JOHANNES KEPLER
UNIVERSITY LINZ

Submitted by
Lukas Weigert, BSc.

Submitted at
Research Institute for Symbolic Computation

Supervisor
Univ.-Prof. DI. Dr. Franz Winkler

April 2020

Strong Rational General Solutions of AODEs using Optimal Curve Parametrization

Master Thesis
to obtain the academic degree of
Diplom-Ingenieur
in the Master's Program
Computermathematik

JOHANNES KEPLER
UNIVERSITY LINZ
Altenbergerstraße 69
4040 Linz, Österreich
www.jku.at
DVR 0093696

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Masterarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Die vorliegende Masterarbeit ist mit dem elektronisch übermittelten Textdokument identisch.

. . . .

Lukas Weigert

Abstract

The aim of this thesis is to implement an algorithm that finds rational solutions of first-order algebraic ordinary differential equations (AODEs). We are interested in the general solution that depends on a transcendental constant.

To tackle this problem, a geometric approach is used. We neglect the differential aspect and consider the derivative as new variable. This leads to an algebraic equation. So we consider the AODE as an algebraic curve, in which the coefficients are rational functions. We have to compute the rational parametrization of the obtained curve. Since we look for rational solutions, we also require the coefficients of the parametrization to be rational. Every curve over the field of rational functions admits such a parametrization. Therefore, the key notion is optimal parametrization.

For parametrizing over the rational numbers, there are already implementations available. But these are not applicable for our problem, since they require field extensions. So we have to construct a new implementation.

Our goal is to decide whether the AODE has a rational general solution and in the affirmative case compute it. To do so, we have to modify the problem and search for solutions where also the arbitrary constant appears rationally. Such a solution is called strong rational general solution. Thus, we achieve a decision algorithm.

Kurzfassung

Das Ziel dieser Arbeit ist die Implementierung von einem Algorithmus zum Finden rationaler Lösungen von algebraischen gewöhnlichen Differenzialgleichungen erster Ordnung. Wir sind interessiert an der allgemeinen Lösung, die von einer transzendenten Konstante abhängt.

Für dieses Problem wird ein geometrischer Ansatz verwendet. Wir vernachlässigen den differenziellen Aspekt und betrachten die Ableitung als neue Variable. Dies führt zu einer algebraischen Gleichung. Somit betrachten wir die Differenzialgleichung als algebraische Kurve, wobei die Koeffizienten rationale Funktionen sind. Wir bestimmen die rationale Parametrisierung der dadurch entstandenen Kurve. Weil wir nach rationalen Lösungen suchen, müssen auch die Koeffizienten der Parametrisierung rational sein. Jede Kurve über dem Körper der rationalen Funktionen besitzt solch eine Parametrisierung. Somit benötigen wir die optimale Parametrisierung.

Zum Parametrisieren über rationale Zahlen sind bereits Implementierungen vorhanden. Aber diese können wir für unser Problem nicht anwenden, da sie Körpererweiterungen benötigen. Somit müssen wir eine neue Implementierung erstellen.

Wir wollen entscheiden, ob eine Differenzialgleichung eine rationale allgemeine Lösung besitzt und im positiven Fall diese bestimmen. Dazu müssen wir das Problem etwas verändern, indem wir nach Lösungen suchen, in denen auch die Konstante rational vorkommt. Solche Lösung nennt man strikt rationale allgemeine Lösung. Somit erreichen wir einen Entscheidungsalgorithmus.

Thanks

First of all, I would like to thank my supervisor Franz Winkler for giving me the chance to write my master thesis at the Research Institute for Symbolic Computation. I appreciate his relaxed style and the nice conversations.

This work was in cooperation with Johann Mitteramskogler. Special thanks to him for helping me in Maple and for many interesting discussions. It was a great pleasure to work together with him.

I also thank Georg Grasegger for giving me lots of valuable hints, which made a big improvement of my thesis.

Further thanks to Ralf Wahner for helping me with the organizational stuff and for dealing with my computer questions and for the funny time together.

Additionally, I would like to thank all my friends at university for having a nice time together and for helping me a lot at my studies.

All in all, I really enjoyed working on this exciting topic.

Lukas Weigert
April 2020

Contents

1. Introduction

In this thesis we study differential equations. A differential equation is a relation depending on an unknown function and some of its derivatives. Our particular interest are algebraic differential equations, which are defined by polynomials. The aim of this thesis is to construct a program that solves differential equations.

Differential equations are studied a lot, and they play an important role in numerous areas such as physics, biology, chemistry, engineering and economics. Many scientific laws are formulated by such equations.

Differential equations have a long history. For the first time, they were studied by Newton and Leibniz in the 1670s. In 1746, d'Alembert discovered the wave equation that determines the spreading of sound and light. The Euler–Lagrange equation was developed in the 1750s. A solution determines a curve where a particle reaches a fixed point in the same amount of time, independent of the starting point.

We do not only want to state relations, but also solve the equations. In the best case, we can find closed-form expressions for the solution. If finding such an explicit solution gets too hard, one may use numerical approximation to evaluate at a specific point. Thus, numerical methods play an important role in the task of solving differential equations.

In symbolic computation, we aim to determine solution formulas. A solution method for all differential equations does not exist and probably never will. Often we just consider particular classes of equations. Bernoulli proposed the Bernoulli differential equations and solved them. Linear differential equations are studied a lot. Such types may often be solved by making an Ansatz as exponential or trigonometric function. Kovacic [Kov86] gave an algorithm for determining all solutions of Riccati equations. But so far, not even for first-order differential equations a general algorithm exists.

Another question that may arise, is whether there exists a solution in a certain class of function. A solution can be e.g. rational, radical, algebraic or a power series. We want to decide the existence of such type of solution and in the affirmative case compute it.

Differential algebra was introduced by Joseph Ritt in [Rit50], which raised interest also to algebra of this analytical problem. In differential algebra, we view an algebraic differential equation as polynomial and work with the generated ideal. This enables us to use algebraic methods.

In [Kam83], Erich Kamke presents a wide collection of examples and solution methods of various differential equations. We frequently state some of his examples and solve them by using our own algorithms.

In this thesis we are concerned about a solution method for *algebraic ordinary differential equations* (AODEs). An AODE is a polynomial relation between a univariate function, some of its derivatives and the variable of differentiation. Let $\mathbb{K}$ be an algebraically closed field of characteristic 0. In practise, $\mathbb{K}$ might be $\overline{\mathbb{Q}}$, the field of algebraic numbers. For a polynomial F with coefficients in $\mathbb{K}$, an AODE can be written as

$$F(x, y, y', \ldots, y^{(k)}) \; = \; 0 \; , \tag{1.1}$$

where y is a function in the variable x and $k \in \mathbb{N}$. Our goal is to find the function $y(x)$ such that (1.1) is satisfied. The highest derivative appearing explicitly in F is called the *order* of the AODE (1.1). Without loss of generality, let the polynomial F be irreducible. Otherwise, the whole set of solutions consists of the solutions of the individual factors. If F does not depend on x, we call the AODE autonomous. Then it is of the form

$$F(y, y', \ldots, y^{(k)}) \;=\; 0 \;.$$

We aim to find symbolic expressions. Solutions are not unique. We do not want just one particular solution, but the whole family of solutions depending on some transcendental constants. Such a solution is called a *general solution.* The order of the AODE determines the number of independent constants. So a general solution of order k depends on k transcendental constants. A solution can be in a certain class of functions: rational, radical, algebraic, power series. We are interested in rational solutions. A rational general solution is of the form

$$y(x) = \frac{a_0 + a_1 x + \cdots + a_m x^m}{b_0 + b_1 x + \cdots + b_n x^n} \;,$$

where a_i, b_i are constants in a differential field extension of $\mathbb{K}$, i.e. $a_i, b_i \in \overline{\mathbb{K}(c_1, \ldots, c_k)}$.

Outline

We aim for an implementation in Maple of a decision algorithm by Vo, Grasegger and Winkler [VGW18] for existence of so-called strong rational general solutions, i.e. solutions in which also the constants appear rationally.

In Chapter 2 the basics of commutative algebra and differential algebra are recalled. In Chapter 3 the algebro-geometric method for solving AODEs is presented. For dealing with first-order equations, three procedures are discussed. One of these is explained in more detail in the remaining part of the thesis. The method is heavily based on parametrization. Chapters 4-6 are dedicated to the task of finding a suitable rational parametrization. In Chapter 7 the results are combined together and we obtain a decision algorithm. Since we aim to find an algorithmic procedure, we particularly care about the computational point of view. An implementation in Maple is given in the appendix.

In this thesis we assume that all domains are of characteristic 0. For a field K, we denote by $\overline{K}$ its algebraic closure.

2. Preliminaries in Commutative and Differential Algebra

Before we go into details, some basic notions in commutative algebra and differential algebra are discussed. We consider the connection of algebraic ideals and differential ideals, and we study their generic zeros.

Polynomial and Differential Ideals

Definition 2.1. Let R be a commutative ring with 1 and $R[x_1, \dots, x_n]$ the polynomial ring. A set $I \subseteq R[x_1, \dots, x_n]$ is an *algebraic (polynomial) ideal* iff it is closed under linear combination, i.e. if $F_1, \dots, F_n \in I$ and $P_1, \dots, P_n \in R[x_1, \dots, x_n]$, then also

$$\sum_{i=1}^{n} P_i F_i \in I \ .$$

If I is generated by $F_1, \dots, F_n$, we write $I = \langle F_1, \dots, F_n \rangle$. The set $\{F_1, \dots, F_n\}$ is called a *basis* for I.

Definition 2.2. A commutative ring with 1 in which every ideal has a finite basis is called a *Noetherian ring.*

Theorem 2.3 (Hilbert's Basis Theorem)**.** If R is a Noetherian ring, then also $R[x]$ is Noetherian.

Since every field is Noetherian (the only ideals are $\langle 0 \rangle$ and $\langle 1 \rangle$), it follows by inductively applying Hilbert's Basis Theorem that $K[x_1, \dots, x_n]$ is a Noetherian ring. So every polynomial ideal has a finite basis. This enables us to compute Gröbner Bases, which help us in deciding whether a polynomial is contained in the ideal.

Definition 2.4. A set $V \subseteq \mathbb{A}^n(K)$ is an *algebraic set (variety)* iff there is a set of polynomials $\mathcal{S} \subseteq K[x_1, \dots, x_n]$ such that V consists of those points P vanishing on all $F \in \mathcal{S}$, i.e.

$$V = V(\mathcal{S}) = \{P \in \mathbb{A}^n(K) \mid F(P) = 0 \text{ for all } F \in \mathcal{S}\} \ .$$

Let $I = \langle \mathcal{S} \rangle$, then $V(\mathcal{S}) = V(I)$. Since every ideal in $K[x_1, \dots, x_n]$ has a finite basis, every algebraic set consists of the common solutions of finitely many polynomials.

The following definitions can be found in [Rit50].

Definition 2.5. Let R be a commutative ring with 1. A derivation $'$ is a map from R to R such that for all $r, s \in R$ we have

1. $(r + s)' = r' + s'$,
2. $(rs)' = r's + rs'$.

$(R,')$ is called a *differential ring*. If R is a field, we call it a *differential field*.

Example 2.6.

- Any ring R with the trivial derivative, which maps everything to 0, is a differential ring.
- The univariate polynomial ring $\mathbb{Q}[x]$ with $' = \frac{d}{dx}$ is a differential ring. But we could also obtain one by setting $x' = 2$. In fact, x' could be anything in $\mathbb{Q}$.
- The field of rational functions $\mathbb{Q}(x)$ with $' = \frac{d}{dx}$ is a differential field.

Definition 2.7. Let $(R,')$ be a differential ring. Consider $R\{y\} = R[y^{(0)}, y^{(1)}, y^{(2)}, \dots]$ the polynomial ring in infinitely many variables. Then $'$ can be extended to a derivation δ on $R\{y\}$ by

$$\delta\left(\sum a_i y^{(i)}\right) = \sum \delta(a_i) y^{(i)} + a_i y^{(i+1)} \ .$$

The differential ring $(R\{y\}, \delta)$ is called the *ring of differential polynomials* in y. From now on we write $y, y', y'', \dots$ for $y^{(0)} y^{(1)}, y^{(2)}, \dots$.

Definition 2.8. A polynomial ideal I in $(R\{y\}, \delta)$ is called a *differential ideal* iff it is closed under the derivation δ, i.e. if $F \in I$, then also $\delta(F) \in I$.

If I is generated by some differential polynomials $F_1, \dots, F_n \in R\{y\}$, we write $I = [F_1, \dots, F_n]$.

Example 2.9. Let $F = y' + y^2 - 3x \in \mathbb{Q}[x]\{y\}$ be a differential polynomial. Then $F' = \delta(F) = y'' + 2yy' - 3$, $F'' = \delta(\delta(F)) = y''' + 2y'^2 + 2yy''$.

Note that $R\{y\}$ is a non-Noetherian ring. The algebraic ideal $\langle y, y', y'', \dots \rangle$, for $' = \frac{d}{dx}$, does not have a finite basis. But as a differential ideal $[y, y', y'', \dots]$, it has a finite basis, namely it can be written as $[y]$.

Generic Zeros and General Solutions

Definition 2.10. Let K be a field and L a field extension of K. Let I be an ideal in $K[x_1, \dots, x_n]$. A point $P \in \mathbb{A}^n(L)$ is a *zero* of I iff for all $F \in I$ we have $F(P) = 0$. It is a *generic zero* iff I is the defining ideal of P, i.e. $F \in I$ if and only if $F(P) = 0$.

Example 2.11. Consider $I = \langle y - x^2 \rangle$ in $\mathbb{Q}[x, y]$. All its zeros are of the form (t, t^2), for $t \in \mathbb{C}$. Therefore, $P = (t, t^2) \in \mathbb{C}(t)^2$ is a generic zero of I.

Definition 2.12. Let K be a differential field. Let I be a differential ideal in $(K\{y\}, \delta)$. An element p in a differential field extension is a *zero* iff for all $F(y) \in I$ we have $F(p) = 0$. It is a *generic zero* iff I is the defining ideal of p, i.e. $F(y) \in I$ if and only if $F(p) = 0$.

Example 2.13. The differential ideal $[y' - 2x]$ in $\mathbb{Q}(x)\{y\}$ has the generic zero $x^2 + c \in \mathbb{Q}(x)(c)$, where c is a transcendental constant. The corresponding differential equation $y' - 2x = 0$ has the general solution $y(x) = x^2 + c$.

We are in fact interested in the *radical* of I, denoted by $\sqrt{I}$. It consists of all those polynomials F such that a power F^n is contained in I. So

$$\sqrt{I} = \{F \mid \exists n \in \mathbb{N} : F^n \in I\} \ .$$

For those we have a very important property:

Theorem 2.14 (Hilbert's Nullstellensatz)**.** Let I be an ideal in $K[x_1, \dots, x_n]$, where K is an algebraically closed field. Then $\sqrt{I}$ consists exactly of those polynomials which vanish on all zeros on I.

Geometrically, Hilbert's Nullstellensatz says that the zeros of I and $\sqrt{I}$ coincide. Therefore, we can assume I to be radical.

In the same way we define the radical differential ideal, denoted by $\{I\}$. The differential Nullstellensatz states that $\{I\}$ consists of those polynomials which vanish on all zeros on I.

Exactly the prime ideals admit a generic zero. For an ideal in $K[x_1, \dots, x_n]$, the generic zero lies in a field extension of K. For a differential ideal in $(K\{y\}, \delta)$, it lies in a differential field extension of K.

Therefore, we aim to obtain prime ideals. Over the polynomial ring every radical ideal can be decomposed into a finite intersection of prime ideals. For principle ideals we have that if F is irreducible, then $\langle F \rangle$ is a prime ideal. This, however, is not true anymore for differential ideals. But we can do a similar approach.

Let $[F]$ be the differential ideal generated by F and its derivatives. From the differential Nullstellensatz, it is sufficient to consider its radical $\{F\}$.

Theorem 2.15. Let $F \in \mathbb{K}(x)\{y\}$, where F is irreducible as a polynomial in $K[x, y', \dots, y^{(n)}]$. Then we have the decomposition

$$\{F\} \;=\; (\{F\} : S) \;\cap\; \{F, S\}\;,$$

where S is the separant of F, the derivative of F w.r.t. $y^{(n)}$.

Proof. See [Rit50, Chapter 2]. □

$\{F\} : S$ is called the *general component*. Ritt shows that it is a prime differential ideal, which therefore has a generic point depending on some transcendental constants. The generic zero of $\{F\} : S$ is called *general solution*. But there might also be some elements in $\{F, S\}$, called *singular solutions*. We are mainly concerned in finding general solutions.

Example 2.16. Consider the differential equation $F = y'^2 + 2y' - 4y - 4x = 0$. A general solution of F is $y(x) = (x + c)^2 + c$. The separant is $\frac{\partial F}{\partial y'} = 2y' + 2$. So F also has a singular solution $y(x) = -x - \frac{1}{4}$.

Rational Parametrization of Algebraic Curves

Algebraic curves are defined by the zero set of a bivariate polynomial $F(x, y)$. We consider $\langle F \rangle$, the ideal generated by F. From Hilbert's Nullstellensatz, it suffices to look at the radical. Since the radical of $\langle F \rangle$ is given by the squarefree part of F, we may assume F to be squarefree.

Definition 2.17. Let K be a field and $F \in K[x, y]$. An *algebraic plane curve* over K is defined as the set

$$\mathcal{C}_F = \{(x, y) \in \mathbb{A}^2(\overline{K}) \mid F(x, y) = 0\}\;,$$

where F is a non-constant squarefree polynomial.

More generally, an algebraic curve is a hypersurface of dimension 1. So in the plane, a curve is generated by one single bivariate polynomial.

Even though K is the field of definition, a solution may lie in some field extension of K. The whole curve lives in $\mathbb{A}^2(\overline{K})$.

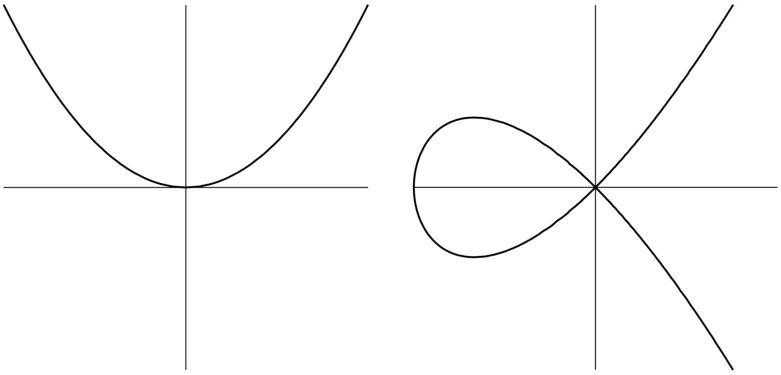
If F is irreducible, $\langle F \rangle$ is a prime ideal and therefore admits a generic point. A *parametrization* is a map

$$\begin{aligned} \mathcal{P}:\ \mathbb{A}^1(\overline{K}) &\to \mathcal{C}_F \\ t &\mapsto (p_1(t), p_2(t)) \end{aligned}$$

such that $F(p_1(t), p_2(t)) = 0$ for all values of t, where p_1, p_2 are not both constant. $\mathcal{P}$ describes a generic point on the curve. Only irreducible curves can have a generic point.

In the following, by abuse of notation, we denote the defining polynomial F also as the curve itself.

