(\gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}}))$. \square

Theorem 4.28. *Let $\mathcal{P}(t)$ be a parametrization in reduced form of the curve \mathcal{C} . Then*

$$\text{index}(\mathcal{P}(t)) = \deg_t(\gcd(G_1^{\mathcal{P}}(s, t), G_2^{\mathcal{P}}(s, t))).$$

Proof. The result follows from Theorem 4.25, Lemma 4.27, and Theorem 2.43. \square

Now from Lemma 4.26, Theorem 4.28, and the proof of Lemma 4.27 we get the following corollary.

Corollary 4.29. *Let $\mathcal{P}(t)$ be a parametrization in reduced form, and let $G^{\mathcal{P}}(s, t) = \gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}})$. We define $T(s) = \text{res}_t(\frac{G_1^{\mathcal{P}}}{G^{\mathcal{P}}}, \frac{G_2^{\mathcal{P}}}{G^{\mathcal{P}}})$ if \mathcal{P} does not have constant components, and $T(s) = 1$ otherwise. Then, for $\alpha \in K$ such that $\chi_{12}(\alpha)\chi_{22}(\alpha)T(\alpha) \neq 0$, and such that α is not a common root of the leading coefficients of $G_1^{\mathcal{P}}$ and $G_2^{\mathcal{P}}$ w.r.t. t , we have*

- (1) $\text{card}(\mathcal{F}_{\mathcal{P}}(\mathcal{P}(\alpha))) = \deg_t(G^{\mathcal{P}}(\alpha, t)) = \deg_t(G^{\mathcal{P}}(s, t)),$
- (2) $\mathcal{F}_{\mathcal{P}}(\mathcal{P}(\alpha)) = \{\beta \in K \mid G^{\mathcal{P}}(\alpha, \beta) = 0\}.$ \square

Since a parametrization is proper if and only if it defines a birational mapping between the affine line and the curve, it is clear that a parametrization is proper if and only if its tracing index is 1.

Theorem 4.30. *A rational parametrization is proper if and only if its tracing index is 1, i.e. if and only if $\deg_t(\gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}})) = 1$.*

The previous results can be used to derive the following algorithm for computing the tracing index of a given parametrization. This algorithm can also be used for checking the properness of a parametrization.

Algorithm TRACING INDEX

Given a rational parametrization $\mathcal{P}(t)$ in reduced form, the algorithm computes $\text{index}(\mathcal{P}(t))$, and decides whether the parametrization is proper.

1. Compute the polynomials $G_1^{\mathcal{P}}(s, t), G_2^{\mathcal{P}}(s, t)$.
2. Determine $G^{\mathcal{P}}(s, t) := \gcd(G_1^{\mathcal{P}}, G_2^{\mathcal{P}})$.
3. $\ell := \deg_t(G^{\mathcal{P}}(s, t))$.
4. If $\ell = 1$ then return “ $\mathcal{P}(t)$ is proper and $\text{index}(\mathcal{P}(t)) = 1$ ” else return “ $\mathcal{P}(t)$ is not proper and $\text{index}(\mathcal{P}(t)) = \ell$ ”

We illustrate the algorithm by an example.

Example 4.31. Let $\mathcal{P}(t)$ be the rational parametrization

$$\mathcal{P}(t) = \left(\frac{(t^2 - 1)t}{t^4 - t^2 + 1}, \frac{(t^2 - 1)t^2}{t^6 - 3t^4 + 3t^2 - 1 - 2t^3} \right).$$

In Step 1 the polynomials

$$G_1^{\mathcal{P}}(s, t) = s^3t^4 - st^4 + s^2t^3 - s^4t^3 - t^3 - s^3t^2 + st^2 + s^4t - s^2t + t + s^3 - s$$

$$G_2^{\mathcal{P}}(s, t) = s^4t^6 - s^2t^6 - s^6t^4 + 2s^3t^4 + t^4 - 2s^4t^3 + 2s^2t^3 + s^6t^2 - 2s^3t^2 - t^2 - s^4 + s^2,$$

are generated. Their gcd, computed in Step 2, is $G^{\mathcal{P}}(s, t) = st^2 - s^2t + t - s$. Thus, $\text{index}(\mathcal{P}(t)) = 2$, and therefore the parametrization is not proper.

For a generalization of these results to the surface case see [PDS04].

4.3.2 Tracing Index Under Reparametrizations

In order to study the behavior of the index under reparametrizations we first prove a technical lemma where we show that, in the case of a single nonconstant rational function $R(t)$, the degree w.r.t. t of $R(t)$ is the degree of the rational map from K to K induced by $R(t)$.

Lemma 4.32. *Let $R(t) = p(t)/q(t) \in K(t)$ be nonconstant and in reduced form. Let $R : K \rightarrow K$ be the rational map induced by $R(t)$. Then $\text{card}(R^{-1}(a)) = \deg(R(t))$ for almost all $a \in K$.*

Proof. Let W_0 be the nonempty open subset of K where R is defined, and let V_0 be the subset of points $a \in K$ such that $p(t) - aq(t)$ is square-free, and such that $\deg(p(t) - aq(t)) = \deg(R(t))$. From Lemma 4.19 we get that V_0 is open and nonempty. Furthermore, since R is nonconstant, $R(W_0)$ is also a nonempty open set (see Exercise 4.5). We consider the set $U = V_0 \cap R(W_0)$. So also U is a nonempty open set. We show that $\text{card}(R^{-1}(a)) = \deg(R(t))$ for all $a \in U$. Indeed: take $a \in U$. Then $R^{-1}(a)$ is nonempty. Moreover, since $\gcd(p, q) = 1$, $p(t) - aq(t)$ is square-free, and $\deg(p(t) - aq(t)) = \deg(R(t))$. Then, $\text{card}(R^{-1}(a)) = \deg(R(t))$. \square

Theorem 4.33. *Let $\mathcal{P}(t)$ be a rational parametrization, and $R(t) \in K(t) \setminus K$. Then*

$$\text{index}(\mathcal{P}(R(t))) = \deg(R(t)) \cdot \text{index}(\mathcal{P}(t)).$$

Proof. The statement follows from Lemmas 2.42 and 4.32. \square

Corollary 4.34. *Let \mathcal{C} be an affine rational curve defined over K by $f(x, y)$, and let $\mathcal{P}(t) = (\chi_1(t), \chi_2(t))$ be a parametrization of \mathcal{C} . If $\chi_1(t)$ is nonzero then $\deg_y(f) = \frac{\deg(\chi_1(t))}{\text{index}(\mathcal{P})}$; similarly if $\chi_2(t)$ is nonzero then $\deg_x(f) = \frac{\deg(\chi_2(t))}{\text{index}(\mathcal{P})}$.*

Proof. By Lemmas 4.13 and 4.17, there exists a proper parametrization $\mathcal{Q}(t) = (\xi_1(t), \xi_2(t))$ of \mathcal{C} , and $R(t) \in K(t) \setminus K$ such that $\mathcal{P}(t) = \mathcal{Q}(R(t))$. By Theorem 4.33

$$\text{index}(\mathcal{P}(t)) = \deg(R(t)) \cdot \text{index}(\mathcal{Q}(t)) = \deg(R(t)).$$

Moreover, $\deg(\chi_i(t)) = \deg(R(t)) \cdot \deg(\xi_i(t))$. Now, the result follows from Theorem 4.21. \square

In Theorem 4.35 we show the relation between the index of a parametrization, the degree of a parametrization and the degree of the curve.

Theorem 4.35. *Let \mathcal{C} be an affine rational curve defined by $f(x, y) \in K[x, y]$, let $n = \max\{\deg_x(f), \deg_y(f)\}$, and let $\mathcal{P}(t)$ be a rational parametrization of \mathcal{C} . Then,*

$$\text{index}(\mathcal{P}(t)) = \frac{\deg(\mathcal{P}(t))}{n}.$$

Proof. Because of Lemma 4.13 there exists a proper parametrization $\mathcal{P}'(t)$ of \mathcal{C} , and because of Lemma 4.17 there exists $R(t) \in K(t) \setminus K$ such that $\mathcal{P}(t) = \mathcal{P}'(R(t))$. From Theorem 4.33 and the fact that $\mathcal{P}'(t)$ is proper we get that

$$\text{index}(\mathcal{P}(t)) = \deg(R(t)) \cdot \text{index}(\mathcal{P}'(t)) = \deg(R(t)).$$

Furthermore, since the degree of rational functions under composition is multiplicative, we arrive at $\deg(\mathcal{P}(t)) = \deg(R(t)) \cdot \deg(\mathcal{P}'(t))$. Thus

$$\text{index}(\mathcal{P}(t)) = \frac{\deg(\mathcal{P}(t))}{\deg(\mathcal{P}'(t))}.$$

Applying Theorem 4.21 we see that $\deg(\mathcal{P}'(t)) = n$, which completes the proof. \square

4.4 Inversion of Proper Parametrizations

In Theorems 4.14, 4.21, and 4.30 we have deduced various different criteria for deciding the properness of a parametrization. Now, we show how to compute the inverse map of a proper rational parametrization. Let $\mathcal{P}(t)$ be a proper parametrization of an affine rational curve \mathcal{C} . Then the *inversion problem* consists of computing the inverse rational mapping of the birational map (compare Definition 4.12)

$$\mathcal{P} : \mathbb{A}^1(K) \longrightarrow \mathcal{C}.$$

More precisely, we want to compute the rational map

$$\begin{aligned} \varphi : \mathcal{C} &\longrightarrow \mathbb{A}^1(K) \\ (x, y) &\longmapsto \varphi(x, y), \end{aligned}$$

satisfying

- (1) $\varphi \circ \mathcal{P} = id_{\mathbb{A}^1(K)}$, i.e. $\varphi(\mathcal{P}(t)) = t$, and
- (2) $\mathcal{P} \circ \varphi = id_{\mathcal{C}}$, i.e. $\chi_{i2}(\varphi)x - \chi_{i1}(\varphi) = 0 \pmod{I(\mathcal{C})}$ for $i = 1, 2$,

where χ_{i1}/χ_{i2} is the i -th component of $\mathcal{P}(t)$. In this case φ is the inverse \mathcal{P}^{-1} we are looking for.

So the inversion problem is essentially an elimination problem, and therefore elimination techniques such as Gröbner bases can be applied. Here we give a different approach to the problem based on the computation of gcds over the function field of the curve. A generalization to surfaces of these ideas can be found in [PDSS02]. For a more general statement of the problem, namely inversion of birational maps, see [Sch98b]. Alternative methods for inverting proper parametrizations can be found in [BuD06], [ChG92b], and [GSA84].

In addition, in order to check whether a rational function is the inverse of a given parametrization, it is enough to test one of the two conditions given above. A proof of this fact, for the general case of hypersurfaces, can be found in [PDSS02]. Thus, in the sequel, we will choose freely one of the conditions to check the rational invertibility of a parametrization.

Lemma 4.36. *Let*

$$\begin{aligned} \mathcal{P} : \mathbb{A}^1(K) &\longrightarrow \mathcal{C} \subset \mathbb{A}^2(K) \\ t &\longmapsto (\chi_1(t), \chi_2(t)) \end{aligned}$$

be a rational parametrization of a plane curve \mathcal{C} , and let

$$\begin{aligned} \mathcal{U} : \mathcal{C} &\longrightarrow \mathbb{A}^1(K) \\ (x, y) &\longmapsto \mathcal{U}(x, y) \end{aligned}$$

be a rational map, where the denominators of \mathcal{U} do not belong to the ideal of \mathcal{C} . The following statements are equivalent:

- (1) \mathcal{U} is the inverse of \mathcal{P} .
- (2) $\mathcal{P}(\mathcal{U}(P)) = P$ for almost all points $P \in \mathcal{C}$.
- (3) $\mathcal{U}(\mathcal{P}(t)) = t$ for almost all values $t \in K$. □

First we observe that $K(\mathcal{C})[t]$ is a Euclidean domain. Furthermore, since we know how to computationally perform the arithmetic in the coordinate ring $\Gamma(\mathcal{C})$ (see Sect. 2.2), we know how to compute gcds in $K(\mathcal{C})[t]$. Moreover, since $I(\mathcal{C})$ is principal, all computations can be carried out by means of remainders w.r.t. the defining polynomial. Alternatively we may use the parametrization $\mathcal{P}(t)$ to check whether a class in the quotient ring $\Gamma(\mathcal{C})$ is zero. Of course, this second approach avoids the use of the implicit equation but representatives of the classes are not reduced.

Theorem 4.37. *Let $\mathcal{P}(t)$ be a proper parametrization in reduced form with nonconstant components of a rational curve \mathcal{C} . Let $H_1^{\mathcal{P}}(t, x), H_2^{\mathcal{P}}(t, y)$ be considered as polynomials in $K(\mathcal{C})[t]$. Then,*

$$\deg_t(\gcd_{K(\mathcal{C})[t]}(H_1^{\mathcal{P}}, H_2^{\mathcal{P}})) = 1.$$

Moreover, the single root of this gcd is the inverse of \mathcal{P} .

Proof. Let $R(t) = \gcd_{K(\mathcal{C})[t]}(H_1^{\mathcal{P}}, H_2^{\mathcal{P}})$, and let φ be the inverse of \mathcal{P} . Then φ is a root of $R(t)$, and therefore $\deg_t(R) \geq 1$. Now, since R is the gcd, there exist polynomials $M_i(x, y, t) \in K(\mathcal{C})[t]$ such that $H_i^{\mathcal{P}}(x, y, t) = M_i(x, y, t)R(x, y, t) \bmod I(\mathcal{C})$. Thus, if f defines \mathcal{C} , the above equality can be written in $K[x, y, t]$ as:

$$N_i(x, y)H_i^{\mathcal{P}}(x, y, t) = M_i^*(x, y, t)S(x, y, t) + A(x, y)f(x, y) ,$$

where $\deg_t(S) = \deg_t(R)$, and neither N_i nor all coefficients of M_i^* w.r.t. t , nor the leading coefficient of S w.r.t. t belong to $I(\mathcal{C})$. Thus, substituting $\mathcal{P}(s)$ into this formula and clearing denominators, we see that $\deg_t(S) \leq \deg_t(\gcd(G_1^{\mathcal{P}}(s, t), G_1^{\mathcal{P}}(s, t)))$. Now, by Theorem 4.30, we get that $\deg_t(R) = \deg_t(S) \leq 1$. \square

In the following we outline an algorithm for inverting a proper parametrization, based on Theorem 4.37.

Algorithm INVERSE

Given an affine rational parametrization $\mathcal{P}(t)$, in reduced form, the algorithm decides whether the parametrization is proper, and in the affirmative case it determines the inverse of the mapping \mathcal{P} .

1. Apply algorithm TRACING INDEX to check whether $\mathcal{P}(t)$ is proper. If $\mathcal{P}(t)$ is not proper then return “not proper” and **exit**.
2. Compute $H_1^{\mathcal{P}}(t, x)$ and $H_2^{\mathcal{P}}(t, y)$.
3. Determine $M(x, y, t) = \gcd_{K(\mathcal{C})[t]}(H_1^{\mathcal{P}}, H_2^{\mathcal{P}})$. By Theorem 4.37 $M(x, y, t)$ is linear in t ; let us say

$$M(x, y, t) = D_1(x, y)t - D_0(x, y) .$$

4. Return “the inverse is $\frac{D_0(x, y)}{D_1(x, y)}$.”

Example 4.38. Let \mathcal{C} be the plane curve over \mathbb{C} defined by the rational parametrization

$$\mathcal{P}(t) = \left(\frac{t^3 + 1}{t^2 + 3}, \frac{t^3 + t + 1}{t^2 + 1} \right) .$$

It is easy to check, applying algorithm TRACING INDEX, that $\text{index}(\mathcal{P}(t)) = 1$ and therefore $\mathcal{P}(t)$ is proper. Furthermore, the implicit equation of \mathcal{C} is

$$f(x, y) = -4x^2y^3 + 4xy^3 - 2y^3 + 4x^3y^2 - 8x^2y^2 + 4xy^2 + 3y^2 + 4x^3y - 3x^2y - 11xy + 13x^3 + 8x^2 + 3x - 1 .$$

For a method for computing the implicit equation see Theorem 4.39. In Step 2 we consider the polynomials in $K(\mathcal{C})[t]$

$$H_1^{\mathcal{P}}(t, x) = -t^3 + xt^2 + 3x - 1, \quad H_2^{\mathcal{P}}(t, y) = -t^3 + yt^2 - t + y - 1.$$

In Step 3, we determine $\gcd_{\mathbb{C}(C)[t]}(H_1^{\mathcal{P}}, H_2^{\mathcal{P}})$. The polynomial remainder sequence of $H_1^{\mathcal{P}}$ and $H_2^{\mathcal{P}}$ is:

$$R_0(t) = -t^3 + xt^2 + 3x - 1$$

$$R_1(t) = -t^3 + yt^2 - t + y - 1$$

$$R_2(t) = (x - y)t^2 + t + 3x - y$$

$$R_3(t) = \frac{2x^2 - 3yx - 1 + y^2}{(-x + y)^2}t + \frac{(-2y - 1)x^2 + (2y^2 + 2y - 3)x - y^2 + y}{(-x + y)^2}$$

$$R_4(t) = 0.$$

Thus, $\gcd_{\mathbb{C}(C)[t]}(H_1^{\mathcal{P}}, H_2^{\mathcal{P}})$

$$= \frac{(2x^2 - 3yx - 1 + y^2)}{(-x + y)^2}t + \frac{-y^2 + 2y^2x + 2yx - 3x - 2yx^2 - x^2 + y}{(-x + y)^2}.$$

Therefore, the inverse mapping is:

$$\mathcal{P}^{-1}(x, y) = -\frac{-y^2 + 2y^2x + 2yx - 3x - 2yx^2 - x^2 + y}{2x^2 - 3yx - 1 + y^2}.$$

4.5 Implicitization

Given an affine rational parametrization $\mathcal{P}(t)$, the *implicitization problem* consists of computing the defining polynomial for the Zariski closure of the set

$$S = \{\mathcal{P}(t) \mid t \in K \text{ such that } \mathcal{P}(t) \text{ is defined}\}.$$

Therefore, the problem consists of finding the smallest algebraic set in $\mathbb{A}^2(K)$ containing S . Note also, that if we are given a projective rational parametrization the implicitization problem is the same since the defining polynomial of the projective curve is the homogenization of the defining polynomial of the affine curve.

The problem can be solved by general elimination techniques such as Gröbner bases ([AdL94] and [CLO97]). This approach is valid not only for curves but for the more general case of parametric varieties in $\mathbb{A}(K)^n$. Also, for surfaces, different approaches can be found in [BCD03], [ChG92a], [Gon97], [Kot04], [SGD97]. However, for the case of plane curves, the implicit equation can be found by means of gcd's and resultants alone. For instance, applying Lemma 4.6, the defining polynomial of the curve parametrized by $\mathcal{P}(t)$ can be obtained by computing the square-free part of a resultant. Moreover,

if properness is guaranteed, Theorem 4.39 shows that the implicit equation can be computed by a single resultant. This result can be found in [SGD97], [SeW89], or in [SeW01a]. In addition to these results, in Theorem 4.41 we see that in this resultant the implicit equation appears to the power of the tracing index. Similar results on implicitization can be found in [ChG92a] and [CLO97].

