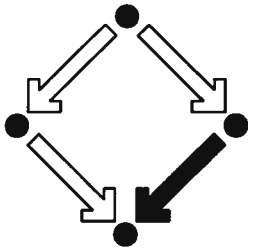
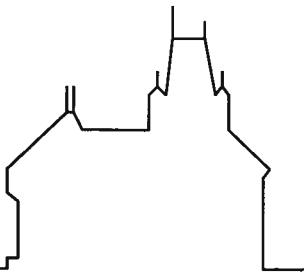


RISC-Linz
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria, Europe



Algebraic and Geometric Approach to Parametrization of Rational Curves

Michal MNUK

(December 1995)

RISC-Linz Report Series No. 95-58

Editors: RISC-Linz Faculty
E.S. Blurock, B. Buchberger, H. Hong, T. Jebelean, F. Lichtenberger, H. Mayr, P. Paule, H. Rolletschek, W. Schreiner, S. Stifter, F. Winkler.

Supported by: Fellowship from BMWF (1990 – 1992), FWF project P8573-PHY (1992 – 1994), ESPRIT III project BRA 6846 (1994 – 1995), also the Institute of Informatics, Slovak Academy of Sciences.

PhD Thesis

Algebraic and Geometric Approach to Parametrization of Rational Curves

Michal Mňuk

Research Institute for Symbolic Computation

Johannes Kepler University, Linz

E-mail: mmnuk@risc.uni-linz.ac.at

PhD thesis

December 1995

Algebraic and Geometric Approach to Parametrization of Rational Curves

Dissertation

zur Erlangung des akademischen Grades
„Doktor der Naturwissenschaften"

Eingereicht von
Michal Mňuk
Dezember 1995

Erster Begutachter : Univ.-Doz. Dr. Franz Winkler
Zweiter Begutachter : Univ.-Doz. Dr. Peter Fuchs

Angefertigt am: Forschungsinstitut für symbolisches Rechnen
Technisch-Naturwissenschaftliche Fakultät
Johannes Kepler Universität Linz

To my wife Eva

Summary

This thesis is devoted to the problem of parametrization of curves. It provides a good reference of known geometric methods. Some subproblems, e.g. constructing neighborhood graphs, are studied closely and several improvements are suggested. A complete binary complexity analysis of parametrization is included.

This work is partially aimed at the study of the parametrization problem from the algebraic point of view replacing classical algorithms by new sophisticated methods. Some subproblems are reconsidered as problems in commutative algebra opening new horizons. A new algorithm for computing adjoint curves based on integrally closed rings is presented. It plays a central role in many other applications.

Zusammenfassung

Diese Dissertation widmet sich dem Problem der Parametrisierung von Kurven. Sie dient als gutes Referenzwerk für bekannte geometrische Methoden. Einige Teilprobleme, wie z.B. Konstruktion benachbarter Graphen, werden näher betrachtet und mehrere Verbesserungen ausgearbeitet. Die Komplexität der Parametrisierung wird eingehend analysiert.

Diese Arbeit ist zum Teil auf das Studium des Parametrisierungsproblems vom algebraischen Standpunkt ausgerichtet. Klassische Algorithmen werden durch effizientere ersetzt. Einige Teilprobleme werden als Probleme in Algebra betrachtet, was zu völlig neuen Gesichtspunkten führt. Ein neuer Algorithmus zur Berechnung adjungierter Kurven, der auf ganzzahlig abgeschlossenen Ringen basiert, wird präsentiert. Dieser Algorithmus spielt eine zentrale Rolle in vielen anderen Applikationen.

Ich versichere, daß ich die Dissertation selbständig verfaßt, andere als angegebene Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

Hagenberg, den 13. Dezember 1995 Michal Mňuk

Acknowledgments

I wish to thank my advisor, Franz Winkler, for his support and encouragement in the course of work on this thesis.

My thanks go also to all members of *Research Institute for Symbolic Computation* who were forming a highly creative, stimulating, and intrinsically human environment.

The support of "Bundesministerium für Wissenschaft und Forschung" in the period 1990–1992, of "Fonds zur Förderung der wissentschaftlichen Forschnung" under project number P8573-PHY in the period 1992–1994, and the "EC Project PoSSo" (Esprit III Basic Research Action No. 6846) in the period 1994–1995, as well as of Institute of Informatics, Slovak Academy of Sciences, is greatfully acknowledged.

Vita

Aug 25, 1965	Born, Opočno, Czech Republic.
Jun 1988	Graduation in mathematics, Humboldt-University at Berlin, Germany.
Aug 1988 – Dec 1989	Research assistant, Institute for Technical Cybernetics, Slovak Academy of Sciences, Bratislava, Slovak Republic.
Jan 1990 – Sep 1990	Research assistant, Institute for Informatics,Slovak Academy of Sciences, Bratislava, Slovak Republic.
Oct 1990 – Dec 1995	PhD study, Research Institute for Symbolic Computation, Linz, Austria.
Apr 1992 – Nov 1994	Assistant professor, Johannes Kepler University, Linz, Austria.
Sep 1993 –	Lecturer, Technical college, Hagenberg, Austria.

Publications and Presentations

[1] M. Mňuk, Rafael Sendra, Franz Winkler. On the complexity of parametrizing curves. Technical report RISC-94-45, Research Institute for Symbolic Computation, Linz, Austria, 1994.

[2] M. Mňuk. Computing adjoint curves (An algebraic approach). Technical report RISC-95-43, Research Institute for Symbolic Computation, Linz, Austria, 1995.

[3] M. Mňuk. Computing Adjoint Curves (Geometric and Algebraic Approach). Talk at CoCoA workshop, May 29 – June 2, 1995, Genova. Italy.

[4] M. Mňuk, Bernhard Wall, Franz Winkler. CASA Reference Manual (Version 2.1). Technical report, Research Institute for Symbolic Computation, Linz, Austria, 1993.

[5] M. Mňuk, Bernhard Wall, Franz Winkler. CASA Reference Manual (Version 2.2). Technical report RISC-95-05, Research Institute for Symbolic Computation, Linz, Austria, 1995.

Preface

The modern algebraic geometry developed to an interdisciplinary mathematical subject studying manifold faces of geometric objects. The 20-th century brought up many excellent results clarifying basic principles of mathematics. These days, in the period of evolution of symbolic algebra systems, old constructive results are revived to be implemented in computers, and classical achievements are reconsidered to prove them suitable for computer aided research. Even simplest objects – the curves – despite of having been extensively studied for a long time, are still bearing many opened questions.

This work concentrates on the problem of parametrization of rational curves. Proceeding use of computers is posing new problems asking for feasible solutions. In this frame, a solution of the parametrization problem requires going new ways. One of main aims of this work is to study and utilize modern algebraic methods to parametrize curves instead of easy, constructive, but in many cases inefficient methods developed by founders of this subject. All concepts which appear in parametrization are considered from both geometric and algebraic point of view. It is shown that even rather abstract methods of commutative algebra may be successfully used in computing. In many cases, they open new views and reveal properties hidden when using geometric methods.

In the first chapter a brief overview over some elementary concepts of algebraic geometry is given. The second chapter deals with basic ingredients

of parametrization – singular points. Basic properties are described in both geometric and algebraic language. An analysis of the impact of the quadratic transformation from new points of view is provided. In Appendix A, a new algorithm for computing adjoint curves is studied. It provides natural algebraic means to study the structure of singular points. The third chapter offers a complete treatment of the parametrization problem. In the fourth chapter some complexity questions regarding the parametrization are considered. Appendix B yields a detailed complexity analysis of a parametrization algorithm.

Contents

Chapter 1

Algebraic Geometry of Varieties

This chapter serves as an introduction into basic principles of algebraic geometry of varieties. It describes in moderate detail all notions used throughout this work. It is not meant to duplicate introductory sections of any textbook on algebraic geometry. It merely introduces concise notation and most of basic theorems used later. For a detailed introduction to algebraic geometry and proofs of most of theorems mentioned in this chapter we refer to [Sha94]. A part of the theory developed here pertaining to commutative algebra may be found in [ZS75].

1.1 Closed Subsets in Affine Space

Let k be a fixed field called *ground field*. It is assumed to be algebraically closed unless stated otherwise. We consider the n-dimensional affine space over this field $\mathbb{A}^n(k)$ which is often referred to as just $\mathbb{A}^n$ if no confusion may arise.

1.1.1 Closed Sets

The basic notion of elementary algebraic geometry is that of a closed set.

Definition 1.1.1. A *closed subset* (algebraic set) of $\mathbb{A}^n$ is a subset $X \subset \mathbb{A}^n$ [1] consisting of all common zeros of a finite number of polynomials with coefficients in k.

Proposition 1.1.2.

(i) The intersection of any number of closed sets is a closed set.

(ii) The union of finitely many closed sets is a closed set.

Analogously to the topology we may introduce the notion of a closure of an arbitrary set.

Definition 1.1.3. The intersection of all closed subsets of X containing a given set $M \subset X$ is a closed set called the *closure* of M denoted by $\bar{M}$. A subset $M \subset X$ is dense in X if $\bar{M} = X$.

Now we are able to define a topology of the affine space using complements of closed sets.

Definition 1.1.4. Let $X \subset \mathbb{A}^n$ be a closed set. A set $U \subset X$ is said to be *open* if its complement $X \setminus U$ is closed. Any open subset $U \ni x$ is called a *neighborhood* of x.

From Proposition 1.1.2 we immediately see that the system of open sets provides a topology of $\mathbb{A}^n$.

The smallest elements among closed sets are irreducible ones, i.e., closed sets which may not be split further.

Definition 1.1.5. A closed algebraic set X is *reducible* if there exist proper closed subsets $X_1, X_2 \subsetneq X$ such that $X = X_1 \cup X_2$. Otherwise X is *irreducible*.

[1] We use the symbol $\subset$ to denote an inclusion or equality. If the possibility of an equality of two sets has to be emphasized, the symbol $\subseteq$ is used instead.

The following proposition yields a description of the structure of closed sets.

Proposition 1.1.6. *Any closed set is a finite union of irreducible closed sets which may be chosen in a way that there is no closed set contained in another one.*

1.1.2 Regular Functions and Maps

We consider now functions mapping points of a closed set $X \subset \mathbb{A}^n$ to the ground field which have the same behaviour as polynomials (viewed as functions on X). The set of all these functions yield the first fundamental invariant of a closed set – the coordinate ring.

Let X be a closed set in the affine space $\mathbb{A}^n$.

Definition 1.1.7. A function f defined on X with values in k is called *regular* (on X) if there exists a polynomial $F(T)$ with coefficients in k such that $f(x) = F(x)$ for all $x \in X$. The set of all functions which are regular on X is a ring called the *coordinate ring* of X denoted by $k[X]$.

Remark 1.1.8. If a closed set X is irreducible, the coordinate ring $k[X]$ is an integral domain, i.e., without zero divisors.

Lemma 1.1.9. *Let $\mathfrak{A}_X \subset \mathbb{A}^n$ be the* ideal of the closed set X, *i.e., a set of polynomials $F(T) = F(T_1, \ldots, T_n)$ which vanish on all points of X. Then*

$$k[X] = k[T_1, \ldots, T_n]/\mathfrak{A}_X$$

Definition 1.1.10. Let $X \subset \mathbb{A}^n$ and $Y \subset \mathbb{A}^m$. A map $f : X \to Y$ is *regular* if there exist m regular functions $f_1, \ldots, f_m$ on X such that $f(x) = (f_1(x), \ldots, f_m(x))$ for all $x \in X$

Remark 1.1.11. Let $f : X \to Y$ be a regular map. Then f induces a ring homomorphism

$$f^* : k[Y] \longrightarrow k[X]$$
$$g \longmapsto g \circ f$$

Definition 1.1.12. A regular map $f : X \to Y$ of closed sets is an *isomorphism* if there exists a regular map $g : Y \to X$ such that $f \circ g = 1$ and $g \circ f = 1$

Proposition 1.1.13. *Isomorphic maps induce isomorphisms between coordinate rings.*

1.1.3 Rational Functions and Maps

Similarly as in the previous section for an irreducible closed set we may consider fractions of regular functions (see the remark after Definition 1.1.7). This lead us to the notion of a function field.

Definition 1.1.14. For an irreducible closed set X the quotient field of $k[X]$, denoted by $k(X)$, is called the *function field* or the *field of rational functions on* X.

Definition 1.1.15. A rational function $\varphi \in k(X)$ is *regular at* $x \in X$ if it can be written in the form $\varphi = \frac{f}{g}$ with $f, g \in k[X]$ and $g(x) \neq 0$.

The following theorem reveals a connection between regular and rational functions.

Theorem 1.1.16. *A rational function φ that is regular at all points of a closed set X is a regular function on X.*

A tuple of rational functions on a closed set may be regarded as a map to $\mathbb{A}^1$.

Definition 1.1.17. A *rational map* $\varphi : X \to Y \subset \mathbb{A}^m$ is an m-tuple of rational functions $\varphi_1, \ldots, \varphi_m \in k(X)$ such that for all points $x \in X$ at which all the φ_i are regular, $\varphi(x) = (\varphi_1(x), \ldots, \varphi_m(x)) \in Y$. We say φ is regular at such point x and $\varphi(x) \in Y$ is the *image* of x. The *image of* X under a rational map φ is the set of points

$$\varphi(X) = \{\varphi(x) \mid x \in X \text{ and } \varphi \text{ regular at } x\}.$$

Proposition 1.1.18. *Similarly to regular maps a rational map $\varphi : X \to Y$ between two closed irreducible sets induces a field homomorphism $\varphi^* : k(Y) \to k(Y)$.*

The counterpart of an isomorphism in the context of rational functions is a birational equivalence.

Definition 1.1.19. A rational map $\varphi : X \to Y$ is called *birational* or a *birational equivalence* if φ has an inverse rational map $\psi : Y \to X$ such that $\varphi(X)$ is dense in Y, $\psi(Y)$ is dense in X, and $\psi \circ \varphi = 1$, $\varphi \circ \psi = 1$ whenever both are defined. In this case, X and Y are said to be *birationally equivalent*.

Proposition 1.1.20. *Birational maps induce isomorphisms between function fields.*

1.2 Quasiprojective Varieties

Closed sets introduced in the previous section may be viewed as local snapshots of object we are interested in. In making the view more complete we pass to *projective* and *quasiprojective varieties*.

Let $\mathbb{P}^n$ be the n-dimensional projective space. A point $P \in \mathbb{P}^n$ is represented by a $n+1$ tuple $(x_0 : \cdots : x_n)$, $x_i \in k$. Two such representations $(x_0 : \cdots : x_n)$ and $(y_0 : \cdots : y_n)$ describe the same point P if there is a non-zero constant $c \in k$ such that $(x_0 : \cdots : x_n) = (c \cdot y_0 : \cdots : c \cdot y_n)$. If $x_0 \neq 0$, we may identify $(x_0 : \cdots : x_n)$ with the point $(\alpha_1, \ldots, \alpha_n)$ by setting $\alpha_i = x_i/x_0$. This yields a 1-1 correspondence between points of the open set $x_0 \neq 0$, denoted as an *affine piece* $\mathbb{A}^n_i$ of $\mathbb{P}^n$, and we have $\mathbb{P}^n = \bigcup_i \mathbb{A}^n_i$.

A polynomial $f \in k[S_1, \ldots, S_n]$ vanishes at a point $P = (x_0, \ldots, x_n) \in \mathbb{P}^n$ if $f(x_0, \ldots, x_n) = 0$ for all representations of P. In this case, if $f = f_r + f_{r+1} + \cdots + f_k$, $0 \leq r \leq k$, where f_i is a homogeneous polynomial of degree i, then $f_i(x_0, \ldots, x_n) = 0$ for $r \leq i \leq k$.

The notion of a closed set is defined in analogy to the affine case.

Definition 1.2.1. A subset $X \subset \mathbb{P}^n$ is a *closed set* if it consists of all common zeros of a finite number of polynomials in $k[x_0, \ldots, x_n]$.

Remark 1.2.2. The notion of an *open projective set* and a *projective closure* of a subset of $\mathbb{P}^n$ is introduced in the same way as in the case of the affine space.

So far, open and closed subsets of affine and projective spaces have been introduced. The notion of a quasiprojective variety includes all of them.

Definition 1.2.3. A *quasiprojective variety* is an open subset of a closed projective set.

1.2.1 Regular Functions

Functions on projective sets require more care to reflect the ambiguous nature of a representation of a point.

Definition 1.2.4. Let $X \subset \mathbb{P}^n$ be a quasiprojective variety, $x \in X$, and $f = P/Q$ where P and Q are homogeneous polynomials of the same degree. Then f is said to be *regular* at x if $Q(x) \neq 0$. If f is regular at all points $x \in X$, it is said to be a *regular function* on X. All regular functions on X form a ring denoted by $k[X]$.

Remark 1.2.5. The representation of f as the quotient of two forms of same degree allows to regard f as a function of a projective point. Note that the representation is not unique.

We use regular functions to construct maps between quasiprojective varieties. A map of a quasiprojective variety $X \subset \mathbb{P}^m$ into an affine space $\mathbb{A}^n$ is given by n functions on X with values in k. If these functions are regular on X, then the map is called *regular*.

Definition 1.2.6. Let $f : X \to Y$ be a map between quasiprojective varieties, $Y \subset \mathbb{P}^m$. This map is *regular* if for every point $x \in X$ and for some affine piece $\mathbb{A}_i^m$ containing $f(x)$ there exists a neighborhood $U \ni x$ such that $f(U) \subset \mathbb{A}_i^m$ and the map $f : U \to \mathbb{A}_i^m$ is regular.

Remark 1.2.7. A regular map to $Y \subset \mathbb{P}^m$ may be given by a m-tuple of forms $(F_0 : \cdots : F_m)$. Two tuples $(F_0 : \cdots : F_n)$ and $(G_0 : \cdots : G_m)$ define the same map if and only if

$$F_i G_j = F_j G_i \quad \text{for } 0 \leq i, j \leq m.$$

A reformulation of the previous definition according to this remark yields an alternative description of regular maps.

Definition 1.2.8. A *regular map* $f : X \to \mathbb{P}^m$ of an irreducible quasiprojective variety X to projective space $\mathbb{P}^m$ is given by a $(m+1)$-tuple of forms $(F_0 : \cdots : F_m)$ of the same degree such that for every point $x \in X$ at least one F_i does not vanish at x.

Remark 1.2.9. The notion of an isomorphism is defined in the same way as for affine closed sets.

We will often reduce investigations of projective sets to investigations of varieties contained in the affine space which allow more concise and clear description. Hence, if a quasiprojective variety is isomorphic to a closed subset of an affine space, we will call it *affine variety*. In the same way, if a quasiprojective variety is isomorphic to a closed subset of an projective space, it will be called *projective variety*.

In many cases, properties of varieties do not change when only open subsets are considered. We say, a property of X is *local* if it suffices to check it only for a certain neighborhood U_x of any point $x \in X$. When studying local properties of quasiprojective varieties, it is sufficient to restrict our consideration to affine varieties, i.e., to those embedded in an affine space.

Lemma 1.2.10. *Every point x of a quasiprojective variety X has a neighborhood isomorphic to an affine variety.*

Remark 1.2.11. The neighborhood described in the preceeding lemma is called an *affine neighborhood*.

1.2.2 Rational Functions

Consider an irreducible quasiprojective variety $X \subset \mathbb{P}^n$. Write O_X for the set of rational functions $f = P/Q$ where P, Q are forms of the same degree in the homogeneous variables $S_0, \ldots, S_n$ such that $Q \notin \mathfrak{A}_X$. If X is irreducible, O_X is a ring.

Definition 1.2.12. Let M_X denote the set of all functions $f = P/Q \in O_X$ with $P \in \mathfrak{A}_X$. The quotient ring $O(X) = M_X/O_X$ of is a field, called *function field* of X. It is denoted by $k(X)$.

Remark 1.2.13. It may be easily seen that rational functions are defined only on certain open subsets of X (where the denominator does not vanish). Since for an open subset $U \subset X$ there is $\mathfrak{A}_U = \mathfrak{A}_X$, we conclude $k(U) = k(X)$.

Similarly to the case of affine varieties we introduce rational maps.

Definition 1.2.14. A rational map $f : X \to \mathbb{P}^m$ is given by $m+1$ forms

$$(F_0 : \cdots : F_m)$$

of the same degree in the $n+1$ homogeneous coordinates of $\mathbb{P}^n$, and at least one F_i is not contained in $\mathfrak{A}_X$. Rational maps of projective varieties are subject to a similar equvalence relation as introduced for rational maps of affine varieties.

Remark 1.2.15. Let $F_i(x) \neq 0$. Then in a certain neighborhood of x the map $(F_0 : \cdots : F_m)$ is given by m rational functions $f_j = F_j/F_i$. Each f_j is regular at x.

Definition 1.2.16. Let $f : X \to \mathbb{P}^m$ be a rational map, and $Y \subset \mathbb{P}^m$ a quasiprojective variety. We say that f maps X to Y if there is a open subset $U \subset X$ where f is regular and $f(U) \subset Y$. The union $\widetilde{U}$ of all such sets is called the *domain of definition* of f, and $f(\widetilde{U}) \subset Y$ the *image* of X in Y.

Remark 1.2.17. As in the case of affine sets, we may define birational equivalence which induces an isomorphism of function fields.

Proposition 1.2.18. *Two irreducible varieties X and Y are birationally equivalent if and only if there are open subsets $U \subset X$ and $V \subset Y$ such that f induces an isomorphism of U onto V.*

1.3 Local Properties

In this section we proceed to define those properties of varieties which remain invariant when the variety is replaced by some neighborhood of a point on it. Such properties are called *local*.

1.3.1 The Local Ring of a Point

One of most important invariants of a point is the *local ring*.

Definition 1.3.1. Let X be a variety and $x \in X$. The local ring $O_x(X)$ is a subring of $k(X)$ consisting of all equivalence classes of functions which are regular on some neighborhood of x. Two functions are said to be equivalent if they agree on some neighborhood of x. In other words,

$$O_x(X) = \{\frac{f}{g} | f, g \in k[X] \wedge g(x) \neq 0\}.$$

Two functions f/g and f'/g' in $O_x(X)$ are equivalent if there is a h with $h(x) \neq 0$ and $h(fg' - f'g) = 0$.

The following theorem relates the local ring to the coordinate ring.

Theorem 1.3.2. *Let X be a variety. Then*

$$k[X] = \bigcap_{x \in X} O_x(X)$$

1.3.2 The Tangent Space

Another important invariant is the tangent space. Let $X = V(f_1, \ldots, f_m) \subset \mathbb{A}^n$ be an affine variety and $x \in X$. We may assume $x = (0, \ldots, 0)$. Let $L_a = \{ta \mid t \in k\}$ be a line through x.

Definition 1.3.3. The *intersection multiplicity* of L and X at x is the multiplicity of the root $t = 0$ of $\gcd(f_1(at), \ldots, f_m(at))$.

Definition 1.3.4. A line L is *tangent* to X at x if its intersection multiplicity with X at x is bigger or equal 2.

Definition 1.3.5. The locus of points on lines tangent to X at x is called the *tangent space* to X at x, denoted by $\Theta_x(X)$ or by Θ_x if the variety is fixed.

Proposition 1.3.6. *Let $x = (0, \ldots, 0)$ and $L_a := \{at \mid t \in k\}$ be a line given by an element $a \in \mathbb{A}^n$. The tangent space $\Theta_x(X)$ of a variety $X \subset \mathbb{A}^n$ is the set*

$$\Theta_x(X) = \{y \in L_a \mid \partial F/\partial T_i(a) = 0 \quad \text{for all } i \text{ and for all } F \in \mathfrak{A}_X\}.$$

Let now X be a hypersurface in $\mathbb{A}^n$ given by a polynomial $F(T_1, \ldots, T_n)$. From the preceeding proposition we see that the equation of the tangent space of X at $x = (x_1, \ldots, x_n)$ is

$$\sum_{i=1}^{n} \frac{\partial F}{\partial T_i}(x)(T_i - x_i) = 0. \tag{1.1}$$

A special case occurs if the left hand side of the equation (1.1) vanishes identically, i.e., if $\partial F/\partial T_i(x) = 0$ for all i. Points x satisfying this condition are called *singular*.

Definition 1.3.7. We say, a point x on a hypersurface $X \subset \mathbb{A}^n$ given by a polynomial F is *singular* or *multiple* if $\partial F/\partial T_i(x) = 0$ for all i. A point x is called *simple* if it is not singular.

The most interesting features are observed at singular points. However, simple points bear many remarkable properties too.

Theorem 1.3.8. *The local ring $O_x(X)$ of a non-singular point $x \in X$ is a unique factorization domain.*

1.3.3 The Tangent Cone

As we saw in the previous section, the tangent space of a hypersurface at a simple point is a uniquely defined hyperplane given by the equation (1.1). However, the tangent space of a hypersurface at a singular point is the whole space itself. In order to obtain more information about the structure at a singular point $x = (0, \ldots, 0) \in X$, we will consider a distinguished system of hyperplanes which span the tangent space at x.

Let $X \subset \mathbb{A}^n$ be a hypersurface given by a polynomial $F = F_k + F_{k+1} + \cdots + F_l$, where F_i are forms of degree i, $F_k \neq 0$.

Definition 1.3.9. The *tangent cone* of a hypersurface $X \subset \mathbb{A}^n$ at x is the set $\{y \in L_a \mid F_k(a) = 0\} \subseteq \Theta_x$.

Consider an example of an algebraic, not necessarily irreducible, plane curve $C \subset \mathbb{A}^2$ given by a bivariate polynomial $F(X, Y)$. The form of lowest degree F_k factors in a product of lines $F_k(X, Y) = \prod(\alpha_i X + \beta_i Y)^{e_i}$. The tangent cone consists in this case of a number of lines $(\alpha_i X + \beta_i Y) = 0$ called *tangent lines*. Each tangent line $l_i : (\alpha_i X + \beta_i Y) = 0$ is assigned an integer e_i called the multiplicity of l_i. The number $\sum e_i = k$ is called the *multiplicity* of C at x. Usually, the lines l_i will be referred to as *tangents* if no confusion with the objects introduced in the Definition 1.3.4 may arise.

1.4 Integrally Dependent Rings and Finite Maps

In previous sections we introduced some very basic principles of algebraic geometry. We observed a tight connection between properties of the varieties and of the corresponding algebraic objects – coordinate rings and function fields. This fact enables us to study varieties in two ways – by examin-

ing their points and maps defined on points, or their coordinate rings and function fields and homomorphisms between them.

In this section we will elaborate this correspondence for a special case. We will consider finite maps between varieties, and study the actions they induce on coordinate rings. This theory then ultimately leads to the existence of non-singular models of varieties, i.e., of varieties lacking complicated singular points. In the case of curves we arrive at transformations devoid of all singularities.

1.4.1 Integrally Dependent Rings

In this section we recall some important results from commutative algebra. For detailed treatment or proofs we refer to [ZS75].

Definition 1.4.1. Let A be a ring, B an overring of A, and $x \in B$. The element x is said to be *integral over* A if it satisfies one of the following equivalent conditions:

(i) There exists a finite set $\{a_1, \ldots, a_n\}$ of elements of A such that

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

(ii) The ring $A[x]$ is a finite A-module.

(iii) The ring $A[x]$ is contained in a subring R of B which is a finite A-module.

(iv) There exists a finite A-module $M \subset B$ with:

(a) $xM \subset M$;

(b) zero is the only element y of $A[x]$ such that $yM = 0$.

Lemma 1.4.2. *Let A be a ring and B an overring of A. The set of elements of B which are integral over A form a ring containing A.*

Definition 1.4.3. A ring B is said to be *integral* over A (or integrally dependent on A) if all elements of B are integral over A.

The following proposition shows that integral dependence satisfies the tower theorem.

Proposition 1.4.4. *Let $A \subset B \subset C$ be rings such that B is integral over A and C is integral over B. Then C is integral over A.*

Definition 1.4.5. The set $\overline{A}_B$ of all elements of B which are integral over a subring A is called the *integral closure* of A in B. If $A = \overline{A}_B$, we say that A is *integrally closed* in B.

Remark 1.4.6. Usually, the role of B in the previous definition is played by the total quotient ring. In that case, we say A is integrally closed.

Integrally closed rings are well studied objects. The following theorem gives a sufficient condition for a ring to be integrally closed.

Theorem 1.4.7. *Any unique factorization domain is integrally closed.*

The following corollary is an immediate consequence of the Theorem 1.3.8.

Corollary 1.4.8. *The local ring of a simple point is integrally closed.*

Since local rings are noetherian local domains, we have:

Corollary 1.4.9. *The local ring of a simple point is a discrete valuation ring.*

The integral dependence is retained if we pass to factor rings or to localizations.

Lemma 1.4.10. *Let A be a ring, A' a ring integral over A, and $\mathfrak{I} \subset A'$. Then $A'/\mathfrak{I}'$ in integral over $A/A \cap \mathfrak{I}'$.*

Lemma 1.4.11. *Let A' be integral over A, and let S be a multiplicatively closed set of non-zero elements of A. Then the localization A'_S is integral over A_S.*

1.4.2 Finiteness Theorems

From the computational point of view, finitely generated structures are of high importance. Those objects may be effectively represented in a computer. The following theorems show that under certain conditions the integral closure of a ring is a finite module.