Example 2.18. The parabola $y = x^2$ has the parametrization (t, t^2). The node $y^2 - x^3 - x^2 = 0$ has the parametrization $(t^2 - 1, t^3 - t)$.



Parabola Node

Implicit representations and parametrizations have their advantages and disadvantages. Given an implicit equation $F(x, y) = 0$, it is easy to check whether a point lies on the curve. But it is hard to find some points on the curve. On the other hand, if we have a parametrization $(p_1(t), p_2(t))$, we can easily generate points. But for checking whether a given point lies on the curve, we have to solve algebraic equations.

Parametrizations can be in a certain class of functions: rational, radical, algebraic, power series. If p_1 and p_2 are rational, we speak of a rational parametrization.

If a curve admits a rational parametrization, we call it *rational* or *parametrizable*. Rationality depends on the number of singularities. A regular point is a point on the curve that has a simple unique tangent. Otherwise, it is called a singular point, i.e. there is no unique tangent. Singularities include multiple points. P is a singular point on F if and only if $F(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0$. Since F is squarefree, the set of solutions is finite. Thus, a curve can only have finitely many singularities. P has multiplicity k if all derivatives up to $k-1$ vanish on P, we denote it by $mult_P(F)$. The set of all singularities is denoted by $Sing(F)$.

We can always decide whether a curve is rational. The following theorem gives a necessary and sufficient condition.

Theorem 2.19. An algebraic curve is rational if and only if its genus is equal to 0.

Proper parametrizations are those with lowest degree. Let F be a curve having only ordinary singularities, i.e. singular points where all its tangents are distinct. Then the genus can be computed by

$$genus(F) = \frac{1}{2}\left((d-1)(d-2) - \sum_{P \in Sing(F)} mult_P(F)(mult_P(F)-1)\right) .$$

In general, for an irreducible curve, the relation $(d-1)(d-2) \geq \sum mult_P(mult_P - 1)$ holds. So the rational curves are those having as many singularities as their degree permits.

d	$(d-1)(d-2)$	$\sum mult_P(mult_P - 1)$
1	0	0
2	0	0
3	2	$2 \cdot 1$
4	6	$3 \cdot 2 = 2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1$

Irreducible lines and conics cannot have any singularity. A cubic is rational if and only if it has one singular point. Rational curves of degree 4 either have a triple point or 3 double points.

Although the implicit representation is unique up to a constant, there are infinitely many rational parametrizations. In fact, if $\mathcal{P}(t)$ is such a parametrization, then so is $\mathcal{P}(f(t))$ for any rational function f. We want to extract those parametrizations with lowest degree, which are satisfied by proper parametrizations.

Definition 2.20. A rational parametrization is called *proper* iff it has a rational inverse.

For proper parametrizations every curve point is generated only once, except some singularities. This is equivalent to $K(p_1(t), p_2(t)) = K(t)$. If an algebraic curve admits a rational parametrization, then it also admits a proper one. Proper parametrizations satisfy some degree equalities:

Theorem 2.21. Let $(p_1(t), p_2(t))$ be a proper parametrization of $F(x, y) = 0$. Then

1. $deg_t(p_1) = deg_y(F)$,
2. $deg_t(p_2) = deg_x(F)$,
3. if $(q_1(t), q_2(t))$ is another proper parametrization, then there exists a Möbius transformation, i.e. a linear rational function $l(t) = \frac{at+b}{ct+d}$ with $ad - bc \neq 0$ such that $p_1(l(t)) = q_1(t)$, $p_2(l(t)) = q_2(t)$.

3. The Algebro-Geometric Method

In the algebro-geometric method for solving AODEs $F(x, y, y', \dots, y^{(n)}) = 0$ we first neglect the differential aspect by introducing new variables $y_1 = y', \dots, y_n = y^{(n)}$. So we consider the derivatives as new indeterminates. This leads to an algebraic equation $F(x, y, y_1, \dots, y_n) = 0$.

A solution of the AODE can be regarded as a parametrization of the corresponding hypersurface $F(x, y, y_1, \dots, y_n) = 0$. Depending on the function class of the parametrization, we will arrive at different classes of solutions.

So we first compute a parametrization of F. Parametrizations are not unique. We try to transform it into another one, but now satisfying the differential conditions.

In this thesis we only consider rational solutions of first-order AODEs. Not every differential equation has a rational general solution. Let $\mathbb{K}$ be an algebraically closed field. We deal with the following problem:

Given: An AODE of order 1

$$F(x, y, y') \;=\; 0\;,$$

where $F \in \mathbb{K}[x, y, z]$ is irreducible and y is a function in the variable x.

Decide: Does the AODE have a rational general solution?

If so, find: The rational general solution $y(x)$ depending on a transcendental constant c.

In order for $F(x, y, y') = 0$ to be a differential equation, y' has to occur explicitly in F, therefore $F \in \mathbb{K}[x, y, z] \backslash \mathbb{K}[x, y]$. Since we work with first-order AODEs, a general solution depends on exactly one independent constant. We seek the rational general solution $y(x) \in \overline{\mathbb{K}(c)}(x)$. The constant does not need to occur rationally. We aim to construct an algorithm that decides whether an AODE has a rational general solution and in the positive case compute it.

In [FG04] Feng and Gao introduced the algebro-geometic method for solving autonomous differential equations. The idea of their approach consists in relating the AODE $F(y, y') = 0$ to an algebraic plane curve $F \in \mathbb{K}[y, z]$. A rational solution $(y(x), y'(x))$ is a rational parametrization of the corresponding curve.

There are two ways to extend this method to the general case $F(x, y, y') = 0$: Either we view $F \in \mathbb{K}[x, y, z]$ as a surface in the sphere $\mathbb{A}^3(\mathbb{K})$. This approach was developed in [NW10] and [NW11]. For almost all cases, it computes the rational general solution. Unfortunately, sometimes we have no stopping criterion. Thus, it is no decision procedure.

Alternatively, we view $F \in \mathbb{K}(x)[y, z]$ as a plane curve, but now over the field of rational functions $\mathbb{K}(x)$. This approach was developed in [VGW18]. We have to modify the problem and look for strong rational general solutions, i.e. rational general solutions where also c appears rationally. Then we achieve a decision algorithm.

So for one algorithm we lack a decision procedure, while for the other we can only find strong rational solutions. But neither of them reaches both tasks. We further briefly discuss these three methods.

3.1. Autonomous Case: Curve over $\mathbb{A}^2(\mathbb{K})$

First, we consider the case where the variable x does not appear explicitly in the AODE. So the AODE is autonomous and can be written as

$$F(y, y') = 0 \ .$$

This case was treated by Feng and Gao in [FG04] and [FG06]. They gave a decision algorithm for finding rational general solutions. We present an outline of their approach. The missing proofs can be found in [FG04].

Lemma 3.1. Let $\bar{y} = \frac{a_0+a_1x\cdots+a_mx^m}{b_0+b_1x+\cdots+b_nx^n}$ be a nontrivial solution of $F(y, y') = 0$. Then

$$y = \frac{a_0 + a_1(x + c) + \cdots + a_m(x + c)^m}{b_0 + b_1(x + c) + \cdots + b_n(x + c)^n}$$

is a rational general solution, where c is a transcendental constant.

This fact reduces the problem of finding the rational general solution of $F(y, y') = 0$ to the problem of finding just one particular rational solution. For the non-autonomous case, Lemma 3.1 is not valid anymore: $y' - x = 0$ has a solution $\frac{x^2}{2}$. The lemma would suggest the rational general solution to be $\frac{(x+c)^2}{2}$, but it is $\frac{x^2}{2} + c$.

We view F as defining an algebraic plane curve $\mathcal{C}_F$. We consider the algebraic equation $F(y, z) = 0$, where $F \in \mathbb{K}[y, z]$. Let $y(x)$ be a rational solution of the AODE $F(y, y') = 0$. Then the pair $(y(x), y'(x))$ can be regarded as a rational parametrization of $F(y, z) = 0$. Therefore, only parametrizable curves have a rational general solution.

In fact, the parametrization is even proper:

Theorem 3.2. Let $y(x)$ be a rational function. Then $\mathbb{K}(y(x), y'(x)) = \mathbb{K}(x)$.

So $(y(x), y'(x))$ is a proper parametrization of $\mathcal{C}_F$. This gives rise to the following strategy: We first compute a proper rational parametrization

$$\mathcal{P} = (p_1(x), p_2(x)) \in \mathbb{K}(x)^2$$

of $\mathcal{C}_F$. Then we try to transform this parametrization into another proper one such that the second component is the derivative of the first. From Theorem 2.21 we know that each proper parametrization can be transformed to another one by a linear rational function $T(x) = \frac{ax+b}{cx+d}$. This leads to a decision method. We have to find such a transformation such that $p_1(T(x))' = p_2(T(x))$. F has a rational general solution if and only if there exists such a T. In the affirmative case,

$$(p_1(T(x)),\ p_1(T(x))')$$

corresponds to a solution of the AODE, and $y(x) = p_1(T(x + c))$ is the rational general solution of $F(y, y') = 0$.

Example 3.3. Consider the autonomous differential equation

$$y' + y^2 = 0 \ .$$

A proper rational parametrization of the associated curve is

$$\mathcal{P}(x) = (x,\ -x^2) \ .$$

Using $T(x) = \frac{1}{x}$, we get another parametrization, where the second is the derivative of the first:

$$(y,\ y') = \left(\frac{1}{x},\ -\frac{1}{x^2}\right)\ .$$

So $y(x) = \frac{1}{x+c}$ is the rational general solution.

From the degree equalities of a proper parametrization, Theorem 2.21, we additionally get

Corollary 3.4. Let y be a rational general solution of $F(y, y') = 0$. Then

$$deg_x(y) = deg_{y'}(F)\ .$$

With that knowledge, we could actually take a general function of given degree, insert in F and solve for the coefficients. But this would soon get very expensive. Thus, the above approach is definitely preferable. Corollary 3.4 is not true for the non-autonomous case anyway: Consider $F = y' - x^n$. Then $deg_{y'}(F) = 1$, and the rational general solution is $y(x) = \frac{x^{n+1}}{n+1} + c$, so $deg_x(y)$ can get arbitrarily large. Therefore, we really need the parametrization.

3.2. General Case: Surface over $\mathbb{A}^3(\mathbb{K})$

We now consider the non-autonomous first-order AODE

$$F(x, y, y') = 0$$

and proceed as described in [NW10]. We view F as defining an algebraic surface in the sphere. We consider the algebraic equation $F(x, y, z) = 0$. Let $y(x)$ be a rational solution of the AODE $F(x, y, y') = 0$. Then the triple $(x, y(x), y'(x))$ can be regarded as a rational space curve on the surface $F(x, y, z) = 0$.

We compute a rational parametrization

$$\mathcal{P}(s, t) = (p_1(s, t), p_2(s, t), p_3(s, t)) \in \mathbb{K}(s, t)^3\ .$$

Then we try to transform this parametrization in such a way that the differential conditions are satisfied. Thus, we arrive at a system of quasilinear first-order autonomous equation, called associated system:

$$\begin{aligned} s' &= \frac{p_{2t} - p_3 p_{1t}}{p_{1s} p_{2t} - p_{1t} p_{2s}}\ , \\ t' &= \frac{p_{1s} - p_3 p_{2s}}{p_{1s} p_{2t} - p_{1t} p_{2s}}\ . \end{aligned} \tag{3.1}$$

There is a 1-1-correspondence between solutions of the initial equation and the associated system (3.1). It is chosen in such a way that

$$\mathcal{P}(s(x), t(x)) = (x + c,\ p_2(s(x), t(x)),\ p_2(s(x), t(x))')\ .$$

Then $y(x) = p_2(s(x - c), t(x - c))$ is the rational general solution of $F(x, y, y') = 0$.

Invariant Algebraic Curves

We still have to solve the associated system (3.1). The system is autonomous and of order 1. Thus, it can be described as a vector field. We follow the approach of [NW11].

Definition 3.5. An *invariant algebraic curve* of the rational system

$$s' = \frac{M_1(s,t)}{N_1(s,t)} \ , \ t' = \frac{M_2(s,t)}{N_2(s,t)} \ ,$$

where M_1, M_2, N_1, N_2 are polynomials, is an algebraic curve $G(s,t) = 0$ such that

$$G_s \ M_1 N_2 + G_t \ M_2 N_1 = G \ K \ ,$$

where K is any polynomial.

A rational general solution of the associated system parametrizes a rational invariant curve. The factors of an invariant curve are again invariant curves. Therefore, it suffices to look at all irreducible invariant algebraic curves. A rational parametrization $(s(x), t(x))$ is a candidate for a solution of the associated system. In general, we have an upper degree bound for an irreducible invariant curve. But in the unlikely case the system has some dicritical points, we have no boundary condition and might search forever. Thus, the above method is no decision procedure.

3.3. General Case: Curve over $\mathbb{A}^2(\mathbb{K}(x))$

We again consider the non-autonomous first-order AODE

$$F(x, y, y') = 0$$

and proceed as described in [VGW18]. As in the autonomous case, we view F as defining an algebraic plane curve $\mathcal{C}_F$, but now F has coefficients in $\mathbb{K}(x)$, the field of rational functions in x. We consider the algebraic equation $F(y,z) = 0$, where $F \in \mathbb{K}(x)[y,z]$. Let $y(x)$ be a rational solution of the AODE $F(x,y,y') = 0$. Then the pair $(y(x), y'(x))$ can be regarded as a rational point on the curve $F(y,z) = 0$. Therefore, F has to be parametrizable as a curve over $\mathbb{K}(x)$.

We compute a rational parametrization

$$\mathcal{P}(t) = (p_1(x,t), p_2(x,t)) \in (\mathbb{K}(x)(t))^2 \ .$$

Then we try to transform this parametrization into another one such that the second component is the derivative of the first. We have to find a rational function $T(x)$ such that $p_1(x, T(x))' = p_2(x, T(x))$. This transformation $T(x)$ satisfies some quasilinear first-order equation, called associated equation. There is a 1-1-correspondence between solutions of these two equations. If the associated equation has a rational general solution, it is a Riccati Equation

$$T'(x) = a_0(x) + a_1(x)T(x) + a_2(x)T(x)^2 \ , \qquad \text{for some } a_0, a_1, a_2 \in \mathbb{K}(x).$$

For this type of equation there are solution methods available. Then

$$(p_1(x, T(x)), \ p_1(x, T(x))')$$

corresponds to a solution of the AODE, and $y(x) = p_1(x, T(x,c))$ is the rational general solution of $F(x, y, y') = 0$.

Example 3.6. Consider the first-order AODE

$$y'^2 + 2y' - 4y - 4x = 0 \ .$$

A rational parametrization of the associated curve is

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

Setting $t = x + c$, we get

$$(y, \ y') = \Big((x+c)^2 + c, \ 2(x+c)\Big) \ .$$

So $y(x) = (x+c)^2 + c$ is the rational general solution.

Strong Rational Solution

This approach actually does not work for the whole class of rational general solutions $y(x,c)$. The problem has to be weakened a little bit. We also want the c to appear rationally in y.

Definition 3.7. A solution y of $F(x,y,y') = 0$ is called a *strong rational general solution* iff $y \in \mathbb{K}(x,c) \backslash \mathbb{K}(x)$, where c is a transcendental constant over $\mathbb{K}$.

This modification enables us to state the following fundamental theorem:

Theorem 3.8. Let $F \in \mathbb{K}[x,y,z] \backslash \mathbb{K}[x,y]$ be irreducible. If $F(x,y,y') = 0$ has a strong rational general solution $y(x,c)$, then

1. F is irreducible as a polynomial in $\overline{\mathbb{K}(x)}[y,z]$.
2. $F(y,z)$ is parametrizable with coefficients in $\mathbb{K}(x)$. In particular, $\mathcal{P}(t) = (y(x,t), \frac{d}{dx}y(x,t))$ is such a rational parametrization.

Proof. See [VGW18, Theorem 3.1]. □

This theorem helps us in deciding the existence of a strong rational general solution. It promises us that we do not miss any solution. Only parametrizable AODEs admit strong rational general solutions. Therefore, parametrizability can be seen as a necessary condition for an AODE, having a strong rational general solution.

Example 3.9. A rational general solution which is not strong is

$$y(x) = cx + \sqrt{c^3 + 1} \ .$$

An AODE having this solution is

$$y^2 - 2xyy' + x^2y'^2 - y'^3 - 1 = 0 \ .$$

The corresponding curve has genus 1. Thus, it violates the conditions in Theorem 3.8. Therefore, the differential equation cannot have any strong rational general solution.

We further focus on the approach considering the differential equation as a curve over $\mathbb{K}(x)$. Chapters 4 is devoted to parametrizing curves with coefficients in $\mathbb{K}(x)$. Parametrization requires some base points on the curve. In Chapter 5 and 6 it is explained how to find such points. Finally, as described in Chapter 7, we transform the differential equation into a quasilinear one, which is easier to solve. Thus, we achieve a decision algorithm.

4. Optimal Parametrization

The algebro-geometric approach for solving differential equations depends highly on parametrization. Since we work with the class of rational solutions, we require rational parametrizations. In our case, the coefficients may occur as rational functions.

We want a "good" parametrization. A proper rational parametrization is minimal w.r.t. the degree of $\mathcal{P}$. But in this chapter we particularly take care of the coefficients. To motivate this, let us look at the following example:

Example 4.1. Consider the square function $y = x^2$ over $\mathbb{Q}$. It has a proper rational parametrization $\mathcal{P}_1(t) = (t, t^2)$. But another proper parametrization would be $\mathcal{P}_2(t) = (\sqrt{2}t, 2t^2)$. Here, we had to extend the field of coefficients. Thus, we prefer $\mathcal{P}_1$ of course.

Since we are looking for rational solutions of AODEs, it is crucial for the coefficients to stay in the ground field $\mathbb{K}(x)$. Only such a parametrization allows us to transform the AODE into a quasilinear one. This gives rise to the following definition:

Definition 4.2. Let F be an algebraic curve over K. A field $L \supseteq K$ is called a *field of parametrization* iff there exists a rational parametrization $\mathcal{P}(t)$ with coefficients in L. A point on F is called *L-rational* iff it has coordinates in L.

We will see that the existence of a parametrization in L depends on the existence of an L-rational point. Clearly, if L is a field of parametrization, then there exists an L-rational point. But also the converse is true. Chapter 5 is devoted to the search of $\mathbb{K}(x)$-rational points.

Definition 4.3. A field of parametrization L is called *optimal* iff the extension degree $[L : K]$ is minimal. The corresponding rational parametrization is called an *optimal parametrization.*

Example 4.4. As we have seen above, $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$ are fields of parametrization of the square function, where obviously $\mathbb{Q}$ is optimal. $\mathcal{P}_1$ is an optimal parametrization.

From Theorem 3.8 we know that if an AODE $F(x, y, y') = 0$ has a strong rational general solution $y(x, c)$, then there exists a rational parametrization of F with coefficients in $\mathbb{K}(x)$, take $\mathcal{P}(t) = (y(x, t), \frac{d}{dx}y(x, t))$. Thus, it suffices to find an optimal parametrization.

The parametrization algorithm relies on intersecting the given curve with a system of curves in some specific points and some specific multiplicities. For two plane curves A and B, the intersection multiplicity in a point P, denoted by $mult_P(A, B)$, can be described axiomatically, see [Ful08, Section 3.3].