Theorem 4.39. *Let $\mathcal{P}(t)$ be a proper parametrization in reduced form of a rational affine plane curve \mathcal{C} . Then, the defining polynomial of \mathcal{C} is the resultant*

$$\text{res}_t(H_1^{\mathcal{P}}(t, x), H_2^{\mathcal{P}}(t, y)).$$

Proof. Let $\mathcal{P}(t) = (\chi_1(t), \chi_2(t))$. We know from Theorem 4.21 that, if $f(x, y)$ is the implicit equation of \mathcal{C} , then $\deg_y(f) = \deg(\chi_1(t))$, and $\deg_x(f) = \deg(\chi_2(t))$. The polynomials $H_i^{\mathcal{P}}$ can be written as

$$\begin{aligned} H_1^{\mathcal{P}}(t, x) &= a_m(x)t^m + \cdots + a_0(x), & \text{where } m = \deg_y(f), \\ H_2^{\mathcal{P}}(t, y) &= b_n(y)t^n + \cdots + b_0(y), & \text{where } n = \deg_x(f), \end{aligned}$$

where $\deg_x(a_i) \leq 1$ and $\deg_y(b_i) \leq 1$.

Let $R(x, y)$ be the resultant of $H_1^{\mathcal{P}}$ and $H_2^{\mathcal{P}}$ with respect to t , and let A be the Sylvester matrix of $H_1^{\mathcal{P}}, H_2^{\mathcal{P}} \in K(x, y)[t]$ seen as univariate polynomials in t :

$$A = \begin{pmatrix} a_m(x) & \cdots & \cdots & \cdots & a_0(x) & & \\ & \ddots & & & & \ddots & \\ & & a_m(x) & \cdots & \cdots & & a_0(x) \\ b_n(y) & \cdots & \cdots & \cdots & b_0(y) & & \\ & \ddots & & & & \ddots & \\ & & b_n(y) & \cdots & \cdots & & b_0(y) \end{pmatrix}.$$

Therefore, since only the entries in the first n rows depend on x , and this dependence on x is linear, $\deg_x(R) \leq n$. Analogously, $\deg_y(R) \leq m$. On the other hand, it is known that $f(x, y)$ is a factor of $R(x, y)$ (compare Lemma 4.6). Thus, $\deg_x(f) = \deg_x(R)$ and $\deg_y(f) = \deg_y(R)$. Therefore, up to a constant, $f(x, y) = R(x, y)$. \square

We finish this section showing how Lemma 4.6, Theorem 4.39, and the notion of tracing index of a parametrization (compare Definition 4.24) are related. Basically, the result follows from the next lemma on resultants, which is valid for an arbitrary field.

Lemma 4.40. *Let $A, B \in \mathbb{L}[t]$ be nonconstant polynomials over a field \mathbb{L} :*

$$A(t) = a_m t^m + \cdots + a_0, \quad B(t) = b_n t^n + \cdots + b_0, \quad a_m b_n \neq 0$$

and let $R(t) = \frac{M(t)}{N(t)} \in \mathbb{L}(t)$ be a nonconstant rational function in reduced form, such that $\deg(M - \beta N) = \deg(R)$ for every root β of $A(t)B(t)$. Let $A'(t)$ and $B'(t)$ be the polynomials

$$\begin{aligned} A'(t) &= a_m M(t)^m + a_{m-1} M(t)^{m-1} N(t) + \cdots + a_0 N(t)^m, \\ B'(t) &= b_n M(t)^n + b_{n-1} M(t)^{n-1} N(t) + \cdots + b_0 N(t)^n. \end{aligned}$$

Then, if b' is the leading coefficient of B' ,

$$\text{res}_t(A', B') = \frac{(b')^{m(\deg(R) - \deg(N))}}{b_n^{m \deg(R)}} \text{res}_t(A, B)^{\deg(R)} \cdot \text{res}_t(B', N)^m.$$

Proof. Let B decompose over the algebraic closure of \mathbb{L} as

$$B(t) = b_n \prod_{i=1}^n (t - \beta_i).$$

Since $B'(t) = N^n \cdot B(R)$ one has that

$$B'(t) = b_n \prod_{i=1}^n (M(t) - \beta_i N(t)).$$

Therefore, since $\deg(M - \beta_i N) = \deg(R)$ for every $i \in \{1, \dots, n\}$, we have $\deg(B') = n \cdot \deg(R)$. In particular, since R is nonconstant, B' is not a constant polynomial. Similarly we see that $\deg(A') = m \cdot \deg(R)$, and that A' is also a nonconstant polynomial.

Now, observe that if $r = \deg(R)$, every root β_i of B generates r roots $\{\beta_{i,1}, \dots, \beta_{i,r}\}$ of $B'(t)$, namely the roots of $M(t) - \beta_i N(t)$. Moreover, if α is a root of B' then $N(\alpha) \neq 0$, since otherwise one gets that $M(\alpha) = 0$, which is impossible because of $\gcd(M, N) = 1$. Therefore,

$$\beta_i = \frac{M(\beta_{i,j})}{N(\beta_{i,j})} = R(\beta_{i,j}), \quad j = 1, \dots, r.$$

Let $S = \text{res}_t(A, B)$, $S' = \text{res}_t(A', B')$ and $S'' = \text{res}_t(B', N)$. From the relation $A' = N^m \cdot A(R)$ we get

$$S' = (b')^{mr} \prod_{B'(\alpha)=0} A'(\alpha) = (b')^{mr} \prod_{i=1}^n \prod_{j=1}^r A'(\beta_{i,j}) = (b')^{mr} \prod_{i=1}^n A(\beta_i)^r \prod_{j=1}^r N(\beta_{i,j})^m.$$

Furthermore, if $k = \deg(N)$, we have

$$S = b_n^m \prod_{i=1}^n A(\beta_i), \quad S'' = (b')^k \prod_{i=1}^n \prod_{j=1}^r N(\beta_{i,j}).$$

Thus,

$$S' = \frac{(b')^{mr}}{b_n^{rm}} S^r \prod_{i=1}^n \prod_{j=1}^r N(\beta_{i,j})^m = \frac{(b')^{mr-km}}{b_n^{rm}} S^r \cdot (S'')^m. \quad \square$$

Theorem 4.41. *Let $\mathcal{P}(t)$ be a parametrization in reduced form of an affine rational plane curve \mathcal{C} , and let $f(x, y)$ be the defining polynomial of \mathcal{C} . Then for some nonzero constant c we have*

$$\text{res}_t(H_1^{\mathcal{P}}(t, x), H_2^{\mathcal{P}}(t, y)) = c \cdot (f(x, y))^{\text{index}(\mathcal{P})}.$$

Proof. If \mathcal{C} is a line parallel to one of the axes, let us say $y = a$, then $\mathcal{P}(t) = (\frac{\chi_{11}(t)}{\chi_{12}(t)}, a)$. By Lemma 4.32 $\text{index}(\mathcal{P}) = \deg(\mathcal{P})$. Therefore,

$$\begin{aligned} & \text{res}_t(H_1^{\mathcal{P}}(t), H_2^{\mathcal{P}}(t)) \\ &= \text{res}_t(x \cdot \chi_{12}(t) - \chi_{11}(t), y - a) = (y - a)^{\deg(\mathcal{P}(t))} = (y - a)^{\text{index}(\mathcal{P})}. \end{aligned}$$

Let us now assume that the irreducible curve \mathcal{C} is not a line parallel to one of the axes, i.e. its defining polynomial depends on both variables x, y . By Lemma 4.18 there is a proper parametrization of \mathcal{C} in which the degrees of numerator and denominator at each component agree. So let

$$\mathcal{P}'(t) = \left(\frac{\xi_{11}(t)}{\xi_{12}(t)}, \frac{\xi_{21}(t)}{\xi_{22}(t)} \right)$$

be a proper parametrization, in reduced form, of \mathcal{C} where $\deg(\xi_{i1}) = \deg(\xi_{i2})$. By Lemma 4.17 there exists a nonconstant rational function $R(t)$ such that $\mathcal{P}(t) = \mathcal{P}'(R(t)) = \left(\frac{\chi_{11}(t)}{\chi_{12}(t)}, \frac{\chi_{21}(t)}{\chi_{22}(t)} \right)$. Let $R(t) = \frac{M(t)}{N(t)}$ be in reduced form. We consider the polynomials

$$\begin{aligned} H_1^{\mathcal{P}}(t) &= x \cdot \chi_{12}(t) - \chi_{11}(t), & H_2^{\mathcal{P}}(t) &= y \cdot \chi_{22}(t) - \chi_{21}(t), \\ H_1^{\mathcal{P}'}(t) &= x \cdot \xi_{12}(t) - \xi_{11}(t), & H_2^{\mathcal{P}'}(t) &= y \cdot \xi_{22}(t) - \xi_{21}(t). \end{aligned}$$

Note that $H_i^{\mathcal{P}}, H_i^{\mathcal{P}'} \in (\mathbb{K}[x, y])[t]$.

We structure the remaining part of the proof in the following way:

- (1) we relate the polynomials $H_i^{\mathcal{P}}$ and $\overline{H}_i^{\mathcal{P}'}$ (the result of substituting the rational function R into $H_i^{\mathcal{P}'}$),
- (2) we extract common factors in these relations,
- (3) we derive a nontrivial relation between $\text{res}_t(H_1^{\mathcal{P}}, H_2^{\mathcal{P}})$ and $\text{res}_t(\overline{H}_1^{\mathcal{P}'}, \overline{H}_2^{\mathcal{P}'})$,
- (4) these resultants contain powers of the defining polynomial of \mathcal{C} . We express the exponent as $\text{index}(\mathcal{P})$.

So let us deal with step (1). Let

$$\xi_{i1}(t) = \sum_{j=0}^{n_i} a_{i,j} t^j, \quad \xi_{i2}(t) = \sum_{j=0}^{n_i} b_{i,j} t^j, \quad H_i^{\mathcal{P}'}(t) = \sum_{j=0}^{m_i} h_{i,j} t^j, \quad \text{for } i = 1, 2.$$

Observe that $m_i = n_i$. For $i = 1, 2$, we introduce the new polynomials

$$\begin{aligned}\bar{\xi}_{i1}(t) &= \sum_{j=0}^{n_i} a_{i,j} M(t)^j N(t)^{n_i-j}, & \bar{\xi}_{i2}(t) &= \sum_{j=0}^{n_i} b_{i,j} M(t)^j N(t)^{n_i-j}, \\ \bar{H}_i^{\mathcal{P}'}(t) &= \sum_{j=0}^{m_i} h_{i,j} M(t)^j N(t)^{m_i-j},\end{aligned}$$

which result from $\xi_{i1}, \xi_{i2}, H_i^{\mathcal{P}'}$ by substituting $R(t)$ for t and clearing denominators. In order to apply Lemma 4.40 to the nonconstant polynomials $H_1^{\mathcal{P}'}(t), H_2^{\mathcal{P}'}(t) \in K(x, y)[t]$ and the rational function $R(t)$, let us see that $\deg(M(t) - \beta N(t)) = \deg(R)$ for every root β of $H_1^{\mathcal{P}'}(t) \cdot H_2^{\mathcal{P}'}(t)$. Indeed, if β is such that $\deg(M(t) - \beta N(t)) < \deg(R)$ then $\beta \in K$. Therefore, either $H_1^{\mathcal{P}'}(\beta) = 0$ or $H_2^{\mathcal{P}'}(\beta) = 0$ and $\beta \in K$. This implies that either $\gcd(\xi_{11}, \xi_{12}) \neq 1$ or $\gcd(\xi_{21}, \xi_{22}) \neq 1$, which is impossible. The application of Lemma 4.40 leads to

$$\begin{aligned}\text{res}_t(\bar{H}_1^{\mathcal{P}'}, \bar{H}_2^{\mathcal{P}'}) &= \\ \frac{(b')^{m_1(\deg(R) - \deg(N))}}{h_{2,m_2}^{\deg(R)m_1}} \cdot \text{res}_t(H_1^{\mathcal{P}'}, H_2^{\mathcal{P}'})^{\deg(R)} \cdot \text{res}_t(\bar{H}_2^{\mathcal{P}'}, N)^{m_1},\end{aligned}\quad (4.1)$$

where b' is the leading coefficient of $\bar{H}_2^{\mathcal{P}'}$ w.r.t. t . In addition, since $\mathcal{P}(t) = \mathcal{P}'(R(t))$, we have

$$\chi_{j1}(t) \cdot \xi_{j2}(R(t)) = \xi_{j1}(R(t)) \cdot \chi_{j2}(t), \quad j = 1, 2.$$

Thus,

$$\chi_{j1}(t) \cdot H_j^{\mathcal{P}'}(R(t)) = \xi_{j1}(R(t)) \cdot H_j^{\mathcal{P}}(t), \quad j = 1, 2,$$

and (note that $m_j = n_j$)

$$\chi_{j1}(t) \bar{H}_j^{\mathcal{P}'}(t) = \bar{\xi}_{j1}(t) H_j^{\mathcal{P}}(t), \quad \chi_{j1}(t) \bar{\xi}_{j2}(t) = \bar{\xi}_{j1}(t) \chi_{j2}(t), \quad \text{for } j = 1, 2.$$

Next we deal with step (2). We prove that $\gcd(\chi_{11}, \chi_{21}) = \gcd(\bar{\xi}_{11}, \bar{\xi}_{21})$. Indeed: from the line above and the fact that the numerators and denominators in the parametrization are relatively prime we deduce $\chi_{j1} | \bar{\xi}_{j1}$ and thus $\gcd(\chi_{11}, \chi_{21}) | \gcd(\bar{\xi}_{11}, \bar{\xi}_{21})$. In order to prove that $\gcd(\bar{\xi}_{11}, \bar{\xi}_{21})$ divides $\gcd(\chi_{11}, \chi_{21})$, we first see that $\gcd(\bar{\xi}_{j1}, \bar{\xi}_{j2}) = 1$. Let a be a common root of $\bar{\xi}_{j1}$ and $\bar{\xi}_{j2}$. Note that by definition of $\bar{\xi}_{j1}$ it follows that $N(a) \neq 0$, since otherwise it would imply that $M(a) = 0$, which is impossible since $\gcd(M, N) = 1$. Therefore, taking into account that $\bar{\xi}_{j1} = N^{n_j} \xi_{j1}(R)$, $\bar{\xi}_{j2} = N^{n_j} \xi_{j2}(R)$, one deduces that $\xi_{j1}(R(a)) = \xi_{j2}(R(a)) = 0$ which is impossible since $\gcd(\xi_{j1}, \xi_{j2}) = 1$. So we have $\gcd(\bar{\xi}_{j1}, \bar{\xi}_{j2}) = 1$, from which we get by a similar reasoning as above that $\gcd(\bar{\xi}_{11}, \bar{\xi}_{21})$ divides $\gcd(\chi_{11}, \chi_{21})$.

As a consequence of this remark we can extract this gcd from the equalities above and express them as:

$$\chi_{j1}^*(t) \overline{H}_j^{P'}(t) = \overline{\xi}_{j1}^*(t) H_j^P(t), \quad \chi_{j1}^*(t) \overline{\xi}_{j2}(t) = \overline{\xi}_{j1}^*(t) \chi_{2j}(t), \quad \text{for } j = 1, 2,$$

where $\gcd(\chi_{11}^*, \chi_{21}^*) = \gcd(\overline{\xi}_{11}^*, \overline{\xi}_{21}^*) = 1$.

Now we come to step (3). Observe that

$$\text{res}_t(\chi_{11}^* \overline{H}_1^{P'}, \chi_{21}^* \overline{H}_2^{P'}) = \text{res}_t(\overline{\xi}_{11}^* H_1^P, \overline{\xi}_{21}^* H_2^P).$$

So,

$$\begin{aligned} & \text{res}_t(\chi_{11}^*, \chi_{21}^*) \cdot \text{res}_t(\overline{H}_1^{P'}, \overline{H}_2^{P'}) \cdot \text{res}_t(\overline{H}_1^{P'}, \chi_{21}^*) \cdot \text{res}_t(\overline{H}_1^{P'}, \overline{H}_2^{P'}) \\ &= \text{res}_t(\overline{\xi}_{11}^*, \overline{\xi}_{21}^*) \cdot \text{res}_t(\overline{\xi}_{11}^*, H_2^P) \cdot \text{res}_t(H_1^P, \overline{\xi}_{21}^*(t)) \cdot \text{res}_t(H_1^P, H_2^P). \end{aligned}$$

Let us see that none of the factors involving χ_{j1}^* or $\overline{\xi}_{j1}^*$ vanishes. Since χ_{11}^*, χ_{21}^* are relatively prime, their resultant does not vanish. Analogously for $\overline{\xi}_{j1}^*$. In order to see that the remaining factors do not vanish, we prove that if $L(t) \in K[t]^*$ then $\gcd(L, H_i^P) = \gcd(L, \overline{H}_i^{P'}) = 1$; note that since we have assumed that \mathcal{C} is not a line parallel to the axes, none of the polynomial $\overline{\xi}_{ij}^*, \chi_{ij}^*$ can be zero. Indeed: if the gcd is not trivial there exists $a \in K$ such that, for instance, $H_i^P(a) = 0$. But this implies that $\gcd(\chi_{i1}, \chi_{i2}) \neq 1$, which is impossible. Also, if $\overline{H}_i^{P'}(a) = 0$, from its definition it follows that $N(a) \neq 0$. Therefore, since $\overline{H}_i^{P'}(t) = N^{m_i} H_i^{P'}(R(t))$, one would deduce that $H_i^{P'}(R(a)) = 0$, and hence $\gcd(\xi_{i1}, \xi_{i2}) \neq 1$, which is impossible.

Taking into account this fact, the previous equality on resultants can be written as

$$T_1(y) T_2(x) \text{res}_t(\overline{H}_1^{P'}, \overline{H}_2^{P'}) = T_1'(y) T_2'(x) \text{res}_t(H_1^P, H_2^P), \quad (4.2)$$

where T_i, T_i' are univariate nonzero polynomials over K . Now, combining (4.1) and (4.2) we get

$$\begin{aligned} & T_1(y) T_2(x) \left(\frac{(b')^{m_1(\deg(R) - \deg(N))}}{h_{2,m_2}^{\deg(R)m_1}} \text{res}_t(H_1^{P'}, H_2^{P'})^{\deg(R)} \cdot \text{res}_t(\overline{H}_2^{P'}, N)^{m_1} \right) \\ &= T_1'(y) T_2'(x) \text{res}_t(H_1^P, H_2^P). \end{aligned}$$

Finally we come to step (4). If $f(x, y)$ is the implicit equation of \mathcal{C} , from Lemma 4.6 and Theorem 4.39 we see that there exists $\ell \in \mathbb{N}$ such that

$$\begin{aligned} & T_1(y) T_2(x) \left(\frac{(b')^{m_1(\deg(R) - \deg(N))}}{h_{2,m_2}^{\deg(R)m_1}} f(x, y)^{\deg(R)} \cdot \text{res}_t(\overline{H}_2^{P'}, N)^{m_1} \right) \\ &= T_1'(y) T_2'(x) f(x, y)^\ell. \end{aligned}$$

Moreover, since $b', h_{2,m_2} \in K[y]^*$ and $\text{res}_t(\overline{H}_2^{\mathcal{P}'}, N)^{m_1} \in K[y]^*$ (note that we have already proved that the gcd of $\overline{H}_2^{\mathcal{P}'}$ and a nonzero polynomial depending only on t is trivial) the above equality can be rewritten as

$$U_1(y)U_2(x)f(x,y)^{\deg(R)} = U_1'(y)U_2'(x)f(x,y)^\ell$$

for some nonzero polynomials U_i, U_i' . Therefore, since $f(x,y)$ is irreducible and it depends on both variables x, y (note that we are assuming that \mathcal{C} is not a line parallel to the axes), we conclude that $\deg(R) = \ell$. Furthermore, from Theorem 4.33 we get that

$$\text{index}(\mathcal{P}(t)) = \text{index}(\mathcal{P}'(R(t))) = \deg(R) \cdot \text{index}(\mathcal{P}'(t)) = \deg(R),$$

which finishes the proof. \square

4.6 Parametrization by Lines

In this section we treat some straight-forward cases in which we can easily parametrize implicitly given algebraic curves. This approach will be generalized in Sect. 4.7. The basic idea consists in using a pencil of lines through a suitable point on the curve such that by computing an intersection point of a generic element of the pencil with the curve one determines a parametrization of the curve. Of course every line \mathcal{L} can be rationally parametrized, in fact by a pencil of lines with a base point not on \mathcal{L} . In the following we will not consider lines.