Theorem 1.4.12. *Let A be an integrally closed domain, K its quotient field, F a finite separable algebraic extension of K, and A' the integral closure of A in F. There exists a basis $\{x_1, \ldots, x_n\}$ of $F|K$ such that A' is contained in the A-module $\sum_i Ax_i$.*

Now we show two important special cases where the integral closure is a finite A-module.

Corollary 1.4.13. *Under the assumptions of Theorem 1.4.12, and if A is noetherian, the integral closure A' is a finite A-module.*

Corollary 1.4.14. *Under the assumptions of Theorem 1.4.12, and if A is a principal ideal domain, the integral closure A' is a finite A-module.*

1.4.3 Conductor and Different

Conductor and different are important objects related to integrally dependent rings which may be assigned a clear meaning in algebraic geometry.

Definition 1.4.15. Let A be a domain and A' integral closure of A in its quotient field F. The set of elements

$$\mathfrak{C} := \{x \in A \mid xA' \subset A\}$$

is called the *conductor* of A in A'.

Remark 1.4.16. The conductor is the largest ideal of A which remains an ideal in A'.

Before we proceed to the different, an important class of rings will be introduced – *Dedekind domains*. These arouse in an attempt to retain nice properties of unique factorization domains in ring extensions. We will see, Dedekind domains play an important role in the algebraic geometry of curves.

Definition 1.4.17. An integral domain R is called *Dedekind domain* if every ideal in R is a product of prime ideals.

In this context, a natural extension of the notion of an ideal is discovered – the *fractional ideal*.

Definition 1.4.18.

(i) Let R be a domain and K its quotient field. An R-submodule $\mathfrak{b}$ of K is called *fractional ideal* if there is a non-zero element d in R such that $\mathfrak{b} \subset \frac{1}{d}R$.

(ii) A fractional ideal $\mathfrak{b}$ is called *invertible* if there is a fractional ideal $\mathfrak{b}'$ such that $\mathfrak{b} \cdot \mathfrak{b}' = R$.

Remark 1.4.19. Any fractional ideal $\mathfrak{b}$ may be written as $\mathfrak{b} = \frac{1}{d}\mathfrak{a}$ for some non-zero $d \in R$ and an ordinary ideal $\mathfrak{a} \subset R$.

Using fractional ideals we may derive another characterization of Dedekind domains.

Proposition 1.4.20. *In a Dedekind domain, all fractional ideals are invertible.*

Now we introduce a distinguished fractional ideal – the *different*.

Definition 1.4.21. Let R be an integrally closed ring, K its quotient field, K' a finite separable extension of K, and R' an integral extension of R admitting K' as quotient field. Let $T_{K'|K} : K' \to K$ denote the trace of $K'|K$. The set

$$\mathcal{C}_{R'|R} := \{z \in K' \mid T(zR') \subset R\}$$

is called *complementary module of R' with respect to R*.

Definition 1.4.22. Let $\mathcal{C}_{R'|R}$ be as above. The set

$$\mathfrak{D}_{R'|R} := (R' : \mathcal{C}_{R'|R}) = \{z \in K' \mid z\mathcal{C}_{R'|R} \subset R'\}$$

is called the *different* of R' over R.

The following theorem describes a relation between the conductor and the different.

Theorem 1.4.23. *With the notation as above let α be an element of R' such that $K' = K(\alpha)$ and let $F(S)$ be the minimal polynomial of α over K. Then we have*

$$F'(\alpha)R' = \mathfrak{C}_{R'|R[\alpha]}\mathfrak{D}_{R'|R}.$$

Proof. See [ZS75], Ch. V, §11. □

1.4.4 Finite Maps

Finally we establish a connection between integrally dependent rings and finite maps.

Let X and Y be affine varieties and $f : X \to Y$ a regular map such that $f(X)$ is dense in Y. Then f^* defines an embedding $k[Y] \hookrightarrow k[X]$. By means of f^*, we identify $\sigma \in k[Y]$ and $f^*(\sigma)$. Hence, $k[Y]$ is viewed as a subring of $k[X]$.

Definition 1.4.24. A regular map $f : X \to Y$ of affine varieties is called to be *finite* if $k[X]$ is integral over $k[Y]$.

Finite maps have a number of interesting properties.

Proposition 1.4.25.

(i) Finite maps are surjective.

(ii) Finite maps take closed sets to closed sets.

The following theorem shows that finiteness is a local property. As a consequence, we obtain an extension of this notion to arbitrary varities.

Theorem 1.4.26. *If $f : X \to Y$ is a regular map of affine varieties, and every point $y \in Y$ has an affine neighborhood $V \ni y$ such that $U = f^{-1}(V)$ is affine, and $f : U \to V$ is finite, then f is finite.*

Definition 1.4.27. A regular map $f : X \to Y$ of quasiprojective varieties is *finite* if any point $y \in Y$ has an affine neighborhood V such that $U = f^{-1}(V)$ is affine, and $f : U \to V$ is finite map between affine varieties.

Following theorems show that some fundamental maps are finite maps.

Theorem 1.4.28. *Let $X \subset \mathbb{P}^n$ be a close variety and $F_0, \ldots, F_s$ forms of the same degree having no common solution on X. Then the projection map*

$$\varphi(x) = (F_0(x) : \cdots : F_s(x))$$

is a finite map $\varphi : X \to \varphi(X)$.

As a consequence of the Noether Normalization Lemma we have the following theorems.

Theorem 1.4.29. *For any irreducible projective variery X there exists a finite map*

$$\varphi : X \to \mathbb{P}^m$$

to some projective space $\mathbb{P}^m$.

Theorem 1.4.30. *For any irreducible affine variery X there exists a finite map*

$$\varphi : X \to \mathbb{A}^m$$

to some affine space $\mathbb{A}^m$.

Chapter 2

Singular Points

2.1 Points on Plane Curves

Every curve possesses many different kinds of points. However, we distinguish only two basis classes of them– *singular* and *non-singular*. For an introductory exposition we refer to Section 1.3.2.

2.1.1 Non-singular Points

From the geometric point of view, a point $P = (x, y)$ on a curve C given by a polynomial $F(X, Y) = \sum_{i+j\geq 1} f_{ij}(X - x)^i(Y - y)^j$ is non-singular if either $f_{10} \neq 0$ or $f_{01} \neq 0$. In this case, the line

$$f_{10}(X - x) + f_{01}(Y - y) = 0$$

is called a tangent to C at P. Assuming $P = (0, 0)$ we may rewrite the polynomial $F(X, Y)$ as

$$F(X, Y) = F_1(X, Y) + \ldots + F_n(X, Y)$$

where $F_i(X, Y)$ are homogeneous polynomials of degree i. The form F_1, if $F_1 \neq 0$, defines the (unique) tangent to C at P.

From the algebraic point of view, the local ring $O_P(C)$ of a non-singular point P is a discrete valuation ring (cf. [Ful89]). Let L be a line which is not a tangent to C at P. Its image l in $O_P(C)$ generates the maximal ideal $\mathfrak{m}$ of $O_P(C)$. Then l is called *uniformizing parameter* at P. Thus, any non-singular point P on C defines a valuation of the coordinate ring $k[C]$ which may be canonically extended to a valuation of the function field $k(C)$.

Local rings of non-singular points on C almost exhaust the set of discrete valuation rings of the function field $k(C)$. Later we will see that there is still a finite set of discrete valuation rings of $k(C)$ which do not stem from any non-singular point on C.

2.1.2 Singular Points

The set of non-singular points of a curve C is open in C, i.e. they make up the majority of all points. The residual set consists of singular points which make up a close subset of C. Consequently, its dimension is zero, i.e. there are only finitely many singular points. From many points of view, these are the most interesting points on a curve. For the sake of parameterization, singular points belong to the most essential information needed to accomplish this task.

Even though there are only finitely many singular points it is not always obvious to *find* them. What do we mean by finding singular points? The answer is not easy to give, in general. It substantially depends on what do we intend to do with them. From the theoretical point of view, using the Definition 1.3.7 we immediately obtain that singular points of an irreducible plane curve C described by a polynomial $F(X,Y)$ are given by solutions of the system

$$F(X,Y) = 0 \qquad \frac{\partial F(X,Y)}{\partial X} = 0 \qquad \frac{\partial F(X,Y)}{\partial Y} = 0 \tag{2.1}$$

For some applications, this may be enough to solve the problem in question.

In general, however, it turns out that such description will not suffice to provide a good starting point to attack singular points. Let us try to postulate some conditions on a description of singular points which, in our opinion, are necessary and general enough at the same time to provide sufficient information for subsequent steps of whatever is needed to be done. Such a description of singular points has to satisfy following requirements:

1. It has to retain enough information to recover an exact description of all coordinates of singular points, especially, all algebraic extensions of the ground field.

2. If the subsequent steps do not explicitly require an irreducible representation, it should not require it either (In most cases we may successfully utilize "dynamic evaluation" (see [DD84]), i.e., work with reducible representations as long as possible.

3. The description has to be constructed in at most polynomial timein the size of the defining polynomial F.

In particular, the second point is very important. Theoretically, the complexity of factorization is much bigger than that of gcd computation, in practice, however, it is often easier to factorize a polynomial than to compute one gcd with coefficients having many bits. Nevertheless, we want to avoid redundant factorization whenever possible.

We present an algorithm which provides us with a suitable description of all singular points of a plane curve. Moreover, it satisfies all above requirements from above.

Let C be a plane curve without multiple components defined by a bivariate polynomial $F(X,Y) \in k[X,Y]$. First, we rotate the curve to a position where there are no two singular points having the same x-coordinate. Curves satisfying this property are called to be in a *regular position*. In [SF90] it is shown that this situation may be achieved by a suitable change of co-

ordinates. Now we may split all singularities of C into classes $\{\mathcal{C}_i\}$ where each class contains points of the same multiplicity i. Within $\mathcal{C}_i$, points are grouped into subclasses $\mathcal{D}_i$ represented by tuples of the form

$$(p_i(x), q_i(x,y)),\ p_i \in k[x],\ q_i \in k[x][y] \tag{2.2}$$

where $p_i(x)$ is an reducible polynomial describing the x-coordinates of all points in $\mathcal{D}_i$, and $q_i(x,y)$ is a polynomial linear in y with coefficients over $k[x]$. The linearity of q in y results from the fact that the curve is in regular position.

This kind of representation of singular points was studied in [SW91]. It turns out that the standard decomposition of singularities is a suitable representation with respect to the problem of parameterization. It can be shown that for the purpose of parameterization we may even drop the condition on p_i to be irreducible. The price we pay is that two possibly different (classes of) points $(\beta, q_1(\beta, y))$ and $(\gamma, q_2(\gamma, y))$ may collapse into a single one.

The Algorithm 1 on page 48 yields the standard decomposition of singularities of a plane curve. In [SW91] and [MSW94] some of theoretical and computational aspects were investigated. It was shown that the standard decomposition is a suitable representation for parameterization. In [MSW94], an estimate of the running time of the Algorithm 1 is given.

Theorem 2.1.1. *Let* $L_F := \text{length}(\|F\|_{max})$. *The worst case complexity of the algorithm* SINGULARITY *is* $O(n^{12}(n \log n + L_F)^2)$ *where* $n = \deg F$.

2.2 Structure of Singular points

In the previous section we considered singular points, some of their basic properties and possible representations. Now we want to investigate them in a greater detail.

Consider a plane curve C_a given by

$$x^4 + x^2y^2 - y^2 - 2a^2x^2 + a^4 \tag{2.3}$$

where a is a free parameter. One can immediately see that there are two singular points in the affine plane – $(\pm a, 0)$. The Figure 2.1 shows the curve (2.3) for $a = \frac{1}{2}$. If we let a go to zero, then the two separate singularities ultimately

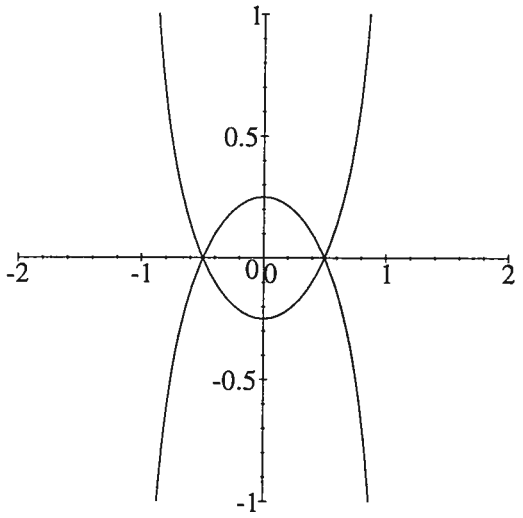


Figure 2.1: Curve $C_{\frac{1}{2}}$

merge into a single one. See Figure 2.2 on the following page. In this case we want to consider the origin as two singular points. The first being a real double point on the curve, the second being another double point associated with it. This leads to deep investigations of properties and structures behind singular points. One of tried methods to approach this goal is the expansion of neighborhood graphs. See e.g. [Wal50]. This method uses a sequence of transformation to extract and collect informations used to completely describe the structure of singular points. In the course of this process the structure of singularities gets simplified. It will be shown later that by this process a (possibly singular) curve C may be transformed into a bira-

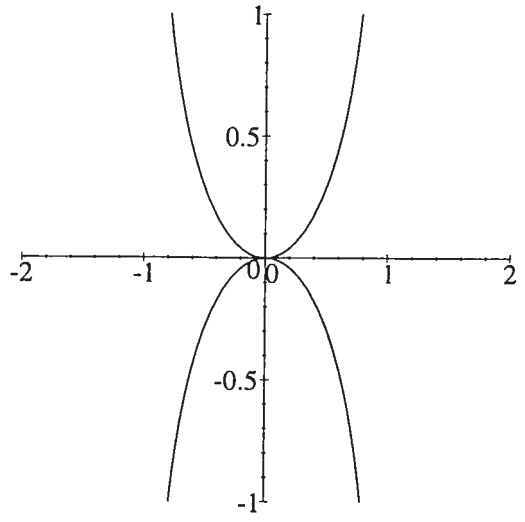


Figure 2.2: Curve C_0

tionally equivalent non-singular curve C' called a non-singular model (see Section 2.3). In the sequel, we give two descriptions of how to obtain the non-singular model. One based on geometric properties of curves utilizing quadratic transformation, and another one using ring theoretic properties of the coordinate ring and its integral closure.

2.2.1 Quadratic Transformation

This section describes a classical method to study the structure of singular points – the quadratic transformation. It enables us to reverse the process sketched in Section 2.2 when two double point on a curve were merged into a (seemingly) single double point. For a detailed treatment and proofs of theorems in this section we refer to [Wal50].

Definition 2.2.1. A regular map $\Psi : \mathbb{P}^{2'} \longmapsto \mathbb{P}^2$ given by

$$\begin{aligned} X &= Y'Z' \\ Y &= X'Z' \\ Z &= X'Y' \end{aligned} \tag{2.4}$$

is called a *quadratic transformation* of $ProjSpace2'$ into $\mathbb{P}^2$.

The following properties of quadratic transformation are easily shown.

Proposition 2.2.2.

(i) Each point of $\mathbb{P}^{2'}$ *except* $(0:0:1)$, $(0:1:0)$ *and* $(1:0:0)$ *is transformed by* (2.4) *into a unique point of* $\mathbb{P}^2$. *The three exceptional points are called* fundamental points.

(ii) Any non-fundamental point on $X = 0$, $Y = 0$, *and* $Z = 0$ *is transformed into* $(1:0:0)$, $(0:1:0)$, *and* $(0:0:1)$, *respectively. The lines* $X = 0$, $Y = 0$ *and* $Z = 0$ *are called* exceptional lines.

The following proposition describes the action of quadratic transformation on non-singular points not lying on exceptional lines.

Proposition 2.2.3. *Let* C *be an irreducible plane curve given by a homogeneous polynomial* $F(X, Y, Z)$, *and let* $C' = \Psi(C)$, C' *given by* $G(X', Y', Z')$. *With a finite number of exceptions the points on* C *and* C' *are in 1–1 correspondence.*

Remark 2.2.4. The curve $C' = \Psi(C)$ is called the *total transform* of C.

Consider the projective closure C_0' of C_0 defined in (2.3). It is given by

$$X^4 + X^2Y^2 - Y^2Z^2 \tag{2.5}$$

There are two double points on $C_0' - (0:0:1)$ and $(0:1:0)$. The total transform of C_0' is given by

$$Y^2Z^2\left(Y^2Z^2 + Z^2X^2 - X^4\right) \tag{2.6}$$

which contains two double lines Y^2 and Z^2. Later we will see that these extraneous factors always emerge originating from singular points. This fact motivates the following definition.

Definition 2.2.5. Let C' be the total transform of a projective curve C defined by a homogeneous polynomial F. Let the defining polynomial of C' be G, and let F' be such that $G = \gamma F'$, F' not divisible by any X, Y, or Z. Then the curve defined by F' is called the *proper transform* of C.

Applying the quadratic transformation to non-singular points yields nothing interesting. Those points are in a 1–1 correspondence, and, as we will see later, their basic invariants stay the same.

The quadratic transformation was designed to simplify the structure of singular points in such a way that preimages of fundamental points under T are in a 1–1 correspondence with intersections of C' with exceptional lines. The following theorem analyzes the action of quadratic transformation on singular points lying on exceptional lines.

Theorem 2.2.6. *Let C, C', F, and F' be as above. Let $n = \deg F$, $X_0 = X$, $X_1 = Y$, $X_2 = Z$, $X_0' = X'$, $X_1' = Y'$, $X_2' = Z'$. Assume that C has an r_i-fold point, $r_i \geq 0$, at the fundamental point $X_j = X_k = 0$ (i, j, k all different), and no tangent at any of these points being exceptional lines. Then the following holds:*

(i) The proper transform C' of C has the line $X_i = 0$ as an r_i-fold component. Hence

$$\deg F' = \deg F - \sum r_i$$

(ii) There is a 1–1 correspondence, preserving multiplicities, between the tangents to F at $X_j = X_k = 0$ and the non-fundamental intersections of C' with $X_i = 0$.

(iii) The total tranform F' has a multiplicity $n - r_j - r_k$ at $X_j' = X_k' = 0$, the tangents being distinct from the exceptional lines and corresponding to the non-fundamental intersections of C with $X_i = 0$.

The theorem shows that the proper transform of a curve possibly acquires some new singular points arising from fundamental points on the original curve. Even though quadratic transformations was meant to simplify the structure of singular points, it actually introduces some new ones. This is the price for staying globally in the projective plane. This means, the proper transform of a curve is still a projective plane curve, and the whole process might be applied again.

Outside of exceptional lines, however, there is no change of multiplicities.

Theorem 2.2.7. *An r-fold point on C not on an exceptional line is transformed into an r-fold point on C', and the tangents at these two points correspond in multiplicities.*

The following important theorem shows that quadratic transformations lead to an extensive simplification of singular points.

Theorem 2.2.8. *By a succession of quadratic transformations any irreducible curve can be transformed into one having only ordinary points.*

The above theorem asserts the existence of a finite sequence of quadratic transformations

$$\mathbb{P}^2 \xrightarrow{\Psi_k} \mathbb{P}^2 \xrightarrow{\Psi_{k-1}} \cdots \xrightarrow{\Psi_1} \mathbb{P}^2 \tag{2.7}$$

such that for a given curve C the transform

$$\Psi_k \circ \Psi_{k-1} \circ \cdots \circ \Psi_1(C) \tag{2.8}$$

has only ordinary points. Having arrived at a curve with only ordinary singularities, subsequent application of quadratic transformations will not change the structure of singular points any more. Later, the concept of quadratic transformation will be reformulated in local terms. It will be shown that a curve with only ordinary multiple points may be transformed

into a curve devoid singularities. The resulting curve will not be a plane curve any more. However, we may fing a certain neighborhood in which it is isomorphic to a plane curve.

The quadratic transformation is a regular map between projective spaces. It is easily seen that the inverse of (2.4) is the mapping $\varphi : \mathbb{P}^2 \to \mathbb{P}^{2'}$

$$\begin{aligned} X' &= YZ \\ Y' &= XZ \\ Z' &= XY \end{aligned} \tag{2.9}$$

It is clear that the quadratic transformation is a rational map between projective spaces having a rational inverse. Hence, a curve C and its proper transform C' are birationally equivalent. This important property will be used later on in parametrization of curves.

2.2.2 Infinitely Near Points

In Section 2.2.1 we described the basic tool to study the structure of singular points – quadratic transformations. Let us consider the action it performs on a curve. For the sake of simplicity in this section we consider only curves in affine space. This does not impose any restriction as all essential information – singular points – may be brought to the affine plane loosing only non-singular points at infinity. Since every curve has only finitely many points at infinity, having the goal of parametrization in mind, we will see that this loss will not affect solutions to this problem.

Let a curve C be given by an irreducible polynomial $F = F_r + F_{r+1} + \cdots + F_n$, F_i a form of degree i, have a singular point at P of multiplicity r. Assume that X is not a tangent to C at P. By a change of coordinates we may move P to the origin. It can be shown that there is an open affine set where the map (2.4)

is given by

$$\begin{aligned} \psi : \mathbb{A}^2 &\longrightarrow \mathbb{A}^2 \\ (X', Y') &\longmapsto (X', X'Z') \end{aligned} \tag{2.10}$$

The curve C in the (X, Y)-plane is transformed by (2.4) to a curve C' such that all points on $C \setminus \{P\}$ are in an 1–1 correspondence with points on C'. The polynomial F' describing the transformed curve C' is

$$F' = F_r(1, Z) + XF_{r+1}(1, Z) + \cdots + X^{n-r}F_n(1, Z). \tag{2.11}$$

Let $F_r(X, Y) = \prod L_i$ be the factorization of $F_r(X, Y)$ where L_i are linear forms describing the tangent lines to C at P. The point P is transformed to a set of points $\{P_1, \ldots, P_r\}$ where $P_i = (0, \alpha_i)$, α_i being a zero of $F_r(1, Z)$. Precisely, if we write $L_i = Y - \alpha_i X$, the Y-coordinates of P_i's correspond to tangents to C at P. The set $\psi^{-1}(P) = \{P_1, \ldots, P_r\}$ is called the *first neighborhood* of P. Points in the first neighborhood of P are called *infinitely near* to P. Points on C are referred to as *distinct*. For a detailed treatment of neighborhood points we refer to [Wal50, Abh90].

Let us look at a curve C_1 given by a polynomial

$$\begin{aligned} xy^4 + xy^5 + x^2y^3 + x^5y^2 - 19x^2y^5 - 53x^3y^4 + x^5y + x^5y^5 + x^5 \\ + 43x^3y^3 + x^4y^3 + 12x^4y^4 + 57x^3y^5 - 19x^5y^3 \\ - 36x^4y^5 + y^5 + 21x^5y^4 - 15x^3y^2 \end{aligned} \tag{2.12}$$

See Figure 2.3 on the next page. The curve C_1 has two singular points in the affine plane. One 4-fold point at $(1, 1)$ and one 5-fold point at $(0, 0)$. Note that there are yet two more singularities at infinity. The tangents to C_1 at $(0, 0)$ are given by linear factors of the form of lowest degree in (2.12)

$$xy^4 + x^2y^3 + x^5 + y^5 - 15x^3y^2$$

Applying ψ to C_1 we obtain a new curve C_1' such that there is a 1–1 correspondence between points of C_1 and C_1' except at P. We see that $P = (0, 0)$

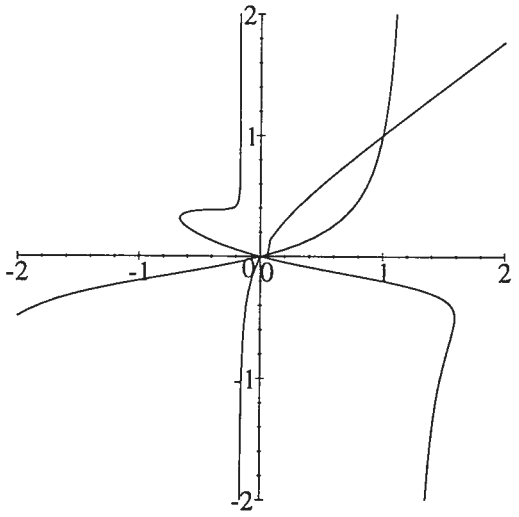


Figure 2.3: Curve C_1

has more preimages under the map ψ. The points P_i have coordinates $(0, \alpha)$ where α is a root of the polynomial

$$y^4 + y^3 + 1 + y^5 - 15y^2$$

The picture of C_1' is at Figure 2.4 on the facing page. The resulting curve C_1' is again a plane curve given by the polynomial

$$y^5x^5 - 36y^5x^4 + 57y^5x^3 + 21y^4x^4 - 19y^5x^2 + 12y^4x^3 + y^5x - 53y^4x^2 \\ - 19y^3x^3 + y^5 + y^3x^2 + y^4 + 43y^3x + y^2x^2 + y^3 - 15y^2 + yx + 1$$

We check that this curve has only one 4-fold point $(1,1)$ which corresponds to the 4-fold point $(1,1)$ on C. Otherwise there are no singularities in the affine plane. After moving the point $(1,1)$ to the origin and applying the quadratic transformation again we obtain a curve C_1'' devoid of multiple points in the affine plane. Note that there are still two singular points at infinity which can be resolved in the same way after moving them to the affine plane by an appropriate change of coordinates. Concentrating only to

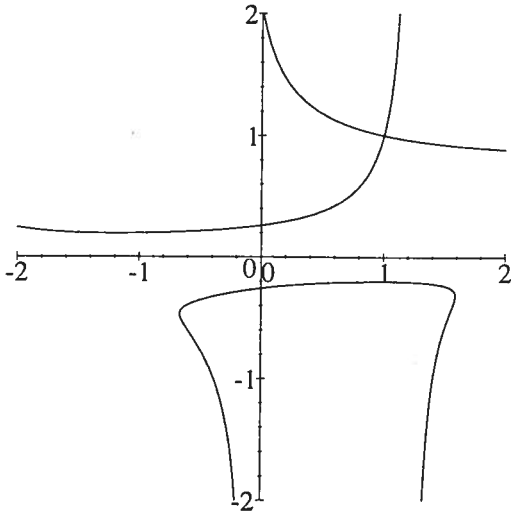


Figure 2.4: Quadratic transform of C_1

affine points we see that there are five non-singular points in the first neighborhood of $(0,0)$ and four non-singular points in the first neighborhood of $(1,1)$. As the quadratic transformation has no effect on non-singular points, nothing essential will change by applying it to C_1'' again. We may depict the structure of affine singular points and their neighborhoods. See Figure 2.5.

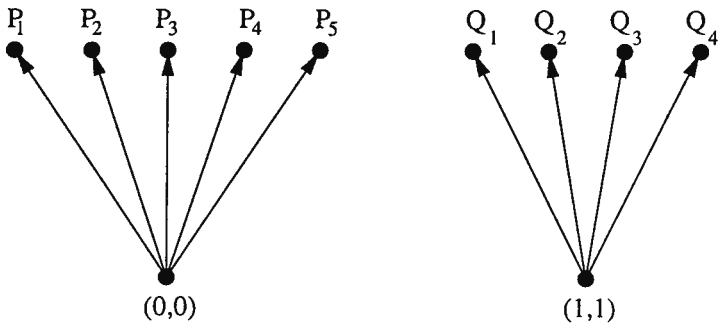


Figure 2.5: Neighborhood graph of C_1

In general, however, we will obtain more complicated pictures. Consider the curve C_2 given by the polynomial $y^2 - x^7 - x^6$. See Figure 2.6. This

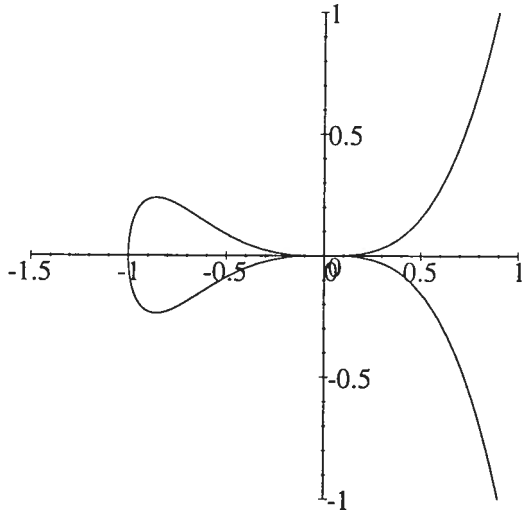


Figure 2.6: Curve C_2

curve has only one affine singular point P at the origin. If we apply the quadratic transformation to C_2, the resulting curve C_2' is given by the polynomial $y^2 - x^5 - x^4$. In this case, the double point at the origin has one double point $(0,0)$ in its first neighborhood, and the quadratic transformation may be applied again yielding the curve C_2'' given by a polynomial $y^2 - x^3 - x^2$. See Figure 2.7 on the facing page. This curve has already two distinct tangents and after next application of quadratic transformation we will obtain two non-singular points in the first neighborhood of $(0,0)$ on the curve C_2''. The first neighborhood of a point Q from the first neighborhood of Q' is called the *second neighborhood* of Q'. By induction we define arbitrary neighborhoods. The neighborhood graph of C_2 is depicted in the Figure 2.8.