During this chapter we frequently use Bézout's theorem, telling about the number of intersections. So we once state it here:

Theorem 4.5 (Bézout)**.** Let A and B be two projective plane curves over K of degree m and n without common components, then

$$\sum_{P \in \mathbb{P}^2(K)} mult_P(A, B) = m \cdot n \ .$$

We abbreviate the set of intersection points as $A \cap B$, knowing that we in fact talk about multisets. If the intersection points of two curves are $P_1, \dots, P_n$ with associated multiplicities $m_1, \dots, m_n$, we express this by the divisor

$$m_1 \cdot P_1 + \cdots + m_n \cdot P_n \ .$$

Now we come to the parametrization methods, as described in [SWPD08]. Since only irreducible curves are parametrizable, we consider a curve defined by an irreducible polynomial $F(y, z)$ with coefficients in a field K. Typically, K might be $\mathbb{Q}$ or $\mathbb{K}(x)$.

4.1. Linear Occurrence of a Variable

If one variable occurs linearly, the parametrization can be found by just converting the equation. Suppose w.l.o.g. z occurs linearly in F. Then

$$F(y, z) = G_0(y) + zG_1(y) = 0 \ .$$

Simple transformation gives

$$z = -\frac{G_0(y)}{G_1(y)} \ .$$

So the rational parametrization is given by

$$\mathcal{P}(t) = \left(t, -\frac{G_0(t)}{G_1(t)}\right) \ .$$

Obviously, we do not need to extend the field of coefficients. In projective space this can be written as

$$\mathcal{P}(t) = (tG_1(y) : -G_0(t) : G_1(t)) \ .$$

4.2. Parametrization by Lines

Many observations are taken from [SWPD08, Section 4.6].

Parametrization of a conic

We first compute a K-rational point R on the conic. Then we take a system of lines $L(t)$ through R and intersect the conic with $L(t)$. By Bézout, they have $2 \cdot 1 = 2$ intersection points. So

$$F \cap L(t) = 1 \cdot R + 1 \cdot \mathcal{P}(t) \ ,$$

where the second intersection point depends rationally on the parameter t. The parametrization is given by this point. First let us assume that the curve passes through the origin, so $(0, 0) \in \mathcal{C}_F$. We can write F as

$$F(y, z) = F_2(y, z) + F_1(y, z) \ ,$$

where F_i are the homogeneous components of degree i. Observe that since F is irreducible, F_1 is not zero. We intersect the conic with a system of lines through the origin $L(t) = z - ty$. The slope of the lines depend on a running parameter t. We consider

$$\begin{aligned} F(y, z) &= 0 \ , \\ z &= ty \ . \end{aligned}$$

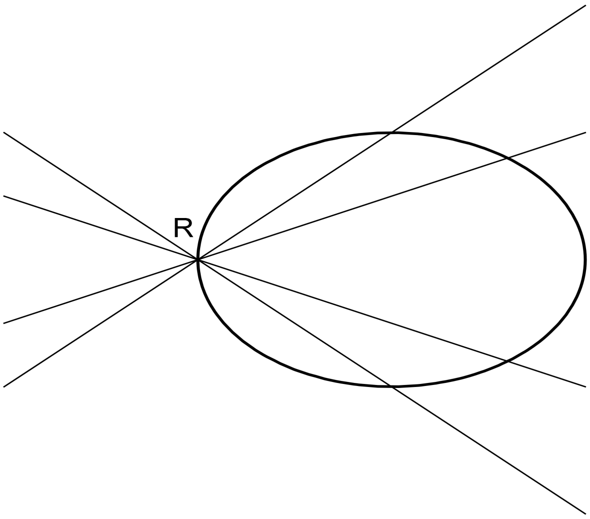


Figure 4.1.: System of lines intersects conic

Each line intersects the conic, additionally to the origin, one more time. We compute the second point:

$$F(y,ty)=0 \Longrightarrow F_2(y,ty)=-F_1(y,ty) \Longrightarrow y^2F_2(1,t)=-yF_1(1,t)\ .$$

The condition $y=0$ would lead to the origin as solution. So we can assume $y\neq 0$ and divide through. We obtain $y=\frac{-F_1(1,t)}{F_2(1,t)}$ and $z=ty=\frac{-tF_1(1,t)}{F_2(1,t)}$. So the two intersection points are

$$(0,0) \qquad \text{and} \qquad \left(\frac{-F_1(1,t)}{F_2(1,t)}, \frac{-t\ F_1(1,t)}{F_2(1,t)}\right) =: \mathcal{P}(t)\ .$$

The second point depends rationally on the parameter t, which traverses the whole curve. This gives the parametrization of a conic through the origin. Clearly, we do not have to extend the field of coefficients.

For parametrizing a general conic we have to find a point $(a,b)\in\mathcal{C}_F$. Then we transform the curve to origin using $G(y,z):=F(y+a,z+b)$ and compute the parametrization of G as described above. At the end, we transform the curve back. So the parametrization is given by

$$\mathcal{P}(t)=\left(\frac{-G_1(1,t)}{G_2(1,t)}+a, \frac{-t\ G_1(1,t)}{G_2(1,t)}+b\right)\ .$$

From this formula one immediately observes that if the given point (a,b) is rational, then so are coefficients in $\mathcal{P}$. More generally, $(a,b)\in\mathbb{A}^2(L)$ if and only if L is the field of parametrization, where L is a field extension.

Algorithm 1: *ConicParametrization*(F)

```
Input: Conic $F(y,z)=0$, where $F\in K[y,z]$
Output: Rational parametrization of $F$ with coefficients in $K$
1 Compute a rational point $(a,b)$ on $F$
2 Transform to origin: $G(y,z):=F(y+a,z+b)=G_2(y,z)+G_1(y,z)$
3 Return $\mathcal{P}(t):=\left(\frac{-G_1(1,t)}{G_2(1,t)}+a, \frac{-t\ G_1(1,t)}{G_2(1,t)}+b\right)$
```

The first step is the hardest one. In Chapter 5 it is shown, how to find a rational point on the conic. We will see that for $K = \mathbb{K}(x)$ this is always possible.

Example 4.6 (Kamke 446)**.** Consider

$$F(x, y, y') = y^2 - 2xy'y + (x^2 + 1)y'^2 - 1 = 0 \ .$$

The corresponding curve is

$$F(y, z) = y^2 - 2xyz + (x^2 + 1)z^2 - 1 \ .$$

We can easily see that $(0, 1) \in \mathcal{C}_F$. We transform the curve to

$$G(y, z) = F(y + 1, z) = y^2 - 2xyz + (x^2 + 1)z^2 + 2y - 2xz \ .$$

Therefore

$$\mathcal{P}(t) = (p_1(t), p_2(t)) \ ,$$

where

$$\begin{aligned} p_1 &= \frac{-2 + 2xt}{1 - 2xt + (x^2 + 1)t^2} + 1 = \frac{-1 + (x^2 + 1)t^2}{1 - 2xt + (x^2 + 1)t^2} \ , \\ p_2 &= \frac{-2t + 2xt^2}{1 - 2xt + (x^2 + 1)t^2} \ . \end{aligned}$$

Sometimes, it is useful to extend this approach to projective space. Suppose we found the point $R = (a : b : c) \in \mathbb{P}^2(K)$. If $c \neq 0$, R corresponds to $(\bar{a} : \bar{b} : 1)$. Then for $G(y, z) = F(y+\bar{a}, z+\bar{b}, 1)$, the parametrization is given by

$$\mathcal{P}(t) = \big(- G_1(1, t) + \bar{a}\ G_2(1, t) : -t\ G_1(1, t) + \bar{b}\ G_2(1, t) : G_2(1, t)\big) \ .$$

But if $c = 0$, the point lies at infinity. Fortunately, we can normalize one of the other coordinates instead and proceed similarly. Note that not all three values can be simultaneously 0, because we are in projective space.

Parametrization of a cubic

Cubics of genus 0 must always have one double point as only singularity. Let F be defined over K, then this point is always a K-rational point. This can be shown as follows:

Let $S = (p_1(\alpha) : p_2(\alpha) : p_3(\alpha)) \in K(\alpha)$ be the singularity, where $m(\alpha) = 0$ is the minimal polynomial. Then

$$\begin{aligned} F(p_1(\alpha), p_2(\alpha), p_3(\alpha)) &= 0 \bmod m(\alpha) \ , \\ \partial F(p_1(\alpha), p_2(\alpha), p_3(\alpha)) &= 0 \bmod m(\alpha) \ . \end{aligned}$$

These relations provide $deg(m)$ solutions. But since there exists only one singularity, it must hold $deg(m) = 1$. Therefore, S is a rational point. □

We first compute the singularity S on the cubic. Then we take a system of lines $L(t)$ through S and intersect the cubic with $L(t)$. By Bézout, they have $3 \cdot 1 = 3$ intersection points. So

$$F \cap L(t) = 2 \cdot S + 1 \cdot \mathcal{P}(t) \ ,$$

where the third intersection point depends rationally on the parameter t. So the parametrization is given by this point.

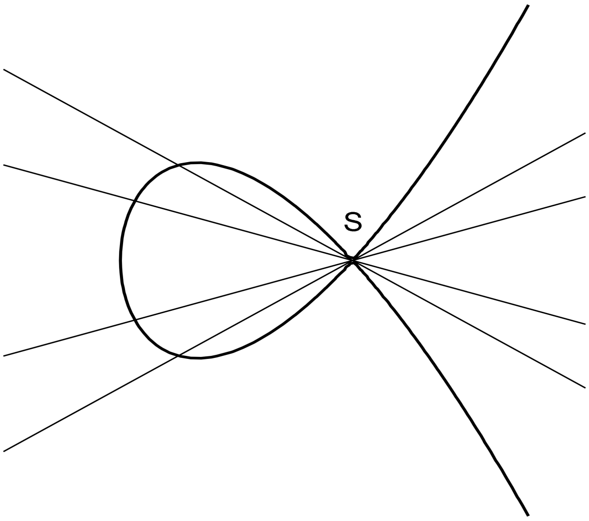


Figure 4.2.: System of lines intersects cubic

Higher degree

This approach can be easily generalized to curves of degree d having a $(d-1)$-fold point S. By similar arguments, S is rational. Intersecting F with a system of lines $L(t)$ through S, one gets

$$F \cap L(t) = (d-1) \cdot S + 1 \cdot \mathcal{P}(t) \ ,$$

where again the last point depends rationally on the parameter t and therefore gives the rational parametrization.

The following algorithm generalizes that one for conic parametrization.

```
Algorithm 2: $ParametrizationByLines(F)$
  Input: Curve $F(y,z) = 0$, where $F \in K[y,z]$ of degree $d > 1$, having a $(d-1)$-fold point
  Output: Rational parametrization of $F$ with coefficients in $K$
  Compute the $(d-1)$-fold point $(a,b)$ on $F$, if $d = 2$ any rational point on $F$
  Transform to origin: $G(y,z) := F(y+a, z+b) = G_d(y,z) + G_{d-1}(y,z)$
  Return $\mathcal{P}(t) := \left( \frac{-G_{d-1}(1,t)}{G_d(1,t)} + a, \frac{-t\ G_{d-1}(1,t)}{G_d(1,t)} + b \right)$
```

A curve of degree d can be parametrized by lines if and only if it has a $(d-1)$-fold point. If the base point is rational, then the parametrization has coefficients in the ground field.

4.3. Parametrization by Adjoint Curves

In general, a curve may have several singularities, therefore, it cannot be parametrized by lines. We need higher degree curves to parametrize. This task can be done by adjoint curves. See also [SWPD08, Section 4.7]. In this section let F be a curve of degree $d \geq 3$. We further assume that F has only ordinary singularities, i.e. tangents are distinct.

For dealing with non-ordinary singularities, one can apply blowing-up at these singularities and arrive at neighbouring singularities. By applying a certain quadratic transformation, so-called Cremona transformation, we obtain a curve having only ordinary singularities. In this procedure we do not need to extend the field of coefficients. For further details we refer to [SW91] and [SWPD08].

Definition 4.7. A curve H is called an *adjoint curve* to F iff for all singular points S, $mult_S(H) \geq mult_S(F) - 1$.

So an adjoint curve has to pass through all singularities of multiplicity n at least $n-1$ times. Clearly, for almost all adjoint curves it holds $mult_S(H) = mult_S(F) - 1$. The system of adjoint curves to F of degree k is denoted by $\mathcal{A}_k$. If F is rational and $k \geq d-2$, then $\mathcal{A}_k \neq \emptyset$.

Proposition 4.8. Let F be a projective curve with coefficients in K. Then every adjoint curve has coefficients in K.

Proof. Let $S = (p_1(\alpha) : p_2(\alpha) : p_3(\alpha)) \in K(\alpha)$ be a singularity, where $m(\alpha) = 0$ is the minimal polynomial. Define

$$r(\alpha) := rem(F(p_1(\alpha), p_2(\alpha), p_3(\alpha)), m(\alpha)) \ .$$

Then $deg(r) < deg(m)$. But since m is the minimal polynomial, it must hold $r(\alpha) = 0$. Therefore, S provides $deg(m)$ linear conditions.

If $mult_S(F) > 2$, we consider the partial derivatives of F. By similar arguments, S provides linear conditions. □

Let $H \in \mathcal{A}_{d-2}$ be such that $mult_S(H) = mult_S(F) - 1$. The number of intersection points are $|F \cap H| = d(d-2)$. Because $genus(F) = 0$, there are $\sum_{P \in Sing(F)} m_P(m_P - 1) = (d-1)(d-2)$ intersections fixed by the singularities. Therefore, $dim(\mathcal{A}_{d-2}(F)) = d-2$.

We further force the generic representative H of $\mathcal{A}_{d-2}$ to pass through $d-3$ additional points on F. Each point provides one new linear condition on H. In order to let H be a rational polynomial, these points have to be rational, or a family of rational points. Then there is only one point left depending rationally on t, because

$$d(d-2) = (d-1)(d-2) + (d-3) + 1 \ .$$

So we first compute the system of adjoint curves $\mathcal{A}_{d-2}$. We further compute $d-3$ rational simple points R_i on F and let a generic element $H \in \mathcal{A}_{d-2}$ pass through all R_i. Intersecting the curve with the obtained system $H(t)$ yields

$$F \cap H(t) = \sum m_i(m_i - 1) \cdot S_i + \sum_{i=1}^{d-3} 1 \cdot R_i + 1 \cdot \mathcal{P}(t) \ .$$

Then the parametrization is given by the remaining intersection point, see Figure 4.3. We call this the *generic intersection point.* To compute the singularities, we have to solve the system $\{F = 0, \frac{\partial F}{\partial y} = 0, \frac{\partial F}{\partial z} = 0\}$. Finding rational simple points is hard, in general. In Chapter 6 it is described how to find such points. For curves defined over $\mathbb{K}(x)$, we can always find rational points. This is not the case for $\mathbb{Q}$.

Remark 4.9. Instead of computing $d-3$ rational simple points, we could alternatively use families of k conjugate points for $k \leq d-3$. Similarly to Proposition 4.8, one can show that this provides linear conditions.

As it is shown in [SW97], for a general field one can compute families of $d-2$ simple points. Thus, we only need one simple point in a field extension of degree at most two. In the odd case, we can even compute $\frac{d-3}{2}$ families of two simple points and therefore do not need to compute any rational point. But since we can produce arbitrary many $\mathbb{K}(x)$-rational points, we do not need to care about these considerations.

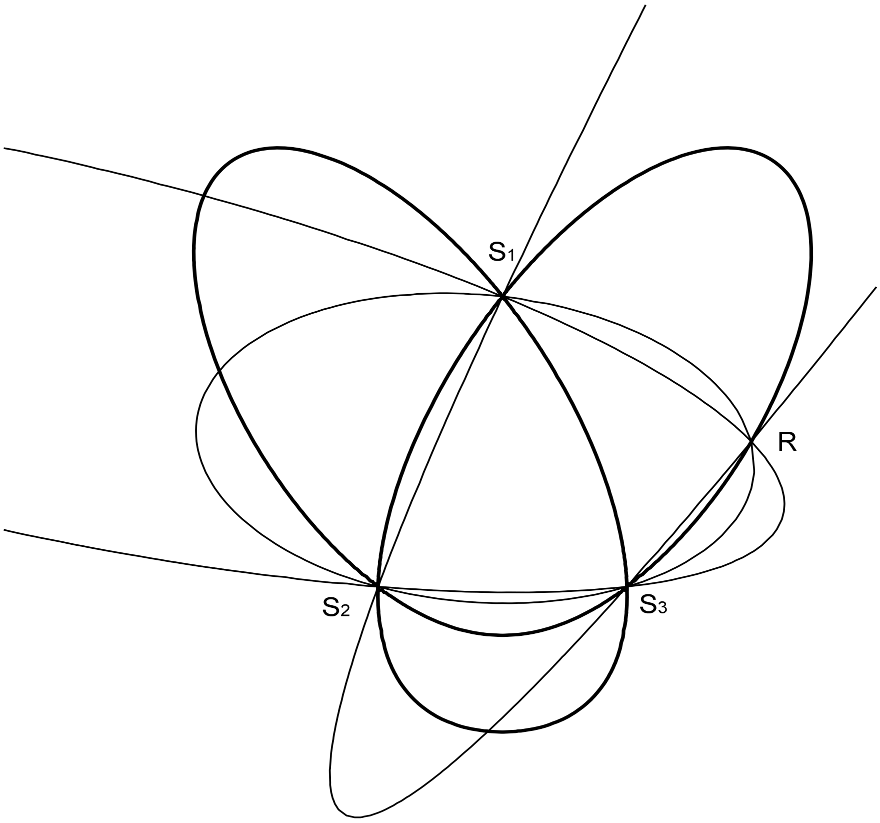


Figure 4.3.: System of adjoint curves of degree 2 intersects curve of degree 4

Theorem 4.10. Let F and $H(t)$ be as described above. Then the generic intersection point $\mathcal{P}(t)$ is always a $K(t)$-rational point, i.e. $\mathcal{P}(t) \in \mathbb{P}^2(K(t))$.

Proof. For almost all values of t, $H(t)$ and F have exactly one intersection point. Let us fix such an H. Let $P = (p_1(\alpha) : p_2(\alpha) : p_3(\alpha)) \in K(\alpha)$ be this intersection point, where $m(\alpha) = 0$ is the minimal polynomial. Then

$$F(p_1(\alpha), p_2(\alpha), p_3(\alpha)) = 0 \text{ mod } m(\alpha) \ ,$$
$$H(p_1(\alpha), p_2(\alpha), p_3(\alpha)) = 0 \text{ mod } m(\alpha) \ .$$

These relations provide $deg(m)$ solutions. But since, by construction, there exists only one more intersection, it must hold $deg(m) = 1$. Therefore, P is a K-rational point.

Since t was chosen arbitrary, $\mathcal{P}(t)$ is K-rational for all $t \in K$, and therefore, it is a $K(t)$-rational point. □

We conclude that $\mathcal{P}(t)$ is a rational parametrization. If we take $K = \mathbb{K}(x)$, we obtain:

Corollary 4.11. Every rational curve defined over $\mathbb{K}(x)$ admits a rational parametrization with coefficients in $\mathbb{K}(x)$.

In Theorem 3.8 we have seen that for an AODE having a strong rational general solution, the associated curve admits a rational parametrization with coefficients in $\mathbb{K}(x)$. Here we have proven even more: Actually, every rational curve admits such a parametrization.

Now we aim to compute the remaining intersection point. In order to do so, it requires to solve the polynomial system $F(y,z)=0, H(y,z,t)=0$. For this task resultants are suitable to eliminate one variable. By above construction, F and H do not have any common component, therefore, the resultant cannot be identically 0.