4.6.1 Parametrization of Conics

Only irreducible curves can be rational (see Theorem 4.4). So let \mathcal{C} be an irreducible conic defined by the quadratic polynomial

$$f(x,y) = f_2(x,y) + f_1(x,y) + f_0(x,y),$$

where $f_i(x,y)$ are homogeneous of degree i . Let us first assume w.l.o.g. that \mathcal{C} passes through the origin, so $f_0(x,y) = 0$. Let $\mathcal{H}(t)$ be the linear system $\mathcal{H}(1, O)$ of lines through the origin (compare Sect. 2.4), the elements of $\mathcal{H}(t)$ being parametrized by their slope t . So the defining polynomial of $\mathcal{H}(t)$ is

$$h(x,y,t) = y - tx.$$

Now, we compute the intersection points of a generic element of $\mathcal{H}(t)$ and \mathcal{C} . That is, we solve the system

$$\begin{cases} y = tx \\ f(x,y) = 0 \end{cases}$$

w.r.t. the variables x, y . The solutions are

$$O = (0, 0) \quad \text{and} \quad Q(t) = \left(-\frac{f_1(1, t)}{f_2(1, t)}, -\frac{t \cdot f_1(1, t)}{f_2(1, t)} \right).$$

Note that $f_1(x, y)$ is not identically zero, since \mathcal{C} is an irreducible curve. Therefore, Q depends on the parameter t . Furthermore, $f(Q(t)) = 0$, so by Theorem 4.7 $Q(t)$ is a parametrization of \mathcal{C} .

Theorem 4.42. *The irreducible projective conic \mathcal{C} defined by the polynomial $F(x, y, z) = f_2(x, y) + f_1(x, y)z$ (f_i a form of degree i , respectively), has the rational projective parametrization*

$$\mathcal{P}(t) = (-f_1(1, t), -tf_1(1, t), f_2(1, t)).$$

Corollary 4.43. *Every irreducible conic is rational.*

So after a suitable change of coordinates, Theorem 4.42 yields a parametrization of the irreducible conic \mathcal{C} . We summarize this process in the following algorithm.

Algorithm CONIC-PARAMETRIZATION.

Given the defining polynomial $F(x, y, z)$ of an irreducible projective conic \mathcal{C} , the algorithm computes a rational parametrization.

1. Determine a point $(a : b : 1) \in \mathcal{C}$.
2. $g(x, y) = F(x + a, y + b, 1)$. Let $g_2(x, y)$ and $g_1(x, y)$ be the homogeneous components of $g(x, y)$ of degree 2 and 1, respectively.
3. Return $\mathcal{P}(t) = (-g_1(1, t) + ag_2(1, t), -tg_1(1, t) + bg_2(1, t), g_2(1, t))$.

Remarks. Note that, because of the geometric construction, the output parametrization of algorithm CONIC-PARAMETRIZATION is proper. Moreover, if $\mathcal{P}_{*,z}(t)$ is the affine parametrization of $\mathcal{C}_{*,z}$ derived from $\mathcal{P}(t)$, and $(a : b : 1)$ is the point on \mathcal{C} used in the algorithm, then its inverse can be expressed as

$$\mathcal{P}_{*,z}^{-1}(x, y) = \frac{y - b}{x - a}. \quad \square$$

Example 4.44. Let \mathcal{C} be the ellipse defined by

$$F(x, y, z) = x^2 + 2y^2 - z^2.$$

We apply algorithm CONIC-PARAMETRIZATION. In Step (1) we take the point $(1 : 0 : 1)$ on \mathcal{C} . Then, performing Step (2), we get $g(x, y) = x^2 + 2x + 2y^2$. So, a parametrization of \mathcal{C} is

$$\mathcal{P}(t) = (-1 + 2t^2, -2t, 1 + 2t^2).$$

4.6.2 Parametrization of Curves with a Point of High Multiplicity

Obviously, this approach can be immediately generalized to the situation where we have an irreducible projective curve \mathcal{C} of degree d with a $(d-1)$ -fold point P . W.l.o.g. we assume that $P = (0 : 0 : 1)$. So the defining polynomial of \mathcal{C} is of the form

$$F(x, y, z) = f_d(x, y) + f_{d-1}(x, y)z,$$

where f_i is a form of degree i , respectively. Of course, there can be no other singularity of \mathcal{C} , since otherwise the line passing through the two singularities would intersect \mathcal{C} more than d times.

As above, let $\mathcal{H}(t)$ be the linear system of lines $\mathcal{H}(1, O)$ through $O = (0 : 0 : 1)$. Intersecting \mathcal{C} with an element of $\mathcal{H}(t)$ we get the origin as an intersection point of multiplicity at least $d-1$. Reasoning as in the case of conics, we see that

$$Q(t) = (-f_{d-1}(1, t), -t \cdot f_{d-1}(1, t), f_d(1, t)).$$

is a rational parametrization of the curve \mathcal{C} . We summarize this in the following theorem.

Theorem 4.45. *Let \mathcal{C} be an irreducible projective curve of degree d defined by the polynomial $F(x, y, z) = f_d(x, y) + f_{d-1}(x, y)z$ (f_i a form of degree i , resp.), i.e. having a $(d-1)$ -fold point at $(0 : 0 : 1)$. Then \mathcal{C} is rational and a rational parametrization is*

$$\mathcal{P}(t) = (-f_{d-1}(1, t), -tf_{d-1}(1, t), f_d(1, t)).$$

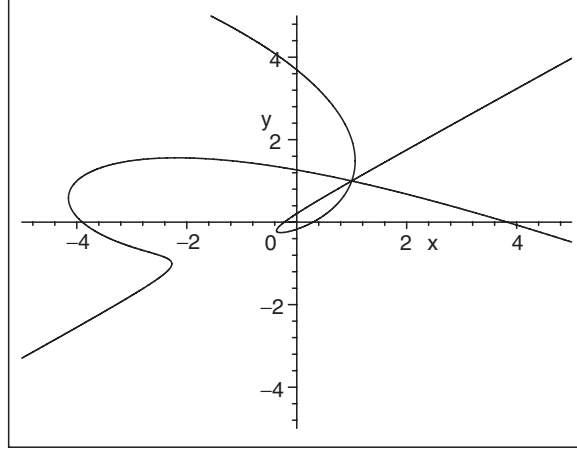
Corollary 4.46. *Every irreducible curve of degree d with a $(d-1)$ -fold point is rational.*

So after a suitable change of coordinates Theorem 4.45 yields a parametrization of the irreducible curve \mathcal{C} . We summarize this process in the following algorithm.

Algorithm PARAMETRIZATION-BY-LINES.

Given the defining polynomial $F(x, y, z)$ of an irreducible projective curve \mathcal{C} of degree d , having a $(d-1)$ -fold point, the algorithm computes a rational parametrization of \mathcal{C} .

1. If $d = 1$, then proceed as in Remark to Definition 4.48. If $d > 1$, compute the $(d-1)$ -fold point P of \mathcal{C} . W.l.o.g., perhaps after renaming the variables, let $P = (a : b : 1)$.
2. $g(x, y) := F(x + a, y + b, 1)$. Let $g_d(x, y)$ and $g_{d-1}(x, y)$ be the homogeneous components of $g(x, y)$ of degree d and $d-1$, respectively.
3. Return $\mathcal{P}(t) = (-g_{d-1}(1, t) + ag_d(1, t), -tg_{d-1}(1, t) + bg_d(1, t), g_d(1, t))$.

Fig. 4.2. Quartic \mathcal{C}

Remarks. Note that, because of the underlying geometric construction, the parametrization computed by algorithm PARAMETRIZATION-BY-LINES is proper. Furthermore, if $\mathcal{P}_{*,z}(t)$ is the affine parametrization of $\mathcal{C}_{*,z}$ derived from $\mathcal{P}(t)$, then its inverse can be computed as follows. W.l.o.g., perhaps after renaming the variables, let $P = (a : b : 1)$ be the singularity of the curve. Then

$$\mathcal{P}_{*,z}^{-1}(x, y) = \frac{y - b}{x - a}.$$

Example 4.47. Let \mathcal{C} be the affine quartic curve defined by (see Fig. 4.2)

$$f(x, y) = 1 + x - 15x^2 - 29y^2 + 30y^3 - 25xy^2 + x^3y + 35xy + x^4 - 6y^4 + 6x^2y.$$

\mathcal{C} has an affine triple point at $(1, 1)$. We apply algorithm PARAMETRIZATION-BY-LINES to parametrize \mathcal{C} . In Step 2, we compute the polynomial

$$g(x, y) = 5x^3 + 6y^3 - 25xy^2 + x^3y + x^4 - 6y^4 + 9x^2y,$$

and determining the homogeneous forms of $g(x, y)$, we get the rational parametrization of \mathcal{C}

$$\mathcal{P}(t) = \left(\frac{4 + 6t^3 - 25t^2 + 8t + 6t^4}{-1 + 6t^4 - t}, \frac{4t + 12t^4 - 25t^3 + 9t^2 - 1}{-1 + 6t^4 - t} \right).$$

Furthermore, taking into account the remark to the algorithm we have that

$$\mathcal{P}^{-1}(x, y) = \frac{y - 1}{x - 1}.$$

4.6.3 The Class of Curves Parametrizable by Lines

A natural question is whether only the rational curves considered previously are those parametrizable by lines. In order to answer this question, first of all, we must be more precise and give a formal definition of what we mean by a curve parametrizable by lines.

Definition 4.48. *The irreducible projective curve \mathcal{C} is parametrizable by lines if there exists a linear system of curves \mathcal{H} of degree 1 such that*

- (1) $\dim(\mathcal{H}) = 1$,
- (2) *the intersection of a generic element in \mathcal{H} and \mathcal{C} contains a nonconstant point whose coordinates depend rationally on the free parameter of \mathcal{H} .*

We say that an irreducible affine curve is parametrizable by lines if its projective closure is parametrizable by lines.

- Remarks.**
1. Note that in Definition 4.48 we have not required that the base point of \mathcal{H} is on the curve. Later, we will see that in fact the base point must lie on \mathcal{C} , unless \mathcal{C} is a line.
 2. Any line is parametrizable by lines (see Exercise 4.12).
 3. Note that an affine curve parametrizable by lines is in fact rational. Moreover, the implicit equation of \mathcal{C} vanishes on the generic intersection point depending rationally on the parameter. So, by Theorem 4.7, this generic point is a rational parametrization of \mathcal{C} . Furthermore, if the irreducibility condition in Definition 4.48 is not imposed, then the curve has a rational component (see Exercises 4.13 and 4.14).
 4. Let \mathcal{C} be an affine curve such that its associated projective curve \mathcal{C}^* is parametrizable by the linear system of lines $\mathcal{H}(t)$ of equation $L_1(x, y, z) - tL_2(x, y, z)$. Then, the affine parametrization of \mathcal{C} , generated by $\mathcal{H}(t)$, is proper and $\frac{L_1(x, y, 1)}{L_2(x, y, 1)}$ is its inverse (see Exercise 4.15). In fact, $\mathcal{H}(t)$ is a pencil of lines (Definition 2.53) and its base point is $L_1 \cap L_2$.

Theorem 4.49. *Let \mathcal{C} be an irreducible projective plane curve of degree $d > 1$. The following statements are equivalent:*

- (1) *\mathcal{C} is parametrizable by a pencil of lines $\mathcal{H}(t)$.*
- (2) *\mathcal{C} has a point of multiplicity $d - 1$ which is the base point of $\mathcal{H}(t)$.*

Proof. That (2) implies (1) follows from Definition 4.48 and Theorem 4.45. Conversely, let $L_1(x, y, z) - tL_2(x, y, z)$ be the defining polynomial of $\mathcal{H}(t)$, let $\mathcal{P}(t)$ be the proper parametrization derived from $\mathcal{H}(t)$, and let Q be the base point of $\mathcal{H}(t)$. Since $d > 1$, for almost all $t_0 \in K$, $\mathcal{H}(t_0)$ intersects \mathcal{C} in at least two points, and one of them is $\mathcal{P}(t_0)$. First we prove that $\mathcal{H}(t_0) \cap \mathcal{C} = \{\mathcal{P}(t_0), Q\}$ for almost all $t_0 \in K$. Let $P \in [\mathcal{H}(t_0) \cap \mathcal{C}] \setminus \mathcal{P}(t_0)$. If P is reachable by $\mathcal{P}(t)$, then there exists $t_1 \in K$, $t_1 \neq t_0$, such that $\mathcal{P}(t_1) = P$. This implies that $P \in \mathcal{H}(t_1) \cap \mathcal{H}(t_0)$. Therefore, $P = Q$. If P is not reachable, the inverse

of $\mathcal{P}(t)$ is not defined at P , and hence $L_2(P) = 0$. But, since $P \in \mathcal{H}(t_0)$, then $L_1(P) = 0$. Thus P is in all the lines of the system of lines $\mathcal{H}(t)$, so $P = Q$.

Now, since \mathcal{C} is irreducible, it has only finitely many singularities. Thus $\text{mult}_{\mathcal{P}(t_0)}(\mathcal{C}, \mathcal{H}(t_0)) = 1$ for almost all $t_0 \in K$. This implies, by Bézout's Theorem, that $\text{mult}_Q(\mathcal{C}, \mathcal{H}(t_0)) = d - 1$ for almost all $t_0 \in K$. Therefore, $d - 1 = \text{mult}_Q(\mathcal{C})$, i.e. the base point of $\mathcal{H}(t)$ is a point on \mathcal{C} of multiplicity $d - 1$. Thus, (1) implies (2). \square

We have seen that the inverse of an affine parametrization generated by the algorithm PARAMETRIZATION-BY-LINES is linear. In the next theorem we see that this phenomenon also characterizes the curves parametrizable by lines.

Theorem 4.50. *Let \mathcal{C} be an irreducible affine plane curve. The following statements are equivalent:*

- (1) \mathcal{C} is parametrizable by lines.
- (2) There exists a proper affine parametrization of \mathcal{C} with a linear inverse.
- (3) The inverse of any proper affine parametrization of \mathcal{C} is linear.

Proof. Let d be the degree of \mathcal{C} . If $d = 1$ the result is trivial. Let us assume that $d > 1$. If (1) holds, by Theorem 4.49 we know that \mathcal{C}^* has a $(d - 1)$ -fold point. Therefore, applying algorithm PARAMETRIZATION-BY-LINES one gets a proper affine parametrization of \mathcal{C} with linear inverse. Thus, (2) holds.

We prove now that (2) implies (3). Let $\mathcal{P}(t)$ be a proper affine parametrization with linear inverse, and let $\mathcal{P}'(t)$ be any other proper affine parametrization of \mathcal{C} . Because of Lemma 4.17 (2) there exists a linear rational function $L(t)$ such that $\mathcal{P}'(t) = \mathcal{P}(L(t))$. Therefore, $\mathcal{P}'^{-1} = L^{-1} \circ \mathcal{P}^{-1}$ is also linear.

Finally, we prove that (3) implies (1). Let $\mathcal{P}(t)$ be a proper affine parametrization of \mathcal{C} with a rational inverse of the form $(ax + by + c)/(a'x + b'y + c')$. Let $\mathcal{P}^*(t)$ be the projective parametrization generated by $\mathcal{P}(t)$. Then, we consider the pencil of lines $\mathcal{H}(t)$ defined by $H(x, y, z, t) = (ax + by + cz) - (a'x + b'y + c'z)t$. Clearly, $H(\mathcal{P}^*(t), t) = 0$. Thus, $\mathcal{P}^*(t) \in \mathcal{H}(t) \cap \mathcal{C}^*$. Therefore, \mathcal{C}^* is parametrizable by lines. \square

4.7 Parametrization by Adjoint Curves

In Theorem 4.11 we saw that only curves of genus 0 have any chance of being rationally parametrizable. In this section we conclude that the curves of genus 0 are exactly the rational curves.

In Theorem 4.49 we have seen that, in general, rational curves can not be parametrized by lines. In fact, we have proved that a rational curve \mathcal{C} of degree $d \geq 2$ is parametrizable by lines if and only if it has a $(d - 1)$ -fold point. In order to treat the general case, we develop here a method based on the notion of adjoint curves that, intuitively speaking, is a generalization of the

idea underlining the parametrization by lines method. The method described in this section follows basically the approach in [Wal50] and [SeW91]. There are alternative parametrization methods such as [VaH97] based on the computation of the anticanonical divisor, or [Sch92] where adjoints of high degree are used.

Throughout this section, \mathcal{C} will be an irreducible projective curve of degree $d > 2$ and genus 0. Note that this is not a loss of generality, because we have seen in the previous section that lines and irreducible conics can be parametrized by lines. Before showing how adjoints are defined and how they can be used to solve the parametrization problem, we first generalize the notion of parametrization by lines. We need to guarantee that every curve in the parametrizing system \mathcal{H} intersects \mathcal{C} in finitely many points. This is trivial when we parametrize by lines, but in the generalization it leads to an additional condition.

Definition 4.51. *A linear system of curves \mathcal{H} parametrizes \mathcal{C} iff*

- (1) $\dim(\mathcal{H}) = 1$,
- (2) *the intersection of a generic element in \mathcal{H} and \mathcal{C} contains a nonconstant point whose coordinates depend rationally on the free parameter in \mathcal{H} ,*
- (3) \mathcal{C} is not a component of any curve in \mathcal{H} .

In this case we say that \mathcal{C} is parametrizable by \mathcal{H} .

Lemma 4.52. *Let $\mathcal{H}(t)$ be a linear system of curves parametrizing \mathcal{C} , then there exists only one nonconstant intersection point of a generic element of $\mathcal{H}(t)$ and \mathcal{C} depending on t , and it is a proper parametrization of \mathcal{C} .*

Proof. By condition (2) in Definition 4.51 we know that there exists a non-constant point $\mathcal{P}(t)$ in $\mathcal{H}(t) \cap \mathcal{C}$ depending rationally on t . Let us see that $\mathcal{P}(t)$ is a proper parametrization of \mathcal{C} . It is clear that the defining polynomial of \mathcal{C} vanishes at it. Thus, $\mathcal{P}(t)$ is a parametrization of \mathcal{C} . In order to see that it is proper, we find the inverse of the affine parametrization $\mathcal{P}_{\star,z}(t)$ of $\mathcal{C}_{\star,z}$ generated by $\mathcal{P}(t)$. Let $H(t, x, y, z) = H_0(x, y, z) - tH_1(x, y, z)$ be the defining polynomial of $\mathcal{H}(t)$. Then, $H(t, \mathcal{P}(t)) = 0$. Moreover, $H_1(\mathcal{P}(t)) \neq 0$, because otherwise we would have that $H_0(\mathcal{P}(t)) = 0$, which is impossible because of condition (3) in Definition 4.51. Therefore, $M = H_0/H_1$ is defined at $\mathcal{P}(t)$ and $M(\mathcal{P}(t)) = t$. Thus, by Lemma 4.36, $M(x, y, 1)$ is the inverse of $\mathcal{P}_{\star,z}(t)$.