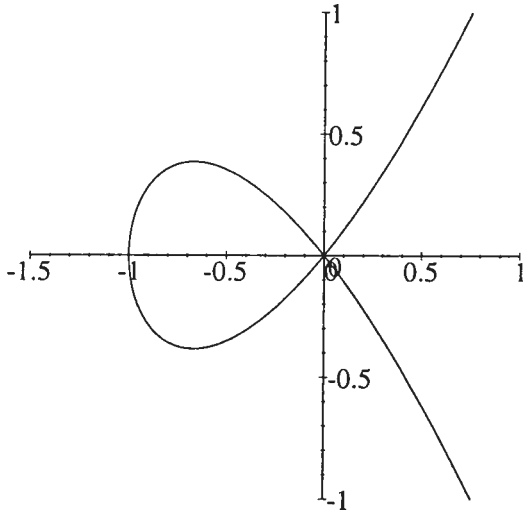


Figure 2.7: Curve C_2''

Neighborhood graphs provide an elementary mean to describe the structure of singular points. First we determine all singular points on a curve. Then we choose one of them, move it to a fundamental point and apply the quadratic transformation. By repeating this process we obtain a sequence of curves arising from the chain (2.7).

In this way, we obtain a sequence of curves

$$C_k \xrightarrow{\psi_k} C_{k-1} \xrightarrow{\psi_{k-1}} \dots \xrightarrow{\psi_1} C_1 \xrightarrow{\psi_0} C_0 = C$$

where at each step we move one singular point to the origin and apply the quadratic transformation. The Theorem 2.2.8 shows that this process terminates, and the curve C_k has only ordinary singular points.

The Algorithm 2 on page 49 (cf. [MSW94]) yields the resolution of a sin-

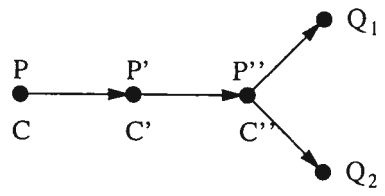


Figure 2.8: Neighborhood graph of C_2

gle distinct singular point.

To obtain a complete description, this algorithm has to be called on all singular points. See Algorithm 3 on page 49.

The above procedure to determine the structure of singular points has been implemented in the Maple package CASA (see [MWW95]).

2.2.3 Chains of Neighboring Points

Neighborhood graphs described in previous sections yield a complete description of the structure of singular points. Sometimes, however, this structure turns out to be particularly simple. In other words, singular points may "resist" quadratic transformation, i.e., it will not get resolved. This section attempts to find some criteria which would give a good procedure to predict whether and how long may a singular point withstand until it gets resolved. Based on such prediction the quadratic transform may be modified in such a way that just one application is necessary to resolve a point.

Singular points on plane curves may have arbitrarily complex structure. Let us consider a curve C of degree n, and let P be a singular point on C of multiplicity r. Then there is a natural restriction on the number and/or multiplicity of neighboring points to P. We have

$$\sum_{Q} \frac{r_Q(r_Q - 1)}{2} \leq \frac{(n-1)(n-2)}{2} \tag{2.13}$$

The sum is taken over all points Q from arbitrary neighborhood of P. This is the only restriction imposed on the structure of a singular point. The equa-

tion 2.13 determines a trade-off between the degree of the neighborhood tree (the maximum number of points in a neighborhood) with root P and its depth. The computational complexity of quadratic transformation heavily depends on both of these parameters (cf. [MSW94]). If the neighborhood tree has a rather high degree, its depth has to be small, and only a few quadratic transforms are needed to resolve all singular points. On the other hand, the opposite case reveals a substantial weakness of the quadratic transform as a method for resolving singularities. An example of a curve which has minimal degree of the neighborhood graph has been given in the Section 2.2.2. We considered a curve of degree 7 given by the polynomial

$$y^2 - x^7 - x^6.$$

The structure of the neighborhood tree is shown in Figure 2.8 on the preceding page. We may consider curves of higher degree with the same arrangement of consecutive neighborhoods. Let for any $k \geq 0$ D_k be a plane curve given by the polynomial

$$y^2 - x^{2k+1} - x^{2k}.$$

In [MSW94] we have proved that D_k has only one affine double point which will not get resolved until the last step. The depth of the tree is then k. The Figure 2.9 shows the neighborhood tree with root at the origin. In order to

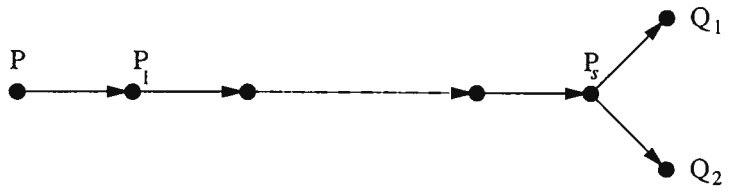


Figure 2.9: Neighborhood tree of D_k

resolve the origin completely, we have to perform k steps each involving

one quadratic transformation. This example shows clearly a deficiency of the quadratic transformation. Although the structure of the neighborhood graph is very easy, it requires a lot of work to arrive at the final resolution where the only double point splits into two non-singular points. This lack of efficiency is magnified by the fact that in each step the degree of the defining polynomial is almost doubled. Fortunately, in some cases we are able to predict this behavior and by a slight change of the classical quadratic transformation we may considerably speed up the resolution process. The important issue will be the prediction of such pathological cases.

Let C be a curve given by a polynomial F. Let us assume that C has a purely non-ordinary r-fold point at the origin.

Definition 2.2.9. Let C and F be as above. Let F have the form $F(X,Y) = F_r(X,Y) + F_{r+1}(X,Y) + \dots$ where F_i is a form of degree i, F_r being non-zero. The origin is called a *purely non-ordinary* r-fold point of C if F_r is a r-th power of some linear polynomial.

Let us consider the quadratic transform F' of F. We want to derive a condition under which the point $(0,0)$ will be again a r-fold point on F', i.e. no splitting in the neighborhood graph occurs.

We have

$$F(X,Y) = \sum_{i+j \geq r} f_{ij} X^i Y^j.$$

By a change of coordinates we can make $f_{0r} \neq 0$. The proper quadratic transform of F is then

$$F'(X',Y') = \sum_{i+j \geq r} f_{ij} X^{i+j-r} Y^j.$$

Assume that the origin is a purely non-ordinary r-fold point on F'. If we

write $F'(X',Y') = F'_r(X',Y') + F'_{r+1}(X',Y') + \dots$ we get

$$F'(X',Y') = \sum_k \sum_{j=0}^{k} f_{k+r-2j,j} X'^{k-j} Y'^{j} \tag{2.14}$$

$$= \sum_{i+j \geq r} f'_{ij} X'^{i} Y'^{j} \tag{2.15}$$

where $f'_{ij} = f_{i-j+r,j}$. Hence $F'_k(X',Y') = \sum_{j=0}^{k} f_{k+r-2j,j} X'^{k-j} Y'^{j}$, and $F'_r(X',Y') = \sum_{j=0}^{r} f_{2r-2j,j} X^{r-j} Y^{j}$. Obviously, F'_r does not vanish identically since $f_{0r} \neq 0$. As the origin is an r-fold point we have that all coefficients $f_{2r-2j,j}$ are zero for $0 \leq j < r$. This situation is depicted in the Figure 2.10. The line l_1 cor-

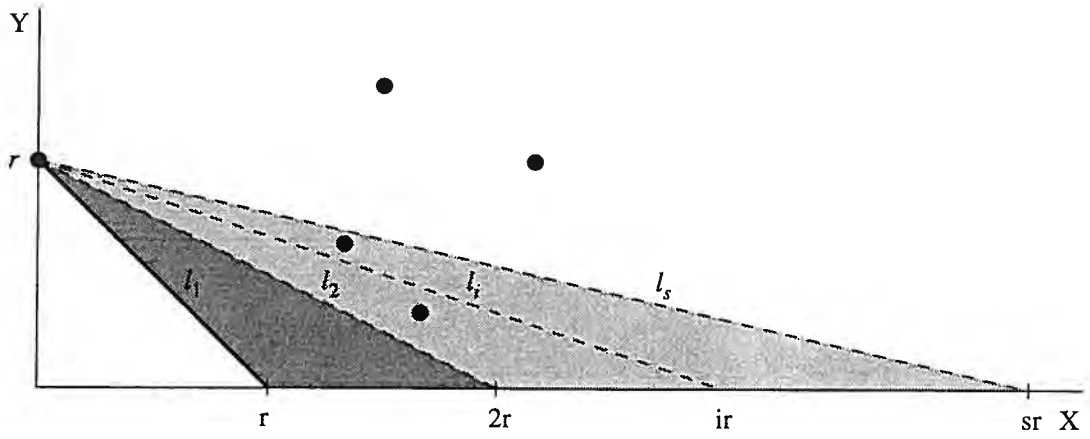


Figure 2.10: Chains of neighborhood points

responds to monomials of degree r in F with non-zero coefficients. If the origin is again a purely non-ordinary r-fold point on F', previous reasoning has shown that all coefficients at monomials under or on the line l_2, on which the coefficients $f_{2r-2j,j}$ are lying, have to vanish except f_{0r}. This observation leads to the following proposition.

Proposition 2.2.10. *Let $s \geq 1$ be an integer such that*

$$f_{ij} = 0 \text{ for } i + sj \leq sr,\ j \neq r. \tag{2.16}$$

Then

(i) $\bar{F}(X_{s-1}, Y_{s-1}) = X_{s-1}^{(s-1)r} F(X_{s-1}, X_{s-1}^{s-1} Y_{s-1})$ *has an r-fold purely non-ordinary singular point at the origin.*

(ii) *The first neighborhood of the origin on* $\bar{F}$ *contains either at least two different points or an r-fold purely non-singular point different from the origin.*

Proof. We have

$$\bar{F}(X_{s-1}, Y_{s-1}) = X_{s-1}^{(s-1)r} F(X_{s-1}, X_{s-1}^{s-1} Y_{s-1}) \tag{2.17}$$

$$= \sum_{i+j \geq r} f_{ij} X_{s-1}^{i+(s-1)j-(s-1)r} Y_{s-1}^{j}. \tag{2.18}$$

Since $i + s(j-r) < i + (s-1)j - (s-1)r = i + (s-1)(j-r) <\leq 0$, the right hand side of 2.17 is a polynomial. Consider the form $\bar{F}_k$ of degree k in $\bar{F}$. We have

$$\bar{F}_k = \sum f_{k+(s-1)r-sj,j} X_{s-1}^{k-j} Y_{s-1}^{j}. \tag{2.19}$$

From (2.19) we have $\bar{F}_r = \sum f_{sr-sj,j} X_{s-1}^{r-j} Y_{s-1}^{j} = f_{0r} T_{s-1}^{r}$.

The proof of the second assertion is trivial. □

The proposition yields a criterion to decide how long an r-fold purely non-ordinary point will not be resolved by quadratic transformation. The importance of the Proposition 2.2.10 lies in the fact that we are able to make an a priori decision on the length of the path in the neighborhood graph along which no splitting occurs. Starting from a given polynomial $F(X, Y) = \Sigma_{i+j \geq r} f_{ij} X^i Y^j$ we find the largest s such that (2.16) is satisfied. Then we may apply the extended quadratic transformation defined by

$$\begin{aligned} X &= X' \\ Y &= Y' X'^{s-1} \end{aligned} \tag{2.20}$$

We obtain a polynomial

$$F'(X', Y') = X'^{(s-1)r} F(X', X'^{(s-1)r} Y') \tag{2.21}$$

called the *(s − 1)-st proper quadratic transform* of F. The Proposition 2.2.10 implies that this transform has an r-fold purely non-ordinary point at the origin. However, the first neighborhood of the origin on F' may already contain more than one point.

Let us assume that a curve C has a chain of r-fold purely non-ordinary points in its neighborhood graph. In the case when these points are located at the origin, the Proposition 2.2.10 yield a condition to recognize at least a part of the chain a priori. Let s be the maximal integer satisfying the condition (2.16), and F' the $s-1$-st quadratic transform of the polynomial F defining C. The first neighborhood of the origin on F' may contain according Proposition 2.2.10 either at least two points, in which case a split occurs, or again an r-fold purely non-ordinary point different from the origin. We will focus on the recognition of the latter case since then the quadratic transformation may be speed up by (2.20). Let

$$F'(X',Y') = \sum_{i+j\geq r} f'_{ij} X'^i Y'^j.$$

Let us find a condition for the first neighborhood of the origin on F' to contain again an r-fold purely non-ordinary point P' different from the origin. Let $P' = (0,a)$, $a \in \mathbb{Q}$. Let the quadratic transform of F' be

$$F''(X'',Y'') = \sum_{i+j\geq 0} f''_{ij} X''^i Y''^j$$

where $f''_{ij} = f'_{i-j+r,j}$. If $F''(X'',Y'')$ has an purely non-ordinary r-fold point at P in the first neighborhood of the origin on F', we may derive necessary conditions on the coefficients f''_{ij}. The form $F''_r(0,Y'')$ is a perfect power, i.e.

$$F''_r(0,Y'') = \sum_j f''_{0j} Y''^j = (Y'' - a)^r.$$

Using the binomial theorem we obtain

$$f''_{0j} = \binom{r}{j} a^{r-j}, \text{ for } 0 \leq j \leq r. \tag{2.22}$$

Especially

$$a = \frac{f''_{0,r-1}}{r}. \tag{2.23}$$

Moreover, the following equation is satisfied

$$\frac{f''_{0j}}{f''_{0,j+1}} = a\frac{j+1}{r-j}. \tag{2.24}$$

In particular, from (2.22) we have that all coefficients

$$f''_{0j} \neq 0,\ 0 \leq j \leq r. \tag{2.25}$$

Since $f''_{ij} = f'_{i-j+r,j}$, from (2.25) we obtain

$$f'_{r-j,j} \neq 0,\ 0 \leq j \leq r. \tag{2.26}$$

The condition 2.19 yields a decision whether the $(s-1)$-st quadratic transform has again an r-fold purely non-ordinary point in the first neighborhood of the origin. Hence, we have proved

Proposition 2.2.11. *Let*

$$F'(X',Y') = \sum_{i+j\geq r} f'_{ij} X'^i Y'^j.$$

Then the first neighborhood of $P = (0,0)$ on F' consists of a single point $Q = (0,a)$, $a \in \mathbb{Q}$, if and only if

$$\frac{f'_{r-j,j}}{f'_{r-j+1,j+1}} = a\frac{j+1}{r-j}$$

If a purely non-ordinary r-fold point on F'' in the first neighborhood of the origin has been detected, using the transformation

$$X = \bar{X} \tag{2.27}$$

$$Y = \bar{Y} + a \tag{2.28}$$

the singularity is moved to the origin and the Proposition 2.2.10 may be used to detect another chain.

To sum up, in this section we derived some criteria to determine long non-branching chains in neighborhood graphs. Points in those chains withstand the quadratic transformation which has to be applied many times to achieve a split. This redundantly explodes the degree of the defining polynomial. Even though some of these pathological cases may be predicted and a modification of the classical quadratic transformation will partially compensate its weakness this section stresses the one of the main problems of the quadratic transformation – its inability to exploit the structures inherent to the problem.

2.3 Desingularization of Curves

The quadratic transformation may be used, starting with an arbitrary plane projective curve without multiple components, to obtain a curve without non-ordinary singular points. The Theorem 2.2.6 shows that each quadratic transformation introduces new singularities arising from fundamental points. The advantage of this approach lies in the fact that the transform stays in the same space as the original curve. If we admit the transformed curve to lie in a different space, is is possible to resolve the singularities completely, i.e. to find a birationally equivalent curve devoid multiple points. The price paid for this extension is that the transformed curve does not stay in the same space. However, focusing only on a certain neigborhood of a curve it will be shown that the transform of a plane curve is again a plane curve.

In the sequel we give a description of blowing up a point in an affine plane which plays a central role in the desingularization of curves. This concept will be expressed in two different languages. The geometric approach uses the restriction of the quadratic transformation to an affine plane. Another approach is based on commutative algebra. The latter belongs to mod-

ern algebraic geometry opening new views to known phenomena providing us with better means to study underlying structures.

2.3.1 Blowing Up a Point – Geometric Description

Since the properties we want to study are all local, we will confine ourselves to points in an affine plane. Let P be a point in $\mathbb{A}^2$. We may assume, by a change of coordinates, $P = (0,0)$. Let $U = \{(x,y) \in \mathbb{A}^2 \mid x \neq 0\}$. Consider the regular map

$$\sigma' : U \longrightarrow U \times \mathbb{A}^1$$
$$(x,y) \longmapsto (x,y,y/x).$$

Let B be the closure of $\sigma'(U)$ in $\mathbb{A}^3$. Then $B = \{(x,y,z) \in \mathbb{A}^3 \mid xz - y = 0\}$. Since $XZ - Y$ is irreducible, B is a variety.

Definition 2.3.1. The map $\sigma : B \to \mathbb{A}^2$ defined by the restriction of the projection $\mathbb{A}^3 \to \mathbb{A}^2$ given by $(x,y,z) \to (x,y)$ to B is called the *blowup of* $\mathbb{A}^2$ *with the center at* P.

The map σ is a most representative example of a *birational equivalence*. The open subset $\sigma^{-1}(U) \subset B$ is isomorphically mapped onto $U \subset \mathbb{A}^2$. The only interesting points of B are preimages of P under σ. The set $E = \sigma^{-1}(P) = \{(0,0,z) | z \in k\}$ is called the *exceptional variety*.

Let $\varphi : \mathbb{A}^2 \to B$ be defined by $\varphi(x,z) = (x,xz,z)$. Then φ is an isomorphism of $\mathbb{A}^2$ onto B. The inverse map is given by the projection $\pi : B \to \mathbb{A}^2$ taking $(x,y,z) \in B$ to $(x,z) \in \mathbb{A}^2$. The composition of φ and σ is a birational equivalence of affine planes

$$\psi = \varphi \circ \pi : \mathbb{A}^2 \longrightarrow \mathbb{A}^2 \tag{2.29}$$
$$(x,z) \longmapsto (x,xz). \tag{2.30}$$

Let us consider an irreducible plane curve $C \subset \mathbb{A}^2$ given by a polynomial $f \in k[X,Y]$, and a point P on C. For the sake of simplicity, assume $P = (0,0)$

and X is not a tangent to C at P. We are going to study the preimage of C in $\mathbb{A}^2$ under the action of the map ψ. For this, let $C_0 = C \cap U$, $C_0' = \psi^{-1}(C_0)$, and C' the closure of C_0' in $\mathbb{A}^2$. Then ψ restricted to C' is a birational map of C' to C. In particular, $\psi(C')$ is dense in C, hence the coordinate ring $k[C]$ can be viewed as a subring of $k[C']$. Let the lower case letters x, y, z denote the images of variables X, Y, Z in the corresponding coordinate rings.

The following theorems describe the most important properties of C'. The proofs are easy, and may be found in [Ful89].

Theorem 2.3.2. *Let C be a plane irreducible curve given by a polynomial $F(X,Y)$, and $P = (0,0)$ a point on C. Let C' be as above, and let the restriction of ψ to C' be denoted by the same symbol. The polynomial f may be written as $F = F_r + F_{r+1} + \cdots + F_n$, $r \geq 0$, F_i a form of degree i (P is a r-fold point on C). Then it holds:*

(i) C' is given by the polynomial $F' = F_r(1,Z) + XF_{r+1}(1,Z) + \cdots + X^{n-r}F_n(1,Z)$.

(ii) $\psi^{-1}(P) = \{P_1, \ldots, P_s\}$, where $P_i = (0, \alpha_i)$, $F_r(1, \alpha_i) = 0$.

2.3.2 Blowing Up a Point – Algebraic Description

In this section we describe the process of blowing up by algebraic means. We merely reformulate the principles of the previous section within commutative algebra. However, we will see that by using an algebraic language more structure of objects is revealed. All principles may be formulated coordinate-free making it easier to concentrate on essential properties.

Instead of polynomials defining curves C and C' we use their coordinate rings $k[C]$ and $k[C']$, respectively. Let $P = (0,0)$ be a point on C. The local ring $O_P(C)$ of P thoroughly describes the point P, it has a unique maximal ideal $\mathfrak{m} = \mathfrak{m}_P$ consisting of functions regular at P which vanish there.

First, we describe the process of blowing up a point of the affine plane $\mathbb{A}^2$. Similarly as in the previous section we start with a point $P = (0,0) \in \mathbb{A}^2$ given by a maximal ideal $\mathfrak{m} = (x,y) \subset k[\mathbb{A}^2]$ (x and y being functions of $k[\mathbb{A}^2]$

given by polynomials X and Y, respectively). Let B be as in the previous section and $k[B]$ its associated coordinate ring. The projection map $\pi : B \to \mathbb{A}^2$ defined by $\varphi(x,y,z) = (x,y)$ is regular on B and induces an embedding

$$k[\mathbb{A}^2] \longrightarrow k[B].$$

The blowup of a variety at a point is a process of an inherently local nature. Hence, we narrow the view to a certain neighborhood U of P, and replace the coordinate ring of the whole affine plane by the local ring $O_P(\mathbb{A}^2)$. The above map may be extended to the embedding

$$k[\mathbb{A}^2]_{\mathfrak{m}} \longrightarrow k[B]_{\mathfrak{m}}.$$

The local ring $k[B]_{\mathfrak{m}}$ may be regarded as $k[\mathbb{A}^2]_{\mathfrak{m}}[z]$ where z satisfies $zx = y$. Finally, we arrive at an algebraic description of the blowup of an affine plane $\mathbb{A}^2$ at a point P given by a maximal ideal $\mathfrak{m}$:

$$O_P(\mathbb{A}^2) \longrightarrow O_P(\mathbb{A}^2)[\mathfrak{m}x^{-1}]. \tag{2.31}$$

The injection (2.31) is the algebraic analog of the map σ from the Definition 2.3.1.

We have seen that the blowup of the affine space $\mathbb{A}^2$ at P is given by the ring $R' = O_P(\mathbb{A}^2)[\mathfrak{m}x^{-1}]$ which is isomorphic to the localization of $k[B]$ at $\mathfrak{m}$. Using the embedding (2.31), we identify elements of $O_P(\mathbb{A}^2)$ with their images in R'.

After having worked out the theory for an affine plane, we use these results to establish the algebraic counterpart of the Theorem 2.3.2.

Theorem 2.3.3. *Let C be an irreducible plane curve given by a polynomial $F \in k[X,Y]$ and F' its proper quadratic transform. Assume that X is not a tangent to C at P. Then*

$$(O_P(\mathbb{A}^2)/(F'))[Z] \cong O_P(C)[\mathfrak{m}x^{-1}] \tag{2.32}$$

where $ZX - Y = 0$.

Proof. The surjective map

$$\kappa : O_P(\mathbb{A}^2)[Z] \longrightarrow O_P(C)[z], \tag{2.33}$$

where $ZX - Y = 0$ and $zx - y = 0$, takes $g(X,Z)$ to $g(x,z)$ (the elements of $O_P(\mathbb{A}^2)[Z]$ are polynomials $g(X,Y,Z)$ which may be viewed as bivariate polynomials in X and Z). We show that $\operatorname{Ker}\gamma = F'(X,Z)$. Let r be the multiplicity of C at P, and $F(X,XZ) = X^rF'(X,Z)$. Now $0 = F(x,y) = F(x,xz) = x^rF'(x,z)$. Since $x \neq 0$ we conclude $F'(x,z) = 0$, and $F' \in \operatorname{Ker}\gamma$. Let now $g(X,Z)/h(X,XZ) \in \operatorname{Ker}\gamma$. Then $g(x,z) = 0$. Let p be such that $X^pg(X,Z) = u(X,XZ) = u(X,Y)$ where X does not divide u. Since $u(x,z) = 0$, $F(X,Y)|u(X,Y)$. Let $u(X,Y) = F(X,XZ)t(X,XZ)$. Then $X^pg(X,Z) = u(X,XZ) = X^qF'(X,Z)t(X,XZ)$, and hence $F'(X,Z)$ divides $g(X,Z)$.

□

The last theorem completed the algebraic description of the proper quadratic transform of an irreducible plane curve. Finally, we want to find neighboring points on the transform C' given by $R' = O_P(C)[\mathfrak{m}x^{-1}] = O_P(C)[z]$ where $xz - y = 0$. The neighboring points are zeros of elements of the ideal $(x)R'$. Consider the factor ring $\Phi = R'/(x)R'$. The image of $F' = H(Z) + XU(X,Z)$ ($X \nmid U(X,Z)$) in Φ is $\bar{H}(z)$. The ring Φ is a semi-local ring where maximal ideals describe neighboring points on C'. We see that they are given by ideals $(Z - \alpha_i)\Phi$ where $H(Z) = \prod(Z - \alpha_i)$. If a neighboring point P_i is singular, we may localize R' at the ideal $(z - \alpha_i)R'$ which corresponds to P_i. We arrive at a local ring and may repeat the procedure.

We proceed to explore a relationship between $R = O_P(C)$ and R'.

Proposition 2.3.4. *Let P, C, F be as above. There is an affine neighborhood W of P on C such that $W' = \sigma^{-1}(W)$ is an affine open subvariety of C', $\sigma(W') = W$, $k[W']$ is integral over $k[W]$, and $x^{r-1}k[W'] \subset k[W]$.*

Proof. Let $F = \sum_{i+j\geq r} a_{ij}X^iY^j$. Consider the neighborhood of P defined by the image h of $H(Y) = Y^{-r}F(0,Y) = \sum_{j\geq r} a_{0j}Y^{j-r}$ in $k[C]$. We set $W = \{Q \in$

$C \mid h(Q) \neq 0\}$. Since X is not a tangent to C at P, $H(0,0) = 1$ and $P \in W$. Then $W' := \sigma^{-1}(W)$ is affine neighborhood on C' containing all points in the first neighborhood of P.

To prove that $k[W'] = k[W][z]$ is integral over $k[W]$, observe that

$$F'(x,z) = \sum a_{ij} x^{i+j-r} z^j = \sum a_{ij} y^{i+j-r} z^{r-i}. \tag{2.34}$$

The leading coefficient of this polynomial is h which does not vanish at any point of W'. Hence h is a unit in $k[W']$, and 2.34 yields the desired integral dependence of z on $k[W]$. The last assertion follows from the fact that $x^{r-1}z^i = x^{r-1} * \frac{y^i}{x^i} = x^{r-i-1}y^i$ for $0 \leq i \leq r-1$. □

Corollary 2.3.5. *Let S be a finite set of points in $\mathbb{A}^2$. The neighborhood W in the Proposition 2.3.4 may be chosen such that is does not contain any point from S.*

Proof. For any $Q \in S$ consider a line L_Q passing through Q and not through any other point of S. Then replace h in the proposition by $h \prod_{Q \in S} L_Q$. □

The relations between the original curve C and their proper quadratic transform C' are reflected in local rings of points. Since the blowup is an isomorphism everywhere except P, local rings $O_Q(C')$ of points $Q \in C'$ different from any P_i ($P_i \in \sigma^{-1}(P)$) are isomorphic to the corresponding local rings $O_{\sigma(Q)}(C)$ on C. The differences are concentrated to local rings of points on C' lying *above* P. If $g = \frac{a}{b} \in O_P(C)$, then obviously g is regular at all P_i on C' lying above P. Hence we have an embedding

$$O_P(C) \hookrightarrow \bigcap_{P_i \in \sigma^{-1}(P)} O_{P_i}(C').$$

The Proposition 2.3.4 on the preceding page allows us to describe this relationship precisely.