If a partial solution, obtained from the resultant, does not let both leading terms of F and $H(t)$ w.r.t. the other variable vanish, it can be extended to a full solution. Since $deg(F) \geq 3$, neither of the components of $\mathcal{P}(t)$ are constant. Let $y(t)$ be a partial solution. Consider

$$F(y,z) = F_n(y)z^n + \cdots + F_1(y)z + F_0(y) \ , \qquad \text{where } n \geq 1.$$

The term $F_n(y(t))$ cannot be identically 0, since F_n only depends on y. Therefore, if $\mathcal{P}(t) = \left(\frac{p_{11}(t)}{p_{12}(t)}, \frac{p_{21}(t)}{p_{22}(t)}\right)$ is the generic intersection point, the resultant factors as

$$\begin{aligned} res_z(F,H) &= \big(p_{12}(t)y - p_{11}(t)\big) \prod_{i=1}^{m} (b_i y - a_i)^{r_i} \ , \\ res_y(F,H) &= \big(p_{22}(t)z - p_{21}(t)\big) \prod_{i=1}^{n} (d_i z - c_i)^{s_i} \ . \end{aligned}$$

We just need to consider the primitive part with respect to t. Only one factor will stay, because we left only one intersection free. The rational parametrization can be obtained by the solutions of the linear equations

$$\begin{aligned} pp_t(res_z(F,H)) &= 0 \ , \\ pp_t(res_y(F,H)) &= 0 \ . \end{aligned}$$

Since p_{ij} are rational functions, the solution is rational too.

The following algorithm computed the optimal parametrization of a curve with coefficients in $\mathbb{K}(x)$, which again has coefficients in $\mathbb{K}(x)$. It is similar to that one in [SWPD08, page 133].

Algorithm 3: *OptimalParametrization*(F)

```
Input: Rational curve $F(y,z) = 0$, where $F \in \mathbb{K}(x)[y,z]$
Output: Proper rational parametrization of $F$ with coefficients in $\mathbb{K}(x)$
if $deg(F) \leq 3$ then
    return $ParametrizationByLines(F)$
Compute system of adjoint curves $\mathcal{A}_{d-2}(F)$
$R := PointsOnCurve(d-3, F)$
$H(t) := \mathcal{A}_{d-2}(F) \cap R$
$\mathcal{P}(t) := \big(solve(pp_t(res_z(F,H)) = 0), solve(pp_t(res_y(F,H)) = 0)\big)$
return $\mathcal{P}(t)$
```

This algorithm is much simpler than for a general field, since we are able to find $\mathbb{K}(x)$-rational points and therefore do not need to care about field extensions. Otherwise, we would have to proceed as described in Remark 4.9, see [SW97, Section 3.2].

Example 4.12 (Kamke 496)**.** Consider

$$F(x,y,y') = (x-y)^2(y'^2+1) - (y'+1)^2 = 0 \ .$$

The projective curve in $\mathbb{K}(x)[y,z,w]$ is

$$F(y,z,w) = (xw-y)^2(z^2+w^2) - (zw+w^2)^2 = 0 \ .$$

It has three double points $(1:0:0)$, $(0:1:0)$, $(x:-1:1)$. The system of adjoint curves is

$$\mathcal{A}_{d-2}(F) = t_1yz + t_2yw + t_3zw + xt_1w^2 - xt_2w^2 + t_3w^2 \ .$$

Since $deg(F) = 4$, we need one more simple point. We take $(x-1:0:1)$. The system of curves passing through these points is

$$t_1yz + t_2yw - xt_1zw + t_2zw - xt_2w^2 + t_2w^2 = 0 \ .$$

Setting $t_1 = t$ and $t_2 = 1$ yields

$$H(t) = tyz + yw - txzw + zw - xw^2 + w^2 \ .$$

We intersect F with $H(t)$. The resultant factors as

$$\begin{aligned} res_z(F,H) &= (x-1-y)(x-y)^2(-t^2y - y + (x+1)t^2 - 2t + x - 1) \ , \\ res_y(F,H) &= -z(z+1)^2(t^2z - z + 2t) \ . \end{aligned}$$

The last factor gives the primitive part with respect to t. We solve it for y and z. The remaining intersection point gives the parametrization

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

We further discuss the missing parts of the parametrization algorithm, the search of rational point on the curve.

5. Rational Points on Conics

For rational parametrization of conics we need an intersection point for the system of lines. In order to achieve that $\mathcal{P}$ has rational coefficients, this point has to be rational. For higher-degree curves we need rational simple points where our adjoint curves pass through. By Hilbert-Hurwitz, every curve can be transformed birationally to a curve of degree $d-2$. If the curve has odd degree, this leads to a line, which is easy to solve. But in the even case, we still remain with a conic. Our task now is to find one rational point on a conic.

To find any point is easy: Intersection of the conic with any line yields a family of two algebraic points. We aim to find a $\mathbb{K}(x)$-rational point, where $\mathbb{K}$ is algebraically closed. Note that $\mathbb{K}(x)$ is not.

For the rational numbers $\mathbb{Q}$, this problem was treated in [HW97]. A necessary and sufficient condition for the existence of a solution is given. We mainly follow this approach and refer to [HW97] for more details. The analogies and differences between $\mathbb{Q}$ and $\mathbb{K}(x)$ are pointed out. Many steps are similar. Not every conic has rational points. For example, the conic defined by the equation $x^2 + y^2 = 3$ does not have any rational point. In contrast to $\mathbb{Q}$, we actually can always find a $\mathbb{K}(x)$-rational point without having to extend the coefficient field.

For ease of computation, we expand our search to the projective plane $\mathbb{P}^2(\mathbb{K}(x))$. Allowing infinity relieves us to find points and enables us shorter expressions. This leads to shorter terms in the parametrization.

A general projective conic has the following form:

$$F = a\ y^2 + b\ yz + c\ z^2 + d\ yw + e\ zw + f\ w^2 = 0\ , \qquad \text{for } a,b,c,d,e,f \in \mathbb{K}(x). \tag{5.1}$$

It depends on 6 parameters, where in fact 5 are independent. We have to find $y, z, w \in \mathbb{K}(x)$ solving the equation (5.1). Since we can clear denominators, this task is equivalent to find $y, z, w \in \mathbb{K}[x]$.

We distinguish between parabolas, hyperbolas and ellipses. A parabola always admits a rational point, and we can give an explicit formula for it. In the hyperbolic/elliptic case we need an algorithmic approach. But for $\mathbb{K}(x)$ this will always succeed.

5.1. Trivial Case

If some parameters in (5.1) are 0, one can immediately find a point. In particular,

$$\begin{aligned} a = 0 &\Longrightarrow (1:0:0) \in \mathcal{C}_F\ , \\ c = 0 &\Longrightarrow (0:1:0) \in \mathcal{C}_F\ , \\ f = 0 &\Longrightarrow (0:0:1) \in \mathcal{C}_F\ . \end{aligned}$$

5.2. Parabolic Case

The conic (5.1) is a parabola if and only if the coefficients satisfy one of the following equalities

$$b^2 = 4ac \text{ or } d^2 = 4af \text{ or } e^2 = 4cf\ . \tag{5.2}$$

W.l.o.g. let $b^2 = 4ac$. The other cases are analogously. We can assume that $a, c, f \neq 0$. Then

$$\begin{aligned} 4cF &= \underbrace{4ac}_{b^2} y^2 + 4bcy + 4c^2z^2 + 4cdyw + 4cezw + 4cfw^2 \\ &= (by + 2cz)^2 + 4cw(dy + ez + fw) \ . \end{aligned}$$

If we can set the above equation to 0, we have found a point. This can be achieved by letting both summands be 0, so $by = -2cz$ and $w = 0$. The first equality is fulfilled by taking $y = -2c$ and $z = b$. So $(-2c : b : 0)$ lies on the conic.

Proceeding similarly, we can also find a point for the other cases. To sum up, we have the following results:

$$\begin{aligned} b^2 = 4ac &\Longrightarrow (-2c : b : 0) \in \mathcal{C}_F \ , \\ d^2 = 4af &\Longrightarrow (d : 0 : -2a) \in \mathcal{C}_F \ , \\ e^2 = 4cf &\Longrightarrow (0 : -2f : e) \in \mathcal{C}_F \ . \end{aligned}$$

5.3. Hyperbolic/Elliptic Case

In this case, the conic satisfies none of the previous relations in (5.2). This is characterized by

$$b^2 \neq 4ac \text{ and } d^2 \neq 4af \text{ and } e^2 \neq 4cf \ .$$

We define $D := b^2 - 4ac \neq 0$ and use the linear transformation

$$\begin{aligned} y &= D\bar{y} - b\bar{z} + a(2cd - be)\bar{w} \ , \\ z &= 2a\bar{z} + a(2ae - bd)\bar{w} \ , \\ w &= aD\bar{w} \ . \end{aligned}$$

Note that this is indeed a bijection. From the previous cases we can exclude $a = 0$ and $D = 0$. Therefore, the diagonal entries of the transformation matrix are non-zero. Then, some long computation yields

$$F = \underbrace{aD}_{\neq 0}(D\bar{y}^2 - \bar{z}^2 + M\bar{w}^2) \ ,$$

where $M = acd^2 - abde + a^2e^2 + ab^2f - 4a^2cf$. We need to find values $\bar{y}, \bar{z}, \bar{w}$ such that the above equation is set to 0.

We reach a conic in canonical form, i.e. where the mixed terms are eliminated

$$ay^2 + bz^2 + cw^2 = 0 \ , \qquad \text{for } a, b, c \in \mathbb{K}(x).$$

We want to work with polynomials instead of rational functions. This can be achieved by clearing denominators. The conic has the shape

$$Ay^2 + Bz^2 + Cw^2 = 0 \ , \qquad \text{for } A, B, C \in \mathbb{K}[x].$$

For $\mathbb{Q}$ one has to proceed similarly and arrive at integers A, B, C. Note that $\mathbb{K}(x)$ is the quotient field of $\mathbb{K}[x]$, like $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$. Both $\mathbb{Z}$ and $\mathbb{K}[x]$ are Euclidean domains, which allow modular arithmetic.

For further simplification, we divide by the $gcd(A, B, C)$. This modification does not change the solution.

We aim to make the coefficients squarefree. Therefore, we factor each polynomial into a squarefree and a square part. This requires the well-known squarefree factorization, but it is a bit different.

Proposition 5.1. Let F be a polynomial. Then there are unique F_1, F_2 such that $F = F_1 F_2^2$, and F_1 is squarefree.

Proof. Existence: Compute the squarefree decomposition $F = f_1\, f_2^2\, f_3^3 \ldots$, where $deg(f_i) = i$. Then we split up

$$f_1\, f_2^2\, f_3^3 \cdots = (\underbrace{f_1\, f_3\, f_5 \ldots}_{F_1})(\underbrace{f_2\, f_3\, f_4^2\, f_5^2\, f_6^3 \ldots}_{F_2})^2 \ .$$

The uniqueness follows from the uniqueness of the squarefree decomposition. □

This theorem can, in fact, be generalized to any Euclidean domain. Every Euclidean domain is a unique factorization domain. We proceed as described above and factor $A = A_1 A_2^2$, $B = B_1 B_2^2$, $C = C_1 C_2^2$, where A_1, B_1, C_1 are squarefree. This enables us the following substitution:

$$A_1 A_2^2 y^2 + B_1 B_2^2 z^2 + C_1 C_2^2 w^2 = A_1(\underbrace{A_2 y}_{\bar{y}})^2 + B_1(\underbrace{B_2 z}_{\bar{z}})^2 + C_1(\underbrace{C_2 w}_{\bar{w}})^2 \ .$$

We first search for a point $(\bar{y} : \bar{z} : \bar{w})$ of the simpler conic $A_1\bar{y} + B_1\bar{z} + C_1\bar{w} = 0$, then we compute the original solution $y = \frac{\bar{y}}{A_2}$, $z = \frac{\bar{z}}{B_2}$, $w = \frac{\bar{w}}{C_2}$. Thus, we have reduced the problem to squarefree polynomials. By a similar process, we can make all polynomials pairwise coprime. We reach the so-called Legendre Equation for polynomials:

$$Ay^2 + Bz^2 + Cw^2 = 0 \ , \qquad \text{for } A, B, C \in \mathbb{K}[x] \text{ pairwise coprime, squarefree.}$$

For integers we have a necessary and sufficient condition for the existence of a solution. This requires the following definition:

Definition 5.2. Let $A, B \in E$, where E is a Euclidean domain. We say that A is a *quadratic residue* modulo B, written as $A \mathcal{R} B$, iff there exists an $R \in \mathbb{K}[x]$ such that $R^2 \equiv A\ mod\ B$. In the affirmative case, we call R a *modular squareroot.*

Theorem 5.3 (Legendre, Version 1)**.** Let $A, B, C \in \mathbb{Z}$ pairwise coprime, squarefree and not all of them having the same sign. Then the equation

$$Ay^2 + Bz^2 + Cw^2 = 0$$

has a non-trivial solution if and only if

$$-AB \mathcal{R} C \text{ and } -AC \mathcal{R} B \text{ and } -BC \mathcal{R} A \ .$$

We try to adapt it to the polynomial case. The condition of the sign can be neglected, since we work with polynomials.

We consider a slightly different equation by clearing one polynomial:

$$\underbrace{AC}_{-\bar{A}}\,\bar{y}^2 + \underbrace{BC}_{-\bar{B}}\,\bar{z}^2 + (\underbrace{Cw}_{\bar{w}})^2 = 0 \ .$$

Of course, this step can be done with any of these three polynomials. To work with lower polynomial degrees afterwards, it makes sense to use the one with lowest degree.

Eventually, we reach the following state (Legendre, Version 2):

$$Ay^2 + Bz^2 - w^2 = 0 \ , \qquad \text{for } A, B \in \mathbb{K}[x] \text{ squarefree.} \tag{5.3}$$

We have to find a $\mathbb{K}(x)$-rational point on a conic of this form. For integers we have:

Theorem 5.4 (Legendre, Version 2)**.** Let $A, B \in \mathbb{Z}$ positive and squarefree. Then the equation

$$Ay^2 + Bz^2 - w^2 = 0$$

has a non-trivial solution if and only if

$$A \ \mathcal{R} \ B \text{ and } B \ \mathcal{R} \ A \text{ and } -\frac{AB}{gcd(A,B)^2} \ \mathcal{R} \ gcd(A,B) \ .$$

The proof of this theorem, as well as the equivalence of the two versions, can be found in [HW97].

Proposition 5.5. Let $A, B \in \mathbb{K}[x]$ squarefree. Then $A \ \mathcal{R} \ B$, i.e. there always exists a modular squareroot.

Proof. If $deg(A) = 0$, then every polynomial is a modular squareroot.

Otherwise, define R such that $R(x_i) = \sqrt{B(x_i)}$, where $x_i \in \mathbb{K}$ are the zeros of A. It holds $R(x)^2 \equiv B(x) \ mod \ x - x_i$, and because A is squarefree also $R(x)^2 \equiv B(x) \ mod \ A(x)$. □

This, however, is not the case for integers, namely $2 \not\mathcal{R} 3$. Therefore, the equation $2y^2 + 3z^2 - w^2 = 0$ does not have a solution in $\mathbb{Q}$.

Note that this fact makes the crucial difference between integers and polynomials. Since for any $A, B \in \mathbb{K}[x]$ the relation $A \ \mathcal{R} \ B$ holds, the right-hand-side of Theorems 5.3 and 5.4 are always satisfied. By combining the previous results, we obtain that the Legendre equation always admits a polynomial solution. So we have:

Theorem 5.6. Every projective conic with coefficients in $\mathbb{K}(x)$ has a $\mathbb{K}(x)$-rational point. Therefore, every irreducible conic admits a parametrization in $\mathbb{K}(x)$.

This theorem tells us that we do not need to extend the field of coefficients. It is particularly incredible, since it is not true for the simpler field $\mathbb{Q}$.

Now we aim to find a solution for (5.4). If $deg(A) = 0$, then $(1 : 0 : \sqrt{A})$ lies on the transformed conic. This point is really in $\mathbb{P}^2(\mathbb{K}(x))$, because B actually is constant and the ground field $\mathbb{K}$ is algebraically closed. So in that case, we finally have found a desired point on the conic. If $deg(B) = 0$, we have the point $(0 : 1 : \sqrt{B})$.

W.l.o.g. assume $deg(A) \geq deg(B)$. The strategy is the following: We construct a new conic $A_1y^2 + Bz^2 - w^2 = 0$ satisfying the same conditions as (5.3) with $deg(A_1) < deg(A)$. This process is carried out until one of the degrees becomes 0.

We again compute somehow the squareroot, but now the modular one. Let R be the modular squareroot of B modulo A, which from Proposition 5.5 always exists. So

$$R(x)^2 \equiv B(x) \ mod \ A(x) \ .$$

We consider the difference $R^2 - B$. This is a multiple of A. We compute the quotient $\frac{R^2-B}{A}$. From Proposition 5.1 we know that we can factor this into A_1S^2, where A_1 is squarefree.

We have shown that there exist $A_1, S \in \mathbb{K}[x]$ such that

$$R^2 - B = A\ A_1 S^2 \ .$$

We consider the new conic

$$A_1 y^2 + Bz^2 - w^2 = 0 \ . \tag{5.4}$$

We show that this conic is indeed "simpler". By construction of R, we have $deg(R) \leq deg(A) - 1$. We have

$$deg(A_1) = deg(R^2 - B) - deg(AS^2) \leq max\{2\underbrace{deg(R)}_{\leq deg(A)-1}, deg(B)\} - deg(A) < deg(A) \ .$$

If $deg(A) \geq 2$, the jump is even at least 2, since $max\{2(deg(A) - 1), deg(B)\} - deg(A) = deg(A) - 2$. So we really reached a conic with lower degree.

Assume we have a solution $(\bar{y} : \bar{z} : \bar{w})$ of the conic (5.4). Then

$$A_1 \bar{y}^2 + B\bar{z}^2 - \bar{w}^2 = 0 \ .$$

We multiply by $R^2 - B = AA_1S^2$ and obtain

$$AA_1S^2A_1\bar{y}^2 + (R^2 - B)(B\bar{z}^2 - \bar{w}^2) = 0$$

and further

$$A(A_1S\bar{y})^2 + B(R\bar{z} + \bar{w})^2 - (B\bar{z} + R\bar{w})^2 = 0 \ .$$

This gives us a point on the initial conic. Written in matrix notation, we have to use the following linear transformation

$$\begin{pmatrix} y \\ z \\ w \end{pmatrix} = \begin{pmatrix} A_1S & 0 & 0 \\ 0 & R & 1 \\ 0 & B & R \end{pmatrix} \begin{pmatrix} \bar{y} \\ \bar{z} \\ \bar{w} \end{pmatrix} \ .$$

The transformation is clearly invertible: It is a block matrix. Since $deg(A) > 0$, R is not identically zero. Since $deg(B) > 0$, $R^2 - B$ is not zero, and so neither is A_1.

Using these facts, we have the following properties:

1. $deg(A_1) < deg(A)$,
2. $Ay^2 + Bz^2 - w^2 = (\underbrace{R^2 - B}_{\neq 0})(A_1\bar{y}^2 + B\bar{z}^2 - \bar{w}^2)$.