Finally, let us see that $\mathcal{P}(t)$ is unique. Let $\mathcal{Q}(t)$ be another intersection point depending rationally on t . By the argument above, we know that both are proper rational parametrizations, and that $\mathcal{P}_{\star,z}^{-1}(t) = \mathcal{Q}_{\star,z}^{-1}(t)$. Thus, $\mathcal{P}(t) = \mathcal{Q}(t)$. \square

Now let us see how to actually compute a parametrization from a parametrizing linear system of curves. For this purpose, for a polynomial G in $K[x, y, z][t]$ we use the notation $\text{pp}_t(G)$ to denote the primitive part of G w.r.t. t , i.e. G divided by the gcd of its coefficients.

Theorem 4.53. *Let $F(x, y, z)$ be the defining polynomial of \mathcal{C} , and let $H(t, x, y, z)$ be the defining polynomial of a linear system $\mathcal{H}(t)$ parametrizing \mathcal{C} . Then, the proper parametrization $\mathcal{P}(t)$ generated by $\mathcal{H}(t)$ is the solution in $\mathbb{P}^2(K(t))$ of the system of algebraic equations*

$$\left. \begin{aligned} \text{pp}_t(\text{res}_y(F, H)) &= 0 \\ \text{pp}_t(\text{res}_x(F, H)) &= 0 \end{aligned} \right\}.$$

Proof. Let $\{P_1, \dots, P_s, \mathcal{P}(t)\}$ be the intersection points of $\mathcal{H}(t)$ and \mathcal{C} . By Lemma 4.52 we know that $P_i \in \mathbb{P}^2(K)$ and $\mathcal{P}(t) \in \mathbb{P}^2(K(t))$. Let $P_i = (a_i : b_i : c_i)$ and $\mathcal{P}(t) = (\chi_1(t), \chi_2(t), \chi_3(t))$. Condition (3) in Definition 4.51 implies that $\text{res}_y(F, H)$ and $\text{res}_x(F, H)$ are not identically zero. Furthermore, from Bézout's Theorem we get that

$$\begin{aligned} \text{res}_y(F, H) &= (\chi_3(t)x - \chi_1(t)z)^\beta \prod_{i=1}^s (c_i x - a_i z)^{\alpha_i} \\ \text{res}_x(F, H) &= (\chi_3(t)y - \chi_2(t)z)^{\beta'} \prod_{i=1}^s (c_i y - b_i z)^{\alpha'_i} \end{aligned}$$

for some $\alpha_i, \alpha'_i, \beta, \beta' \in \mathbb{N}$. So, obviously, the parametrization is determined by the primitive parts of these resultants. \square

The following theorem gives sufficient conditions for a linear system of curves to be a parametrizing system.

Theorem 4.54. *Let \mathcal{H} be a linear system of curves of degree k and let \mathcal{B} be the set of base points of \mathcal{H} (cf. Definition 2.54). If*

- (1) $\dim(\mathcal{H}) = 1$,
- (2) $\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') = dk - 1$ for almost all curves $\mathcal{C}' \in \mathcal{H}$, and
- (3) \mathcal{C} is not a component of any curve in \mathcal{H} ,

then \mathcal{H} parametrizes \mathcal{C} .

Proof. We just have to prove that condition (2) in the statement of the theorem implies condition (2) in Definition 4.51. By condition (3) we know that \mathcal{C} is not a component of any curve in \mathcal{H} . Thus, by Bézout's Theorem and condition (2) we see that $(\mathcal{C}' \cap \mathcal{C}) \setminus \mathcal{B}$ consists of a single point for almost all $\mathcal{C}' \in \mathcal{H}$. Therefore, this point depends rationally on the parameter of \mathcal{H} . \square

Now, the natural question is how to determine parametrizing linear systems of curves. We will show that adjoints provide an answer to this question. Adjoint curves can be defined for reducible curves. However, since our final goal is to work with rational curves, we will only consider irreducible curves. For the reducible case we refer to [BrK86], [Ful89], [Wal50].

Before we introduce the notion of adjoint curves and establish some of their important properties, we remind the reader of some of the notation introduced in Sect. 3.2 concerning the blowing up of curves:

1. $\text{Sing}(\mathcal{C})$ denotes the singular locus of \mathcal{C} .
2. $\text{Ngr}(\mathcal{C})$ denotes the neighboring graph of \mathcal{C} , i.e. $\text{Ngr}(\mathcal{C})$ comprises the singularities and neighboring singularities of \mathcal{C} .
3. For $P \in \text{Sing}(\mathcal{C})$, $\text{Ngr}_P(\mathcal{C})$ denotes the subgraph of $\text{Ngr}(\mathcal{C})$ with root at P .
4. For $P \in \text{Ngr}(\mathcal{C})$ we denote by \mathcal{Q}_P the sequence of quadratic transformations and linear transformations generating the neighborhood where P belongs to. Moreover, for any projective curve \mathcal{C}' we denote by $\mathcal{Q}_P(\mathcal{C}')$ the quadratic transform of \mathcal{C}' by \mathcal{Q}_P .

Definition 4.55. A projective curve \mathcal{C}' is an adjoint curve of the irreducible projective curve \mathcal{C} iff $\text{mult}_P(\mathcal{Q}_P(\mathcal{C}')) \geq \text{mult}_P(\mathcal{Q}_P(\mathcal{C})) - 1$ for every $P \in \text{Ngr}(\mathcal{C})$. We say that \mathcal{C}' is an adjoint curve of degree k of \mathcal{C} , if \mathcal{C}' is an adjoint of \mathcal{C} and $\deg(\mathcal{C}') = k$.

All algebraic conditions required in the definition of adjoint curves are linear. Therefore if one fixes the degree, the set of all adjoint curves of \mathcal{C} is a linear system of curves (see Sect. 2.4). In fact, if \mathcal{C} has only ordinary singularities, then the set of adjoint curves of degree k of \mathcal{C} is the linear system generated by the effective divisor

$$\sum_{P \in \text{Sing}(\mathcal{C})} (\text{mult}_P(\mathcal{C}) - 1)P.$$

This remark motivates the following definition.

Definition 4.56. The set of all adjoints of \mathcal{C} of degree k , $k \in \mathbb{N}$, is called the system of adjoints of \mathcal{C} of degree k . We denote this system by $\mathcal{A}_k(\mathcal{C})$.

Theorem 4.57. Let \mathcal{C} be a projective curve of degree d and genus 0, and let $k \geq d - 2$, then $\mathcal{A}_k(\mathcal{C}) \neq \emptyset$.

Proof. The full linear system of curves of degree k has dimension $k(k + 3)/2$ (cf. Sect. 2.4). Since $\text{genus}(\mathcal{C}) = 0$, the number of linear conditions required by $\mathcal{A}_k(\mathcal{C})$ is

$$\sum_{P \in \text{Ngr}(\mathcal{Q}_P(\mathcal{C}))} \frac{\text{mult}_P(\mathcal{Q}_P(\mathcal{C}))(\text{mult}_P(\mathcal{Q}_P(\mathcal{C})) - 1)}{2} = \frac{(d - 1)(d - 2)}{2}.$$

Therefore,

$$\dim(\mathcal{A}_k(\mathcal{C})) \geq \frac{k(k + 3)}{2} - \frac{(d - 1)(d - 2)}{2}$$

(compare to Theorem 2.59 for the case of curves with only ordinary singularities). Now, if $k \geq d - 2$, then $\dim(\mathcal{A}_k(\mathcal{C})) \geq d - 2 > 0$ and hence $\mathcal{A}_k(\mathcal{C}) \neq \emptyset$. \square

In [Noe83], Sect. 50, the dimension of the linear system of adjoints of an irreducible curve is determined. Applying this result one has the following result.

Theorem 4.58. *Let \mathcal{C} be a projective curve of degree d and genus 0, and let $k \geq d - 2$, then*

$$\dim(\mathcal{A}_k(\mathcal{C})) = \frac{k(k+3)}{2} - \frac{(d-1)(d-2)}{2}.$$

Now, we proceed to show how from linear systems of adjoint curves we may generate parametrizing linear systems. For this purpose, we first prove two preliminary lemmas. In the first one, if $\mathcal{C}_1, \mathcal{C}_2$ are projective curves defined respectively by the forms F_1, F_2 , we denote by $\mathcal{C}_1\mathcal{C}_2$ the curve defined by F_1F_2 , and by $\lambda\mathcal{C}_1 + \mu\mathcal{C}_2$ the curve defined by $\lambda F_1 + \mu F_2$ where $\lambda, \mu \in K$, assuming that the corresponding polynomial is not identically zero.

Lemma 4.59. *Let \mathcal{C} be an irreducible projective curve of degree d , let $k \in \{d, d-1, d-2\}$, let $\mathcal{F} \subset \mathcal{C} \setminus \text{Sing}(\mathcal{C})$ be a finite set and let*

$$\mathcal{H}_k := \mathcal{A}_k(\mathcal{C}) \cap \mathcal{H}(k, \sum_{P \in \mathcal{F}} P).$$

Then the following hold:

- (1) *If $k = d$, for every $\mathcal{C}' \in \mathcal{H}_d$, and for almost all $(\lambda, \mu) \in K^2$ we have $\mu\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}_d$, and $\mu\mathcal{C}' + \lambda\mathcal{C}$ does not have multiple components.*
- (2) *If we take a fixed $k \in \{d-1, d-2\}$, then for every $\mathcal{C}' \in \mathcal{H}_k$, for every projective curve \mathcal{M} of degree $d-k$, and for almost all $(\lambda, \mu) \in K^2$ we have*

$$\mu\mathcal{M}\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}_d \cap \mathcal{H}(d, \sum_{P \in \mathcal{M} \cap \mathcal{C}} P),$$

and $\mu\mathcal{M}\mathcal{C}' + \lambda\mathcal{C}$ does not have multiple components.

Proof. If $\mathcal{H}_k = \emptyset$, then there is nothing to prove. Let us assume that $\mathcal{H}_k \neq \emptyset$. Let F, G, M be the defining polynomials of $\mathcal{C}, \mathcal{C}', \mathcal{M}$, respectively.

In order to prove Statement (1), we first observe that if $\mathcal{C}' = \mathcal{C}$ the result trivially holds for $\lambda, \mu \in K$ such that $\lambda + \mu \neq 0$. Let us assume that $\mathcal{C}' \neq \mathcal{C}$. We observe that $\mathcal{C}', \mathcal{C} \in \mathcal{H}_d$. Therefore, since \mathcal{H}_d is a projective linear variety, if λ, μ are such that $\mu G + \lambda F$ is not identically zero, then $\mu\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}_d$. Moreover, since $\mathcal{C}' \neq \mathcal{C}$, for all $(\lambda, \mu) \in \Omega_1 := K^2 \setminus \{(0, 0)\}$ we have that $\mu G + \lambda F$ is not identically zero. Let us prove the second part of Statement (1). For this purpose, we take the polynomial $A(\lambda, \mu, x, y, z) := \mu G + \lambda F$, where λ, μ are considered as formal parameters. Let us see that A is irreducible as a polynomial in $\mathbb{K}[\lambda, \mu, x, y, z]$. Indeed, if it factors, since A is linear in $\{\lambda, \mu\}$, one factor belongs to $\mathbb{K}[x, y, z]$. But this implies that F is either reducible or $F = G$ up to constant, which is impossible since F is irreducible and we have assumed that $\mathcal{C}' \neq \mathcal{C}$. Moreover, taking into account that F is irreducible and nonlinear (lines have been excluded), A does depend on $\{x, y, z\}$, and hence A can be seen as a nonconstant polynomial in $K[\lambda, \mu, x, y][z]$. Now, because of the irreducibility of A , one has that A is primitive w.r.t. z , and it

is square-free. Therefore, by Theorem 8.1, p. 338, in [GCL92], the discriminant of A w.r.t. z is not identically zero. Thus, computing this discriminant, we find a nonempty open Zariski subset Ω_2 of K^2 , such that $A(\lambda_0, \mu_0, x, y, z)$ is squarefree for every $(\lambda_0, \mu_0) \in \Omega_2$. So, for every $(\lambda, \mu) \in \Omega_1 \cap \Omega_2$, which is nonempty because K^2 is irreducible, we have that $\mu\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}_d$, and $\mu\mathcal{C}' + \lambda\mathcal{C}$ does not have multiple components.

Let us prove Statement (2). F is irreducible and $k < d$, so $\mu MG + \lambda F$ is identically zero if and only if $\lambda = \mu = 0$. We prove that if $(\lambda, \mu) \neq (0, 0)$ then $\mu\mathcal{M}\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}_d \cap \mathcal{H}(d, \sum_{P \in \mathcal{M} \cap \mathcal{C}} P)$. Indeed:

- (i) Let us see that $\mu\mathcal{M}\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}(d, \sum_{P \in \mathcal{F}} P)$. Clearly, $\mathcal{C} \in \mathcal{H}(d, \sum_{P \in \mathcal{F}} P)$. Moreover, by hypothesis, $\mathcal{C}' \in \mathcal{H}(k, \sum_{P \in \mathcal{F}} P)$, hence $\text{mult}_P(\mathcal{C}') \geq 1$ for $P \in \mathcal{F}$. Furthermore, $\text{mult}_P(\mathcal{M}\mathcal{C}') = \text{mult}_P(\mathcal{M}) + \text{mult}_P(\mathcal{C}') \geq 1$ for $P \in \mathcal{F}$ (see Exercise 2.10). So, since $\deg(\mathcal{M}\mathcal{C}') = d$, one gets that $\mathcal{M}\mathcal{C}' \in \mathcal{H}(d, \sum_{P \in \mathcal{F}} P)$. Now, the statement follows from the linearity of $\mathcal{H}(d, \sum_{P \in \mathcal{F}} P)$; note that $\mu MG + \lambda F$ is not identically zero.
- (ii) Reasoning similarly as in (i) we deduce that $\mu\mathcal{M}\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}(d, \sum_{P \in \mathcal{M} \cap \mathcal{C}} P)$.
- (iii) Let us see that $\mu\mathcal{M}\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{A}_d(\mathcal{C})$. First, we observe that $\mathcal{C} \in \mathcal{A}_d(\mathcal{C})$, so we have to prove that $\mathcal{M}\mathcal{C}' \in \mathcal{A}_d(\mathcal{C})$. For this purpose, we first note that $\deg(\mathcal{M}\mathcal{C}') = d$. We analyze separately the required conditions on the singularities and on the neighboring points (see Definition 4.55).
 - (iii.i) Let $P \in \text{Sing}(\mathcal{C})$. Then, taking into account that $\mathcal{C}' \in \mathcal{A}_k(\mathcal{C})$, we have

$$\text{mult}_P(\mathcal{M}\mathcal{C}') = \text{mult}_P(\mathcal{M}) + \text{mult}_P(\mathcal{C}') \geq \text{mult}_P(\mathcal{C}') \geq \text{mult}_P(\mathcal{C}) - 1.$$
 - (iii.ii) Let $P \in \text{Ngr}(\mathcal{C})$, and let \mathcal{Q}_P as above. Observe that $\mathcal{Q}_P(\mathcal{M}\mathcal{C}') = \mathcal{Q}_P(\mathcal{M})\mathcal{Q}_P(\mathcal{C}')$. Therefore,

$$\begin{aligned} \text{mult}_P(\mathcal{Q}_P(\mathcal{M}\mathcal{C}')) &= \text{mult}_P(\mathcal{Q}_P(\mathcal{M})\mathcal{Q}_P(\mathcal{C}')) = \\ &= \text{mult}_P(\mathcal{Q}_P(\mathcal{M})) + \text{mult}_P(\mathcal{Q}_P(\mathcal{C}')) \geq \text{mult}_P(\mathcal{Q}_P(\mathcal{C}')) \\ &\geq \text{mult}_P(\mathcal{Q}_P(\mathcal{C})) - 1. \end{aligned}$$

Summarizing, we get that if $(\lambda, \mu) \neq (0, 0)$ then $\mu\mathcal{M}\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}_d \cap \mathcal{H}(d, \sum_{P \in \mathcal{M} \cap \mathcal{C}} P)$. In order to prove that for almost all $(\lambda, \mu) \in K^2$ the curve $\mu\mathcal{M}\mathcal{C}' + \lambda\mathcal{C}$ does not have multiple components, one reasons analogously as in the proof of Statement (1). In this case, $A(\lambda, \mu, x, y, z) := \mu MG + \lambda F$. \square

The following lemma can be found in [Wal50] Chap. III, Theorem 7.6.

Lemma 4.60. *Let \mathcal{C}_1 and \mathcal{C}_2 be two projective curves of degrees d_1 and d_2 respectively, having no common components and neither \mathcal{C}_1 nor \mathcal{C}_2 having any multiple components. Then*

$$d_1 d_2 \geq \sum_{\substack{P \in \text{Ngr}_{P'}(\mathcal{C}_1) \\ P' \in \mathcal{C}_1 \cap \mathcal{C}_2}} \text{mult}_P(\mathcal{Q}_P(\mathcal{C}_1)) \text{mult}_P(\mathcal{Q}_P(\mathcal{C}_2)),$$

where $\text{Ngr}_{P'}(\mathcal{C}_1) = \{P'\}$ if $P' \in [\mathcal{C}_1 \cap \mathcal{C}_2] \setminus \text{Sing}(\mathcal{C}_1)$.

Now, we show how from linear systems of adjoint curves we may generate parametrizing linear systems.

Theorem 4.61. *Let \mathcal{C} be a projective curve of degree d and genus 0, let $k \in \{d-1, d-2\}$, and let $\mathcal{S}_k \subset \mathcal{C} \setminus \text{Sing}(\mathcal{C})$ be such that $\text{card}(\mathcal{S}_k) = kd - (d-1)(d-2) - 1$. Then*

$$\mathcal{A}_k(\mathcal{C}) \cap \mathcal{H}(k, \sum_{P \in \mathcal{S}_k} P)$$

parametrizes \mathcal{C} .