Corollary 2.3.6.

$$\bigcap_{P_i \in \sigma^{-1}(P)} O_{P_i}(C') \quad \textit{is integral over} \quad O_P(C). \tag{2.35}$$

Proof. Let $g \in \bigcap_{P_i \in \sigma^{-1}(P)} O_{P_i}(C')$, i.e. g is regular at all P_i's. Let $\mathcal{P}$ be the set of poles of g on C'. This set is algebraic, and hence finite. We may thus find a neighborhood W of P on C such that W' does not contain any pole of g, i.e. $g \in k[W']$. This means that g is integral over $k[W]$, and hence over $O_P(W)$ since $O_P(C) \supset k[W]$. The fact $O_P(W) = O_P(C)$ concludes the proof. □

SINGULARITY(C)

Input: $F \in k[Y,Y]$ - defining polynomial of a plane curve C of degree n in regular position having no multiple components

Output: standard decomposition of singularities of C

1. $\mathcal{F} \leftarrow \varnothing$
2. $B_1 \leftarrow f$
3. $\bar{B}_1 \leftarrow \gcd(\mathrm{res}_{x_2}(f, \frac{\partial f}{\partial x_1}), \mathrm{res}_{x_2}(f, \frac{\partial f}{\partial x_2}))$
4. $B_1 \leftarrow \frac{\bar{B}_1}{\gcd(\bar{B}_1, \bar{B}_1')}$
5. **for** $i \geq 2$ **while** $\deg(B_{i-1}) > 0$ **do**
6. $\quad \bar{B}_i \leftarrow \gcd(\mathrm{res}_{x_2}(f, \frac{\partial^i f}{\partial x_1^i}), \ldots, \mathrm{res}_{x_2}(f, \frac{\partial^i f}{\partial x_2^i}))$
7. $\quad B_i \leftarrow \frac{\bar{B}_i}{\gcd(\bar{B}_i, \bar{B}_i')}$
8. $\quad \bar{A}_{i-1} \leftarrow \frac{B_{i-1}}{B_i}$
9. $\quad$ **if** $\deg(\bar{A}_{i-1}) > 0$ **then**
10. $\quad\quad q_{i-1}(x_2) \leftarrow \tilde{p}_{i-1}(x_1)x_2 - p_{i-1}(x_1) = \mathrm{subres}_1(f(x_1,x_2), \frac{\partial f}{\partial x_1}(x_1,x_2), x_2) \mod \bar{A}_{i-1}(x_1)$
11. $\quad\quad \mathcal{F}_{i-1}^* \leftarrow \{(\alpha, p_{i-1}(\alpha), 1)\}_{\bar{A}_{i-1}(\alpha)=0}$
12. $\quad\quad$ determine the expanded neighboring graph $\mathcal{F}_{i-1}$ of $\mathcal{F}_{i-1}^*$
13. $\quad\quad \mathcal{F} \leftarrow \mathcal{F} \cup \mathcal{F}_{i-1}$
14. $\quad$ **end**
15. $\quad i \leftarrow i+1$
16. **end**
17. **return** $\mathcal{F}$

Algorithm 1:

NEIGHBORHOOD TREE(P)

Input: A singular point P of a curve

Output: Neighborhood tree rooted in P

1. determine a change of coordinates T_1 moving the projective point $(0:0:1)$ to P;
2. determine a change of coordinates T_2 such that $F' = F \circ T_1 \circ T_2$ contains $(0:0:1)$ but none of $(1:0:0)$, $(0:1:0)$ and such that no axis is tangent at $(0:0:1)$ to F';
3. perform the quadratic transformation on F' centered at $(0:0:1)$ yielding a new curve F'';
4. compute the set $\mathcal{S}$ of singularities on $F'' \cap V(Z)$;
5. **for all** $R \in \mathcal{S}$ **do**
6. call NEIGHBORHOOD TREE recursively on R;

end

Algorithm 2:

NEIGHBORHOOD GRAPH(C)

Input: A projective plane curve C having no multiple components

Output: Neighborhood graph of C

1. determine the set $\mathcal{S}$ of all singular points of C
2. **for all** $Q \in \mathcal{S}$ **do**
3. NEIGHBORHOOD TREE(Q)
4. **end**

Algorithm 3:

Chapter 3

Parametrization of Plane Curves

Algebraic sets may be represented in many different ways. Practice shows that each representation is suitable for solving different types of problems. Usually, only some (problem related) information is made easily accessible by each representation. In general, it is required that no essential information, even though possibly not relevant to the problem under consideration, must be lost when converting from one representation to some other. If necessary, hidden information may be recomputed. In this chapter, we will study two different kinds of representations of algebraic sets given by mappings between varieties.

The isomorphism is the most complete algebraic correspondence between varieties. It provides not only a 1–1 mapping of points on varieties, but it retains even their complete structure. Let us consider two different representations of the two-dimensional unit circle S_2 in the plane $\mathbb{A}^2$. It is determined by the set of all solutions of

$$x^2 + y^2 - 1 = 0 \tag{3.1}$$

in a certain field k. An isomorphic set of points S_2' is described by the inter-

section of a unit sphere and the xy-plane in $\mathbb{A}^3$

$$x^2 + y^2 + z^2 - 1 = 0 \qquad z = 0. \tag{3.2}$$

The two sets (3.1) and (3.2) are isomorphic, the isomorphism is given by the map $\iota : (x, y) \mapsto (x, y, 0)$. Each point on S_2 corresponds to a unique point on S_2 and vice versa. Now, the variety given by equation (3.2) may be represented as the image of $S_2 \subset \mathbb{A}^2$ under the mapping ι.

Sometimes it is sufficient to give a description of algebraic sets which retains only some easily accessible properties most important for a particular problem. The result is a simplified model stripped of all unnecessary information. Let us return to the circle from above. The functions

$$\begin{aligned} x(t) &= \frac{2t}{t^2+1} \\ y(t) &= \frac{t^2-1}{t^2+1} \end{aligned} \tag{3.3}$$

define a map from $\mathbb{A}^1$ to S_2 which yields for almost all values of parameter t a point on S_2. Thus we may consider S_2 to be represented as the image of the affine line under the map given by equations (3.3). However, the point $(0, 1) \in S_2$ is not in the image of this map. It is approached asymptotically from right for values $t \to \infty$ and from left for values $t \to -\infty$. If we used the projective line $\mathbb{P}^1$ instead of the affine one, we would get the point $(0, 1)$ too. We see, the map (3.3) is an isomorphism of the set $\mathbb{A}^1 \setminus \{0\}$ and the open affine subset of points of S_2 with non-zero x-coordinate. Such correspondence is called birational isomorphism (cf. Definition 1.1.19). This chapter is devoted to the problem of finding birational maps between an affine line and arbitrary plane curves. This kind of maps does not preserve all points, but the 1–1 correspondence is restricted only to affine open subsets (cf. Proposition 1.2.18). In the case of curves, a 1–1 correspondence for all but finitely many points is obtained.

If we expand functions $x(t)$ and $y(t)$ into power series, we get

$$\begin{aligned} x(t) &= 2t - 2t^3 + 2t^5 - 2t^7 + 2t^9 + O(t^{10}) \\ y(t) &= -1 + 2t^2 - 2t^4 + 2t^6 - 2t^8 + O(t^{10}) \end{aligned} \tag{3.4}$$

These functions satisfy the equation

$$(x(t))^2 + (y(t))^2 = 1$$

identically as well as equations (3.3) do. Hence, (3.4) may be viewed as another way of representing the circle using transformations defined by power series. However, the series (3.4) are convergent only for $|t| < 1$ which corresponds to the lower half of the circle. We may overcome this deficiency by giving other pairs of series such that they together cover the whole circle.

Yet another representation of the circle is given by Puiseux series

$$\begin{aligned} x(t) &= t \\ y_1(t) &= 1 - \frac{t^2}{2} - \frac{t^4}{8} - \frac{x^6}{16} - \frac{5t^8}{128} - \frac{7t^{10}}{256} + O(t^{11}), \\ y_2(t) &= -1 + \frac{t^2}{2} + \frac{t^4}{8} + \frac{t^6}{16} + \frac{5t^8}{128} + \frac{7t^{10}}{256} + O(t^{11}) \end{aligned} \tag{3.5}$$

This type of series plays an important role in the study of structure of singular points on curves.

So far, we presented some possibilities to represent one dimensional algebraic sets in a plane. The first representation – *implicit* – is usually the starting point in solving different problems. It evolves in the process of satisfying constraints given by polynomial equations. The implicit representation allows us to give a quick answer to questions like

Is a given point on/below/above an algebraic set?

The spots where singular points are lying may be "quickly" located using implicit representation. On the other hand, it does not provide an easy access to information suitable to find points in an algebraic set. Except the

intersections of the circle with axes it is not clear how to determine other points lying on it. This question is easily answered having the *parametric* representation of an algebraic set, i.e. a birational map from the affine space to the algebraic set. In the example above we may evaluate the functions 3.3 for an arbitrary argument, and obtain a point on S_2 (there are only finitely many bad choices of t). The parametric representation of algebraic sets allows us to decide easily questions like

Find points on an algebraic set.

In contrast, it is not easy to see how to determine e.g. singular points of an algebraic set given in parametric representation. The representation by *series* bears a lot of easily accessible information about in their coefficients and exponents. A set of series centered at a singular point of a curve describe all branches and provides complete structure of the singularity.

3.1 Overview of Parametrization

In this section we give a short overview over major steps of parametrization of curves.

Let us consider the curve in Figure 2.7 on page 33 given by the polynomial $y^2 - x^3 - x^2$. We intersect it with a line

$$L_t : y = tx$$

passing through the origin, and look for intersection points different from $(0,0)$. See Figure 3.1 on the facing page. The number of intersections of plane curves is stated in the following theorem.

Theorem 3.1.1 (Bezout). *Let C and D be two projective plane curves without common components defined over an algebraically closed field k. Let C be given by a*

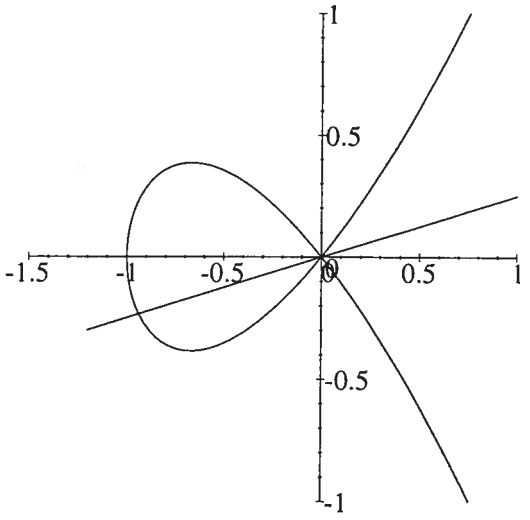


Figure 3.1:

form of degree m and D by a form of degree n, and let $I_P(C, D)$ *denote the* intersection multiplicity *of C and D at the point P (distinct or infinitely near). Then*

$$\sum_{P \in C \cap D} I_P(C, D) = mn \tag{3.6}$$

where P runs over all intersection (distinct or infinitely near) points of C and D.

Bezout's Theorem applied to the above example guarantees the existence of exactly one additional intersection point P. For almost all values of parameter t this points will be different from $(0, 0)$. Its coordinates are given by $P(t) = (t^2 - 1, t(t^2 - 1))$. This construction yields immediately a birational correspondence between the curve $y^2 - x^3 - x^2$ and the affine line $\mathbb{A}^1$. The process applied in the example may be easily generalized to determine parametric equations of arbitrary plane curves (if possible at all).

After we have seen some examples, we give a precise formulation of the goal of parametrization, and a brief overview of major steps in this process. Details will be worked out later in this chapter. The reader may consult [AB88a, SW91, Wal50].

Let C be a projective absolutely irreducible plane curve, i.e. irreducible over the algebraic closure of k, given by a homogeneous polynomial $F(X,Y,Z) \in k[X,Y,Z]$ of degree n. The field k is supposed to be algebraically closed of characteristic zero. However, parametrization algorithms never use this assumption in its entirety. Extensions of k are constructed only when there is a need to represent algebraic sets which either do not have any description over k or their description would require factorization. The whole process of parametrization is performed in k or in a finite extension of it.

Definition 3.1.2. Let C be a curve as above. Then C is called *k-parametrizable* (or *k-rational*) if there is an isomorphism $\tau^* : k(C) \to k(t)$ where $k(t)$ is the field of rational functions in t. If no confusion may arise, the reference to the ground field is skipped. A *parametrization* of C is a birational map

$$\tau : \mathbb{P}^1 \longrightarrow C$$

induced by τ^*.

Remark 3.1.3. A birational map between $\mathbb{P}^1$ and C gives raise to an isomorphism between open sets (cf. Proposition 1.2.18). Since projective curves have only finitely many points at infinity, we may find a transformation such that all singular points are lying in the affine plane. After passing from the projective to the affine space only finitely many (non-singular) points are lost. Due to the Proposition 1.2.18 this does not cause any problems concerning parametrization. In order to keep the description simple, we often deal only with an affine part of C.

The first question which arises is whether a parametrization of a given curve exists at all.

Definition 3.1.4. Let C be an irreducible plane projective curve given by a

form F of degree n. The number

$$g = \frac{(n-1)(n-2)}{2} - \sum_P \frac{m_P(C)(m_P(C)-1)}{2}, \tag{3.7}$$

where P runs over all (distinct of infinitely near) singularities of C, is called *genus* of C.

Theorem 3.1.5. *An irreducible curve is parametrizable if and only if its genus is zero.*

Proof. See [Wal50]. □

This theorem provides a necessary and sufficient condition to decide whether a curve is parametrizable or not. At the moment, the author is not aware of any other efficient algorithmic decision procedure for this problem. It will be shown later that the ingredients necessary to apply the previous theorem to decide the rationality are hard to compute. In other words, if we have all distinct and infinitely near singular points of C with their multiplicities, it is then rather easy to compute the parametrization. From this point of view, the theorem is not very suitable as a decision procedure as the saving gained by stopping the parametrization algorithm due to the fact that no parametrization exists is in many cases relatively small compared to the time spent on trying to compute a parametrization itself and failing. We are not aware of any deterministic procedure to decide the rationality of a curve without actually computing the genus.

A.B. Sørensen ([Sør91]) developed a heuristic algorithm to decide the rationality of a curve based on counting the number of points over finite fields (see Algorithm 4 on the next page). This approach utilizes the fact that for curves of genus 0 the exact number of points over a finite field is known.

Let $\mathbb{F}_q$ denote a finite field with q elements, q being a prime power, and N_m the number of $\mathbb{F}_{q^m}$-rational points on a curve X.

Proposition 3.1.6. *Let X be a non-singuar curve of genus 0. Then*

$$N_m = 1 + q^m$$

This proposition may be used as a decision procedure to recognize rationality of a curve.

RATIONAL(C)

Input: A curve C defined over $\mathbb{F}_q$ and a bound $B \geq 1$

Output: Is C rational?

1. determine the number N_1^* of of non-singular points on C over $\mathbb{F}_q$ and a bound δ_1 on $|N_1 - N_1^*|$
2. **if** $|N_1^* - (1+q)| > \delta_1$ **then return** "Not rational"
3. $i \leftarrow 1$
4. **while** $|N_i^* - (1+q^i)| > \delta_i$ **and** $i < B$ **do**
5. $\quad i \leftarrow i+1$
6. $\quad$ compute N_i^* and a bound δ_i on $|N_i - N_i^*|$
7. $\quad$ **if** $|N_i^* - (1+q^i)| > \delta_i$ **then return** "Not rational"
8. **end**
9. **return** "Probably rational"

Algorithm 4:

To recognize a curve of genus 0 using Algorithm 4 is rather difficult, it requires availability of some bound B, and is not worked out in full detail yet. Nevertheless, this approach could prove to be a good starting point to attack the problem of efficient decision procedure for rationality without actually computing the genus. Despite of this fact, the Theorem 3.1.5 provides a feasible algorithmic decision procedure. From now on, whenever a curve is to be parametrized, it is supposed that a parametrization exists.

Recalling the example from the beginning of this section we may sketch main steps in the process of determining a parametrization of a plane curve. The parametrization is supposed to exist. In the first step we found some

distinguished points on the curve – the singular points. In general, it will not suffice to compute only distinct singular points, it will be necessary to determine the whole neighborhood graph of the curve. In the next step, a generic line L_t was passed through the double point at the origin. In general, we set up a generic system of curves with undetermined coefficients and force it through all singular points of the curve. This lowers the dimension of the system causing some coefficients to get fixed values. In the example, the line had exactly one intersection point with the given curve depending on the only free parameter t of the line L_t. In general, the dimension of the system after specialization of parameters will be greater than one. It will be necessary to find some additional points to decrease the dimension to one. Finally, determining the only intersection of the system and the curve yields a parametrization. This process is summarized in Algorithm 5.

PARAMETRIZATION(C)
Input: plane irreducible curve C
Output: parametrization of C

1. Determine complete structure of singular points of C
2. Set up a generic system H of curves
3. Pass H through all singularities with prescribed multiplicity
4. Pass the system H through additional points to lower its dimension to 1
5. Determine the only intersection of H and C depending on the only free parameter of H

Algorithm 5: Parametrization – sketch

Basically, the Algorithm 5 consists of two major tasks. First, description of the structure of singular points is computed, and, second, a system of curves is passed through certain points in such a way that it finally contains

only a single undetermined coefficient. A more detailed description of this traditional method will be given in Section 3.4.

3.2 Resolution of Singularities, Adjoint Curves

In the first step of Algorithm 5 on the page before the structure of singular points is determined. The Section 2.3 describes two basic ways to obtain the full description of singular points of a curve. Using geometric methods (quadratic transformation), the resulting data structure is a tree of (distinct and infinitely near) singular points associated with their multiplicities. The algebraic approach, on the other hand, yields the integral closure of the coordinate ring of the curve as a finite module. This structure contains description of all singular points. We show, how either of the two structures above, the neighborhood graph and the integral closure of the coordinate ring, can be used to determine the system of *adjoint curves* which is the main goal of the first part of the parametrization algorithm. This construction appears in many algorithms in algebraic geometry, number and coding theory, and in other fields of mathematics, and is of interest on its own.

3.2.1 Geometric Methods

Let us assume, for the given curve C, the neighborhood graph has been computed (see Section 2.1.2). We present how to determine the system of adjoint curves to C based on the neighborhood graph. For detailed description of this approach we refer to [AB88a, SW91].

Consider the example at the beginning of Section 3.1. In order to parametrize the curve $y^2 - x^3 - x^2$, we passed a line through the origin. This choice of reference point was not accidental. If we had passed it through any other (non-singular) point Q, we would have obtained two intersections of L_t and the curve C_2'' instead of a single one.

In general, instead of a line, a system $H_a = \sum h_{ijk}X^iY^jZ^k$ (h_{ijk} undetermined coefficients) of curves of degree a is passed though all singular points (distinct an infinitely near) with prescribed multiplicity. In the subsequent step in the parametrization algorithm, H_a (with some coefficients already fixed) is forced to pass though a certain number of additional points to decrease the dimension of H_a to one. A good choice of the degree a may greatly simplify the search for these points. In this section, the degree a is kept undetermined. At the end we discuss some possibilities for the value of a and its impact on the number of additional points which have to be chosen.

Now, we proceed to set up the system of adjoint curves. Assume, the curve C to be parametrized is given by a form of degree n. Let

$$H_a = H = \{ \sum_{i+j+k=a} h_{ijk}X^iY^jZ^k \mid h_{ijk} \in k\}. \tag{3.8}$$

Curves of fixed degree may be considered as points in certain projective space. In particular, concerning the coefficients $(h_{a00}, \ldots, h_{00a})$ of H_a defining a projective point we see that there is a bijective mapping between H_a and $\mathbb{P}^{\frac{1}{2}a(a+3)}$. If an arbitrary coefficient $h_{i_0j_0k_0}$ is set to a fixed value, the corresponding subspace of $\mathbb{P}^{\frac{1}{2}a(a+3)}$ is linear (defined by $hi_0j_0k_0 = 0$).

Let us consider a slightly more general situation. Let $P_1, \ldots, P_l \in \mathbb{P}^2$, and $r_1, \ldots, r_l$ be non-negative integers. Let

$V_a(r_1P_1, \ldots, r_lP_l) =$

$\{$ projective curves D of degree a such that $\mathrm{m}_{P_i}(D) \geq r_i$, $i = 1, \ldots, l\}$.

It is important to be able to determine the dimension of such a system. The following theorem provides a very complete answer to this question.

Theorem 3.2.1.

(i) $V_a(r_1P_1, \ldots, r_lP_l)$ *is a linear subspace of* $\mathbb{P}^{\frac{1}{2}a(a+3)}$,

$$\dim V_a(r_1P_1, \ldots, r_lP_l) \geq \frac{d(d+3)}{2} - \sum_{i=1}^{l} \frac{r_i(r_i+1)}{2} \tag{3.9}$$

(ii) If $a \geq (\sum_{i=1}^{l}) - 1$, *then*

$$\dim V_a(r_1P_1, \ldots, r_lP_l) = \frac{d(d+3)}{2} - \sum_{i=1}^{l} \frac{r_i(r_i+1)}{2} \tag{3.10}$$

Proof. See [Ful89], Chap. IV, §2. □

The geometric approach outlined in this section starts from the system

$$H_a = V_a(0P_1, \ldots, 0P_l).$$

In the course of computation its dimension is successively decreased forcing it to have a maximal number of a priori determined intersections with the original curve C. According to the Theorem 3.2.1, every r-fold point, H_a is forced through, drops its dimension by $\frac{r(r+1)}{2}$. Singular points is a suitable choice for such points. The reason for this is that they appear on the curve always in whole classes. If a singular point is given by $(p(\alpha), q(\alpha), r(\alpha))$ where α defines an extension of k, all elements of this class are lying on the curve. Forcing H_a trough such class of points does not introduce any algebraic extensions. All computations may be performed in the ground field using gcd computations and resultants. This fact motivates the following definition.

Definition 3.2.2. Let C be an irreducible plane curve. Let P be a singular point (distinct or infinitely near) of C of multiplicity $m_P(C)$. A curve D is called an *adjoint curve* to C at P if

$$m_P(D) \geq m_P(C) - 1. \tag{3.11}$$

The set of curves which are adjoint to C at P is denoted by $\mathrm{Adj}_P(C)$. If (3.11) holds for all singular points P on C (distinct or infinitely near), and hence for all P, D is called an *adjoint curve* to C. The set of adjoint curves to C is denoted by $\mathrm{Adj}(C)$.

Let us now consider

$$V_a((m_{P_1}(C) - 1)P_1, \ldots, (m_{P_l}(C) - 1)P_l) \text{ for } a \geq n - 2 \tag{3.12}$$

where P_i's are singular points of C. Any curve in (3.12) is an adjoint curve to C. The previous theorem shows that for $a \geq n-2$

$$\begin{aligned}
&\dim V_a((m_{P_1}(C)-1)P_1,\ldots,(m_{P_l}(C)-1)P_l)\\
&\geq \frac{1}{2}a(a+3) - \sum_{P_i}\frac{m_{P_1}(C)(m_{P_1}(C)-1)}{2}\\
&= \frac{1}{2}a(a+3) - \frac{(n-1)(n-2)}{2}\\
&= n(a-n+3)-3 \geq 0.
\end{aligned}$$

On the other hand, by Bezout's Theorem, H_a and C have an intersections (properly counted). This number includes

$$\sum_P I_P(C,H_a) \geq \sum_P m_P(C)(m_P(C)-1) \tag{3.13}$$

intersections at singular points $P_1,\ldots,P_l$ of C. The above inequality is strict if and only if H_a and C have common tangents at some P. However, there are only finitely many singular points and at each point only finitely many tangents exist, for almost all choices of (yet) free parameters the equality in 3.13 holds. If $n \geq 3$, there must be other intersection points different from $P_1,\ldots,P_l$, N_a in number, say. Bezout's Theorem yields

$$N_a = an - \sum_P m_P(C)(m_P(C)-1) = an-(n-1)(n-2) \tag{3.14}$$

for almost any choice of free parameters in H_a. Moreover, Theorem 3.2.1 implies

$$\dim H_a = \frac{1}{2}a(a+3) - \sum_{P_i}\frac{m_{P_1}(C)(m_{P_1}(C)-1)}{2}. \tag{3.15}$$

For, if $a \geq n-2$, we have

$$a(a+1) \geq (n-1)(n-2). \tag{3.16}$$

On the other hand, if $a < (\sum_P m_P(C)) - 1$, then using the Cauchy inequality

we obtain

$$a(a+1) < (\sum_P m_P(C) - 1)(\sum_P m_P(C)) = (\sum_P m_P(C))^2 - \sum_P m_P(C)$$
$$\leq \sum_P (m_P(C))^2 - \sum_P m_P(C) = \sum_P m_P(C)(m_P(C) - 1) = (n-1)(n-2) \tag{3.17}$$

which contradicts to (3.16).

Let $k \geq -2$. If we set $a = n + k$, we obtain

$$\dim H_a = (k+3)n + \frac{1}{2}(k^2 + 3k - 2) \tag{3.18}$$

$$N_a = (k+3)n - 2. \tag{3.19}$$

In particular, for $a \in \{n-2, n-1\}$, we have $\dim H_a = N_a$.

At this moment, there is no preference for the value of a. However, we will see later that the choice may have an enormous impact on the complexity of subsequent steps. Some possibilities of choosing a will be discussed in Section 3.3.

Example 3.2.3. Let C be a projective curve defined by the polynomial

$$Y^3 - Y^2Z - X^3 - X^2Y + X^2Z$$

See Figure 3.2 on the facing page. The curve C has only one ordinary singular point at the origin. Obviously, the system of adjoint curves consists of all curves passing through $(0,0)$

$$\sum_{i+j+k \geq 1} h_{ijk} X^i Y^j Z^k$$

where $h_{ijk} \in k$.

The approach to compute adjoint curves presented in this section uses only elementary polynomial arithmetic. This fact makes it easy to implement. Polynomials are treated here just as lists of coefficients and their exponents. This *naive* view makes this approach computationally rather simple, but hard to keep it efficient. One of main problems is the strong dependence on coordinate changes which may cause a dramatic speed-up on

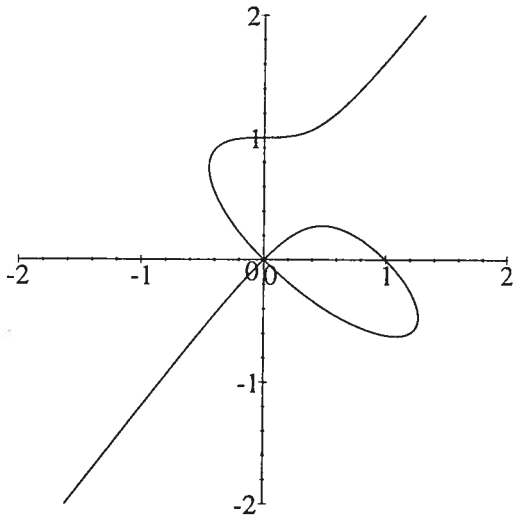


Figure 3.2:

the one side, but also unnecessary complications introduced into, in their nature possibly easy, problems (see discussion at the end of Section 2.2.3) on the other side. Another inconvenience arises from the fact that only adjoint curves of a fixed degree are obtained. It is not obvious to see how to reuse already computed adjoint curves to construct other ones with possibly higher degree. We will see that the latter question does not arise in the context of parametrization. However, as already mentioned, computing adjoint curves arises in many fields where it is sometimes necessary to obtain all adjoint curves regardless of the degree.

3.2.2 Algebraic Methods

In the previous section we presented an approach to compute adjoint curves using facts based on geometric properties. On this way, an easy algorithm can be proposed. However, there are some serious drawbacks which restrict the usefulness of this method.

One of main disadvantages of the geometric approach was a rather strong

dependence on changes of coordinate system which will be studied in our forthcoming paper. Hence, we are looking for a coordinate-free description of an algorithm for adjoint curves. We will present here only a brief sketch of the method which is thoroughly described in [Mňu95a] (see Appendix A. This method works along the same lines as the geometric one. However, it exploits more intrinsic structures of the problem which the geometric method was unable to do as it depends on rather easy properties derived from the defining polynomial.

Again, we start from an irreducible plane curve C given by a form F of degree n. Since all notions in this section are of local nature, we consider only the affine part of C defined by a polynomial $f(x,y) = F(X,Y,1)$ (see also Remark 3.1.3). The basic knowledge required to construct adjoint curves is, similarly to the geometric method, a complete description of the structure of singular points. Now, however, no expansion techniques using quadratic transformation is used. Instead, the non-singular model of C is obtained by computing the integral closure $\overline{k[C]}$ of the coordinate ring of C. It can be shown that this ring may be represented as a finite module which is a basic prerequisite for this method to become algorithmic. Moreover, the integral closure naturally corresponds to a plane curve – the non-singular model of C. Having arrived at this point, a description of the structure of singularities is accomplished. Hence, the method has achieved the same stage as the geometric one after the expansion of the neighborhood graph.

Next, the system of adjoint curves Adj(C) is computed using the integral closure of the coordinate ring. The theoretical basis of this method is established in following theorems (cf. Appendix A).

Theorem 3.2.4. *Let C be an absolutely irreducible plane curve. Then*

$$\mathrm{Adj}(C) = \mathfrak{C}_{\overline{k[C]}|k[C]} \tag{3.20}$$

Corollary 3.2.5. *It holds*

$$F'(y)\mathcal{C}_{\overline{k[C]}|k[x]} = \mathfrak{C}_{\overline{k[C]}|k[C]}$$

Main steps are summarized in the Algorithm 6. For precise description and details of the underlying theory we refer to [Mňu95a].

ADJOINTS ALGEBRAIC(C)

Input: absolutely irreducible plane curve C

Output: basis of Adj(C) as a finite $k[x]$ module

Description: Main steps of the algorithm.