The first statement promises us that the transformation serves us a new polynomial with lower degree. We repeat until we reach a conic $A_k y^2 + Bz^2 - w^2$ with $deg(A_k) < deg(B)$. Then we swap roles of A and B and continue. Eventually, one of the polynomials will get degree 0, and we can read off the solution as described above. The number of recurrences can be bounded by

$$\left\lceil \frac{deg(A)}{2} \right\rceil + \left\lceil \frac{deg(B)}{2} \right\rceil - 1 \ .$$

The second statement tells us that the new conic $A_1\bar{y}^2 + B\bar{z}^2 - \bar{w}^2$ will again have the same shape. We can proceed in the same way, then transform back. By using all the previous considerations, we obtain an algorithm.

Algorithm 4: *PointOnConic*(A, B)

```
Input: A projective conic of the form $Ay^2 + Bz^2 - w^2 = 0$, where $A, B \in \mathbb{K}[x]$ squarefree
Output: A $\mathbb{K}(x)$-rational point on this conic
if $deg(A) < deg(B)$ then
    $(z : y : w) := PointOnConic(B, A)$
    return $(y : z : w)$
if $deg(B) = 0$ then
    return $(0 : 1 : \sqrt{B})$
$R :=$ modular squareroot of $B$ modulo $A$
factor $\frac{R^2-B}{A}$ into $A_1S^2$
$(\bar{y} : \bar{z} : \bar{w}) := PointOnConic(A_1, B)$
return $\begin{pmatrix} y \\ z \\ w \end{pmatrix} = \begin{pmatrix} A_1S & 0 & 0 \\ 0 & R & 1 \\ 0 & B & R \end{pmatrix} \begin{pmatrix} \bar{y} \\ \bar{z} \\ \bar{w} \end{pmatrix}$
```

The algorithm clearly terminates, because $deg(A_1) < deg(A)$. It always finds a rational point, since for the base case we can read off a solution. At the end, we transform the point back to the initial curve.

Example 5.7. Consider the conic

$$F = (x^2 - x)\ y^2 + 4x\ z^2 - w^2 = 0\ .$$

So we have $A = x^2 - x$ and $B = 4x$. We have $R(0) = 0$ and $R(1) = \sqrt{4} = 2$, and therefore the modular squareroot $R = 2x$. Then $\frac{R^2-B}{A} = 4 \cdot 1$.

We obtain a new conic

$$G = 4\ y^2 + 4x\ z^2 - w^2 = 0\ ,$$

where we can read of $(1 : 0 : 2)$ as rational point. Backtransformation yields

$$\begin{pmatrix} 4 & 0 & 0 \\ 0 & 2x & 1 \\ 0 & 4x & 2x \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 4 \\ 2 \\ 4x \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \\ 2x \end{pmatrix}\ .$$

So $(2 : 1 : 2x)$ is a rational point on F.

In this chapter we have seen that there always exists a $\mathbb{K}(x)$-rational point and how to compute it. The main difference of $\mathbb{K}(x)$ to $\mathbb{Q}$ is the existence of a modular squareroot, i.e. an $R \in \mathbb{K}[x]$ such that

$$R(x)^2 \equiv B(x)\ mod\ A(x)\ .$$

Still, it is a hard task to find this R. The proof of Proposition 5.5 is constructive. R can be computed by polynomial interpolation: Let R pass through the points $(x_i, \sqrt{x_i})$, for all zeros x_i of A.

An alternative way is to use partial fraction decomposition. Let $x_1, \dots, x_n$ be the zeros of A. We compute

$$\frac{B}{A} = \frac{c_1}{x - x_1} + \cdots + \frac{c_n}{x - x_n} \ , \qquad \text{for some } c_i \in \mathbb{K}.$$

Further assume

$$\frac{R}{A} = \frac{d_1}{x - x_1} + \cdots + \frac{d_n}{x - x_n} \ , \qquad \text{for some } d_i \in \mathbb{K}.$$

We define $A_i(x) = \prod_{j \neq i}(x - x_j)$. Then

$$\begin{aligned} B &= A \ \frac{B}{A} = c_1 A_1 + \cdots + c_n A_n \ , \\ R &= A \ \frac{R}{A} = d_1 A_1 + \cdots + d_n A_n \ . \end{aligned}$$

For all x_i, we require

$$R(x_i)^2 = B(x_i) \ .$$

Since $R(x_i) = d_i A_i(x_i)$ and $B(x_i) = c_i A_i(x_i)$, we conclude

$$\begin{aligned} d_i^2 A_i^2 &= c_i A_i \ , \\ d_i &= \sqrt{\frac{c_i}{A_i(x_i)}} \ . \end{aligned}$$

Although there is this nice property of the existence of $\mathbb{K}(x)$-rational points on conics, it can be tedious to find one. Mostly, this is the hardest part of the computation. A development of better methods would improve the algorithm.

6. Hilbert-Hurwitz Method

The parametrization algorithm requires $d-3$ simple points on F. Letting the system of adjoint curves pass through all of them, leaves exactly one parameter free, which leads to the parametrization of F. So we have reduced our problem of finding a rational parametrization to the problem of finding rational simple points on F. In this chapter let K be a field, e.g. $\mathbb{Q}$ or $\mathbb{K}(x)$, where $\mathbb{K}$ is algebraically closed.

Given: An algebraic projective plane curve $F(y,z,w) = 0$, where $F \in K[y,z,w]$ defines a curve of genus 0.

Find: Rational simple points on F, i.e. points $P = (p_1 : p_2 : p_3) \in \mathbb{P}^2(K)$ such that $F(p_1,p_2,p_3) = 0$.

Note that it is an easy task to find singular points, which are not of our interest. This requires to solve a system of non-linear equations. But they might appear in a family of conjugate points, which are not rational anyway.

Already in 1890, David Hilbert and Adolf Hurwitz considered that problem in [HH90]. They suggested a method using birational transformation. We basically follow their ideas.

Let F be an irreducible, rational curve of degree d. We again require F having only ordinary singularities.

6.1. Birational Transformation

Before we go through the method, we state some definitions.

Definition 6.1. Let $V \subseteq \mathbb{A}^m(K)$, $W \subseteq \mathbb{A}^n(K)$ be two algebraic sets. A *rational mapping* $\varphi = (\varphi_1, \ldots, \varphi_n)$ is an n-tuple of rational functions such that for almost all points $P \in V$, we have $(\varphi_1(P), \ldots, \varphi_n(P)) \in W$.

Definition 6.2. A rational mapping $\varphi : V \to W$ is a *birational isomorphism* iff it has a rational inverse, i.e. there exits a rational map $\psi : W \to V$ such that $\psi \circ \varphi = id_V$ and $\varphi \circ \psi = id_W$. A birational isomorphism into itself is called a *birational transformation.*

In the following, we consider birational transformations of algebraic curves. Such a map can be seen as a bijection up to finitely many exceptions.

The idea of the following approach consists of using birational transformation defined by the adjoint curves to F of degree $d-2$.

Theorem 6.3 (Hilbert-Hurwitz)**.** Let F be a rational curve of degree $d > 2$. For almost all $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \in \mathcal{A}_{d-2}(F)$, the mapping

$$\mathcal{T} \; = \; (y : z : w) \mapsto (\mathcal{T}_1(y,z,w) : \mathcal{T}_2(y,z,w) : \mathcal{T}_3(y,z,w))$$

transforms F birationally to a rational curve of degree $d-2$.

Proof. See [SW97, Theorem 2.1]. Take $a = d - 2$. □

The above theorem gives rise to the following idea: We successively apply birational transformation to obtain a curve of degree $d - 2$. This procedure has to be continued until eventually we reach a line or a conic, depending on whether the degree of the curve was odd or even. In total, $\mathcal{O}(d)$ steps are required.

- d odd:
$$F \longrightarrow \ldots \longrightarrow \text{line}$$
- d even:
$$F \longrightarrow \ldots \longrightarrow \text{conic}$$

Let H be the generic representative of the adjoint curves of degree $d - 2$. Then

$$H = t_1\phi_1 + t_2\phi_2 + \cdots + t_{d-1}\phi_{d-1} \ ,$$

where $t_i \in K$ and $\phi_i \in K[y, z, w]$ are homogeneous of degree $d - 2$. We pick three elements $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ of the system generated by H and define $\mathcal{T} = (\mathcal{T}_1(y, z, w) : \mathcal{T}_2(y, z, w) : \mathcal{T}_3(y, z, w))$.

Let G be the curve obtained after applying the transformation $\mathcal{T}$ to F, see Figure 6.1. Since $\mathcal{T}$ is birational, almost every rational point on F corresponds to a rational point on G and vice versa. Note that the birational transformation leaves the genus invariant, see [Wal78, Section VI.5.3]. So rationality is preserved.

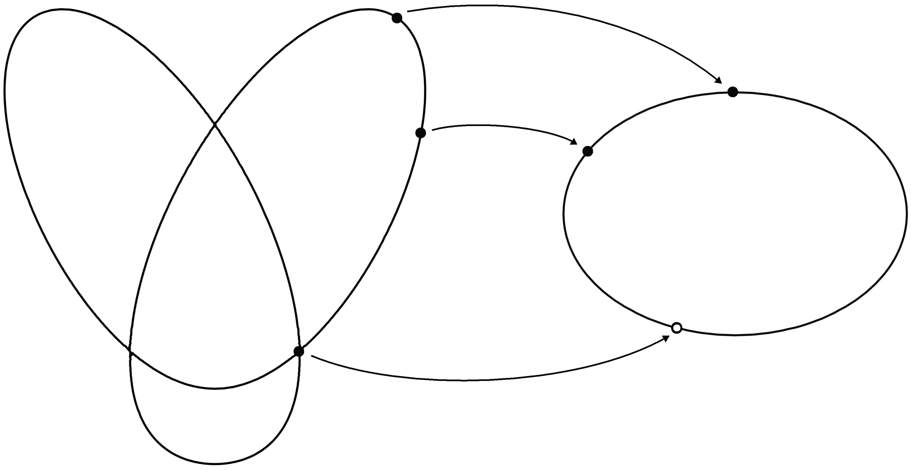


Figure 6.1.: Birational transformation

The new curve $G(\bar{y}, \bar{z}, \bar{w}) = 0$ consists of the points

$$(\bar{y} : \bar{z} : \bar{w}) = (\mathcal{T}_1(y, z, w) : \mathcal{T}_2(y, z, w) : \mathcal{T}_3(y, z, w)) \ . \tag{6.1}$$

G is irreducible and of degree $d-2$. The original problem is reduced to finding points on a curve of degree $d - 2$. But since we do not know any point on F, we neither know any of G. We need to find the implicit equation $G(\bar{y}, \bar{z}, \bar{w}) = 0$. From (6.1) we obtain the following relations:

$$\begin{aligned} F(y, z, w) &= 0 \ , \\ \mathcal{T}_1(y, z, w) &= \bar{y} \ , \\ \mathcal{T}_2(y, z, w) &= \bar{z} \ , \\ \mathcal{T}_3(y, z, w) &= \bar{w} \ . \end{aligned}$$

Since we are in the projective space, we could actually choose $(\bar{y}, \bar{z}, \bar{w}) = (a\mathcal{T}_1, a\mathcal{T}_2, a\mathcal{T}_3)$ for any $a \in K\backslash\{0\}$. The resulting polynomial differs only up to a constant, and therefore, it defines the same curve. But for simplicity, we just take $i = 1$.

To obtain the implicit equation, we have to solve this non-linear system for $\bar{y}, \bar{z}, \bar{w}$. We have to find the polynomial in

$$\langle F, \mathcal{T}_1 - \bar{y}, \mathcal{T}_2 - \bar{z}, \mathcal{T}_3 - \bar{w} \rangle \cap K[\bar{y}, \bar{z}, \bar{w}] \ .$$

Any elimination technique might be used. Gröbner Bases are a common tool to deal with that problem, because of the elimination property, see [Win96, Theorem 8.4.5]. So G can be computed by

$$GB(\langle F, \mathcal{T}_1 - \bar{y}, \mathcal{T}_2 - \bar{z}, \mathcal{T}_3 - \bar{w} \rangle)_{lex\ \bar{y},\bar{z},\bar{w}<y,z,w} \cap K[\bar{y}, \bar{z}, \bar{w}] \ .$$

We continue this reduction, until we finally reach a line or a conic. For these types, there are methods available. In Chapter 5 it is described how to find a rational point on a conic. Every conic has a $\mathbb{K}(x)$-rational point. In the odd case, in practise, we already stop at degree 3. For cubics, the only singularity is always rational. More points can be found using parametrization by lines. This gives arbitrary many rational points.

Example 6.4 (Kamke 496)**.** Consider the curve

$$F(y, z, w) = (xw - y)^2(z^2 + w^2) - (zw + w^2)^2 = 0$$

defined over $\mathbb{K}(x)$. The system of adjoint curves is

$$\mathcal{A}_{d-2}(F) = t_1 yz + t_2 yw + t_3 zw + xt_1 w^2 - xt_2 w^2 + t_3 w^2 \ .$$

We choose the following transformation

$$\mathcal{T} = (yz + xw^2, yw - xw^2, zw + w^2) \ .$$

In order to compute the transformed curve, we have to solve

$$\begin{aligned} F(y, z, w) &= 0 \ , \\ yz + xw^2 &= \bar{y} \ , \\ yw - xw^2 &= \bar{z} \ , \\ zw + w^2 &= \bar{w} \end{aligned}$$

for $\bar{y}, \bar{z}, \bar{w}$. We obtain a conic defined by

$$G(\bar{y}, \bar{z}, \bar{w}) = \bar{y}^2 + \bar{z}^2 - 2x\bar{y}\bar{w} + (x^2 - 1)\bar{w}^2 \ .$$

With the help of Chapter 5, we can find the rational point $(x : -1 : 1)$ on G.

6.2. Inversion of Points

We have seen how to map an algebraic curve into a conic or a cubic and how to eventually find some rational points on the transformed curve. But we also have to get back to the initial curve. Fortunately, we just have to invert some particular points and do not need to compute the inverse of the map $\mathcal{T}$.

Let $Q = (q_1 : q_2 : q_3)$ on G be an invertible point and $\mathcal{T}$ a birational transformation from F to G. Then there exists exactly one $P = (p_1 : p_2 : p_3)$ on F such that

$$(\mathcal{T}_1(p_1, p_2, p_3) : \mathcal{T}_2(p_1, p_2, p_3) : \mathcal{T}_3(p_1, p_2, p_3)) = (q_1 : q_2 : q_3) \ .$$

Assume w.l.o.g. $q_3 \neq 0$. Then we have to solve the non-linear system

$$\begin{aligned} F(p_1, p_2, p_3) &= 0 \ , \\ \mathcal{T}_1(p_1, p_2, p_3)q_3 - \mathcal{T}_3(p_1, p_2, p_3)q_1 &= 0 \ , \\ \mathcal{T}_2(p_1, p_2, p_3)q_3 - \mathcal{T}_3(p_1, p_2, p_3)q_2 &= 0 \ . \end{aligned} \tag{6.2}$$

Since $\mathcal{T}$ is birational, we expect only one point. However, the solution of (6.2) is not unique. Observe that every singularity is a solution. But after removing all solutions of

$$(\mathcal{T}_1(p_1, p_2, p_3), \mathcal{T}_2(p_1, p_2, p_3), \mathcal{T}_3(p_1, p_2, p_3)) = (0, 0, 0) \ ,$$

equation (6.2) will have a unique solution.

Since we work in the projective plane, the outcome is in fact 1-dimensional. To avoid this, we can solve the system separately for $p_3 = 1$ and $p_3 = 0$ and union the obtained sets. This approach also reduces the number of unknown variables.

The inversion of a rational point again delivers a rational point: Let $P = (p_1(\alpha) : p_2(\alpha) : p_3(\alpha)) \in \mathbb{P}^2(K(\alpha))$ be the result of the inversion in (6.2), where $m(\alpha) = 0$ is the minimal polynomial. Let $n = deg(m)$. But then there would exist $P_1, \ldots, P_n$ such that $\mathcal{T}(P_1) = Q, \ldots, \mathcal{T}(P_n) = Q$. But since $\mathcal{T}$ is birational, it has to be $n = 1$, and therefore, P is rational. □

Example 6.5 (Kamke 496)**.** The transformed curve G contains the rational point $q = (x : -1 : 1)$. In order to transform the point back to the initial curve, we have to solve

$$\begin{aligned} &F(p_1, p_2, p_3) = (xp_3 - p_1)^2(p_2^2 + p_3^2) - (p_2p_3 + p_3^2)^2 = 0 \ , \\ &\mathcal{T}_1 - x\mathcal{T}_3 = p_1p_2 + xp_3^2 - x(p_2p_3 + p_3^2) = 0 \ , \\ &\mathcal{T}_2 + 1\mathcal{T}_3 = p_2p_3 - xp_3^2 + p_2p_3 + p_2^2 = 0 \ . \end{aligned}$$

This system has the solution points $(1 : 0 : 0)$, $(0 : 1 : 0)$, $(x : -1 : 1)$ and $(x - 1 : 0 : 1)$. The first three are the singularities of F. So the remaining point $p = (x - 1 : 0 : 1)$ is the inverse of q, and it is a rational simple point on F. Indeed,

$$\mathcal{T}(x - 1, 0, 1) = (x : -1 : 1) \ .$$

A birational transformation might have some points where the relation is not 1-1. We call them exceptional points. The image of these points are not invertible. In particular, they come from the application of $\mathcal{T}$ to a singularity, see Figure 6.1. We just have to take another point Q on G. Since a curve has only finitely many singularities, there can only be finitely many exceptional points. Therefore, termination is ensured.

6.3. Algorithms

We have seen how to transform a curve birationally to a curve of lower degree where we can already find points on it, and we showed how to invert the discovered points back.

This method suggests a recursive approach. After each transformation we have to deal with a curve of degree $d-2$ and proceed similarly.

```
Algorithm 5: $PointsOnCurve(n, F)$
Input: $n \in \mathbb{N}$, rational curve $F = 0$ having only ordinary singularities
Output: $n$ rational simple points on $F$
if $deg(F) \leq 3$ then
    $\mathcal{P} := ParametrizationByLines(F)$
    return $\{\mathcal{P}(i_1), \ldots, \mathcal{P}(i_n)\}$
$\mathcal{T} :=$ any birational transformation
$G := \mathcal{T}(F)$
$Q := PointsOnCurve(n, G)$
return $\mathcal{T}^{-1}(Q)$
```

In the base case we can easily compute the parametrization. This enables us to pick arbitrary many points. To obtain short expressions, we might use the sequence $\{i_1, \ldots, i_n\} = \{0, 1, -1, 2, -2, \ldots\}$.

Unfortunately, this attempt has one problem: Since some points might not be invertible, we will lose them during one of the inversion steps. We can trace them by computing

$$\lim_{t \to t_S} \mathcal{T}(\mathcal{P}(t)) ,$$

where $\mathcal{P}(t_S)$ is a singularity. But since we do not know the parametrization in advance, we neither can avoid taking an exceptional point. There are only finitely many non-invertible points, so it is unlikely to pick one of those. But since our choices for points on G are not random, we still might hit some of them.

Example 6.6 (Kamke 496)**.** The points $(x \pm 1 : 0 : 1)$ of the transformed curve are not invertible. Using the already in Example 4.12 calculated parametrization $\mathcal{P}(t) = \big((x+1)t^4 - 2t^3 - 2t^2 + 2t - x + 1 : -2t^3 - 2t : t^4 - 1\big)$, we can find out that $\mathcal{P}(1) = \mathcal{P}(-1) = (0 : 1 : 0)$ is a singularity of F. We have

$$(\mathcal{T} \circ \mathcal{P})(t) = (t^2 x - 2t + x : t^2 - 1 : t^2 + 1) .$$

Then $(\mathcal{T} \circ \mathcal{P})(1) = (x - 1 : 0 : 1)$ and $(\mathcal{T} \circ \mathcal{P})(-1) = (x + 1 : 0 : 1)$ are their targets on G. So $\mathcal{T}$ maps the point $(0 : 1 : 0)$ simultaneously to $(x - 1 : 0 : 1)$ and $(x + 1 : 0 : 1)$. Therefore, these points cannot be invertible.