Proof. Let $\mathcal{H} = \mathcal{A}_k(\mathcal{C}) \cap \mathcal{H}(k, \sum_{P \in \mathcal{S}_k} P)$. We check whether the conditions in Theorem 4.54 are satisfied. Note that Condition (3) holds trivially, because \mathcal{C} is irreducible and $k < d$. Let us check Condition (1), i.e. $\dim(\mathcal{H}) = 1$. $\dim(\mathcal{H}) \geq \dim(\mathcal{A}_k(\mathcal{C})) - [kd - (d-1)(d-2) - 1]$, and by Theorem 4.58 we know that $\dim(\mathcal{H}) \geq 1$. Now, let us assume that $\dim(\mathcal{H}) > 1$. We take two different points $Q_1, Q_2 \in \mathcal{C} \setminus (\text{Sing}(\mathcal{C}) \cup \mathcal{S}_k)$, and we consider the linear subsystem

$$\mathcal{H}' = \mathcal{H} \cap \mathcal{H}(k, Q_1 + Q_2).$$

Observe that $\dim(\mathcal{H}') \geq 0$. Thus, $\mathcal{H}' \neq \emptyset$. Let $\mathcal{C}' \in \mathcal{H}'$. Since $\deg(\mathcal{C}') < \deg(\mathcal{C})$ and \mathcal{C} is irreducible, we know that \mathcal{C}' and \mathcal{C} do not have common components. Now, we distinguish two different cases:

- (i) If \mathcal{C}' does not have multiple components, then since \mathcal{C} does not have common components either, by Lemma 4.60 and the fact that $\text{genus}(\mathcal{C}) = 0$, we get that

$$\begin{aligned} kd &\geq \\ \sum_{P \in \text{Ngr}(\mathcal{C})} \text{mult}_P(Q_P(\mathcal{C})) \text{mult}_P(Q_P(\mathcal{C}')) + \sum_{P \in \mathcal{S}_k \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}') &\geq \\ \sum_{P \in \text{Ngr}(\mathcal{C})} \text{mult}_P(Q_P(\mathcal{C})) (\text{mult}_P(Q_P(\mathcal{C})) - 1) + \sum_{P \in \mathcal{S}_k \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}') & \\ \geq (d-1)(d-2) + [kd - (d-1)(d-2) - 1] + 2 = kd + 1, & \end{aligned}$$

which is impossible.

- (ii) Let us assume that \mathcal{C}' has multiple components. Then, we consider $d-k$ different lines $\mathcal{L}_1, \dots, \mathcal{L}_{d-k}$ such that \mathcal{L}_i and \mathcal{C} intersects in d different points and

$$(\mathcal{L}_i \cap \mathcal{C}) \cap (\text{Sing}(\mathcal{C}) \cup \mathcal{S}_k \cup \{Q_1, Q_2\} \cup_{j \neq i} (\mathcal{L}_j \cap \mathcal{C})) = \emptyset.$$

Let L_i be the defining polynomial of \mathcal{L}_i and let \mathcal{M} be the curve of defining polynomial $L_1 \cdots L_{d-k}$. Now, applying Lemma 4.59 (2) to \mathcal{C} and taking \mathcal{F} as $\mathcal{S}_k \cup \{Q_1, Q_2\}$, we take $\lambda, \mu \in K$ such that

$$\mathcal{C}'' := \mu \mathcal{M} \mathcal{C}' + \lambda \mathcal{C} \in \mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, \sum_{P \in \mathcal{S}_k \cup \{Q_1, Q_2\}} P) \cap \mathcal{H}(d, \sum_{P \in \mathcal{M} \cap \mathcal{C}} P),$$

and \mathcal{C}'' does not have common components. In this situation we apply Lemma 4.60 to \mathcal{C}'' and \mathcal{C} ; note that \mathcal{C}'' and \mathcal{C} do not have common components because both curves have the same degree and \mathcal{C} is irreducible. So

$$\begin{aligned}
d^2 &\geq \\
&\sum_{P \in \text{Ngr}(\mathcal{C})} \text{mult}_P(Q_P(\mathcal{C})) \text{mult}_P(Q_P(\mathcal{C}'')) + \sum_{P \in \mathcal{S}_k \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}'') + \\
&\sum_{P \in \mathcal{M} \cap \mathcal{C}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}'') \geq \sum_{P \in \text{Ngr}(\mathcal{C})} \text{mult}_P(Q_P(\mathcal{C})) (\text{mult}_P(Q_P(\mathcal{C})) - 1) \\
&\quad + \sum_{P \in \mathcal{S}_k \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}'') + d(d - k) \\
&= (d - 1)(d - 2) + \sum_{P \in \mathcal{S}_k \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}'') + d(d - k) \\
&\geq (d - 1)(d - 2) + [kd - (d - 1)(d - 2) - 1] + 2 + d(d - k) \\
&= kd + 1 + d(d - k) = d^2 + 1,
\end{aligned}$$

which is impossible.

Now, let us check that Condition (2) holds in Theorem 4.54. For this purpose, we first prove that the set of base points \mathcal{B} of \mathcal{H} is $\text{Sing}(\mathcal{C}) \cup \mathcal{S}_k$. It is clear that $\text{Sing}(\mathcal{C}) \cup \mathcal{S}_k \subset \mathcal{B}$. Let us assume that $\mathcal{B} \neq \text{Sing}(\mathcal{C}) \cup \mathcal{S}_k$, so there exists $Q \in \mathcal{B} \setminus (\text{Sing}(\mathcal{C}) \cup \mathcal{S}_k)$. We choose a curve $\mathcal{C}' \in \mathcal{H}$ passing through a point $Q' \in \mathcal{C} \setminus \mathcal{B}$. This is possible because $\dim(\mathcal{H}) = 1$. Then, since \mathcal{C} and \mathcal{C}' do not have common components, we argue similarly as above distinguishing two different cases:

- (i) Let \mathcal{C}' be without multiple components. Since \mathcal{C} does not have multiple components either, we can apply Lemma 4.60. Reasoning as in (i) above, we arrive at the contradiction $kd \geq kd + 1$. Thus, $\mathcal{B} = \text{Sing}(\mathcal{C}) \cup \mathcal{S}_k$.
- (ii) Let us assume that \mathcal{C}' has multiple components. We consider $d - k$ different lines $\mathcal{L}_1, \dots, \mathcal{L}_{d-k}$ such that \mathcal{L}_i and \mathcal{C} intersect in d different points and

$$(\mathcal{L}_i \cap \mathcal{C}) \cap (\text{Sing}(\mathcal{C}) \cup \mathcal{S}_k \cup \{Q, Q'\} \cup_{j \neq i} (\mathcal{L}_j \cap \mathcal{C})) = \emptyset.$$

Let L_i be the defining polynomial of \mathcal{L}_i and let \mathcal{M} be the curve defined by $L_1 \cdots L_{d-k}$. Now, applying Lemma 4.59 (2) to \mathcal{C} and taking \mathcal{F} as $\mathcal{S}_k \cup \{Q, Q'\}$, we take $\lambda, \mu \in K$ such that

$$\mathcal{C}'' := \mu \mathcal{M} \mathcal{C}' + \lambda \mathcal{C} \in \mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, \sum_{P \in \mathcal{S}_k \cup \{Q, Q'\}} P) \cap \mathcal{H}(d, \sum_{p \in \mathcal{M} \cap \mathcal{C}} P),$$

and \mathcal{C}'' does not have multiple components. In this situation we apply Lemma 4.60 to \mathcal{C}'' and \mathcal{C} ; note that \mathcal{C}'' and \mathcal{C} do not have common components because both curves have the same degree and \mathcal{C} is irreducible. So, reasoning as in (ii) above, we arrive at the contradiction $d^2 \geq d^2 + 1$. Thus, $\mathcal{B} = \text{Sing}(\mathcal{C}) \cup \mathcal{S}_k$.

Now that we have proved that $\mathcal{B} = \text{Sing}(\mathcal{C}) \cup \mathcal{S}_k$, we show that Statement (2) in Theorem 4.54 holds. That is, we have to prove

$$\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') = dk - 1$$

for almost all $\mathcal{C}' \in \mathcal{H}$. We structure the proof as follows: First, we prove that for all $\mathcal{C}' \in \mathcal{H}$ we have

$$\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') \geq dk - 1.$$

Second, we show that there exists at least one curve $\mathcal{C}' \in \mathcal{H}$ such that

$$\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') = dk - 1,$$

and finally we show that the equality holds for almost all curves in \mathcal{H} .

- (a) Let us assume that there exists $\mathcal{C}' \in \mathcal{H}$ such that the sum of multiplicities of intersection at \mathcal{B} is equal to $dk - \ell$, where $\ell > 1$. Then, since \mathcal{C} and \mathcal{C}' do not have common components, by Bézout Theorem we deduce that there exists a set of points $\mathcal{E} \subset (\mathcal{C} \cap \mathcal{C}') \setminus \mathcal{B}$ such that

$$\sum_{P \in \mathcal{E}} \text{mult}_P(\mathcal{C}, \mathcal{C}') = \ell.$$

Now we argue similarly as above distinguishing two different cases:

- (a.1) Let \mathcal{C}' be without multiple components. Since \mathcal{C} does not have multiple components either, we can apply Lemma 4.60. Reasoning as in (i) above, and using the fact that $\mathcal{B} = \text{Sing}(\mathcal{C}) \cup \mathcal{S}_k$, we derive $kd \geq kd + \ell - 1$, which is impossible since $\ell > 1$.
- (a.2) Let us assume that \mathcal{C}' has multiple components. Then, we consider $d - k$ different lines $\mathcal{L}_1, \dots, \mathcal{L}_{d-k}$ such that \mathcal{L}_i and \mathcal{C} intersect in d different points and

$$(\mathcal{L}_i \cap \mathcal{C}) \cap (\text{Sing}(\mathcal{C}) \cup \mathcal{S}_k \cup \mathcal{E} \cup_{j \neq i} (\mathcal{L}_j \cap \mathcal{C})) = \emptyset.$$

Let L_i be the defining polynomial of \mathcal{L}_i and let \mathcal{M} be the curve of defining polynomial $L_1 \cdots L_{d-k}$. Now, applying Lemma 4.59(2) to \mathcal{C} , and taking \mathcal{F} as $\mathcal{S}_k \cup \mathcal{A}$, we take $\lambda, \mu \in K$ such that

$$\mathcal{C}'' := \mu \mathcal{M} \mathcal{C}' + \lambda \mathcal{C} \in \mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, \sum_{P \in \mathcal{S}_k \cup \mathcal{A}} P) \cap \mathcal{H}(d, \sum_{p \in \mathcal{M} \cap \mathcal{C}} P),$$

and \mathcal{C}'' does not have multiple components. In this situation we apply Lemma 4.60 to \mathcal{C}'' and \mathcal{C} ; note that \mathcal{C}'' and \mathcal{C} do not have common components because both curves have the same degree and \mathcal{C} is irreducible. So, reasoning as in (ii), we derive $d^2 \geq d^2 + \ell - 1$, which is impossible since $\ell > 1$.

- (b) Let us assume that for all curves in \mathcal{H} the sum of multiplicities of intersection at \mathcal{B} is dk . Then, since $\dim(\mathcal{H}) = 1$, we consider a point $Q \in \mathcal{C} \setminus \mathcal{B}$, and we take $\mathcal{C}' \in \mathcal{H}$ such that $Q \in \mathcal{C}'$. In this situation we have

$$\sum_{P \in \mathcal{C}' \cap \mathcal{C}} \text{mult}_P(\mathcal{C}, \mathcal{C}') \geq \sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') + \text{mult}_Q(\mathcal{C}, \mathcal{C}') \geq dk + 1.$$

Therefore, by Bézout's theorem, the curves \mathcal{C} and \mathcal{C}' have a common component, which is impossible.

- (c) Let $\mathcal{C}' \in \mathcal{H}$ be the curve whose existence ensures step (b) of our reasoning. Since the sum of multiplicities of intersection at \mathcal{B} is $dk - 1$, and since \mathcal{C}' and \mathcal{C} do not have common components, by Bézout's theorem we know that $\mathcal{C} \cap \mathcal{C}' = \mathcal{B} \cup \{Q\}$, where $Q := (a : b : c) \notin \mathcal{B}$. Now, let $H(t_0, t_1, x, y, z) := t_0 G_0 + t_1 G_1$ be the defining polynomial of a generic element in \mathcal{H} , where we assume w.l.o.g. that G_0 is the defining polynomial of \mathcal{C}' . Furthermore we assume w.l.o.g., probably after performing a suitable linear change of coordinates, that $F(0, 0, 1) \neq 0$, $G_i(0, 0, 1) \neq 0$, and that $(0 : 0 : 1)$ is not on any line connecting two different points in $\mathcal{B} \cup \{Q\}$. Note that if $F(0, 0, 1) \neq 0$ then, in particular, one has that the leading coefficient of F w.r.t. z is constant and that $(0 : 0 : 1) \notin \mathcal{B} \cup \{Q\}$. Also, condition $G_i(0, 0, 1) \neq 0$ implies that $(0 : 0 : 1)$ is neither on \mathcal{C}' nor on the curve defined by H over the algebraic closure of $K(t_0, t_1)$. Then let $R(t_0, t_1, x, y) := \text{res}_z(H, F)$. Taking into account the previous steps (a) and (b), one has that R factors as

$$R(t_0, t_1, x, y) = (\alpha_2(t_0, t_1)x - \alpha_1(t_0, t_1)y) \prod_{(a_i : b_i : c_i) \in \mathcal{B}} (b_i x - a_i y)^{r_i},$$

where $\sum r_i = dk - 1$.

Now, for every i we introduce the polynomials $\delta_i(t_0, t_1) = \alpha_2 a_i - \alpha_1 b_i$. Let us see that none of these polynomials is identically zero. For this purpose, we first observe that, since the leading coefficient of F w.r.t. z is constant, the resultant specializes properly and therefore $(\alpha_2(1, 0)x - \alpha_1(1, 0)y) = \lambda(bx - ay)$ for some $\lambda \in K^*$. Therefore if δ_i is identically zero then $ba_i - ab_i = 0$, which is impossible because $(0 : 0 : 1)$ is not on any line connecting a point in \mathcal{B} and Q . We consider the set

$$\Omega = \{(t_0, t_1) \in K^2 \setminus \{(0, 0)\} \mid \prod \delta_i(t_0, t_1) \neq 0\}.$$

Note that Ω is open and nonempty. Moreover, because of the construction, for every $(t_0, t_1) \in \Omega$, if \mathcal{C}'' is the curve defined by $H(t_0, t_1, x, y, z)$, then

$$\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}'') = dk - 1. \quad \square$$

Theorem 4.62. *Let \mathcal{C} be a projective curve of degree d and genus 0, let $Q \notin \mathcal{C}$, and let $\mathcal{S}_d \subset \mathcal{C} \setminus \text{Sing}(\mathcal{C})$ be such that $\text{card}(\mathcal{S}_d) = 3(d-1)$. Then*

$$\mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, Q + \sum_{P \in \mathcal{S}_d} P)$$

parametrizes \mathcal{C} .

Proof. Let $\mathcal{H} = \mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, \sum_{P \in \mathcal{S}_d} P + Q)$. We prove that the conditions in Theorem 4.54 are satisfied. First, we observe that for every $\mathcal{C}' \in \mathcal{H}$, since $\deg(\mathcal{C}) = \deg(\mathcal{C}')$, since $Q \in \mathcal{C}'$ but $Q \notin \mathcal{C}$, and since \mathcal{C} is irreducible, the curves \mathcal{C} and \mathcal{C}' do not have common components. Therefore, Condition (3) holds.

Let us now check Condition (1), i.e. $\dim(\mathcal{H}) = 1$. Since $\dim(\mathcal{H}) \geq \dim(\mathcal{A}_d(\mathcal{C})) - [3(d-1)] - 1$, by Theorem 4.58, we know that $\dim(\mathcal{H}) \geq 1$. Now, let us assume that $\dim(\mathcal{H}) > 1$. Then, we take two different points $Q_1, Q_2 \in \mathcal{C} \setminus (\text{Sing}(\mathcal{C}) \cup \mathcal{S}_d)$, and we consider the linear subsystem

$$\mathcal{H}' = \mathcal{H} \cap \mathcal{H}(d, Q_1 + Q_2).$$

Observe that $\dim(\mathcal{H}') \geq 0$. Thus, $\mathcal{H}' \neq \emptyset$. Let $\mathcal{C}' \in \mathcal{H}'$. Note that, since $\mathcal{C}' \in \mathcal{H}' \subset \mathcal{H}$, reasoning as above one has that \mathcal{C}' and \mathcal{C} do not have common components. Now, we distinguish two different cases:

- (i) If \mathcal{C}' does not have multiple components, then since \mathcal{C} does not have common components either, applying Lemma 4.60 and that $\text{genus}(\mathcal{C}) = 0$, one has that (note that $Q \notin \mathcal{C} \cap \mathcal{C}'$)

$$\begin{aligned} d^2 &\geq \\ &\sum_{P \in \text{Ngr}(\mathcal{C})} \text{mult}_P(Q_P(\mathcal{C})) \text{mult}_P(Q_P(\mathcal{C}')) + \sum_{P \in \mathcal{S}_d \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}') \geq \\ &\sum_{P \in \text{Ngr}(\mathcal{C})} \text{mult}_P(Q_P(\mathcal{C})) (\text{mult}_P(Q_P(\mathcal{C})) - 1) + \sum_{P \in \mathcal{S}_d \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}') \\ &= (d-1)(d-2) + \sum_{P \in \mathcal{S}_d \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}') \\ &\geq (d-1)(d-2) + 3(d-1) + 2 = d^2 + 1, \end{aligned}$$

which is impossible.

- (ii) Let us assume that \mathcal{C}' has multiple components. Then, we consider the linear system $\mathcal{H}^* := \mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, \sum_{P \in \mathcal{S}_d} P) \cap \mathcal{H}(d, Q_1 + Q_2)$. We observe that, since $\mathcal{C}' \in \mathcal{H}'$, then $\mathcal{C}' \in \mathcal{H}^*$. Now, we apply Lemma 4.59(1) to \mathcal{C} and $\mathcal{F} := \mathcal{S}_d \cup \{Q_1, Q_2\}$, and we take $\lambda, \mu \in K$ such that

$$\mathcal{C}'' := \mu \mathcal{C}' + \lambda \mathcal{C} \in \mathcal{H}^*,$$

and such that \mathcal{C}'' does not have common components. In this situation we apply Lemma 4.60 to \mathcal{C}'' and \mathcal{C} ; note that \mathcal{C}'' and \mathcal{C} do not have common components because otherwise this would imply that \mathcal{C}' and \mathcal{C} have a common component, which is a contradiction.

$$\begin{aligned}
d^2 &\geq \\
&\sum_{P \in \text{Ngr}(\mathcal{C})} \text{mult}_P(Q_P(\mathcal{C})) \text{mult}_P(Q_P(\mathcal{C}'')) + \sum_{P \in \mathcal{S}_d \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}'') \geq \\
&\sum_{P \in \text{Ngr}(\mathcal{C})} \text{mult}_P(Q_P(\mathcal{C})) (\text{mult}_P(Q_P(\mathcal{C})) - 1) + \sum_{P \in \mathcal{S}_d \cup \{Q_1, Q_2\}} \text{mult}_P(\mathcal{C}) \text{mult}_P(\mathcal{C}'') \\
&\geq (d-1)(d-2) + 3(d-1) + 2 = d^2 + 1,
\end{aligned}$$

which is impossible.