1. compute a basis of integral closure $\overline{k[C]}$ of $k[C]$ in $k(C)$
2. compute a basis $\{\eta_i\}_{i=1}^n$ of the complementary module $\mathcal{C}$ of $\overline{k[C]}$ with respect to $k[x]$
3. **return**$(\{\frac{\partial F}{\partial Y}\eta_i\}_{i=1}^n)$

Algorithm 6:

Example 3.2.6. Let us consider the curve from Example 3.2.3. We have

$$k[C] = k[x,y]/(y^3 - y^2 - x^3 - x^2y + x^2)$$

Moreover, the closure of $k[C]$ is a finite $k[x]$-module

$$\overline{k[C]} = k[x] + yk[x] + \frac{y(y-1)}{x}k[x]$$

We set

$$e_1 = 1$$

$$e_2 = y$$

$$e_3 = \frac{y(y-1)}{x}$$

Then the matrix of traces of e_ie_j is

$$\begin{pmatrix} 3 & 1 & 2x \\ 1 & 2x^2+1 & 3x^2-2x \\ 2x & 3x^2-2x & 2-2x+2x^2 \end{pmatrix}$$

The complementary module has the following basis as a $k[x]$-module

$$\eta_1 = -2x^2 - 8x^3 + 5x^4 - 2 + 2x - 2y + yx + 2x^2y - 6yx^3 - 3y^2x + 4y^2 + 4y^2x^2$$
$$\eta_2 = 2 - 2x + 6x^2 - 6x^3 + 2y - 3yx - 2x^2y + 9y^2x - 8y^2$$
$$\eta_3 = \frac{-3x^3 + 4x^2 + 4x^4 + 9yx^3 - 2x^2y - 6y^2x^2 + 2y - 2y^2}{x}$$

The basis of the conductor is given by

$$\zeta_1 = \left(-36x^3 + 23x^4 - 4 + 4x + 8x^2\right)y^2 + \left(36x^3 - 23x^4 + 4 - 4x - 8x^2\right)y$$
$$- 4x^3 + 36x^5 - 8x^4 + 4x^2 - 23x^6$$
$$\zeta_2 = \left(-36x^3 + 23x^4 - 4 + 4x + 8x^2\right)y$$
$$\zeta_3 = -36x^4 + 23x^5 - 4x + 4x^2 + 8x^3$$

Hence, the adjoint system

$$\mathrm{Adj}(C) = \zeta_1 k[x] + \zeta_2 k[x] + \zeta_3 k[x].$$

The Algorithm 6 on the preceding page yields a description of the system of adjoint curves represented as a finite $k[x]$ module. The advantage compared with the geometric method appears in the fact that the complete module of adjoint curves is available while the former method provided only some elements of Adj(C). The algebraic method is completely coordinate-free which makes it less dependent on the way the input is represented. As the whole module of adjoint curves is constructed, more flexible strategies in decreasing of the dimension may be applied in subsequent steps (see Section 3.3).

3.2.3 Approximate Methods

In [Tra95] a novel approach to computing adjoint curves was started. The assumption that objects are represented exactly has been droped working on approximate representations.

Let C be a curve defined by a polynomial $f(x,y)$ of degree n with only approximately known coefficients. Under the assumption that C has only ordinary singularities an algorithm to compute all adjoint curves of degree $n-3$ is presented. It uses the singular value decomposition to obtain generators of the adjoint ideal. The lack of exactness of representations is counterbalanced by a knowledge of the rank of a linear subspace of polynomials generating the adjoints.

3.3 Searching for Rational Points

In the previous section we gave a detailed description of how adjoint curves for a given curve C are computed provided a description of the structure of singular points is available. When considering the geometric method to solve this problem, a system of curves of certain degree H_a was defined, and its dimension successively reduced. As already mentioned, a good choice of the degree a of H_a is of great importance for step 4 of Algorithm 5 on page 59. Now we will analyze this problem in more detail.

Assume, a system adjoint curves H_a to C has already been computed. Here, H_a is used to denote the system

$$V_a((\mathrm{m}_{P_1}(C)-1)P_1,\ldots,(\mathrm{m}_{P_l}(C)-1)P_l)$$

The next task is to decrease its dimension to 1 in such a way that all but one intersection of the resulting pencil of curves and C are a priori known. A possible solution is to find additional non-singular points on C and force the adjoints to pass through all these points reducing the dimension step–by–step to one. We have already seen that passing a system of curves through one additional point leads to one independent condition imposed on its coefficients. Hence, the reduction of the dimension to one may be achived. The crucial role in the reduction plays the efficiency of computing the necessary points.

In some cases, no additional points to pass the adjoint curves through are needed. For the curve in Figure 2.7 on page 33 given by

$$y^2 - x^3 - x^2$$

almost all adjoint curves intersect C in one point. In other cases, it may be possible to reduce the dimension of the system of adjoint curves by passing it through some of singular points with a higher multiplicity. It is a non-trivial combinatorical task to choose the degree of the system H_a in such a way that as many as possible already known points on the curve may be reused, or such that no additional (non-singular) points have to be computed. In the sequel, we present some strategies to choose the degree a to fulfil these conditions.

Let us consider under which condition additional points may be chosen efficiently. The original parametrization algorithm (see [Wal50, SW91]) used $a = n - 2$. Using equations (3.18) and (3.19) (Figure 3.3 shows some values of $\dim H_a$ and N_a) it may be easily seen that there are still $n - 2$ intersection points of H_a and C. Reducing the dimension of H_a to one requires choosing $n - 3$ non-singular points on C. A similar situation arises for $a = n - 1$.

k	$\dim H_a$	N_a
-2	$n-2$	$n-2$
-1	$2n-2$	$2n-2$
0	$3n-1$	$3n-2$
1	$4n+1$	$4n-2$
2	$5n+4$	$5n-2$

Figure 3.3:

For $a = n$ the situation seemingly stays unchanged. To reduce the dimension of H_n to one, $3n - 3$ non-singular points are to be chosen. In [SW91] it is shown that in this case the curve may be cut by three different lines meeting

in one simple point. The intersection points form, for almost all selections of lines, three classes each containing $n-1$ non-singular points of C. The advantage lies in the fact that passing through classes of points no algebraic extension of the ground field is necessary.

The same idea works also for $a = n+1$ where four lines are used to obtain a set of $4n-3$ non-singular points. In general, combinatoric criteria impose conditions on the choice of a. A proper value of a should allow to obtain the additional points required in step 4 of Algorithm 5 on page 59 by easy means, e.g. by intersecting the original curve with a number of lines. The acquired points are either all necessary additional points or the number of remaining point is to be kept minimal. J. Schicho and J.R. Sendra (see [SS92]) formalized this process of choosing an optimal degree of H_a, and derived some theorems describing principles behind this combinatorial problem. The basis of their considerations is to regard the Bezout's Theorem and the genus formula (3.7) as Diophantine equations in some set of parameters.

Let $\{Q_i\}_{i=1}^{k}$ be arbitrary points of C, $r_i = \mathrm{m}_{Q_i}(C)$. If the coordinates of Q_i lie in some algebraic extension $k(\alpha)|k$ of degree s_i, the "point" $Q_i = (p(\alpha_i), q(\alpha_i), r(\alpha_i))$, p, q, r polynomials, defines a class of s_i points. Let $m_i \geq 1$ denote an arbitrary integer. The intention is to pass the generic system of curves through each class of points Q_i with multiplicity m_i. Let $t \geq 1$ denote the number of residual intersections. By Bezout's Theorem we get

$$\sum_{Q_i} m_i s_i r_i = na - t. \tag{3.21}$$

Another condition on m_i arises by requiring C not to be a component of the resulting system. The problem of finding a suitable value for a may be viewed as an optimization problem with parameters $a, t, m_1, \ldots, m_l$ to minimize the value of t. In [SS92], possible solutions of (3.21) are studied, and a number of important consequences is derived for special curves. In certain cases, this approach may lead to a quick detection of optimal value for

a, in general, however, a may turn out to be rather large causing subsequent operations on polynomials to prove prohibitively expensive.

Example 3.3.1. Let us assume three points $\{Q_1, Q_2, Q_3\}$ on a curve of degree 7 have been found with $s_1r_1 = 4$, $s_2r_2 = 6$, $s_3r_3 = 6$. The equation (3.21) becomes

$$4m_1 + 6m_2 + 6m_3 = 7a - t$$

This Diophantine equation has a solution for $t = 1$: $m_1 = 2$, $m_2 = 1$,$m_3 = 1$, $a = 3$.

After the system H_a has been passed through all singularities, some additional (non-singular) points C may be required to reduce the dimension of H_a to one. Note that selecting good points on C is a highly non-trivial task. By intersecting the curve by lines or other curves it is possible to obtain classes of points. Their coordinates may, however, contain algebraic numbers introducing possibly unnecessary ground field extensions in the parametization step. In special cases, passing H_a through singular point P with a multiplicity higher than $m_P(C) - 1$ may effectively decrease its dimension. This strategy is usually applicable only in cases where there are singular points having small multiplicity. Obviously, the best choice is provided by points with coordinates in the ground field itself. The Definition 3.1.2 and the parametrization algorithm in [Wal50] show that if a curve defined over a (not necessarily algebraically closed) field k has a point with coordinates in k, then there are infinitely many such points on the curve. Despite of this, searching for such points by brute force may turn out to be extraordinarily time consuming task. It was shown that there exist plane curves of degree n whose smallest $\mathbb{Q}$-rational point (with respect to the bit-length of its coordinates) is of magnitude bigger than 2^n. Some curves might not have points with coordinates in k at all. However, in [HH90] a birational map of an arbitrary curve of genus 0 and degree n to a curve of degree $n - 2$

is constructed. Moreover, the coefficients of this map lie in the ground field k. Hence, there is a birational equivalence over k mapping a curve to a conic or a line. In the latter case, a k-rational point on a line may be lifted to a k-rational point on the curve. In the former case, if there are no k-rational points on the conic, a point with coordinates in an extension of k of degree 2 may be found by intersecting the conic by a line.

The approach of Hilbert and Hurwitz requires to compute the system of adjoint curves in each reduction step. For a curve of degree n, about $\lfloor n/2 \rfloor$ adjoint systems would have to be computed. This turns out to be not feasible for higher degree curves. Recently, R. Sendra and F. Winkler (see [SW93]) used a variant of this approach to design an efficient algorithm which performs the reduction to a conic in two steps. Let us give a brief outline of this method. For details we refer to [SW93].

Let C be a curve given by a homogeneous polynomial $F(X,Y,Z)$ of degree n. The algorithm in [HH90] is based on considerations of a birational transformation defined by

$$\begin{aligned} X' &= \varphi_1(X,Y,Z) \\ Y' &= \varphi_2(X,Y,Z) \\ Z' &= \varphi_3(X,Y,Z) \end{aligned} \tag{3.22}$$

where $\varphi_i \in \mathrm{Adj}_{n-2}(C)$, $i = 1,2,3$. The following theorem describes the transformation of F under the inverse of the map (3.22).

Theorem 3.3.2. *Let $H_{n-2} \subset \mathrm{Adj}_{n-2}(C)$ be a system of curves of degree $n-2$ intersecting C in $n-2-r$ non-singular points. Let $\varphi_i \in H_{n-2}$, $i = 1,2,3$, are such that they define a birational transformation. Then the transform $G(X',Y',Z')$ of F under the inverse of the map* (3.22) *is an irreducible curve of degree r.*

Using this theorem, if a system of curves intersecting C in $n-4$ points is found, the polynomial F transformed by the inverse of (3.22) is of degree

2. The system of adjoint curves of C of degree $n-2$ intersects C in $n-2$ additional points (cf. table 3.3 on page 70). On this way, a class of $n-2$ points may be computed.

Now, after the first step of Hilbert–Hurwitz algorithm a curve D of degree $n-2$ birationally equivalent to C is obtained. Starting from D, we may compute a system $\mathcal{S}$ of curves intersecting C in $n-4$ points. Choosing curves $\varphi_i \in \mathcal{S}$, $i = 1,2,3$, according to Theorem 3.3.2 there is a birational transformation mapping the defining polynomial F of C to a quadratic form. Hence arriving at a projective conic. See Algorithm 7.

REDUCE TO CONIC(C)

Input: rational curve C

Output: birational map σ and a conic

Description: Reduction of a rational curve to a conic.

1. determine $H_{n-2} := \mathrm{Adj}_{n-2}(C)$
2. compute $n-4$ non-singular points on C
3. pass H_{n-2} through all points determined in previous step obtaining a new system H'_{n-2}
4. choose three curves $\varphi_1, \varphi_2, \varphi_3 \in H'_{n-2}$ inducing a birational transformation Φ as in (3.22)
5. apply Φ^{-1} to C to obtain a curve of degree 2

Algorithm 7:

The correctness of the algorithm follows from Theorem 3.3.2.

In the case $k = \mathbb{Q}$, the problem of deciding whether there is a $\mathbb{Q}$-rational point on a conic amounts to decide solvability of a Diophantine equation. A projective conic over $\mathbb{Q}$ is equivalent to a conic with integral coefficients. A classical result by Legendre yields necessarily and sufficient condition.

Let $m\,R\,n$ denote the fact that m is a square modulo n, i.e. there is an integer x such that $x^2 \equiv m \mod n$.

Theorem 3.3.3. *Let a, b, c be nonzero integers, squarefree, pairwise relatively prime, and not all positive nor all negative. Then*

$$ax^2 + by^2 + cz^2 = 0 \tag{3.23}$$

has a non-trivial solution iff the following conditions are satisfied

(i) $-ab\,R\,c$

(ii) $-ac\,R\,b$

(iii) $-bc\,R\,a$

Proof. See e.g. [IR82]. □

Summarizing, rational points on C may be found by, first, reducing the curve to a conic, and deciding whether there are rational points on it. In the affirmative case, such points are found and using the birational transformation returned by the Algorithm 7 on the preceding page transformed to the original curve. As we already mentioned, this approach is capable to yield not only rational points, but also providing parametrizations.

3.4 Parametrization

In previous sections we considered in detail all necessary subalgorithms needed to determine a parametrization of a curve. Now we assemble all pieces to a parametrization algorithm.

Let C be a absolutely irreducible projective curve given by a homogeneous polynomial $F(X, Y, Z) \in k[X, Y, Z]$ of degree n. We are looking for a parametrization of C if it exists.

In the first step we want to test whether C posesses a parametrization. For this purpose, the Algorithm 4 on page 58 may be applied, provided, reasonable bounds are given. This algorithm may be used to check the rationality over more than one finite fields to increase the probability of detecting

possible non-rationality. If it fails, the parametrization algorithm is started. In case that C is non-rational the process will fail after resolving all singular points. In this step there is already enough information available to compute the genus.

The parametrization algorithm starts by computing adjoint curves of C. This may be done either by fixing the degree A of the adjoint system and using the method described in Section 3.2.1, or by using Algorithm 6 on page 67. In the latter case, the method to minimize the number of additional points described in [SS92] (cf. Section 3.4). If some non-singular points are necessary, the Algorithm 7 on page 74 may be used to find points having their coordinates in a smallest extension of the ground field. In successive steps, the dimension of the system of adjoint curves is lowered until it becomes one.

In the final step, the coordinates of the only intersection of the system of adjoint curves are expressed as rational functions in one parameter.

The above process results in Algorithm 8 on the next page. The correctness was proved in previous sections, the steps 17 and 18 are described in [SW91].

The Algorithm 8 on the facing page follows the classical line in parametrization. Recently, using a basis of the integral closure of $k[C]$, M. van Hoeij designed a new algorithm to compute a parametrization of a curve (see [vH94]). This method determines a rational function τ such that $k(C) = k(\tau)$. Then the coordinates x and y are expressed as rational functions of τ by resultant computation.

PARAMETRIZATION(C)

Input: a rational curve C

Output: parametrization of C

1. [Try to decide whether C has a parametrization]
2. **if** RATIONAL(C)="Not rational" **then**
3. **return** "C is not parametrizable"
4. **end**
5. [Compute adjoints]
6. $A \leftarrow$ ADJOINTS ALGEBRAIC(C)
7. [Determine genus of C using the structure of singular points]
8. **if** GENUS(C)$\neq 0$ **then**
9. **return** "C is not parametrizable"
10. **end**
11. [Reduce the dimension of A to one]
12. **if** a solution of (3.21) with $t = 1$ may easily be found **then**
13. pass A through singular points reducing the dimension to one
14. **else**
15. Determine one simple point on C over a smallest extension of k using REDUCE TO CONIC(C)
16. **end**
17. pass A through additional points determined in previous steps obtaining a pencil A' of dimension 1
18. determine the only intersection $(x(t), y(t))$ of A' and C
19. **return** $(x(t), y(t))$

Algorithm 8:

Chapter 4

Complexity of Parametrization

Parametrization of curves is a complex task requiring a large machinery of symbolic algorithms interlaced in manyfold ways. Especially, multivariate gcd's and resultants are indispensable in this field. They are utilized instead of factorization which is to be avoided if possible at all. However, due to the rapid growth of coefficients during the process of parametrization, in certain cases, factoring of polynomials turns out to be preferable method compared to e.g. subresultant chain computation. Even though factorization of polynomials over rationals or over algebraic number fields runs in polynomial time in the bit-complexity model, these algorithms are inefficient in practice. Factorization is required mainly to maintain algebraic extensions arising in the process of resolution of singularities. In [DD84] it is shown that this problem may be handled by resorting to *dynamic evaluation* where a computation in a domain is performed in the same way as in a field even though there might be some zero divisors. At a step when a zerodivisor is to be possibly inverted a partial factorization of some elements defining extensions is discovered and the computation splits into independent branches. A drawback of this very intuitive method is that the splitting requires deep control over the whole computation possibly imposing strong restrictions on subsequent steps.

The complexity of parametrization using the RAM model with unit cost for field operations has been analyzed in [AB89]. It was shown that the parametrization requires polynomial number of field operations.

Theorem 4.0.1. *A rational algebraic plane curve of degree n can be parametrized in $O(n^6 \log^3 n + n^2 T(n^2))$ where $T(n) = O(n^3 \log^2 n + n^2 \log n \log(1/\varepsilon))$ denotes the time taken to compute all roots of a polynomial of degree n with accuracy ε.*

4.1 Parametrization

In [MSW94], using the RAM model counting binary operations, which is more realistic for analysis of symbolic algorithms, the following theorem was proved.

Theorem 4.1.1. *The worst case complexity for the algorithm PARAMETRIZE ([MSW94]) is*

$$O(n^{26}(n + L_F)^2 + n^5 \log n L_R^2)$$

where n is the degree of the curve, $L_F = \text{length}(||F||_{max})$, L_R is the maximum length of coordinates of simple points returned from the procedure POINTS.

Remark 4.1.2. The above theorem holds under the restriction that all singular points are ordinary. When using towers of fields to represent multiple extensions, the complexity might turn out to be exponential in the size of the input curve. This is due to the non-constant number of additional variables which are introduced in the process of expanding singular points.

Let us now consider some larger subproblems of parametrization which have been analyzed separately. All particular procedures used in geometric parametrization (see Algorithm 8 on page 77) has been thoroughly studied in the literature and their complexity is known.

4.2 Singularities and Neighboring Graphs

Resolution of singular points is one of central parts of all known parametrization algorithms. Many other interesting problems depend on thourough knowledge of their structure. In [Tei90] an algorithm for resolution of a singular point represented by power series running in polynomial time in the size of the singularity is proposed. The model used to estimate the complexity is based on field operations. This is, however, a strong simplification, and may invalidate many results. When using exact arithmetic in the field of rational numbers, the length of intermediate results may be much larger than the initial data. A single computation of a pseudoremainder of polynomials over $\mathbb{Q}$ dramatically blows up coefficients. For this reason, counting field operations is not an appropriate measure to estimate the true complexity of symbolic algorithms over infinite fields.

In [Koz94] an algorithm based on a Puiseux series for resolution of singularities of plane curves is presented. This algorithm requires polynomial number of bit operation to resolve all singular points.

Another estimate for the number of bit operation reqired to compute all distinct singularities of a plane curve is given in [MSW94]. This approach, based on computation of the neighborhood graph by utilizing quadratic transformations, is of exponential complexity when infinitely near singular points are present.

Theorem 4.2.1. *Let C be a irreducible projective curve given by a homogeneous polynomial F of degree n. Let $L_F := \text{length}(\|F\|_{max})$. The worst case complexity of the algorithm for computing all singularities is $O(n^{12}(n \log n + L_F)^2)$.*

4.3 Rational Points

In most cases, parametrization algorithms require finding at least one non-singular point on the curve. The extension in which coordinates of this

point are lying heavily influence the coefficients of the final parametrization. In [SW93] an algorithm is presented to compute such point over the smallest extension of the ground field. The computational complexity of this procedure has not been studied yet.

Appendix A

Adjoint Curves – Algebraic Approach

Computing Adjoint Curves (An Algebraic Approach)

Michal Mňuk*
Research Institute for Symbolic Computation
Linz, Austria
mmnuk@risc.uni-linz.ac.at

7 November 1995

Abstract

This paper describes an algebraic approach to computing a system of adjoint curves to a given absolutely irreducible plane algebraic curve. The proposed algorithm utilizes integral closure of the coordinate ring rather than expanding neighborhood graphs by quadratic transformation.

1 Introduction

Adjoint curves (curves passing through all singularities of a given curve with a "high enough" multiplicity) are important objects in various areas of mathematics – number theory, coding theory, algebraic geometry, etc. This paper aims at a solution of the problem of computing the system of adjoint curves for a given absolutely irreducible plane curve (see e.g. [4], [2], [9]).

The inherent tight binding of this problem to the structure of singularities makes it very difficult to avoid explicit computation of the non-singular model. This may be done either by using geometry and expanding the neighborhood graph of the curve, or by using algebra and computing the normalization of the coordinate ring. The computation of the non-singular model turns out to be an extraordinarily laborious task. The expansion of the neighborhood graph may quickly prove to be prohibitively complicated, at least in characteristic zero (cf. [3]). The reason for this seems to be hidden in the imperfect exploitation of the structure of singularities of the quadratic transformation which is used to compute the neighborhood graph. On the other hand, the normalization technique may circumvent some difficulties of the

*This work was partially supported by the FWF under the project POSSO, Nr. P9181-TEC.

expansion approach. There is a strong hope, that it may be refined to a feasible and powerful method to obtain the non-singular model.

In this paper we make use the structure of the coordinate ring and its integral closure in the function field to get a description of the non-singular model. The adjoint curves may then be extracted from this data by solving a system of linear equations. The principles of this approach are based on the theory of Dedekind domains. Even though only a little is known about the comparison of above methods, there is a strong hope that this approach will introduce new and/or clearer structures, open alternative views, and make the problem more comprehensible.

The paper contains three basic parts. In the Section 2 we briefly sketch the algorithm for computing adjoint curve. The Section 3.1 recalls some basic definitions and theorems from the theory of Dedekind domains. The mathematical background for the proof of correctness of the main algorithm is collected in the Section 3.3. Finally, in the Section 4 we give a detailed description of the main algorithm.

2 Main result

In this section we present a sketch of an algorithm for determining all adjoint curves using information extracted from the integral closure of the coordinate ring of a plane curve.

Let us now briefly describe the ideas behind the algorithm. We will give here only a very coarse description of underlying concepts. We refer to the Section 3 for detailed exposition.

Throughout this paper, let $F(X,Y)$ be an irreducible bivariate polynomial describing an affine plane curve C. Note that since all notions are of local nature, the results easily extend to projective curves.

Let $k[C] = k[X,Y]/(F)$ denote the coordinate ring of C, and $k(C)$ the field of rational functions. Let $\mathrm{Adj}(C)$ be the system of adjoint curves to C, $\mathfrak{C} = \mathfrak{C}_{\overline{k[C]}|k[C]}$ the *conductor* of $\overline{k[C]}$ over $k[C]$, and $\mathcal{C}$ the *complementary module* of $\overline{k[C]}$ over the polynomial ring $k[X]$ (for definitions of these notions we refer to Section 3.1 or to [11]).

Theorem 2.1. *The notations being as above. Then*

$$\mathrm{Adj}(C) = \frac{\partial F}{\partial Y}\mathfrak{D}^{-1} = \frac{\partial F}{\partial Y}\mathcal{C}.$$

This theorem provides a useful knowledge to give a first sketch of a procedure (see Algorithm 1 on the following page) which will be worked out in more detail later.

The rest of this paper deals with the proof of the correctness of the Algorithms 1. Following sections will introduce all necessary definitions and

ADJOINT SYSTEM(C)
Input: absolutely irreducible plane curve C given by $F(X,Y)$
Output: basis of Adj(C) as a finite $k[x]$ module

1. compute a basis of integral closure $\overline{k[C]}$ of $k[C]$ in $k(C)$
2. compute a basis $\{\eta_i\}_{i=1}^n$ of the complementary module $\mathcal{C}$ of $\overline{k[C]}$ with respect to $k[x]$
3. **return** $\{\frac{\partial F}{\partial Y}\eta_i\}_{i=1}^n$

Algorithm 1: Adjoint system - sketch

theorems from the theory of Dedekind domains needed in the proof. At the end we present a refined version of the above algorithm providing details of computations of bases in steps 2 and 3.

3 Dedekind domains and singular points on plane curves

In this section we provide the basics of the theory of Dedekind domains as far as they are used to prove the correctness of the above algorithm. For more details and proofs we refer e.g. to [11] and [1].

3.1 Basic notions of Dedekind domains

Let $F(X,Y)$ be a bivariate polynomial over a field k. Let x and y be images of X and Y in $k[C]$, respectively. We consider $F(X,Y)$ as a univariate polynomial $G(Y)$ in Y over $k(X)$. Assume $G(Y)$ is separable. Then $\{x\}$ is a separating transcendence basis of $k(x,y)|k$, i.e. any element $z \in k(x,y)$ is a root of a separable polynomial over $k(x)$.

Due to the Normalization Lemma (see e.g. [11], Ch. 5, Thm. 8) we may assume that F is monic in Y, more precisely, there exists a change of coordinates τ of the affine plane $\mathbb{A}^2(k)$ such that $k[x',y'] = k[\tau(x),\tau(y)]$ is integral over $k[x']$. Moreover $k(x',y')$ is separable over $k(x')$. Thus $y \in k[C]$ is an integral element over the subring $k[x]$ and the integral closure of $k[x]$ in $k(x,y)$ coincides with the integral closure $\overline{k[C]}$ of $k[C]$ in $k(x,y)$. The coordinate ring $k[C]$ is integrally closed in $k(C)$ if and only if C is a non-singular curve (see e.g. [6]).

The integral closure of the coordinate ring is the basic piece of data we need to extract all necessary information to compute the system of adjoint curves. The following theorem is very essential from the algorithmic point of view. It guarantees the representability of the integral closure of certain types of integral domains as a module in terms of a finite number of basis elements.

Theorem 3.1. *Let R be a finitely generated integral domain over a field k, and let K' be a finite algebraic extension of the quotient field of R. Then the integral closure R' of R in K' is a finitely generated integral domain, and is a finite R-module.*

Proof. See [11], Ch. V, §4. □

Note that coordinate rings of curves and their quotient fields obviously satisfy the prerequisites of the theorem.

Let for the rest of this section R, R', and K, K' denote arbitrary rings and fields, respectively. The notion of an ideal of a ring may be extended to a fractional ideal to allow to impose the group structure onto the set of ideals.

Definition 3.2. Let R be an integral domain and K its quotient field. An R-submodule $\mathfrak{a}$ of K is called a *fractional ideal of* R if there is some $d \neq 0$, $d \in R$, such that $\mathfrak{a} \subset \frac{1}{d}R$.

Remark 3.3.

1. It is easy to see that if $\mathfrak{a}$ is a fractional ideal of R then there is an ordinary ideal $\mathfrak{b} \subset R$ and a non-zero element $d \in R$ with $\mathfrak{a} = \frac{1}{d}\mathfrak{b}$.
2. Let $\mathfrak{a}$ be a fractional ideal of an integral domain R. We define $(R : \mathfrak{a}) := \{z \in K \mid z\mathfrak{a} \subset R\}$. This set is again a fractional ideal.
3. A fractional ideal $\mathfrak{a}$ of R is said to be *invertible* if $\mathfrak{a}\,(R : \mathfrak{a}) = R$.

The nice property of some rings to permit unique factorization into prime elements can not, in general, be retained when passing to extensions. However, in numerous cases unique factorization of ideals into primes is still possible. In this context, the notion of a Dedekind domain plays a central role.

Definition 3.4. A ring R is said to be a *Dedekind domain* if it is an integral domain and if every ideal in R is a product of prime ideals.

Dedekind domains bear a number of interesting properties.

Remark 3.5.

1. In a Dedekind domain, every fractional ideal invertible.
2. The integral closure of a Dedekind domain in a finite separable extension of its quotient field is again a Dedekind domain.

The proofs of these claims may be found in most books on commutative algebra (e.g. [11]).

In the sequel we will define two important fractional ideals – the *conductor* and the *different*. They are closely related to each other. The different behaves like the reciprocal of the conductor.

Definition 3.6. Let S and T be two rings, $S \subset T$. The *conductor* $\mathfrak{C}_{T|S}$ of S in T is defined as

$$\mathfrak{C} := \{s \in S \mid sT \subset S\}.$$

Remark 3.7. The conductor of S in T is the largest ideal of S which stays an ideal in T.

We proceed to definition of the different.

Definition 3.8. Let R be an integrally closed ring, K its quotient field, K' a finite separable (and hence simple) extension of K, and R' an integral extension of R admitting K' as quotient field. Let $T_{K'|K} : K' \to K$ denote the trace of $K'|K$. The set

$$\mathcal{C}_{R'|R} := \{z \in K' \mid T_{K'|K}(zR') \subset R\}$$

is called the *complementary module of R' with respect to R.*

Remark 3.9. The complementary module is a fractional ideal of R' (see [11]).

Definition 3.10. Let $\mathcal{C}_{R'|R}$ be the complementary module as above. The set

$$\mathfrak{D}_{R'|R} := (R' : \mathcal{C}_{R'|R}) = \{z \in K' \mid z\mathcal{C}_{R'|R} \subset R'\}$$

is called the *different* of R' over R.

Let R be an integrally closed ring and K its quotient field. Let K' be a finite separable extension of K and R' the integral closure of R in K'. The Remark 3.5 shows that R' is again a Dedekind domain. We establish now an important connection between the conductor and the different.

Theorem 3.11. *With above notations, let y be an element of R' such that $K' = K(y)$ and let $F(T)$ be the minimal polynomial of y over K. Then we have*

$$F'(y)R' = \mathfrak{C}_{R'|R[y]}\mathfrak{D}_{R'|R}$$

where F' denotes the derivative of F.