We can bound the number of exceptional points by $\sum_{S \in Sing(F)} mult_S(F)$. We would need to compute $n + \sum_{S \in Sing(F)} mult_S(F)$ rational points on G to be sure that we receive enough points on F. But then we would do many inversions in vain. Thus, we definitely prefer the iterative approach:

Algorithm 6: *PointsOnCurve*(n, F)

```
Input: $n \in \mathbb{N}$, rational curve $F = 0$ having only ordinary singularities
Output: $n$ rational simple points on $F$
$\mathcal{T} := id$
$G := F$
while $deg(G) > 3$ do
    $\bar{\mathcal{T}}$ := any birational transformation
    $G := \bar{\mathcal{T}}(G)$
    $\mathcal{T} := \bar{\mathcal{T}} \circ \mathcal{T}$
$\mathcal{P}(t) := ParametrizationByLines(G)$
$P := \emptyset$
while $|P| < n$ do
    $i$ := new $K$-rational number
    $q := \mathcal{P}(i)$
    $P := P \cup \mathcal{T}^{-1}(q)$
return $P$
```

Here, we concatenate all transformations. Another advantage is that for each point the inversion requires to solve only one system of equations, instead of $\mathcal{O}(d)$.

6.4. The Choice of the Transformation

So far, we have highly taken for granted that our transformation is birational. Indeed, for all but a set of lower dimension, it is the case. So the chances for a wrong choice are very low, and in the negative case, we can just pick a new one. But still the question remains how to detect a transformation that was not birational.

The system of adjoint curves of degree $d-2$ can be written as

$$\mathcal{A}_{d-2}(F) = t_1\phi_1 + t_2\phi_2 + \cdots + t_{d-1}\phi_{d-1} \ .$$

For almost all $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3 \in \mathcal{A}_{d-2}$, the mapping $\mathcal{T} = (\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3)$ defines a birational transformation to a curve of degree $d-2$. In the following, we study what choice to make to ensure that $\mathcal{T}$ is birational and how to catch a transformation that is not birational.

Let $\mathcal{P}(t)$ be a proper rational parametrization of F. Consider the rational mapping $\mathcal{T}$ from F to G. Then $\mathcal{T}$ is birational if and only if $\mathcal{Q}(t) = \mathcal{T}(\mathcal{P}(t))$ is proper. $\mathcal{Q}(t)$ parametrizes G. Let $\mathcal{Q}(t) = \left(\frac{q_{11}(t)}{q_{12}(t)}, \frac{q_{21}(t)}{q_{22}(t)}\right)$. $\mathcal{Q}$ is proper if and only if the *gcd* of

$$\begin{aligned} &q_{11}(s)q_{12}(t) - q_{12}(s)q_{11}(t) \text{ and} \\ &q_{21}(s)q_{22}(t) - q_{22}(s)q_{21}(t) \end{aligned}$$

is linear in t. For almost all choices of $\mathcal{T}$, the degree is 1. But since we do not know the parametrization in advance, we are not able to check this condition.

If $\mathcal{T}$ is not birational, the degree might drop by more than 2. This does not bother us, as long as the new curve is still irreducible and of genus 0. Both can be checked easily. In fact, if G is reducible, we can just consider one component of this curve. We only need any rational points on F. They do not need to be distributed over the whole curve. Actually, this would make the computation even faster, since fewer transformation steps are needed.

The problem actually occurs in inverting. If $\mathcal{T}$ is not surjective, it still does not matter, since we only need to invert some particular points and not the whole map. But if $\mathcal{T}$ is not injective, a rational point Q on G might came from many points $P_1, \ldots, P_n$ on F, i.e. we have $\mathcal{T}(P_1) = \cdots = \mathcal{T}(P_n) = Q$. If those points are rational, this is still okay. But otherwise, we have to break up the computation and restart with new $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$.

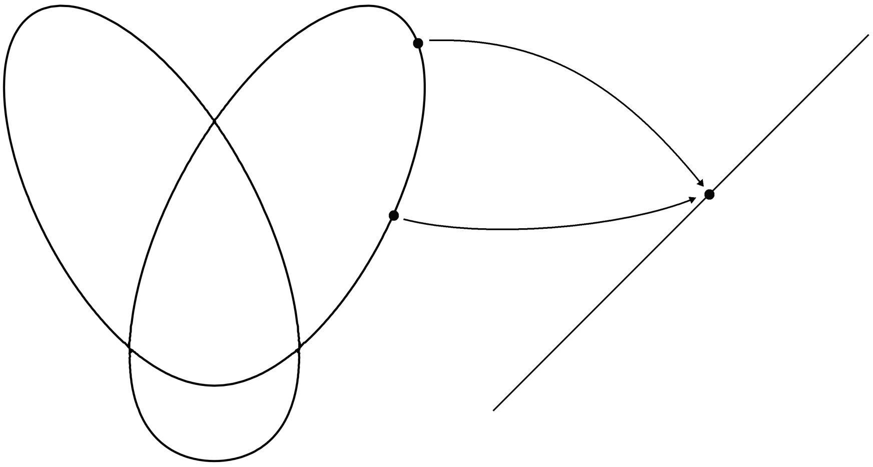


Figure 6.2.: Transformation not birational

Even if $\mathcal{T}$ is birational, the degree might decrease by more than 2. If the adjoint curves are chosen in such a way that points are fixed by the singularities, then there is less degree of freedom, hence $deg(G) < d - 2$.

The system of adjoint curves of degree $d - 2$ can be written as

$$\mathcal{A}_{d-2}(F) = t_1\phi_1 + t_2\phi_2 + \cdots + t_{d-1}\phi_{d-1} \; .$$

First observe that if $\mathcal{T}_1, \mathcal{T}_2, \mathcal{T}_3$ are linearly dependent, then G is linear. Thus, the degree reduction is not 2, and the risk of not being birational is high.

So on the one hand, $\mathcal{T}$ should be chosen simple in order to receive simpler polynomials. But if the selection is to simple, e.g. linear dependency, we run in danger that the transformation is not birational. The most natural choice is $\mathcal{T} = (\phi_1 : \phi_2 : \phi_3)$. Since $d \geq 4$, this selection is always possible. In the very unlikely negative case, one can try every permutation and combination of three of the $d - 1$ ϕ_i's.

This concludes the discussion about the parametrization algorithm. We now turn back to algebraic differential equations and use parametrization to eventually solve them.

7. Solving Differential Equations

In the following, we combine the results of the previous chapters to finally solve first-order AODEs.

7.1. The Associated Equation

We aim to solve the differential equation $F(x, y, y') = 0$ and consider the algebraic curve $F(y, z) = 0$ over $\mathbb{K}(x)$. Let $\mathcal{P} = (p_1(x, t), p_2(x, t)) \in (\mathbb{K}(x)(t))^2$ be a proper rational parametrization of F. We want the first coordinate to be the desired function y and the second its derivative y'. Since curve parametrization is invariant under transformation, we have to find a $T(x)$ such that

$$(p_1(x, T(x)), p_2(x, T(x))) = (y(x), y'(x)) \ .$$

So the second coordinate should be the derivative of the first. We conclude

$$p_2(x, T(x)) = \frac{d}{dx} p_1(x, T(x)) = \frac{\partial p_1}{\partial x}(x, T) + T'(x) \frac{\partial p_1}{\partial t}(x, T) \ .$$

Thus, $T(x)$ satisfies the following equation:

$$T' = \frac{p_2(x, T) - \frac{\partial p_1}{\partial x}(x, T)}{\frac{\partial p_1}{\partial t}(x, T)} \ . \tag{7.1}$$

The denominator of (7.1) cannot be 0. Assume for contrary, $\frac{\partial p_1}{\partial t}(x, T) = 0$. Then p_1 would only depend on x and therefore also the solution y. Hence, it can be no rational general solution.

$(y(x), y'(x))$ has to lie in the image of $\mathcal{P}$. Since $im(\mathcal{P})$ is dense in $\mathcal{C}_F$, the set $\mathcal{C}_F \backslash im(\mathcal{P})$ consists of only finitely many isolated points. But then y would not be a general solution. Therefore, $(y(x), y'(x)) = \mathcal{P}(T(x))$, for some function $T(x)$.

Definition 7.1. Let $\mathcal{P} = (p_1(x, t), p_2(x, t)) \in (\mathbb{K}(x)(t))^2$ be a rational parametrization of F. The differential equation

$$T' = \frac{p_2(x, T) - \frac{\partial p_1}{\partial x}(x, T)}{\frac{\partial p_1}{\partial t}(x, T)}$$

is called *associated differential equation* to F.

Theorem 7.2. Let $\mathcal{P} = (p_1, p_2)$ be a proper rational parametrization with coefficients in $\mathbb{K}(x)$. Then there is a 1-1-correspondence between rational solutions of the initial AODE $F(x, y, y') = 0$ and the associated equation (7.1).

Proof. Let $T(x)$ be a rational solution of the associated equation. Then, by the above construction, $y(x) = p_1(x, T(x))$ solves the AODE. Since all operations are rational, $y(x)$ is rational too.

On the other hand, let $y(x)$ be a rational solution of the AODE. Then $(y(x), y'(x)) = \mathcal{P}(T(x))$, for some $T(x)$. Since $\mathcal{P}$ is proper, it has a rational inverse, and therefore, $T(x) = \mathcal{P}^{-1}(y(x), y'(x))$ is rational. □

From the proof we can conclude how to transform one solution to the other. Given the rational general solution $T(x)$ of the associated equation, we can compute

$$y(x) = p_1(x, T(x))$$

to obtain the rational general solution of the AODE.

Example 7.3. The AODE

$$F = y'^2 - 3xy' - y + 3x^2 = 0$$

has the rational proper parametrization

$$\mathcal{P}(x,t) = (t^2 - 3xt + 3x^2,\ t)\ .$$

We compute

$$\frac{p_2(x,t) - \frac{\partial p_1}{\partial x}(x,t)}{\frac{\partial p_1}{\partial t}(x,t)} = \frac{t - (-3t + 6x)}{2t - 3x} = 2\ .$$

The associated equation $T' = 2$ has the rational general solution $T(x) = 2x + c$, leading to the rational general solution of F by

$$y(x) = p_1(x, T(x)) = x^2 + cx + c^2\ .$$

Example 7.4. Theorem 7.2 is not true if $\mathcal{P}$ is not proper or has coefficients in a field extension of $\mathbb{K}(x)$. Consider the differential equation

$$F = y' + y^2 = 0\ .$$

This equation clearly has a rational general solution $y(x) = \frac{1}{x+c}$. Therefore, one side of Theorem 7.2 is satisfied.

A rational parametrization which is not proper is

$$\mathcal{P} = (t^2, -t^4)\ .$$

Then

$$\frac{p_2(x,t) - \frac{\partial p_1}{\partial x}(x,t)}{\frac{\partial p_1}{\partial t}(x,t)} = -\frac{t^3}{2}\ .$$

The equation $T' = -\frac{T^3}{2}$ has the algebraic general solution

$$T(x) = \frac{1}{\sqrt{x+c}}\ .$$

A rational proper parametrization in which the coefficients do not lie in $\mathbb{K}(x)$ is

$$\mathcal{P} = (\sqrt{x}t, -xt^2)\ .$$

Then

$$\frac{p_2(x,t) - \frac{\partial p_1}{\partial x}(x,t)}{\frac{\partial p_1}{\partial t}(x,t)} = -\sqrt{x}t^2 - \frac{t}{2x}\ .$$

The general solution of the associated equation is

$$T(x) = \frac{1}{\sqrt{x}(x+c)}\ .$$

In both cases, we can actually still obtain the rational general solution of F by computing $p_1(x, T(x)) = \frac{1}{x+c}$.

Since we choose $\mathcal{P}$ to be an optimal parametrization, we can expect its coefficients to lie in $\mathbb{K}(x)$. Therefore, the associated equation is of the form

$$T' = \frac{a_0 + a_1 T + \cdots + a_m T^m}{b_0 + b_1 T + \cdots + b_n T^n} \ , \qquad \text{for some } a_i, b_i \in \mathbb{K}(x). \tag{7.2}$$

Thus, it is a quasilinear first-order differential equation. For such type of equation there exists a wide range of solution methods. If $m > 2$ or $n > 0$, this equation only has finitely many rational solutions, see [BC11]. Thus, (7.2) cannot have a rational general solution and so neither has $F(x, y, y') = 0$.

Note that we require the coefficients to be rational functions. Otherwise, all the above considerations would not be applicable.

Summarizing, we get the following theorem.

Theorem 7.5. If $F(x, y, y') = 0$ has a rational general solution and is parametrizable, where $\mathcal{P}$ is proper and has coefficients in $\mathbb{K}(x)$, then its associated equation is of the form

$$T'(x) = a_0(x) + a_1(x)T(x) + a_2(x)T(x)^2 \ ,$$

for some $a_0, a_1, a_2 \in \mathbb{K}(x)$.

This type is called a Riccati equation. Kovacic [Kov86] gave an algorithm for solving linear second-order differential equations. As a side-calculation, he computed Riccati equations. We can decide the existence of a rational general solution.

Note that every Riccati equation can be transformed into a linear second-order differential equation: Consider

$$r' + ar^2 + br + cr = 0 \ .$$

Let $r = a\frac{y'}{y}$. Then $r' = a\frac{y''y - y'^2}{y^2} = a\frac{y''}{y} - ar^2$. Substituting into the Riccati equation leads to

$$a\frac{y''}{y} + \underbrace{ab}_{\bar{b}}\frac{y'}{y} + c = 0 \ ,$$

$$ay'' + \bar{b}y' + cy = 0 \ .$$

The same is true for the other direction: Consider

$$y'' + ay' + by = 0 \ .$$

Let $y = e^{\int r}$. Then $y' = e^{\int r} r$ and $y'' = e^{\int r} r' + e^{\int r} r^2$. Inserting yields

$$r' + r^2 + ar + b = 0 \ ,$$

which is again a Riccati equation.

In the result of a Riccati equation also the constant c appears rationally. Therefore, for parametrizable AODEs, the notion of rational and strong rational coincide.

7.2. Decision Algorithm for AODEs

In this section we finally state an algorithm that decides whether an AODE has a strong rational general solution and if so, computes it. See also [VGW18, Algorithm 2].

Algorithm 7: *StrongRational*(F)

```
Input: An AODE $F(x, y, y') = 0$, where $F \in \mathbb{K}[x, y, z] \backslash \mathbb{K}[x, y]$ irreducible
Output: A strong rational general solution of $F$, or "No strong rational general solution exist"
if $F$ is reducible over $\overline{\mathbb{K}(x)}$ or genus$(F) > 0$ then
    return "No strong rational general solution exists"
compute the rational proper optimal parametrization $\mathcal{P} = (p_1(x,t), p_2(x,t)) \in (\mathbb{K}(x)(t))^2$
$f(x,t) := \frac{p_2(x,t) - \frac{\partial p_1}{\partial x}(x,t)}{\frac{\partial p_1}{\partial t}(x,t)}$
if $f$ has the form $a_0(x) + a_1(x)t + a_2(x)t^2$ then
    solve the Riccati equation $T'(x) = f(x, T(x))$
    if it has a rational general solution then
        return $y(x) := p_1(x, T(x,c))$
return "No (strong) rational general solution exists"
```

The first condition comes from Theorem 3.8. For parametrizable AODEs we compute the optimal parametrization over $\mathbb{K}(x)$, in which the coefficients are still in $\mathbb{K}(x)$. This leads us to the associated equation. From that solution we obtain the solution of the AODE by substituting into p_1.

In the last step we can actually omit the word "strong", since for parametrizable AODEs, a rational general solution is a strong rational general solution. But only for strong rational general solutions we have a full decision algorithm.

Example 7.6 (Kamke 547)**.** Consider the equation

$$F(x, y, y') = y'^4 - 4y(xy' - 2y)^2 = 0 \ .$$

The corresponding curve has one triple point at the origin, intersection with $L(t) = z - ty$ yields

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

We compute

$$\frac{p_2(x,t) - \frac{\partial p_1}{\partial x}(x,t)}{\frac{\partial p_1}{\partial t}(x,t)} = -\frac{t^2}{2} \ .$$

The associated equation

$$T' = -\frac{T^2}{2}$$

has the solution $T(x) = \frac{2}{x+c}$. The solution of F is given by

$$y(x) = p_1(x, T(x)) = c^2(x+c)^2 \ .$$

So far, neither Mathematica nor Maple are able to give a general solution of this differential equation.

Example 7.7 (Clairaut's equation)**.** Consider the differential equation

$$y = xy' + f(y') \ .$$

A parametrization can be immediately found by conversion:

$$\mathcal{P}(t) = (xt + f(t), t) \ .$$

In this case, the second component is already the derivative of the first. We can read off the general solution

$$y(x) = cx + f(c) \ .$$

Example 7.8 (Chrystal's equation)**.** The equation reads as

$$y' + Axy' + By + Cx^2 = 0 \ ,$$

for some constants A, B, C. The rational parametrization is

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

We compute

$$\frac{p_2(x,t) - \frac{\partial p_1}{\partial x}(x,t)}{\frac{\partial p_1}{\partial t}(x,t)} = \frac{(A+B)t + 2Cx}{-2t - Ax} \ .$$

Chrystal's equation has a rational general solution if and only if the remainder is zero. This is the case if and only if $A^2 + AB = 4C$. Then the associated equation is

$$T' = -\frac{A+B}{2} \ ,$$

which has the solution $T(x) = -\frac{A+B}{2}x + c$. The rational general solution of the Chrystal's equation is

$$y(x) = p_1(x, T(x)) = \frac{A^2 - B^2 - \overbrace{4C}^{A^2+AB}}{4B} x^2 + cx - \frac{1}{B}c^2 = -\frac{A+B}{4}x^2 + cx - \frac{1}{B}c^2 \ .$$

8. Conclusion

We have seen a method that decides whether a first-order AODE has a strong rational general solution and in the affirmative case computes it.

Since the AODE is considered as curve, this approach requires curve parametrization. The coefficients lie in the field of rational functions. It turns out that this field has the nice property that we do not need to extend the field of coefficients.

The parametrization requires rational points on the curve. The key observation is the existence of a rational point on a conic. Birational transformation is used to transform a curve to another one of lower degree. Unfortunately, birationality cannot be checked in advance. For almost all cases, the transformation is indeed birational. But in practice, one might pick a bad choice, and therefore, we have to take care how to deal with that case. For every curve it is possible to find rational points on it. But though having these nice properties, the computation gets very tedious. Better methods would promote the algorithm.

We use the computed rational parametrization to transform the initial AODE into a quasilinear one, where we rely on proven methods. Since only Riccati-equations admit rational general solutions, we have reduced the problem to solving Riccati-equations.

The particular strength of this program is the ability to deal with differential equations where the derivative occurs in higher degree. Conventional methods often fail. For those AODEs having no strong rational general solution, still the existence can be decided.

A. Implementation

The implementation will be integrated into the program system of finding rational general solutions of differential equations which is currently developed at RISC.

In the following implementation, our ground field $\mathbb{K} = \overline{\mathbb{Q}}$, the field of algebraic numbers. For the main functions `ParametrizeKx` and `StrongRational` input and output conditions are checked. The others rely on a correct usage.