Now, let us check whether Condition (2) in Theorem 4.54 holds. For this purpose, we first prove that the set of base points \mathcal{B} of \mathcal{H} is $\text{Sing}(\mathcal{C}) \cup \mathcal{S}_d \cup \{Q\}$. It is clear that $\text{Sing}(\mathcal{C}) \cup \mathcal{S}_d \cup \{Q\} \subset \mathcal{B}$. Let us assume that $\mathcal{B} \neq \text{Sing}(\mathcal{C}) \cup \mathcal{S}_d \cup \{Q\}$. Then there exists $R \in \mathcal{B} \setminus (\text{Sing}(\mathcal{C}) \cup \mathcal{S}_d \cup \{Q\})$. We choose a curve $\mathcal{C}' \in \mathcal{H}$ passing through a point $R' \in \mathcal{C} \setminus \mathcal{B}$. This is possible because $\dim(\mathcal{H}) = 1$. Then, since \mathcal{C} and \mathcal{C}' do not have common components, we argue similarly as above distinguishing two different cases:

- (i) Let \mathcal{C}' be without multiple components. Since \mathcal{C} does not have common components either, we can apply Lemma 4.60. Reasoning as in (i) above, we arrive at the contradiction $d^2 \geq d^2 + 1$. Thus, $\mathcal{B} = \text{Sing}(\mathcal{C}) \cup \mathcal{S}_d \cup \{Q\}$.
- (ii) Let us assume that \mathcal{C}' has multiple components. Then, we consider the linear system $\mathcal{H}^* := \mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, \sum_{P \in \mathcal{S}_d} P) \cap \mathcal{H}(d, R + R')$. We observe that, since $\mathcal{C}' \in \mathcal{H} \cap \mathcal{H}(d, R + R')$, then $\mathcal{C}' \in \mathcal{H}^*$. Now, we apply Lemma 4.59(1) to \mathcal{C} and $\mathcal{F} := \mathcal{S}_d \cup \{R, R'\}$, and we take $\lambda, \mu \in K$ such that

$$\mathcal{C}'' := \mu \mathcal{C}' + \lambda \mathcal{C} \in \mathcal{H}^*,$$

and \mathcal{C}'' does not have multiple components. In this situation we apply Lemma 4.60 to \mathcal{C}'' and \mathcal{C} ; note that \mathcal{C}'' and \mathcal{C} do not have common components because otherwise it would imply that \mathcal{C}' and \mathcal{C} have a common component, which is not the case. Now, reasoning as in (ii) above, we arrive at the contradiction $d^2 \geq d^2 + 1$. Thus, $\mathcal{B} = \text{Sing}(\mathcal{C}) \cup \mathcal{S}_d \cup \{Q\}$.

Once we have proved that $\mathcal{B} = \text{Sing}(\mathcal{C}) \cup \mathcal{S}_d \cup \{Q\}$, we show that Statement (2) in Theorem 4.54 holds. That is, we have to prove that for almost all $\mathcal{C}' \in \mathcal{H}$ one has that

$$\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') = d^2 - 1.$$

We structure the proof as follows: First, we prove that for all $\mathcal{C}' \in \mathcal{H}$ it holds that

$$\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') \geq d^2 - 1.$$

Second, we show that there exists at least one curve $\mathcal{C}' \in \mathcal{H}$ such that

$$\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') = d^2 - 1,$$

and finally we show that the equality holds for almost all curves in \mathcal{H} .

- (a) Let us assume that there exists $\mathcal{C}' \in \mathcal{H}$ such that the sum of multiplicities of intersection at \mathcal{B} is equal to $d^2 - \ell$, where $\ell > 1$. Then, since \mathcal{C} and \mathcal{C}' do not have common components, by Bézout Theorem we deduce that there exists a set of points $\mathcal{E} \subset (\mathcal{C} \cap \mathcal{C}') \setminus \mathcal{B}$ such that

$$\sum_{P \in \mathcal{E}} \text{mult}_P(\mathcal{C}, \mathcal{C}') = \ell.$$

Now we argue similarly as above distinguishing two different cases:

- (a.1) Let \mathcal{C}' be without multiple components. Since \mathcal{C} does not have multiple components either, we can apply Lemma 4.60. Reasoning as in (i) above, and using the fact that $\mathcal{B} = \text{Sing}(\mathcal{C}) \cup \mathcal{S}_k$, we derive $d^2 \geq d^2 + \ell - 1$, which is impossible since $\ell > 1$.
- (a.2) Let us assume that \mathcal{C}' has multiple components. Then, we consider the linear system $\mathcal{H}^* := \mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, \sum_{P \in \mathcal{S}_d} P)$. We observe that, since $\mathcal{C}' \in \mathcal{H}$, then $\mathcal{C}' \in \mathcal{H}^*$. Now, we apply Lemma 4.59(1) to \mathcal{C} and $\mathcal{F} := \mathcal{S}_d$, and we take $\lambda, \mu \in K$ such that

$$\mathcal{C}'' := \mu\mathcal{C}' + \lambda\mathcal{C} \in \mathcal{H}^*,$$

and \mathcal{C}'' does not have multiple components. In this situation we apply Lemma 4.60 to \mathcal{C}'' and \mathcal{C} ; note that \mathcal{C}'' and \mathcal{C} do not have common components because otherwise also \mathcal{C}' and \mathcal{C} would have common components, which we have excluded. Also, note that by assumption $\mathcal{E} \subset \mathcal{C}' \cap \mathcal{C}$, and therefore $\mathcal{E} \subset \mathcal{C}'' \cap \mathcal{C}$. So, reasoning as in (ii), we derive $d^2 \geq d^2 + \ell - 1$, which is impossible since $\ell > 1$.

- (b) Let us assume that for all curves in \mathcal{H} the sum of multiplicities of intersection is d^2 . Then, since $\dim(\mathcal{H}) = 1$, we consider a point $R \in \mathcal{C} \setminus \mathcal{B}$, and we take $\mathcal{C}' \in \mathcal{H}$ such that $R \in \mathcal{C}'$. In this situation we have

$$\sum_{P \in \mathcal{C}' \cap \mathcal{C}} \text{mult}_P(\mathcal{C}, \mathcal{C}') \geq \sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}') + \text{mult}_R(\mathcal{C}, \mathcal{C}') \geq d^2 + 1.$$

Therefore, by Bézout's theorem, the curves \mathcal{C} and \mathcal{C}' have a common component, which is impossible.

- (c) Let $\mathcal{C}' \in \mathcal{H}$ be the curve whose existence ensures step (b) of our reasoning. Since the sum of multiplicities of intersection at \mathcal{B} is $d^2 - 1$, since \mathcal{C}' and \mathcal{C} do not have common components, and since $Q \in \mathcal{B}$ but $Q \notin \mathcal{C} \cap \mathcal{C}'$, by Bézout's theorem we know that $\mathcal{C} \cap \mathcal{C}' = (\mathcal{B} \setminus \{Q\}) \cup \{R\}$, where $R := (a : b : c) \notin \mathcal{B}$. Now, let $H(t_0, t_1, x, y, z) := t_0 G_0 + t_1 G_1$ be the defining polynomial of a generic element in \mathcal{H} , where we assume w.l.o.g. that G_0 is the defining polynomial of \mathcal{C}' , and let F be the defining polynomial of \mathcal{C} . We assume w.l.o.g., probably after performing a suitable linear change of coordinates, that $F(0, 0, 1) \neq 0$, $G_i(0, 0, 1) \neq 0$, and that $(0 : 0 : 1)$ is not on any line connecting two different points in $(\mathcal{B} \setminus \{Q\}) \cup \{R\}$. Note that if $F(0, 0, 1) \neq 0$ then, in particular, one has that the leading coefficient of F w.r.t. z is constant and that $(0 : 0 : 1) \notin (\mathcal{B} \setminus \{Q\}) \cup \{R\}$. Also, condition $G_i(0, 0, 1) \neq 0$ implies that $(0 : 0 : 1)$ is neither on \mathcal{C}' nor on the curve defined by H over the algebraic closure of $K(t_0, t_1)$. Then let $R(t_0, t_1, x, y) := \text{res}_z(H, F)$. Taking into account the previous steps (a) and (b) one has that R factors as

$$R(t_0, t_1, x, y) = (\alpha_2(t_0, t_1)x - \alpha_1(t_0, t_1)y) \prod_{(a_i : b_i : c_i) \in \mathcal{B} \setminus \{Q\}} (b_i x - a_i y)^{r_i},$$

where $\sum r_i = d^2 - 1$.

Now, for every i we introduce the polynomials $\delta_i(t_0, t_1) = \alpha_2 a_i - \alpha_1 b_i$. Let us see that none of these polynomials is identically zero. For this purpose, we first observe that, since the leading coefficient of F w.r.t. z is constant, the resultant specializes properly and therefore $(\alpha_2(1, 0)x - \alpha_1(1, 0)y) = \lambda(bx - ay)$ for some $\lambda \in K^*$. Therefore if δ_i is identically zero then $ba_i - ab_i = 0$ which is impossible because $(0 : 0 : 1)$ is not on any line connecting a point in $(\mathcal{B} \setminus \{Q\})$ and R . We consider the set

$$\Omega = \{(t_0, t_1) \in K^2 \setminus \{(0, 0)\} \mid \prod \delta_i(t_0, t_1) \neq 0\}.$$

Note that Ω is open and nonempty. Moreover, because of the construction, for every $(t_0, t_1) \in \Omega$, if \mathcal{C}'' is the curve defined by $H(t_0, t_1, x, y, z)$, then

$$\sum_{P \in \mathcal{B}} \text{mult}_P(\mathcal{C}, \mathcal{C}'') = d^2 - 1. \quad \square$$

From these theorems, one deduces the following result:

Theorem 4.63. *An algebraic curve \mathcal{C} is rational if and only if $\text{genus}(\mathcal{C}) = 0$.*

Proof. One implication is already stated in Theorem 4.11. In this section we have developed an algorithm which can parametrize every curve of genus 0. \square

The results proved in this section provide a family of algorithms for parametrizing any rational curve by means of adjoints.

Algorithm PARAMETRIZATION-BY-ADJOINTS.

Given the defining polynomial $F(x, y, z)$ of an irreducible projective curve \mathcal{C} of degree d and genus 0, the algorithm computes a rational parametrization of \mathcal{C} .

1. If $d \leq 3$ or $\text{Sing}(\mathcal{C})$ contains exactly one point of multiplicity $d - 1$, apply algorithm PARAMETRIZATION-BY-LINES.
2. Choose $k \in \{d - 2, d - 1, d\}$ and compute the defining polynomial of $\mathcal{A}_k(\mathcal{C})$.
3. Choose a set $\mathcal{S} \subset (\mathcal{C} \setminus \text{Sing}(\mathcal{C}))$ such that $\text{card}(\mathcal{S}) = kd - (d - 1)(d - 2) - 1$.
4. If $k < d$ then
 - compute the defining polynomial H of $\mathcal{A}_k(\mathcal{C}) \cap \mathcal{H}(k, \sum_{P \in \mathcal{S}} P)$;
 - else (i.e. $k = d$)
 - choose $Q \notin \mathcal{C}$ and
 - compute the defining polynomial H of $\mathcal{A}_k(\mathcal{C}) \cap \mathcal{H}(k, Q + \sum_{P \in \mathcal{S}} P)$.
5. Set one of the parameters in H to 1 and let t be the remaining parameter in H . Return the solution in $\mathbb{P}^2(K(t))$ of $\{\text{pp}_t(\text{res}_y(F, H)) = 0, \text{pp}_t(\text{res}_x(F, H)) = 0\}$.

From the point of view of time efficiency one must choose $k = d - 2$ in Step 2, since then degrees of polynomials are the smallest. Nevertheless, the selection of $k = d$ can be also interesting in the sense that at most one algebraic number of degree d has to be introduced (see Theorem 4.72), and therefore it is a first approach to algebraic optimality of the output (see Chap. 5). In the next section, we will consider the algebraic extensions of the field of definition required by the parametrization algorithm. But first, we illustrate the algorithm by two examples.

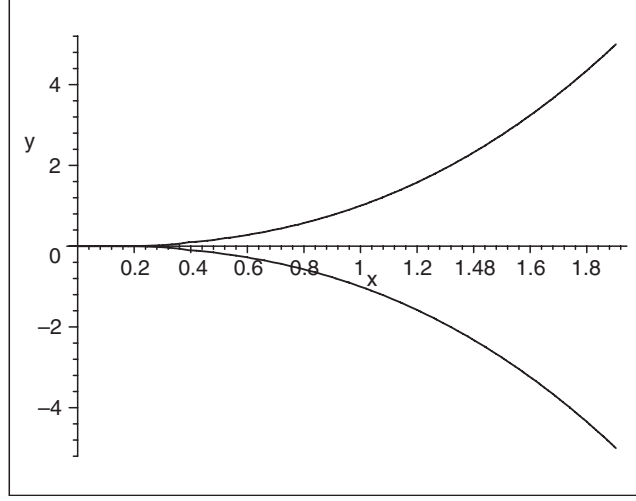
Example 4.64. Let \mathcal{C} be the quintic over \mathbb{C} (see Figure 4.3) of defining polynomial (see Example 3.13)

$$F(x, y, z) = y^2 z^3 - x^5.$$

From the implicit equation it is clear that $(t^2, t^5, 1)$ is a parametrization of \mathcal{C} . Nevertheless, let us see how the algorithm works. In Example 3.13 we have determined that

$$\text{Sing}(\mathcal{C}) = \{(0 : 1 : 0), (0 : 0 : 1)\},$$

where $P_1 = (0 : 1 : 0)$ is a triple nonordinary point, and $P_2 = (0 : 0 : 1)$ is a nonordinary double point. Furthermore, in Example 3.13 the neighboring graph of \mathcal{C} was computed. We have obtained that $P_{1,1} = (1 : 1 : 0)$ is an ordinary double point in the first neighborhood of P_1 , $P_{2,1} = (1 : 1 : 0)$ is a nonordinary double point in the first neighborhood of P_2 , and $P_{2,2} = (-2 : 1 : 0)$ is a simple point in the second neighborhood of P_2 .

**Fig. 4.3.** $\mathcal{C}_{*,z}$

Therefore, $\text{genus}(\mathcal{C}) = 0$, and hence \mathcal{C} is rational (see Theorem 4.63). We proceed to parametrize the curve. In Step 2 we choose $k = d - 2 = 3$. In order to compute $\mathcal{A}_k(\mathcal{C})$, we consider a generic form in $\{x, y, z\}$ of degree 3:

$$H = a_{00} z^3 + a_{01} yz^2 + a_{02} y^2 z + a_{03} y^3 + a_{10} xz^2 + a_{11} xyz + a_{12} xy^2 + a_{20} x^2 z + a_{21} x^2 y + a_{30} x^3.$$

First, we require P_1 to be a double point on $\mathcal{A}_3(\mathcal{C})$, and P_2 to be a simple point on $\mathcal{A}_3(\mathcal{C})$. That is, we consider the equations:

$$\left\{ \frac{\partial H}{\partial x}(P_1) = 0, \frac{\partial H}{\partial y}(P_1) = 0, \frac{\partial H}{\partial z}(P_1) = 0, H(P_2) = 0 \right\}.$$

Solving the linear system of equations in $a_{i,j}$ derived from the system above one gets:

$$H = a_{01} yz^2 + a_{10} xz^2 + a_{11} xyz + a_{20} x^2 z + a_{21} x^2 y + a_{30} x^3$$

Next, we consider the neighboring points. That is, we impose that

$$\{ \mathcal{Q}_{P_1}(H)(P_{1,1}) = 0, \mathcal{Q}_{P_2}(H)(P_{2,1}) = 0 \}.$$

This leads to

$$H = a_{01} yz^2 + a_{11} xyz + a_{20} x^2 z + a_{30} x^3,$$

as the defining polynomial of $\mathcal{A}_3(\mathcal{C})$.

In Step 3 we choose a set $\mathcal{S} \subset (\mathcal{C} \setminus \text{Sing}(\mathcal{C}))$ with 2 points, namely

$$\mathcal{S} = \{(1 : 1 : 1), (1 : -1 : 1)\}.$$

In Step 4 we compute the defining polynomial of $\mathcal{A}_3(\mathcal{C}) \cap \mathcal{H}(3, Q_1 + Q_2)$, where $Q_1 = (1 : 1 : 1)$ and $Q_2 = (1 : -1 : 1)$. That is, we solve the equations

$$H(1, 1, 1) = 0, H(1, -1, 1) = 0,$$

which leads to

$$H(x, y, z) = -a_{11}yz^2 + a_{11}xyz - x^2za_{30} + a_{30}x^3.$$

Setting $a_{11} = 1, a_{30} = t$, we get the defining polynomial

$$H(t, x, y, z) = -yz^2 + xyz - x^2zt + tx^3$$

of the parametrizing system. Finally, in Step 5, the solution of the system

$$\begin{cases} -x + t^2z = 0 \\ -y + t^5z = 0 \end{cases}$$

provides the parametrization

$$\mathcal{P}(t) = (t^2, t^5, 1).$$

Example 4.65. Let \mathcal{C} be the quartic over \mathbb{C} (see Fig. 4.4) of

$$F(x, y, z) = -2xy^2z - 48x^2z^2 + 4xyz^2 - 2x^3z + x^3y - 6y^4 + 48y^2z^2 + 6x^4.$$

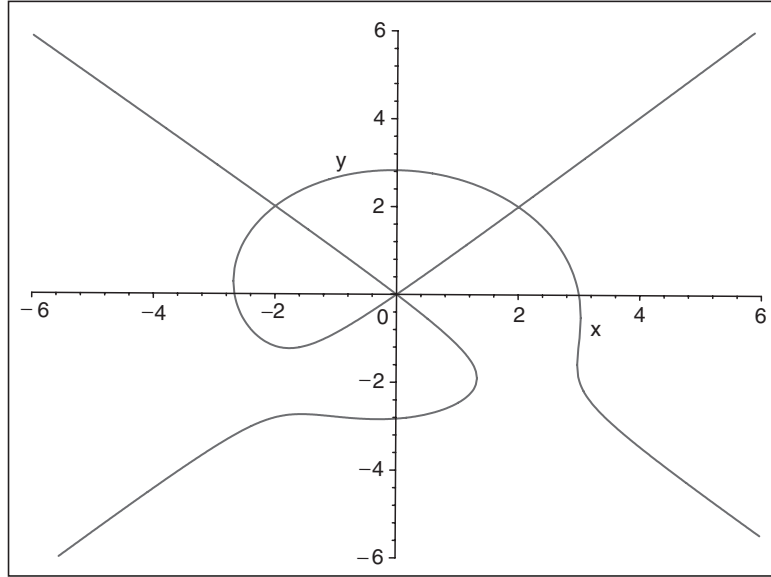


Fig. 4.4. $\mathcal{C}_{*,z}$

The singular locus of \mathcal{C} is

$$\text{Sing}(\mathcal{C}) = \{(0 : 0 : 1), (2 : 2 : 1), (-2 : 2 : 1)\},$$

all three points being double points. Therefore, $\text{genus}(\mathcal{C}) = 0$, and hence \mathcal{C} is rational (see Theorem 4.63). Note that no blowing up is required. We proceed to parametrize the curve. In Step 2 we choose $k = d - 2 = 2$. The defining polynomial of $\mathcal{A}_2(\mathcal{C})$ is

$$H(x, y, z) = (-2a_{02} - 2a_{20})yz + a_{02}y^2 - 2a_{11}xz + a_{1,1}xy + a_{20}x^2.$$

In Step 3 we choose a set $\mathcal{S} \subset (\mathcal{C} \setminus \text{Sing}(\mathcal{C}))$ with 1 point, namely $\mathcal{S} = \{(3 : 0 : 1)\}$. In Step 4, we compute the defining polynomial of $\mathcal{H} := \mathcal{A}_2(\mathcal{C}) \cap \mathcal{H}(2, Q)$, where $Q = (3 : 0 : 1)$. This leads to

$$H(x, y, z) = (-2a_{02} - 2a_{20})yz + a_{02}y^2 - 3a_{20}xz + \frac{3}{2}a_{20}xy + a_{20}x^2.$$

Setting $a_{02} = 1, a_{20} = t$, we get the defining polynomial

$$H(t, x, y, z) = (-2 - 2t)yz + y^2 - 3txz + \frac{3}{2}txy + tx^2$$

of the parametrizing system. Finally, in Step 5, the solution of the system defined by the resultants provides the following affine parametrization of \mathcal{C} : $\mathcal{P}(t) =$

$$\left(12 \frac{9t^4 + t^3 - 51t^2 + t + 8}{126t^4 - 297t^3 + 72t^2 + 8t - 36}, -2 \frac{t(162t^3 - 459t^2 + 145t + 136)}{126t^4 - 297t^3 + 72t^2 + 8t - 36} \right).$$

4.8 Symbolic Treatment of Parametrization

In algorithm PARAMETRIZATION-BY-ADJOINTS we have described how to parametrize rational curves. However, from the symbolic point of view, we still want to clarify some steps. For instance, we want to explain how to symbolically compute the system of adjoints, and how to choose and manipulate the simple points that are taken in Step 3 of the algorithm. Obviously, one can always approach the problem directly, by introducing algebraic numbers and carrying out all computations over algebraic extensions of the ground field. However, we take here a different approach, using the notion of a family of conjugate points (see Definition 3.15). This means that we do not need to work with individual points, and hence we save time in computation.