Proof. See [11], Ch. V, §11. □

Corollary 3.12. *It holds*

$$F'(y)\mathcal{C}_{R'|R} = \mathfrak{C}_{R'|R[y]}$$

Proof. The assertion follows from the fact that the different is a fractional ideal of R' and that in a Dedekind domain every fractional ideal is invertible. □

Remark 3.13. Note that $F'(y)$ is always in $\mathfrak{C}_{R'|R[y]}$.

3.2 Computing a basis of the conductor

In the previous section we summarized basic properties of Dedekind domains. The conductor was in the center of our observation as it will turn out to be closely related to the system of adjoint curves. In this section we describe a way to compute a basis of the conductor in terms of a basis of the integral closure.

Let F, R, R', K, K' be as in the Theorem 3.11. Observing that the integral closure R' is a finite R-module and that the complementary module is a fractional ideal of R', we may determine a finite basis of $\mathcal{C}_{R'|R}$ thus obtaining a finite basis for the conductor using the Corollary 3.12. This yields an algorithmic way of describing the conductor of $R[y]$ in R'.

A basis of the complementary module may be computed as follows. Let $\{e_i\}_{i=1}^n$ be an integral basis of R' over R (hence $K' = \sum_i Ke_i$). Consider the following matrix $A := (T_{K'|K}(e_ie_j))_{i,j=1}^n$. Since $K'|K$ is a separable extension, the matrix A is invertible. Then the linear system

$$\sum_{j=1}^{n} a_{lj} T_{K'|K}(e_ie_j) = \delta_{il}, \quad i = 1, \ldots, n \tag{1}$$

has a unique solution $(a_{l1}, \ldots, a_{ln})$ over K for any l (δ_{il} denotes the Kronecker symbol). Now let

$$\eta_i := \sum_{j=1}^{n} a_{ji} e_j. \tag{2}$$

Then η_i is another basis of $K'|K$. For

$$\sum_j T_{K'|K}(e_ie_j)\eta_j = \sum_{jk} a_{lj} T_{K'|K}(e_ie_j)e_l = \sum_l \delta_{il}e_l = e_i.$$

Moreover, from (1) we have

$$T_{K'|K}(\eta_i e_j) = \delta_{ij}. \tag{3}$$

Now let $z' = \sum_i \zeta_i\eta_i \in K'$ be an element of K', and $r' = \sum_j \alpha_j e_j \in R'$. Then

$$T_{K'|K}(z'r') = \sum_{ij} \zeta_i\alpha_j\delta_{ij} = \sum_i \zeta_i\alpha_i. \tag{4}$$

Now we claim that $\{\eta_i\}_i$ is a basis of $\mathcal{C}_{R'|R}$ as an R-module. Assume, $z' \in K'$ and $T_{K'|K}(z'R') \subset K$. Setting successively $\alpha_1 = 0, \ldots, \alpha_i = 1, \ldots, \alpha_n = 0$ in (4) we get $\zeta_i \in R$ for all i. On the other hand, if $\zeta_i \in R$ for all i, then $T_{K'|K}(z'R') \subset R$. Thus

$$\mathcal{C}_{R'|R} = \sum_i R\eta_i. \tag{5}$$

The equation (5) together with Corollary 3.12 yields a complete description of the conductor of $R[y]$ in R'. In the next section we will relate this object to the system of adjoint curves hence providing a new possibility to determine the adjoints.

3.3 Singular points and the non-singular model

This section introduces some basic notions from the algebraic geometry of plane curves. We will mainly focus on the algebraic way of the description of singular points and other related notions. For detailed description of notions introduced in this section we refer to [6], [1], or [10].

First, we recall the concept of blowing-up an affine space. Let O be an arbitrary point of the affine plane $\mathbb{A}^2$. Since translations map $\mathbb{A}^2$ isomorphically, we may assume $O = (0,0)$. Let ψ be the blowup of $\mathbb{A}^2$ centered at O:

$$\begin{aligned} \psi : \mathbb{A}^2 &\longrightarrow \mathbb{A}^2 \\ (x,z) &\longmapsto (x,xz) \end{aligned} \tag{6}$$

Let C be an absolutely irreducible plane curve given by a polynomial $F(X,Y)$ defined over a separable field k such that X is not a tangent to C at any singular point. The latter condition may be satisfied by a suitable change of coordinates. Using the Normalization Lemma ([11]) we may assume that F is monic in Y, in other words, the coordinate ring $k[C]$ is integral over the ring of univariate polynomials $k[x]$. For an arbitrary point $P \in C$ (we can assume $P = (0,0)$) we may consider the action of ψ centered at P on points of C. Let $C' := \psi^{-1}(C)$ denote the blowup of C centered at P, and σ be the restriction of ψ to C'. Note that if P is a non-singular point on C, the map σ yields an isomorphism of C' to C. However, if P is singular, there will be at least two pre-images of P on C', and σ defines just a birational correspondence between C and C'. The pre-images are called *points in the first neighborhood* of P. If some of them are singular, the structure of their singularities is simpler than that of P. There is a chain of blowups

$$X = C_k \xrightarrow{\sigma_k} C_{k-1} \xrightarrow{\sigma_{k-1}} \dots \xrightarrow{\sigma_1} C_1 \xrightarrow{\sigma_0} C_0 = C$$

such that $\sigma_i : C_{i+1} \to C_i$ is a birational map, and X, the *non-singular model* of C, has no singular points. The set $\sigma_{i-1}^{-1} \circ \sigma_{i-2}^{-1} \circ \cdots \circ \sigma_0^{-1}(P)$ is called the i-th neighborhood of P. The collection of all neighborhoods forms a *neighborhood graph* (see [1]) completely describing the nature of all points on C. Note that only singular points have non-trivial neighborhoods. The singularities on C are called *distinct singular points* while those in their neighborhoods are called *infinitely near*.

All properties studied in this paper are of local nature, i.e. they remain the same if the curve is replaced by a neighborhood of a point. Since

$$k[C] = \bigcap_{P' \in C} O_{P'}(C), \tag{7}$$

where $O_{P'}(C)$ denotes the local ring of C at P', we may obtain facts about $k[C]$ by studying local rings $O_{P'}(C)$ for any point $P' \in C$. The equation (7) enables

us to recover properties of $k[C]$ from $O_{P'}(C)$. Therefore we fix an affine neighborhood $W \subset C$ of P such that P is the only singular point in W. This neighborhood induces an affine set $W' \subset C'$ containing all points from the first neighborhood of P. We may shrink W such that W' contains no singularities of C' except possibly $\sigma^{-1}(P)$.

The regular map σ induces a homomorphism of $k[C]$ into $k[C']$:

$$\begin{aligned} \sigma^* : k[C] &\longrightarrow k[C'] \\ g &\longmapsto g \circ \sigma \end{aligned} \tag{8}$$

Let us have a closer look to the action of σ^* on $k[C]$. Let $g \in k[C]$ and $s = m_P(g)$. Then

$$\sigma^*(g) = x^s g', \tag{9}$$

$g' \in k[C']$. For, let $G(X,Y) = G_s(X,Y) + G_{s+1}(X,Y) + \cdots + G_m(X,Y)$, where $G_i(X,Y)$ are forms of degree i, be a polynomial corresponding to g. Then the image of g' is given by $G'(X,Z) = X^s(G_s(1,Z) + XG_{s+1}(1,Z) + \cdots + X^{m-s}G_m(1,Z)$. We call $\sigma^*(g)$ the *total quadratic transform* of g, and g' the *proper quadratic transform* of g. From (9) we see that if g passes through the origin with multiplicity s, then the total quadratic transform of g passes through any points in the first neighborhood of P with multiplicity at least s. However, the proper quadratic transform need not pass through those points at all. The map σ^* may be extended to $\sigma^* : k[X] \to k[C]$.

Let now D be a plane curve given by a polynomial G, and g be the image of G in $k[C]$. We extend the notion of the multiplicity of a curve at a point to arbitrary neighborhood points. We say that D passes through a point $Q \in C'$ in the first neighborhood of P with multiplicity s if the multiplicity of the proper quadratic transform of g at Q is s. Points in i-th neighborhood are handled analogously. Curves having a *high enough* multiplicity at all neighborhood points bear a number of important properties.

Definition 3.14. Let C be an irreducible plane curve. Let P be a singular point (distinct or infinitely near) of C of multiplicity $m_P(C)$. A curve D is called an *adjoint curve* to C at P if

$$m_P(D) \geq m_P(C) - 1. \tag{10}$$

The set of curves which are adjoint to C at P is denoted by $\mathrm{Adj}_P(C)$. If (10) holds for all singular points P on C (distinct or infinitely near), and hence for all P, D is called an *adjoint curve* to C. The set of adjoint curves to C is denoted by $\mathrm{Adj}(C)$.

Remark 3.15. When referring to functional properties of adjoint curves, we use the notation $\mathrm{Adj}(C)$ also for the ideal of $k[C]$ generated by images of polynomials which define adjoint curves. This identification does not cause any confusion.

For the sake of simplicity we replace C by an affine neighborhood of P, passing from $k[C]$ to $O_P(C)$, such that this neighborhood does not contain any other singular point except P. Hence C' will be replaced by the inverse image of this neighborhood which is again affine. Local results may then be easily globalized to $k[C]$ using (7).

Let $\sigma^{-1}(P) = \{P_1, \ldots, P_{r'}\}$ be points in the first neighborhood of P. Then we say that P_i lies *above* P and denote this fact by $P_i \succ P$. This notation naturally extends to points in arbitrary neighborhoods of P. In the sequel, we show that the local ring of a point $Q \succ P$ is integral over $O_P(C)$.

Proposition 3.16. *There is an affine neighborhood W of P on C such that $W' = \sigma^{-1}(W)$ is an affine open subvariety of C', $\sigma(W') = W$, $k[W']$ is integral over $k[W]$, and $x^{r-1}k[W'] \subset k[W]$.*

Proof. Let $F = \sum_{i+j\geq r} a_{ij}X^iY^j$. Consider the neighborhood of P defined by the image h of $H(Y) = Y^{-r}F(0,Y) = \sum_{j\geq r} a_{0j}Y^{j-r}$ in $k[C]$. We set $W = \{Q \in C \mid h(Q) \neq 0\}$. Since X is not a tangent to C at P, $H(0,0) = 1$ and $P \in W$. Then $W' := \sigma^{-1}(W)$ is affine neighborhood on C' containing all points in the first neighborhood of P.

To prove that $k[W'] = k[W][z]$ is integral over $k[W]$, observe that

$$F'(x,z) = \sum a_{ij}x^{i+j-r}z^j = \sum a_{ij}y^{i+j-r}z^{r-i}. \tag{11}$$

The leading coefficient of this polynomial is h which does not vanish at any point of W'. Hence h is a unit in $k[W']$, and 11 yields the desired integral dependence of z on $k[W]$. The last assertion follows from the fact that $x^{r-1}z^i = x^{r-1} * \frac{y^i}{x^i} = x^{r-i-1}y^i$ for $0 \leq i \leq r-1$. □

Corollary 3.17. *Let S be a finite set of points in $\mathbb{A}^2$. The neighborhood W in the Proposition 3.16 may be chosen such that is does not contain any point from S.*

Proof. For any $Q \in S$ consider a line L_Q passing through Q and not through any other point of S. Then replace h in the proposition by $h\prod_{Q\in S} L_Q$. □

The relations between the original curve C and C' are reflected in the relations of respective local rings. Since the blowup is an isomorphism everywhere except at P, local rings $O_Q(C')$ of points $Q \in C'$ different from any P_i ($P_i \in \sigma^{-1}(P)$) are isomorphic to the corresponding local rings $O_{\sigma(Q)}(C)$ on C. Note that we are considering only a neighborhood of P devoid of singularities other than P. Differences arise between local rings of points on C' lying above P. If $g \in O_P(C)$, then obviously g is regular at all P_i on C' lying above P. Hence we have an embedding

$$O_P(C) \hookrightarrow \bigcap_{P_i\in\sigma^{-1}(P)} O_{P_i}(C').$$

The Proposition 3.16 allows us to describe this relationship precisely.

Corollary 3.18. *It holds*

(i)

$$\bigcap_{P_i \in \sigma^{-1}(P)} O_{P_i}(C') \quad \textit{is integral over} \quad O_P(C).$$

(ii)

$$\overline{O_P(C)} = \bigcap_{Q \succ P} O_Q(X)$$

Proof. Let $g \in \bigcap_{P_i \in \sigma^{-1}(P)} O_{P_i}(C')$, i.e. g is regular at all P_i's. Let $\mathcal{P}$ be the set of poles of g on C'. This set is algebraic, and hence finite. We may thus find a neighborhood W of P on C such that W' does not contain any pole of g, i.e. $g \in k[W']$. This means that g is integral over $k[W]$, and hence over $O_P(W)$ since $O_P(C) \supset k[W]$. The fact $O_P(W) = O_P(C)$ concludes the proof of the first assertion. A proof of the second fact may be found in [7], Chapter III. □

Remark 3.19. Note that the local rings $O_Q(X)$ are discrete valuation rings, i.e. noetherian, integrally closed, and the maximal ideal is principal. Hence each $Q \in X$ may be assigned a valuation ord_Q^X of $O_Q(X)$. This valuation naturally extends to the function field $k(C) = k(X)$.

3.4 Adjoint curves and the conductor

In this section we prove that the adjoint curves are precisely those in the conductor of the coordinate ring in its closure. The following lemma will be used in the proof of the theorem. Its proof was greatly inspired by ideas of J. Schicho ([5]).

Lemma 3.20. *Let C be an irreducible plane curve defined by a polynomial $F \in k[X,Y]$, $F = F(X,Y)_r + F(X,Y)_{r+1} + \cdots + F(X,Y)_n$, and P a point on it. Let C' be the blowup of C centered at the origin, and $\{P_1, \ldots, P_{r'}\}$ be points in the first neighborhood of P. For any $g \in k[C]$ such that*

$$g \in \mathfrak{C}_{\bigcap_{i=1}^{r'} O_{P_i}(C') | O_P(C)}$$

there is

$$g \in \mathfrak{m}^{r-1}$$

where $\mathfrak{m}$ is the maximal ideal of $O_P(C)$.

Proof. Let $\mathcal{M} = \cap_{i=1}^{r'} O_{P_i}(C')$. We see that $y/x \in \mathcal{M}$. Hence $g\frac{y}{x} \in O_P(C)$, and there is $\alpha \in O_P(C)$ such that

$$gy - x\alpha = 0.$$

Let G, X, Y, and A be pre-images of g, x, y, and α, resp., under the map $k[X,Y]_{(X,Y)} \to O_P(C)$. Let $\mathfrak{M}$ be the maximal ideal in $k[X,Y]_{(X,Y)}$. Then

$$GY - XA \in \mathfrak{M}^r. \tag{12}$$

Now let $G(X,Y) = G_k(X,Y) + \cdots + G_m(X,Y)$ where $G_i(X,Y)$ are forms of degree i. Assume that at least one $G_l(X,Y)$, where $k \le l < r$, is not identically zero, and let

$$GY - XA = \sum_{k \le i+j} \gamma_{ij} X^i Y^j. \tag{13}$$

From (12) we have

$$\sum_{k \le i+j < r} \gamma_{ij} X^i Y^j = 0. \tag{14}$$

This is impossible since otherwise we would have an algebraic dependence of y upon $k[x]$ of degree less than $n = \deg(F)$. Hence the coefficients of GY at monomials of degree at most $r-1$ are zero. The assertion follows then immediately. □

Theorem 3.21. *Let C be an absolutely irreducible plane curve. Then*

$$\mathrm{Adj}(C) = \mathfrak{C}_{\overline{k[C]}|k[C]} \tag{15}$$

Proof. Referring to the discussion about connections between local and global properties in Section 3.3 we prove $\mathrm{Adj}_P(C) = \mathfrak{C}_{\overline{O_P(C)}|O_P(C)}$. The theorem follows then using the equation (7).

First, let D be an adjoint curve to C at P given by a polynomial $G(X,Y)$. Let g be the image of G in $k[C]$. We have to show that

$$g \in \mathfrak{C}_{\overline{O_P(C)}|O_P(C)}.$$

The claim will be proved by induction on the depth N of the neighborhood tree rooted in P. If $N = 0$, i.e. P is a non-singular point, then the local ring $O_P(C)$ is integrally closed. Hence (3.4) is trivially fulfilled. Let C be a curve having the neighborhood graph of depth $N+1$. Let $\sigma^{-1}(P) := \{P_1, \ldots, P_{r'}\}$ be the first neighborhood of P. Now G passes through P with multiplicity at least $r-1$, where $r = \mathrm{m}_P(C)$. Then $G(X,Y) = \sum_{i+j \ge r-1} g_{ij} X^i Y^j$, $g_{ij} \in k$. For $1 \le k \le r'$ consider the image $\sigma^*(g) \in O_{P_k}(C')$. From (9) we have

$$g' = \sigma^*(g) = x^{r-1} g'', \; g'' \in O_{P_k}(C'). \tag{16}$$

Moreover, g'' was assumed to be adjoint at all points $Q \succ P_k$, i.e.

$$g'' \in \bigcap_{k=1}^{r'} O_{P_k}(C') \tag{17}$$

where C' is the blowup of C centered at P. Now from (16) and the Proposition 3.16 we have

$$g' \in O_P(C). \tag{18}$$

On the other hand, let us denote the i-th neighborhood of P by $\mathcal{N}_i$ ($\mathcal{N}_0 = \{P\}$). We will show by induction that if

$$g \in \mathfrak{C}_{\overline{O_P(C)}|O_P(C)},$$

then for any $Q \in \mathcal{N} = \cup_{i=0}^{N} \mathcal{N}_i$

$$m_Q(g) \geq r_Q - 1$$

where r_Q is the multiplicity of the corresponding blowup of C at Q.

If $Q \in \mathcal{N}_N$, i.e. Q lies on the non-singular model of C, then the assertion is trivial since Q is non-singular. Assume that it holds for any $Q \in \cup_{i=1}^{N} \mathcal{N}_i$. Let

$$g \in \mathfrak{C}_{\overline{O_P(C)}|O_P(C)}. \tag{19}$$

We have

$$\bigcap_{P_i \in \mathcal{N}_1} O_{P_i}(C') \subset \overline{O_P(C)}.$$

From (19) we conclude $g(\cap O_{P_i}(C')) \subset O_P(C)$. This implies

$$g \in \mathfrak{C}_{\cap O_{P_i}(C')|O_P(C)}.$$

The assertion then follows from the Lemma 3.20. □

4 The refined algorithm

The connection between the ideal of adjoint curves and the conductor established in previous sections enables us to refine the Algorithm 1 which was sketched in the Section 2.

Let C be an absolutely irreducible plane curve given by a polynomial $F(X,Y) \in k[X,Y]$. Let x and y be images of X and Y in $k[C]$, respectively. Let us denote by R the ring $k[x]$ and by R' its integral closure in the function field $k(C)$.

In the first step, the algorithm determines the integral closure R' of R in $k(C)$. The Theorem 3.1 shows that this can be done effectively by providing a finite basis of R' as a finite R-module. Note, that there is an computationally feasible solution to this problem (see [8]. The next step computes a basis of the complementary module $\mathcal{C}_{R'|R}$ of R' with respect to R. Finally, having its basis, it is only a matter of multiplying it by the Y-derivative of F to obtain a basis of the system of adjoint curves.

ADJOINT SYSTEM(C)
Input: absolutely irreducible plane curve C given by $F(X,Y)$
Output: basis of Adj(C) as finite R module

1. determine a basis $\{e_i\}_{i=1}^n$ of R' as a R-module
2. **for** $j \leftarrow 1$ **to** n **do**
3. solve the linear system

$$\delta_{ij} = \sum_{k=1}^{n} a_{ik} T_{K'|K}(e_k e_j), \quad i = 1, \ldots, n$$

for a_{ij} over K
4. **end**
5. compute $\{\eta_i := \sum_{j=1}^n a_{ij} e_j\}_{i=1}^n$
6. **return** $\{\frac{\partial F}{\partial Y}(x,y)\,\eta_i\}_{i=1}^n$

Algorithm 2: Adjoint system – full version

Acknowledgments

I would like to express deep thanks to my colleges J. Schicho and E. Volcheck who spent hours for fruitful discussions about the topic of this paper.

References

[1] William Fulton. *Algebraic Curves*. Addison–Wesley, 1989.

[2] Gaétan Haché and Dominique Le Brigand. Effective constructions of algebraic geometry codes. To be published.

[3] Michal Mňuk, J. Rafael Sendra, and Franz Winkler. On the complexity of parametrizing curves. Technical Report 94–45, Research Institute for Symbolic Computation, 1994.

[4] Despina Polemi, Carlos Moreno, and Oscar Moreno. Search and construction of good a.g. goppa codes. Preprint, 1992.

[5] Josef Schicho. Adjoints and conductors. Private communication, 1995.

[6] Igor A. Shafarevich. *Basic Algebraic Geometry*, volume 1. Springer Verlag, second edition, 1994.

[7] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer Verlag, 1993.

[8] Mark van Hoeij. An algorithm for computing an integral basis in an algebraic function field. Description of the IntBasis package contained in the Maple share library.

[9] Mark van Hoeij. Computing parametrizations of rational algebraic curves. In *ISSAC*, 1994.

[10] Robert J. Walker. *Algebraic Curves*. Princeton University Press, 1950.

[11] Oscar Zariski and Pierre Samuel. *Commutative Algebra*, volume 1. Springer Verlag, 1975.

Appendix B

Complexity

On the Complexity of Parametrizing Curves

Michal Mňuk
Research Institute for Symbolic Computation,
Johannes-Kepler University, Linz, Austria*

J. Rafael Sendra
Departamento de Matemáticas,
Universidad de Alcalá, Spain†

Franz Winkler
Research Institute for Symbolic Computation,
Johannes-Kepler University, Linz, Austria‡

1 December 1995

Abstract

Given a rational algebraic plane curve C in implicit representation we consider the bit complexity of describing C by parametric equations. Estimates for subalgorithms for computing the standard decomposition of singularities and the genus are also abtained.

1 Introduction

Rational parametrization of algebraic curves is one of the basic computational problems in constructive algebraic geometry. A completely symbolic approach to this problem has been published in [11] and it has been implemented in the program system CASA ([4, 9]). The main goal of this paper is to give a thorough theoretical worst case complexity analysis of this parametrization algorithm.

In the first part we limit the complexity analysis to the case in which the curve has rational coefficients and only ordinary singularities, i.e. no blowing up is necessary to resolve them. In the Section 4 we discuss questions related to the presence of neighboring points.

*Supported by the "Fonds zur Förderung der wissenschaftlichen Forschung" under project number P8573-PHY and the Grant of Slovak Academy of Sciences No. 88.

†Partially supported by DGICYT A.I. Spain–Austria HU-007 and ÖAD Int. Akt. 16.

‡Supported by the "Fonds zur Förderung der wissenschaftlichen Forschung" under project number P8573-PHY

Since the main steps of the parametrization algorithm consist of solving systems of algebraic equations in two variables, solving linear systems, and computing gcd's and resultants of polynomials of two or three variables, it is easy to see that the complexity is polynomial in the size of the input. In this paper we give a precise analysis in terms of bit complexity of the parametrization problem and some of its important subproblems.

Section 2 contains a summary of complexity bounds for basic integer and polynomial arithmetic algorithms (gcd, polynomial remainder sequences, etc.). Section 3 is dedicated to the computing time analysis of the parametrization problem. In Subsection 3.1, description and analysis of an algorithm for the decomposition of the set of singularities is given. Subsection 3.2 is devoted to the main algorithm for parametrization. A brief description of and a detailed analysis in terms of bit complexity are provided. In order to obtain tighter bounds for special cases we distinguish whether coordinates of all singularities are rational or not. In Subsections 3.2.1 and 3.2.2 we give the analysis for both cases. Section 4 discusses the complexity of algorithms designed so far in the case when the input curve possesses neighboring singularities.

2 Complexity of integer and polynomial arithmetic

In this section we briefly recall complexity bounds for basic algorithms for integers and polynomials. For some of them we give also short proofs to make the methods used here more transparent. Throughout this paper we use classical algorithms for both integers and polynomials. Even though this will not yield the best possible estimate of the complexity the main goal of this paper is to reveal computationally expensive parts of the parametrization algorithm. For detailed description of algorithms in this section we refer to [6, 7], etc. For elementary introduction the reader may refer to [2].

2.1 Integer arithmetic

The computational complexity of operations over integers is measured in terms of length of input, i.e. the number of bits needed to store the input into the memory. By length(a), $a \in \mathbb{Z}$ we denote $\lfloor \log_2(|a|) \rfloor + 2$ (we take the most significant bit as sign bit).

Remark 2.1. Throughout this paper all logarithms are taken to the base 2.

The following proposition summarizes classical results on integer arithmetic.

Proposition 2.2. *Let $a, b \in \mathbb{Z}$ and l_a, l_b be the length of a and b, respectively. Then it holds:*

(i) *The worst case complexity for adding a and b is* $O(\max\{l_a, l_b\})$ *and*

$$\text{length}(a+b) = O(\max\{l_a, l_b\})$$

(ii) *The worst case complexity for multiplying a and b is* $O(l_a l_b)$ *and*

$$\text{length}(ab) = O(l_a + l_b)$$

(iii) *The worst case complexity for computing* a^n *is* $O(n \log n l_a^2)$.

(iv) *The worst case complexity for computing* $a \mod b$ $(|a| > |b|)$ *is* $O(l_b(l_a - l_b + 1))$.

(v) *The worst case complexity for computing the greatest common divisor of a and b is* $O(l_a(l_b - l_c + 1))$, *where* l_c *is the length of the gcd.*

2.2 Polynomial arithmetic

Before we start to give complexity analysis of polynomial arithmetic we need to define some measures for the size of polynomials. Let $a = a_n x_r^n + \cdots + a_0$ be a multivariate polynomial in $\mathbb{Z}[x_1, \ldots, x_{r-1}][x_r]$ with $a_i \in \mathbb{Z}[x_1, \ldots, x_{r-1}]$. The complexity of various operations with a is determined by the degree of a (regarded as a univariate polynomial in x_r) and by the size of its coefficients. In the sequel, we recall three well-known notions of a norm. In order to obtain an estimate of the size of coefficients we define the *max-norm* of a by

$$||a||_{\max} := \max_{i=0,\ldots,n} \{||a_i||_{\max}\}.$$

However this norm does not comprise any information on the degree of the polynomial. Hence numerous complexity estimates are given in terms of the *1-norm* defined by

$$||a||_1 := \sum_{i=0}^{n} ||a_i||_1$$

or the *2-norm* defined by

$$||a||_2 := \left(\sum_{i=0}^{n} ||a_i||_2^2\right)^{1/2}.$$

For $a \in \mathbb{Z}$ we define

$$||a||_{\max} = ||a||_1 = ||a||_2 = |a|.$$

We have obvious relations among these norms. For $a \in \mathbb{Z}[x_1, \ldots, x_r]$ it holds

$$\begin{aligned} \|a\|_{\max} &\leq \|a\|_1 && (1)\\ \|a\|_{\max} &\leq \|a\|_2 && (2)\\ \|a\|_1 &\leq n^r \|a\|_{\max} && (3)\\ \|a\|_2 &\leq n^{r/2} \|a\|_{\max} && (4) \end{aligned}$$

Throughout this paper, for $a \in \mathbb{Z}[x_1, \ldots, x_r]$, we will use $L_{\max}(a)$ and $L_1(a)$ to abbreviate length($\|a\|_{\max}$) and length($\|a\|_1$), respectively.

Proposition 2.3. *Let $A, B \in \mathbb{Z}[x_1, \ldots, x_r]$, $n = \max\{\deg_{x_i}(A) | \ i = 1, \ldots, r\}$, $m = \max\{deg_{x_i}(B) | \ i = 1, \ldots, r\}$, and $L_A = L_{max}(A)$, $L_B = L_{max}(B)$. Then we have:*

(i) The worst case complexity for adding A and B is $O(k^r L)$ where $k = \max\{m, n\}$, $L = \max\{L_A, L_B\}$.

(ii) The worst case complexity for multiplying A and B is $O(L_A L_B n^r m^r)$.

(iii) The worst case complexity for computing the pseudoquotient and pseudoremainder of A and B w.r.t. x_r ($\deg_{x_r}(A) \geq \deg_{x_r}(B)$) is

$$O(n^r m^{r-1}(n - m + 1)((n - m + 1)L_B + L_A)L_B).$$

Furthermore, for univariate polynomials the length of the max-norm of quotient and remainder is dominated by $O((n - m + 1)L_B + L_A)$.