A.1. Parametrization over $\mathbb{K}(x)$

In the following, an implementation of rational parametrization of curves over $\mathbb{K}(x)$ is given, as described in Algorithm 3.

FUNCTION ParametirzeKx

Input:

- `F` $\in \mathbb{K}[$`x`$,$`y`$,$`z`$]$ rational affine curve over $\mathbb{K}($`x`$)$ having only ordinary singularities
- `x`,`y`,`z`,`t`: variables

Output:

A proper rational parametrization of `F` with coefficients in $\mathbb{K}($`x`$)$, i.e. `P` $\in \mathbb{K}($`x`$,$`t`$)^2$ such that `F`(`P[1]`(`t`)$,$`P[2]`(`t`)) $= 0$.

Description:

For lines, convert the equation. For conics and curves having one singularity, do parametrization by lines. Otherwise, compute system of adjoits `H`. Find $deg($`F`$)-3$ points on `F`, and force `H` to go through them. Intersect `F` with `H`. The last intersection point gives the parametrisation.

Source code:

```
ParametrizeKx := proc(F, x::name, y::name, z::name, t::name)
  local F_, P, w;
  F_ := Algebraic:-ConvertRootOf(F);
  if not type(F_, 'polynom'('radalgnum', [x, y, z])) then
    error "input must be a polynomial in the given variables";
  end if;
  if not evala(AIrreduc(primpart(F_, {y, z}))) then
    error "input is reducible";
  end if;
  if numelems({x,y,z,t}) <> 4 then
    error "input variables must be distinct";
  end if;
  if algcurves:-genus(F_, y, z) <> 0 then
    error "genus not 0";
  end if;
  P := parametrizeKxProj(Groebner:-Homogenize(F_, w, {y, z}), x, y, z, w, t);
  if P[3] = 0 then
    error "check input condition";
  end if;
  P := evala(Simplify([P[1]/P[3], P[2]/P[3]]));
  # check if parametrization is generic point on F
  if simplify(eval(F_, {y = P[1], z = P[2]})) = 0 and member(t, indets(P)) then
    return P;
  end if;
  error "incorrect parametrization";
end proc;
```

```
parametrizeKxProj := proc(F, x, y, z, w, t)
  local a, b, c, deg, p, sing, ext, H, P, i, cond, v, ppt;
  deg := degree(F, {y, z, w});
  if deg = 1 then
    # F = a*y+b*z+c*w
    a, b, c := coeff(F, y), coeff(F, z), coeff(F, w);
    if b <> 0 then return [b*t, -a*t - c, b]; end if;
    if a <> 0 then return [-b*t - c, a*t, a]; end if;
    error "Not possible";
  elif deg = 2 then
    # F = a*y^2+b*yz+c*z^2+d*yw+e*zw+f*w^2
    p := pointOnConic(F, x, y, z, w);
    return parametrizeByLines(F, p, x, y, z, w, t);
  end if;
  sing := algcurves:-singularities(eval(F, w = 1), y, z);
  if nops(sing) = 1 and sing[1, 2] = deg - 1 then
    return parametrizeByLines(F, sing[1, 1], x, y, z, w, t);
  end if;
  ext := indets[flat](F, ':-`radalgext`'); # extension of field of definition
  if add(sing[i][2]*(sing[i][2] - 1)
     *Algebraic:-Degree(indets[flat](sing[i], ':-`radalgext`') minus ext),
     i = 1 .. nops(sing)) < (deg - 1)*(deg - 2) then
    error "non-ordinary singularity";
  end if;
  H := adjoints(deg - 2, sing, t, y, z, w, ext);
  # find additional points on the curve
  P := pointsOnCurve(deg - 3, F, x, y, z, w);
  # let H pass through these points
  cond := map(p -> eval(H, {w = p[3], z = p[2], y = p[1]}) = 0, P);
  H := subs(solve(cond, {seq(t[i], i = 1 .. deg - 1)}), H);
  v := indets(H) intersect {seq(t[i], i = 1 .. deg - 1)};
  H := simplify(subs(v[1] = t, v[2] = 1, H));
  # intersect F and H
  ppt := map(v -> Algebraic:-PrimitivePart(
          Algebraic:-Resultant(eval(F, w = 1), eval(H, w = 1), v), t), [y, z]);
  return [-coeff(ppt[2], y, 0)/coeff(ppt[2], y),
          -coeff(ppt[1], z, 0)/coeff(ppt[1], z), 1];
end proc;
```

Example:

```
> ParametrizeKx(z^4 - 4*y*(x*z - 2*y)^2, x, y, z, t)
>      [4*(t^2*x^2 - 4*t*x + 4)/t^4, 4*(t^2*x^2 - 4*t*x + 4)/t^3]
```

There is already a function available for parametrization over the rationale numbers $\mathbb{Q}$. We could actually also use it by just neglecting `x`.

```
> algcurves:-parametrization(z^4 - 4*y*(x*z - 2*y)^2, y, z, t)
>      [4*(t^2*x^2 - 4*t*x + 4)/t^4, 4*(t^2*x^2 - 4*t*x + 4)/t^3]
```

But since this function might use field extensions, we cannot apply it for our problem.

```
> algcurves:-parametrization(x*y^2 + z^2 - 1, y, z, t)
>       [(RootOf(_Z^2 + x)*t^2 - RootOf(_Z^2 + x))/(2*x*t), (t^2 + 1)/(2*t)]
```

Therefore, the above method is really necessary.

Unfortunately, irreducibility over $\overline{\mathbb{K}(x)}$ cannot be checked in Maple 2019. For instance, $(y+z)^2 - x = (y+z-\sqrt{x})(y+z+\sqrt{x})$ is reducible, but in Maple it is considered to be irreducible.

```
> evala(AIrreduc((y+z)^2 - x));
>       true
```

For this problem, Magma provides a method. But the given Maple implementation relies on a correct input.

A.2. Parametrization by Lines

If the curve has not more than one singularity, we can parametrize by lines. The following function is an implementation of Algorithm 2.

FUNCTION parametrizeByLines

Input:

- $\mathtt{F} \in \mathbb{K}(\mathtt{x})[\mathtt{y},\mathtt{z},\mathtt{w}]$ projective curve that is parametrizable by lines
- p: point on F, which is any rational point (if F is a conic) or the only singularity (for higher degree)
- x,y,z,t,w: variables

Output:

A proper rational parametrization of F with coefficients in $\mathbb{K}(\mathtt{x})$, i.e. $\mathtt{P} \in \mathbb{K}(\mathtt{x},\mathtt{t})^3$ such that $\mathtt{F}(\mathtt{P[1](t)},\mathtt{P[2](t)},\mathtt{P[3](t)}) = 0$.

Description:

Make a change of coordinates to move p to the origin. Intersect F with a pencil of lines through the origin. Then move the curve back. (If last entry of p is 0, swap roles, and proceed analogously.)

Source code:

```
parametrizeByLines := proc(F, p, x, y, z, w, t)
  local P;
  if p[3] <> 0 then
    return parametrizeByLinesAux(F, p, x, y, z, w, t);
  elif p[2] <> 0 then
    P := parametrizeByLinesAux(F, [p[1], p[3], p[2]], x, y, w, z, t);
    return [P[1], P[3], P[2]];
  elif p[1] <> 0 then
    P := parametrizeByLinesAux(F, [p[2], p[3], p[1]], x, z, w, y, t);
    return [P[3], P[1], P[2]];
  end if;
  error "invalid point";
end proc;
```

```
parametrizeByLinesAux := proc(F, p, x, y, z, w, t)
  local deg, G, Gd, Gd_1;
  deg := degree(F, {y, z, w});
  G := subs(y = y + p[1]/p[3], z = z + p[2]/p[3], w = 1, F);
  Gd, Gd_1 := homogeneousPart(G, {y, z}, deg), homogeneousPart(G, {y, z}, deg-1);
  return [p[1]*eval(Gd, {y = 1, z = t}) - p[3]*eval(Gd_1, {y = 1, z = t}),
          p[2]*eval(Gd, {y = 1, z = t}) - p[3]*t*eval(Gd_1, {y = 1, z = t}),
          p[3]*eval(Gd, {y = 1, z = t})];
end proc;
```

Example:

```
> parametrizeByLines(-w^2 + y^2 + z^2, [-1, 0, 1], x, y, z, w, t)
>       [-t^2 + 1, 2*t, t^2 + 1]
```

FUNCTION homogeneousPart

Input:

- `F` polynomial
- `vars`: set of variables
- `d`: integer

Output:

The homogeneous part of `F` of degree `d`.

Source code:

```
homogeneousPart := proc(F, vars, d)
  local F_, monomlist, hom;
  F_ := collect(F, vars, 'distributed'); # expand to sum of monomials
  monomlist := ifelse(type(F_, '`+`'), [op(F_)], [F_]); # collect monoms in a list
  hom := select(m -> evalb(degree(m, vars) = d), monomlist);
  return foldl(`+`, 0, op(hom));
end proc;
```

Example:

```
> homogeneousPart(y^2 + 3*y*z + 2*z, {y, z}, 2)
>       y^2 + 3*y*z
```

A.3. Points on Conics

We need one point on the conic. The following functions are dedicated to this search. We proceed as described in Chapter 5.

FUNCTION pointOnConic

Input:

- $\mathtt{F} \in K(\mathtt{x})[\mathtt{y}, \mathtt{z}, \mathtt{w}]$ projective conic
- `x`,`y`,`z`,`w`: variables

Output:

A point the conic, i.e. $(\mathtt{y} : \mathtt{z} : \mathtt{w}) \in \mathbb{P}^2(\mathbb{K}(\mathtt{x}))$ such that $\mathtt{a}\,\mathtt{y}^2 + \mathtt{b}\,\mathtt{yz} + \mathtt{c}\,\mathtt{z}^2 + \mathtt{d}\,\mathtt{yw} + \mathtt{e}\,\mathtt{zw} + \mathtt{f}\,\mathtt{w}^2 = 0$.

Description:

Distinguish between the different cases. If the curve is elliptic/hyperbolic, transform conic to canonical form, and find a point there. Then transform the discovered point back.

Source code:

```
pointOnConic := proc(F, x::name, y::name, z::name, w::name)
  local a, b, c, d, e, f, D, y_, z_, w_;
  a, b, c, d, e, f := coeff(F,y^2), coeff(coeff(F,y),z), coeff(F,z^2),
                      coeff(coeff(F,y),w), coeff(coeff(F,z),w), coeff(F,w^2);
  if f = 0 then return [0, 0, 1];
  elif c = 0 then return [0, 1, 0];
  elif a = 0 then return [1, 0, 0];
  end if;
  D := simplify(b^2 - 4*a*c);
  # parabolic case
  if D = 0 then
    return simplifyProjPoint([-2*c, b, 0], x);
  end if;
  # elliptic, hyperbolic case
  y_, z_, w_ := op(pointOnConicCanonicalForm(D, -1,
                 a^2*e^2 - b*a*d*e + a*c*d^2 + a*b^2*f - 4*a^2*c*f, x));
  return simplifyProjPoint([D*y_ - b*z_ + a*(2*d*c - b*e)*w_,
                           2*a*z_ + a*(2*a*e - b*d)*w_, a*D*w_], x);
end proc;
```

Example:

```
> pointOnConic(x*y^2 - w^2 - y*z + z^2, x, y, z, w)
>       [0, 1, -1]
```

FUNCTION pointOnConicCanonicalForm

Input:

- $\mathtt{a}, \mathtt{b}, \mathtt{c} \in \mathbb{K}(\mathtt{x})$ rational functions
- $\mathtt{x}$: variable

Output:

A point on a conic in canonical form, i.e. $\mathtt{y}, \mathtt{z}, \mathtt{w} \in \mathbb{K}(\mathtt{x})$ such that $\mathtt{a}\ \mathtt{y}^2 + \mathtt{b}\ \mathtt{z}^2 + \mathtt{c}\ \mathtt{w}^2 = 0$.

Source code:

```
pointOnConicCanonicalForm := proc(a, b, c, x)
  local A, B, C, A1, A2, B1, B2, C1, C2, y, z, w, i;
  # clear denominators: A*y^2+B*z^2+C*w^2 = 0
  A, B, C := numer(a)*denom(b)*denom(c), denom(a)*numer(b)*denom(c),
             denom(a)*denom(b)*numer(c);
  A, B, C := op(divByGCD([A, B, C], x));
  A1, A2 := factorLinearSquare(A, x);
  B1, B2 := factorLinearSquare(B, x);
  C1, C2 := factorLinearSquare(C, x);
  # A1*A2^2*y^2+B1*B2^2*z^2+C1*C2^2*w^2 = A1*(A2*y)^2+B1*(B2*z)^2+C1*(C2*w)^2
  i := min[index]([degree(A1), degree(B1), degree(C1)]); # find poly of min degree
  if i = 1 then
    z, w, y := op(legendre(B1, C1, A1, x));
  elif i = 2 then
    y, w, z := op(legendre(A1, C1, B1, x));
  else # i=3
    y, z, w := op(legendre(A1, B1, C1, x));
  end if;
  return simplifyProjPoint([y/A2, z/B2, w/C2], x);
end proc;
```

FUNCTION legendre

Input:

- $\mathtt{A}, \mathtt{B}, \mathtt{C} \in \mathbb{K}[\mathtt{x}]$ squarefree polynomials, where $deg(\mathtt{C})$ should be lowest
- $\mathtt{x}$: variable

Output:

$\mathtt{y}, \mathtt{z}, \mathtt{w} \in \mathbb{K}(x)$ such that $\mathtt{A}\ \mathtt{y}^2 + \mathtt{B}\ \mathtt{z}^2 + \mathtt{C}\ \mathtt{w}^2 = 0$.

Source code:

```
legendre := proc(A, B, C, x)
  local y, z, w;
  # clear one polynomial: A*C*y^2 + B*C*z^2 + C^2*w^2 = A1*y^2 + B1*z^2 + w1^2
  y, z, w := op(legendreAux(-A*C, -B*C, x));
  return simplifyProjPoint([y, z, w/C], x);
end proc;
```

We again have transformed the equation to $Ay^2 + Bz^2 - w^2 = 0$ and apply the same procedure as Algorithm 4.

FUNCTION legendreAux

Input:

- $\mathtt{A}, \mathtt{B} \in \mathbb{K}[\mathtt{x}]$ squarefree polynomials
- $\mathtt{x}$: variable

Output:

$\mathtt{y}, \mathtt{z}, \mathtt{w} \in \mathbb{K}(\mathtt{x})$ such that $\mathtt{A}\ \mathtt{y}^2 + \mathtt{B}\ \mathtt{z}^2 - \mathtt{w}^2 = 0$.

Description:

Transform the conic into $\mathtt{A1}\ \mathtt{y}^2 + \mathtt{B}\ \mathtt{z}^2 - \mathtt{w}^2 = 0$, where $deg(\mathtt{A1}) < deg(\mathtt{A})$. Find a point on that conic. Transform the discovered point back.

Source code:

```
legendreAux := proc(A, B, x)
  local y, z, w, R, A1, S;
  if degree(A, x) < degree(B, x) then
    z, y, w := op(legendreAux(B, A, x));
    return simplifyProjPoint([y, z, w], x);
  end if;
  if degree(B, x) = 0 then
    return [0, 1, sqrt(B)];
  end if;
  R := msqrt(B, A, x); # R^2 = A mod M
  A1, S := factorLinearSquare(quo(R^2 - B, A, x), x); # R^2 - B = A*A1*S^2
  # A*y_^2 + B*z_^2 - w_^2 = (R^2 - B) * (A1*y^2 + B*z^2 - w^2)
  y, z, w := op(legendreAux(A1, B, x));
  # A*(A1*S*y)^2 + B*(R*z + w)^2 - (B*z + R*w)^2 = 0
  return simplifyProjPoint([A1*S*y, R*z + w, B*z + R*w], x);
end proc;
```

Example:

```
> legendreAux(x^2 - x, 4*x, x)
>      [2, 1, 2*x]
```

FUNCTION factorLinearSquare

Input:

- $\mathtt{F} \in \mathbb{K}[\mathtt{x}]$ polynomial
- x: variable

Output:

$\mathtt{L}, \mathtt{S} \in \mathbb{K}[\mathtt{x}]$ such that $\mathtt{F} = \mathtt{L}\ \mathtt{S}^2$, where L is squarefree.

Description:

Compute the squarefree factorization of F and order the terms in a suitable way.

Source code:

```
factorLinearSquare := proc(F, x)
  local cont, f, odd, i;
  cont, f := op(sqrfree(F, x));
  # F = F1*F2^2*F3^3*... = (F1*F3*F5*...)*(F2*F3*F4^2*F5^2*F6^3*...)^2
  odd := select(a -> a[2] mod 2 = 1, f); # select those factors with odd powers
  return cont*mul(odd[i][1], i = 1 .. nops(odd)),
         mul(f[i][1]^floor(1/2*f[i][2]), i = 1 .. nops(f));
end proc;
```

Example:

```
> factorLinearSquare((x + 1)*(x + 2)^2*(x - 1)^3*x^4, x)
>       (x + 1)*(x - 1), (x + 2)*(x - 1)*x^2
```

FUNCTION msqrt

Input:

- $\mathtt{A}, \mathtt{M} \in \mathbb{K}[\mathtt{x}]$ squarefree polynomials
- x: variable

Output:

The modular squareroot $\mathtt{R} \in \mathbb{K}[\mathtt{x}]$ such that $\mathtt{R}^2 = \mathtt{A}$ *mod* M.

Description:

Compute R by polynomial interpolation of the points $(\mathtt{xi}, \sqrt{\mathtt{A(xi)}})$, for all roots xi of M.

Source code:

```
msqrt := proc(A, M, x)
  local rts, pts, xi, R;
  rts := [solve(M, x)];
  pts := map(xi -> [xi, sqrt(eval(A, x = xi))], rts);
  R := CurveFitting:-PolynomialInterpolation(pts, x);
  return evala(Simplify(R));
end proc;
```

Example:

```
> msqrt(4*x, x^2 - x, x)
>       2*x
```

A.4. Adjoint Curves

To compute the adjoint curves, we have to generate a linear system of curves. It is also useful to construct curves passing through given points.

FUNCTION linearSystem

Input:

- `deg`: integer
- `P`: list of projective points with associated multiplicities
- `t`,`y`,`z`,`w`: variables
- `ext`: set of extensions to $\mathbb{Q}$

Output:

System of curves of degree `deg` passing through all points in `P` with corresponding multiplicities.

Description:

Set up a linear system of curves `H` of degree `deg`. Go through all points `p` in `P`. If `p` is rational, `H(p[1],p[2],p[3])` = 0 provides one linear condition on `H`. If `p` is a family of points, *rem*(`H(p[1](a),p[2](a),p[3](a))`,`m(a)`) = 0 provides *deg*(`m`) linear conditions on `H`. If *mult* `p` > 1, also consider the partial derivatives.