In Sect. 3.3 we have seen how to symbolically analyze the genus by introducing families of conjugate points. In this section we show how to use the standard decomposition of the singularities to compute linear systems of adjoints, and we describe a first approach for choosing the simple points.

In the next chapter, we will develop an optimal approach for the choice of the necessary simple points.

Throughout this section, we assume that \mathcal{C} is a projective rational curve of degree d , and that its not necessarily algebraically closed ground field \mathbb{K} (see Definition 3.14) is a computable field.

We start by proving that linear systems of adjoint curves can be computed without extending \mathbb{K} .

Theorem 4.66. *Let \mathcal{C} be a rational projective curve of degree d and ground field \mathbb{K} . Then \mathbb{K} is also the ground field of $\mathcal{A}_k(\mathcal{C})$, $k \geq d - 2$.*

Proof. The linear system of adjoints $\mathcal{A}_k(\mathcal{C})$ can be expressed as

$$\mathcal{A}_k(\mathcal{C}) = \mathcal{H}(k, \sum_{P \in \mathcal{D}(\text{Ngr}(\mathcal{C}))} (\text{mult}_P(Q_P(\mathcal{C})) - 1) \cdot P),$$

where $\mathcal{D}(\text{Ngr}(\mathcal{C}))$ is the standard decomposition of the neighboring graph of \mathcal{C} (see Definition 3.27). Observe that all the transformations for dealing with the neighboring graph of \mathcal{C} are performed over the ground field. So Theorem 3.26 and Lemma 3.19 yield the result. \square

Combining the results in Sect. 4.6 and Theorem 4.66, we can guarantee that the output of Step 2 in algorithm PARAMETRIZATION-BY-ADJOINTS is defined over \mathbb{K} . In Step 3 we have to compute simple points on \mathcal{C} . In Chap. 5 we will see that we can find such points in a field extension of \mathbb{K} of degree at most 2. Here we prove a more modest result, namely that we can always parametrize using a field extension of \mathbb{K} of degree at most d . Note that if the simple points are taken randomly, and adjoints of degree $d - 2$ are considered, then in general a field extension of degree $(d - 3)^d$ has to be introduced. Moreover, this bound is even worse if adjoints of higher degree are used.

Lemma 4.67. *Let P be a simple point on an irreducible projective curve \mathcal{C} of degree $d > 1$. There exist at most $d(d - 1)$ tangents to \mathcal{C} , at a simple point on \mathcal{C} , passing through P .*

Proof. We assume w.l.o.g. that $P = (0 : 0 : 1)$. If $Q \in \mathcal{C} \setminus \text{Sing}(\mathcal{C})$, then the tangent to \mathcal{C} at Q is given by

$$x \frac{\partial F}{\partial x}(Q) + y \frac{\partial F}{\partial y}(Q) + z \frac{\partial F}{\partial z}(Q) = 0,$$

where F is the defining polynomial of \mathcal{C} (see Theorem 2.13). Thus, the simple points of \mathcal{C} with tangent passing through P are solutions of $\{\frac{\partial F}{\partial z} = 0, F = 0\}$. Since F is irreducible and since $\partial F / \partial z$ has total degree $d - 1$, according to Bézout's Theorem there are at most $d(d - 1)$ different solutions. \square

In the following we show how the simple points in algorithm PARAMETRIZATION-BY-ADJOINTS can be taken in families of conjugate points for different options of the degree of the adjoint curves.

Theorem 4.68 (Parametrizing with adjoints of degree $d-2$). *If algorithm PARAMETRIZATION-BY-ADJOINTS is performed with adjoints of degree $k = d-2$, the set \mathcal{S} of simple points in Step 3 of the algorithm can be taken as a family of conjugate points over a field extension of \mathbb{K} of degree at most $d(d-1)(d-2)$.*

Proof. Let $F(x, y, z) \in \mathbb{K}[x, y, z]$ be the defining polynomial of \mathcal{C} . The theorem obviously holds for curves of degree ≤ 4 . So w.l.o.g. we may assume that $\deg(\mathcal{C}) > 4$. Note that $\text{card}(\mathcal{S}) = d-3$ in Step 3. Take $b_1, b_2 \in \mathbb{K}$ such that no singular point of \mathcal{C} is of the form $(b_1 : b_2 : c)$. Now, compute an irreducible factor $p_1(t)$ of $F(b_1, b_2, t)$ over \mathbb{K} . Then,

$$P_1 = (b_1 : b_2 : \beta_1) \in \mathbb{P}^2(\mathbb{K}(\beta_1)),$$

where $p_1(\beta_1) = 0$, is a simple point of \mathcal{C} . Note that $\deg(p_1) \leq d$. In this situation, choose $\lambda, \mu \in \mathbb{K}$ such that:

- (1) $b_1 \neq \lambda\beta_1, b_2 \neq \mu\beta_1$,
- (2) $\text{res}_t \left(\bar{q}(t), \frac{\partial \bar{q}}{\partial t} \right) \neq 0$, where $\bar{q}(t) = F(\lambda t + b_1, \mu t + b_2, t + \beta_1) \in \mathbb{K}(\beta_1)[t]$.

Condition (2) implies that the line $\mathcal{L} = \{(\lambda t + b_1 : \mu t + b_2 : t + \beta_1) \mid t \in K\}$ does not pass through the singularities and that \mathcal{L} is not tangent to \mathcal{C} . The reason for Condition (1) will become clear later. Note that Lemma 4.67 implies that Condition (2) can always be achieved. Condition (1) is clearly reachable. Now, we consider the polynomial

$$q(t) = \frac{\bar{q}(t)}{t} \in \mathbb{K}(\beta_1)[t]$$

(note that $\bar{q}(0) = F(P_1) = 0$), and choose an irreducible factor $p_2(t)$ over $\mathbb{K}(\beta_1)$ of $q(t)$. Thus, from the above construction we deduce that

$$P_2 = (\lambda\beta_2 + b_1 : \mu\beta_2 + b_2 : \beta_2 + \beta_1) \in \mathbb{P}^2(\mathbb{K}(\beta_1, \beta_2)),$$

where $p_2(\beta_2) = 0$, is a simple point of \mathcal{C} because of (2). Note that $\deg(p_2) \leq d-1$. Then, we introduce the polynomial

$$q^*(t) = \frac{q(t)}{t - \beta_2} \in \mathbb{K}(\beta_1, \beta_2)[t].$$

Take an irreducible factor $p_3(t)$ of $q^*(t)$ over $\mathbb{K}(\beta_1, \beta_2)$, and consider the point

$$P_3 = (\lambda\beta_3 + b_1 : \mu\beta_3 + b_2 : \beta_3 + \beta_1) \in \mathbb{P}^2(\mathbb{K}(\beta_1, \beta_2, \beta_3)),$$

where $p_3(\beta_3) = 0$. Note that $\deg(p_3) \leq d-2$. Observe that P_3 is a simple point on \mathcal{C} because of (2). Finally, we introduce the polynomial

$$m(t) = \frac{q^*(t)}{t - \beta_3} \in \mathbb{K}(\beta_1, \beta_2, \beta_3)[t].$$

In this situation, we claim that

$$\mathcal{F} = \{(\lambda t + b_1 : \mu t + b_2 : t + \beta_1)\}_{m(t)}$$

is a family of $(d - 3)$ conjugate simple points on \mathcal{C} over $\mathbb{K}(\beta_1, \beta_2, \beta_3)$. First, note that $m(t) \in \mathbb{K}(\beta_1, \beta_2, \beta_3)[t]$, thus \mathcal{F} contains conjugate points over $\mathbb{K}(\beta_1, \beta_2, \beta_3)$. Moreover, because of Condition (1), the coordinate polynomials in \mathcal{F} are coprime and with coefficients in $\mathbb{K}(\beta_1) \subset \mathbb{K}(\beta_1, \beta_2, \beta_3)$. Hence, Condition (1) in Definition 3.15 is satisfied. Furthermore, by construction $\bar{q}(t)$ is squarefree. Thus, since $m(t)$ is a factor of $\bar{q}(t)$, also $m(t)$ must be squarefree. So Condition (2) in Definition 3.15 is satisfied. Moreover $\deg(\bar{q}(t)) = d > 4$, hence $\deg(m(t)) = d - 3 > 1$ and the degree of the polynomials defining the coordinates of \mathcal{F} is 1. Thus, Condition (3) in Definition 3.15 is also satisfied. Now, we check that $\text{card}(\mathcal{F}) = d - 3$. Let α_1, α_2 be two different roots of $m(t)$, and let P_{α_i} be the point in \mathcal{F} generated by the root α_i . If $\alpha_1 = -\beta_1$ then $\alpha_2 \neq -\beta_1$ and hence $P_{\alpha_1} \neq P_{\alpha_2}$ (similarly if $\alpha_2 = -\beta_1$). Let α_1, α_2 be different from $-\beta_1$. Then $P_{\alpha_1} = P_{\alpha_2}$ implies

$$\frac{\lambda\alpha_1 + b_1}{\alpha_1 + \beta_1} = \frac{\lambda\alpha_2 + b_1}{\alpha_2 + \beta_1}, \quad \frac{\mu\alpha_1 + b_2}{\alpha_1 + \beta_1} = \frac{\mu\alpha_2 + b_2}{\alpha_2 + \beta_1}.$$

Since $\alpha_1 \neq \alpha_2$, this implies $\lambda\beta_1 = b_1$ and $\mu\beta_1 = b_2$, which is impossible because of Condition (1) in the construction. Summarizing, \mathcal{F} is a family of $(d - 3)$ conjugate simple points over $\mathbb{K}(\beta_1, \beta_2, \beta_3)$, which is an extension of \mathbb{K} of degree at most $d(d - 1)(d - 2)$. \square

Corollary 4.69. *If algorithm PARAMETRIZATION-BY-ADJOINTS is performed with adjoints of degree $k = d - 2$, and \mathcal{S} in Step 3 of the algorithm is taken as in Theorem 4.68, the algorithm outputs a parametrization over a field extension of \mathbb{K} of degree at most $d(d - 1)(d - 2)$.*

Proof. In Theorem 4.66 we have seen that the defining polynomial of $\mathcal{A}_{d-2}(\mathcal{C})$ has coefficients over \mathbb{K} . By Theorem 4.68, points in \mathcal{S} are in a family of conjugate points over a field extension \mathbb{L} of \mathbb{K} of degree at most $d(d - 1)(d - 2)$. Thus, by Lemma 3.19 the defining polynomial of

$$\mathcal{A}_{d-2}(\mathcal{C}) \cap \mathcal{H} \left(d - 2, \sum_{P \in \mathcal{S}} P \right)$$

has coefficients in \mathbb{L} . Therefore, the resultant polynomials in Step 5 are over \mathbb{L} , and hence also the parametrization. \square

Theorem 4.70 (Parametrizing with adjoints of degree $d - 1$). *If algorithm PARAMETRIZATION-BY-ADJOINTS is performed with adjoints of degree $k = d - 1$, the set \mathcal{S} of simple points in Step 3 of the algorithm can be taken as the union of two families of conjugate points over a field extension of \mathbb{K} of degree at most $d(d - 1)$.*

Proof. Let $F(x, y, z) \in \mathbb{K}[x, y, z]$ be the defining polynomial of \mathcal{C} . The theorem obviously holds for curves of degree ≤ 4 . So w.l.o.g. we may assume that $\deg(\mathcal{C}) > 4$. Note that $\text{card}(\mathcal{S}) = 2d - 3 = (d - 1) + (d - 2)$ in Step 3. Then, the idea is to express \mathcal{S} as the union of two families of conjugate simple points, one with $(d - 2)$ points and the other with $(d - 1)$. More precisely, take $b_1, b_2 \in \mathbb{K}$ such that no singular point of \mathcal{C} is of the form $(b_1 : b_2 : c)$. Now, compute an irreducible factor $p_1(t)$ of $F(b_1, b_2, t)$ over \mathbb{K} . Then,

$$P_1 = (b_1 : b_2 : \beta_1) \in \mathbb{P}^2(\mathbb{K}(\beta_1)),$$

where $p_1(\beta_1) = 0$, is a simple point of \mathcal{C} . Note that $\deg(p_1) \leq d$. In this situation, choose $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{K}$ such that:

- (1) $\lambda_1\mu_2 \neq \lambda_2\mu_1$, $b_1 \neq \lambda_i\beta_1$, $b_2 \neq \mu_i\beta_1$ for $i = 1, 2$,
- (2) $\text{res}_t \left(\overline{q_i}(t), \frac{\partial \overline{q_i}}{\partial t} \right) \neq 0$, for $i = 1, 2$, where $\overline{q_i}(t) = F(\lambda_i t + b_1, \mu_i t + b_2, t + \beta_1) \in \mathbb{K}(\beta_1)[t]$.

Condition (1) implies in particular that the lines $\mathcal{L}_i = \{(\lambda_i t + b_1 : \mu_i t + b_2 : t + \beta_1) \mid t \in K\}$ are different. Condition (2) guarantees that the lines \mathcal{L}_i do not pass through any singularities and that \mathcal{L}_i is not tangent to \mathcal{C} . Note that Lemma 4.67 implies that Condition (2) can always be achieved. Condition (1) is easily reachable. Now, we consider the polynomials

$$q_i(t) = \frac{\overline{q_i}(t)}{t} \in \mathbb{K}(\beta_1)[t], \quad i = 1, 2,$$

(note that $\overline{q_i}(0) = F(P_1) = 0$). We claim that

$$\mathcal{F}_1 = \{(\lambda_1 t + b_1 : \mu_1 t + b_2 : t + \beta_1)\}_{q_1(t)}$$

is a family of $(d - 1)$ conjugate simple points on \mathcal{C} over $\mathbb{K}(\beta_1)$. The proof of this fact is similar to the proof of Theorem 4.68 and we leave it to the reader.

In order to generate the second family we use $q_2(t)$. More precisely, let $p_2(t)$ be an irreducible factor of $q_2(t)$ over $\mathbb{K}(\beta_1)$. Then, we introduce the point

$$P_2 = (\lambda_2\beta_2 + b_1 : \mu_2\beta_2 + b_2 : \beta_2 + \beta_1),$$

where $p_2(\beta_2) = 0$. Note that $\deg(p_2) \leq d - 1$. $P_2 \in \mathcal{L}_2 \cap \mathcal{C}$, and therefore it is a simple point on \mathcal{C} . Now, we take

$$m(t) = \frac{q_2(t)}{t - \beta_2} \in \mathbb{K}(\beta_1, \beta_2)[t].$$

Then, reasoning similarly as above, we deduce that

$$\mathcal{F}_2 = \{(\lambda_2 t + b_1 : \mu_2 t + b_2 : t + \beta_1)\}_{m(t)}$$

is a family of $(d - 2)$ conjugate simple points on \mathcal{C} over $\mathbb{K}(\beta_1, \beta_2)$. Thus, we have expressed \mathcal{S} as $\mathcal{F}_1 \cup \mathcal{F}_2$. The only thing that we still have to prove is that $\mathcal{F}_1 \cap \mathcal{F}_2 = \emptyset$. Indeed, $\mathcal{L}_1 \cap \mathcal{L}_2 = \{P_1\}$, and $\mathcal{F}_i \subset \mathcal{L}_i \cap \mathcal{C}$. Thus the only common point of \mathcal{F}_1 and \mathcal{F}_2 is P_1 . But the root corresponding to P_1 has been crossed out in both polynomials defining the families. \square

Corollary 4.71. *If algorithm PARAMETRIZATION-BY-ADJOINTS is performed with adjoints of degree $k = d-1$, and \mathcal{S} in Step 3 of the algorithm is taken as in Theorem 4.70, the algorithm outputs a parametrization over a field extension of \mathbb{K} of degree at most $d(d-1)$.*

Proof. Similar to the proof of Corollary 4.69. \square

Theorem 4.72 (Parametrizing with adjoints of degree d). *If algorithm PARAMETRIZATION-BY-ADJOINTS is performed with adjoints of degree $k = d$, the set \mathcal{S} of simple points in Step 3 of the algorithm can be taken as the union of three families of conjugate points over a field extension of \mathbb{K} of degree at most d .*

Proof. Let $F(x, y, z) \in \mathbb{K}[x, y, z]$ be the defining polynomial of \mathcal{C} . As in the previous proofs we may assume w.l.o.g. that $\deg(\mathcal{C}) > 4$. Note that $\text{card}(\mathcal{S}) = 3(d-1)$ in Step 3. The idea is to express \mathcal{S} as the union of three families of $(d-1)$ conjugate points. For this purpose, we proceed as in the previous theorems. We take a simple point on the curve. This implies, in general, an extension of degree d , and we consider three lines through this point. More precisely, take $b_1, b_2 \in \mathbb{K}$ such that no singular point of \mathcal{C} is of the form $(b_1 : b_2 : c)$. Now, compute an irreducible factor $p_1(t)$ of $F(b_1, b_2, t)$ over \mathbb{K} . Therefore,

$$P_1 = (b_1 : b_2 : \beta_1) \in \mathbb{P}^2(\mathbb{K}(\beta_1)),$$

where $p_1(\beta_1) = 0$, is a simple point of \mathcal{C} . Note that $\deg(p_1) \leq d$. In this situation, choose $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3 \in \mathbb{K}$ such that:

- (1) $\lambda_i \mu_j \neq \lambda_j \mu_i$, for $i \neq j$, and $b_1 \neq \lambda_i \beta_1$, $b_2 \neq \mu_i \beta_1$ for $i = 1, 2, 3$,
- (2) $\text{res}_t \left(\overline{q_i}(t), \frac{\partial \overline{q_i}}{\partial t} \right) \neq 0$, for $i = 1, 2, 3$, where $\overline{q_i}(t) = F(\lambda_i t + b_1, \mu_i t + b_2, t + \beta_1) \in \mathbb{K}(\beta_1)[t]$.