Proof. First two assertions are obvious. Let $n_r := \deg_{x_r}(A)$, $m_r := \deg_{x_r}(B)$. Computation of pseudo-quotient and pseudo-remainder can be described by the following recurrence relation:

$$\begin{aligned} A^{(0)} &\leftarrow A \\ A^{(k)} &\leftarrow \mathrm{lc}(B)A^{(k-1)} - x_r^{\deg_{x_r}(A^{(k-1)})-m_r+1} \mathrm{lc}(A^{(k-1)})B \end{aligned}$$

where $k = 1, \ldots, \deg_{x_r}(A) - m_r + 1$. We see that

$$\|A^{(i)}\|_{\max} = O(2^i \|A\|_{\max} \|B\|^i_{\max}).$$

Each loop of the above recurrence requires $O(n)$ multiplications of $(r-1)$-variate polynomials with lengths of max-norms $O((n - m + 1)L_B + L_A)$ and L_B. Combining these results together we get a bound as stated in the theorem. □

Corollary 2.4. *Let A, B be univariate polynomials, $n \geq \max\{\deg(A), \deg(B)\}$, and $e \in \mathbb{N}$. Let $e = \sum_{i=0}^{k} e_i 2^i$ be the binary representation of e, $L_A = L_{max}(A)$, $L_B = L_{max}(B)$. The worst case complexity for computing $C \equiv A^e \mod B$ is*

$$O(n^2 \log e(eL_A + n \log eL_B)^2)$$

Moreover, $L_{max}(C) = O(eL_A + n \log eL_B)$.

Proof. Without loss of generality we may assume $e = 2^k$. We use the well-known algorithm for exponentiation based on repeated squaring. See Algorithm 1.

EXPPOLY(A, B, e)
Input: univariate polynomials A, B, and $e \in \mathbb{N}$, $e = \sum_{i=0}^{k} e_i 2^i$
Output: $A^e \mod B$

1. $S_0 \leftarrow 1$; $T_0 \leftarrow A$;
   for $i = 0$ **to** k **do**
2. **if** $e_i = 1$ **then** $S_i \leftarrow S_{i-1} T_{i-1} \mod B$

3. $T_i \leftarrow T_{i-1}^2 \mod B$
   end

Algorithm 1:

Let us estimate the length of T_i in step 3. We easily obtain $L_{\max}(T_{i-1}^2) = O(\log n + 2L_{\max}(T_{i-1}))$. Using results of Proposition 2.3 we conclude $L_{\max}(T_i) = O(2L_{\max}(T_{i-1}) + nL_B)$. By induction $L_{\max}(T_i) = O(2^i L_A + niL_B)$. Hence upon termination

$$L_{\max}(A^e \mod B) = O(eL_A + n \log eL_B).$$

When counting bit operations we may restrict the analysis to step 3. In the i-th loop, the multiplication costs $O(n^2(2^i L_A + niL_B)^2)$ and computing residuum $O(n^2(nL_B + 2^i L_A + niL_B)L_B)$. The overall complexity is then

$$O(n^2 \log e(eL_A + n \log eL_B)^2).$$

□

We will often need estimates of norms of polynomial divisors. The following lemma can be found in [8].

Lemma 2.5 (Landau-Mignotte-bound). *Let A and C be univariate polynomials with integral coefficients. Moreover let $C = AB$ for some $B \in \mathbb{Z}[x]$. Then*

(i) $||B||_{max} \leq O(2^n ||C||_2) = O(2^n n^{1/2} ||C||_{max}) = O(2^n ||C||_{max})$

(ii) $L_{max}(B) = O(n + L_{max}(C))$

where $n = \deg(C)$.

In the next proposition, we summarize some basic results on polynomial remainder sequences, resultants, polynomial gcd's and on solving linear systems (cf. [1] and others).

Proposition 2.6. *Let $A, B \in \mathbb{Z}[x_1, \ldots, x_r]$, n the maximum degree in any variable of A and B, and $L_{max} := \max\{L_{max}(A), L_{max}(B)\}$. Then the following holds:*

(i) *The worst case complexity of the subresultant chain algorithm over* $\mathbb{Z}[x_1,\ldots,x_{r-1}][x_r]$ *is* $O(n^{2r+2}(r\log n + L_{max})^2)$. *Furthermore, the subresultant coefficients are bounded in length by* $O(n(\log n + L_{max}))$, *and the degree of the k-th subresultant is at most k.*

(ii) *The worst case complexity of Brown's modular gcd algorithm is*

$$O(n^{2r+1}(r\log n + L_{max})^2).$$

(iii) *The worst case complexity of Collins' modular resultant algorithm is*

$$O(n^{2r+1}(r\log n + L_{max}) + n^{2r}(r\log n + L_{max})^2)$$
$$= O(n^{2r+1}(\log n + L_{max}) + n^{2r}(\log n + L_{max})^2)$$

(iv) *The worst case complexity of Bareiss' algorithm for a linear system over* $\mathbb{Z}[x_1,\ldots,x_r]$ *is* $O(k^{2r+5}n^{2r}L^2)$, *where k is the order of the matrix of the system, L is the maximum length of 1-norms of its entries, and n bounds the degrees.*

In the course of parametrization we will have to compute primitive part of polynomials in $\mathbb{Z}[x_1][x_2]$. Thus, we will need bounds for computing the gcd of several polynomials in $\mathbb{Z}[x_1]$.

Corollary 2.7. *Let* $G = \{g_1,\ldots,g_s\}$ *be a set of univariate polynomials over* $\mathbb{Z}$, $\Gamma := \max\{\|g_i\|_{max} \mid g_i \in G\}$, $L := \text{length}(\Gamma)$, *and* $n := \max\{\deg(g_i) \mid g_i \in G\}$. *The worst case complexity for computing* $\gcd(g_1,\ldots,g_s)$ *is*

$$O(sn^3(n^2 + nL + L^2)).$$

Moreover, the max-norm of $\gcd(g_1,\ldots,g_s)$ *if bounded by*

$$\|\gcd(g_1,\ldots,g_s)\|_{max} = O(2^n\Gamma)$$
$$L_{max}(\gcd(g_1,\ldots,g_s)) = O(n+L)).$$

Proof. Without loss of generality we may assume $s = 2^k$ for some k. We will proceed by divide-and-conquer. Using the following recurrence

$$S_j^{(0)} \leftarrow g_j,\ j = 1,\ldots,2^k$$
$$S_j^{(i)} \leftarrow \gcd(S_{2j-1}^{(i-1)}, S_{2j}^{(i-1)}),\ j = 1,\ldots,2^{k-i},\ i = 1,\ldots,k.$$

Upon termination the element $S_1^{(s)}$ will contain the result. In the i-th step 2^{k-i} gcd's of pairs of polynomials are computed. From Lemma 2.5 we see that the max-norm of polynomials in the i-th step is bounded by $O(2^n\Gamma)$ (as they all divide some of g_i's). Using Proposition 2.6 we may bound the number of bit-operations by

$$O(\sum_{i=1}^{k} \frac{s}{2^i} n^3(n+L)^2)).$$

Evaluating the closed form of this sum at $k = \log s$ we get the assertion of the corollary. □

3 Parametrization algorithm

In this section we briefly describe an algorithm for parametrizing plane curves, that we will analyze in next subsections. For further details we refer to [11].

Basically, the parametrization process consists of two parts. First, the standard decomposition of singularities (including the neighboring ones, in general) is determined. In this step, the set of all singularities is decomposed according to their multiplicities. In the course of this process the genus is determined yielding a decision of rationality of the curve. Second, using these informations a rational parametrization is computed.

In the sequel, algorithms corresponding to the two steps from above are outlined. For this purpose, we will assume that the given curve is rational and therefore the algorithm will not compute the genus. The curve is supposed to be in regular position (i.e. no line parallel to axes cut the curve in more than one singularity). This can always be achieved by a suitable change of coordinates (cf. [10]).

3.1 Standard decomposition of singularities

Let K be a field of characteristic zero in which all the field operations can be carried out effectively. The Algorithm 2 on page 122 yields the standard decomposition of the set of singularities.

Remark 3.1. Some steps in the above algorithm have to be clarified theoretically and computationally. In step 5.3. the polynomials $\bar{A}_i$ defining the families of singularities are obtained. The x_1 coordinates of all the corresponding $(i+1)$-fold affine points of C are exactly the roots of $\bar{A}_i$. Then, in step 5.5. x_2-coordinates of singularities are computed. Let p be an irreducible factor of $\bar{A}_i$. As the curve is supposed to be in regular position, for each α with $p(\alpha) = 0$ there is exactly one β such that $(\alpha : \beta : 1)$ is a singular point of F. Hence in each $\mathbb{Q}(\alpha)[x_2]$ ($p(\alpha) = 0$, p being a factor of $\bar{A}_i$) we have $\deg_{x_2} \gcd(f(\alpha, x_2), \frac{\partial f}{\partial x_1}(\alpha, x_2)) = 1$. This verifies the correctness of step 5.5. Finally, the set of $i+1$-fold singularities is described by

$$\{(\alpha \tilde{p}_i(\alpha) : p_i(\alpha) : \tilde{p}_i(\alpha))\}_{\bar{A}_i(\alpha)=0}.$$

In case $\bar{A}_i$ is reducible, more families of singular points may be put together.

Remark 3.2. The output of algorithm SINGULARITY is a family of singular points separated according their multiplicities. Note that $\{(m(\alpha) : n(\alpha) : p(\alpha))\}_{\bar{A}_i(\alpha)=0}$ stands for a set of $\deg(\bar{A}_i)$ of $i+1$-fold points.

Now we are going to analyze the computing time of the algorithm SINGULARITY. Let $F(x_1, x_2, x_3)$ be a homogeneous polynomial defining an algebraic rational plane curve C of degree n, in regular position, and such that

all the singularities of C are ordinary. Note, that the algorithm SINGULARITY works for algebraic curves of any genus. It computes the neighborhood graph of C from which it is then trivial to read off the genus. Thus, at the same time, we obtain a decision procedure for determining the rationality of C. The analysis applies to curves of arbitrary genus.

Theorem 3.3. *Let* $L_F := \text{length}(||F||_{max})$. *The worst case complexity of the algorithm SINGULARITY is* $O(n^{12}(n \log n + L_F)^2)$.

Proof. One has basically to analyze the loop in step 5. The loop in step 5 will be executed at most $O(n)$ times. Let $T_{\text{SING}}(i, j)$ be the time of execution of step $5.j$ in the i-th loop. Then if I denotes the set of all the different multiplicities of points of C it holds

$$T_{\text{SING}} = \sum_{i \in I} \sum_{j=1}^{11} T_{\text{SING}}(i, j).$$

Let us consider now the worst case complexity of the execution of i-th loop in step 5. We may assume to have all derivatives of F precomputed and stored in a table. It can be easily verified that this step does not affect the overall complexity.

Step 5.1. One has to calculate $i + 1$ derivatives of the form $G_k = \frac{\partial^i f}{\partial x_1^k \partial x_2^{i-k}}$, $i + 1$ resultants of the type $R_k = \text{res}_{x_2}(f, G_k)$, and $\gcd(R_0, \ldots, R_i)$. Using Proposition 2.6 we have for $j = 0, \ldots, i$

$$L_{\max}(\frac{\partial^j f}{\partial x_k^j}) = O(i \log n + L_F)$$

$$L_{\max}(\text{res}_{x_k}(f, \frac{\partial^j f}{\partial x_k^j})) = O(n(i \log n + L_F)).$$

Then it follows that the time for computing the $i + 1$ resultants is dominated by $i(n^5(i \log n + L_F) + n^4(i \log n + L_F)^2)$ which is $O(in^5(i \log n + L_F)^2)$. Finally, the time to compute the greatest common divisor is $O(n^6 i(n^4 + n^4(i \log n + L_F) + (n(i \log n + L_F))^2)) = O(in^{10}(i \log n + L_F)^2)$. Hence

$$T_{\text{SING}}(i, 1) = O(in^{10}(i \log n + L_F)^2).$$

Moreover, $L_{\max}(\bar{B}_i) = O(n(i \log n + L_F))$ and $\deg(\bar{B}_i) \leq n^2$.

Step 5.2. Since the modular gcd algorithm of Brown computes the gcd and the cofactors, it holds that the step 5.2. is bounded in time by the time of computing the $\gcd(\bar{B}_i, \bar{B}_i')$. Now, using Proposition 2.6, and the fact that $L_{\max}(\bar{B}_i) = O(n(i \log n + L_F))$, it follows that

$$T_{\text{SING}}(i, 2) = O(n^8(i \log n + L_F)^2).$$

We also observe that, since B_i is a divisor of $\mathrm{res}_{x_2}(f, \frac{\partial^i f}{\partial x_1^i})$, it holds that $\mathrm{length}(B_i) = O(n(i \log n + L_F))$.

Step 5.3. Applying Proposition 2.3, one has that

$$T_{\mathrm{SING}}(i,3) = O(n^6(i \log n + L_F)^2).$$

Step 5.5. Using Proposition 2.6 and that $L_{\max}(\frac{\partial f}{\partial x_1}) = O(\log n + L_F)$, one has that the subresultant computation requires time $O(n^6(\log n + L_F)^2)$. Now, we have to bound the time for computing $\tilde{p}(x_1) \mod \bar{A}_i$ and $p(x_1) \mod \bar{A}_i$. We observe that $\max\{L_{\max}(p_i), L_{\max}(\tilde{p}_i)\} = O(n \log n + nL_F)$ and $\max\{\deg(p_i), \deg(\tilde{p}_i)\} = O(n^2)$. Furthermore for $\bar{A}_i$, we use the fact that $\bar{A}_i$ divides $\mathrm{res}_{x_2}(f, \frac{\partial f}{\partial x_1})$ (all roots of $\bar{A}_i$ are x_1-coordinates of some singularities), and therefore $\deg(\bar{A}_i) \leq n^2$, $L_{\max}(\bar{A}_i) = O(n(n + L_F))$ (Lemma 2.5). Thus applying Proposition 2.3 one concludes that the time for the two divisions is bounded by $O(n^8(\log n + L_F)^2)$. Hence

$$T_{\mathrm{SING}}(i,5) = O(n^8(\log n + L_F)^2)).$$

By the hypothesis all singularities are ordinary hence no expansion of the neighboring tree is needed and step 5.7. does not contribute to the complexity. Then, The worst case complexity for algorithm SINGULARITY can be bounded by

$$T_{\mathrm{SING}} = O(\sum_{i \in I} in^{10}(i \log n + L_F)^2).$$

Thus, since $\sum_{i \in I} i^2 = O(n^2)$,

$$T_{\mathrm{SING}} = O(n^{12}(n \log n + L_F)^2).$$

□

Corollary 3.4. *Let C be a irreducible plane algebraic curve with no neighboring singularities given by a homogeneous polynomial F of degree n. Then the genus of C can be computed in $O(n^{12}(n \log n + L_F)^2)$ bit operations.*

Proof. Using all informations on singularities of C, we have an algorithm for computing the genus. See Algorithm 3 on page 122.

We have $\mathrm{Card}(\mathcal{F}) = O(n^2)$. Hence the running time is dominated by the computation in step 1. □

In the following theorem we summarize some results on singularities which have partially been proved in course of complexity analysis of the algorithm SINGULARITY.

Theorem 3.5. *Let $F \in K[x_1, x_2, x_3]$ be a homogeneous polynomial of degree n defining an algebraic rational plane curve C with only ordinary singularities and let $L_F := L_{max}(F)$. Then, if*

$$\bigcup_{i \in I} \{(m_{i,1}(\alpha) : m_{i,2}(\alpha) : m_{i,3}(\alpha))\}_{A_i(\alpha)=0}$$

is the standard decomposition of the set of singularities $\mathbb{S}(C)$ of C it holds that:

(i) $\deg(A_i) \leq n^2$, $\deg(m_{i,j}) \leq n^2$ *for* $i \in I$, $j = 1, 2, 3$;

(ii) $L_{max}(A_i) = O(n(n + L_F))$ *for* $i \in I$;

(iii) $L_{max}(m_{i,j}) = O(n^3(n + L_F))$ *for* $i \in I$, $j = 1, 2, 3$.

Proof. The first two statements have already been proved in Theorem 3.3. We also saw there, that any polynomial component $m_{i,j}(t)$ in the standard decomposition is congruent modulo $\bar{A}_i(t)$ to a polynomial dominated in length by $O(n(\log n + L_F))$ and in degree by $O(n^2)$. Therefore, using Proposition 2.3, one has that $L_{\max}(m_{i,j}) = O(n^3(n + L_F))$. □

For rational singularities a better upper bound of the length may be given.

Proposition 3.6. *Let $F \in K[x_1, x_2, x_3]$ be a homogeneous polynomial of degree n defining an algebraic plane curve C. Then, the length of any coordinate of any rational singularity of C is bounded by $O(n(\log n + L_{max}(F)))$.*

Proof. Let $f(x_1, x_2) = F(x_1, x_2, 1)$, $R_1(x_1) = \mathrm{res}_{x_2}(f, \frac{\partial f}{\partial x_1})$, and $R_2(x_1) = \mathrm{res}_{x_2}(f, \frac{\partial f}{\partial x_2})$. Then the x_1-coordinate of any rational affine singularity is a common rational root of R_1 and R_2. Therefore, the length of any x_1-coordinate of any rational singularity is bounded by the maximum of the lengths of R_1 and R_2 (cf. [8]),that is $O(n(\log n + L_{\max}(F))$. Similarly, considering resultants w.r.t. x_1 one obtains the same bound for the x_2-coordinates. □

3.2 Parametrization

In this section we design an algorithm for parametrization of plane rational curves with only ordinary singularities. See Algorithm 4 on page 123. Note, that according to Corollary 3.4 we may apply the subsequent algorithm to any irreducible plane curve regardless whether it is rational or not. In a preprocessing step we may determine the genus and refuse any non-rational curve causing no asymptotic increase of computing time. We assume that POINTS(F,k) is an auxiliary algorithm that computes k simple points on the curve given by F over the smallest algebraic extension of K. Here, we do not want to go into details of construction of such algorithm. For a description we refer to [5, 12].

Remark 3.7. We briefly comment some steps of the algorithm. In step 6, H_a is forced to pass through the standard decomposition of the set of singularities with a specified multiplicity. To achieve it, we refer to [11].

The elimination of factors corresponding to fixed common points of the curve and H_a can be done by computing the primitive part of S_1 and S_2 w.r.t. x_2 and x_1, respectively, or explicitly by dividing by these factors, which are known in advance [11].

In the sequel, the complexity of the algorithm PARAMETRIZE is analyzed. For deriving complexity bounds, two different cases are distinguished. First, we consider only curves whose singularities are ordinary and rational. Second, we deal with the most general case that we consider: curves only with ordinary singularities; probably lying on some algebraic extension of the ground field, Furthermore, as we mentioned in the introduction, we do not take care of simple points on curves. We assume that as many simple points as the algorithm PARAMETRIZE needs are given. For actually finding them, we refer to [5], [12].

3.2.1 Rational ordinary singularities

In this subsection we deal with curves having only rational ordinary singularities.

Let $F(x_1, x_2, x_3) \in K[x_1, x_2, x_3]$ be a homogeneous polynomial defining an algebraic rational curve C of degree n, in regular position, and such that all the singularities are ordinary and rational. We consider given simple points $\{R_1, \ldots, R_k\}$ on C with rational coordinates, where $k = (a - n + 2)n + (n - 3)$ for some $a \in \{n-2, n-1, n\}$.

Lemma 3.8. *The worst case complexity for the algorithm PARAMETRIZE, working on rational ordinary singularities, is*

$$O(n^{12}(n \log n + L_F)^2 + n^{12} \max\{L_R, \log n + L_S\}^2)$$

where n is the degree of the curve, $L_F = L_{max}(F)$, L_R is the maximum length of the given rational simple points, and L_S is the maximum length of singularities.

Proof. Let $T_{\text{PARAM}}(i)$ be the time of execution of step i of the algorithm PARAMETRIZE. Then it holds that

$$T_{\text{PARAM}} = \sum_{i=1}^{14} T_{\text{PARAM}}(i).$$

From the Theorem 3.3 it follows that $T_{PARAM}(1) = O(n^{12}(n \log n + L_F)^2)$. Steps 2 and 3 are irrelevant in terms of complexity. Also since $a \leq n$ one has that

$$T_{\text{PARAM}}(5) = O(n^2).$$

In the step 6, let $P_1, \ldots, P_m$ be the singularities of C and $r_1, \ldots, r_m$ the corresponding multiplicities. Let H_a be a generic tri-variate homogeneous polynomial with undetermined coefficients, i.e. $H_a = \sum_{i+j+k=a} c_{ijk} X^i Y^j Z^k$. Then, passing H_a through $\mathcal{F}$, with the specified multiplicities, implies to compute

$$\left\{ \left\{ \frac{\partial^{r_j-2} H_a}{\partial x_1^{i_1} \partial x_2^{i_2} \partial x_3^{i_3}}(P_j) \right\}_{i_1+i_2+i_3=r_j-2} \right\}_{j=1,\ldots,m}.$$

This follows from the fact that i-th derivatives of H_a may be written as linear combinations of $i+1$-st derivatives (this follows from Euler's Theorem, cf. [3], p. 6).

Since the number of terms of each of the $r_j(r_j-1)/2$ polynomials to be evaluated at P_j is $(a-r_j+3)(a-r_j+4)/2$, then the time for the execution is

$$T_{\text{PARAM}}(6) = O(\sum_{j=1}^{m} \frac{r_j(r_j-1)}{2} \frac{(a-r_j+3)(a-r_j+4)}{2} t_j),$$

where t_j is the time for evaluating any monomial $i_1(i_1-1)\cdot\cdots\cdot(i_1-\alpha_1+1)\, i_2(i_2-1)\cdot\cdots\cdot(i_2-\alpha_2+1)\, i_3(i_3-1)\cdot\cdots\cdot(i_3-\alpha_3+1)\, X^{i_1-\alpha_1} Y^{i_2-\alpha_2} Z^{i_3-\alpha_3}$, $i_1+i_2+i_3=a$, $\alpha_1+\alpha_2+\alpha_3=r_j-2$ at P_j. Then t_j is dominated by the time for computing AB^a, where length$(A) = O(r_j \log a)$, and B is the coordinate of P_j with maximum length. The time to compute B^a is dominated by $a \log a \,\text{length}^2(B)$ hence

$$\begin{aligned} t_j &= O(a \log a \,\text{length}(B)^2 + a \,\text{length}(B) r_j \log a) \\ &= O(a \log a \,\text{length}(B)(\text{length}(B) + r_j)) \end{aligned}$$

Hence using $a \le n$ and $\sum_{i=1}^{m} r_j(r_j-1)/2 = (a-1)(a-2)/2$, we obtain

$$T_{\text{PARAM}}(6) = O(n^4 n \log n L_S (L_S + n)) = O(n^5 \log n L_S^2 + n^6 \log n L_S).$$

In the step 7, let t be the time for passing H_a through one simple point $R \in \{R_1, \ldots, R_k\}$. Then $t \le \frac{(n+1)(n+2)}{2} t^*$, where t^* is now the time for evaluating any monomial of H_a at R. Thus, t^* is dominated by the time for computing B^a, where B is the coordinate of R_i of maximum length. Consequently,

$$T_{\text{PARAM}}(7) = O(k n^2 a \log a L_R^2) = O(n^5 \log n L_R^2).$$

In the step 8, if $a = n$ then coordinates of an additional point not on C can always be taken bounded by n (not all points $(k:1:0)$, $k = 0, \ldots, n$, may lie on C). Forcing H_a to pass through $(k:1:0)$ will result in the linear equation $c_{010} + c_{110} k + \cdots + c_{a10} k^a = 0$. The time for computing its coefficients is

$$T_{\text{PARAM}}(8) = O(a^2 \log^2 a) = O(n^2 \log^2 n).$$

In the step 9, a linear system with $O(n^2)$ equations has to be solved. On the other hand the length of the entries in the system is dominated by $O(n \log n + nL_S)$, for rows coming from step 6, and by $O(nL_R)$, if the equation comes from steps 7 or 8. Thus, applying the Proposition 2.6, one has that the time for solving the system is dominated by

$$n^{10} \max\{n \log n + dL_S, nL_R\}^2 = O(n^{12} \max\{L_R, \log n + L_S\}^2)$$

And since the substitution in H_a of the solution takes $O(n^2)$ it follows that

$$T_{\text{PARAM}}(9) = O(n^{12} \max\{L_R, \log n + L_S\}^2).$$

Now, we are interested in the length of the resulting pencil H_a. Then, taking into account that every coordinate of the solutions of a linear system can be expressed as a fraction of determinants, it follows that

$$L_{\max}(H_a) = O(n^3 \max\{L_R, \log n + L_S\})$$

In steps 10 and 11, we first observe that the maximal length of max-norms of polynomials in $\mathbb{Z}[x_1, x_2, t]$ (t being the remaining undetermined coefficient in the solution of the linear system in step 9) involved in the resultants is bounded by $O(\max\{L_F, n^3 D\})$, where $D = \max\{L_R, \log n + L_S\}$. Therefore, applying the Proposition 2.6 one has that both steps are dominated in time by $n^7(\log n + \max\{L_F, n^3 D\}) + n^6 \max\{L_F, n^3 D\}^2$. But, since $n^3 \leq \max\{L_F, n^3 D\}$ it follows that

$$\begin{aligned} T_{\text{PARAM}}(10) \approx T_{\text{PARAM}}(11) &= O(n^7(\log n + \max\{L_F, n^3 D\}) \\ &\quad + n^6(\log n + \max\{L_F, n^3 D\}^2)) \\ &= O(n^6 \max\{L_F, n^3 D\}^2). \end{aligned}$$

On the other hand, from Proposition 2.6 we have that $L_{\max}(S_i) = O(n^2 \max\{L_F, n^3 D\})$.

In the step 12, the quotient of S_i and a polynomial p_i, obtained as the product of all the factors produced by singular and regular points, has to be calculated. The computation of p_i takes $O(n^4 D^2)$, $\deg(p_i) = O(n^2)$ and $\text{length}(p_i) = O(n^2 D)$. Thus

$$T_{\text{PARAM}}(12) = O(n^6 \max\{L_F, n^3 D\}^2).$$

Finally, since the steps 13 and 14 are irrelevant for the complexity analysis, taking in account the result of Theorem 3.3 one concludes that

$$T_{\text{PARAM}} = O(n^{12}(n \log n + L_F)^2 + n^{12} \max\{L_R, \log n + L_S\}^2).$$

□

Remark 3.9.

1. In deriving complexity bounds for the algorithm PARAMETRIZE, in the rational ordinary singularity case, we have not utilized any special simplified version for the algorithm SINGULARITY. We have just applied the Theorem 3.3. A suitable version for rational singularities may reduce the upper bound.

2. In the proof of the previous lemma, we have implicitly assumed that the coordinates of the rational singularities are known, although algorithm SINGULARITIES returns families of points. This is not any loss of generality, since an optional step for detecting them can be inserted in the outline of SINGULARITY, without modifying th complexity bound in the Theorem 3.3

In the last part of this subsection we apply the Proposition 3.6 and the previous lemma to derive an upper bound depending only on the rational simple points.

Theorem 3.10. *The worst case complexity for algorithm PARAMETRIZE, working on rational ordinary singularities, is*

$$O(n^{12}\max\{L_R, n(\log n + L_F)\}^2)$$

where n is the degree of the curve, $L_F = L_{max}(F)$*, and* L_R *bounds the length of the given rational simple points.*

Proof. By Lemma 3.8, we know that $O(n^{12}(n\log n + L_F)^2 + n^{12}\max\{L_R, \log n + L_S\}^2)$ bounds the worst case complexity of the algorithm. By Proposition 3.6 $L_S = O(n(\log n + L_F))$. Combining these bounds we immediately obtain the assertion of the theorem. □

Corollary 3.11. *The worst case complexity of algorithm PARAMETRIZE, working on rational ordinary singularities, is* $O(n^{14}\log^2 n \max\{L_R, L_F\}^2)$.

3.2.2 Standard families of ordinary singularities

This subsection is dedicated to analysis of the complexity in general. We consider curves having only ordinary singularities (i.e. without neighboring ones), possibly lying in some algebraic extensions of the ground field.

Let $F \in K[x_1, x_2, x_3]$ be a homogeneous polynomial defining an algebraic rational curve C in regular position of degree n with only ordinary singularities. We consider $\{R_1, \ldots, R_k\}$ to be given rational simple points on the curve, where $k = (a - n + 2)n + (n - 3)$ and $a \in \{n-2, n-1, n\}$. Then, the following lemma gives an upper bound for the worst case complexity in terms of the degree and the length of the curve, of the rational simple points and of the standard decomposition.

Theorem 3.12. *The worst case complexity for the algorithm PARAMETRIZE is*

$$O(n^{26}(n+L_F)^2 + n^5 \log n L_R^2)$$

where n is the degree of the curve, $L_F = \text{length}(||F||_{max})$, L_R *is the maximum length of coordinates of simple points returned from the procedure POINTS.*

Proof. We will analyze the algorithm PARAMETRIZE allowing the coordinates of singularities to lie in finite extensions of the ground field. Let T_{PARAM} have the same meaning as in the proof of Lemma 3.8. The complexity of first five steps is independent of the type of singularities and has already been determined.