Source code:

```
linearSystem := proc(deg, P, t, y, z, w, ext)
  local D, power, monom, H, pm, p, mult, deriv, r, n, cond, m, i, v;
  D := (deg + 1)*(deg + 2)/2; # number of coefficients
  power := map(c -> c - [1, 1, 1], combinat:-composition(deg + 3, 3));
  monom := map(c -> y^c[1]*z^c[2]*w^c[3], power);
  H := sum(t[i]*monom[i], i = 1 .. D);
  for pm in P do
    p, mult := pm[1], pm[2];
    deriv := [op(map(c -> c - [1, 1, 1], combinat:-composition(mult + 2, 3)))];
    # linear conditions on point
    r := indets[flat](p, ':-`radalgext`') minus ext; # r contains one element
    n := Algebraic:-Degree(r);
    if n = 1 then # p is rational
      cond := map(d -> eval(diff(H, [y$d[1], z$d[2], w$d[3]]),
                {y=p[1], z=p[2], w=p[3]}) = 0, deriv);
    else # p is family of points
      # minimal polynomial of p, expressed in a
      m := algsubs(_Z = a, op(1, r[1]));
      # remove RootOf(...), make p polynomial point:
      # F(p1(a),p2(a),p3(a)) = 0 mod m(a)
      p := simplifyProjPoint(subs(r[1] = a, p), x);
      cond := map(d -> map(c -> coeff(rem(eval(diff(H, [y$d[1], z$d[2], w$d[3]]),
                {w=p[3], z=p[2], y=p[1]}), m, a), a, c) = 0,
                [seq(i, i = 0 .. n-1)]), deriv);
    end if;
    # substitute linear conditions in H
    H := subs(solve(ListTools:-Flatten(cond), {seq(t[i], i = 1 .. D)}), H);
  end do;
  v := indets(H) intersect {seq(t[i], i = 1 .. D)};
  H := subs({seq(v[i] = t[i], i = 1 .. nops(v))}, H);
  return numer(H);
end proc;
```

Example:

```
> linearSystem(2, [[[0,0,1], 1], [[0,1,1], 1], [[1,0,1], 1]], t, y, z, w, {})
>     w*y*t[1] + w*z*t[3] - y^2*t[1] + y*z*t[2] - z^2*t[3]
```

After setting up a linear system, we are able to compute the adjoint curves, the system of curves passing through all singularities with corresponding multiplicities minus 1.

FUNCTION adjoints

Input:

- `deg`: integer
- `sing`: singularities of a curve
- `t`,`y`,`z`,`w`: variables
- `ext`: set of extensions to $\mathbb{Q}$

Output:

System of adjoint curves of degree `deg`.

Source code:

```
adjoints := (deg, sing, t, y, z, w, ext) ->
            linearSystem(deg, map(s -> [s[1], s[2] - 1], sing), t, y, z, w, ext);
```

A.5. Hilbert-Hurwitz Method

For parametrization we require $d - 3$ simple points on the curve. As described in Chapter 6, this can be done using birational transformation. An implementation of the Hilbert-Hurwitz method, Algorithm 6, is given in the following function.

FUNCTION pointsOnCurve

Input:

- `n`: integer
- $\texttt{F} \in \mathbb{K}(\texttt{x})[\texttt{y}, \texttt{z}, \texttt{w}]$ rational projective curve having only ordinary singularities
- `x`,`y`,`z`,`w`: variables

Output:

`n` rational simple points on `F`.

Description:

Successively use birational transformation defined by adjoint curves to transform `F` into a conic/cubic. The transformed curve `G` can be obtained by the elimination ideal $\langle \texttt{F}, \texttt{T[1]} - \texttt{y\_}, \texttt{T[2]} - \texttt{z\_}, \texttt{T[3]} - \texttt{w\_} \rangle \cap K[\texttt{y\_}, \texttt{z\_}, \texttt{w\_}]$. Compute rational parametrization of `G`. Successively pick a point on `G` and invert it until `n` simple points on `F` are found. If a point is not rational, `T` was not birational. Then try again with different arrangement of adjoint curves.

Source code:

```
pointsOnCurve := proc(n, F, x, y, z, w, num_try := 1)
  local points, T, G, d, sing, ext, H, v, T_, Id, El, P, t, i, q, p;
  points := {};
  T := [y, z, w]; # T=id
  G := F;
  d := degree(G, {y, z, w});
  try
    while d > 3 do # transform to lower degree
      sing := algcurves:-singularities(eval(G, w = 1), y, z);
      ext := Algebraic:-GetAlgebraics(G); # extension of field of definition
      if add(sing[i][2]*(sing[i][2] - 1)
          *Algebraic:-Degree(indets[flat](sing[i], ':-‘radalgext‘'))
```

```
         minus ext), i = 1 .. nops(sing)) < (d - 1)*(d - 2) then
        error "non-ordinary singularity";
      end if;
      H := adjoints(d - 2, sing, t, y, z, w, ext); # deg-1 parameters free
      v := map(i -> LinearAlgebra:-UnitVector(i, d - 1),
           combinat:-permute(d - 1, 3)[num_try]);
      T_ := [eval(H, t = v[1]), eval(H, t = v[2]), eval(H, t = v[3])];
      Id := PolynomialIdeals:-PolynomialIdeal({G, T_[1]-y_, T_[2]-z_, T_[3]-w_},
            variables = {w_, y_, z_, y, z, w});
      # Id intersect K[y_,z_,w_]
      El := PolynomialIdeals:-EliminationIdeal(Id, {w_, y_, z_});
      G := PolynomialIdeals:-Generators(El)[1];
      G := subs(y_ = y, z_ = z, w_ = w, G);
      d := degree(G, {y, z, w});
      T := subs({y = T[1], z = T[2], w = T[3]}, T_); # T=T_(T)
    end do;
    P := parametrizeKxProj(G, x, y, z, w, t);
    i := 0;
    while nops(points) < n do # pick points and invert them
      q := simplifyProjPoint(eval(P, t = i), x);
      p := invertPoint(q, T, F, x, y, z, w);
      points := points union {p};
      i := ifelse(i > 0, -i, -i + 1); # 0, 1, -1, 2, -2, ...
    end do;
    return points;
    catch: return pointsOnCurve(n, F, x, y, z, w, num_try + 1);
  end try;
end proc;
```

FUNCTION invertPoint

Input:

- q: projective point
- T: birational transformation
- $F \in \mathbb{K}(x)[y, z, w]$ rational projective curve having only ordinary singularities
- x,y,z,w: variables

Output:

A point p on F such that T(p) = q.

Description:

Solve F(y, z, w) = 0, (T[1](y,z,w) : T[2](y,z,w) : T[3](y,z,w)) = (q[1] : q[2] : q[3]). Separately solve affine solutions and solutions at infinity. If q is invertible, the system has a unique solution and the singularities. Remove these singularities. If the point is not rational, T was not birational.

Source code:

```
invertPoint := proc(q, T, F, x, y, z, w)
  local M, sol0, sol1, P;
  if q[1] <> 0 then
    M := T[2]*q[1] - T[1]*q[2], T[3]*q[1] - T[1]*q[3];
  elif q[2] <> 0 then
    M := T[1]*q[2] - T[2]*q[1], T[3]*q[2] - T[2]*q[3];
  elif q[3] <> 0 then
    M := T[1]*q[3] - T[3]*q[1], T[2]*q[3] - T[3]*q[2];
  else
    error "invalid point";
  end if;
  # affine solutions
  sol1 := {solve({eval(M[1],w=1)=0, eval(M[2],w=1)=0, eval(F,w=1)=0}, {y,z})};
  # solutions at infinity
  sol0 := {solve({eval(M[1],w=0)=0, eval(M[2],w=0)=0, eval(F,w=0)=0}, {y,z})};
  P := map(s -> subs(s, [y, z, 1]), sol1) union map(s -> subs(s, [y, z, 0]), sol0);
  # remove (T1(p):T2(p):T3(p)) = (0:0:0)
  P := remove(p -> simplify(eval(T, {w=p[3], z=p[2], y=p[1]})) = [0, 0, 0], P);
  if nops(P) = 0 then
    return NULL;
  end if;
  if nops(P) = 1 and type(P[1], 'list'('ratpoly'('anything', x))) then
    return simplifyProjPoint(P[1], x);
  end if;
  error "T not birational";
end proc;
```

A.6. Simplify Points over $\mathbb{K}(x)$

In order to work with shorter expressions, we need a function that simplifies the projective points. Particularly, the search of $\mathbb{K}(x)$-rational points delivers us complicated expressions. So we require our own simplify function.

FUNCTION simplifyProjPoint

Input:

- $\mathtt{p} \in \mathbb{P}^2(\mathbb{K}(\mathtt{x}))$ projective point of rational functions
- `x`: variable

Output:

The same point with polynomial coefficients and in simplified representation.

Description:

Simplify content and primitive part separately, and multiply them together.

Source code:

```
simplifyProjPoint := proc(p, x)
  local P, pp, cont;
  P := [numer(p[1])*denom(p[2])*denom(p[3]),
        denom(p[1])*numer(p[2])*denom(p[3]),
        denom(p[1])*denom(p[2])*numer(p[3])];
  P := evala(Simplify~(P));
  P := divByGCD(P, x);
  # split into content and primitive part
  pp := primpart~(P, x);
  cont := simplifyProjConst(content~(P, x));
  return pp *~ cont;
end proc;
```

Example:

```
> simplifyProjPoint([x^2 - 1, x + 1, x^2 + 2*x + 1], x)
>       [x - 1, 1, x + 1]
```

FUNCTION divByGCD

Input:

- $\mathtt{p} \in \mathbb{P}^2(\mathbb{K}(\mathtt{x}))$ projective point of polynomials
- $\mathtt{x}$: variable

Output:

The same point with coordinates relative prime.

Source code:

```
divByGCD := proc(p, x)
  local g;
  g := gcd(p[1], gcd(p[2], p[3]));
  return evala(Simplify~([quo(p[1], g, x), quo(p[2], g, x), quo(p[3], g, x)]));
end proc;
```

FUNCTION simplifyProjConst

Input:

- $\mathtt{p} \in \mathbb{P}^2(\mathbb{K})$ projective point of constants
- $\mathtt{x}$: variable

Output:

The same point in simplified representation.

Source code:

```
simplifyProjConst := proc(p)
  local n, l;
  n := evala(Simplify(evala(Normal(normalizeProjPoint(p)))));
  l := lcm(denom(n[1]), lcm(denom(n[2]), denom(n[3])));
  return l *~ n;
end proc;
```

FUNCTION normalizeProjPoint

Input:

- $\mathtt{p} \in \mathbb{P}^2(\mathbb{K})$ projective point of constants
- $\mathtt{x}$: variable

Output:

The same point with last non-zero coordinate 1.

Source code:

```
normalizeProjPoint := p -> if p[3] <> 0 then return p /~ p[3];
                           elif p[2] <> 0 then return p /~ p[2];
                           elif p[1] <> 0 then return p /~ p[1];
                           else error "invalid point"; end if;
```

Sometimes it is useful to know whether two projective points are equal. Checking this fact is different to the affine space.

FUNCTION equalProjPoint

Input:

- `p`: projective point
- `x`: variable

Output:

`true` if they are equal, `false` otherwise.

Description:

It suffices to check the following equalities, since $(a : b : c) = (d : e : f) \iff \frac{a}{b} = \frac{d}{e}, \frac{a}{c} = \frac{d}{f}, \frac{b}{c} = \frac{e}{f} \iff ae = bd, af = cd, bf = ce.$

Source code:

```
equalProjPoint := (p, q) -> simplify(p[1]*q[2] - p[2]*q[1]) = 0 and
                            simplify(p[1]*q[3] - p[3]*q[1]) = 0 and
                            simplify(p[2]*q[3] - p[3]*q[2]) = 0;
```

Example:

```
> equalProjPoint([1, 2, 3], [2, 4, 6])
>     true
```

A.7. Strong Rational General Solutions

Using the rational parametrization over $\mathbb{K}(x)$ enables us to find strong rational general solutions of AODEs, as described in Chapter 7. In order to solve Ricatti equations we use the Maple function `dsolve`. Unfortunately, Maple is not able to only look for rational solutions. So we cannot fully decide the existence of a strong rational general solution.

FUNCTION StrongRational

Input:

- $\mathtt{F} \in \mathbb{K}[\mathtt{x}, \mathtt{y}(\mathtt{x}), \mathtt{y}'(\mathtt{x})]$ defining an AODE where `F` is irreducible over $\mathbb{K}(\mathtt{x})$
- `y`,`x`,`c`: variables

Output:

A strong rational solution of the differential equation $\mathtt{F}(\mathtt{x}, \mathtt{y}(\mathtt{x}), \mathtt{y}'(\mathtt{x})) = 0$, or “No strong rational general solution exists” if no such exists, or “No strong rational general solution found” if we cannot say for sure.

Description:

View `F` as curve over $\mathbb{K}(\mathtt{x})$, i.e. $\mathtt{F} \in \mathbb{K}(\mathtt{x})[\mathtt{y}, \mathtt{y}']$, compute rational parametrisation of `F`. Compute the associated equation to `F`. If it is a Riccati equation and has a rational solution `T`, return `P[1](T(x, c))`.

Source code:

```
StrongRational := proc(F, y::name, x::name, c::name := ':-c')
  local F_, z, t, P, f, r, T, y_;
  F_ := Algebraic:-ConvertRootOf(F);
  F_ := convert(F_, ':-‘diff‘');
  if not member(diff(y(x), x), indets(F_)) then
    error "input is no differential equation";
  end if;
  if not type(F_, 'polynom'('radalgnum', [x, y(x), diff(y(x), x)])) then
    error "input must be a polynomial";
  end if;
  if not evala(AIrreduc(primpart(F_, {diff(y(x), x), y(x)}))) then
    error "input is reducible";
  end if;
  if numelems({y,x,c}) <> 3 then
    error "input variables must be distinct";
  end if;
  try
    P := ParametrizeKx(subs({diff(y(x), x) = z, y(x) = y}, F_), x, y, z, t);
    catch "genus": error "No strong rational general solution exists: genus not 0";
    catch "non-ordinary singularity": error "Could not parametrize";
  end try;
  f := evala(Simplify((P[2] - diff(P[1], x))/diff(P[1], t)));
  r := rem(numer(f), denom(f), t);
  f := quo(numer(f), denom(f), t);
  if r <> 0 or degree(f, t) > 2 then
    return "No strong rational gerenal solution exists";
  end if;
  T := rationalSol(diff(t(x), x) = subs(t = t(x), f), x); # t' = a0+a1*t+a2*t^2
  if T = NULL then
    return "No strong rational gerenal solution found";
  end if;
  y_ := simplify(eval(P[1], t = T));
  if simplify(eval(F_, y(x) = y_)) = 0 then # check if solution satisfies DE
    return subs(_C1 = c, y_);
  end if;
  error "incorrect solution";
end proc;
```

```
rationalSol := proc(DE, x)
  local strategy, sol, T;
  for strategy in ['linear', 'Riccati', 'separable', 'homogeneous'] do
    sol := {dsolve(DE, [strategy])}; # solutions of DE
    for T in sol do
      T := rhs(T);
      if type(T, 'ratpoly'('radalgnum', [x, _C1])) and member(_C1, indets(T)) then
        return T; # T is rational general solution
      end if;
    end do;
  end do;
end proc:
```

Example:

```
> StrongRational(diff(y(x), x)^4 - 4*y(x)*(x*diff(y(x), x) - 2*y(x))^2, y, x)
>     4*c^2*(2*c + x)^2
```

The function `dsolve` provides among others the methods `linear`, `Riccati`, `separable` and `homogeneous` which deliver rational solutions. All four are necessary, as can be seen in the following equations.

```
> dsolve(diff(t(x), x) = t(x)/(x + 1) + (x^2 + 2*x)/(x + 1), ['linear'])
>     t(x) = (x + 1)*_C1 + x^2 + x + 1
> dsolve(diff(t(x), x) = t(x)^2/x - 1/x, ['Riccati'])
>     t(x) = 1 - 2*x^2/(x^2 + _C1)
> dsolve(diff(t(x), x) = t(x)^2 + 2*t(x) + 1, ['separable'])
>     t(x) = -(_C1 + x + 1)/(_C1 + x)
> dsolve(diff(t(x), x) = -t(x)^2 + 2/x^2, ['homogeneous']);
>        t(x) = -(2*x^3 + _C1)/((-x^3 + _C1)*x)
```

The following function is not necessary for the computation, but it is useful to generate examples for testing.

FUNCTION constructDE

Input:

- srgs $\in \mathbb{K}(\mathtt{x}, \mathtt{c})$ strong rational general solution
- x,c: variables

Output:

An AODE having srgs as solution.

Description:

Let $\mathtt{y} = \frac{A}{B}$, $\mathtt{y}' = \frac{C}{D}$. Then eliminate from $B\mathtt{y} - A$, $D\mathtt{z} - B$ the c.

Source code:

```
constructDE := proc(srgs, x, c)
  local der, GB, F;
  der := diff(srgs, x);
  GB := Groebner:-Basis([denom(srgs)*y - numer(srgs), denom(der)*z - numer(der)],
          plex(c, y, z, x));
  F := remove(has, GB, {c})[1];
  return subs({y = y(x), z = diff(y(x), x)}, F);
end proc;
```

Example:

```
> constructDE(x*c, x, c)
>       y(x) - x*diff(y(x), x)
```

Bibliography

[BC11] D. Behloul and S.S. Cheng. Computation of Rational Solutions for a first-order nonlinear Differential Equation. *Electronic Journal of Differential Equations*, pages 1–16, 2011.

[FG04] R. Feng and X.S. Gao. Rational General Solutions of Algebraic Ordinary Differential Equations. *ISSAC*, pages 155–162, 2004.

[FG06] R. Feng and X.S. Gao. A polynomial time algorithm for finding rational general solutions of first order autonomous ODEs. *Journal Symbolic Computation 41*, pages 739–762, 2006.

[Ful08] W. Fulton. *Algebraic Curves.* 2008.

[HH90] D. Hilbert and A. Hurwitz. Diophantische Gleichungen vom Geschlecht Null. *Acta mathematica 14*, pages 217–224, 1890.

[HW97] E. Hillgarter and F. Winkler. Points on Algebraic Curves and the Parametrization Problem. *Lecture Notes Artificial Intelegence 1360, D. Wang (ed.), Automated Deduction in Geometry, Springer*, pages 189–207, 1997.

[Kam83] E. Kamke. *Differentialgleichungen: Lösungsmethoden und Lösungen.* Springer, 1983.

[Kov86] J.J. Kovacic. An Algorithm for Solving Second Order Linear Homogeneous Differential Equations. *Journal Symbolic Computation 2*, pages 3–43, 1986.

[NW10] C. Ngo and F. Winkler. Rational general solutions of first order non-autonomous parametrizable ODEs. *Journal Symbolic Computation 45*, pages 1426–1441, 2010.

[NW11] C. Ngo and F. Winkler. Rational general solutions of planar rational systems of autonomous ODEs. *Journal Symbolic Computation 46*, pages 1173–1186, 2011.

[Rit50] Ritt. *Differential Algebra.* Colloquium Publication, Volume 33, American Mathematical Society, 1950.

[SW91] R. Sendra and F. Winkler. Symbolic Parametrization of Curves. *Journal Symbolic Computation 12*, pages 607–631, 1991.

[SW97] R. Sendra and F. Winkler. Parametrization of Algebraic Curves over Optimal Field Extensions. *Journal Symbolic Computation 23*, pages 191–207, 1997.

[SWPD08] R. Sendra, F. Winkler, and S. Perez-Diaz. *Rational Algebraic Curves.* Springer, 2008.

[VGW18] T. Vo, G. Grasegger, and F. Winkler. Deciding the existence of rational general solutions for first-order algebraic ODEs. *Journal Symbolic Computation 87*, pages 127–139, 2018.

[Wal78] R.J. Walker. *Algebraic Curves.* Springer, 1978.

[Win96] F. Winkler. *Polynomial Algorithms in Computer Algebra.* Springer, 1996.