Condition (1) implies in particular that the lines $\mathcal{L}_i = \{(\lambda_i t + b_1 : \mu_i t + b_2 : t + \beta_1) \mid t \in K\}$ are pairwise different, i.e. $\mathcal{L}_i \neq \mathcal{L}_j$ for $i \neq j$. Condition (2) guarantees that the lines \mathcal{L}_i do not pass through any singularities and that \mathcal{L}_i is not tangent to \mathcal{C} . Note that Lemma 4.67 implies that Condition (2) can always be achieved. Condition (1) is easily reachable. Now, we consider the polynomials

$$q_i(t) = \frac{\overline{q_i}(t)}{t} \in \mathbb{K}(\beta_1)[t], \quad i = 1, 2, 3$$

(note that $\overline{q_i}(0) = F(P_1) = 0$). We claim that

$$\mathcal{F}_i = \{(\lambda_i t + b_1 : \mu_i t + b_2 : t + \beta_1)\}_{q_i(t)}, \quad i = 1, 2, 3$$

are families of $(d-1)$ conjugate simple points on \mathcal{C} over $\mathbb{K}(\beta_1)$. The proof of this fact is similar to the proof of Theorem 4.68 and we leave it to the reader. \square

Corollary 4.73. *If algorithm PARAMETRIZATION-BY-ADJOINTS is performed with adjoints of degree $k = d$, S in Step 3 of the algorithm is taken as in Theorem 4.72, and Q in Step 4 is taken over \mathbb{K} , the algorithm outputs a parametrization over a field extension of \mathbb{K} of degree at most d .*

Proof. Similar to the proof of Corollary 4.69. \square

From the constructive proof of Theorem 4.72 it is clear that the field extension of \mathbb{K} introduced in the parametrization method is the one used to define the simple point P_1 through which the three families of $(d - 1)$ conjugate simple points are taken. Therefore, if P_1 can be taken to be rational, i.e. with coordinates in \mathbb{K} , then the output parametrization is defined over \mathbb{K} . In addition, the following result can be also deduced from the proof of Theorem 4.72.

Theorem 4.74. *Let \mathcal{C} be a rational projective curve with ground field \mathbb{K} . Then \mathcal{C} is parametrizable over \mathbb{K} if and only if there exists a simple point on \mathcal{C} with coordinates over \mathbb{K} .*

Proof. If \mathcal{C} is parametrizable over \mathbb{K} , giving values in \mathbb{K} to the parameter, one generates infinitely many points on \mathcal{C} over \mathbb{K} . Thus, since the curve has finitely many singularities, one generates simple points on the curve with coordinates in \mathbb{K} . Conversely, let $P \in \mathcal{C}$ be simple with coordinates over \mathbb{K} . Then, P can be taken as the point P_1 in the proof of Theorem 4.72 to generate the 3 families of $(d - 1)$ conjugate simple points on \mathcal{C} . This implies that these families are over \mathbb{K} , and therefore the output parametrization of the algorithm PARAMETRIZATION-BY-ADJOINTS is over \mathbb{K} . \square

The proofs of the previous theorems are constructive and they provide algorithms. We will outline the algorithm corresponding to adjoint curves of degree $d = \deg(\mathcal{C})$ (see Theorem 4.72 and Corollary 4.73). Algorithms derived from corollaries to Theorems 4.68 and 4.70 are left as exercises.

Algorithm SYMBOLIC-PARAMETRIZATION-BY-DEGREE- d -ADJOINTS.

Given the defining polynomial $F(x, y, z) \in \mathbb{K}[x, y, z]$ of a rational irreducible projective curve \mathcal{C} of degree d , and the standard decomposition $\mathcal{D}(\text{Ngr}(\mathcal{C}))$ of $\text{Ngr}(\mathcal{C})$, the algorithm computes a rational parametrization of \mathcal{C} .

1. If $d \leq 3$ or $\text{Sing}(\mathcal{C})$ contains exactly one point of multiplicity $d - 1$, apply algorithm PARAMETRIZATION-BY-LINES.
2. Take $b_1, b_2 \in \mathbb{K}$ such that no singular point of \mathcal{C} is of the form $(b_1 : b_2 : c)$.
3. Compute an irreducible factor $p(t)$ of $F(b_1, b_2, t)$ over \mathbb{K} . Let β be a root of $p(t)$.

4. Choose $\lambda_1, \lambda_2, \lambda_3, \mu_1, \mu_2, \mu_3 \in \mathbb{K}$ such that:
 - (i) $\lambda_i \mu_j \neq \lambda_j \mu_i$, for $i \neq j$,
 - (ii) $b_1 \neq \lambda_i \beta$, $b_2 \neq \mu_i \beta$ for $i = 1, 2, 3$,
 - (iii) $\text{res}_t \left(\overline{q_i}(t), \frac{\partial \overline{q_i}}{\partial t} \right) \neq 0$, for $i = 1, 2, 3$, where $\overline{q_i}(t) = F(\lambda_i t + b_1, \mu_i t + b_2, t + \beta)$.
5. Compute $q_i(t) = \frac{\overline{q_i}(t)}{t}$ for $i = 1, 2, 3$.
6. Set $\mathcal{F}_i := \{(\lambda_i t + b_1 : \mu_i t + b_2 : t + \beta)\}_{q_i(t)}$ for $i = 1, 2, 3$.
7. Choose a point $Q \in \mathbb{P}^2(\mathbb{K}) \setminus \mathcal{C}$.
8. Let H be the defining polynomial of $\mathcal{H} = \mathcal{A}_d(\mathcal{C}) \cap \mathcal{H}(d, Q + \sum_{i=1}^3 \sum_{P \in \mathcal{F}_i} P)$; use $\mathcal{D}(\text{Ngr}(\mathcal{C}))$ to compute symbolically \mathcal{H} (see Theorem 4.72).
9. Set one of the parameters in H to 1 and let t be the remaining parameter in H . Return the solution in $\mathbb{P}^2(\mathbb{K}(\beta)(t))$ of $\{\text{pp}_t(\text{res}_y(F, H)) = 0, \text{pp}_t(\text{res}_x(F, H)) = 0\}$.

Remarks. Note that in Step 4 and also in the next step, we do not need to isolate an individual root of $p(t)$, but we can simply work modulo $p(t)$.

Example 4.75. We consider the quintic curve \mathcal{C} over \mathbb{C} defined by the polynomial

$$F(x, y, z) = 3y^3z^2 - 3xy^2z^2 - 2xy^3z + y^3x^2 + x^3z^2.$$

The ground field of \mathcal{C} is \mathbb{Q} . In Step 2, we take $b_1 = -1, b_2 = 1$. Thus,

$$F(-1, 1, t) = 5t^2 + 2t + 1.$$

In Step 3, we consider $p(t) = 5t^2 + 2t + 1$ and β with minimal polynomial $p(t)$. In Step 4, we take $\lambda_1 = 1, \lambda_2 = 0, \lambda_3 = 1$ and $\mu_1 = 0, \mu_2 = 1, \mu_3 = 2$. It is easy to check that conditions (i),(ii),(iii) are satisfied. In this situation, the polynomials $q_i(t)$ in Step 5 are

$$\begin{aligned} q_1(t) &= \frac{23}{5}t + t^4 - 3t^3 - \frac{1}{5}t^2 + 8\beta + 2\beta t^3 - \frac{32}{5}\beta t^2 + \frac{6}{5}\beta t, \\ q_2(t) &= 3t^4 + 14t^3 + \frac{107}{5}t^2 + \frac{58}{5}t + 2 + 6\beta t^3 + \frac{124}{5}\beta t^2 + \frac{156}{5}\beta t + 10\beta, \\ q_3(t) &= 5t^4 + 21t^3 + \frac{147}{5}t^2 + \frac{47}{5}t + 10\beta t^3 + \frac{264}{5}\beta t^2 + \frac{294}{5}\beta t + 8\beta. \end{aligned}$$

Therefore, the families in Step 6 are

$$\begin{aligned} \mathcal{F}_1 &= \{(t - 1 : 1 : t + \beta)\}_{q_1(t)}, \quad \mathcal{F}_2 = \{(-1 : t + 1 : t + \beta)\}_{q_2(t)}, \\ \mathcal{F}_3 &= \{(t - 1 : 2t + 1 : t + \beta)\}_{q_3(t)}. \end{aligned}$$

In Step 7, we consider $Q = (1 : -1 : 1)$. In Step 8, we compute \mathcal{H} . For this purpose, first we apply the results on the symbolic computation of the genus (see Sect. 3.3), and we determine the standard decomposition of the singular locus:

$$\mathcal{D}(\text{Sing}(\mathcal{C})) = \mathcal{D}(\text{Ngr}(\mathcal{C})) = \underbrace{\{(0 : 0 : 1)\}}_{\text{triple}} \cup \underbrace{\{(1 : 1 : 1)\} \cup \{(1 : 0 : 0)\} \cup \{(0 : 1 : 0)\}}_{\text{double}},$$

where the first singularity is a triple point and the others are double points. Let H be the defining polynomial of a generic form in x, y, z of degree 5:

$$H = a_{00}z^5 + a_{01}yz^4 + a_{02}y^2z^3 + a_{03}y^3z^2 + a_{04}y^4z + a_{05}y^5 + a_{10}xz^4 + a_{11}xyz^3 + a_{12}xy^2z^2 + a_{13}xy^3z + a_{14}xy^4 + a_{20}x^2z^3 + a_{21}x^2yz^2 + a_{22}x^2y^2z + a_{23}x^2y^3 + a_{30}x^3z^2 + a_{31}x^3yz + a_{32}x^3y^2 + a_{40}x^4z + a_{41}x^4y + a_{50}x^5.$$

Next, we compute the defining polynomial of $\mathcal{A}_5(\mathcal{C})$. That is, we consider the equations

$$\frac{\partial H}{\partial x}(0, 0, 1) = 0, \quad \frac{\partial H}{\partial y}(0, 0, 1) = 0, \quad \frac{\partial H}{\partial z}(0, 0, 1) = 0,$$

$$H(1, 1, 1) = 0, \quad H(1, 0, 0) = 0, \quad H(0, 1, 0) = 0.$$

Solving them and substituting in H we get the defining polynomial of the linear system of adjoints, which we denote again by H :

$$H = (-a_{03} - a_{04} - a_{11} - a_{12} - a_{13} - a_{14} - a_{20} - a_{21} - a_{22} - a_{23} - a_{30} - a_{31} - a_{32} - a_{40} - a_{41})y^2z^3 + a_{03}y^3z^2 + a_{04}y^4z + a_{11}xyz^3 + a_{12}xy^2z^2 + a_{13}xy^3z + a_{14}xy^4 + a_{20}x^2z^3 + a_{21}x^2yz^2 + a_{22}x^2y^2z + a_{23}x^2y^3 + a_{30}x^3z^2 + a_{31}x^3yz + a_{32}x^3y^2 + a_{40}x^4z + a_{41}x^4y.$$

Now, we introduce the new conditions

$$\begin{aligned} H(1, -1, 1) &= 0, \\ H(t-1, 1, t+\beta) &= 0 \quad \text{mod } q_1(t), \\ H(-1, t+1, t+\beta) &= 0 \quad \text{mod } q_2(t), \\ H(t-1, 2t+1, t+\beta) &= 0 \quad \text{mod } q_3(t). \end{aligned}$$

Solving these equations, and substituting in H we get the new linear subsystem of dimension 1 corresponding to Step 8 (we denote it again by H):

$$H = a_{41} - 12340xy^3za_{30} + 47562xy^3za_{41} - 4670xy^2z^2a_{30} - 3024xy^2z^2a_{41} - 1275xyz^3a_{30} - 3435xyz^3a_{41} + 4500y^4za_{30}\beta - 47100y^4z\beta a_{41} - 11280y^3z^2a_{30}\beta + 7425y^3z^2a_{41}\beta - 2900x^4za_{30}\beta - 9130x^4z\beta a_{41} + 600x^3y^2a_{30}\beta - 16505x^3y^2\beta a_{41} - 595x^3yz a_{30} - 16824x^3yz a_{41} + 3160x^2y^3a_{30}\beta - 39113x^2y^3\beta a_{41} + 7830y^2z^3a_{41} + 675y^2z^3a_{30} - 5940y^2z^3\beta a_{41} + 362x^3yz\beta a_{41} - 10965x^3yz a_{30}\beta + 10565x^2y^2z a_{30}\beta + 48008x^2y^2z\beta a_{41} - 36677x^2yz^2\beta a_{41} + 13890x^2yz^2a_{30}\beta + 7729x^2yz^2a_{41} -$$

$$\begin{aligned}
& 915x^2z^3a_{41} - 300x^2z^3a_{30} + 94094xy^3z\beta a_{41} + 11420xy^3za_{30}\beta - 3200xy^4a_{30} - \\
& 6120xy^4a_{41} - 11590xy^2z^2a_{30}\beta - 6225xyz^3a_{30}\beta + 22712xy^2z^2\beta a_{41} + \\
& 19005xyz^3\beta a_{41} - 27633y^3z^2a_{41} + 4860y^3z^2a_{30} - 8700y^4za_{41} + 7500y^4za_{30} - \\
& 37671y^3z^2\beta a_{41} + 3600x^3y^2a_{30} - 4990x^4za_{41} - 500x^4za_{30} - 3115x^3y^2a_{41} - \\
& 9999x^2y^3a_{41} + 5180x^2y^3a_{30}.
\end{aligned}$$

Normalizing to $a_{30} = 1$ and $a_{41} = t$ and performing Step 9 we get the output parametrization

$$\mathcal{P}(t) = \left(\frac{\chi_{11}(t)}{\chi_{12}(t)}, \frac{\chi_{21}(t)}{\chi_{22}(t)} \right),$$

where,

$$\chi_{11}(t) = -293257020t^2 - 37389240\beta t^2 + 1396500 + 12020500\beta + 23655150t - 116431950\beta t + 480367237t^3 + 1072866719\beta t^3,$$

$$\chi_{12}(t) = 54925000t^3,$$

$$\chi_{21}(t) = -5618255790\beta t^2 - 1542285990t^2 + 2931800\beta - 38638880 + 693472350\beta t + 588212970t + 7167937919\beta t^3 - 1401717583t^3,$$

$\chi_{22}(t) = -260t(-69001t + 6701585\beta t - 201199 - 839635\beta + 6739937t^2)$ which requires a field extension of degree 2. However, if in Step 3 we consider $b_1 = -3, b_2 = 1$, then $\beta = 1$, and the algorithm leads to the parametrization

$$\mathcal{P}(t) = \left(\frac{21t + 343t^3 + 1 + 1470t^2}{-9261t^3}, \frac{21t + 343t^3 + 1 + 1470t^2}{21t(931t^2 + 14t + 1)} \right)$$

which is over the ground field. In the next chapter, we will see how to parametrize over the smallest possible field extension.

Exercises

4.1. Let $R(t) \in K(t)$ be nonconstant. Prove that the following statements are equivalent:

- (i) $R(t)$ is invertible.
- (ii) $R(t)$ is linear.
- (iii) $R(t) = \frac{at+b}{ct+d}$, where $a, b, c, d \in K$ and $ad - bc \neq 0$.

4.2. Consider a rational curve \mathcal{C} and a parametrization \mathcal{P} of \mathcal{C} . Is it true that if the degree of \mathcal{P} is prime then \mathcal{P} is proper? If not, what are the exceptions?.

4.3. Compute the tracing index of the parametrization

$$\mathcal{P}(t) = \left(\frac{t^4 + 3t^2 + 3}{t^4 + 3t^2 + 1}, \frac{t^4 + 2t^2 + 3}{t^2 + 2} \right).$$

4.4. May it happen that a proper parametrization is not injective for finitely many parameter values? If so, give an example.

4.5. Let $R(t) = \frac{p(t)}{q(t)} \in K(t)$ be a nonconstant rational function in reduced form, let $U = \{\alpha \in K \mid q(\alpha) \neq 0\}$, and let $R : K \rightarrow K$ be the rational mapping induced by $R(t)$. Prove that $\text{card}(K \setminus R(U)) \leq 1$.

4.6. Apply Exercise 4.5 to show that the number of exceptions in Lemma 4.32 is bounded by $2 \deg(R(t)) + 1$.

4.7. Carry out the computations in Example 4.38 without using the implicit equation of the curve \mathcal{C} .

4.8. Let \mathcal{C} be the plane curve defined by the irreducible polynomial

$$f = -2 + 5y - 2yx + 5y^2x - 4y^2 + 9yx^2 + y^3 - 2x^2 - 12y^2x^2 + 4y^3x^2 - 2y^3x \in \mathbb{C}[x, y],$$

and consider the rational parametrization

$$\mathcal{P}(t) = \left(\frac{t+1}{t^3+1}, \frac{t^2+1}{t^2+t+1} \right),$$

of \mathcal{C} . Determine whether \mathcal{P} is proper, and in the affirmative case compute its inverse.

4.9. Compute the defining polynomial of the curve defined by the rational parametrization

$$\mathcal{P}(t) = \left(\frac{t^5+1}{t^2+3}, \frac{t^3+t+1}{t^2+1} \right)$$

and the inverse of $\mathcal{P}(t)$.

4.10. Prove that the curve \mathcal{C} defined by the polynomial

$$f(x, y) = y^4 + x - \frac{75}{8}x^2y^2 + \frac{125}{8}x^3y - \frac{1875}{256}x^4$$

is parametrizable by lines. Compute a proper parametrization of \mathcal{C} and its inverse.

4.11. Let \mathcal{C} be the affine quintic curve defined by the polynomial

$$\begin{aligned} & -\frac{75}{8}x^2y^2 + \frac{125}{8}x^3y - \frac{1875}{256}x^4 + x + y^4 + \frac{625}{16}x^3y^2 - \frac{9375}{256}x^4y \\ & -\frac{125}{8}x^2y^3 + \frac{3125}{256}x^5 + y^5. \end{aligned}$$

Apply algorithm PARAMETRIZATION-BY-LINES to parametrize \mathcal{C} .

4.12. Prove that any line can be parametrized by lines.

- 4.13.** Give an example of a nonrational curve for which there exists a pencil of lines with the property required in Definition 4.48.
- 4.14.** Prove that for a curve with no rational component, there does not exist a pencil of lines with the property required in Definition 4.48.
- 4.15.** Let \mathcal{C} be an affine curve such that its associated projective curve \mathcal{C}^* is parametrizable by the pencil of lines $\mathcal{H}(t)$ of equation $L_1(x, y, z) - tL_2(x, y, z)$. Then, the affine parametrization of \mathcal{C} , generated by $\mathcal{H}(t)$, is proper and $\frac{L_1(x, y, 1)}{L_2(x, y, 1)}$ is its inverse.
- 4.16.** Extend the notion of proper rational parametrization to hypersurfaces over algebraically closed fields of characteristic zero.
- 4.17.** Construct an algorithm that, given the defining polynomial of a plane rational curve and the inverse φ of a proper rational parametrization, computes the parametrization φ^{-1} . Apply the algorithm to the inverse mapping computed in Example 4.38.
- 4.18.** Prove that irreducible nonrational curves of degree d may have adjoints of degree $d - 3$.
- 4.19.** Let \mathcal{C} be the affine curve defined by $f(x, y) = (x^2 + 4y + y^2)^2 - 16(x^2 + y^2) = 0$. Compute a rational parametrization of \mathcal{C} .
- 4.20.** Let \mathcal{C} be the affine curve defined by $f(x, y) = x^4 + 5xy^3 + y^4 - 20y^3 + 23y^2 - 9x^2y - 6x^3y + 16xy^2 - 11xy$. Compute a rational parametrization of \mathcal{C} .
- 4.21.** Describe an algorithm for parametrizing curves based on Theorem 4.68.
- 4.22.** Describe an algorithm for parametrizing curves based on Theorem 4.70.

Rational Algebraic Curves

A Computer Algebra Approach

Sendra, J.R.; Winkler, F.; Pérez-Díaz, S.

2008, X, 270 p. 24 illus., Hardcover

ISBN: 978-3-540-73724-7