Let $\mathcal{F}_S$ be the standard singularity decomposition computed in step 1. Then $\mathcal{F}_S$ may be written as

$$\mathcal{F}_S = \bigcup_{i \in I} \mathcal{F}_i,$$

where $\mathcal{F}_i = \{(m_i(\alpha), n_i(\alpha), p_i(\alpha))\}_{\bar{A}_i(\alpha)=0}$. In step 6, since $\mathcal{F}_i$ contains $(i+1)$-fold points, passing H_a through $\mathcal{F}_i$ implies to force the polynomials

$$\left\{ \frac{\partial^{i-1} H_a}{\partial x_1^{i_1} \partial x_2^{i_2} \partial x_3^{i_3}} \right\}_{i_1+i_2+i_3=i-1}$$

to vanish on $\mathcal{F}_i$. Therefore, if T_i is the time for forcing one of these $i(i+1)/2$ polynomials to vanish on $\mathcal{F}_i$, it holds that $T_{\text{PARAM}}(6) = O(\sum_{i \in I} i^2 T_i)$. In deriving bounds for T_i, we observe that computing time for obtaining

$$G(t) = \frac{\partial^{i-1} H_a}{\partial x_1^{i_1} \partial x_2^{i_2} \partial x_3^{i_3}}(m_i(t), n_i(t), p_i(t))$$

and $g(t) \equiv G(t) \mod \bar{A}_i(t)$ have to be analyzed. Since $\frac{\partial^{i-1} H_a}{\partial x_1^{i_1} \partial x_2^{i_2} \partial x_3^{i_3}}$ is a polynomial of degree $a-i+1$ with $O(a-i+2)(a-i+3)/2)$ terms, it follows that, as $a \leq n$, $T_i = O(n^2 t_i)$, where t_i is the time for computing $cB(t)^{3n} \mod \bar{A}_i$, with c being an integer of length $O(i \log n)$, $B \in \{m_i, n_i, p_i\}$. Recall (by Theorem 3.5), $L_{\max}(B) = O(n^3(n+L_F))$, $\deg(B) = O(n^2)$, $L_{\max}(\bar{A}_i) = O(n(n+L_F))$, $\deg(\bar{A}_i) = O(n^2)$. Using Corollary 2.4 we obtain $L_{\max}(B(t)^{3n} \mod \bar{A}_i = O(n^4(n+L_F))$ and $t_i = O(n^{10} \log n(n+L_F)^2)$. Hence

$$T_{\text{PARAM}}(6) = O((n^{14} \log n(n+L_F)^2).$$

For steps 7 and 8, reasoning as in the proof of Lemma 3.8, it holds that

$$\begin{aligned} T_{\text{PARAM}}(7) &= O(n^5 \log n L_R^2) \\ T_{\text{PARAM}}(8) &= O(n^2 \log^2 n). \end{aligned}$$

In step 9, linear system of $O(n^2)$ equations has to be solved. Its entries are univariate polynomials $p(t)$ with $L_{\max}(p) = O(n^4(n + L_F))$ (thus also $L_1(p) = O(n^4(n + L_F))$) and $\deg(p) = O(n^2)$. Using Proposition 2.6 we obtain

$$T_{\text{PARAM}}(9) = O(n^{26}(n + L_F)^2).$$

In steps 10 and 11, length of max-norms of polynomials in $\mathbb{Z}[x_1, x_2, t]$ involved in the resultant are bounded by $O(n^4(n + L_F))$, where Applying Proposition 2.6 one has

$$T_{\text{PARAM}}(10) \approx T_{\text{PARAM}}(11) = O(n^{14}(n + L_F)^2)).$$

In step 12 we first compute $\prod(x_1 - \omega_{i,1}(t))$ and $\prod(x_2 - \omega_{i,2}(t))$ where $\omega_{i,1}$ and $\omega_{i,2}$ are first and second coordinates of a singularity of F, respectively. Then an exact division of S_i by these polynomials is performed. Since the degree in x_i is $O(n)$ and the length of max-norm is bounded by $O(n^3(n + L_F))$ (3.5) using Proposition 2.3 we obtain

$$T_{\text{PARAM}}(12) = O(n^{11}(n + L_F)^2).$$

Finally, since steps 13 and 14 are irrelevant in terms of complexity, we conclude

$$T_{\text{PARAM}} = O(n^{26}(n + L_F)^2 + n^5 \log n L_R^2).$$

□

4 Curves with neighboring points

Up to now we considered and analyzed algorithms for curves devoid of complicated singularities, i.e. of those having no neighborhood points. Though curves with complex singularities are encountered very often. In this section we study the classical algorithm for computing the neighborhood tree, give basic analysis of its behavior in terms of complexity, and outline the impact on the algorithm SINGULARITY and PARAMETRIZE.

4.1 Computing neighboring singularities

Now we give a sketch of the algorithm for computing the neighborhood graph for a given absolutely irreducible plane curve. See Algorithm 5 on page 124. As a neighboring singularity is just a usual singularity of a transformed curve we will use the representation as in Section 3.1. Though due to the rather complicated nature of neighboring singularities we will be forced to work in multiple extensions of the underlying field.

Remark 4.1. In the general version of the parametrization algorithm the above procedure will be called in step 5.7. of the algorithm SINGULARITY in Subsection 3.1.

Let us have a closer look at this algorithm. In each recursive call we are computing singular points hence possibly introducing new algebraic extensions. We will examine the two first recursive calls to NEIGHBORHOOD TREE.

(a) Let K be the coefficient domain of the original polynomial F defining the curve. Let P be a singularity of F computed by the algorithm SINGULARITY. Hence

$$P = (m(\alpha) : n(\alpha) : p(\alpha)),\ A(\alpha) = 0$$

where $A(U)$ is a squarefree univariate polynomial (not necessarily irreducible) with a root α. We will mimic the computing in $K[\alpha]$ by performing all computations in $K[U]/(A(U))$. However, care is needed when doing divisions.

(b) In the step 1. of the previous algorithm we set up a transformation T_1 which moves the point $(0:0:1)$ to one singularity. Then T_1 may contain algebraic numbers as coefficients. Following the transformed polynomial F'' has coefficients in $K[\alpha]$. So we have to perform all computations modulo $A(U)$.

(c) Obviously, each recursive call may introduce a new extension of the previously obtained field so that finally we will be computing in $K[\alpha_1, \ldots, \alpha_l]$. All computations in this field will be mimicked in the ring $K[U_1, \ldots, U_l]$ modulo the triangular system of polynomials

$$\begin{aligned} &A_1(U_1) \\ &A_2(U_1, U_2) \\ &\vdots \\ &A_l(U_1, \ldots, U_l). \end{aligned}$$

For the sake of complexity consideration it is important to estimate the depth of the neighborhood graph. As we saw in the Section 3 the number of new variables has an immense impact on the theoretical complexity of the parametrization algorithm. In the sequel we will show that this number may be of the same order as the degree of the curve.

We prove some facts about the depth of the neighborhood graph now.

Theorem 4.2. *There is an infinite family of rational plane curves $\{C_k\}$ where the depth of the neighborhood graph is $\Theta(\deg(C_k))$ (i.e. of the same order as $\deg(C_k)$).*

We will prove some auxiliary lemmas from which the theorem will immediately follow.

Lemma 4.3. *Let* $F_k(X,Y,Z) = X^{2k+1} - Y^2Z^{2k-1}$ *and*

$$\Phi_i^{(k)} = Z^{2k-2i-1}(X+Y)^{2k-2i+1}A_i^{(k)}(X,Y,Z) - (XY)^{2k-1}(X-Y)^2B_i^{(k)}(X,Y,Z) \tag{5}$$

where

$$A_1^{(k)} = 1 \tag{6}$$

$$A_i^{(k)} = A_{i-1}^{(k)}(XY, XY+XZ-YZ, (X+Y)Z)(2XY+XZ-YZ)^{2k-2i+3} \tag{7}$$

$$B_1^{(k)} = 1 \tag{8}$$

$$B_i^{(k)} = B_{i-1}^{(k)}(XY, XY+XZ-YZ, (X+Y)Z)(XY+XZ-YZ)^{2k-1}. \tag{9}$$

Then it holds

(i) For all $k \geq 1$, $C_k = V(F_k)$ *is a parametrizable plane curve.*

(ii) $\Phi_i^{(k)}$ *determines points in the i-th neighborhood of the point* $(0:0:1)$ *on* C_k.

(iii) For all $i \leq k-1$, $\Phi_i^{(k)}$ *has a double non-ordinary point* $(1:1:0)$.

Proof. It is easy to show the rationality of C_k. The transformation $X = T^2$, $Y = T^{2k+1}$, $Z = 1$ yields the desired birational mapping.

In order to verify the second assertion we perform the following changes of coordinates in $\mathbb{P}^2$:

$$\begin{array}{lll} T_1 : X \leftarrow Z & T_2 : X \leftarrow X+Y & T_3 : X \leftarrow YZ \\ \quad Y \leftarrow Y+Z & \quad Y \leftarrow -X+Y & \quad Y \leftarrow XZ \\ \quad Z \leftarrow X & \quad Z \leftarrow Z & \quad Z \leftarrow XY. \end{array}$$

The transformation T_1 moves the point $(0:0:1)$ to $(1:1:0)$, T_2 assures that $\Phi_i^{(k)}$ does not pass through $(1:0:0)$ and $(0:1:0)$, and no axis is a tangent to $\Phi_i^{(k)}$ at $(0:0:1)$. The mapping T_3 is the well known quadratic transformation. Putting them together we obtain

$$\begin{array}{l} T : X \leftarrow XY \\ \quad Y \leftarrow XY+XZ-YZ \\ \quad Z \leftarrow (X+Y)Z. \end{array}$$

First we apply T_1 and then T_3 to C_k getting $\Phi_1^{(k)}$. By induction on i it is not hard to verify Formulae 5 and 6.

For the last assertion of the lemma it is sufficient to consider

$$\frac{\partial \Phi_i^{(k)}(X,1,Z)}{\partial X} \text{ and } \frac{\partial \Phi_i^{(k)}(X,1,Z)}{\partial Z}$$

at $X = 1,\ Z = 0$. It is easy to see that $(1:1:0)$ is exactly a double point on $\Phi_i^{(k)}$, for $1 \le i \le k-1$. □

As we agreed on using multiple extensions whenever an enlargement of the ground field is required every such new extension is represented by a polynomial in one additional variable. From the Theorem 4.2 we see that the computation of the neighborhood graph may extend the ground field several times hence introducing a number of variables asymptotically equivalent to the degree of the curve. The complexity estimates from the Section 2 imply an exponential time growth for the algorithm SINGULARITY and hence for the parametrization when run on curves with neighboring points. This is due to the non-constant number of new variables introduced in the process of expanding the neighborhood graph.

Even though we have an explicit bound for the total number of points in the neighborhood graph of the curve $O(n^2)$, n being the degree of the curve, in the course of the computation we perform arithmetic operations over polynomials with a growing number of variables. In order to stay below a polynomial time bound we would have to require a constant depth of the neighborhood graph of curves under consideration. The Theorem 4.2 shows that this is impossible.

Resuming, we have shown that there is an infinite family of rational curves on which our algorithm takes exponential time in the degree of the curve. Thus no polynomial time bound is possible using algorithms described above to parametrize curves with neighboring points. Only in a special case where the depth of the neighborhood graph is bounded by a constant we may achieve a polynomial running time.

5 Conclusions

Even though the parametrization algorithm is in use for a long time only little was known about its complexity. Mainly due to the prohibitive running time it is not feasible to determine its average behavior by testing it on a large set of data. In this paper, the worst case complexity for the special case of curves lacking neighboring singularities has been proved. Practical examples reveal that the worst case complexity determined in this paper is too pessimistic for most cases (curves of degree 10 have been parametrized in a reasonable amount of time). This is partially due to the high estimate for the length of coordinates of singularities. If this parameter was taken as an input measure, finer theoretical complexity could be obtained and also some bounds observed in practical computations might be matched closely.

In the course of the analysis of parametrization algorithm we obtained an estimate for the time needed to determine the genus of an irreducible curve and an algorithm to decompose the set of singularities.

Moreover, we have shown that allowing neighboring points may considerably increase the amount of time needed to parametrize curves. It turns out that using strategies described in this paper the time to parametrize a curve may be exponential in the degree of the input curve.

All algorithms described in this paper were implemented in the Maple package CASA ([9]) developed at the Research Institute for Symbolic Computation, Linz, Austria.

References

[1] B. Buchberger, G. E. Collins, and R. Loos. *Computer Algebra; Symbolic and Algebraic Computation.* Springer Verlag Wien–New York, second edition, 1982.

[2] G. E. Collins, M. Mignotte, and F. Winkler. Arithmetic in basic algebraic domains. In *Computer Algebra; Symbolic and Algebraic Computation* [1], pages 184–220.

[3] W. Fulton. *Algebraic Curves.* Addison–Wesley, 1989.

[4] R. Gebauer, M. Kalkbrener, B. Wall, and F. Winkler. CASA: A Computer Algebra Package for Constructive Algebraic Geometry. In S. M. Watt, editor, *ISSAC 91*, pages 403–410, Bonn, Germany, July 1991. ACM Press.

[5] D. Hilbert and A. Hurwitz. Über die Diophantischen Gleichungen vom Geschlecht Null. *Acta Math.*, pages 217–224, 1890.

[6] D. E. Knuth. *The Art of Computer Programming: Seminumerical Algorithms*, volume 2. Addison–Wesley, second edition, 1981.

[7] R. Loos. Generalized polynomial remainder sequences. In *Computer Algebra; Symbolic and Algebraic Computation* [1], pages 115–137.

[8] M. Mignotte. Some useful bounds. In *Computer Algebra; Symbolic and Algebraic Computation* [1], pages 259–263.

[9] M. Mňuk, B. Wall, and F. Winkler. CASA reference manual (version 2.2). Technical Report 95-05, Research Institute for Symbolic Computation, Linz, Austria, 1995. See also *http://info.risc.uni-linz.ac.at:/labs-info/compal/software/casa/casa.html.*

[10] T. Sakkalis and R. Farouki. Singular points of algebraic curves. *J. Symb. Comput.*, 9:405–421, 1990.

[11] J. R. Sendra and F. Winkler. Symbolic parametrization of curves. *J. Symb. Comput.*, 12(6):607–631, 1991.

[12] J. R. Sendra and F. Winkler. Determining simple points on rational algebraic curves. Technical Report RISC-93-23, Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria, 1993.

SINGULARITY(F)
Input: $F \in K[x_1, x_2, x_3]$ - defining homogeneous polynomial of an irreducible plane curve C of degree n in regular position
Output: standard decomposition of singularities

1. $\mathcal{F} \leftarrow \emptyset$;
2. $f \leftarrow F(x_1, x_2, 1)$; $B_1 \leftarrow f$;
3. $\bar{B}_1 \leftarrow \gcd(\mathrm{res}_{x_2}(f, \frac{\partial f}{\partial x_1}), \mathrm{res}_{x_2}(f, \frac{\partial f}{\partial x_2}))$;
4. $B_1 \leftarrow \frac{\bar{B}_1}{\gcd(\bar{B}_1, \bar{B}_1')}$;
5. **for** $i \geq 2$ **while** $\deg(B_{i-1}) > 0$ **do**
5.1. $\bar{B}_i \leftarrow \gcd(\mathrm{res}_{x_2}(f, \frac{\partial^i f}{\partial x_1^i}), \ldots, \mathrm{res}_{x_2}(f, \frac{\partial^i f}{\partial x_2^i}))$;
5.2. $B_i \leftarrow \frac{\bar{B}_i}{\gcd(\bar{B}_i, \bar{B}_i')}$;
5.3. $\bar{A}_{i-1} \leftarrow \frac{B_{i-1}}{B_i}$;
5.4. **if** $\deg(\bar{A}_{i-1}) > 0$ **then**
5.5. $q_{i-1}(x_2) \leftarrow \tilde{p}_{i-1}(x_1)x_2 - p_{i-1}(x_1) = \mathrm{subres}_1(f(x_1, x_2), \frac{\partial f}{\partial x_1}(x_1, x_2), x_2) \mod \bar{A}_{i-1}(x_1)$;
5.6. $\mathcal{F}_{i-1}^* \leftarrow \{(\alpha, p_{i-1}(\alpha), 1)\}_{\bar{A}_{i-1}(\alpha)=0}$;
5.7. determine the expanded neighboring graph $\mathcal{F}_{i-1}$ of $\mathcal{F}_{i-1}^*$;
5.8. $\mathcal{F} \leftarrow \mathcal{F} \cup \mathcal{F}_{i-1}$;
end
5.9. $i \leftarrow i + 1$;
end
6. **repeat** the process, dehomogenizing w.r.t. x_2 and then w.r.t. x_1;
7. **return** $\mathcal{F}$

Algorithm 2:

GENUS($\mathcal{F}$)

1. $\mathcal{F} \leftarrow$SINGULARITY(C); $g \leftarrow 0$;
for all $S \in \mathcal{F}$ **do**
2. $m \leftarrow \mathrm{multiplicity}(S)$; $g \leftarrow g + m(m-1)/2$;
end
return $(n-1)(n-2)/2 - g$;

Algorithm 3:

PARAMETRIZE(C)
Input: $F \in K[x_1, x_2, x_3]$ - homogeneous polynomial defining an irreducible rational curve C of degree n
Output: rational parametrization of C

1. $\mathcal{F} \leftarrow$ SINGULARITY(F);
2. choose $a \in \{n-2, n-1, n\}$;
3. $k \leftarrow (a-n+2)n + (n-3)$;
4. $\{R_1, \ldots, R_k\} \leftarrow$ POINTS(F, k);
5. $H_a(x_1, x_2, x_3)$ is a linear system of curves of degree a with undetermined coefficients;
6. pass $H_a(x_1, x_2, x_3)$ through $\mathcal{F}$, such that, if P is an r-fold point in $\mathcal{F}$ (including the neighboring one), then P has multiplicity $r-1$ on H_a;
7. pass $H_a(x_1, x_2, x_3)$ through regular points $\{R_1, \ldots, R_k\}$;
8. **if** $a = n$ **then** pass H_a through an additional point not on C;
9. solve the linear system of equations in the undetermined coefficients of H_a created in steps 6, 7 and 8, and substitute the solution in H_a;
10. $S_1(x_2) \leftarrow \mathrm{res}_{x_1}(F(x_1, x_2, 1), H_a(x_1, x_2, 1))$;
11. $S_2(x_1) \leftarrow \mathrm{res}_{x_2}(F(x_1, x_2, 1), H_a(x_1, x_2, 1))$;
12. remove the factors in S_1 and S_2 coming from fixed intersections of F and H_a;
13. solve the linear system of equations $\{S_1(x_2) = 0, S_2(x_1) = 0\}$, where x_1, x_2 are the unknowns. Say that $(R_1(t), R_2(t))$ is the solution;
14. **return** $(R_1(t), R_2(t))$

Algorithm 4:

NEIGHBORHOOD TREE(P)
Input: A singular point P of a curve
Output: Neighborhood tree rooted in P

1. determine a change of coordinates T_1 moving the projective point $(0:0:1)$ to P;
2. determine a change of coordinates T_2 such that $F' = F \circ T_1 \circ T_2$ contains $(0:0:1)$ but none of $(1:0:0)$, $(0:1:0)$ and such that no axis is tangent at $(0:0:1)$ to F';
3. perform the quadratic transformation on F' centered at $(0:0:1)$ yielding a new curve F'';
4. compute the set $\mathcal{S}$ of singularities on $F'' \cap V(Z)$;
5. **for all** $R \in \mathcal{S}$ **do**
6. call NEIGHBORHOOD TREE recursively on R;

end

Algorithm 5:

Bibliography

[AB88a] Sheeram S. Abhyankar and Chanderjit L. Bajaj. Automatic parametrization of rational curves and surfaces III: Algebraic plane curves. *Comput. Aided Geom. Design*, (5):309–321, 1988.

[AB88b] Sheeram S. Abhyankar and Chanderjit L. Bajaj. Automatic parametrization of rational curves and surfaces IV: Algebraic space curves. Technical report, Computer Science Department, Purdue University, West Lafayette, Indiana, U.S.A., Feb 1988.

[AB89] Sheeram S. Abhyankar and Chanderjit L. Bajaj. Computations with algebraic curves. In *Symbolic and Algebraic Computation, ISSAC'88*, volume 358 of *Lecture Notes in Computer Science*, pages 274–284. Springer Verlag, 1989.

[Abh69] Sheeram S. Abhyankar. A glimpse of algebraic geometry. Lecture notes, 1969. Lokamanya Tilak Memorial Lecture.

[Abh74] Sheeram S. Abhyankar. Lectures in algebraic geometry. Lecture notes, Univ. of Minnesota and Purdue Seminar., 1974.

[Abh76] Sheeram S. Abhyankar. Historical ramblings in algebraic geometry and related algebra. *Amer. Math. Monthly*, 83(6):409–448, 1976.

[Abh83] Sheeram S. Abhyankar. Desingularization of plane curves. *Proceedings of Symposia in Pure Mathematics*, 40:1–45, 1983. Part 1.

[Abh90] Sheeram S. Abhyankar. *Algebraic Geometry for Scientists and Engineers*. Number 35 in Mathematical surveys and monographs. American Mathematical Society, 1990.

[AMNR92] M. E. Alonso, T. Mora, G. Niesi, and M. Raimondo. Local parametrization of space curves at singular points. Technical report, Falcutad de CC. Matemáticas, Universidad Computense, Madrid and Dpto. di Matematica, Università di Genova, Genova, 1992.

[AS74] Sheeram S. Abhyankar and A. M. Sathaya. *Geometric Theory of Algebraic Space Curves*, volume 423 of *Lect. Notes in Math.* Springer–Verlag, 1974.

[Bal86] V. Baladi. Calculs systématiques pour les singularités de courbes planes (computations on the singularities of plane curves) (in french). Master's thesis, Section de Mathématiques, Univerité de Genève, 1986.

[BK86] E. Brieskorn and H. Knörrer. *Plane Algebraic Curves*. Birkhäuser Verlag, 1986.

[Bli33] Gilbert Ames Bliss. *Algebraic Functions*. Number XVI in Colloquium Publications. Amer. Math. Soc., 1933.

[BM91] Edward Bierstone and Pierre D. Milman. A simple constructive proof of canonical resolution of singularities. In T. Mora and C. Traverso, editors, *Effective Methods in Algebraic Geometry*, volume 94 of *Progress in Mathematics*, pages 11–30. Birkhäuser, 1991.

[BV93] Joseph P. Brennan and Wolmer V. Vasconcelos. Effective computation of the integral closure of a morphism. *J. Pure Appl. Algebra*, 86:125–134, 1993.

[Che78] A. Chenciner. Courbes algebriques planes (plane algebraic curves) (in french). Publications mathematiques de l'universite paris vii, Universite de Paris VII, Paris, France, 1978.

[DD84] Claire Dicrescenzo and Dominique Duval. Computation on curves. In *Symbolic and Algebraic Computation, EUROSAM'84*, volume 174 of *LNCS*, pages 100–107. Springer-Verlag, 1984.

[DD89] Claire Dicrescenzo and Dominique Duval. Algebraic extensions and algebraic closure in scratchpad ii. In P. Gianni, editor, *International Symposion on Symbolic and Algebraic Computation, ISSAC'88*, Rome, Italy, 1989.

[DDDD85] Jean Della Dora, Claire Dicrescenzo, and Dominique Duval. About a new method for computing in algebraic number fields. In B. Caviness, editor, *European Conference on Computer Algebra*, volume 204 of *Lect. Notes in Comput. Sci.*, Linz, Austria, 1985. Springer-Verlag.

[Dim87] A. Dimca. *Topics on Real and Complex Singularities. An Introduction.* Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Wiesbaden, 1987.

[Ful89] William Fulton. *Algebraic Curves.* Addison–Wesley, 1989.

[Gor52] Daniel Gorenstein. An arithmetic theory of adjoint plane curves. *Trans. Amer. Math. Soc.*, 1952.

[GSA84] R. N. Goldman, T. W. Sederberg, and D. C. Anderson. Degenerate parametric curves. *Comput. Aided Geom. Design*, 1(4):327–356, 1984.

[HB] Gaétan Haché and Dominique Le Brigand. Effective constructions of algebraic geometry codes. To be published.

[HH90] D. Hilbert and A. Hurwitz. Über die Diophantischen Gleichungen vom Geschlecht Null. *Acta Math.*, pages 217–224, 1890.

[HM87] J. P. G. Henry and M. Merle. Complexity of computation of embedded resolution of algebraic curves. In J. H. Davenport, editor, *European Conference on Computer Algebra*, volume 378 of *LNCS*, pages 381–390, Leipzig, Germany, Jun 1987.

[IR82] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 1982.

[Koz94] Dexter Kozen. Efficient resolution of singularities of plane curves. In *14th Conf. Foundation of Software Technology and Theoretical Computer Science*. Madras, India, December 1994.

[KS92] H. Kobayashi and H. Suzuki. The multiplicity of a solution of a system of algebraic equations. Technical report, Deptartment of Mathematics, Nihon University, Tokyo, and Tokyo Polytechnic College, 1992.

[Mňu95a] Michal Mňuk. Computing adjoint curves (an algebraic approach). Technical Report 95–43, Research Institute for Symbolic Computation, October 1995.

[Mňu95b] Michal Mňuk. Computing adjoint curves (geometric and algebraic approach). Talk at CoCoA workshop. Genova. Italy, May 29 – June 2 1995.

[Mor90] G. Moreno. Lazy resolution of plane curves. In Sakata, editor, *International Conference on Applied Algebra, Algebraic Algorithms and Error Correction Codes*, volume 508 of *Lect. Notes in Comput. Sci.*, Tokyo, Japan, 1990.

[MSW94] Michal Mňuk, J. Rafael Sendra, and Franz Winkler. On the complexity of parametrizing curves. Technical Report 94–45, Research Institute for Symbolic Computation, 1994.

[MWW95] Michal Mňuk, Bernhard Wall, and Franz Winkler. CASA reference manual (version 2.2). Technical Report 95-05, Research Institute for Symbolic Computation, Linz, Austria, 1995. See also *http://info.risc.uni-linz.ac.at:/labs-info/compal/software/casa/casa.html*.

[PHMW93] Despina Polemi, M. Hassner, Oscar Moreno, and C. J. Williamson. A computer algebra algorithm for the adjoint divisor. In *IEEE International Symposium on Information Theory*, page 358, San Antonio, Texas, U.S.A., 1993.

[PMM] Despina Polemi, Carlos J. Moreno, and Oscar J. Moreno. Search and construction of good a.g. goppa codes. To be published.

[PMM92] Despina Polemi, Carlos Moreno, and Oscar Moreno. Search and construction of good a.g. goppa codes. Preprint, 1992.

[Pol] Despina Polemi. Computing the adjoint divisor over finite fields. Preprint.

[RS95] Thomas Recio and J. Rafael Sendra. Real reparametrization of real curves. In *International Symposia on Symbolic and Algebraic Computation*, 1995.

[Sch95] Josef Schicho. Adjoints and conductors. Private communication, 1995.

[Sed86] Thomas W. Sederberg. Improperly parametrized rational curves. *Comput. Aided Geom. Design*, 3(1):67–75, 1986.

[Sei74] A. Seidenberg. Constructions in algebra. *Trans. Amer. Math. Soc.*, 197:273–313, 1974.

[SF90] T. Sakkalis and R. Farouki. Singular points of algebraic curves. *J. Symb. Comput.*, 9:405–421, 1990.

[Sha94] Igor A. Shafarevich. *Basic Algebraic Geometry*, volume 1. Springer Verlag, second edition, 1994.

[Sko94] V. V. Skohurov. Riemann surfaces and algebraic curves. In I. R. Shafarevich, editor, *Algebraic Geometry*, volume 23 of *Encyclopaedia of Mathematica Sciences*, pages 1–166. Springer-Verlag, 1994.

[Sør91] Anders B. Sørensen. A note on algorithms deciding rationality and absolute irreducibility based on the number of rational solutions. Technical Report 91-37, Research Institute for Symbolic Computation, Aug 1991.

[SS92] Josef Schicho and J. Rafael Sendra. On the choice of pencils in the parametrization of curves. *J. Symb. Comput.*, 14:557–576, 1992.

[Sti93] Henning Stichtenoth. *Algebraic Function Fields and Codes*. Springer Verlag, 1993.

[Sto68] Gabriel Stolzenberg. Constructive normalization of an algebraic variety. *Bull. Amer. Math. Soc. (N.S.)*, 74:595–599, 1968.

[SW91] J. Rafael Sendra and Franz Winkler. Symbolic parametrization of curves. *J. Symb. Comput.*, 12(6):607–631, 1991.

[SW93] J. Rafael Sendra and Franz Winkler. Determining simple points on rational algebraic curves. Technical Report RISC-93-23, Research Institute for Symbolic Computation, Johannes Kepler University, Linz, Austria, 1993.

[Tei90] Jeremy Teitelbaum. On the computational complexity of the resolution of plane curve singularities. *Math. Comp.*, (54):797–837, 1990.

[Tra84] Barry M. Trager. *Integration of Algebraic Functions*. PhD thesis, Massachusetts Institute of Technology, Cambrigde, MA, September 1984.

[Tra95] Barry M. Trager. Computation of adjoints for approximate curves. Talk at CoCoA workshop, May 29 – June 2 1995.

[Vas91] Wolmer V. Vasconcelos. Computing the integral closure of an affine domain. *Proc. Amer. Math. Soc.*, 113(3):633–638, 1991.

[vH] Mark van Hoeij. An algorithm for computing an integral basis in an algebraic function field. Description of the IntBasis package contained in the Maple share library.

[vH94] Mark van Hoeij. Computing parametrizations of rational algebraic curves. In *ISSAC*, 1994.

[Wal50] Robert J. Walker. *Algebraic Curves*. Princeton University Press, 1950.

[ZS75] Oscar Zariski and Pierre Samuel. *Commutative Algebra*, volume 1. Springer Verlag, 1975.